[+] (IN)SECURE Magazine

11 | 2020

ISSUE 67

Reducing risk

Hardware security: Emerging attacks and protection mechanisms

Justifying your 2021 cybersecurity budget

Cooking up secure code: A foolproof recipe for open source

Table of contents

Featured experts

GERALD BEUCHELT, CISO, LogMeIn
ADENIKE COSGROVE, Cybersecurity Strategy, International, Proofpoint
TONI GRZINIC, Security Researcher
MAX HENDERSON, Incident Response Lead and Senior Security Analyst, Pondurance
TONIMIR KISASONDI, Co-founder, Apatura
APU PAVITHRAN, CEO, Hexnode
KAREN WALSH, CEO, Allegro Solutions
LIOR YAARI, CTO, YL Ventures
STEVEN ZIMMERMAN, Open Source Strategist, Checkmarx

Visit the magazine website and subscribe at www.insecuremag.com

Mirko Zorz
Editor in Chief
mzorz@helpnetsecurity.com

Zeljka Zorz
Managing Editor
zzorz@helpnetsecurity.com

Berislav Kucan
Director of Marketing
bkucan@helpnetsecurity.com

Cooking up secure code: A foolproof recipe for open source

AUTHOR_Steven Zimmerman, Open Source Strategist, Checkmarx

The use of open source code in modern software has become nearly ubiquitous. It makes perfect sense: facing ever-increasing pressures to accelerate the rate at which new applications are delivered, developers value the ready-made aspect of open source components which they can plug in where needed, rather than building a feature from the ground up. Indeed, this practice has become so common that today the average application is composed mostly of open source libraries, with these components making up more than 80% of the average codebase.

> *Open source code is distinct from custom code, however, in that its vulnerabilities – and many exploits for them – are published online, making it a particularly attractive target for malicious actors.*

But the widespread use of open source code has consequences. As with custom or home-grown code, open source libraries can contain vulnerabilities, and those vulnerabilities may be exploited by cybercriminals as attack vectors to gain access to networks, intercept sensitive data, and influence or impede an application's functionality. Open source code is distinct from custom code, however, in that its vulnerabilities – and many exploits for them – are published online, making it a particularly attractive target for malicious actors.

Calling all "chefs"

Any software developer knows that sometimes solving a problem is as simple as changing one's perspective on the approach, which is why I'd like to introduce the "chef" analogy. It is often said that building software is like cooking fine cuisine. When cooking in your kitchen, you probably use some of your own know-how, a combination of recipes you've researched, and some premade ingredients that would simply be impractical to make on your own when you can get a better version off-the-shelf. Building software that uses open source code follows much the same formula. With this understanding, we can better visualize an approach to how to secure software in the age of open source, as a combination of selecting the right recipe, understanding your ingredients, and having the right tools and utensils in your "kitchen" to get the job done.

Finding the recipe

When getting ready to make a new dish, or in this case application, a common practice is to research a "recipe" as a starting point. Some "recipes" will yield better results than others, and the same applies to open source components.

Even if two components have the same name, they can be very different depending on which organization or developer community has created them, or the various iterations and forks which they have experienced. While they might share similar purpose or functionality, these components might contain slight changes that reflect the needs or preferences of the people who influenced their evolution. A good example of this is the difference between Red Hat Enterprise Linux and Ubuntu. In practice, these slight differences can add up to create a significant impact on functionality, compatibility, and security, and thus must be considered when researching which "recipe" to follow.

> *The equipment in a developer's software "kitchen" is a key factor in whether or not the code they produce is secure and of high quality.*

Choosing the best ingredients

As mentioned, vulnerabilities in open source components mean vulnerabilities in the software that leverages them. Therefore, just as it is important to know that the ingredients you're using when cooking have not spoiled, it is essential to understand any existing vulnerabilities in the open source components being used. Ingredients that have gone bad can ruin what would otherwise be a perfectly good dish and, likewise, vulnerable open source components can ruin an otherwise secure application.

As with ingredients and food products, some vendors will issue recalls for bad batches.
When using open source libraries from known organizations like Red Hat or Apache, for example, developers may receive "recall" notices by way of alerts about new vulnerabilities or patches which address security risks in the software they provide. It is quite possible, however, that a developer may need a community-driven component rather than one supported by large enterprises. In this instance,

the responsibility to identify and fix vulnerabilities falls on the developers. This is much easier said than done, as it is one thing to bear the burden of identifying and resolving these vulnerabilities by developing a new component version, and it is another to communicate the need to address the vulnerabilities to everyone using the vulnerable component version. Getting this done efficiently ultimately comes down to having the right equipment on hand.

> *Applications must be reviewed, then reviewed again to ensure that nothing has been missed.*

Let “utensils” help

Just as some recipes will call for the use of a mixer while specifying that a whisk can be substituted at the cost of time, efficiency, and effectiveness, software being developed with open source code calls for its own tools to maximize quality.

The equipment in a developer’s software “kitchen” is a key factor in whether or not the code they produce is secure and of high quality. When open source code is in use, software composition analysis (SCA) tools are preferred for this.

SCA refers to the process of analyzing software, detecting the open source components within and identifying associated risks, including security risks and license risks. Security risk refers to vulnerabilities that can be tracked in publicly available databases such as the National Vulnerability Database (NVD) or discovered by private security research teams. License risk can be a function of unfavorable license requirements associated with a particular component, the failure to comply with license requirements, or conflicts between unique licenses for different components within the same software project.

SCA solutions help developers by detecting open source components, giving insights into any associated vulnerabilities, and providing actionable information around risk and remediation.

They also need to work well with other “appliances,” such as other security, development, and issue management tools. With the right SCA tool on hand, developers leveraging open source code can be sure that the software they ship will be much more secure.

Cooking up a masterpiece

It’s always important to acknowledge that there is no silver bullet when it comes to software security, and open source is no exception.

Keeping software secure is always going to take careful attention and diligence. Applications must be reviewed, then reviewed again to ensure that nothing has been missed.

Even if a developer follows all best practices, vulnerabilities can persist, or new vulnerabilities may emerge for previously released software.

By following the advice laid out above, developers using open source code have a greater chance to be able to approach the challenge with a fresh perspective and understanding, increasing their open source security and serving software masterpieces in no time.

Hardware security: Emerging attacks and protection mechanisms

AUTHOR_ Mirko Zorz, Editor in Chief, (IN)SECURE Magazine

Maggie Jauregui's introduction to hardware security is a fun story: she figured out how to spark, smoke, and permanently disable GFCI (Ground Fault Circuit Interrupter – the two button protections on plugs/sockets that prevent you from electrocuting yourself by accident with your hair dryer) wirelessly with a walkie talkie.

"I could also do this across walls with a directional antenna, and this also worked on AFCI's (Arc Fault Circuit Interrupts – part of the circuit breaker box in your garage), which meant you could drive by someone's home and potentially turn off their lights," she told (IN)SECURE Magazine.

This first foray into hardware security resulted in her first technical presentation ever at DEF CON and a follow up presentation at CanSecWest about the effects of radio waves on modern platforms.

Jauregui says she's always been interested in hardware. She started out as an electrical engineering major but switched to computer science halfway through university, and ultimately applied to be an Intel intern in Mexico.

> *Hardware-based security typically refers to the defenses that help protect against vulnerabilities targeting these devices, and its main focus it to make sure that the different hardware components working together are architected, implemented, and configured correctly.*

"After attending my first hackathon — where I actually met my husband — I've continued to explore my love for all things hardware, firmware, and security to this day, and have been a part of various research teams at Intel ever since," she added. She's currently a security researcher for Intel's PSG (Programmable Solutions Group) organization.

What do we talk about when we talk about hardware security?

Computer systems – a category that these days includes everything from phones and laptops to wireless thermostats and other "smart" home appliances – are a combination of many hardware components (a processor, memory, i/o peripherals, etc.) that together with firmware and software are capable of delivering services and enabling the connected data-centric world we live in.

Hardware-based security typically refers to the defenses that help protect against vulnerabilities targeting these devices, and its main focus it to make sure that the different hardware components working together are architected, implemented, and configured correctly.

"Hardware can sometimes be considered its own level of security because it often requires physical presence in order to access or modify specific fuses, jumpers, locks, etc.," Jauregui explained. This is why hardware is also used as a root of trust.

Hardware security challenges

But every hardware device has firmware – a tempting attack vector for many hackers. And though the industry has been making advancements in firmware security solutions, many organizations are still challenged by it and don't know how to adequately protect their systems and data, she says.

She advises IT security specialists to be aware of firmware's importance as an asset to their organization's threat model, to make sure that the firmware on company devices is consistently updated, and to set up automated security validation tools that can scan for configuration anomalies within their platform and evaluate security-sensitive bits within their firmware.

> *Every hardware device has firmware – a tempting attack vector for many hackers.*

"Additionally, Confidential Computing has emerged as a key strategy for helping to secure data in use," she noted. "It uses hardware memory protections to better isolate sensitive data payloads. This represents a fundamental shift in how computation is done at the hardware level and will change how vendors can structure their application programs."

Finally, the COVID-19 pandemic has somewhat disrupted the hardware supply chain and has brought to the fore another challenge.

"Because a computing system is typically composed of multiple components from different manufacturers, each with its own level of scrutiny in relation to potential supply chain attacks, it's challenging to verify the integrity across all stages of its lifecycle," Jauregui explained.

"This is why it is critical for companies to work together on a validation and attestation solution for hardware and firmware that can be conducted prior to integration into a larger system. If the industry as a whole comes together, we can create more measures to help protect a product through its entire lifecycle."

There is no single blanket solution approach to implement security of embedded systems.

Achieving security in low-end systems on chips

The proliferation of Internet of Things devices and embedded systems and our reliance on them should make the security of these systems extremely important.

As they commonly rely on systems on chips (SoCs) – integrated circuits that consolidate the components of a computer or other electronic system on a single microchip – securing these devices is a different proposition than securing "classic" computer systems, especially if they rely on low-end SoCs.

Jauregui says that there is no single blanket solution approach to implement security of embedded systems, and that while some of the general hardware security recommendations apply, many do not.

"I highly recommend readers to check out the book Demystifying Internet of Things Security written by Intel scientists and Principal Engineers. It's an in depth look at the threat model, secure boot, chain of trust, and the SW stack leading up to defense-in-depth for embedded systems. It also examines the different security building blocks available in Intel Architecture (IA) based IoT platforms and breaks down some the misconceptions of the Internet of Things," she added.

"This book explores the challenges to secure these devices and provides suggestions to make them more immune to different threats originating from within and outside the network."

For those security professionals who are interested in specializing in hardware security, she advises being curious about how things work and doing research, following folks doing interesting things on Twitter and asking them things, and watching hardware security conference talks and trying to reproduce the issues.

"Learn by doing. And if you want someone to lead you through it, go take a class! I recommend hardware security classes by Joe FitzPatrick and Joe Grand, as they are brilliant hardware researchers and excellent teachers," she concluded.

How can the C-suite support CISOs in improving cybersecurity?

AUTHOR_Gerald Beuchelt, CISO, LogMeIn

> *The shared responsibility in security is closely tied to how employees at all levels perceive the importance of security.*

Among the individuals charged with protecting a company's information security, the CISO is typically seen as the executive for the job. That said, the shift to widespread remote work has made a compelling case for the need to bring security within the remit of other departments.

The pandemic has torn down physical office barriers, opening businesses up to countless vulnerabilities as the number of attack vectors increased. The reality is that every employee is a potential vulnerability and, with the security habits of workers remaining questionable even amid a rising number of data breaches, it's never been more important to foster a culture of security throughout an organization.

Improving security with culture

We continue to see different data breaches in the news, with hundreds of millions of users on Instagram, TikTok and YouTube having their accounts compromised in the latest breach. These instances, and countless others, are a testament to the critical importance of strong security behaviors - both at work and home - and the training and attentiveness they require.

> *While CISOs continue to spearhead the development of the organization's security program and define the security mission and culture, other C-suite executives can vocally support these programs.*

The shared responsibility in security is closely tied to how employees at all levels perceive the importance of security. If this is ingrained within the culture, they will have the abilities and tools to protect themselves. This is, of course, easier said than done.

Creating and maintaining a security culture is a never-ending and constantly evolving mission and influencing people's behavior is often the most challenging part of the effort. People have become numb to the security threats they face, and although they understand the potential risks, they don't do anything about it. For example, recent research revealed that 92 percent of UK workers know that using the same password over and over is risky, but 64 percent of the respondents do it anyway. So, how do we get through that dissonance and get people engaged in security?

Encouraging cyber-secure practices from the top

As security continues to grow in importance, organizations absolutely need an executive at the top to vocally and adamantly advocate for security.

CISOs typically lead this charge. They are often tasked with leading a security team and a program responsible for protecting all information assets, as well as ensuring disaster recovery, business continuity and incident response plans are in place and regularly tested. In addition, CISOs and their teams are usually responsible for evaluating new technologies, staying updated on compliance regulations, overseeing identity and access management, communicating risks and security strategies to the C-suite and providing trainings.

Today, CISOs are also focused on protecting a highly distributed workforce and customers - in offices, at home or a mix of both – and meeting the new security challenges and threats that come along with this hybrid environment. That's why it's more important than ever for other C-suite executives to help promote and drive the organization's security culture, especially through communications, training and enforcement of best practices.

While CISOs continue to spearhead the development of the organization's security program and define the security mission and culture, other C-suite executives can vocally support these programs to ensure their integrity throughout the whole process, from vision and development to implementation and ongoing enforcement.

The participation of the C-suite can also help CISOs focus on the most important security issues and adjust the program to ensure it is aligned with broader business plans and strategies, thereby helping to get broader support without compromising security.

One likely companion for this type of cross-department alignment is the Chief Operating Officer (COO). As this role typically reports directly to the CEO and is considered to be second in the chain of command, the COO will be able to provide the authority needed to advocate for security and how it can impact employees, customers, products and ultimately the business. This means a good COO today needs to encourage a business culture that supports security efforts thoroughly, while also ensuring security is prioritized at a tactical level.

> *The COO can better incorporate input from the board, which is vital to ensuring the CISO understands the company's risk tolerance which will directly impact innovation and revenue.*

However, the COO is not the only one that needs to serve as a security advocate. All C-level executives have a critical role to play in establishing a strong security culture. Because of their connections to different stakeholders, they will be able to share diverse insights.

For example, the COO can better incorporate input from the board, which is vital to ensuring the CISO understands the company's risk tolerance which will directly impact innovation and revenue.

The Chief Financial Officer (CFO) could share insights into the spending priorities and various obligations needed to protect financial systems and the Chief Human Resources Manager (CHRM) could get valuable data from employees. The CHRM is instrumental when driving the development of the security culture; their level of engagement often determines the overall success of developing a successful security-conscious culture.

Security-conscious C-suite executives will be able to step in to support the CISO's mission that security needs to be a top priority.

Think security-first

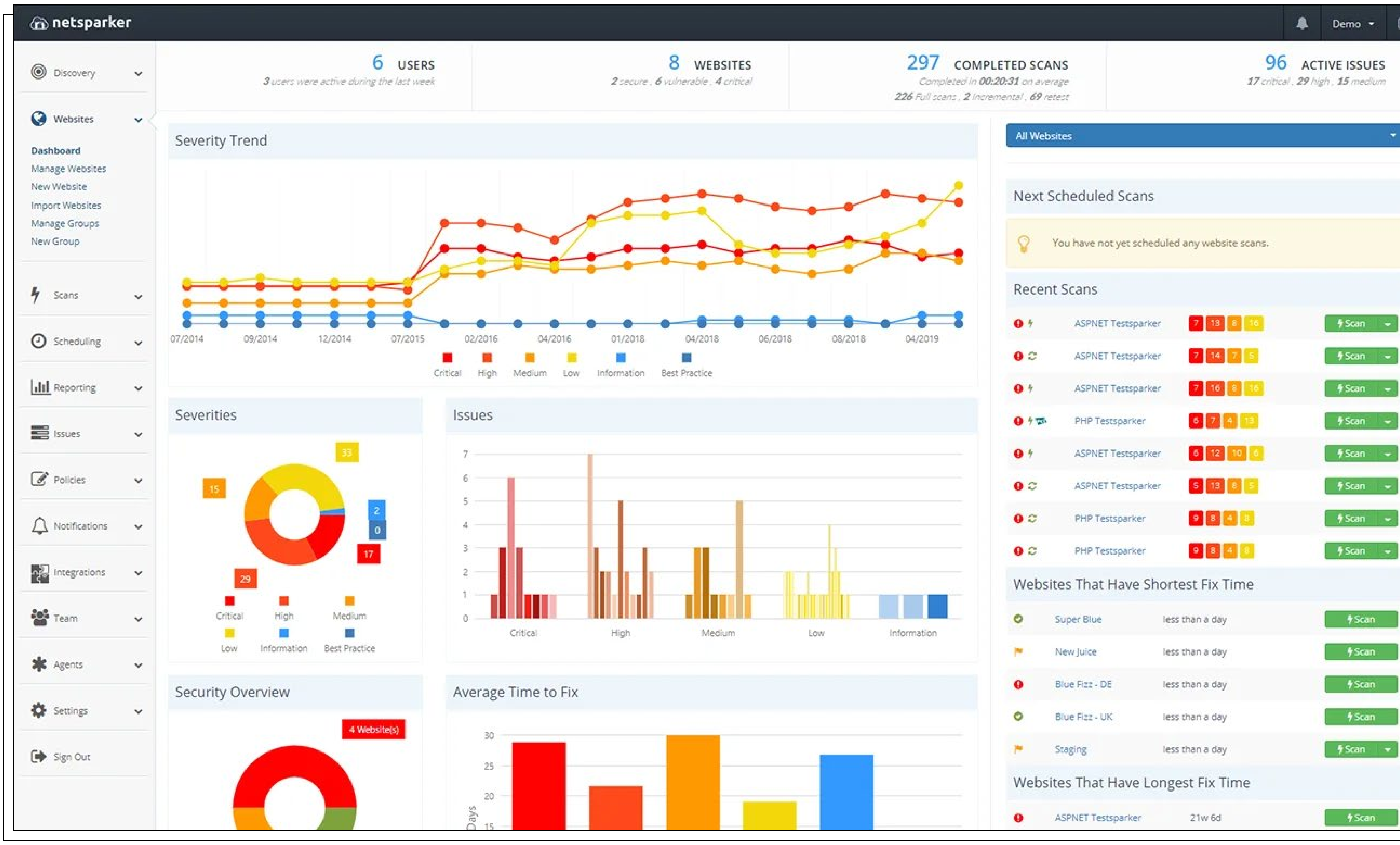
Having model behavior fed from the very top will help to underline an organization's collective commitment to cybersecurity. In doing so, employees are empowered by a sense of shared responsibility around their role in keeping a company's corporate data secure.

To this end, it's crucial that the C-suite of modern companies are trailblazers of security, particularly in the current landscape.

The techniques employed by cybercriminals are becoming more and more sophisticated, and the risk of data breaches and stolen information being offered for sale on the dark web has never been higher.

As the pandemic continues to influence developments in information security, senior leadership, middle management and junior staff members must all work together towards a collective aim of securing their workplace.

Fostering a culture of security awareness is by no means an easy feat, but the long-term gains outweigh any teething issues and will serve to make businesses watertight in the midst of a growing threat landscape.



6 USERS
3 users were active during the last week

8 WEBSITES
2 secure , 6 vulnerable , 4 critical

297 COMPLETED SCANS
Completed in 00:20:31 on average
226 Full scans , 2 Incremental , 69 retest

96 ACTIVE ISSUES
17 critical , 29 high , 15 medium

Next Scheduled Scans

You have not yet scheduled any website scans.

Recent Scans

● ϟ	ASPNET Testsparker	7	13	8	16	ϟ Scan
● ↻	ASPNET Testsparker	7	14	7	5	ϟ Scan
● ϟ	ASPNET Testsparker	7	16	8	16	ϟ Scan
● ϟ	PHP Testsparker	6	7	4	13	ϟ Scan
● ϟ	ASPNET Testsparker	6	12	10	6	ϟ Scan
● ↻	ASPNET Testsparker	5	13	8	5	ϟ Scan
● ↻	PHP Testsparker	9	8	4	8	ϟ Scan
● ↻	PHP Testsparker	9	8	4	8	ϟ Scan

Websites That Have Shortest Fix Time

✓	Super Blue	less than a day	ϟ Scan
⚑	New Juice	less than a day	ϟ Scan
●	Blue Fizz - DE	less than a day	ϟ Scan
✓	Blue Fizz - UK	less than a day	ϟ Scan
⚑	Staging	less than a day	ϟ Scan

Websites That Have Longest Fix Time

●	ASPNET Testsparker	21w 6d	ϟ Scan

Review: Netsparker Enterprise web application scanner

AUTHOR_Tonimir Kisasondi, Co-founder, Apatura

Vulnerability scanners can be a very useful addition to any development or operations process. Since a typical vulnerability scanner needs to detect vulnerabilities in deployed software, they are (generally) not dependent on the language or technology used for the application they are scanning.

This often doesn't make them the top choice for detecting a large number of vulnerabilities or even detecting fickle bugs or business logic issues, but makes them great and very common tools for testing a large number of diverse applications, where such dynamic application security testing tools are indispensable. This includes testing for security defects in software that is being currently developed as a part of a SDLC process, reviewing third-party applications that are deployed inside one's network (as a part of a due diligence process) or - most commonly - finding issues in all kinds of internally developed applications.

> *Netsparker Enterprise is primarily a cloud-based solution, which means it will focus on applications that are publicly available on the open internet, but it can also scan in-perimeter or isolated applications with the help of an agent.*

We reviewed Netsparker Enterprise, which is one of the industry's top choices for web application vulnerability scanning.

Netsparker Enterprise is primarily a cloud-based solution, which means it will focus on applications that are publicly available on the open internet, but it can also scan in-perimeter or isolated applications with the help of an agent, which is usually deployed in a pre-packaged Docker container or a Windows or Linux binary.

To test this product, we wanted to know how Netsparker handles a few things:

1_Scanning workflow
2_Scan customization options
3_Detection accuracy and results
4_CI/CD and issue tracking integrations
5_API and integration capabilities
6_Reporting and remediation efforts.

To assess the tool's detection capabilities, we needed a few targets to scan and assess.

After some thought, we decided on the following targets:

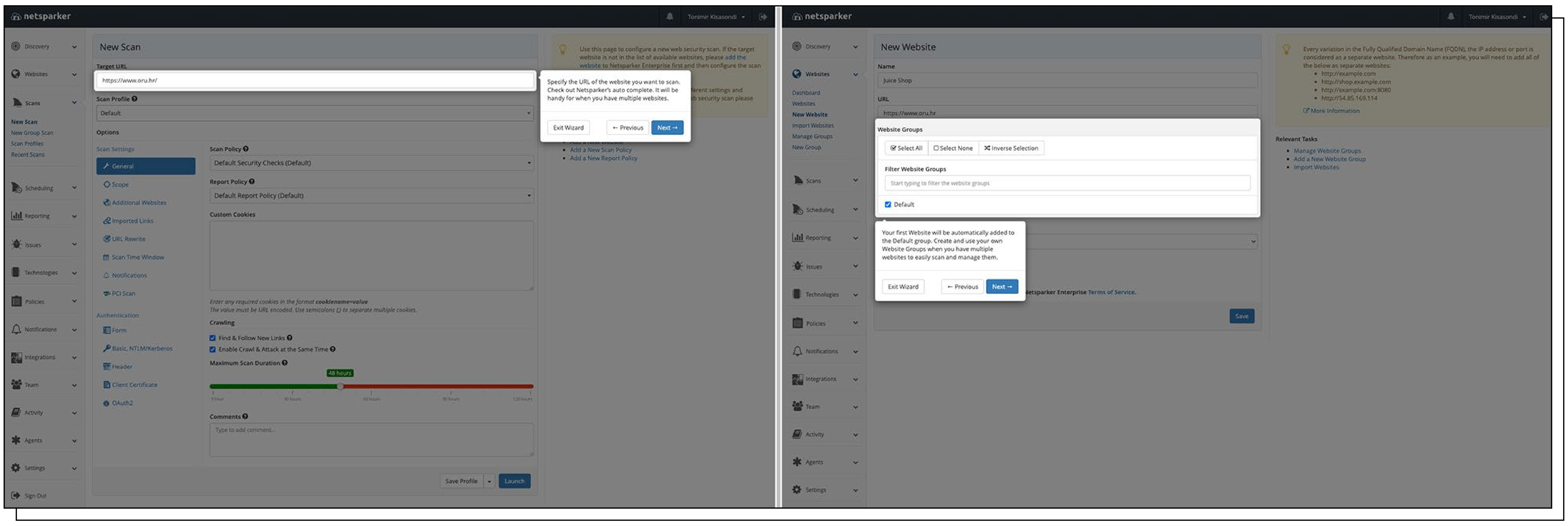
1_DVWA - Damn Vulnerable Web Application - An old-school extremely vulnerable application, written in PHP. The vulnerabilities in this application should be detected without an issue.

2_OWASP Juice Shop simulates a modern single page web application with a REST API backend. It has a Javascript heavy interface, websockets, a REST API in the backend, and many interesting points and vulnerabilities for testing.

3_Vulnapi - A python3-based vulnerable REST API, written in the FastAPI framework running on Starlette ASGI, featuring a number of API based vulnerabilities.

Workflow

After logging in to Netsparker, you are greeted with a tutorial and a "hand-holding" wizard that helps you set everything up. If you worked with a vulnerability scanner before, you might know what to do, but this feature is useful for people that don't have that experience, e.g., software or DevOps engineers, who should definitely use such tools in their development processes.



New Scan

Target URL: https://www.oru.hr/

Scan Profile: Default

Options

Scan Policy: Default Security Checks (Default)

Report Policy: Default Report Policy (Default)

Custom Cookies

Enter any required cookies in the format ***cookiename=value***
The value must be URL encoded. Use semicolons (;) to separate multiple cookies.

Crawling

☑ Find & Follow New Links
☑ Enable Crawl & Attack at the Same Time

Maximum Scan Duration: 48 hours

Comments: Type to add comment...

Use this page to configure a new web security scan. If the target website is not in the list of available websites, please add the website to Netsparker Enterprise first and then configure the scan

Specify the URL of the website you want to scan. Check out Netsparker's auto complete. It will be handy for when you have multiple websites.

- Add a New Scan Policy
- Add a New Report Policy

New Website

Name: Juice Shop

URL: https://www.oru.hr

Website Groups

Filter Website Groups: Start typing to filter the website groups

☑ Default

Your first Website will be automatically added to the Default group. Create and use your own Website Groups when you have multiple websites to easily scan and manage them.

Netsparker Enterprise Terms of Service.

Every variation in the Fully Qualified Domain Name (FQDN), the IP address or port is considered as a separate website. Therefore as an example, you will need to add all of the below as separate websites:

- http://example.com
- http://shop.example.com
- http://example.com:8080
- http://54.85.169.114

More Information

Relevant Tasks

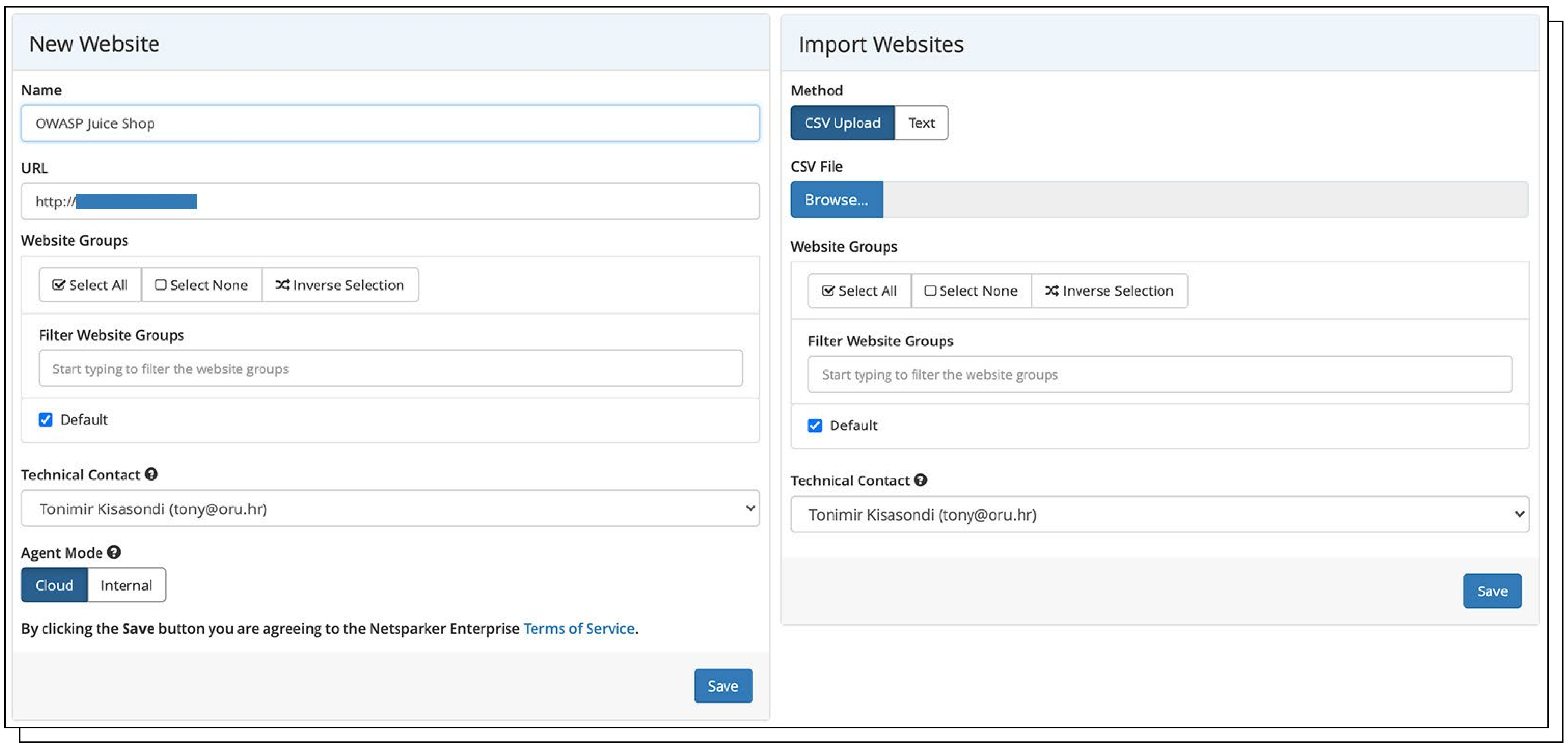
- Manage Website Groups
- Add a New Website Group
- Import Websites

INITIAL SETUP WIZARD

Scanning targets can be added manually or through a discovery feature that will try to find them by matching the domain from your email, websites, reverse IP lookups and other methods. This is a useful feature if other methods of asset management are not used in your organization and you can't find your assets.

New websites or assets for scanning can be added directly or imported via a CSV or a TXT file. Sites can be organized in Groups, which helps with internal organization or per project / per department organization.

ADDING WEBSITES FOR SCANNING


New Website

Name: OWASP Juice Shop

URL: http://[redacted]

Website Groups

Filter Website Groups: Start typing to filter the website groups

☑ Default

Technical Contact: Tonimir Kisasondi (tony@oru.hr)

Agent Mode: [✓ Cloud] Internal

By clicking the **Save** button you are agreeing to the Netsparker Enterprise Terms of Service.

Import Websites

Method: [✓ CSV Upload] Text

CSV File

Website Groups

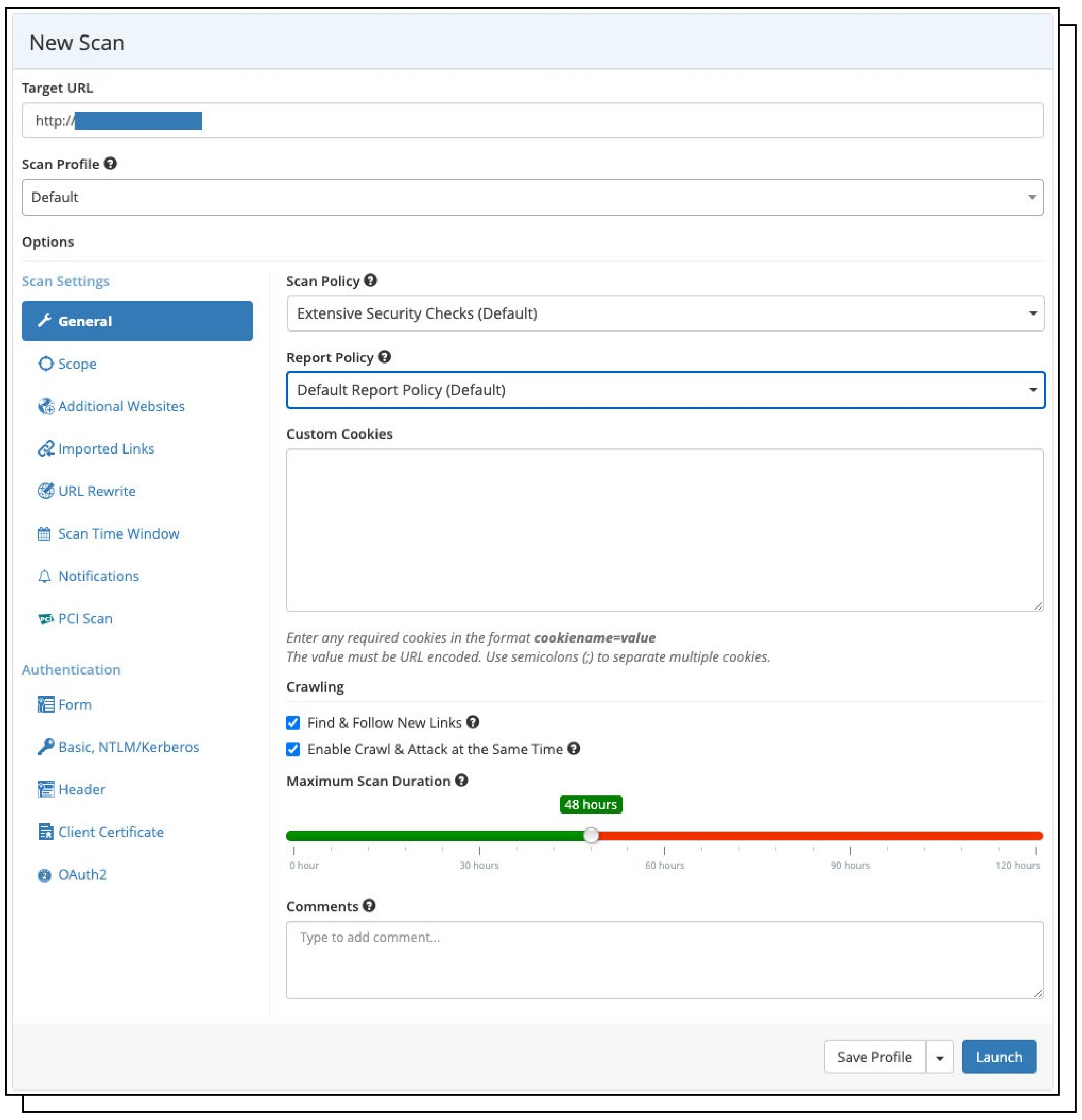
Filter Website Groups: Start typing to filter the website groups

☑ Default

Technical Contact: Tonimir Kisasondi (tony@oru.hr)

Scans can be defined per group or per specific host. Scans can be either defined as one-off scans or be regularly scheduled to facilitate the continuous vulnerability remediation process.

To better guide the scanning process, the classic scan scope features are supported. For example, you can define specific URLs as "out-of-scope" either by supplying a full path or a regex pattern - a useful option if you want to skip specific URLs (e.g., logout, user delete functions). Specific HTTP methods can also be marked as out-of-scope, which is useful if you are testing an API and want to skip DELETE methods on endpoints or objects.


New Scan

Target URL: http://[redacted]

Scan Profile: Default

Options

Scan Policy: Extensive Security Checks (Default)

Report Policy: Default Report Policy (Default)

Custom Cookies

*Enter any required cookies in the format **cookiename=value***
The value must be URL encoded. Use semicolons (;) to separate multiple cookies.

Crawling

☑ Find & Follow New Links

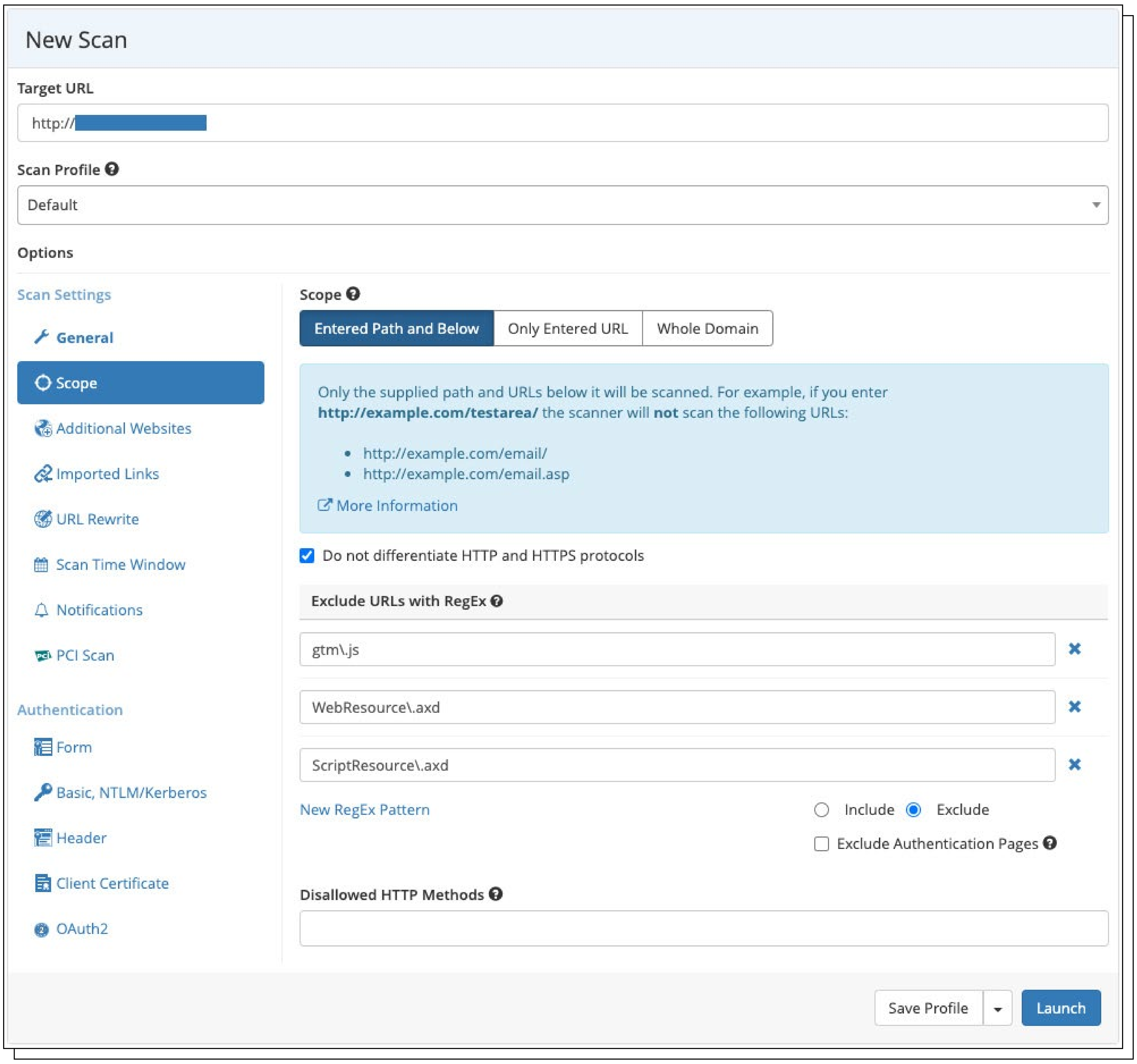
☑ Enable Crawl & Attack at the Same Time

Maximum Scan Duration: 48 hours

Comments: Type to add comment...

INITIAL SCAN CONFIGURATION

SCAN SCOPE OPTIONS



New Scan

Target URL: http://[redacted]

Scan Profile: Default

Options

Scope: Entered Path and Below

Only the supplied path and URLs below it will be scanned. For example, if you enter **http://example.com/testarea/** the scanner will **not** scan the following URLs:

- http://example.com/email/
- http://example.com/email.asp

More Information

☑ Do not differentiate HTTP and HTTPS protocols

Exclude URLs with RegEx

- gtm\.js
- WebResource\.axd
- ScriptResource\.axd

○ Include ● Exclude

□ Exclude Authentication Pages

Disallowed HTTP Methods:

One feature we quite liked is the support for uploading the “sitemap” or specific request information into Netsparker before scanning. This feature can be used to import a Postman collection or an OpenAPI file to facilitate scanning and improve detection capabilities for complex applications or APIs. Other formats such as CSV, JSON, WADL, WSDL and others are also supported.

For the red team, loading links and information from Fiddler, Burp or ZAP session files is supported, which is useful if you want to expand your automated scanning toolbox. One limitation we encountered is the inability to point to an URL containing an OpenAPI definition – a capability that would be extremely useful for automated and scheduled scanning workflows for APIs that have Swagger web UIs.

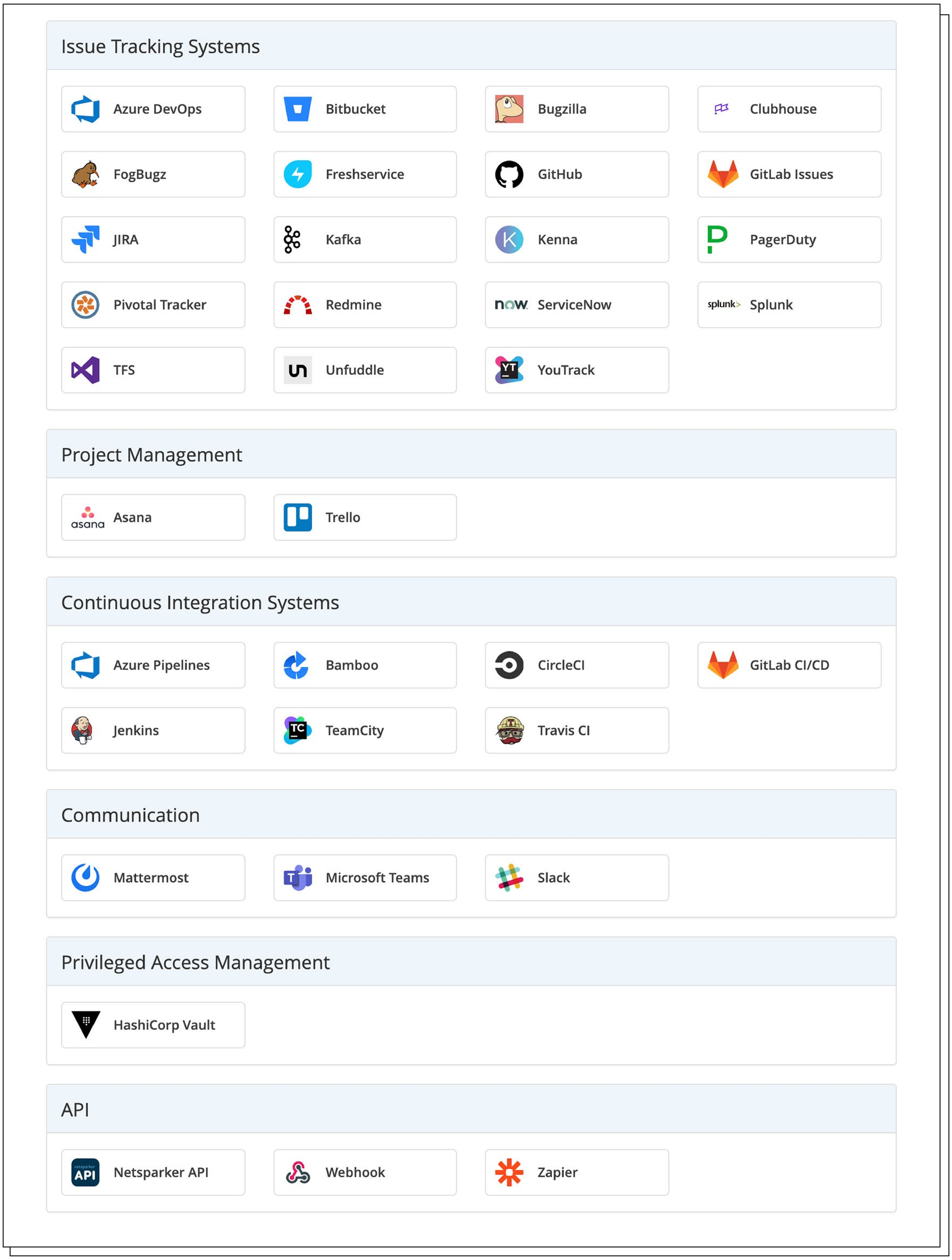
Scan policies can be customized and tuned in a variety of ways, from the languages that are used in the application (ASP/ASP.NET, PHP, Ruby, Java, Perl, Python, Node.js and Other) , to database servers (Microsoft SQL server, MySQL, Oracle, PostgreSQL, Microsoft Access and Others), to the standard choice of Windows or Linux based OSes. Scan optimizations should improve the detection capability of the tool, shorten scanning times, and give us a glimpse where the tool should perform best.

Scan policies can be customized and tuned in a variety of ways, from the languages that are used in the application, to database servers, to the standard choice of Windows or Linux based OSes.

Integrating Netsparker

The next important question is, does it blend… or integrate? From an integration standpoint, sending email and SMSes about the scan events is standard, but support for various issue tracking systems like Jira, Bitbucket, Gitlab, Pagerduty, TFS is available, and so is support for Slack and CI/CD integration. For everything else, there is a raw API that can be used to tie in Netsparker to other solutions if you are willing to write a bit of integration scripting.

INTEGRATION OPTIONS



Issue Tracking Systems

Azure DevOps
Bitbucket
Bugzilla
Clubhouse
FogBugz
Freshservice
GitHub
GitLab Issues
JIRA
Kafka
Kenna
PagerDuty
Pivotal Tracker
Redmine
ServiceNow
Splunk
TFS
Unfuddle
YouTrack

Project Management

Asana
Trello

Continuous Integration Systems

Azure Pipelines
Bamboo
CircleCI
GitLab CI/CD
Jenkins
TeamCity
Travis CI

Communication

Mattermost
Microsoft Teams
Slack

Privileged Access Management

HashiCorp Vault

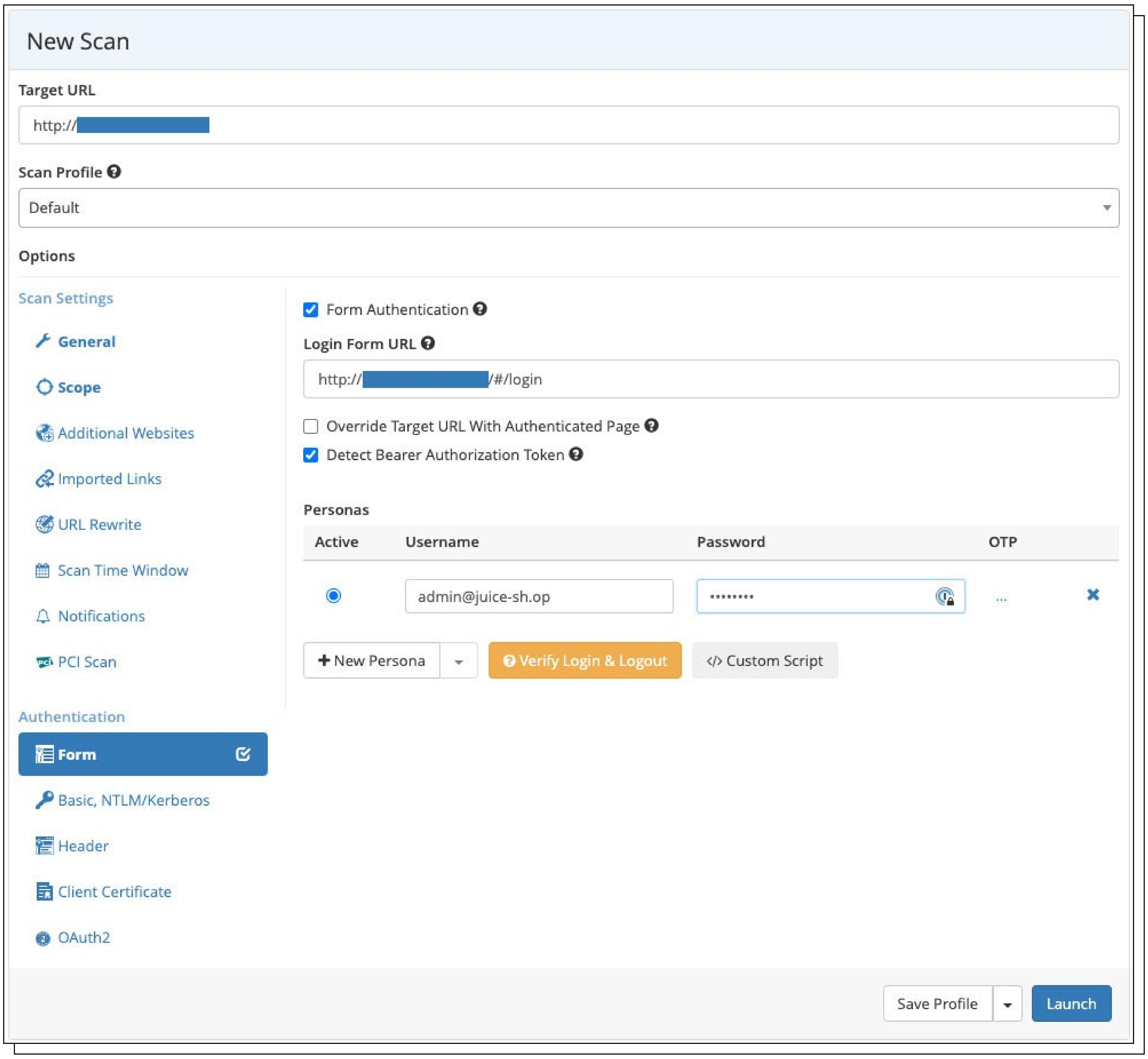
API

Netsparker API
Webhook
Zapier

One really well-implemented feature is the support for logging into the testing application, as the inability to hold a session and scan from an authenticated context in the application can lead to a bad scanning performance.

Netsparker has the support for classic form-based login, but 2FA-based login flows that require TOTP or HOTP are also supported. This is a great feature, as you can add the OTP seed and define the period in Netsparker, and you are all set to scan OTP protected logins. No more shimming and adding code to bypass the 2FA method in order to scan the application.

AUTHENTICATION METHODS



New Scan

Target URL: http://[redacted]

Scan Profile: Default

Options

☑ Form Authentication

Login Form URL: http://[redacted]/#/login

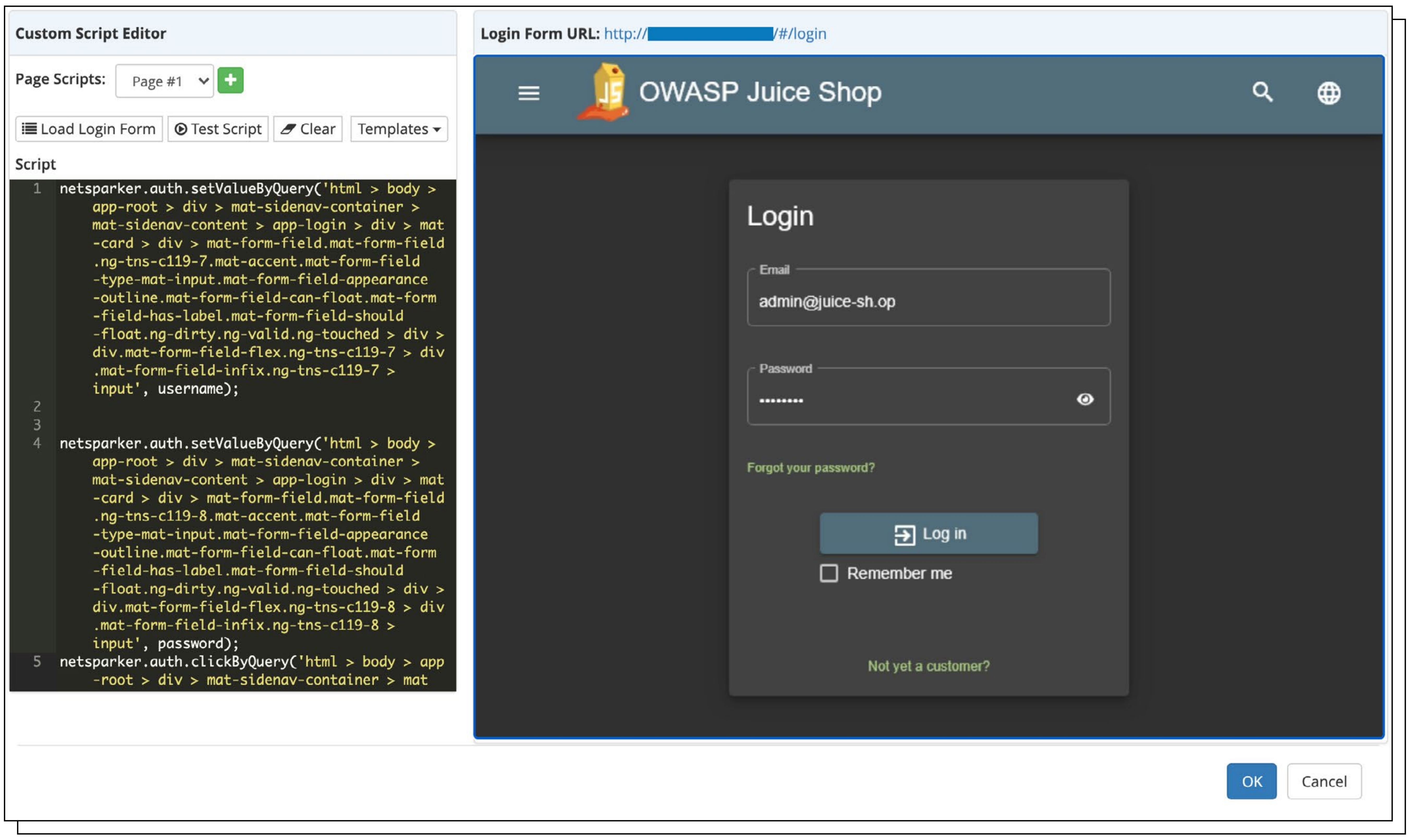
☐ Override Target URL With Authenticated Page
☑ Detect Bearer Authorization Token

Personas

Active	Username	Password	OTP
●	admin@juice-sh.op	••••••••	...

What's more, Netsparker enables you to create a custom script for complex login flows or javascript/ CSS heavy login pages. I was pleasantly surprised that instead of reading complex documentation, I just needed to right click on the DOM elements and add them to the script and press next.

CUSTOM SCRIPTING WORKFLOW FOR AUTHENTICATION



Custom Script Editor

Page Scripts: Page #1

Script

```
netsparker.auth.setValueByQuery('html > body >
    app-root > div > mat-sidenav-container >
    mat-sidenav-content > app-login > div > mat
    -card > div > mat-form-field.mat-form-field
    .ng-tns-c119-7.mat-accent.mat-form-field
    -type-mat-input.mat-form-field-appearance
    -outline.mat-form-field-can-float.mat-form
    -field-has-label.mat-form-field-should
    -float.ng-dirty.ng-valid.ng-touched > div >
    div.mat-form-field-flex.ng-tns-c119-7 > div
    .mat-form-field-infix.ng-tns-c119-7 >
    input', username);


netsparker.auth.setValueByQuery('html > body >
    app-root > div > mat-sidenav-container >
    mat-sidenav-content > app-login > div > mat
    -card > div > mat-form-field.mat-form-field
    .ng-tns-c119-8.mat-accent.mat-form-field
    -type-mat-input.mat-form-field-appearance
    -outline.mat-form-field-can-float.mat-form
    -field-has-label.mat-form-field-should
    -float.ng-dirty.ng-valid.ng-touched > div >
    div.mat-form-field-flex.ng-tns-c119-8 > div
    .mat-form-field-infix.ng-tns-c119-8 >
    input', password);
netsparker.auth.clickByQuery('html > body > app
    -root > div > mat-sidenav-container > mat
```

Login Form URL: http://[redacted]/#/login

Login

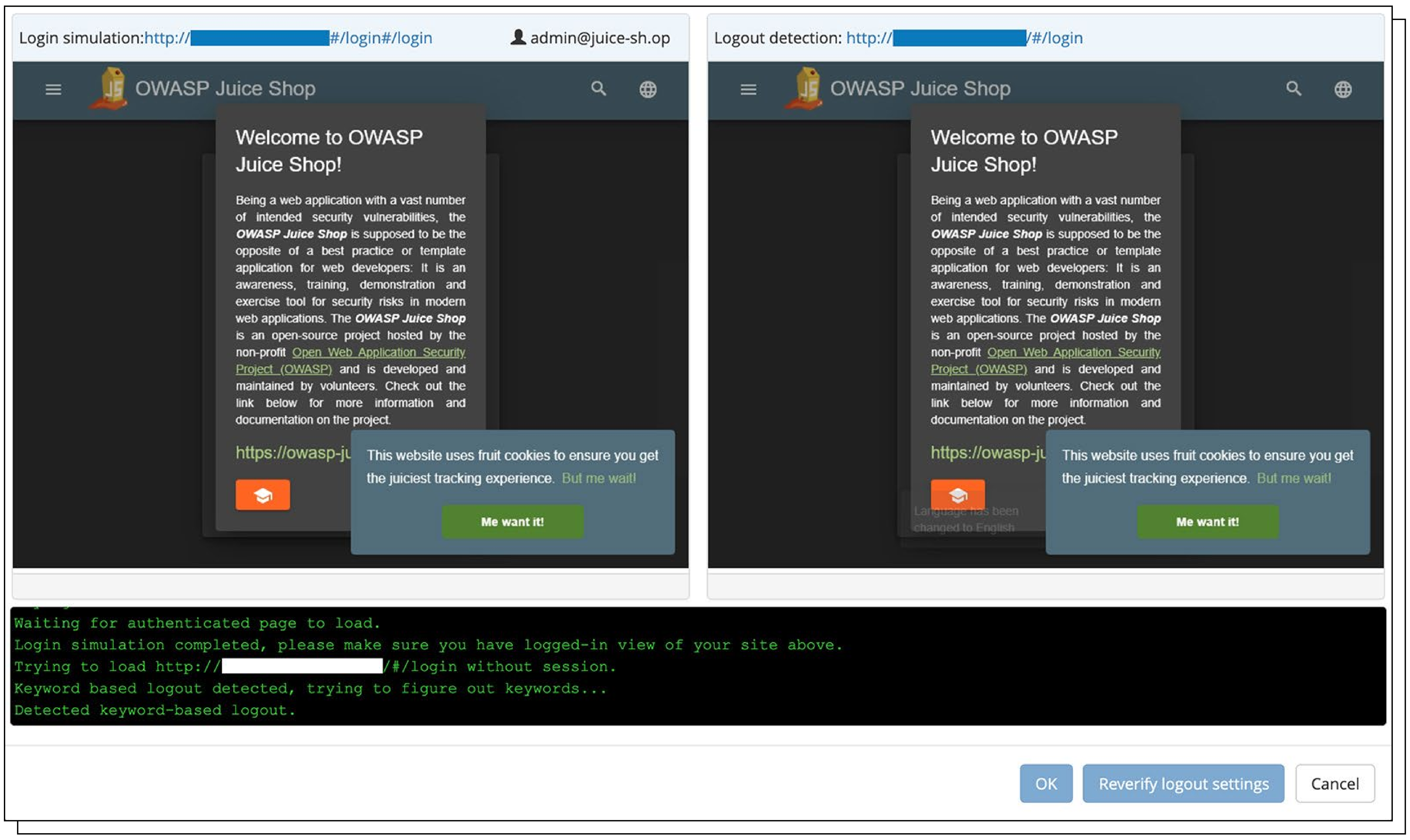
Email: admin@juice-sh.op

Password: ••••••••

If we had to nitpick, we might point out that it would be great if Netsparker also supported U2F / FIDO2 implementations (by software emulating the CTAP1 / CTAP2 protocol), since that would cover the most secure 2FA implementations.

In addition to form-based authentication, Basic NTLM/Kerberos, Header based (for JWTs), Client Certificate and OAuth2-based authentication is also supported, which makes it easy to authenticate to almost any enterprise application. The login / logout flow is also verified and supported through a custom dialog, where you can verify that the supplied credentials work, and you can configure how to retain the session.

LOGIN VERIFICATION HELPER



Login simulation:http://[redacted]#/login#/login admin@juice-sh.op

Logout detection: http://[redacted]/#/login

Welcome to OWASP Juice Shop!

Being a web application with a vast number of intended security vulnerabilities, the ***OWASP Juice Shop*** is supposed to be the opposite of a best practice or template application for web developers: It is an awareness, training, demonstration and exercise tool for security risks in modern web applications. The ***OWASP Juice Shop*** is an open-source project hosted by the non-profit Open Web Application Security Project (OWASP) and is developed and maintained by volunteers. Check out the link below for more information and documentation on the project.

https://owasp-ju

This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!

Welcome to OWASP Juice Shop!

Being a web application with a vast number of intended security vulnerabilities, the ***OWASP Juice Shop*** is supposed to be the opposite of a best practice or template application for web developers: It is an awareness, training, demonstration and exercise tool for security risks in modern web applications. The ***OWASP Juice Shop*** is an open-source project hosted by the non-profit Open Web Application Security Project (OWASP) and is developed and maintained by volunteers. Check out the link below for more information and documentation on the project.

https://owasp-ju

This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!

```
Waiting for authenticated page to load.
Login simulation completed, please make sure you have logged-in view of your site above.
Trying to load http://[redacted]/#/login without session.
Keyword based logout detected, trying to figure out keywords...
Detected keyword-based logout.
```

Scanning accuracy

And now for the core of this review: what Netsparker did and did not detect.

> *One interesting point for vulnerability detection is that Netsparker uses an engine that tries to verify if the vulnerability is exploitable and will try to create a "proof" of vulnerability, which reduces false positives.*

In short, everything from DVWA was detected, except broken client-side security, which by definition is almost impossible to detect with security scanning if custom rules aren't written. So, from a "classic" application point of view, the coverage is excellent, even the out-of-date software versions were flagged correctly. Therefore, for normal, classic stateful applications, written in a relatively new language, it works great.

From a modern JavaScript-heavy single page application point of view, Netsparker correctly discovered the backend API interface from the user interface, and detected a decently complex SQL injection vulnerability, where it was not enough to trigger a ' or 1=1 type of vector but to adjust the vector to properly escape the initial query.

Netsparker correctly detected a stored XSS vulnerability in the reviews section of the Juice Shop product screen. The vulnerable application section is a JavaScript-heavy frontend, with a RESTful API in the backend that facilitates the vulnerability. Even the DOM-based XSS vulnerability was detected, although the specific vulnerable endpoint was marked as the search API and not the sink that is the entry point for DOM XSS. On the positive side, the vulnerability was marked as "Possible" and a manual security review would find the vulnerable sink.

One interesting point for vulnerability detection is that Netsparker uses an engine that tries to verify if the vulnerability is exploitable and will try to create a "proof" of vulnerability, which reduces false positives.

On the negative side, no vulnerabilities in WebSocket-based communications were found, and neither was the API endpoint that implemented insecure YAML deserialization with pyYAML. By reviewing the Netsparker knowledge base, we also found that there is no support for websockets and deserialization vulnerabilities.

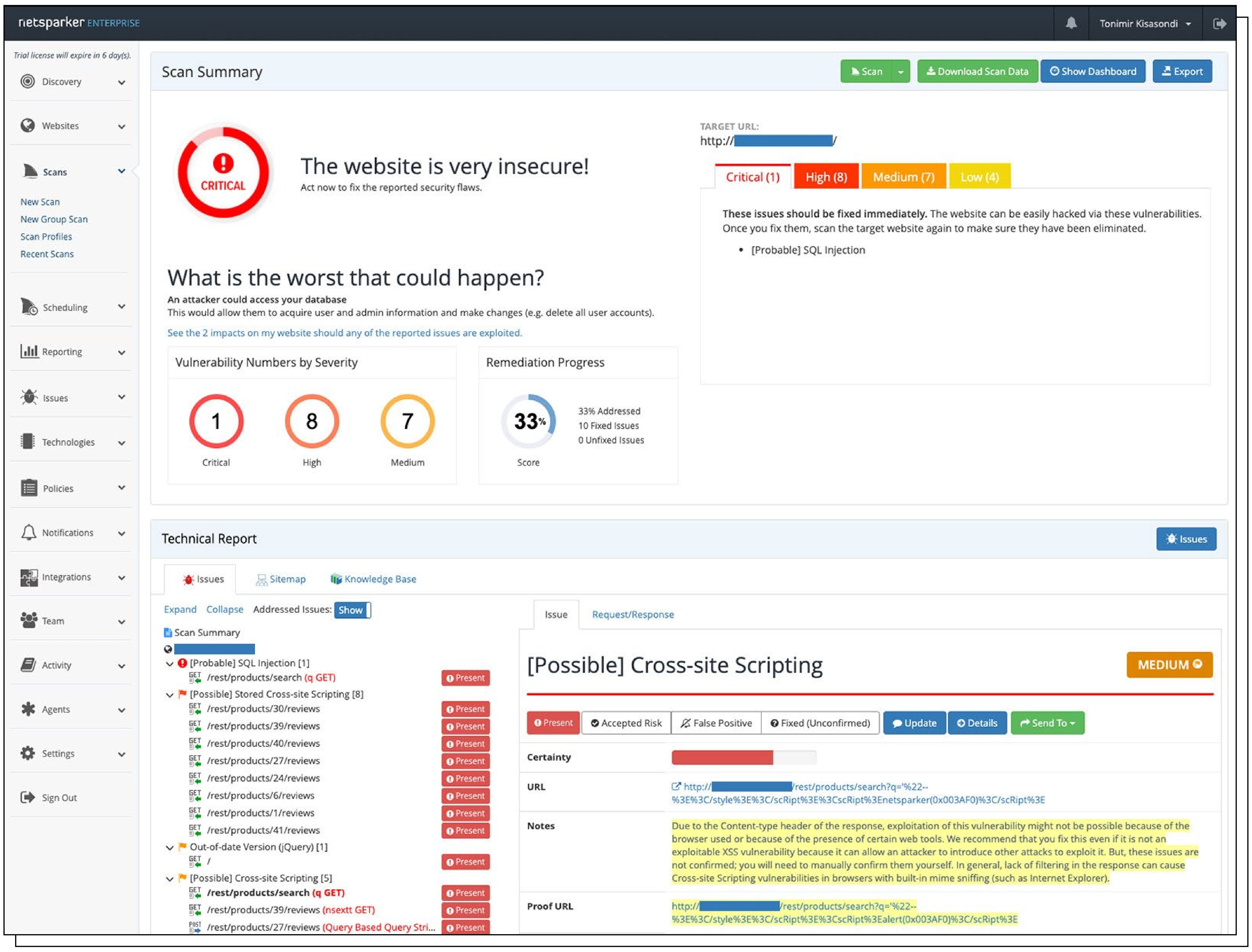
That's certainly not a dealbreaker, but something that needs to be taken into account. This also reinforces the need to use a SAST-based scanner (even if just a free, open-source one) in the application security scanning stack, to improve test coverage in addition to other, manual based security review processes.

Reporting capability

Multiple levels of detail (from extensive, executive summary, to PCI-DSS level) are supported, both in a PDF or HTML export option. One nice feature we found is the ability to create F5 and ModSecurity rules for virtual patching. Also, scanned and crawled URLs can be exported from the reporting section, so it's easy to review if your scanner hit any specific endpoints.

Instead of describing the reports, we decided to export a few and attach them to this review for your enjoyment and assessment. All of them have been submitted to VirusTotal for our more cautious readers.

SCAN RESULTS DASHBOARD



Scan Summary

The website is very insecure!

Act now to fix the reported security flaws.

TARGET URL:
http://[redacted]/

Critical (1) High (8) Medium (7) Low (4)

These issues should be fixed immediately. The website can be easily hacked via these vulnerabilities. Once you fix them, scan the target website again to make sure they have been eliminated.

- [Probable] SQL Injection

What is the worst that could happen?

An attacker could access your database
This would allow them to acquire user and admin information and make changes (e.g. delete all user accounts).

See the 2 impacts on my website should any of the reported issues are exploited.

Vulnerability Numbers by Severity

1	8	7
Critical	High	Medium

Remediation Progress

33% Score

33% Addressed
10 Fixed Issues
0 Unfixed Issues

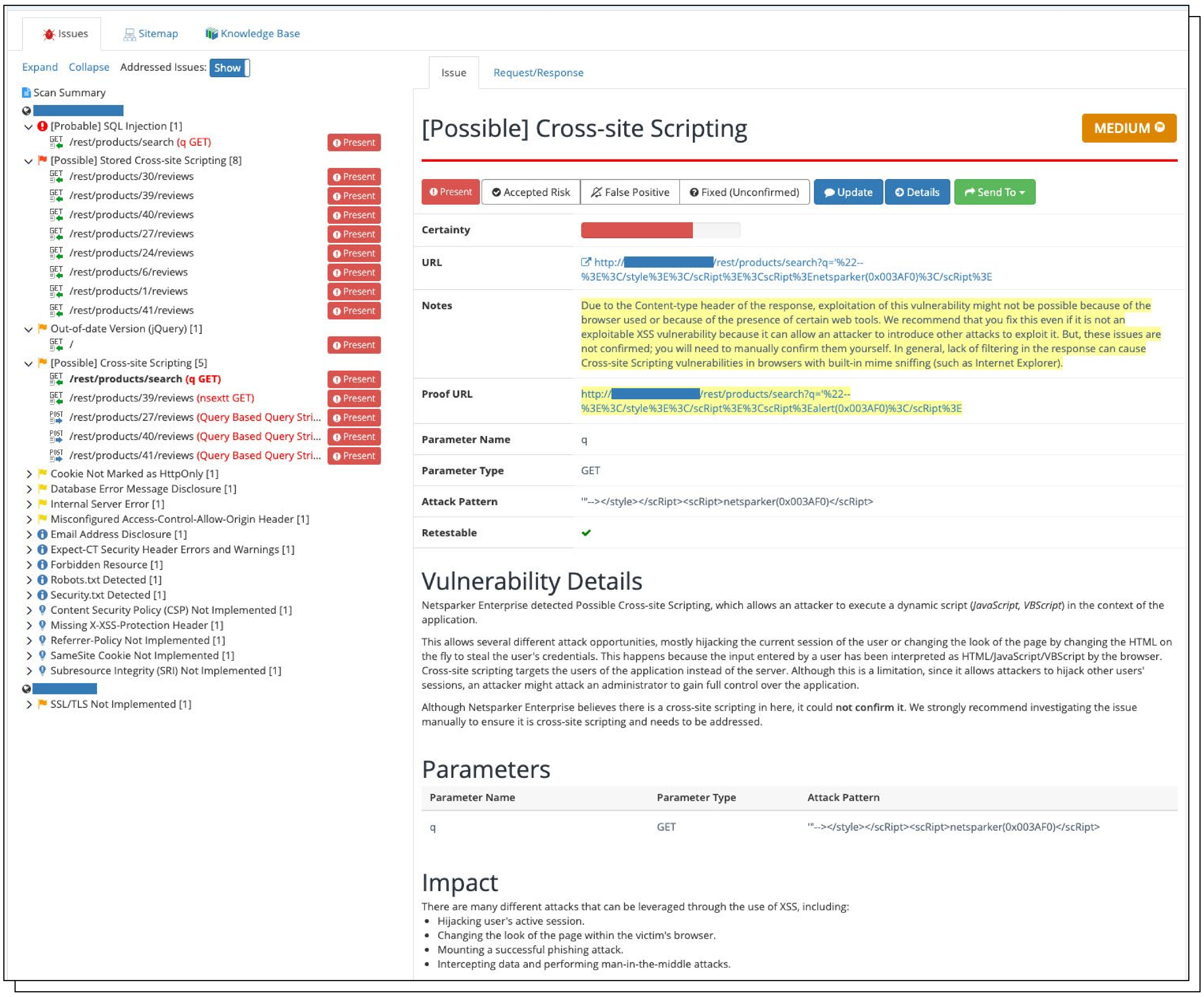
Technical Report

Scan Summary
[redacted]
[Probable] SQL Injection [1]
GET /rest/products/search (q GET) Present
[Possible] Stored Cross-site Scripting [8]
GET /rest/products/30/reviews Present
GET /rest/products/39/reviews Present
GET /rest/products/40/reviews Present
GET /rest/products/27/reviews Present
GET /rest/products/24/reviews Present
GET /rest/products/6/reviews Present
GET /rest/products/1/reviews Present
GET /rest/products/41/reviews Present
Out-of-date Version (jQuery) [1]
GET / Present
[Possible] Cross-site Scripting [5]
GET **/rest/products/search (q GET)** Present
GET /rest/products/39/reviews (nsextt GET) Present
POST /rest/products/27/reviews (Query Based Query Stri... Present

[Possible] Cross-site Scripting

Certainty	
URL	http://[redacted]/rest/products/search?q='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x003AF0)%3C/scRipt%3E
Notes	Due to the Content-type header of the response, exploitation of this vulnerability might not be possible because of the browser used or because of the presence of certain web tools. We recommend that you fix this even if it is not an exploitable XSS vulnerability because it can allow an attacker to introduce other attacks to exploit it. But, these issues are not confirmed; you will need to manually confirm them yourself. In general, lack of filtering in the response can cause Cross-site Scripting vulnerabilities in browsers with built-in mime sniffing (such as Internet Explorer).
Proof URL	http://[redacted]/rest/products/search?q='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert(0x003AF0)%3C/scRipt%3E

SCAN RESULT DETAILS



Scan Summary
[redacted]
[Probable] SQL Injection [1]
GET /rest/products/search (q GET) Present
[Possible] Stored Cross-site Scripting [8]
GET /rest/products/30/reviews Present
GET /rest/products/39/reviews Present
GET /rest/products/40/reviews Present
GET /rest/products/27/reviews Present
GET /rest/products/24/reviews Present
GET /rest/products/6/reviews Present
GET /rest/products/1/reviews Present
GET /rest/products/41/reviews Present
Out-of-date Version (jQuery) [1]
GET / Present
[Possible] Cross-site Scripting [5]
GET **/rest/products/search (q GET)** Present
GET /rest/products/39/reviews (nsextt GET) Present
POST /rest/products/27/reviews (Query Based Query Stri... Present
POST /rest/products/40/reviews (Query Based Query Stri... Present
POST /rest/products/41/reviews (Query Based Query Stri... Present
Cookie Not Marked as HttpOnly [1]
Database Error Message Disclosure [1]
Internal Server Error [1]
Misconfigured Access-Control-Allow-Origin Header [1]
Email Address Disclosure [1]
Expect-CT Security Header Errors and Warnings [1]
Forbidden Resource [1]
Robots.txt Detected [1]
Security.txt Detected [1]
Content Security Policy (CSP) Not Implemented [1]
Missing X-XSS-Protection Header [1]
Referrer-Policy Not Implemented [1]
SameSite Cookie Not Implemented [1]
Subresource Integrity (SRI) Not Implemented [1]
[redacted]
SSL/TLS Not Implemented [1]

[Possible] Cross-site Scripting

Certainty	
URL	http://[redacted]/rest/products/search?q='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x003AF0)%3C/scRipt%3E
Notes	Due to the Content-type header of the response, exploitation of this vulnerability might not be possible because of the browser used or because of the presence of certain web tools. We recommend that you fix this even if it is not an exploitable XSS vulnerability because it can allow an attacker to introduce other attacks to exploit it. But, these issues are not confirmed; you will need to manually confirm them yourself. In general, lack of filtering in the response can cause Cross-site Scripting vulnerabilities in browsers with built-in mime sniffing (such as Internet Explorer).
Proof URL	http://[redacted]/rest/products/search?q='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert(0x003AF0)%3C/scRipt%3E
Parameter Name	q
Parameter Type	GET
Attack Pattern	'"--></style></scRipt><scRipt>netsparker(0x003AF0)</scRipt>
Retestable	✓

Vulnerability Details

Netsparker Enterprise detected Possible Cross-site Scripting, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Although Netsparker Enterprise believes there is a cross-site scripting in here, it could **not confirm it**. We strongly recommend investigating the issue manually to ensure it is cross-site scripting and needs to be addressed.

Parameters

Parameter Name	Parameter Type	Attack Pattern
q	GET	'"--></style></scRipt><scRipt>netsparker(0x003AF0)</scRipt>

Impact

There are many different attacks that can be leveraged through the use of XSS, including:

- Hijacking user's active session.
- Changing the look of the page within the victim's browser.
- Mounting a successful phishing attack.
- Intercepting data and performing man-in-the-middle attacks.

Since Netsparker integrates with JIRA and other ticketing systems, the general vulnerability management workflow for most teams will be supported.

Netsparker's reporting capabilities satisfy our requirements: the reports contain everything a security or AppSec engineer or a developer needs.

Since Netsparker integrates with JIRA and other ticketing systems, the general vulnerability management workflow for most teams will be supported. For lone security teams, or where modern workflows aren't integrated, Netsparker also has an internal issue tracking system that will let the user track the status of each found issue and run rescans against specific findings to see if mitigations were properly implemented. So even if you don't have other methods of triage or processes set up as part of a SDLC, you can manage everything through Netsparker.

Netsparker is extremely easy to set up and use. The wide variety of integrations allow it to be integrated into any number of workflows or management scenarios, and the integrated features and reporting capabilities have everything you would want from a standalone tool. As far as features are concerned, we have no objections.

Verdict

Netsparker is extremely easy to set up and use. The wide variety of integrations allow it to be integrated into any number of workflows or management scenarios, and the integrated features and reporting capabilities have everything you would want from a standalone tool. As far as features are concerned, we have no objections.

The login flow – the simple interface, the 2FA support all the way to the scripting interface that makes it easy to authenticate even in the more complex environments, and the option to report on the scanned and crawled endpoints - helps users discover their scanning coverage.

Taking into account the fact that this is an automated scanner that relies on "black boxing" a deployed application without any instrumentalization on the deployed environment or source code scanning, we think it is very accurate, though it could be improved (e.g., by adding the capability of detecting deserialization vulnerabilities). Following the review, Netsparker has confirmed that adding the capability of detecting deserialization vulnerabilities is included in the product development plans.

Nevertheless, we can highly recommend Netsparker.

Security world

Researchers open the door to new distribution methods for secret cryptographic keys

Researchers from the University of Ottawa, in collaboration with Ben-Gurion University of the Negev and Bar-Ilan University scientists, have been able to create optical framed knots in the laboratory that could potentially be applied in modern technologies.

Their work opens the door to new methods of distributing secret cryptographic keys – used to encrypt and decrypt data, ensure secure communication and protect private information.

“This is fundamentally important, in particular from a topology-focused perspective, since framed knots provide a platform for topological quantum computations,” explained senior author, Professor Ebrahim Karimi, Canada Research Chair in Structured Light at the University of Ottawa.

“In addition, we used these non-trivial optical structures as information carriers and developed a security protocol for classical communication where information is encoded within these framed knots.”

Technologies that enable legal and compliance leaders to spot innovations

COVID-19 has accelerated the push toward digital business transformation for most businesses, and legal and compliance leaders are under pressure to anticipate both the potential improvements and possible risks that come with new legal technology innovations, according to Gartner.

“Legal and compliance leaders must collaborate with other stakeholders to garner support for organization wide and function wide investments in technology,” said Zack Hutto, director in the Gartner Legal and Compliance practice.

“They must address complex business demand by investing in technologies and practices to better anticipate, identify and manage risks, while seeking out opportunities to contribute to growth.”

Analysts said enterprise legal management (ELM), subject rights requests, predictive analytics, and robotic process automation (RPA) are likely to be most beneficial for the majority of legal and compliance organizations within a few years. They are also likely to help with the increased need for cost optimization and unplanned legal work arising from the pandemic.

Cybersecurity practices are becoming more formal, security teams are expanding

Organizations are building confidence that their cybersecurity practices are headed in the right direction, aided by advanced technologies, more detailed processes, comprehensive education and specialized skills, research from CompTIA finds.

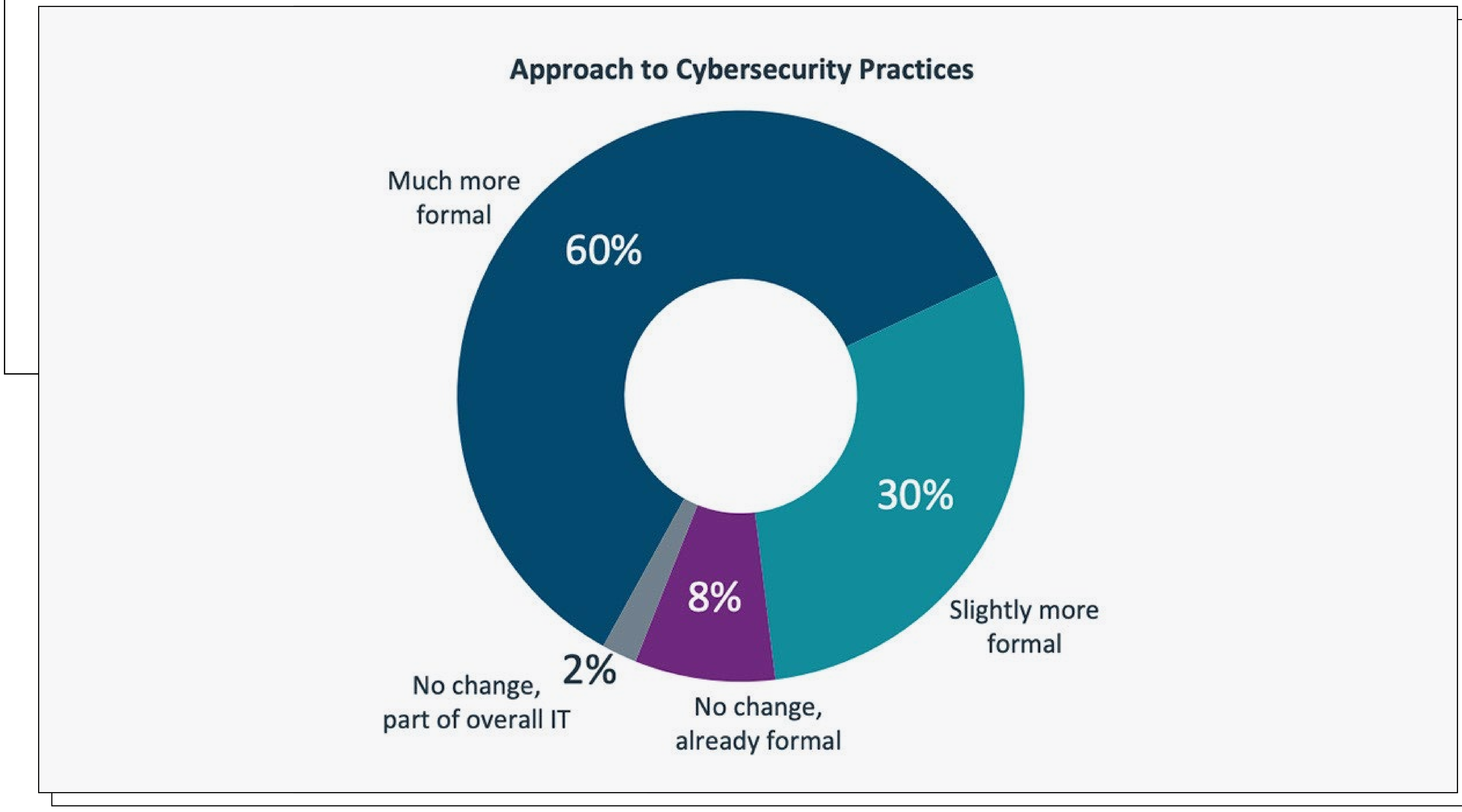
Two factors – one anticipated (digital transformation), the other unexpected (the COVID-19 pandemic) – have contributed to the heightened awareness about the need for strong cybersecurity measures.

The report also highlights how the "cybersecurity chain" has expanded to include upper management, boards of directors, business units and outside firms in addition to IT personnel in conversations and decisions.

Within IT teams, foundational skills such as network and endpoint security have been paired with new skills, including identity management and application security, that have become more important as cloud and mobility have taken hold. On the horizon, expect to see skills related to security monitoring and other proactive tactics gain a bigger foothold. Examples include data analysis, threat knowledge and understanding the regulatory landscape.

Cybersecurity insurance is another emerging area. The report reveals that 45% of large companies, 41% of mid-sized firms and 37% of small businesses currently have a cyber insurance policy.

Common coverage areas include the cost of restoring data (56% of policy holders), the cost of finding the root cause of a breach (47%), coverage for third-party incidents (43%) and response to ransomware (42%).



Why are certain employees more likely to comply with information security policies than others?

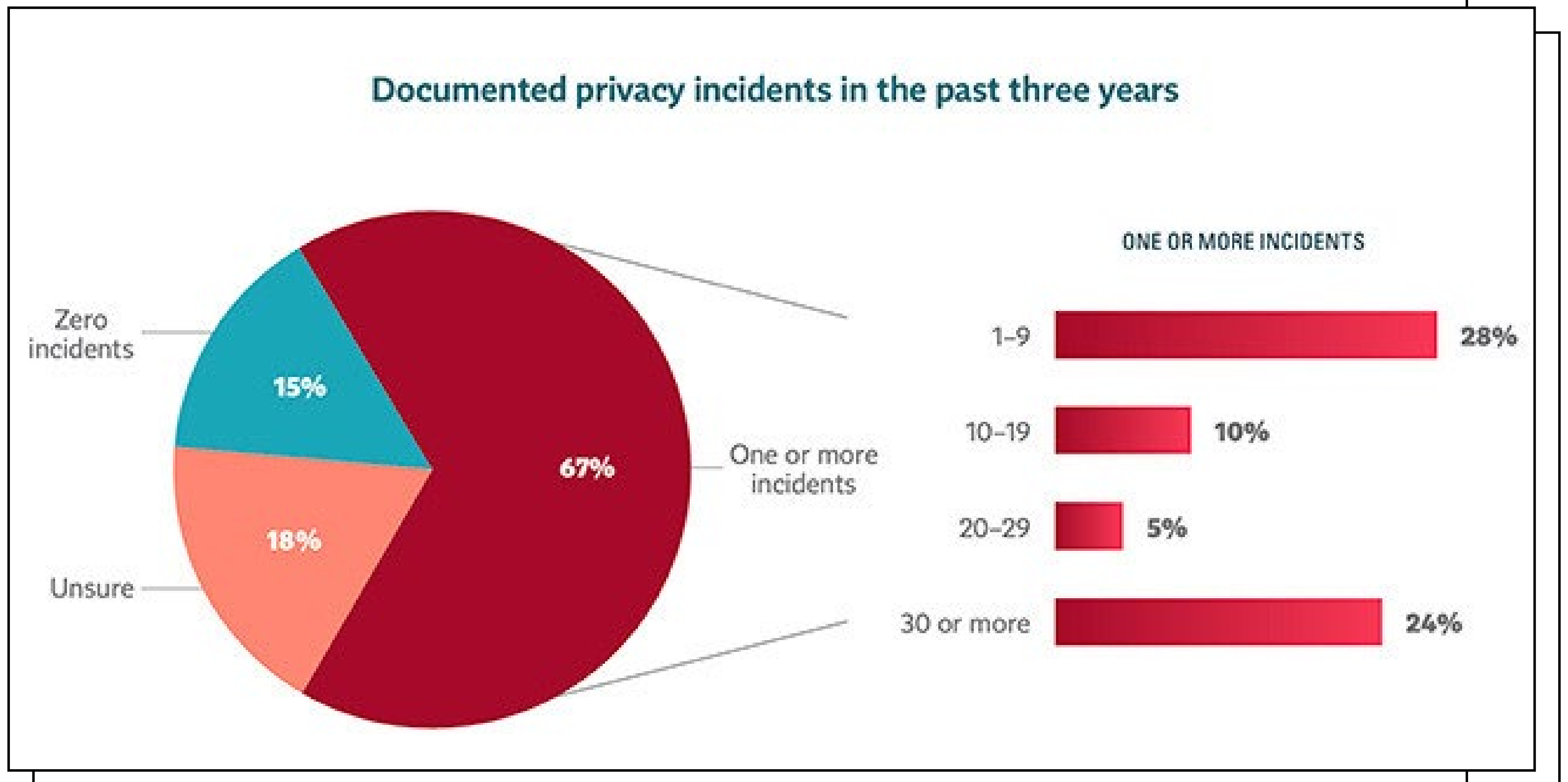
Information security policies (ISP) that are not grounded in the realities of an employee's work responsibilities and priorities expose organizations to higher risk for data breaches, according to a research from Binghamton University, State University of New York.

Researchers concluded that each subculture within an organization will respond differently to the organization-wide ISP, leaving organizations open to a higher possibility of data breaches. Their recommendation? Consult with each subculture while developing ISP.

"Information security professionals should have a better understanding of the day-to-day tasks of each professional group, and then find ways to seamlessly integrate ISP compliance within those job tasks," said said Sumantra Sarkar, associate professor of management information systems in Binghamton University's School of Management. "It is critical that we find ways to redesign ISP systems and processes in order to create less friction."

Global adoption of data and privacy programs still maturing

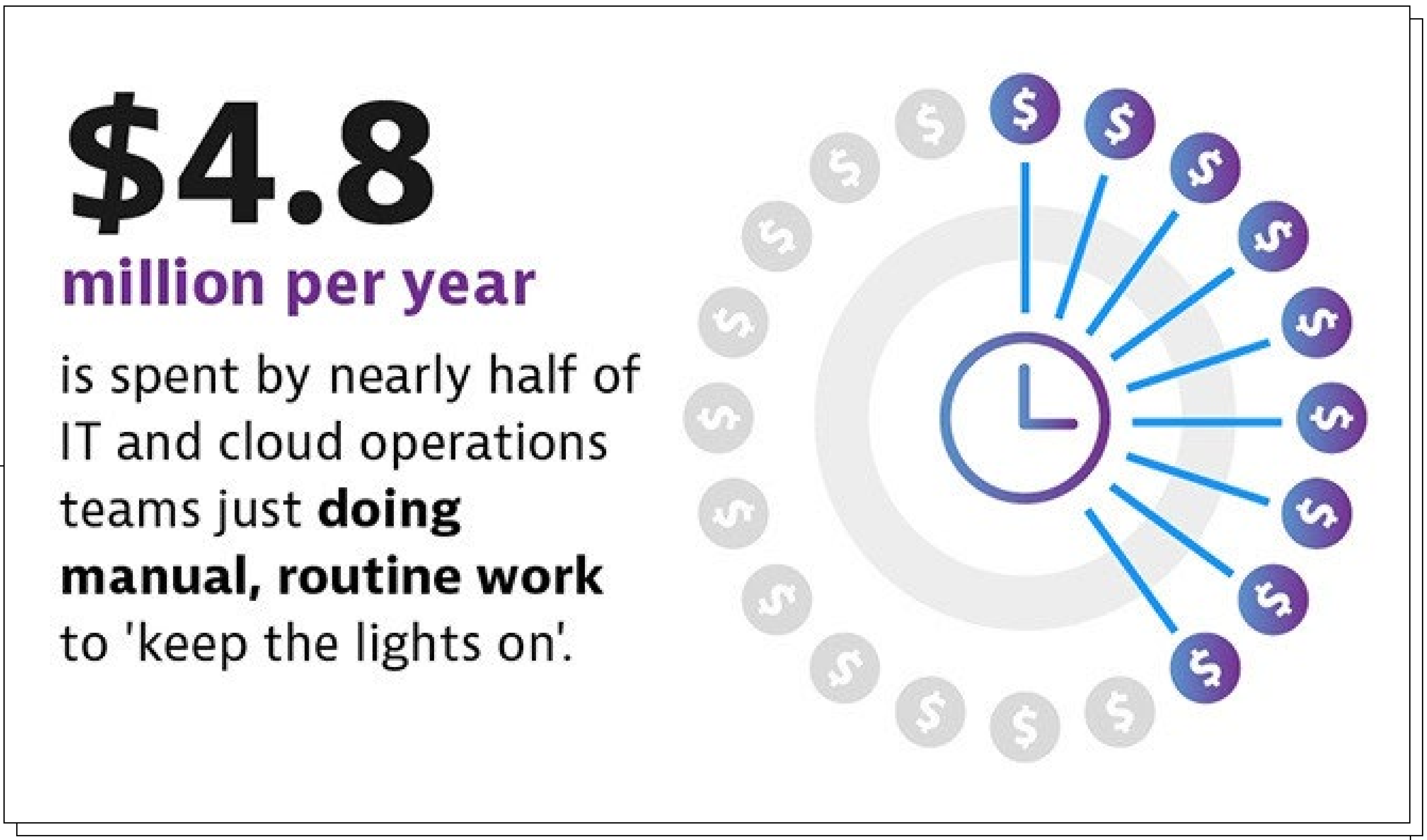
A FairWarning report, based on survey results from more than 550 global privacy and data protection, IT, and compliance professionals, outlined the characteristics and behaviors of advanced privacy and data protection teams.



Insights from the research reinforce the importance of privacy and data protection as 67% of responding organizations documented at least one privacy incident within the past three years, and over 24% of those experienced 30 or more.

Despite increased regulations, breaches and privacy incidents, organizations have not rapidly accelerated the advancement of their privacy programs as 44% responded they are in the early stages of adoption and 28% are in middle stages.

Respondents understand the significant benefits of a mature privacy program as organizations experience greater gains across every area measured including: increased employee privacy awareness, mitigating data breaches, greater consumer trust, reduced privacy complaints, quality and innovation, competitive advantage, and operational efficiency.



$4.8

million per year

is spent by nearly half of IT and cloud operations teams just **doing manual, routine work** to 'keep the lights on'.

Cloud environment complexity has surpassed human ability to manage

IT leaders are increasingly concerned accelerated digital transformation, combined with the complexity of modern multicloud environments, is putting already stretched digital teams under too much pressure, a Dynatrace survey of 700 CIOs revealed.

This leaves little time for innovation, and limits teams' ability to prioritize tasks that drive greater value and better outcomes for the business and its customers.

Key findings:

- 89% of CIOs say digital transformation has accelerated in the last 12 months, and 58% predict it will continue to speed up.
- 86% of organizations are using cloud-native technologies, including microservices, containers, and Kubernetes, to accelerate innovation and achieve more successful business outcomes.
- 63% of CIOs say the complexity of their cloud environment has surpassed human ability to manage.
- 44% of IT and cloud operations teams' time is spent on manual, routine work just 'keeping the lights on', costing organizations an average of $4.8 million per year.
- 56% of CIOs say they are almost never able to complete everything the business needs from IT.
- 70% of CIOs say their team is forced to spend too much time doing manual tasks that could be automated if only they had the means.

Companies that facilitate ransomware payments risk violating US sanctions

Companies that ransomware-hit US organizations hire to facilitate the paying of the ransom are at risk of breaking US sanctions, falling afoul of the US Department of the Treasury's Office of Foreign Assets Control regulations and may end up paying millions in fines. These include financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response.

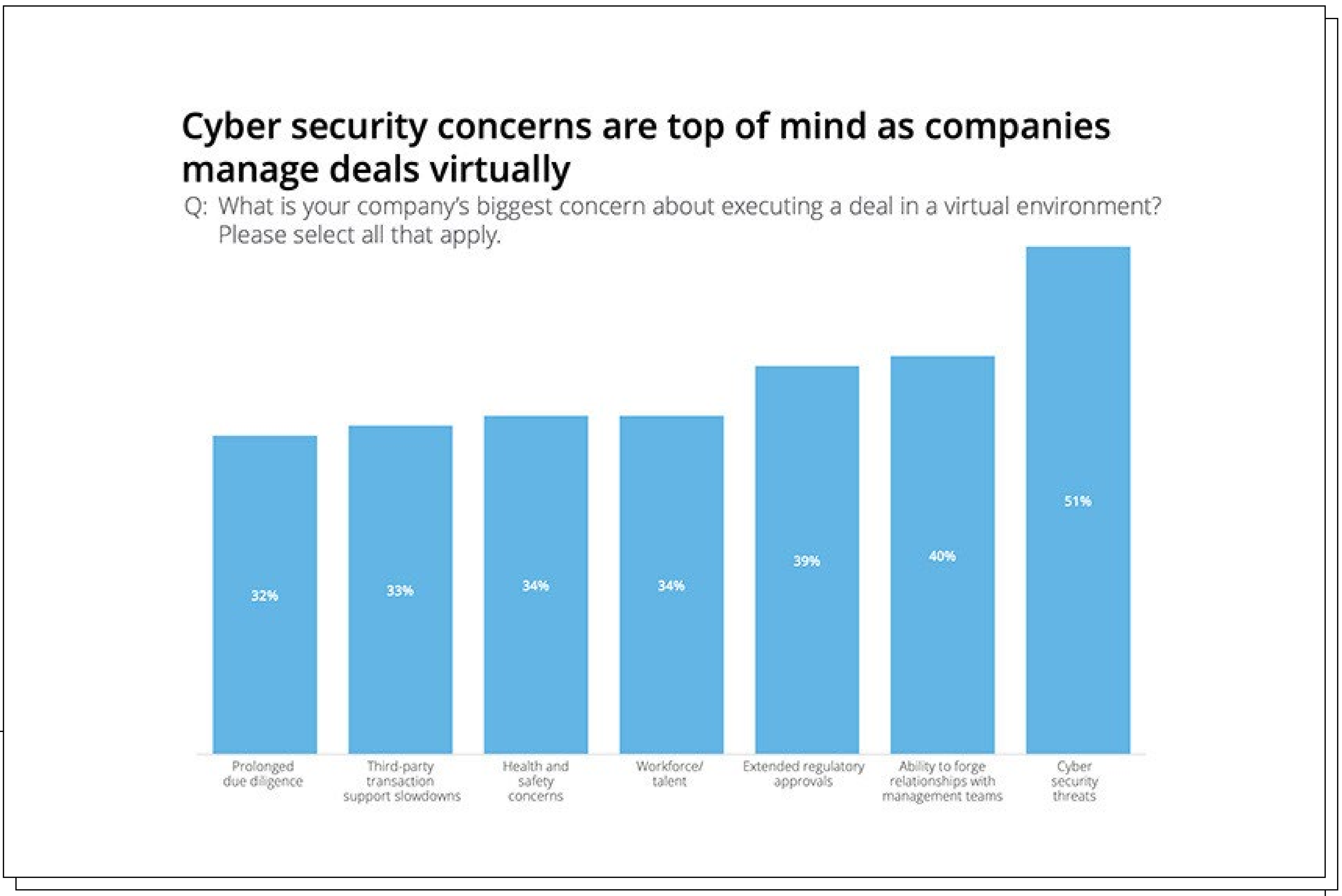
"Ransomware payments made to sanctioned persons or to comprehensively sanctioned jurisdictions could be used to fund activities adverse to the national security and foreign policy objectives of the United States. Ransomware payments may also embolden cyber actors to engage in future attacks. In addition, paying a ransom to cyber actors does not guarantee that the victim will regain access to its stolen data," the OFAC explained.
"OFAC encourages victims and those involved with addressing ransomware attacks to contact OFAC immediately if they believe a request for a ransomware payment may involve a sanctions nexus. Victims should also contact the US Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection if an attack involves a US financial institution or may cause significant disruption to a firm's ability to perform critical financial services."

OFAC might issue a special license allowing them to perform the transaction (the paying of the ransom), but each application will be reviewed by OFAC on a case-by-case basis „with a presumption of denial."

SaaS adoption prompting concerns over operational complexity and risk

A rise in SaaS adoption is prompting concerns over operational complexity and risk, a BetterCloud report revealed. Key findings:

- On average, organizations use 80 SaaS apps today. This is a 5x increase in just three years and a 10x increase since 2015.
- The top two motivators for using more SaaS apps are increasing productivity and reducing costs.
- Only 49 percent of IT professionals inspire confidence in their ability to identify and monitor unsanctioned SaaS usage on company networks—yet more than three-quarters (76 percent) see unsanctioned apps as a security risk.
- The top five places where sensitive data lives are: 1. files stored in cloud storage, 2. email, 3. devices, 4. chat apps, and 5. password managers. But because SaaS apps have become the system of record, sensitive data inevitably lives everywhere in your SaaS environment.
- The top two security concerns are sensitive files shared publicly and former employees retaining data access.
- IT teams spend an average of 7.12 hours offboarding a single employee from a company's SaaS apps.
- Thirty percent of respondents already use the term SaaSOps in their job title or plan to include it soon.



Cyber security concerns are top of mind as companies manage deals virtually

Q: What is your company's biggest concern about executing a deal in a virtual environment? Please select all that apply.

Cyber teams are getting more involved in M&A

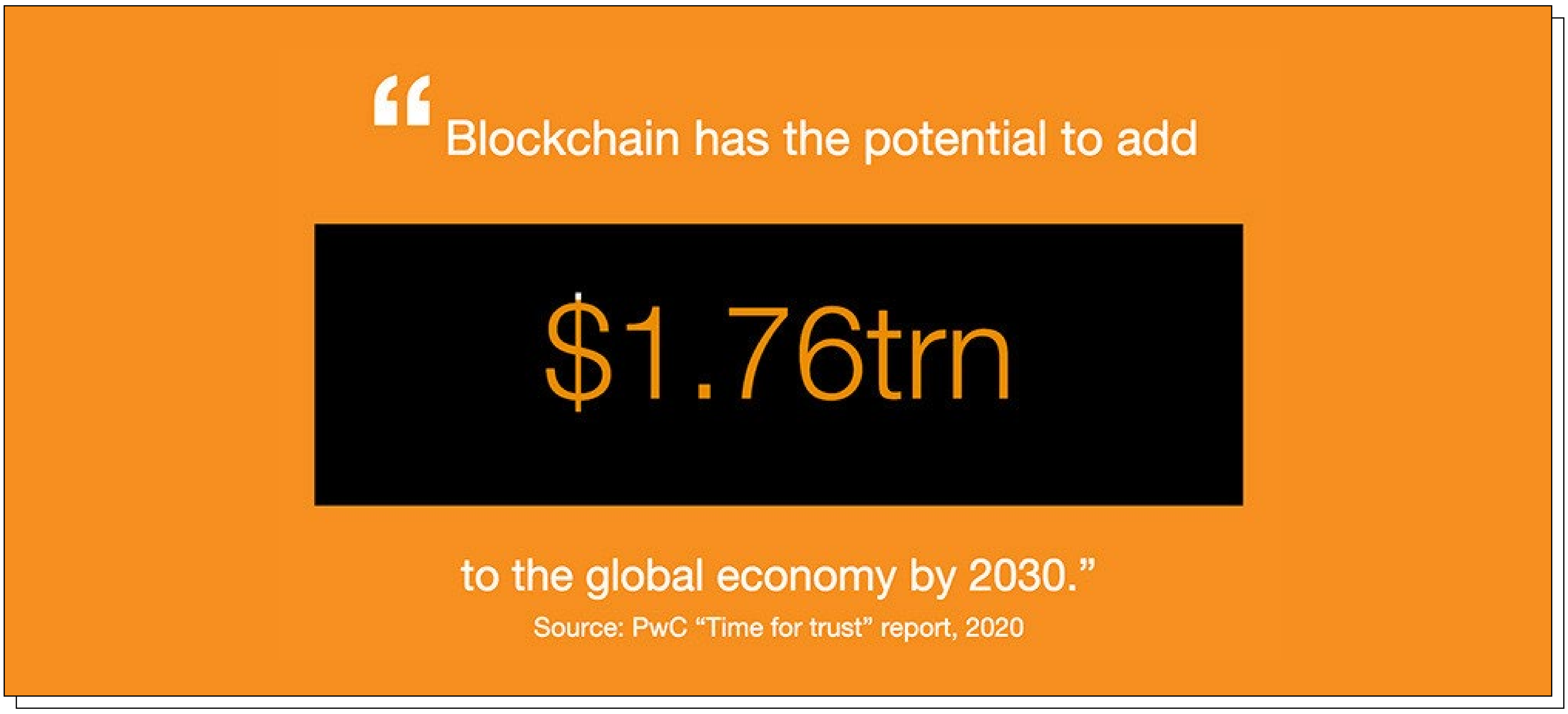
According to a Deloitte survey of 1,000 U.S. corporate merger and acquisition (M&A) executives and private equity firm professionals, 92% of the respondents tentatively paused and 78% abandoned at least one transaction as a result of the pandemic outbreak. However, since March 2020, possibly aiming to take advantage of pandemic-driven business disruptions, 60% say their organizations have been more focused on pursuing new deals.

For many, alternative deals (e.g., alliances, joint ventures, and Special Purpose Acquisition Companies) are quickly outpacing traditional M&A activity as the search for value intensifies in a low-growth environment.

87% of M&A professionals surveyed report that their organizations were able to effectively manage a deal in a purely virtual environment, so much so that 55% anticipate that virtual dealmaking will be the preferred platform even after the pandemic is over.

However, virtual dealmaking does not remain without its own challenges. Fifty-one percent noted that cybersecurity threats are their organizations' biggest concern around executing deals virtually.

Other virtual dealmaking concerns included the ability to forge relationships with management teams (40%) and extended regulatory approvals (39%). When it comes to effectively managing the integration phase in a virtual environment, technology integration (16%) and legal entity alignment or simplification (16%) are surveyed M&A executives' largest and most prevalent hurdles.



“Blockchain has the potential to add

$1.76trn

to the global economy by 2030.”

Source: PwC “Time for trust” report, 2020

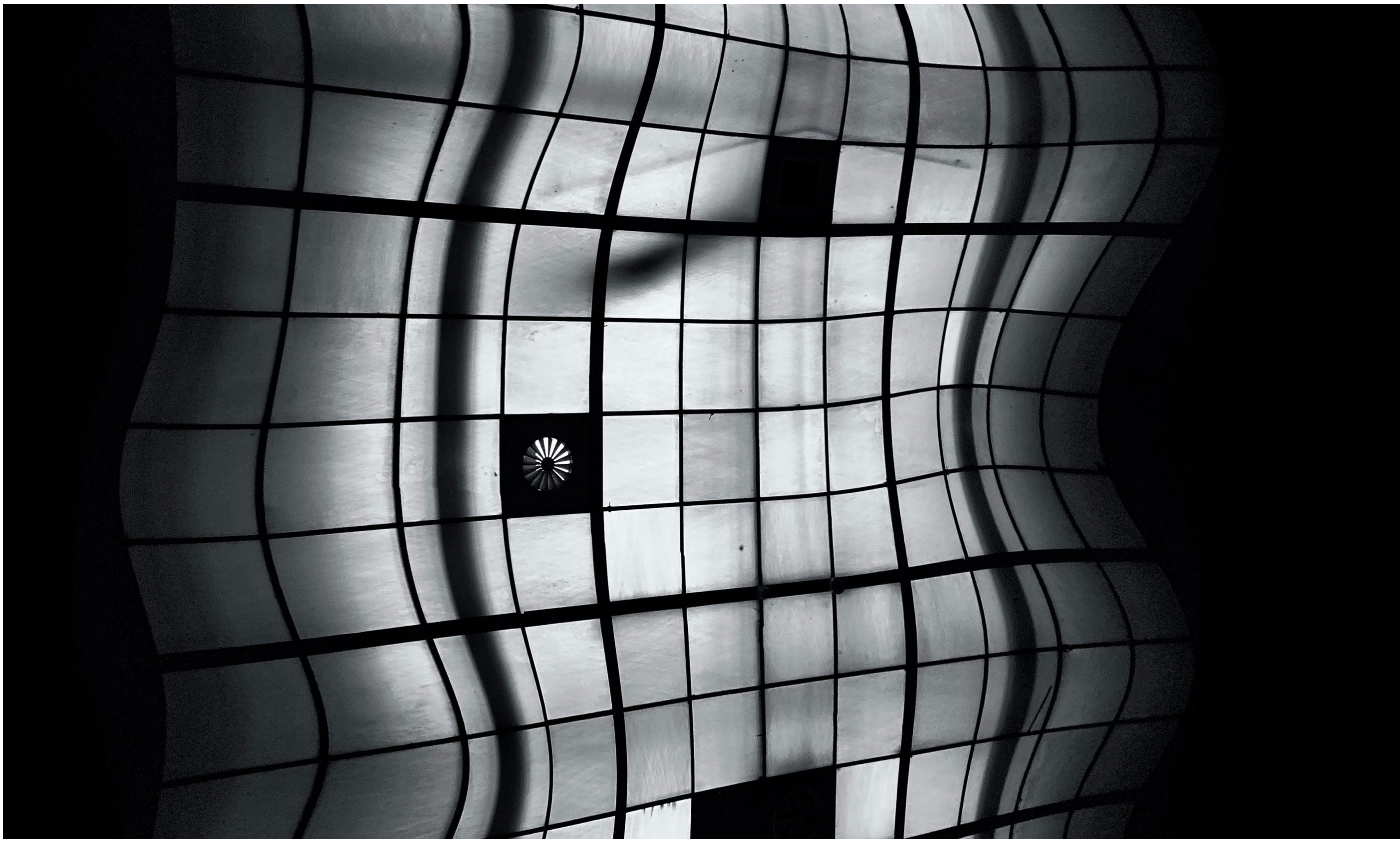
How will blockchain impact the global economy?

An analysis by PwC shows blockchain technology has the potential to boost global gross domestic product (GDP) by $1.76 trillion over the next decade.

“Blockchain technology has long been associated with cryptocurrencies such as Bitcoin, but there is so much more that it has to offer, particularly in how public and private organizations secure, share and use data,” comments Steve Davies, Global Leader, Blockchain and Partner, PwC UK.

Key takeaways:

- The report identifies five key application areas of blockchain and assesses their potential to generate economic value using economic analysis and industry research. The analysis suggests a tipping point in 2025 as blockchain technologies are expected to be adopted at scale across the global economy.
- Tracking and tracing of products and services – or provenance – which emerged as a new priority for many companies’ supply chains during the COVID-19 pandemic, has the largest economic potential ($962bn). Blockchain’s application can be wide ranging and support companies ranging from heavy industries, including mining through to fashion labels, responding to the rise in public and investor scrutiny around sustainable and ethical sourcing.
- Payments and financial services, including use of digital currencies, or supporting financial inclusion through cross border and remittance payments ($433bn).
- Identity management ($224bn) including personal IDs, professional credentials and certificates to help curb fraud and identity theft.
- Application of blockchain in contracts and dispute resolution ($73bn), and customer engagement ($54bn) including blockchain’s use in loyalty programmes further extends blockchain’s potential into a much wider range of public and private industry sectors.



Mapping the motives of insider threats

AUTHOR_Adenike Cosgrove, Cybersecurity Strategy, International, Proofpoint

Unlike many other common attacks, insider attacks are rarely a smash-and-grab. The longer a threat goes undetected, the more damage it can do to your organization.

Insider threats can take many forms, from the absent-minded employee failing to follow basic security protocols, to the malicious insider, intentionally seeking to harm your organization.

Some threats may stem from a simple mistake, others from a personal vendetta. Some insiders will work alone, others at the behest of a competitor or nation-state.

Whatever the method and the motives, the results can be devastating. The average cost of a single negligent insider incident exceeds $300k. That figures increases to over $755k for a criminal or malicious attack and up to $871k for one involving credential theft.

Unlike many other common attacks, insider attacks are rarely a smash-and-grab. The longer a threat goes undetected, the more damage it can do to your organization. The better you understand your people – their motivations, and their relationship with your data and networks – the earlier you can detect and contain potential threats.

Insiders' drivers

Insider threats can be loosely split into two categories – negligent and malicious. Within those categories are a range of potential drivers.

As the mechanics of an attack can differ significantly depending on its motives, gaining a thorough understanding of these drivers can be the difference between a potential threat and a successful breach.

Financial gain

Financial gain is perhaps the most common driver for the malicious insider. Employees across all levels are aware that corporate data and sensitive information has value.

To an employee with access to your data, allowing it to fall into the wrong hands can seem like minimal risk for significant reward.

> *Negligence is the most common cause of insider threats, costing organizations an average of $4.58 million per year.*

This is another threat that is likely higher risk in the current environment. The coronavirus pandemic has placed millions of people under financial pressure, with many furloughed or facing job insecurity. What once seemed an unimaginable decision, may now feel like a quick solution.

Negligence

Negligence is the most common cause of insider threats, costing organizations an average of $4.58 million per year.

Such a threat usually results from poor security hygiene – a failure to properly log in/out of corporate systems, writing down or reusing passwords, using unauthorized devices or applications, and a failure to protect company data.

Negligent insiders are often repeat offenders who may skirt round security for greater speed, increased productivity or just convenience.

Distraction

A distracted employee could fall into the "negligent" category. However, it is worth highlighting separately as this type of threat can be harder to spot.

Where negligent employees may raise red flags by regularly ignoring security best practices, the distracted insider may be a model employee until the moment they make a mistake.

The risk of distraction is potentially higher right now, with most employees working remotely, many for the first time, often interchanging between work and personal applications. Outside of the formal office environment and distracted by home life, they may have different work patterns, be more relaxed and inclined to click on malicious links or bypass formal security conventions.

Organizational damage

Some malicious insiders have no interest in personal gain. Their sole driver is harming your organization.

The headlines are full of stories about the devastating impact of data breaches. For anyone wishing to damage an organization's reputation or revenues, there is no better way in the digital world than by leaking sensitive customer data.

> *Just as they affect method, motives also dictate the appropriate response.*

Insiders with this motivation will usually have a grievance against your business. They may have been looked over for a pay rise or promotion, or recently subject to disciplinary action.

Espionage and sabotage

Malicious insiders do not always work alone. In some cases, they may be passing information to a third-party such as a competitor or a nation-state.

Such cases tend to fall under espionage or sabotage. This could mean a competitor recruiting a plant in your organization to syphon out intellectual property, R&D, or customer information to gain an edge, or a nation-state looking for government secrets or classified information to destabilize another.

Cases like these are on the increase in recent years. Hackers and plants from Russia, China, and North Korea are regularly implicated in cases of corporate and state-sponsored insider attacks against Western organizations.

Defending from within

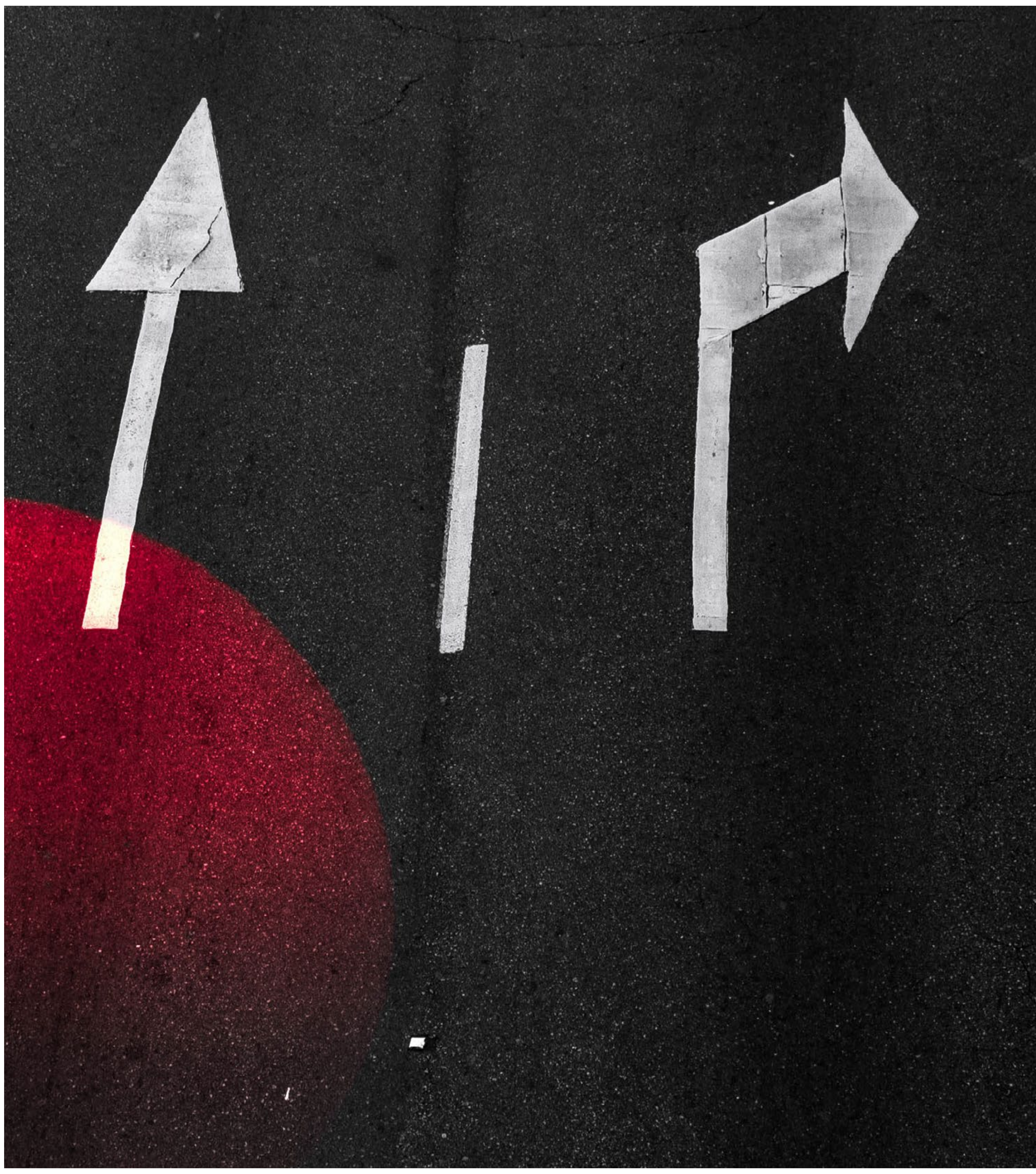
Just as they affect method, motives also dictate the appropriate response. An effective deterrent against negligence is unlikely to deter a committed and sophisticated insider intent on causing harm to your organization.

That said, the foundation for any defense is comprehensive controls. You must have total visibility of your networks – who is using them and what data they are accessing. These controls should be leveraged to limit sensitive information to only the most privileged users and to strictly limit the transfer of data from company systems.

With this broad base in place, you can now add further layers to counter specific threats. To protect against disgruntled employees, for example, additional protections could include filters on company communications to flag high-risk vocabulary, and specific controls applied to high-risk individuals, such as those who have been disciplined or are soon to be leaving the company.

Finally, any successful defense against insider threats should have your people at its heart.

You must create a strong security culture. This means all users must be aware of how their behavior can unintentionally put your organization at risk. All must know how to spot early signs of potential threats, whatever the cause. And all must be aware of the severe consequences of intentionally putting your organization in harm's way.



Three places for early warning of ransomware and breaches that aren't the dark web

AUTHOR_Max Henderson, Incident Response Lead and Senior Security Analyst, Pondurance

The security community is full of Good Samaritans reaching out when they see personal or customer data in harm's way. But are you making it easy for them to find you and are you prepared to act on these discoveries?

For better or worse, a lot of cybercrime sleuthing and forecasting tends to focus on various underground sites and forums across the deep and dark web corners. Whenever a report cites passwords, contraband or fraud kits trafficked in these underground dens, it makes elusive fraudsters and extortion players sound tangible. People instinctively want to infiltrate these spaces to see if their own company and data are up for sale. For time-strapped security professionals, however, the underground's rapidly multiplying corridors are difficult to navigate and correlate at scale. Achieving the capability to sift through these domains productively, without wasting time - or getting in legal entanglements - is no small feat.

But there are three additional, sometimes overlooked sources of early warning clues I have seen yield more direct, actionable insights in my years as an incident response leader.

1_Public sources and Good Samaritans

Sometimes the biggest risks and clues are hiding in plain sight, making it crucial not to overlook less-notorious places and people bringing important things to light. Today the forces of social media and cloud sync-and-share everywhere mean confidential slide decks, C-level cell phone numbers and sensitive databases can hit the public web far too easily. A few configuration swipes on a smartphone can be all that stands between sharing something with a work colleague or with anyone with a search engine. In Verizon's latest Data Breach Investigations Report (DBIR), "misconfiguration" and "misdelivery" errors jumped dramatically as breach factors, now second only to phishing and credential theft on the leader board.

Fortunately, the security community is full of Good Samaritans reaching out when they see personal or customer data in harm's way. But are you making it easy for them to find you and are you prepared to act on these discoveries? Many companies do not have clear, publicly-available contact information and processes for handing security issues and vulnerabilities, which hobbles good faith actors trying to make secure, responsible contact – sometimes until it is too late. Get ahead of any gaps here by establishing dedicated, continuously monitored channels for you to collect and vet inbound tips and concerns.

2_Subtle notes in the 24x7 concert of deployed security tools

> *Keeping an eye on privileged accounts is an invaluable early-warning investment.*

Paradoxically, the more security and compliance tools an organization deploys – ostensibly to gain metrics and situational awareness - the more operators can feel blinded and overwhelmed by data growing faster than they can process it, decide and act on. A strong "defense in depth" gut instinct assumes that for every new control introduced, the bull's-eye visible to attackers must be shrinking. But the bigger assumption here is that we even know "what" and "where" the bull's-eyes are, in the first place. Too often, security tools alone provide data of diminished net value because they are deployed a step behind sprawling cloud systems, IoT devices, increasingly remote employees and other business shifts eclipsing defenders' current understanding of assets.

At the same time, layered product fatigue promotes reliance on security tools' pre-configured alert categories and arbitrary contextualizing, subtly tipping time-strapped administrators to look for reassuring "green light" indicators, before darting to the next dashboard. "What", exactly was detected? Even if it was labeled "low" severity or nuisance activity, does that label change based on what else is being seen on the network? Driving interoperability between tools often trades depth of analysis for speed, burying clues in the process.

Ransomware attacks are a great example: A company typically calls in incident response once an attacker has detonated their ransomware payload and taken infected machines hostage. Yet, the scrambling of data and locking of screens often happens only after a seasoned ransomware gang has gained a foothold in networks for a while and first spent time mapping the size and composition of devices to make sure they hijack every visible device and back-up mechanism.

This precursor activity can get lost in rush-hour noise on the network. Not every security product will classify anomalous indexing and casing of IT systems the same, but setting this activity as critical behavior to recognize helps avert worst-case scenarios by buying time to back-up files or initiate other measures as a precaution.

Likewise, keeping an eye on privileged accounts is an invaluable early-warning investment. First, take stock of who has these accounts in your organization – whether IT administrators, C-suite leaders or their staff. Assume you have too many privileged users in the first place and that some might even be shared. Confirm whether any can be restricted or deleted based on employee turnover or consolidation. Then implement rigorous logging of those narrower accounts' patterns of life. Attackers rely on defenders having incomplete understanding of dormant and other vulnerable accounts. Is the number of privileged accounts changing? Who uses the accounts? Do their logins and behavior match to their role, time zones and workday routines? All things being equal, anomalies with privileged users demand urgent attention.

> *Pinpointing the specific roads business partners have into your environment yields invaluable awareness.*

3_Intersections of third-party risk

The rise and dynamism of third-party developers, resellers, smart building owners and other partners dramatically affects security and compliance inside and outside a company's walls. According to recent Deloitte enterprise risk management research, "information security" and "cyber risk" topped respondents' lists of issues driving budget for greater third-party oversight.

A company may integrate third-party code in its web site or business applications – meaning when that code is compromised, intruders have an express lane into the network. Network and cloud access granted to remote contractors could be compromised, giving criminals the camouflage of previously approved devices and usernames for entry.

Pinpointing the specific roads business partners have into your environment yields invaluable awareness. Take stock of the partners your organization relies on, concentrating on those with the highest associated risk (e.g., close proximity to "crown jewel" data or everyday applications offering wide lateral movement if compromised). Confirm norms and roles for these third-party services and accounts, so logging and monitoring tools can flag deviations immediately, which are often crucial early signs that a third-party might be employed in an attack.

> *Taking stock of a few underutilized, high-yield data sources already in your environment is a powerful way to keep perspective and view all risks on the same plane.*

In addition to serving as a practical early warning outpost, monitoring of third parties yields awareness and influence cybersecurity leaders can use to force wider, strategic conversations in business about risk tolerance and the criticality of these relationships. In addition to weighing the criticality versus risk aspects of these relationships, those watching the third-party touch points are well positioned to advocate for security terms in partner relationships, such as requiring partners to meet thresholds like multi-factor authentication for accounts touching their customers.

Conclusion

Cybersecurity is a constant struggle of measure-versus-countermeasure and the desire to peer into attackers' next move is relentless. While exotic malware and infamous crime rings capture attention and deserve recognition, these threats must still discover and exploit the same vulnerabilities, business churn and network blind spots others have to.

Taking stock of a few underutilized, high-yield data sources already in your environment is a powerful way to keep perspective and view all risks on the same plane. This helps keep things in perspective and frame effective decisions about where and how to prioritize finite resources and test incident response readiness.

The lifecycle of a eureka moment in cybersecurity

AUTHOR_Lior Yaari, CTO, YL Ventures

It takes more than a single eureka moment to attract investor backing, especially in a notoriously high-stakes and competitive industry like cybersecurity.

While every seed-stage investor has their respective strategies for vetting raw ideas, my experience of the investment due diligence process involves a veritable ringer of rapid-fire, back-to-back meetings with cybersecurity specialists and potential customers, as well as rigorous market scoping by analysts and researchers.

> *The cybersecurity industry is saturated with features passing themselves off as platforms.*

As the CTO of a seed-stage venture capital firm entirely dedicated to cybersecurity, I spend a good portion of my time ideating alongside early-stage entrepreneurs and working through this process with them. To do this well, I've had to develop an internal seismometer for industry pain points and potential competitors, play matchmaker between tech geniuses and industry decision-makers, and peer down complex roadmaps to find the optimal point of convergence for good tech and good business.

Along the way, I've gained a unique perspective on the set of necessary qualities for a good idea to turn into a successful startup with significant market traction.

Just as a good idea doesn't necessarily translate into a great product, the qualities of a great product don't add up to a magic formula for guaranteed success. However, how well an idea performs in the categories I set out below can directly impact the confidence of investors and potential customers you're pitching to. Therefore, it's vital that entrepreneurs ask themselves the following before a pitch:

Do I have a strong core value proposition?

The cybersecurity industry is saturated with features passing themselves off as platforms. While the accumulated value of a solution's features may be high, its core value must resonate with customers above all else. More pitches than I wish to count have left me scratching my head over a proposed solution's ultimate purpose. Product pitches must lead with and focus on the solution's core value proposition, and this proposition must be able to hold its own and sell itself.

> *It's critical to factor in the maintenance cost and "tech debt" of solutions that are environment-dependent on account of integrations with other tools or difficult deployments.*

Consider a browser security plugin with extensive features that include XSS mitigation, malicious website blocking, employee activity logging and download inspections. This product proposition may be built on many nice-to-have features but, without a strong core feature, it doesn't add up to a strong product that customers will be willing to buy. Add-on features, should they need to be discussed, ought to be mentioned as secondary or additional points of value.

> *From the moment your idea raises funds, your solution will be running against the clock to provide its promised value, successfully interact with the market and adapt itself where necessary.*

What is my solution's path to scalability?

Solutions must be scalable in order to reach as many customers as possible and avoid price hikes with reduced margins. Moreover, it's critical to factor in the maintenance cost and "tech debt" of solutions that are environment-dependent on account of integrations with other tools or difficult deployments.

I've come across many pitches that fail to do this, and entrepreneurs who forget that such an omission can both limit their customer pool and eventually incur tremendous costs for integrations that are destined to lose value over time.

What is my product experience like for customers?

A solution's viability and success lie in so much more than its outcome. Both investors and customers require complete transparency over the ease-of use of a product in order for it to move forward in the pipeline. Frictionless and resource-light deployments are absolutely key and should always mind the realities of inter-departmental politics. Remember, the requirement of additional hires for a company to use your product is a hidden cost that will ultimately reduce your margins.

Moreover, it can be very difficult for companies to rope in the necessary stakeholders across their organization to help your solution succeed. Finally, requiring hard-to-come-by resources for a POC, such as sensitive data, may set up your solution for failure if customers are reluctant to relinquish the necessary assets.

What is my solution's time-to-value?

Successfully discussing a core value must eventually give way to achieving it. Satisfaction with a solution will always ultimately boil down to deliverables. From the moment your idea raises funds, your solution will be running against the clock to provide its promised value, successfully interact with the market and adapt itself where necessary.

The ability to demonstrate strong initial performance will draw in sought-after design partners and allow you to begin selling earlier. Not only are these sales necessary bolsters to your follow-on rounds, they also pave the way for future upsells to customers. It's critical, where POCs are involved, that the beta content installed by early customers delivers well in order to drive conversions and complete the sales process. It's critical to create a roadmap for achieving this type of deliverability that can be clearly articulated to your stakeholders.

Early-stage startups must build their way up to solving big problems and reconcile with the fact that they are typically only equipped to resolve small ones until they reach maturity.

When will my solution deliver value?

It's all too common for entrepreneurs to focus on "the ultimate solution". This usually amounts to what they hope their solution will achieve some three years into development while neglecting the market value it can provide along the way. While investors are keen to embrace the big picture, this kind of entrepreneurial tunnel vision hurts product sales and future fundraising.

Early-stage startups must build their way up to solving big problems and reconcile with the fact that they are typically only equipped to resolve small ones until they reach maturity. This must be communicated transparently to avoid creating a false image of success in your market validation.

Avoid asking "do you need a product that solves your [high-level problem]?" and ask instead "would you pay for a product that solves this key element of your [high-level problem]?".

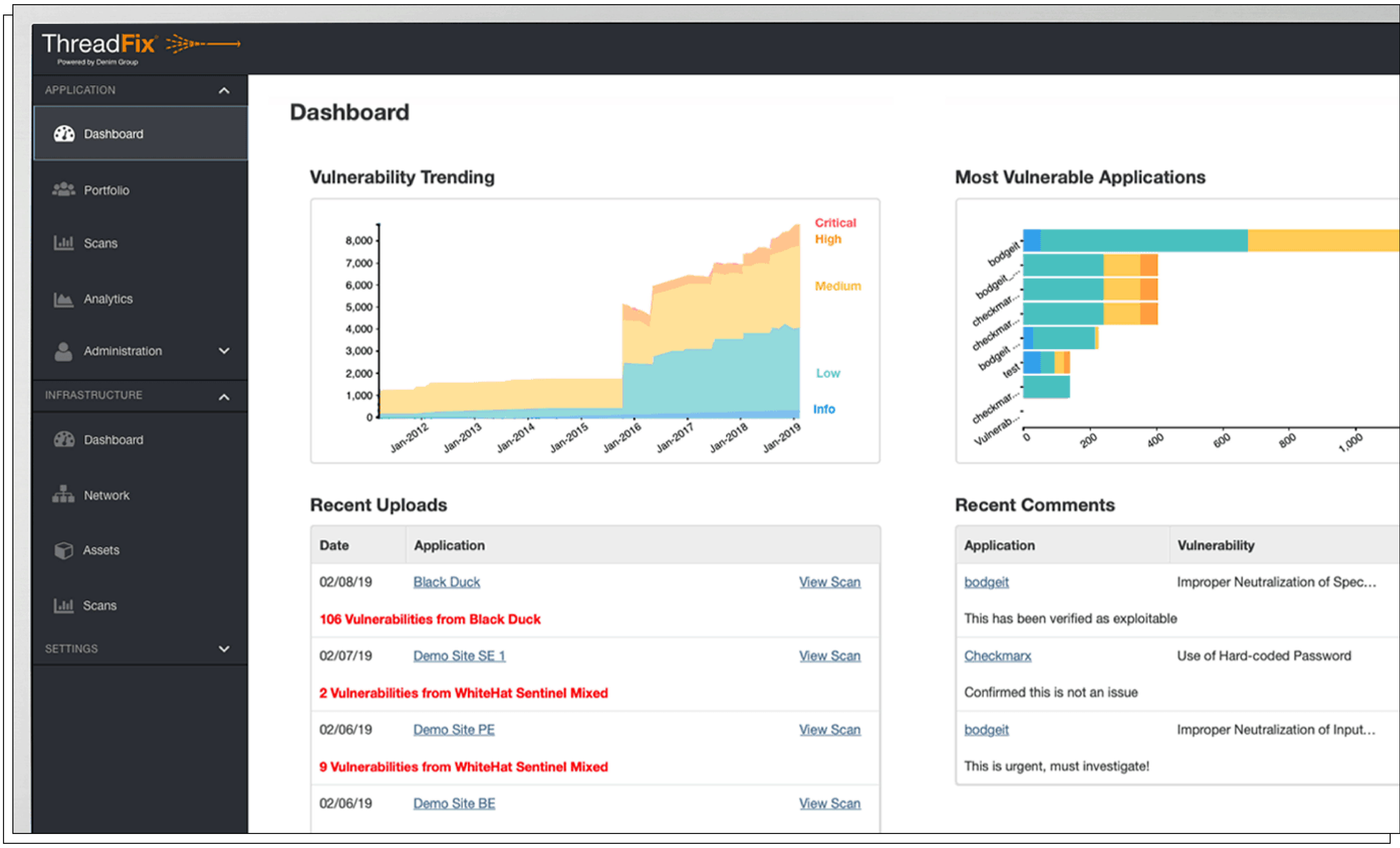
Unless an idea breaks completely new ground or looks to secure new tech, it's likely to be an improvement to an already existing solution. In order to succeed at this, however, it's critical to understand the failures and drawbacks of existing solutions before embarking on building your own.

Cybersecurity buyers are often open to switching over to a product that works as well as one they already use without its disadvantages. However, it's incumbent on vendors to avoid making false promises and follow through on improving their output.

The cybersecurity industry is full of entrepreneurial genius poised to disrupt the current market. However, that potential can only manifest by designing it to address much more than mere security gaps.

The lifecycle of a good cybersecurity idea may start with tech, but it requires a powerful infusion of foresight and listening to make it through investor and customer pipelines. This requires an extraordinary amount of research in some very unexpected places, and one of the biggest obstacles ideating entrepreneurs face is determining precisely what questions to ask and gaining access to those they need to understand.

Working with well-connected investors dedicated to fostering those relationships, ironing out roadmap kinks in the ideation process is one of the surest ways to secure success. We must focus on building good ideas sustainably and remember that immediate partial value delivery is a small compromise towards building out the next great cybersecurity disruptor.



Dashboard

Vulnerability Trending

Most Vulnerable Applications

Recent Uploads

Date	Application	
02/08/19	Black Duck	View Scan
106 Vulnerabilities from Black Duck		
02/07/19	Demo Site SE 1	View Scan
2 Vulnerabilities from WhiteHat Sentinel Mixed		
02/06/19	Demo Site PE	View Scan
9 Vulnerabilities from WhiteHat Sentinel Mixed		
02/06/19	Demo Site BE	View Scan

Recent Comments

Application	Vulnerability
bodgeit	Improper Neutralization of Spec...
This has been verified as exploitable	
Checkmarx	Use of Hard-coded Password
Confirmed this is not an issue	
bodgeit	Improper Neutralization of Input...
This is urgent, must investigate!	

> *Most best practices – e.g. CIS Controls, the OWASP Vulnerability Management Guide – advocate a continuous program of asset discovery and vulnerability management.*

Review: ThreadFix 3.0

AUTHOR_Toni Grzinic, Security Researcher

Maintaining a strong organizational security posture is a demanding task.

Most best practices – e.g. CIS Controls, the OWASP Vulnerability Management Guide – advocate a continuous program of asset discovery and vulnerability management. Due to fundamental changes in infrastructure provisioning and paradigm shifts like Infrastructure as Code (IaC), most organizations had to shift their regular vulnerability assessments to a more frequent pattern.

Adoption of Agile and DevOps practices in managing infrastructure, as well as frequent news about negligent secure practices that led to breaches in high-profile organizations, have pushed organizations to take security practices more seriously and to adopt a continuous vulnerability management process, which moves security tests and controls into earlier stages of the software development lifecycle and becomes a default prerequisite in the product requirements.

Security teams have a wide choice of vulnerability assessment tools, from static code analyzers (SAST) to dynamic ones (DAST). Most of these tools can be used to complement each other and give a wider view on the potential vulnerabilities found in the tested applications and infrastructure.

How to prioritize and follow up on findings of complementary vulnerability scanners? A lot of data is generated during the vulnerability assessment process and most of it should be double-checked to pinpoint only meaningful findings. Viewing a 100+ page PDF report or tracking the remediation status in a spreadsheet that takes an eternity to load can only result in headaches. A manual vulnerability management process also prevents us from tracking defined performance indicators and from achieving efficient collaboration.

This is a review of ThreadFix 3.0, a vulnerability management platform that helps organizations overcome these challenges and manage risky applications and infrastructure efficiently and in alignment with the agile development processes.

ThreadFix vulnerability resolution platform

ThreadFix is a software vulnerability aggregation and management system that can schedule vulnerability scans, organize and merge aggregated vulnerability reports, and integrate with popular security and software development tools. It addresses the problems of organizations that have an established vulnerability management program and have identified challenges in data management and collaboration between teams.

ThreadFix enables organizations to:

- **Consolidate test results** by de-duplicating and merging imported results from more than 40 commercial and open source dynamic (DAST), static (SAST), Software Composition Analysis (SCA) tools, and interactive (IAST) application scanning tools. ThreadFix can track manual findings and observations from code-reviews, threat modelling and penetration tests. Normalization and merging of test results between various types of tools is done by a patented technology called Hybrid Analysis Mapping. It also enables the correlation of found vulnerabilities at the network infrastructure and application level.
- **Improve vulnerability management** by integrating ThreadFix with various defect/bug trackers (Jira, Azure DevOps Server, IBM Rational ClearQuest, etc.) and developer tools. This removes the friction between software developers, system operations and security teams, and helps decrease the time spent on coordinating and fixing prioritized vulnerabilities. As software development and system operations teams resolve found deficiencies, ThreadFix detects these changes, enabling the security team to perform follow-up testing to confirm that these security holes have been closed.
- **Schedule orchestrated scans** with remote scanners. After the scan is finished the report is merged and becomes visible in ThreadFix.
- **Prioritize risk decisions.** ThreadFix reporting and analytics capabilities enable organizations to quickly identify vulnerability trends and make informed remediation decisions based on current vulnerability data. It gives visibility into how quickly the found vulnerabilities are resolved and supports reporting functions that provide security managers with up-to-date metrics

needed to conduct data-driven conversations with upper management, which help estimate the efficiency of the security program or future actions. ThreadFix integrates with GRC tools, like ServiceNow GRC.

- **Quickly isolate and pinpoint suspect vulnerability data** using custom filters, to reprioritize their remediation plan.

Methodology

For this review, we used a test instance of ThreadFix that has been provisioned on Amazon Web Services by the vendor.

> *ThreadFix divides the vulnerability management in infrastructure- and application-related vulnerabilities.*

You can find straightforward instructions in the documentation to spin up your ThreadFix instance, should you wish to do so. All ThreadFix components are dockerized so it takes a Docker Compose one-liner to build the environment – this simplifies a lot the installation procedure and comes handy if you use container orchestration tools.

For testing purposes, we scanned intentionally vulnerable applications to get vulnerability reports that will populate the instance.

ThreadFix divides the vulnerability management in infrastructure- and application-related vulnerabilities.

> *After logging into ThreadFix, you are welcomed with a dashboard page containing statistics about the accumulated infrastructure scans.*

We scanned the infrastructure with Qualys VM and Tenable Nessus. We uploaded manually the scan reports in ThreadFix, but this part can also be automated by configuring remote scanners.

We tested the application capabilities with various SAST and DAST tools: Burp Pro, Brakeman, the Acunetix web vulnerability scanner, Appscan, Fortify SCA, OWASP Zed Attack Proxy and Checkmarx, by scanning intentionally vulnerable applications: bodgeit, RailsGoat and Wavsep.

With the test instance running and the data present, we proceeded to evaluate ThreadFix by its main components:

- Infrastructure vulnerability management
- Applications vulnerability management
- Reporting & analytics
- Integrations (defect trackers and remote scanners)
- API

Tracking infrastructure assets and application vulnerabilities

After logging into ThreadFix, you are welcomed with a dashboard page containing statistics about the accumulated infrastructure scans (Figure 1).

The dashboard shows:

- Statistics about opened, closed and new vulnerabilities
- Vulnerability trends over several months
- A breakdown of operating system used
- Statistics about most vulnerable networks and hosts
- The most common CVEs found on your infrastructure.

The initial dashboard can be customized through the solution's settings, like all the other ThreadFix dashboards.

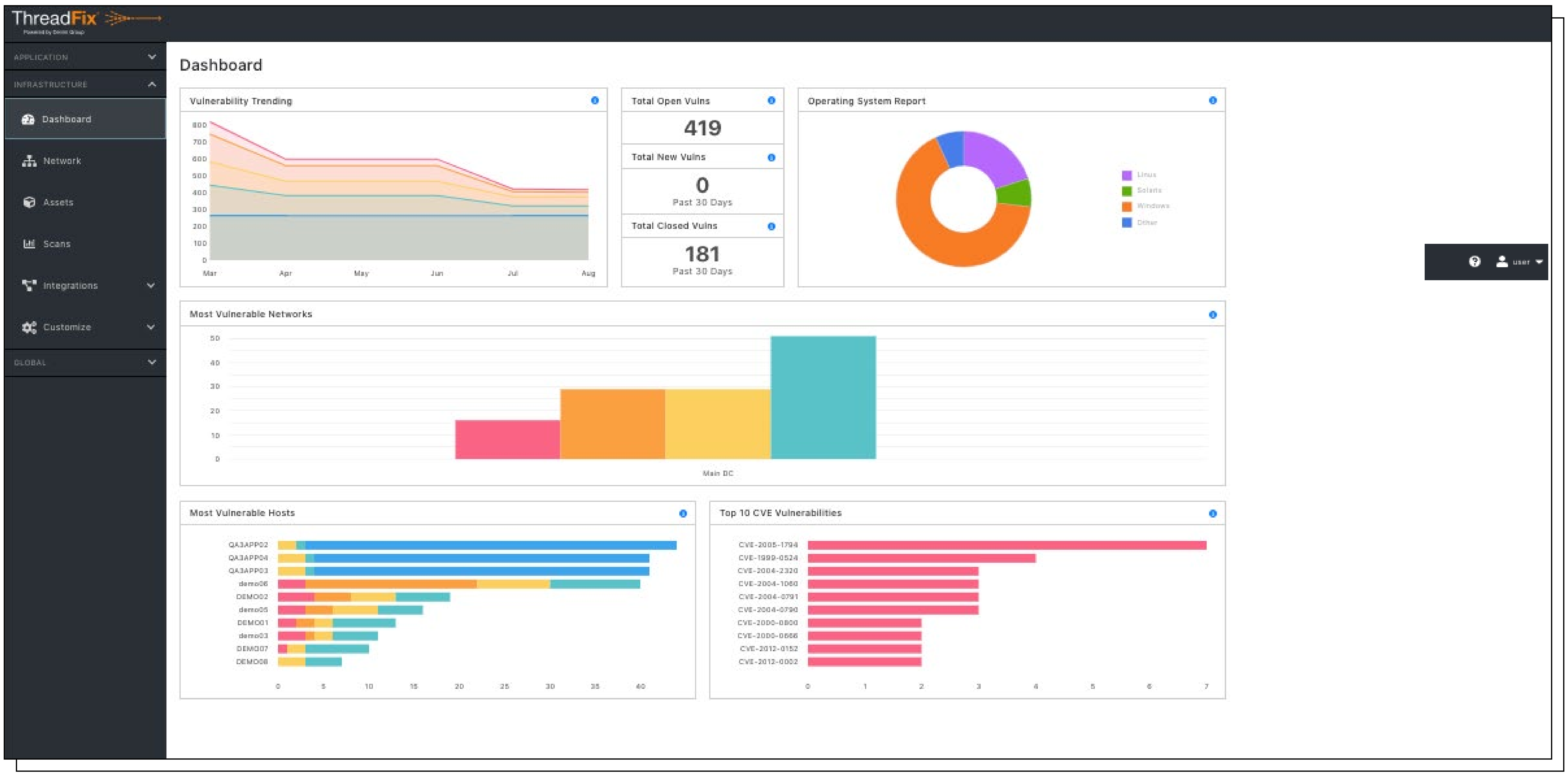


FIGURE 1. INFRASTRUCTURE DASHBOARD

Infrastructure

As previously mentioned, ThreadFix divides the vulnerability management in two sections: infrastructure and application.

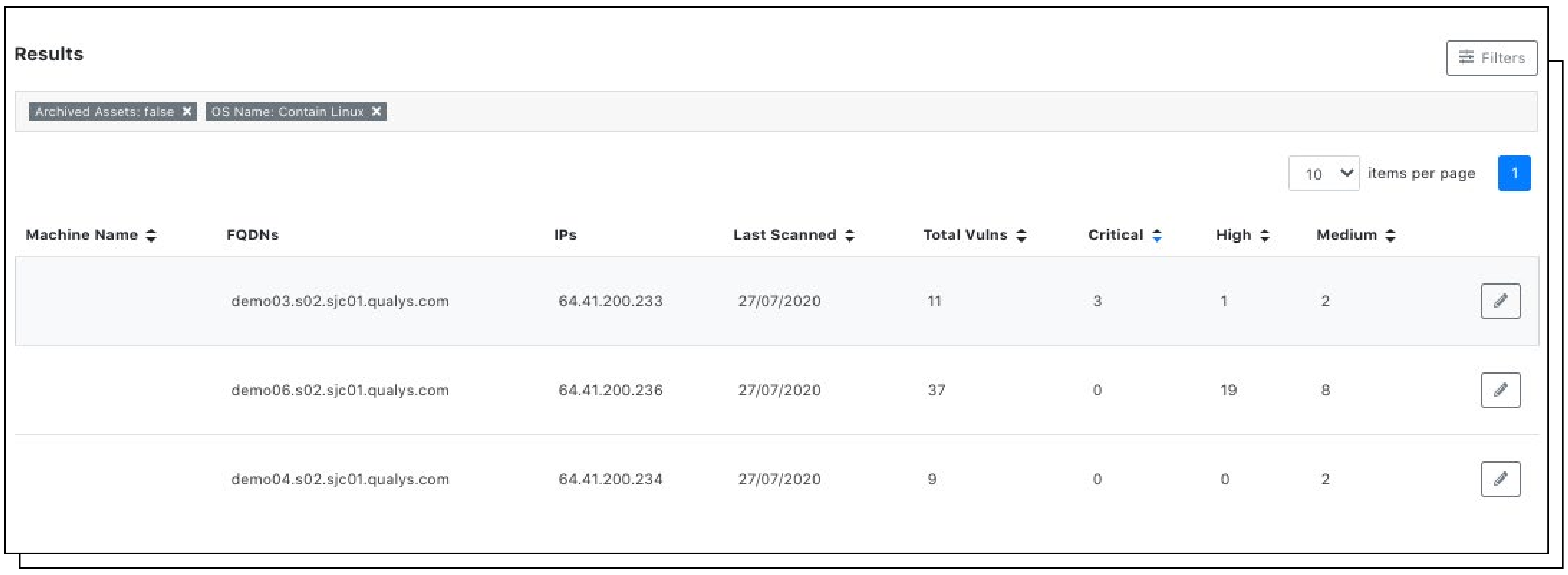
The infrastructure is represented with internal networks and public networks related to data centers or cloud environments where the applications are deployed. The network IP ranges are manually configured and can be enriched with additional metadata (Location, Department, Description). These defined networks are later mapped to uploaded vulnerability reports.

ThreadFix has successfully recognized our efforts to upload duplicated or corrupted reports.

After the reports were successfully uploaded, we started drilling down the findings either by focusing on the network or host level. Hosts are mapped based on scan results and populated with their FQDN (if available), IP and MAC addresses, and recognized operating systems.

You can also search through your assets based on the populated fields, which is efficient when you want to inspect the asset or look at the remediation status.

The infrastructure view enables us to efficiently choose hosts that we want to prioritize for remediation actions by using the available filters and sorting actions. For example, in the hosts table we can sort the vulnerabilities by their severity and choose the hosts with the most critical and high vulnerabilities (see Figure 2). Or, we can narrow down our search by filtering hosts with a specific operating system that share a specific vulnerability and can be fixed jointly.



Results

☰ Filters

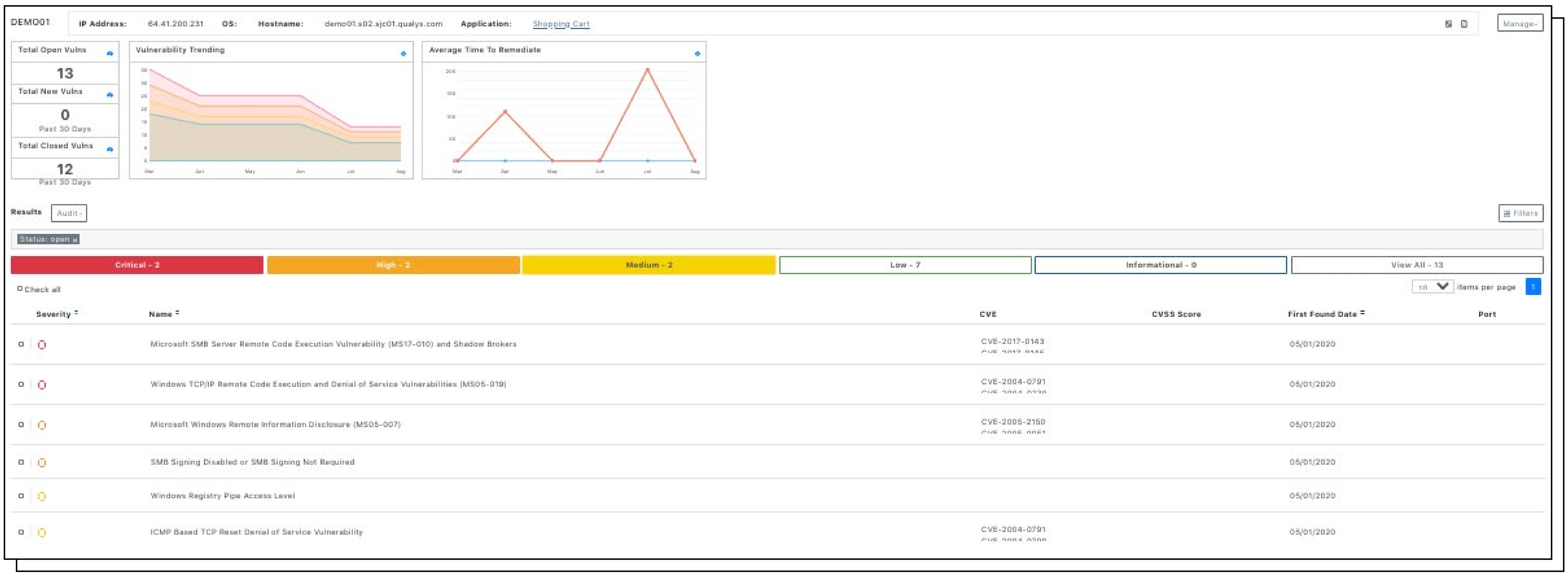
Archived Assets: false ✕ | OS Name: Contain Linux ✕

10 items per page 1

Machine Name	FQDNs	IPs	Last Scanned	Total Vulns	Critical	High	Medium	
	demo03.s02.sjc01.qualys.com	64.41.200.233	27/07/2020	11	3	1	2	✎
	demo06.s02.sjc01.qualys.com	64.41.200.236	27/07/2020	37	0	19	8	✎
	demo04.s02.sjc01.qualys.com	64.41.200.234	27/07/2020	9	0	0	2	✎

FIGURE 2. USING INFRASTRUCTURE FILTERS CAN COME HANDY WHEN PRIORITIZING SPECIFIC REMEDIATION ACTIONS

By clicking on a host you can view vulnerabilities details and audit them (Figure 3), and you can filter vulnerabilities by their severity and status (Open, Closed, Mitigated, Accepted risk, False Positive). This workflow for auditing infrastructure is very user friendly, and the vulnerability mappings work pretty well. Filters are well covered in every infrastructure page, and we can stack vulnerabilities or inspect recurring ones.



DEMO01 | IP Address: 64.41.200.231 | OS: | Hostname: demo01.s02.sjc01.qualys.com | Application: Shopping Cart

Manage-

Total Open Vulns: 13

Total New Vulns: 0 (Past 30 Days)

Total Closed Vulns: 12 (Past 30 Days)

Results Audit -

☰ Filters

Status: open ✕

Critical - 2 | High - 2 | Medium - 2 | Low - 7 | Informational - 0 | View All - 13

□ Check all

10 items per page 1

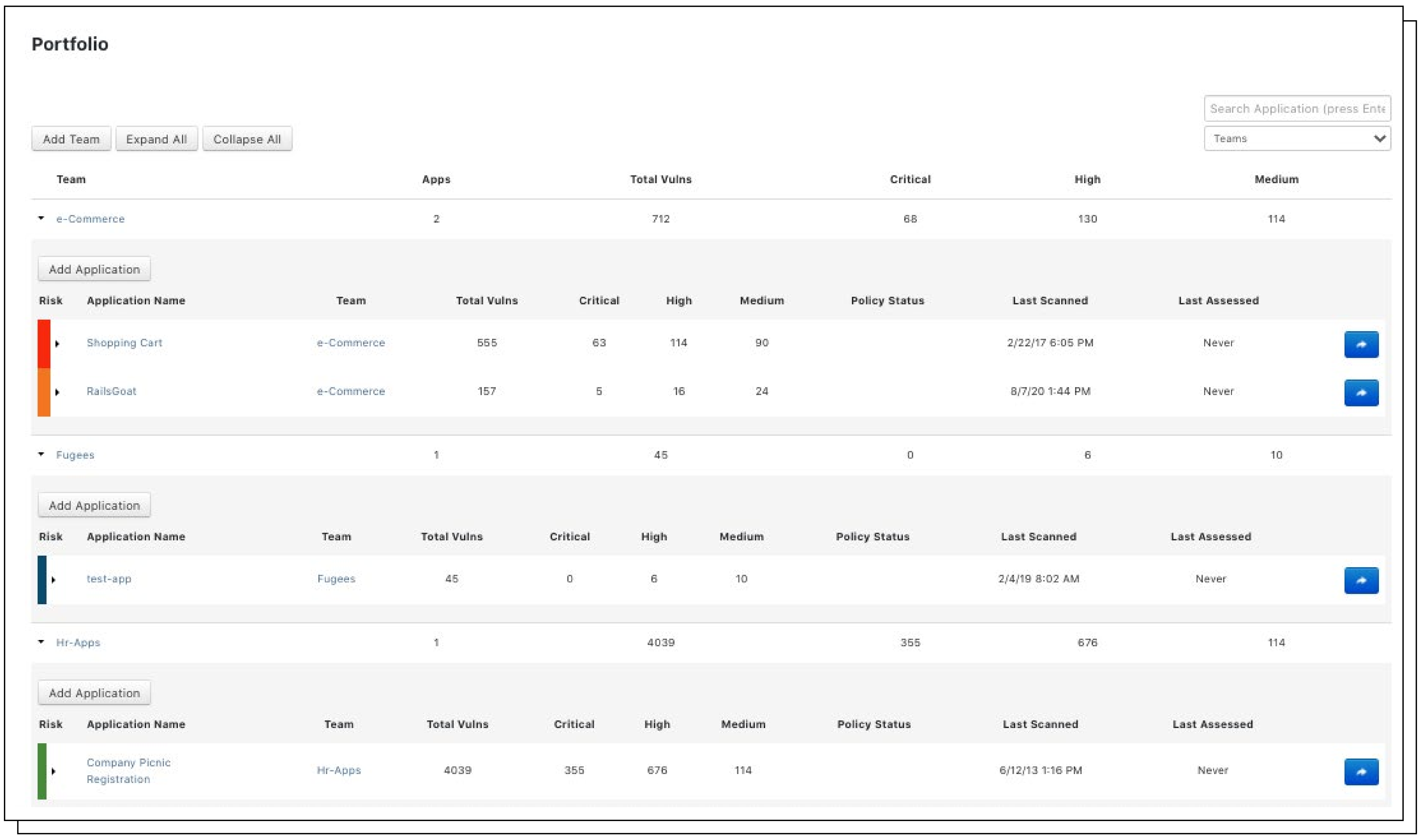
	Severity	Name	CVE	CVSS Score	First Found Date	Port
□	○	Microsoft SMB Server Remote Code Execution Vulnerability (MS17-010) and Shadow Brokers	CVE-2017-0143		05/01/2020	
□	○	Windows TCP/IP Remote Code Execution and Denial of Service Vulnerabilities (MS05-019)	CVE-2004-0791		05/01/2020	
□	○	Microsoft Windows Remote Information Disclosure (MS05-007)	CVE-2005-2150		05/01/2020	
□	○	SMB Signing Disabled or SMB Signing Not Required			05/01/2020	
□	○	Windows Registry Pipe Access Level			05/01/2020	
□	○	ICMP Based TCP Reset Denial of Service Vulnerability	CVE-2004-0791		05/01/2020	

FIGURE 3. HOST VULNERABILITY REPORT

Applications

ThreadFix automatizes the process of application vulnerability management by inspecting source code with a SAST tool and by scanning repeatedly the running application with a DAST tool. In ThreadFix every application is owned by a team and it can be tagged with custom tags that are helpful when used with filters. Tags are identifiers related to applications, vulnerabilities and vulnerability comments.

The applications portfolio shows the current teams and associated applications (Figure 4).



Portfolio

Team	Apps	Total Vulns	Critical	High	Medium
e-Commerce	2	712	68	130	114
Fugees	1	45	0	6	10
Hr-Apps	1	4039	355	676	114

Risk	Application Name	Team	Total Vulns	Critical	High	Medium	Policy Status	Last Scanned	Last Assessed
🟥	Shopping Cart	e-Commerce	555	63	114	90		2/22/17 6:05 PM	Never
🟧	RailsGoat	e-Commerce	157	5	16	24		8/7/20 1:44 PM	Never

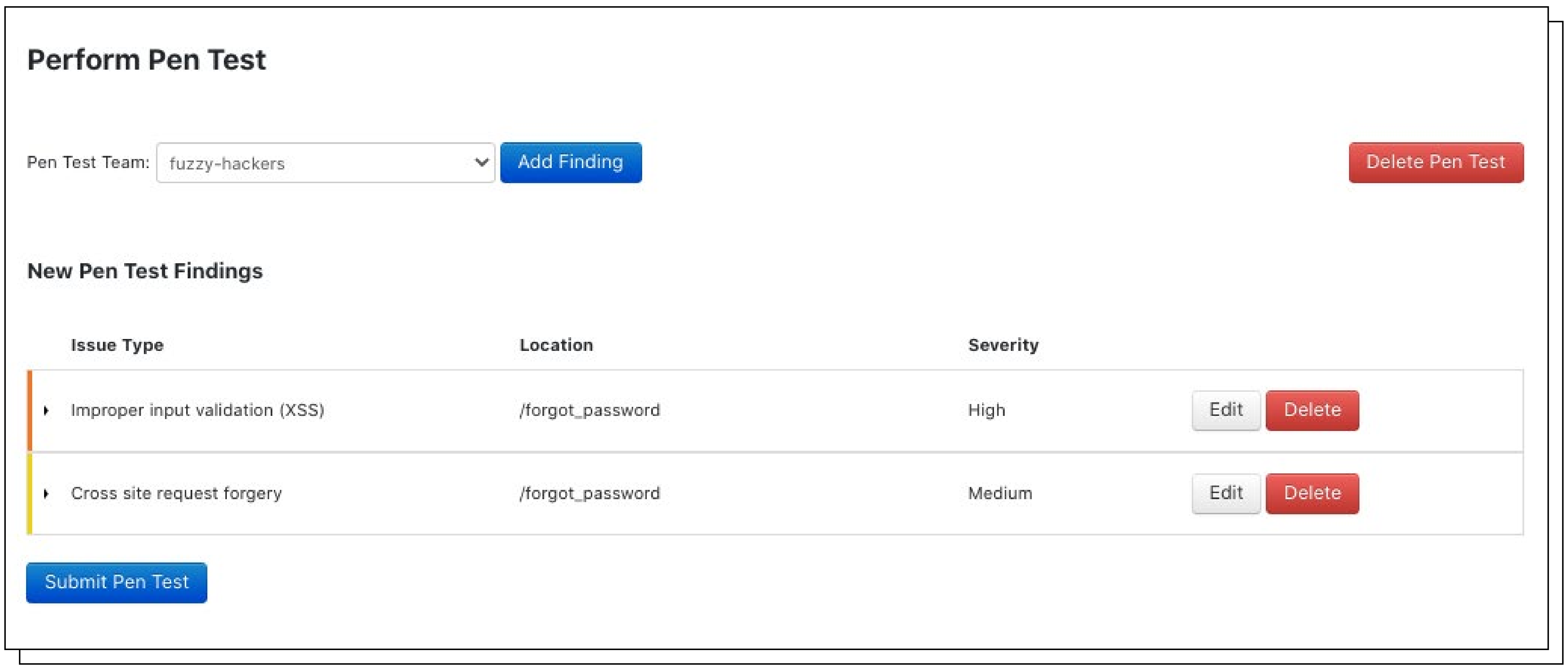
Risk	Application Name	Team	Total Vulns	Critical	High	Medium	Policy Status	Last Scanned	Last Assessed
🟦	test-app	Fugees	45	0	6	10		2/4/19 8:02 AM	Never

Risk	Application Name	Team	Total Vulns	Critical	High	Medium	Policy Status	Last Scanned	Last Assessed
🟩	Company Picnic Registration	Hr-Apps	4039	355	676	114		6/12/13 1:16 PM	Never

FIGURE 4. APPLICATIONS PORTFOLIO

Applications can be connected with a Git repository, which can be used for static code analysis.

The uploading and parsing of vulnerability scans reports went without a hiccup. You can request a service engagement, which comes handy when you need a re-scan or a manual check after fixing an issue in the application. ThreadFix also allows you to define the penetration testing team that can collaborate on findings within the chosen application. After the pen test is done, you can see the results under Assessments (Figure 5).



Perform Pen Test

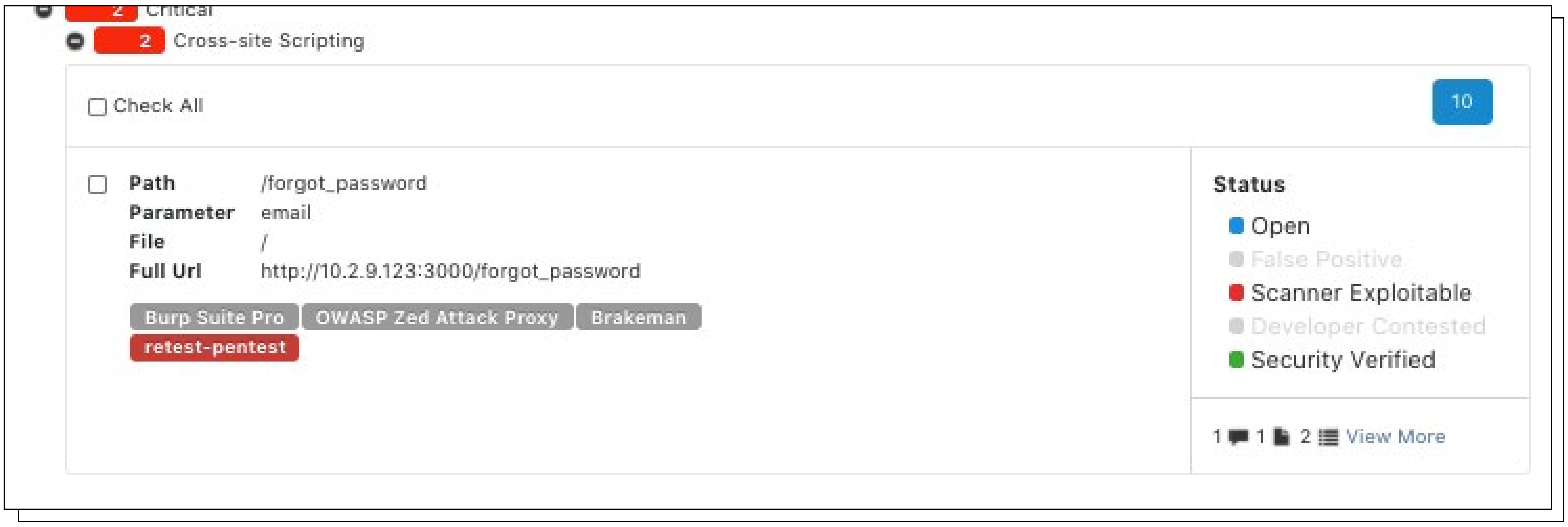
Pen Test Team: fuzzy-hackers

New Pen Test Findings

Issue Type	Location	Severity	
Improper input validation (XSS)	/forgot_password	High	Edit Delete
Cross site request forgery	/forgot_password	Medium	Edit Delete

FIGURE 5. SUMMARY OF A MANUAL PENETRATION TEST

ThreadFix converts all uploaded vulnerability reports to the ThreadFix format and maps vulnerabilities to Common Weakness Enumeration (CWE) identifiers. It also detects and merges similar vulnerabilities found by different tools (Figure 6).



2 Critical

2 Cross-site Scripting

□ Check All

10

□ **Path** /forgot_password
Parameter email
File /
Full Url http://10.2.9.123:3000/forgot_password

Burp Suite Pro | OWASP Zed Attack Proxy | Brakeman
retest-pentest

Status
- ● Open
- ● False Positive
- ● Scanner Exploitable
- ● Developer Contested
- ● Security Verified

1 💬 1 📄 2 ☰ View More

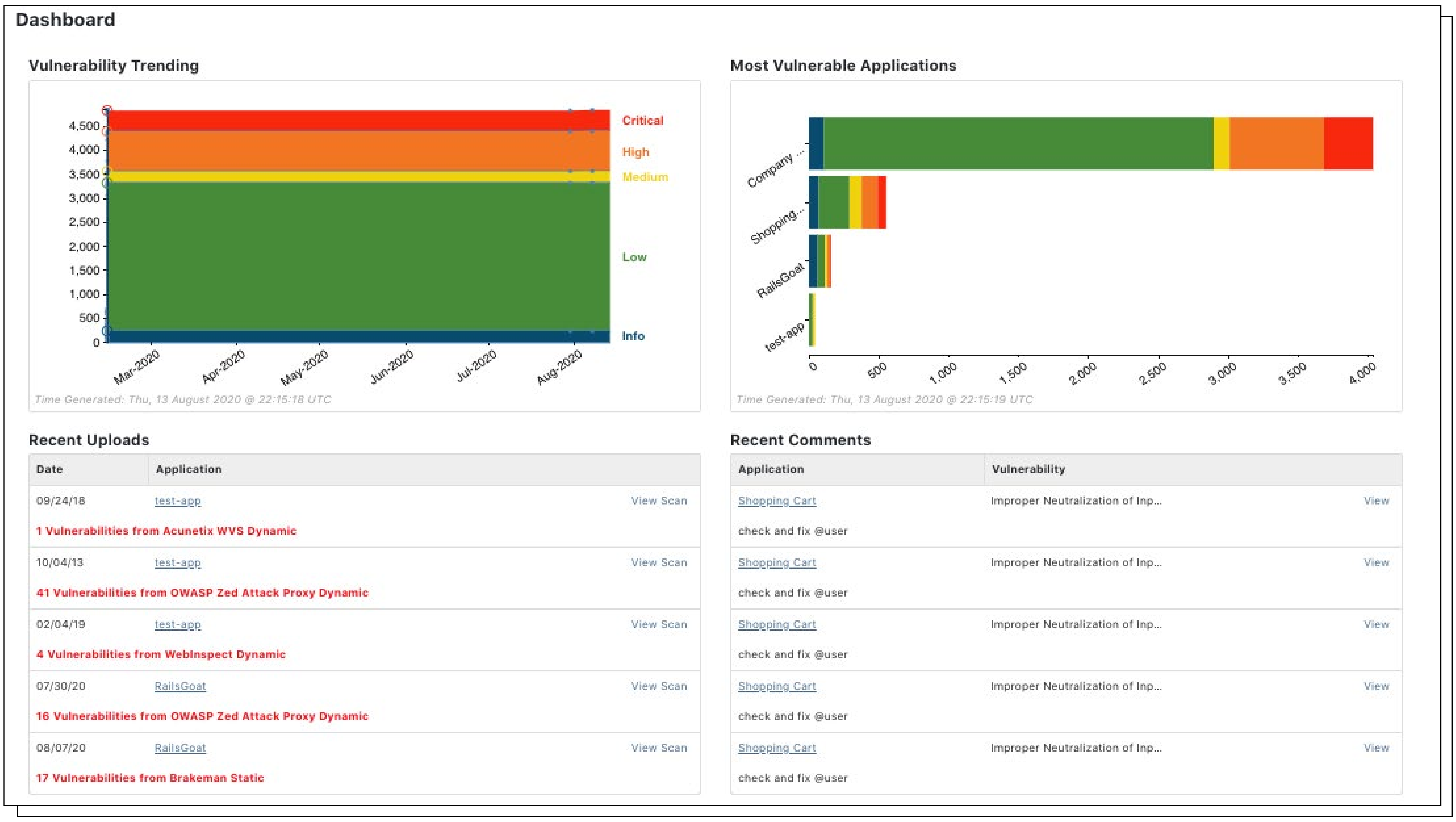
FIGURE 6. THREADFIX MERGED A VULNERABILITY FOUND B Y DIFFERENT TOOLS

ThreadFix offers unlimited search, filter and pivot options for application vulnerability reports. Pivot options allow you to narrow down interesting vulnerabilities but also hunt for potential false positives when comparing various tools (e.g., when you pivot by severity and scanner type). You can search reports by vulnerabilities, scanner, tags, CVE, paths affected, status, date range of scan, and more. ThreadFix also offers to save and export complex filters, which can be handy when you get back to a specific application report after some time.

Saved filters can be also used as a baseline for custom policies in ThreadFix. Policies are calls to action for your team, they usually compare the current remediation status against a desired baseline. Filter policy is a simple rule-based filter that shows a Pass or Fail indicator in the application dashboard if the application meets or fails to meet the defined requirements. For example, filter policy defines that, to pass, an application should have no critical or high vulnerabilities. Another interesting policy is the time-to-remediate policy. The concept is simple: you define a desired fix deadline for a severity level and ThreadFix sets a custom reminder that notifies your team about it.

> *The most popular report is the trending report that shows the remediation effects over time and is also visible under an application dashboard.*

A nice feature that improves collaboration between users is commenting and tagging vulnerabilities in the remediation process. You can filter vulnerabilities that have a comment and continue tracking their progress. This feature can be used during penetration testing engagements when multiple people work on the same application and record their progress but is also useful in the remediation phase (see Figure 7). While commenting, you can attach various files to the comment to clarify the vulnerability. Mature security teams that have established roles and a vulnerability management procedure will find tagging and commenting useful for pushing collaboration efforts while prioritizing next actions and tracking current actions.



Dashboard

Vulnerability Trending

Time Generated: Thu, 13 August 2020 @ 22:15:18 UTC

Most Vulnerable Applications

Time Generated: Thu, 13 August 2020 @ 22:15:19 UTC

Recent Uploads

Date	Application	
09/24/18	test-app	View Scan
1 Vulnerabilities from Acunetix WVS Dynamic		
10/04/13	test-app	View Scan
41 Vulnerabilities from OWASP Zed Attack Proxy Dynamic		
02/04/19	test-app	View Scan
4 Vulnerabilities from WebInspect Dynamic		
07/30/20	RailsGoat	View Scan
16 Vulnerabilities from OWASP Zed Attack Proxy Dynamic		
08/07/20	RailsGoat	View Scan
17 Vulnerabilities from Brakeman Static		

Recent Comments

Application	Vulnerability	
Shopping Cart	Improper Neutralization of Inp...	View
check and fix @user		
Shopping Cart	Improper Neutralization of Inp...	View
check and fix @user		
Shopping Cart	Improper Neutralization of Inp...	View
check and fix @user		
Shopping Cart	Improper Neutralization of Inp...	View
check and fix @user		
Shopping Cart	Improper Neutralization of Inp...	View
check and fix @user		

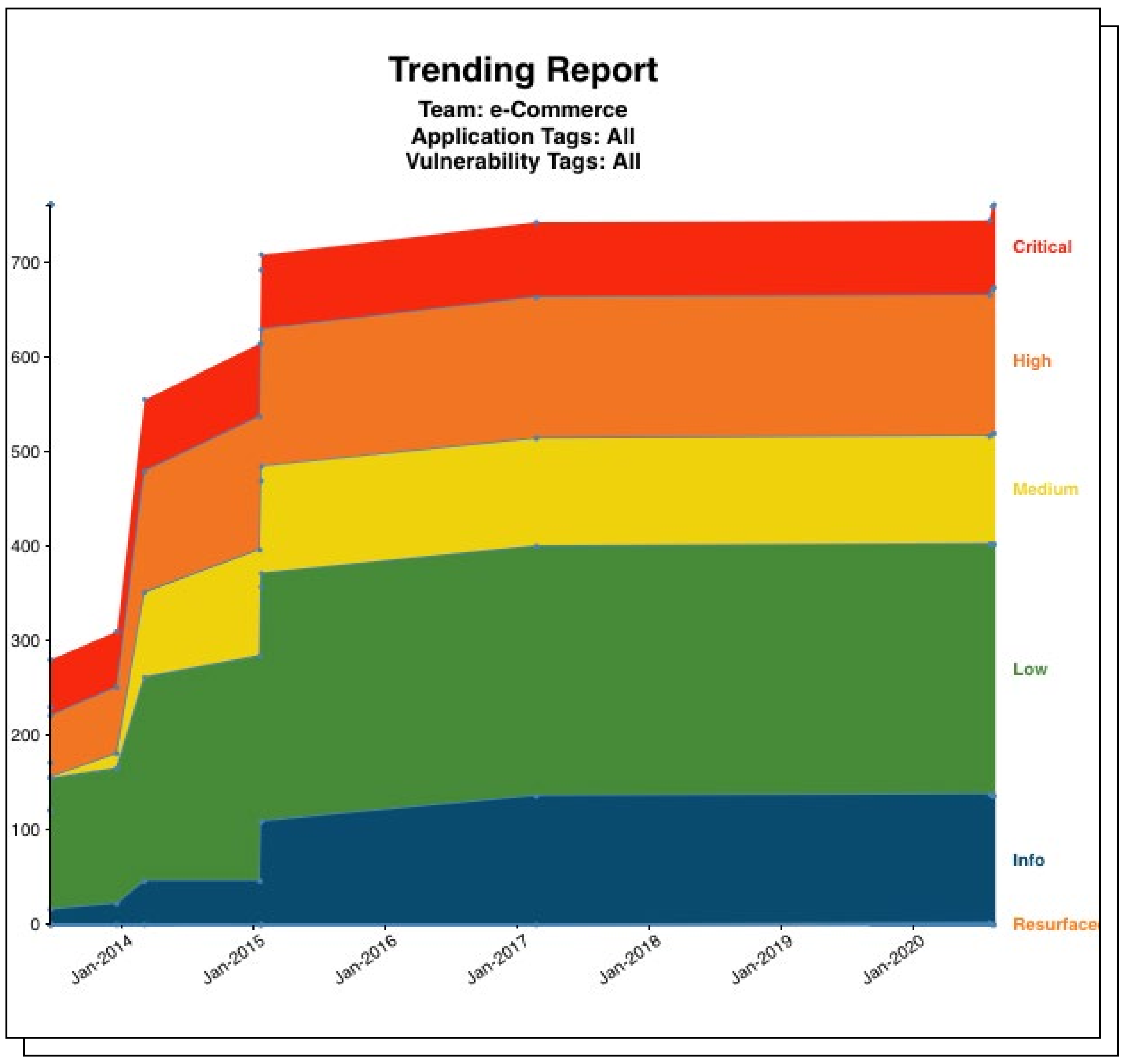
FIGURE 7. APPLICATION DASHBOARD SHOWS RECENT TRENDS, UPLOADS, AND COMMENTS

Reporting and analytics

> *The Most Vulnerable Applications report shows the most affected applications and gives insight into their vulnerability composition.*

ThreadFix has exhaustive options to inspect application vulnerabilities with multiple views and level of detail. There are ten report types, each with its own filter set. This vast number of combinations enables users to be creative when producing data reports for the upper management.

The most popular report is the trending report that shows the remediation effects over time and is also visible under an application dashboard (see Figure 8). This simple but powerful visualization shows how your team is doing on solving found vulnerabilities through a selected time period.



Trending Report

Team: e-Commerce
Application Tags: All
Vulnerability Tags: All

FIGURE 8. TRENDING REPORT EXAMPLE

Other reports available in ThreadFix are:

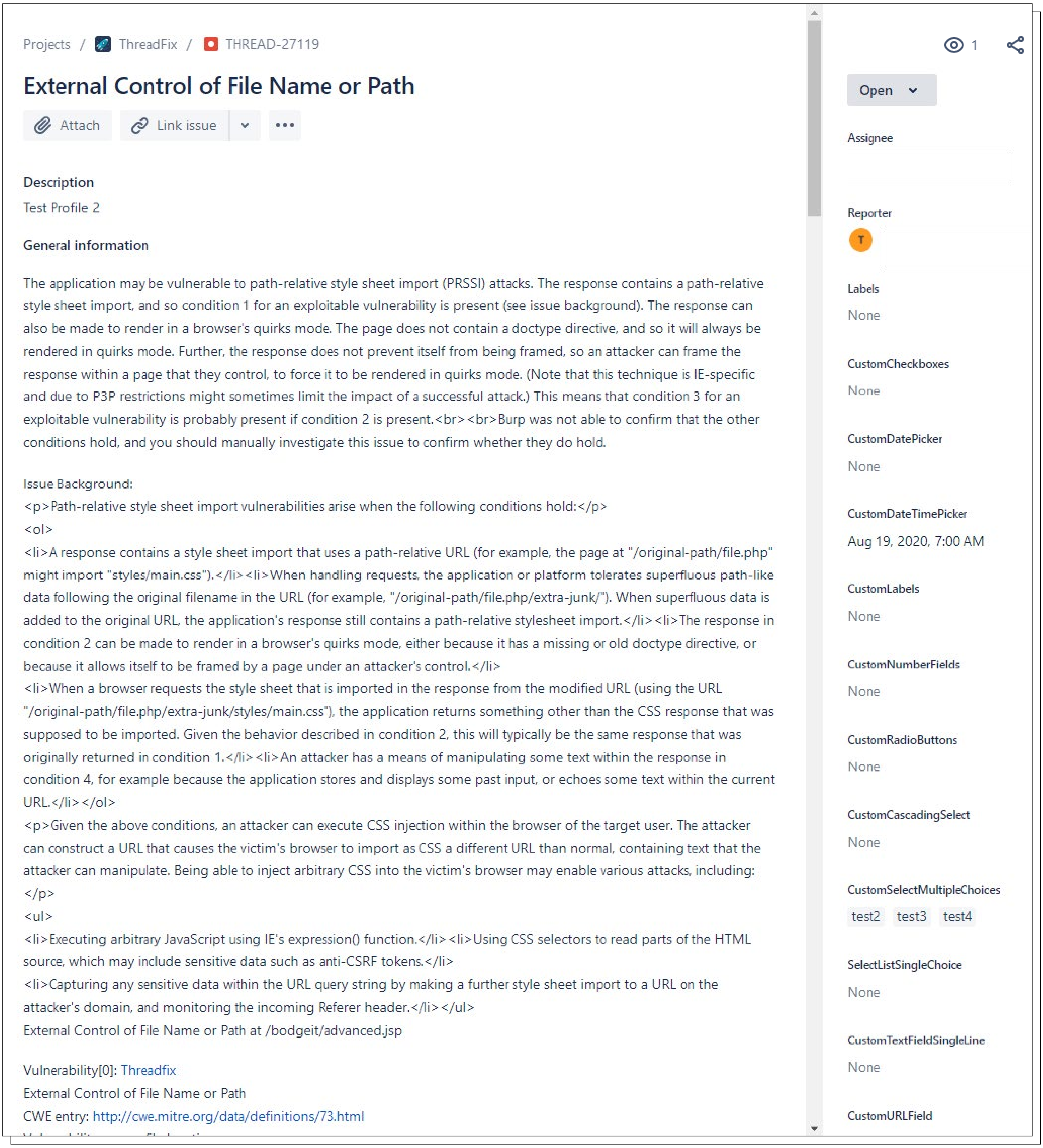
- The Point in Time report shows a breakdown of the team/application vulnerability results by their severity
- The Progress by Vulnerability report is used for tracking the average age of vulnerability types as well as the time to close each vulnerability type
- The Most Vulnerable Applications report shows the most affected applications and gives insight into their vulnerability composition
- OWASP Top 10 maps found vulnerabilities to the OWASP Top 10 list
- The Portfolio report shows how fresh the current scans for each application in your portfolio are. This report can help target specific applications for follow-up scans so you can to stay up to date on your projects' vulnerability status
- The DISA (Defense Information Systems Agency) STIG (Security Technical Information Guide) report displays information on your application's compliance with DISA's Application Security and Development STIG requirements. This report can help plan and execute remediation strategies for maintaining compliance with governmental application security standards
- The Scan Comparison Summary report gives a side-by-side look at how each scanner has been performing, showing the number and percentage of total vulnerabilities found and percent of total false positives discovered among them
- The Remediation report provides the trending report, as well as a more detailed table with starting and ending vulnerability counts to gauge progress
- Vulnerability Search allows to filter and explore vulnerabilities based on the set filters.

Defect tracker integrations

The integration with various defect/bug trackers enables security analysts to provide additional information to application developers about found vulnerabilities. This bi-directional communication removes the need for developers to use an external tool and helps them to quickly start fixing the vulnerabilities (Figure 9).

ThreadFix allows security teams to craft custom templates that will be used when creating a ticket and to define custom fields that will auto-populate the ticket in the defect tracker.

ThreadFix allows security teams to craft custom templates that will be used when creating a ticket and to define custom fields that will auto-populate the ticket in the defect tracker. If there are more teams managing the applications that use different trackers, it allows you to define and open tickets in multiple trackers. Security teams can define a defect tracker policy that automatically opens new tickets based on the severity level(s). For example, you can set a policy that opens tickets when the scanner has found vulnerabilities that have a severity of high or greater. Based on the policy setting, the vulnerabilities that match the criteria will be bundled together and attached to a ticket in the defect tracker.



External Control of File Name or Path

Description

Test Profile 2

General information

The application may be vulnerable to path-relative style sheet import (PRSSI) attacks. The response contains a path-relative style sheet import, and so condition 1 for an exploitable vulnerability is present (see issue background). The response can also be made to render in a browser's quirks mode. The page does not contain a doctype directive, and so it will always be rendered in quirks mode. Further, the response does not prevent itself from being framed, so an attacker can frame the response within a page that they control, to force it to be rendered in quirks mode. (Note that this technique is IE-specific and due to P3P restrictions might sometimes limit the impact of a successful attack.) This means that condition 3 for an exploitable vulnerability is probably present if condition 2 is present.

Burp was not able to confirm that the other conditions hold, and you should manually investigate this issue to confirm whether they do hold.

Issue Background:
<p>Path-relative style sheet import vulnerabilities arise when the following conditions hold:</p>
<ol>
<li>A response contains a style sheet import that uses a path-relative URL (for example, the page at "/original-path/file.php" might import "styles/main.css").</li><li>When handling requests, the application or platform tolerates superfluous path-like data following the original filename in the URL (for example, "/original-path/file.php/extra-junk/"). When superfluous data is added to the original URL, the application's response still contains a path-relative stylesheet import.</li><li>The response in condition 2 can be made to render in a browser's quirks mode, either because it has a missing or old doctype directive, or because it allows itself to be framed by a page under an attacker's control.</li>
<li>When a browser requests the style sheet that is imported in the response from the modified URL (using the URL "/original-path/file.php/extra-junk/styles/main.css"), the application returns something other than the CSS response that was supposed to be imported. Given the behavior described in condition 2, this will typically be the same response that was originally returned in condition 1.</li><li>An attacker has a means of manipulating some text within the response in condition 4, for example because the application stores and displays some past input, or echoes some text within the current URL.</li></ol>
<p>Given the above conditions, an attacker can execute CSS injection within the browser of the target user. The attacker can construct a URL that causes the victim's browser to import as CSS a different URL than normal, containing text that the attacker can manipulate. Being able to inject arbitrary CSS into the victim's browser may enable various attacks, including:
</p>
<ul>
<li>Executing arbitrary JavaScript using IE's expression() function.</li><li>Using CSS selectors to read parts of the HTML source, which may include sensitive data such as anti-CSRF tokens.</li>
<li>Capturing any sensitive data within the URL query string by making a further style sheet import to a URL on the attacker's domain, and monitoring the incoming Referer header.</li></ul>
External Control of File Name or Path at /bodgeit/advanced.jsp

Vulnerability[0]: Threadfix
External Control of File Name or Path
CWE entry: http://cwe.mitre.org/data/definitions/73.html

Assignee

Reporter

Labels
None

CustomCheckboxes
None

CustomDatePicker
None

CustomDateTimePicker
Aug 19, 2020, 7:00 AM

CustomLabels
None

CustomNumberFields
None

CustomRadioButtons
None

CustomCascadingSelect
None

CustomSelectMultipleChoices
test2 test3 test4

SelectListSingleChoice
None

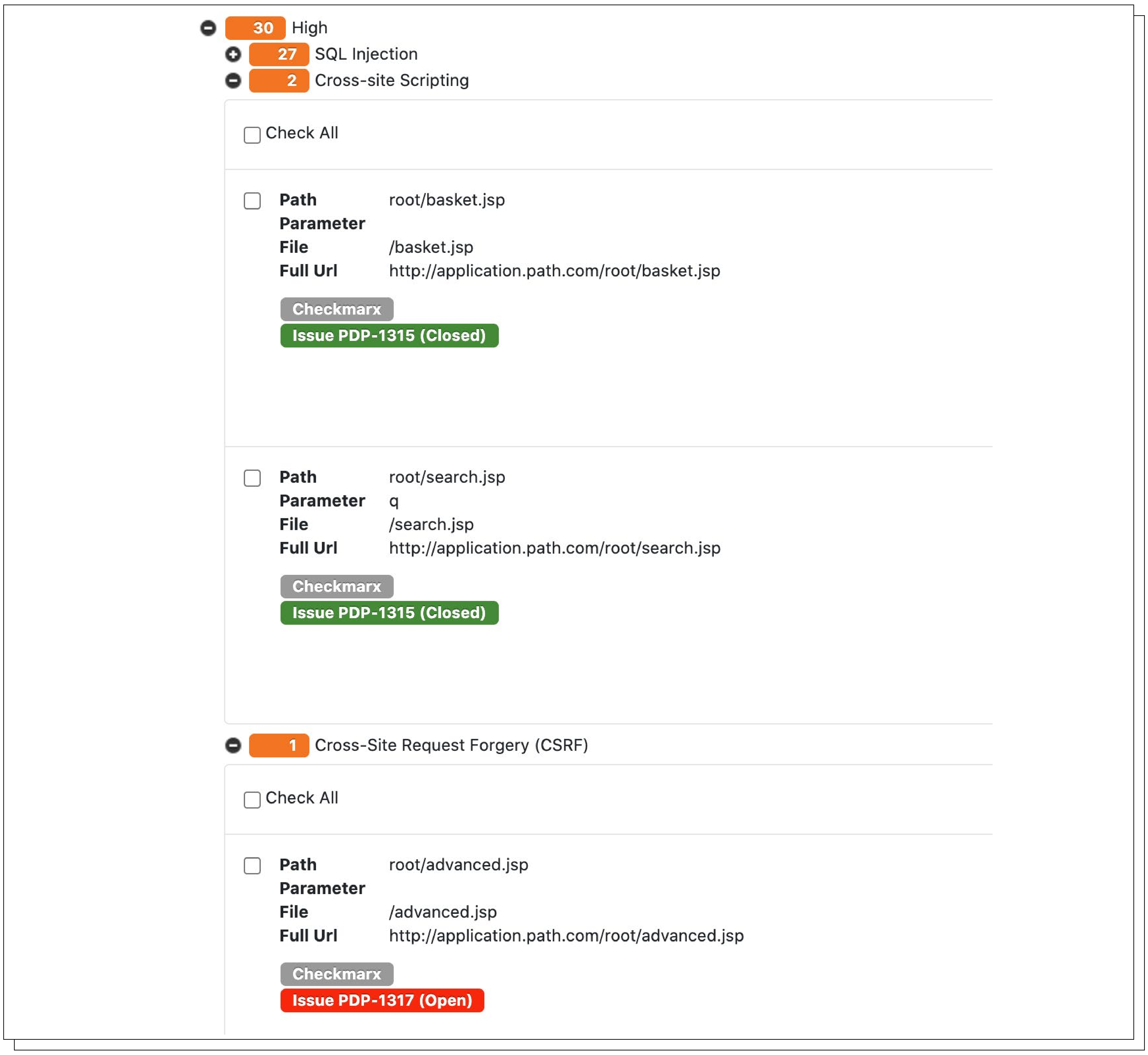
CustomTextFieldSingleLine
None

CustomURLField

FIGURE 9. THREADFIX OPENED A VULNERABILITY TICKET IN JIRA

ThreadFix maintains a link to the issue created in the external defect tracking system, allowing security analysts to see developers' progress in solving the reported vulnerabilities (see Figure 10). In addition, ThreadFix periodically checks the status of associated defects and updates that status in ThreadFix so that when development teams fix defects, security analysts can see their action and later check if the fix is working.

FIGURE 10. VULNERABILITY CONTAINS THE ISSUE STATUS THAT IS MONITORED REGULARLY



```
⊖ 30 High
  ⊕ 27 SQL Injection
  ⊖ 2 Cross-site Scripting
    □ Check All

    □ Path       root/basket.jsp
      Parameter
      File       /basket.jsp
      Full Url   http://application.path.com/root/basket.jsp
      Checkmarx
      Issue PDP-1315 (Closed)

    □ Path       root/search.jsp
      Parameter  q
      File       /search.jsp
      Full Url   http://application.path.com/root/search.jsp
      Checkmarx
      Issue PDP-1315 (Closed)

  ⊖ 1 Cross-Site Request Forgery (CSRF)
    □ Check All

    □ Path       root/advanced.jsp
      Parameter
      File       /advanced.jsp
      Full Url   http://application.path.com/root/advanced.jsp
      Checkmarx
      Issue PDP-1317 (Open)
```

The ThreadFix API

ThreadFix allows users to perform vulnerability management actions via the ThreadFix API. The process follows the ThreadFix application and infrastructure workflow, but in a more step-by-step programmatic fashion and can be useful when automating tedious work. The API documentation is very helpful because it is up to date, well written, and comes with examples for every call.

To support the DevSecOps movement, the ThreadFix API can be used to integrate more complex security testing workflows and vulnerability reporting with the Continuous Integration/Continuous Development process.

We tried replicating the workflow of managing the application portfolio, so we created a new team, assigned to it a new application, uploaded a related scan report and tried changing the status of the open vulnerabilities. We found ThreadFix API pretty versatile and able to replicate all or almost all ThreadFix actions that are provided through the ThreadFix application.

To support the DevSecOps movement, the ThreadFix API can be used to integrate more complex security testing workflows and vulnerability reporting with the Continuous Integration/Continuous Development process.

On specific events, you can schedule remote scanning and report found vulnerabilities back to the security team. Using the API you can also administer and provision ThreadFix more easily.

Conclusion

> *After adopting ThreadFix, you will say goodbye to tracking scan results and managing vulnerabilities via spreadsheets.*

ThreadFix is a helpful and mature tool for vulnerability management. It bridges a lot of gaps between various teams, including those between the security and application developer team(s). Application management enables users to merge and manage vulnerabilities and track their remediation actions.

After adopting ThreadFix, you will say goodbye to tracking scan results and managing vulnerabilities via spreadsheets. ThreadFix supports industry standard vulnerability scanners with vulnerability merging technology that works well. In addition to that, most vulnerability scanners can be directly orchestrated through ThreadFix, and it also allows you to automate a lot of workflows with the API functionalities. ThreadFix enables you to drill down in every vulnerable aspect of your application without losing sight of the big picture that is delivered by the useful analytic charts and trendlines.

One thing that's missing is the integration of the nmap scanner, which many security pros use for mapping infrastructure and scanning for low-hanging fruit vulnerabilities.

Another gap that Threadfix bridges is between operative security and compliance teams because ThreadFix also delivers a solid asset management tool that helps you to track and drive changes to meet the compliance or certification requirements.

CISOs will find ThreadFix analytics options useful because they enable identifying risk patterns in the scanned applications and infrastructure and a better estimate of risk levels and activities related to reducing risk. ThreadFix gives CISOs and other managers a valuable perspective into their software development lifecycle process and enables them to identify and measure segments that can be improved.

ThreadFix "humanizes" the security process with its collaboration features. Finding vulnerabilities is only one piece of the puzzle: remediation efforts are always the hardest and the most time-consuming piece. ThreadFix is not only used as a vulnerability unification and analytics platform but also as a collaboration platform where different teams and perspectives meet and engage in solving organizations deficiencies faster and better than before.

The SCRAM platform allows defenders to learn from past attacks and provides insight into which cyber-risk control areas require additional scrutiny or investment.

Which cybersecurity failures cost companies the most and which defenses have the highest ROI?

AUTHOR_Zeljka Zorz, Managing Editor, (IN)SECURE Magazine

Massachusetts Institute of Technology (MIT) scientists have created a cryptographic platform that allows companies to securely share data on cyber attacks they suffered and the monetary cost of their cybersecurity failures without worrying about revealing sensitive information to their competitors or damaging their own reputation.

The SCRAM platform allows defenders to learn from past attacks and provides insight into which cyber-risk control areas require additional scrutiny or investment.

The researchers recruited seven large companies that had a high level of security sophistication and a CISO to test out the platform.

Privacy-preserving platform offers answers

“In the past, the only way to aggregate and share information about cyber attacks was through a trusted third party,” explained the students, economists, cryptography and internet policy experts who worked on this project under the auspices of MIT’s Computer Science and Artificial Intelligence Lab (CSAIL).

But that third party could be breached, the data stolen and disclosed. The data could also be accidentally disclosed. For these reasons, companies often refused to participate in such schemes and share information about their losses.

SCRAM (Secure Cyber Risk Aggregation and Measurement) has, according to its creators, solved that longstanding cyber-security problem.

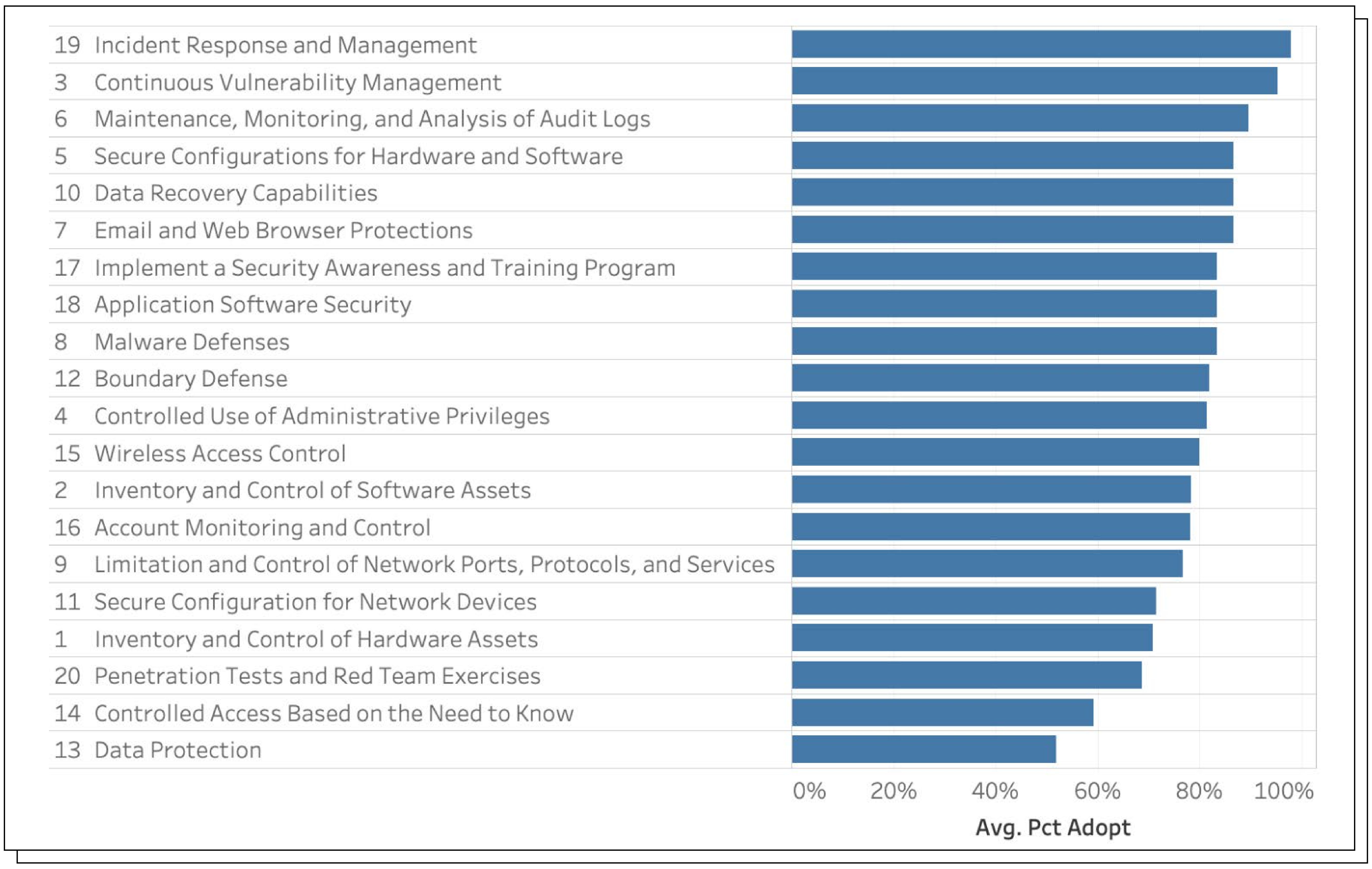
“SCRAM mimics the traditional aggregation technique but works exclusively on encrypted data that it cannot see. The system takes in encrypted data from the participants, runs a blind computation on it, and returns an encrypted result that must be unlocked by each participant separately before anyone can see the answer,” they explained.

“The security of the system comes from the requirement that the keys from all the participants are needed in order to unlock any of the data. Participants guarantee their own security by agreeing to unlock only the result using their privately held key.”

The cost of cybersecurity failures

The researchers recruited seven large companies that had a high level of security sophistication and a CISO to test out the platform, i.e., to contribute encrypted information about their network defenses and a list of all monetary losses from cyber attacks and their associated defensive failures over a two-year period.

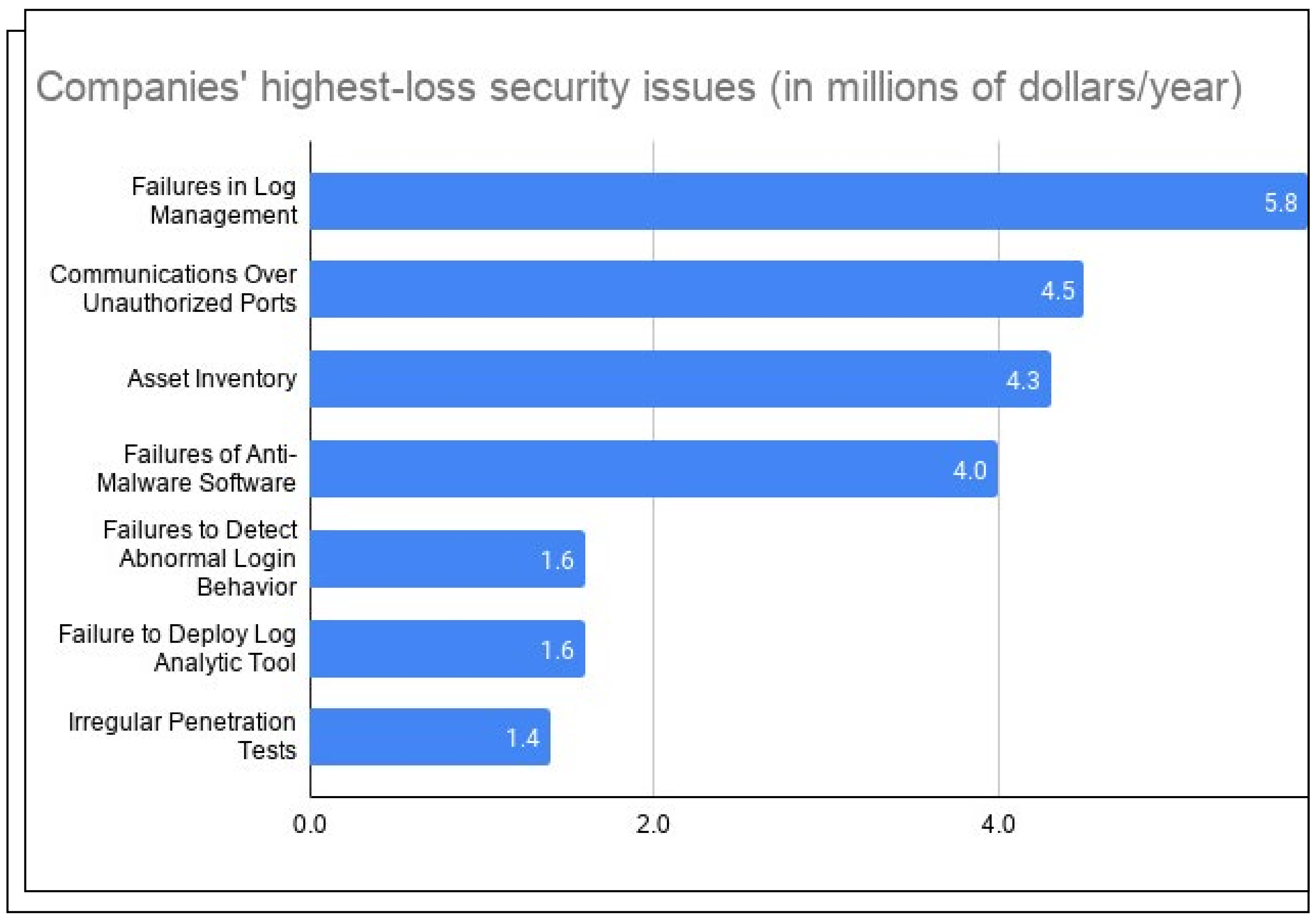
AVERAGE PERCENT ADOPTION BY SECURITY CONTROL



"Firms of this size would have the technological expertise and resources to nominate people on their team to work with us to design the appropriate questions and to perform the internal data collection," the scientists explained the rationale behind their decision to focus on larger companies.

SCRAM returned information about adopted defenses and pointed out which security failures cost companies the most money:

- **Failure to prevent malware** (and especially ransomware) attacks by relying mostly on anti-malware software, regular backups and reminding employees not to click on suspicious emails
- Despite all of the companies saying that they **blocked access to unauthorized ports**, attacks involving attackers accessing and communicating over these ports brought about high losses, meaning those defenses weren't air-tight or were being neglected
- **Failure to perform inventory and control of hardware assets**
- **Failure to perform effective log management and implement ML/AI-powered automated** analysis to identify security incidents as they happen (or even to predict and prevent them)



COMPANIES' HIGHEST-LOSS SECURITY ISSUES (IN MILLIONS OF DOLLARS)

Plans for the future

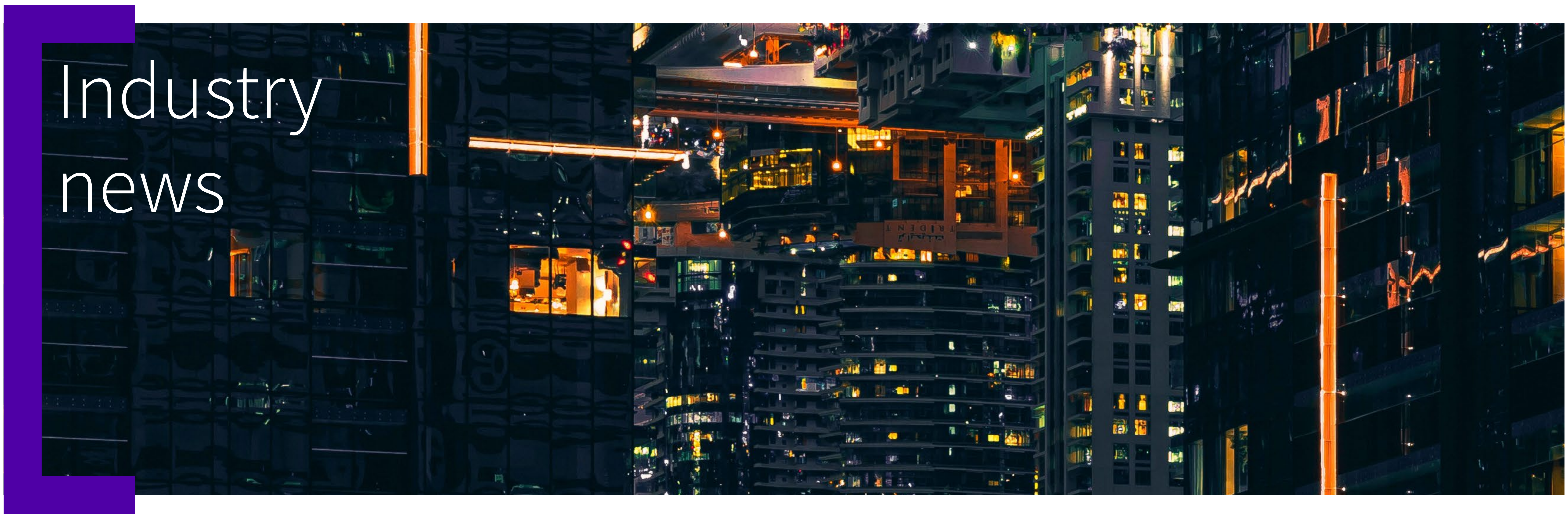
"These results provide a compelling proof-of-concept for how cyber intrusion data can be shared. Our next step will be to increase the number of incidents in future rounds to produce more robust estimates, more complex analyses, and more generalizable results," the scientists noted.

"With a larger data sample, we will also be able to explore loss distribution approaches that cover both the frequency and severity of losses. A larger sample size will also reduce the chance of outliers or single incidents leaking the magnitude of an individual event."

In the meantime, though, they've been able to demonstrate to companies that sensitive cyber attack data can be shared and used without being actually being disclosed.

"What this effectively means is that new cryptographic platforms such as SCRAM can gain access to previously 'untouchable' data that can then be used to inform market participants and meet important challenges," they added.

"Many of the target firms for this multi-party computation were interested in participating, but they wanted to see the results of the first computation before contributing their own data. From a cybersecurity standpoint, this represents a new opportunity to create new cybersecurity aggregation pools with greater reach and precision than ever before."



Industry news

BAE Systems unveils cyber-threat detection and mitigation solution for U.S. military platforms

The Fox Shield suite is designed to help platforms detect, respond, and recover from cyber attacks in real time. The system's cyber resilience capabilities can be integrated into ground, air, and space vehicles to protect our warfighters and platforms from cyber attacks designed to access and degrade mission capabilities.

"Cyber protection was not necessarily a mission-critical capability when some of these platforms were first developed. That's why we designed the Fox Shield cyber resilience system to be easily integrated into new and legacy platforms," said Michael Weber, technical manager for FAST Labs' Cyber Technology group at BAE Systems.

C2A Security launches AutoSec, an automotive cybersecurity lifecycle management platform

AutoSec arrives at a critical time for the industry: modern vehicle architecture is more vulnerable than ever before. OEMs and Tier 1s are grappling with the new ISO/ SAE 21434 standard as well as UNECE WP.29 regulation and cybersecurity teams are struggling to coordinate and effectively communicate responsibility.

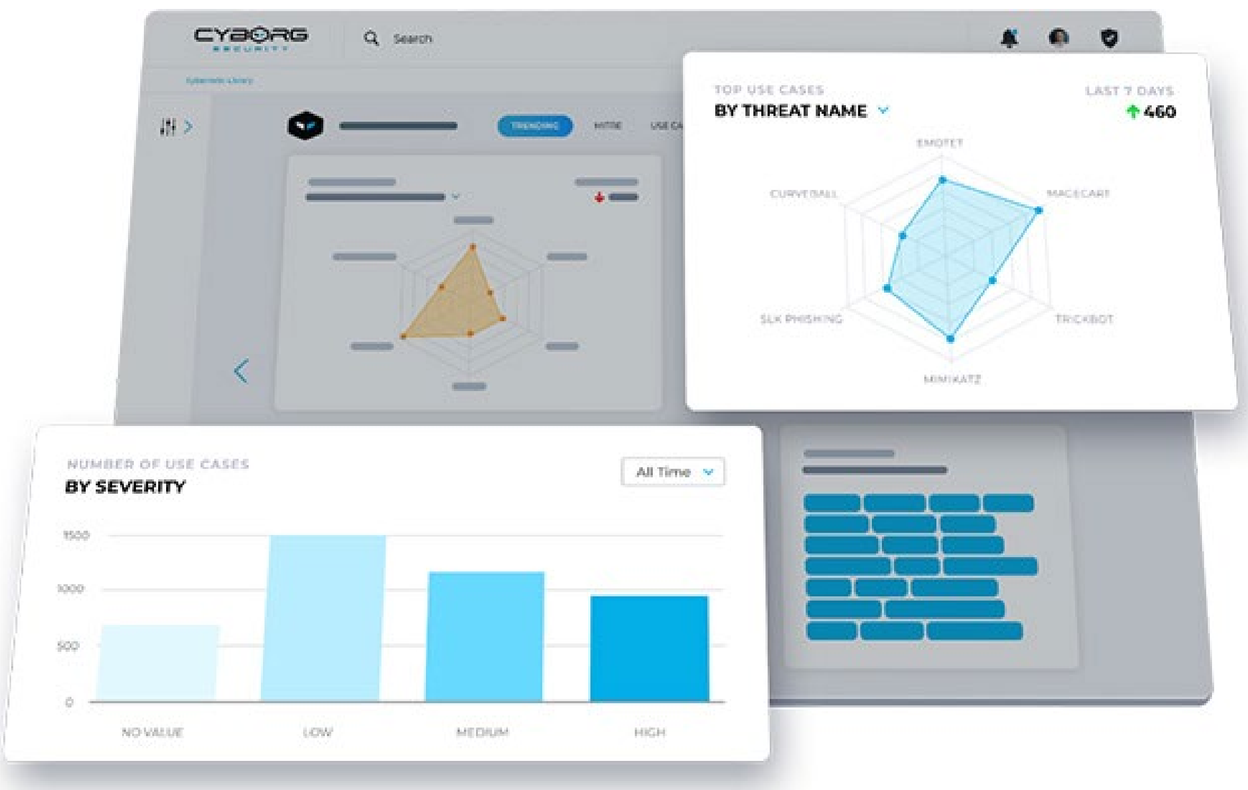
This cybersecurity hub is the first of its kind and gives users unparalleled transparency into the entire cybersecurity lifecycle, enabling streamlined management of each phase–risk assessment, planning, policy creation and enforcement–with just a few clicks.

Raytheon Intelligence & Space provides a virtualized environment to evaluate and reduce cyber threats

DejaVM enables system-level cyber testing without requiring access to the limited number of highly specialized physical hardware assets. The tool creates an emulation environment that virtualizes complex systems to support automated cyber testing. DejaVM focuses on improving software development, testing and security via its advanced analysis features.

"The complexity of cyber threats that organizations face continues to escalate, demanding more sophisticated solutions to evaluate and reduce threats to those missions," said John DeSimone, vice president of Cybersecurity, Training and Services at RI&S. "This robust virtual environment helps our customers do exactly that."

Cyborg Security launches HUNTR platform to help orgs tackle cyber threats



Cyborg Security's HUNTR platform has been developed by a world class team of threat hunting experts to deliver advanced threat hunting and detection content, empowering organizations to move beyond reactive security, to proactive threat hunting.

The platform provides advanced and contextualized threat hunting and detection packages containing behaviorally based threat hunting content, threat emulation, and detailed runbooks, supplying organizations what they need to evolve their security analysts into skilled hunters.

Every HUNTR package is developed by dedicated threat researchers from malware analysis and incident investigations and is combined with unprecedented contextualization derived from cutting edge threat intelligence.

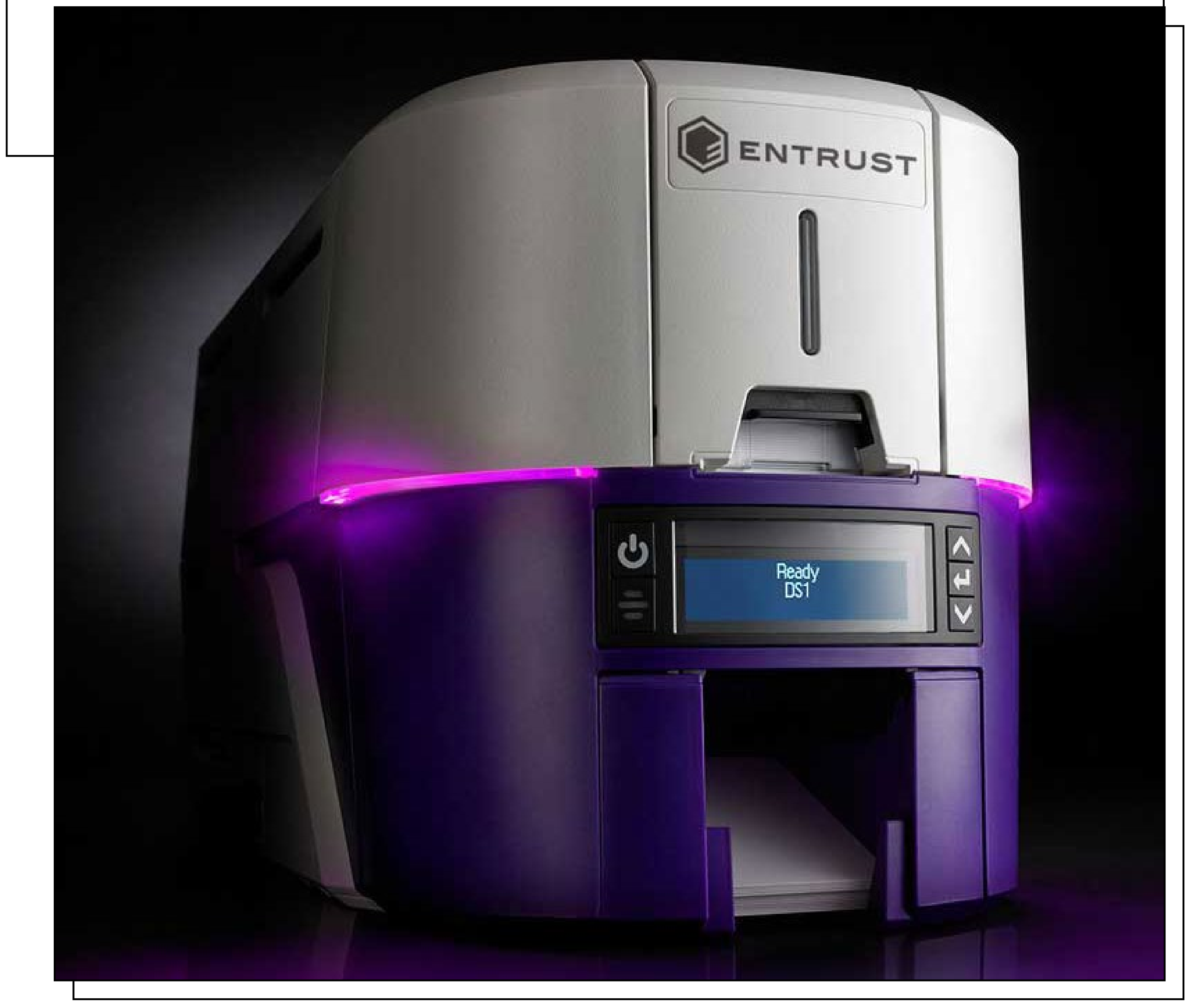
HUNTR content can be deployed using a proprietary patent-pending technology that tailors the hunting and detection packages to an organization's unique environment and existing security toolsets.

Entrust launches direct-to-card solution for instant physical and mobile ID issuance

Sigma systems deliver a seamless user experience across the issuance process for desktop and mobile printing needs. It eliminates the frustrations of printer set-up with a modular design and an out-of-the-box implementation that takes less than 30 minutes for users to begin issuing identities.

Equipped with cloud-based APIs, Sigma systems bring issuance to the cloud without additional hardware — enabling instant printing for both physical IDs, badges and payment cards.

Sigma systems are trusted IoT devices that help ensure organizations and their data are safe with an intelligent network and building connectivity for ultimate enterprise protection.



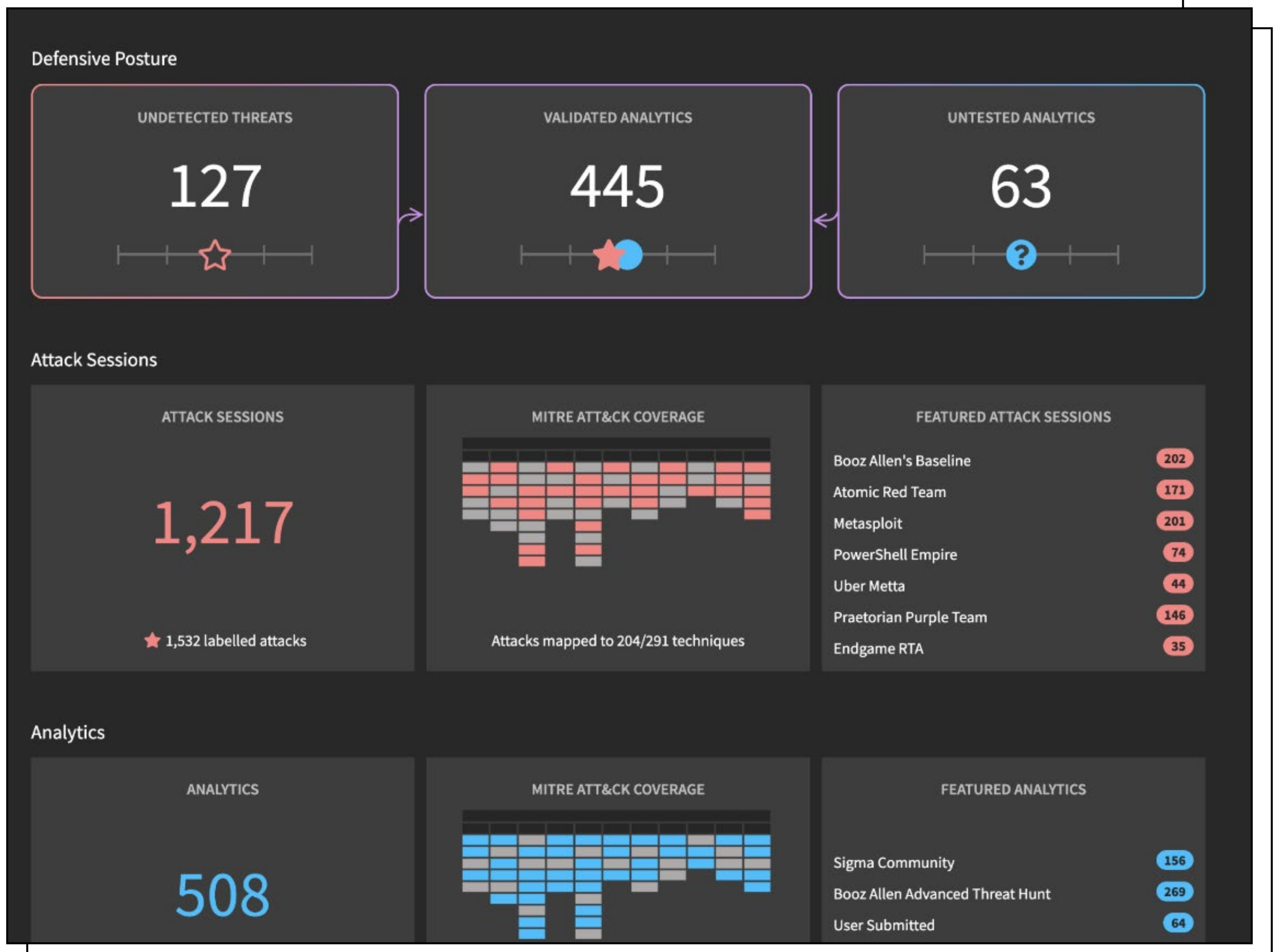
Incognia launches fraud detection solution for QR code contactless payments

Incognia's fraud detection solution for QR code contactless payments uses location behavioral biometrics to verify buyer's and seller's real-time and historical location behavior to protect against fake QR codes, account takeovers and use of fake synthetic identities during transactions.

The solution works for physical in store, remote and peer to peer QR code contactless payments. For consumers, Incognia's technology creates a private digital identity that enables a user's device to produce a unique location fingerprint, without compromising any of the user's personally identifiable information.

The digital identity is also matched to the recent behavior of the device and the known behavior of the account.

Booz Allen Hamilton unveils SnapAttack, bringing together red and blue security teams



Defensive Posture

UNDETECTED THREATS	VALIDATED ANALYTICS	UNTESTED ANALYTICS
127	445	63

Attack Sessions

ATTACK SESSIONS

1,217

★ 1,532 labelled attacks

MITRE ATT&CK COVERAGE

Attacks mapped to 204/291 techniques

FEATURED ATTACK SESSIONS

Booz Allen's Baseline	202
Atomic Red Team	171
Metasploit	201
PowerShell Empire	74
Uber Metta	44
Praetorian Purple Team	146
Endgame RTA	35

Analytics

ANALYTICS

508

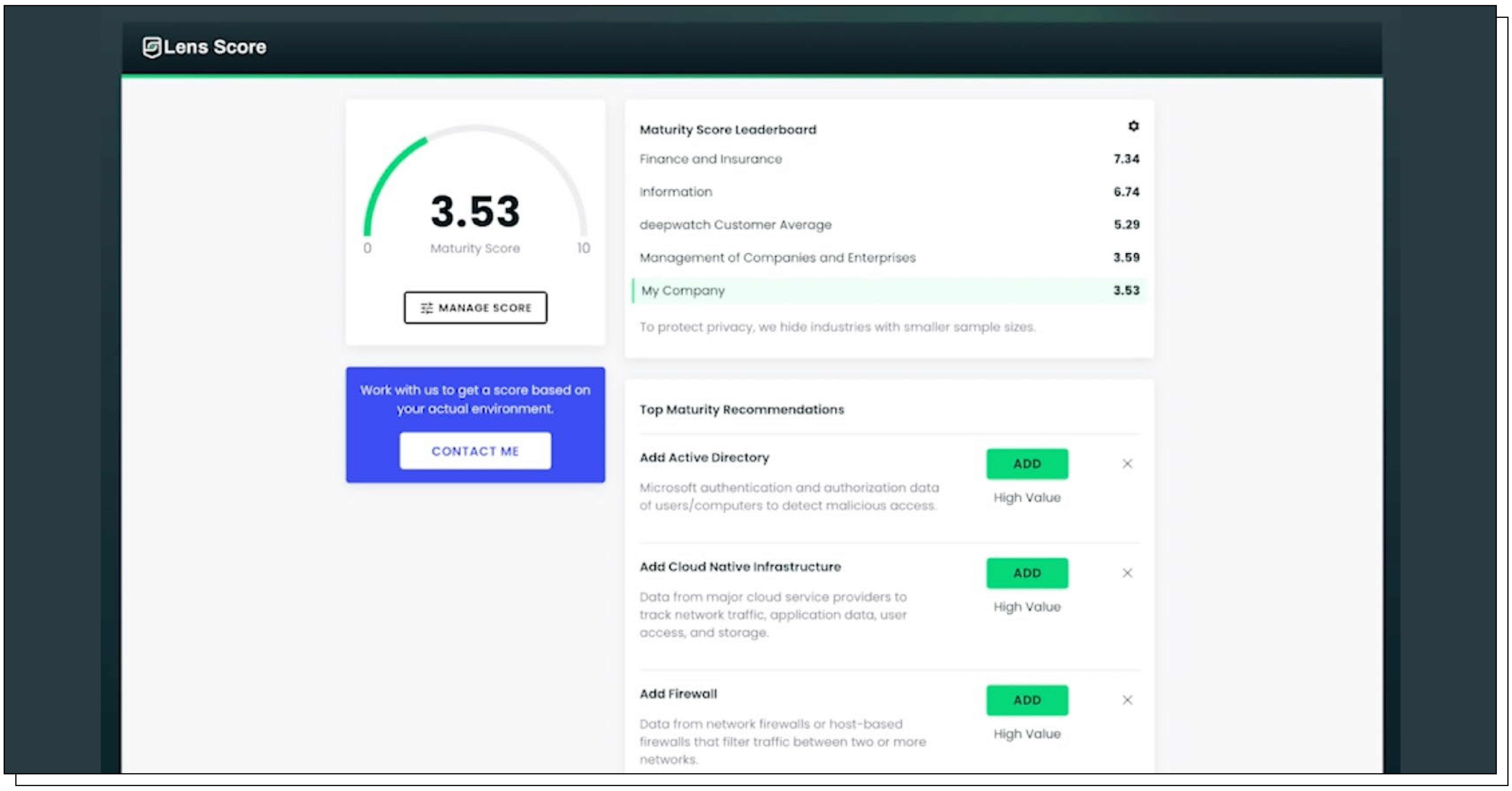
MITRE ATT&CK COVERAGE

FEATURED ANALYTICS

Sigma Community	156
Booz Allen Advanced Threat Hunt	269
User Submitted	64

By unifying the security lifecycle into a single solution, SnapAttack enables red and blue teams to work together, emulating attacks from intelligence data, sharing insights of malicious behavior, and developing vendor-agnostic behavioral detection analytics to stop advanced adversaries.

"We built SnapAttack to satisfy a critical need to help our own red and blue teams collaborate more effectively. This approach continually increases our confidence in detecting sophisticated threats through threat hunting and improving our defenses in support of clients worldwide," said Garrettson Blight, Booz Allen's Director of Dark Labs.



Work with us to get a score based on your actual environment.

Maturity Score Leaderboard

Finance and Insurance	7.34
Information	6.74
deepwatch Customer Average	5.29
Management of Companies and Enterprises	3.59
My Company	3.53

To protect privacy, we hide industries with smaller sample sizes.

Top Maturity Recommendations

Add Active Directory
Microsoft authentication and authorization data of users/computers to detect malicious access.
High Value

Add Cloud Native Infrastructure
Data from major cloud service providers to track network traffic, application data, user access, and storage.
High Value

Add Firewall
Data from network firewalls or host-based firewalls that filter traffic between two or more networks.
High Value

Deepwatch Lens Score: SecOps maturity planning and benchmarking

Deepwatch announced Lens Score, a fast, easy to use application for CISOs and those who are accountable for measuring, monitoring, and improving their company's overall security operations maturity.

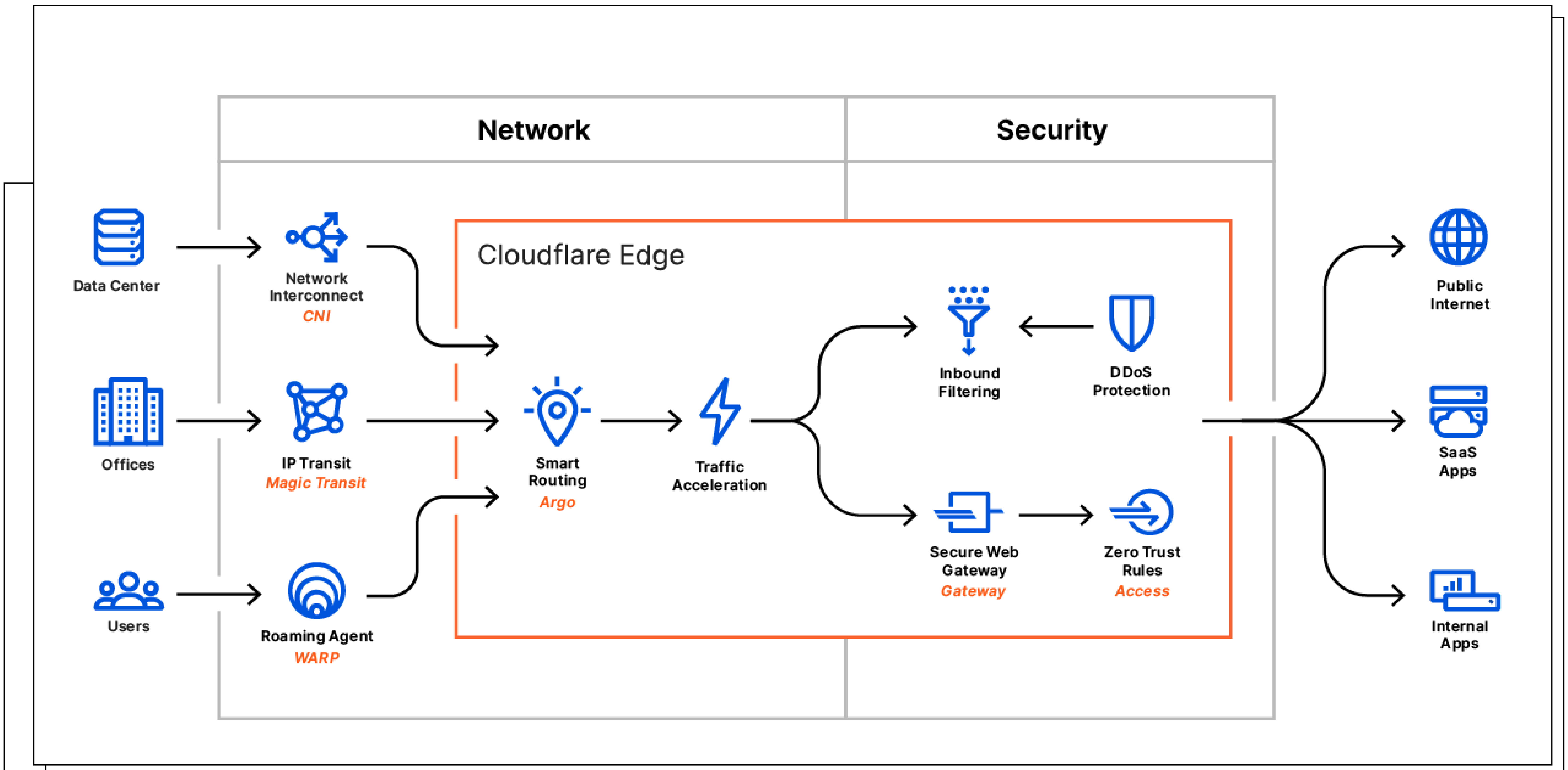
"The unique thing about Lens Score is that it instantly visualizes data collection coverage with a maturity score calculated by our patented Maturity Model algorithms," described Corey Bodzin, CTO.

"The Deepwatch Maturity Model is the industry's first scientific way to measure SOC effectiveness. The Maturity Model Score gives CISO's the immediate ability to benchmark their security program maturity against that of their peers, and quickly uncover gaps and how to address them. CISOs can then track their improvements and estimate the impact of different improvements they might pursue."

Masergy extends the value of Masergy SD-WAN Secure to home and mobile users

Masergy announced SD-WAN Work From Anywhere solutions. The new offerings extend the value of Masergy's Managed SD-WAN Secure solutions to the remote workforce, supporting their network connections with built-in security, dual-link redundancy, load balancing, and dynamic traffic steering capabilities.

Businesses of all sizes use Masergy's SD-WAN to provide secure and reliable cloud application performance to office employees, and now their users at home or on the go have access to the same level of security and performance.



Cloudflare One: A cloud-based network-as-a-service solution for the remote workforce

As more businesses rely on the internet to operate, Cloudflare One protects and accelerates the performance of devices, applications, and entire networks to keep workforces secure.

Now businesses can protect their workforce in a flexible and scalable way, without compromising security as distributed teams work from multiple devices and personal networks.

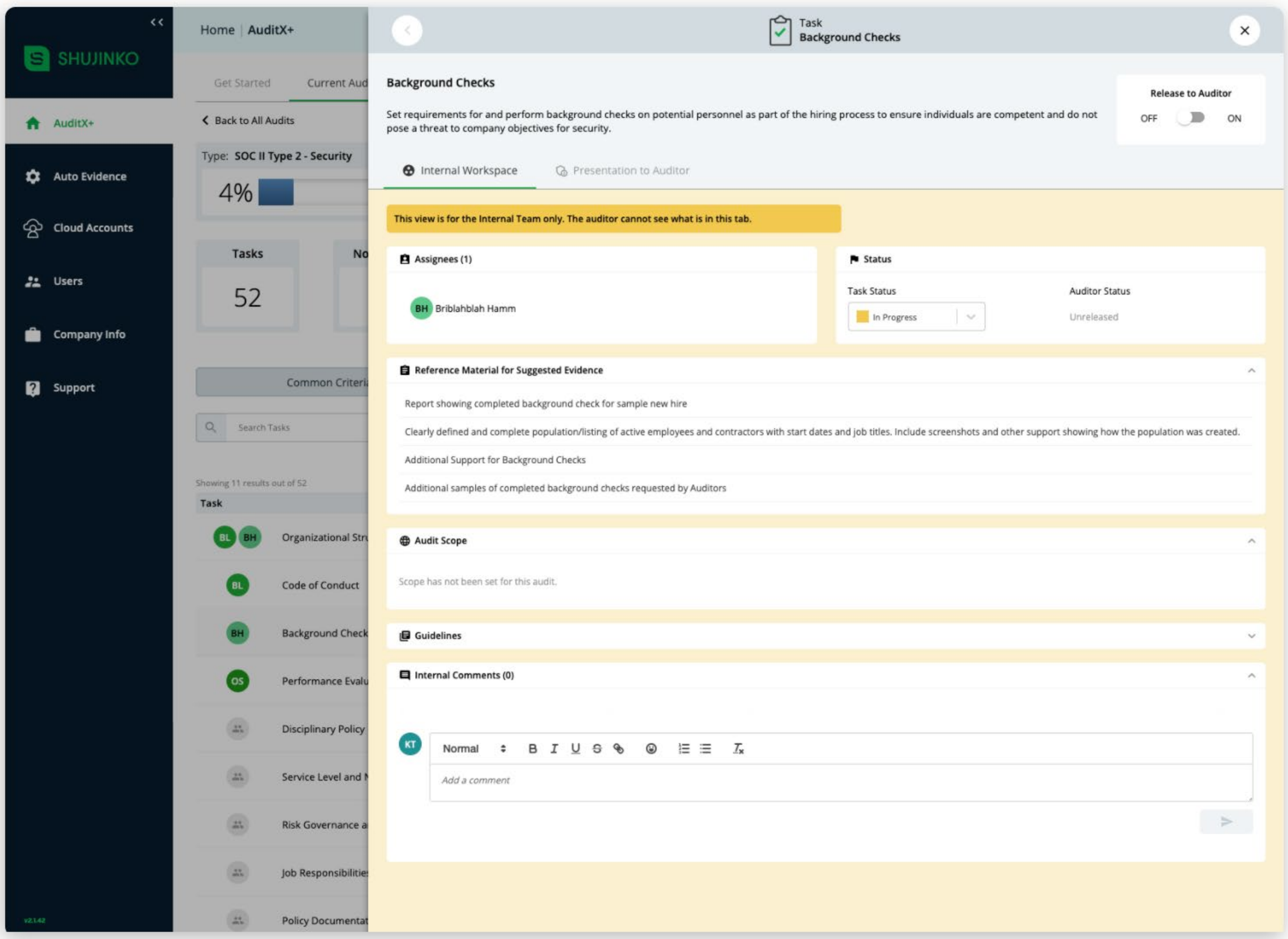
“After decades of building legacy corporate networks, organizations are left with clunky systems designed to protect their now empty offices.

The only way to secure today’s work-from-anywhere economy is to secure each individual employee, protecting their individual networks, devices, and access to business-critical applications,” said Matthew Prince, CEO of Cloudflare.

Splunk helps security teams modernize and unify their security operations in the cloud

Splunk announced a series of new product innovations designed to help security teams around the world modernize and unify their security operations in the cloud.

Led by new, cloud-centric updates to Splunk Enterprise Security, Splunk Mission Control and the newly announced Splunk Mission Control Plug-In Framework, Splunk’s security operations suite enables Splunk customers to secure their cloud journey and solve their toughest cloud security challenges with data.



Background Checks

Set requirements for and perform background checks on potential personnel as part of the hiring process to ensure individuals are competent and do not pose a threat to company objectives for security.

This view is for the Internal Team only. The auditor cannot see what is in this tab.

Report showing completed background check for sample new hire

Clearly defined and complete population/listing of active employees and contractors with start dates and job titles. Include screenshots and other support showing how the population was created.

Additional Support for Background Checks

Additional samples of completed background checks requested by Auditors

Scope has not been set for this audit.

Shujinko AuditX: Simplifying, automating and modernizing audit preparation and compliance

Organizations can use AuditX to speed audits (PCI DSS, SOC 2, ISO 27001, NIST, etc.) across public cloud infrastructure (AWS and Azure) and hybrid environments.
Simultaneously, the company announced its Automated Evidence Collection Engine, the industry's first platform for automatically orchestrating, collecting and transforming compliance evidence directly from public cloud platforms and other SaaS systems.

AuditX automates evidence collection, maps evidence across multiple controls and across different standards, streamlines audit workflow and clarifies communication across teams and with auditors. AuditX organizes evidence in a centralized library for final readiness review and provides a 360-degree dashboard to make the entire process highly visible and predictable.

Checkmarx provides automated security scans within GitHub repositories

Checkmarx announced a new GitHub Action to bring comprehensive, automated static and open source security testing to developers. Checkmarx's new GitHub Action integrates the company's application security testing (AST) solutions – Checkmarx SAST (CxSAST) and Checkmarx SCA (CxSCA) – directly with GitHub code scanning, giving developers more flexibility and power to work with their preferred tools of choice to secure proprietary and open source code.

By automatically triggering SAST and SCA security scans in the event of a pull request, and embedding results directly into the GitHub CI/CD pipeline, Checkmarx streamlines developer workflows and empowers them to code more confidently without sacrificing speed and security.

2020
Cybersecurity INSIDERS
CLOUD SECURITY REPORT
(ISC)²

Justifying your 2021 cybersecurity budget

AUTHOR_Karen Walsh, CEO, Allegro Solutions

Sitting in the midst of an unstable economy, a continued public health emergency, and facing an uptick in successful cyber attacks, CISOs find themselves needing to enhance their cybersecurity posture while remaining within increasingly scrutinized budgets.

Senior leadership recognizes the value of cybersecurity but understanding how to best allocate financial resources poses an issue for IT professionals and executive teams. As part of justifying a 2021 cybersecurity budget, CISOs need to focus on quick wins, cost-effective SaaS solutions, and effective ROI predictions.

Finding the "quick wins" for your 2021 cybersecurity budget

Cybersecurity, particularly with organizations suffering from technology debt, can be time-consuming. Legacy technologies, including internally designed tools, create security challenges for organizations of all sizes.

The first step to determining the "quick wins" for 2021 lies in reviewing the current IT stack for areas that have become too costly to support. For example, as workforce members moved off-premises during the current public health crisis, many organizations found that their technology debt made this shift difficult. With workers no longer accessing resources from inside the organization's network, organizations with rigid technology stacks struggled to pivot their work models.

Going forward, remote work appears to be one way through the current health and economic crises. Even major technology leaders who traditionally relied on in-person workforces have moved to remote models through mid-2021, with Salesforce the most recent to announce this decision.

Looking for gaps in security, therefore, should be the first step in any budget analysis. As part of this gap analysis, CISOs can look in the following areas:

- □ VPN and data encryption
- □ Data and user access
- □ Cloud infrastructure security

Each of these areas can provide quick wins if done correctly because as organizations accelerate their digital transformation strategies to match these new workplace situations, they can now leverage cloud-native security solutions.

Adopting SaaS security solutions for accelerating security and year-over-year value

The SaaS-delivered security solution market exploded over the last five to ten years. As organizations moved their mission-critical business operations to the cloud, cybercriminals focused their activities on these resources.

> *SaaS security solutions offer two distinct budget wins for CISOs.*

Interestingly, a CNBC article from July 14, 2020 noted that for the first half of 2020, the number of reported data breaches dropped by 33%. Meanwhile, another CNBC article from July 29, 2020 notes that during the first quarter, large scale data breaches increased by 273% compared to the same time period in 2019. Although the data appears conflicting, the Identity Theft Research Center research that informed the July 14th article specifically notes, “This is not expected to be a long-term trend as threat actors are likely to return to more traditional attack patterns to replace and update identity information needed to commit future identity and financial crimes.” In short, rapidly closing security gaps as part of a 2021 cybersecurity budget plan needs to include the fast wins that SaaS-delivered solutions provide.

SaaS security solutions offer two distinct budget wins for CISOs. First, they offer rapid integration into the organization’s IT stack. In some cases, CISOs can get a SaaS tool deployed within a few weeks, in other cases within a few months. Deployment time depends on the complexity of the problem being solved, the type of integrations necessary, and the enterprise’s size. However, in the same way that agile organizations leverage cloud-based business applications, security teams can leverage rapid deployment of cloud-based security solutions.

The second value that SaaS security solutions offer is YoY savings. Subscription models offer budget conscious organizations several distinct value propositions. First, the organization can reduce hardware maintenance costs, including operational costs, upgrade costs, software costs, and servicing costs. Second, SaaS solutions often enable companies to focus on their highest risk assets and then increase their usage in the future. Third, they allow organizations to pivot more effectively because the reduced up-front capital outlay reduces the commitment to the project.

Applying a dollar value to these during the budget justification process might feel difficult, but the right key performance indicators (KPIs) can help establish baseline cost savings estimates.

Choosing the KPIs for effective ROI predictions

During an economic downturn, justifying the cybersecurity budget requests might be increasingly difficult. Most cybersecurity ROI predictions rely on risk evaluations and applying probability of a data breach to projected cost of a data breach. As organizations look to reduce costs to maintain financially viable, a “what if” approach may not be as appealing.

> *Cybersecurity initiatives focus on leveraging resources effectively so that they can ensure the most streamlined process possible while maintaining a robust security program.*

However, as part of budgeting, CISOs can look to several value propositions to bolster their spending. Cybersecurity initiatives focus on leveraging resources effectively so that they can ensure the most streamlined process possible while maintaining a robust security program. Aligning purchase KPIs with specific reduced operational costs can help gain buy-in for the solution.

A quick hypothetical can walk through the overarching value of SaaS-based security spending. Continuous monitoring for external facing vulnerabilities is time-consuming and often incorporates inefficiency. Hypothetical numbers based on research indicate:

A poll of C-level security executives noted that 37% said they received more than 10,000 alerts each month with 52% of those alerts identified as false positives.

- The average security analyst spends ten minutes responding to a single alert
- The average security analyst makes approximately $91,000 per year

> *Although CISOs may not want to reduce their number of team members, they may not want to add additional ones, or they may be seeking to optimize the team they have.*

Bringing this data together shows the value of SaaS-based solutions that reduce the number of false positives:

- Every month enterprise security analysts spend 10 minutes for each of the 5,2000 false positives
- This equates to approximately 866 hours
- 866 hours, assuming a 40-hour week, is 21.65 weeks
- Assuming 4 weeks per month, the enterprise needs at least 5 security analysts to manage false positive responses
- These 5 security analysts cost a total of $455,000 per year in salary, not including bonuses and other benefits

Although CISOs may not want to reduce their number of team members, they may not want to add additional ones, or they may be seeking to optimize the team they have. Tracking KPIs such reduction in false positives per month can provide the type of long-term cost value necessary for other senior executives and the board of directors.

Securing a 2021 cybersecurity budget

While the number of attacks may have stalled during 2020, cybercriminals have not stopped targeting enterprise data. Phishing attacks and malware attacks have moved away from the enterprise network level and now look to infiltrate end-user devices. As organizations continue to pivot their operating models, they need to look for cost-effective ways to secure their sensitive resources and data. However, budget constrictions arising from 2020's economic instability may make it difficult for CISOs to gain the requisite dollars to continue to apply best security practices.

As organizations start looking toward their 2021 roadmap, CISOs will increasingly need to be specific about not only the costs associated with purchases but also the cost savings that those purchases provide from both data incident risk and operational cost perspective.

Because of the recent surge in the remote workforce, the security of the remote hosts is on top of the mind for the security teams.

Keep remote workers and their devices secure with one click

AUTHOR_Mirko Zorz, Editor in Chief, (IN)SECURE Magazine

In this interview Shailesh Athalye, VP Compliance at Qualys, discusses cloud-based Remote Endpoint Protection and illustrates how security teams can leverage its numerous features.

_ *Qualys recently added malware detection to its cloud-based Remote Endpoint Protection offering. How does it work?*

Because of the recent surge in the remote workforce, the security of the remote hosts is on top of the mind for the security teams. It became immediately apparent when majority of the hosts shifted remote, that traditional enterprise security solutions deployed inside the organization's network were utterly ineffective in protecting these remote endpoints, due to the sheer volume of remote hosts connecting over VPNs. What would happen when those remote computers needed to be updated? It would be impractical to deliver thousands of security updates, malware updates via the VPN, over limited bandwidth.

Architecturally superior cloud security solutions like Qualys are well positioned to address the need for protecting remote computers as we could connect directly to the cloud over the internet without the need to route a large volume of traffic through the VPN gateways.

We're pleased with the reception the offer has garnered, and we have had more than 700 companies registering for the offer. And we didn't stop there – as we realized we could give customers additional protections by adding the ability to detect malware – and that is the piece that we've recently announced.

Powered by the Qualys Platform and Cloud Agent, malware detection uses file reputation and threat classification to detect known malicious files on endpoints, servers, and cloud workloads. As a result, security practitioners can respond more quickly to malware on employees' systems.

_ *What makes Qualys Remote Endpoint Protection unique?*

In general, cloud-based security services have an advantage as they connect directly to the cloud over the internet without routing a large volume of traffic through the VPN gateways for assessing vulnerabilities and for applying patches. What's unique about the Remote Endpoint Protection Offering is that it:

1_Gives companies visibility into what devices are connecting inside their network and what resources the devices are connecting to.

2_Assesses vulnerabilities, malware and security configurations on remote hosts such as Microsoft Office, the Google Suite of products, VPN software and conferencing solutions such as Zoom or Webex.

3_Detects malicious files and processes often missed because a company's anti-virus tools are only pushed to remote computers connected to the VPN.

4_Prioritizes patches by correlating them with vulnerabilities as well as applying patches directly from the solution vendor's content delivery networks via the internet, without putting pressure on the VPN and available bandwidth due to the size of the patches.

Not only does Qualys address remote endpoint issues, but we do so with one solution providing a continuous and integrated view of remote endpoint inventory, critical vulnerabilities, misconfigurations and now malware to speed remediation while enabling remote patching. This functionality is seamlessly integrated into one solution.

> *The Qualys Remote Endpoint Protection service is extremely easy to enable for customers who already have deployed the lightweight Qualys Cloud Agents.*

This approach is a first in the industry as previously companies would cobble together a solution for detecting vulnerabilities, one for patching and another for malware detection. While it did the job, it was complicated, clunky and the data was not consolidated for a true picture of the risk.

_ *What does the process of integrating Qualys Remote Endpoint Protection into an existing security architecture look like?*

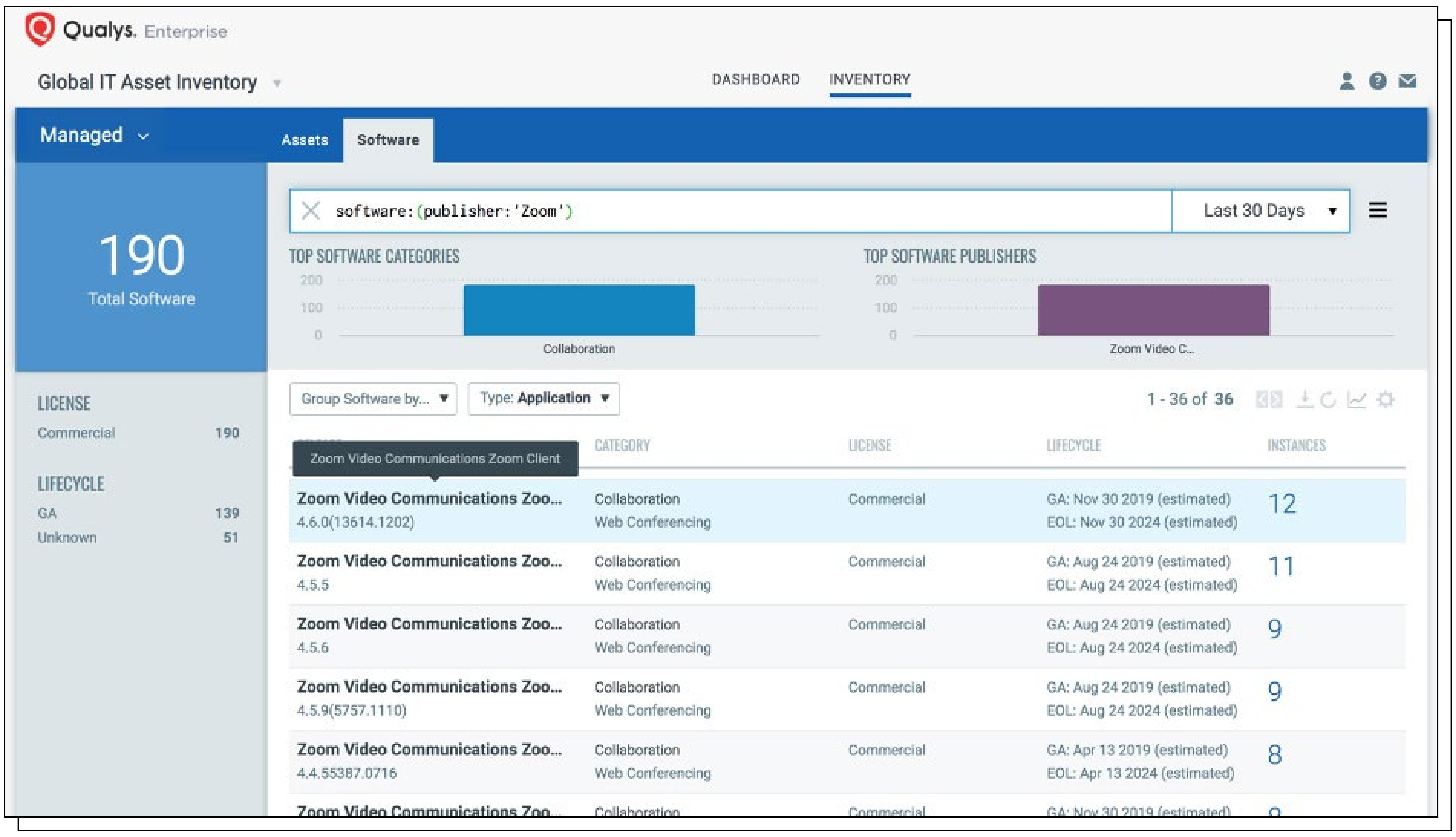
Remote Endpoint Protection is easily enabled through the Qualys Cloud Platform and Cloud Agent. And like all Qualys Apps, it is self-updating, centrally managed and tightly integrated with other apps in the platform. The Cloud Agent continuously communicates and syncs-up collected data with the Qualys platform including pushing the latest vulnerability signatures and vendor patches. All of which, it does without the need for a VPN and or internal network bandwidth.

Qualys applications cover a broad swath of functionality in areas such as IT asset management, IT security, web app security and compliance monitoring. All apps are based on the same platform, share a common UI, feed off of the same scanners and agents, access the same collected data, and leverage the same user permissions. This lowers the complexity of usage while maintaining a high level of access control throughout the organization.

_ *How can security teams leverage the features of Qualys Remote Endpoint Protection?*

The Qualys Remote Endpoint Protection service is extremely easy to enable for customers who already have deployed the lightweight Qualys Cloud Agents. Once the customer signs up for the service, their existing subscription will have workflows and capabilities enabled for remote endpoint security assessment and patching. The free, updated, Qualys Remote Endpoint Protection offer allows security teams to leverage the lightweight Qualys Cloud Agent to:

- □ Identify and inventory all remote endpoints including hardware and the applications they are running in real time
- □ Ensure remote systems are secure with a real-time view of all critical vulnerabilities, malware and misconfigurations impacting the OS and applications
- □ Decrease remediation response time by automatically correlating required patches with identified vulnerabilities, and prioritizing detected malware
- □ Deliver patches and respond to malware from the cloud within hours with one click, and all without using the limited bandwidth available on VPN gateways



software:(publisher:'Zoom')

Type: Application

190
Total Software

LICENSE	
Commercial	190

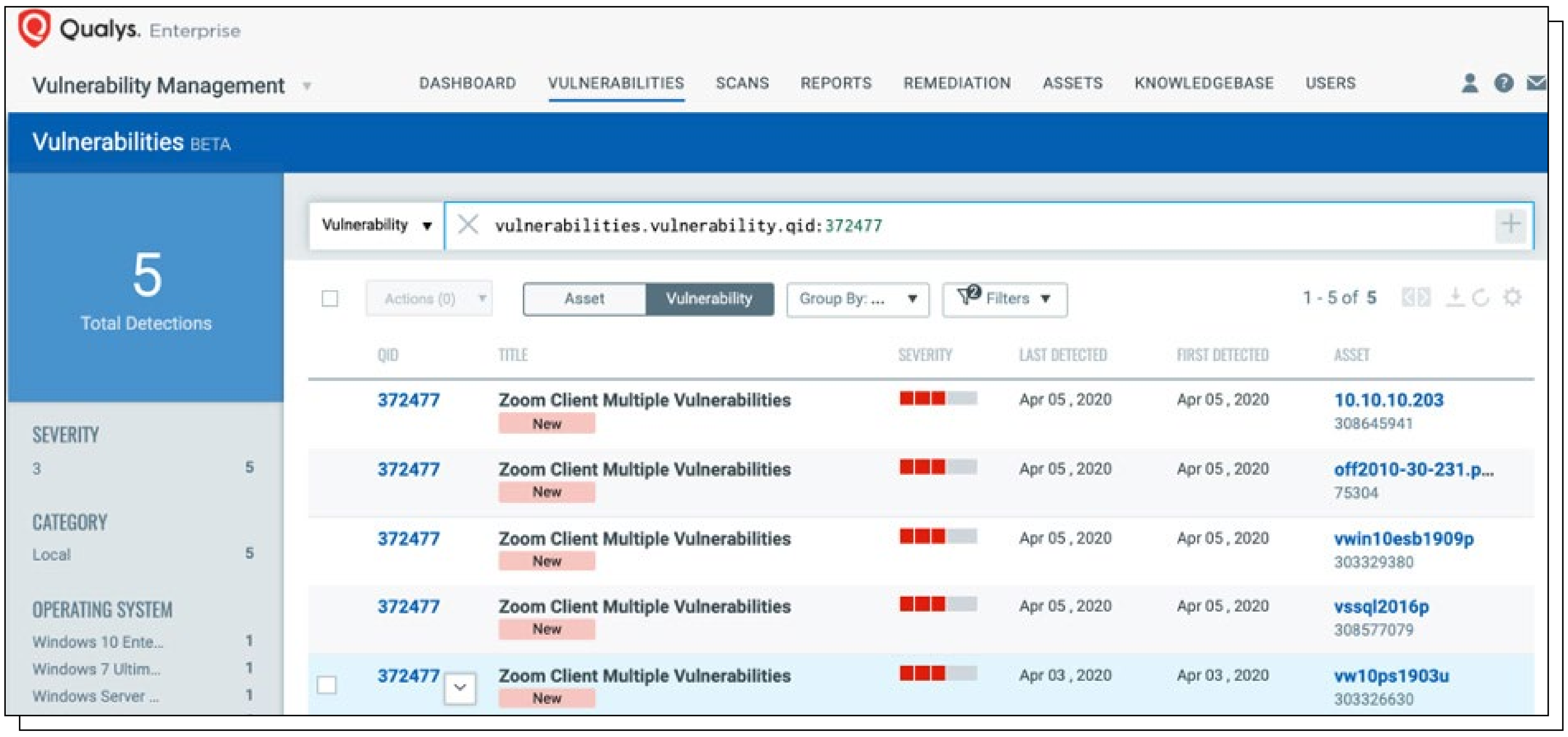
LIFECYCLE	
GA	139
Unknown	51

	CATEGORY	LICENSE	LIFECYCLE	INSTANCES
Zoom Video Communications Zoo... 4.6.0(13614.1202)	Collaboration Web Conferencing	Commercial	GA: Nov 30 2019 (estimated) EOL: Nov 30 2024 (estimated)	12
Zoom Video Communications Zoo... 4.5.5	Collaboration Web Conferencing	Commercial	GA: Aug 24 2019 (estimated) EOL: Aug 24 2024 (estimated)	11
Zoom Video Communications Zoo... 4.5.6	Collaboration Web Conferencing	Commercial	GA: Aug 24 2019 (estimated) EOL: Aug 24 2024 (estimated)	9
Zoom Video Communications Zoo... 4.5.9(5757.1110)	Collaboration Web Conferencing	Commercial	GA: Aug 24 2019 (estimated) EOL: Aug 24 2024 (estimated)	9
Zoom Video Communications Zoo... 4.4.55387.0716	Collaboration Web Conferencing	Commercial	GA: Apr 13 2019 (estimated) EOL: Apr 13 2024 (estimated)	8
Zoom Video Communications Zoo...	Collaboration	Commercial	GA: Nov 30 2019 (estimated)	[illegible]

INVENTORY OF COLLABORATION TOOLS ACROSS REMOTE ENDPOINTS

A simple query tags impacted remote hosts with the “CollaborationTools” asset tag for Zoom vulnerabilities:

COLLABORATIONTOOLS ASSET TAG



5
Total Detections

SEVERITY

3	5

CATEGORY

Local	5

OPERATING SYSTEM

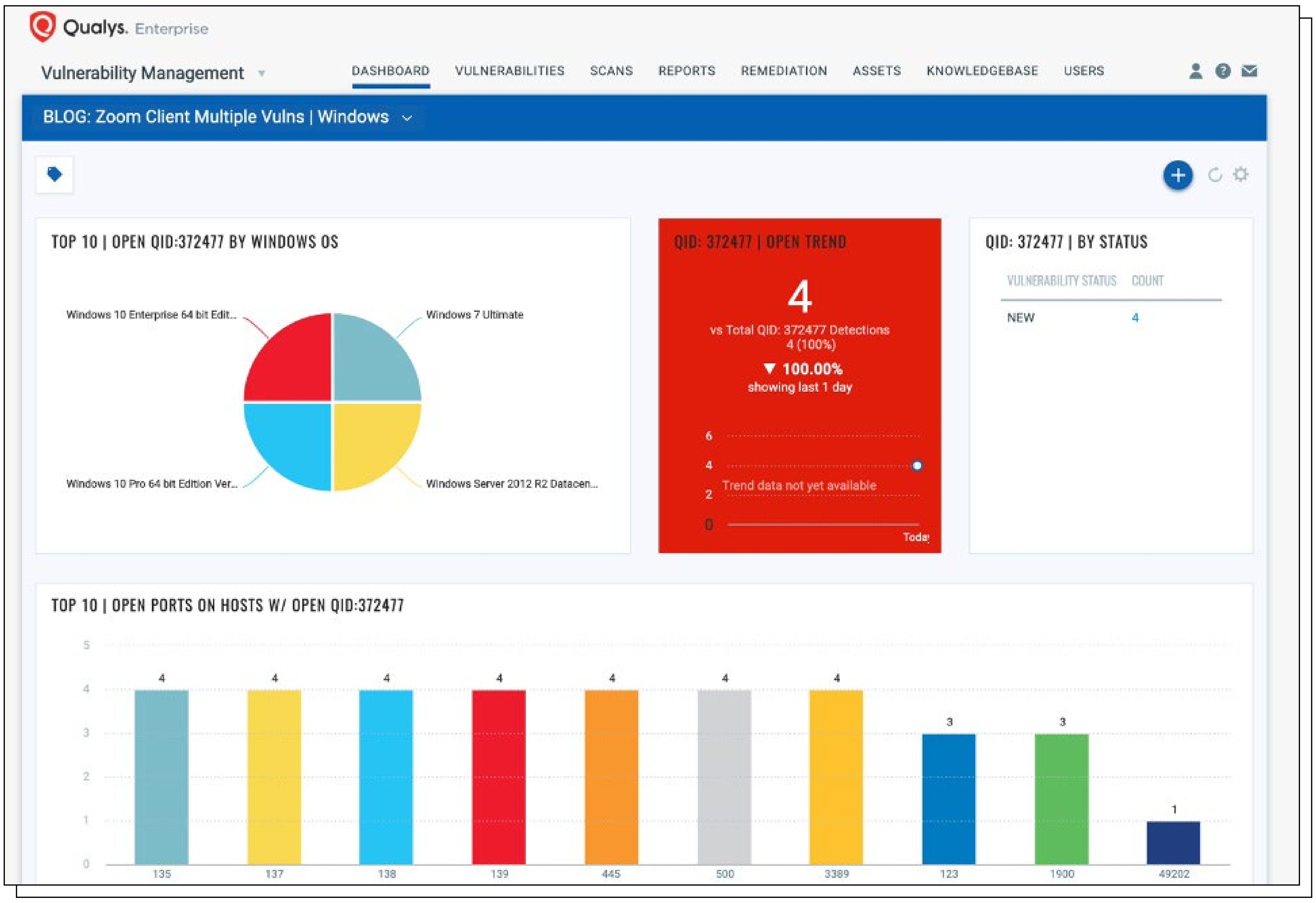
Windows 10 Ente...	1
Windows 7 Ultim...	1
Windows Server ...	1

Vulnerability ▾ vulnerabilities.vulnerability.qid:372477

QID	TITLE	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET
372477	Zoom Client Multiple Vulnerabilities New	■■■□	Apr 05 , 2020	Apr 05 , 2020	10.10.10.203 308645941
372477	Zoom Client Multiple Vulnerabilities New	■■■□	Apr 05 , 2020	Apr 05 , 2020	off2010-30-231.p... 75304
372477	Zoom Client Multiple Vulnerabilities New	■■■□	Apr 05 , 2020	Apr 05 , 2020	vwin10esb1909p 303329380
372477	Zoom Client Multiple Vulnerabilities New	■■■□	Apr 05 , 2020	Apr 05 , 2020	vssql2016p 308577079
372477	Zoom Client Multiple Vulnerabilities New	■■■□	Apr 03 , 2020	Apr 03 , 2020	vw10ps1903u 303326630

To help prioritize patching effort, users are provided with a complete view of all vulnerabilities in collaboration and productivity applications across their remote endpoints.

VULNERABILITY MANAGEMENT

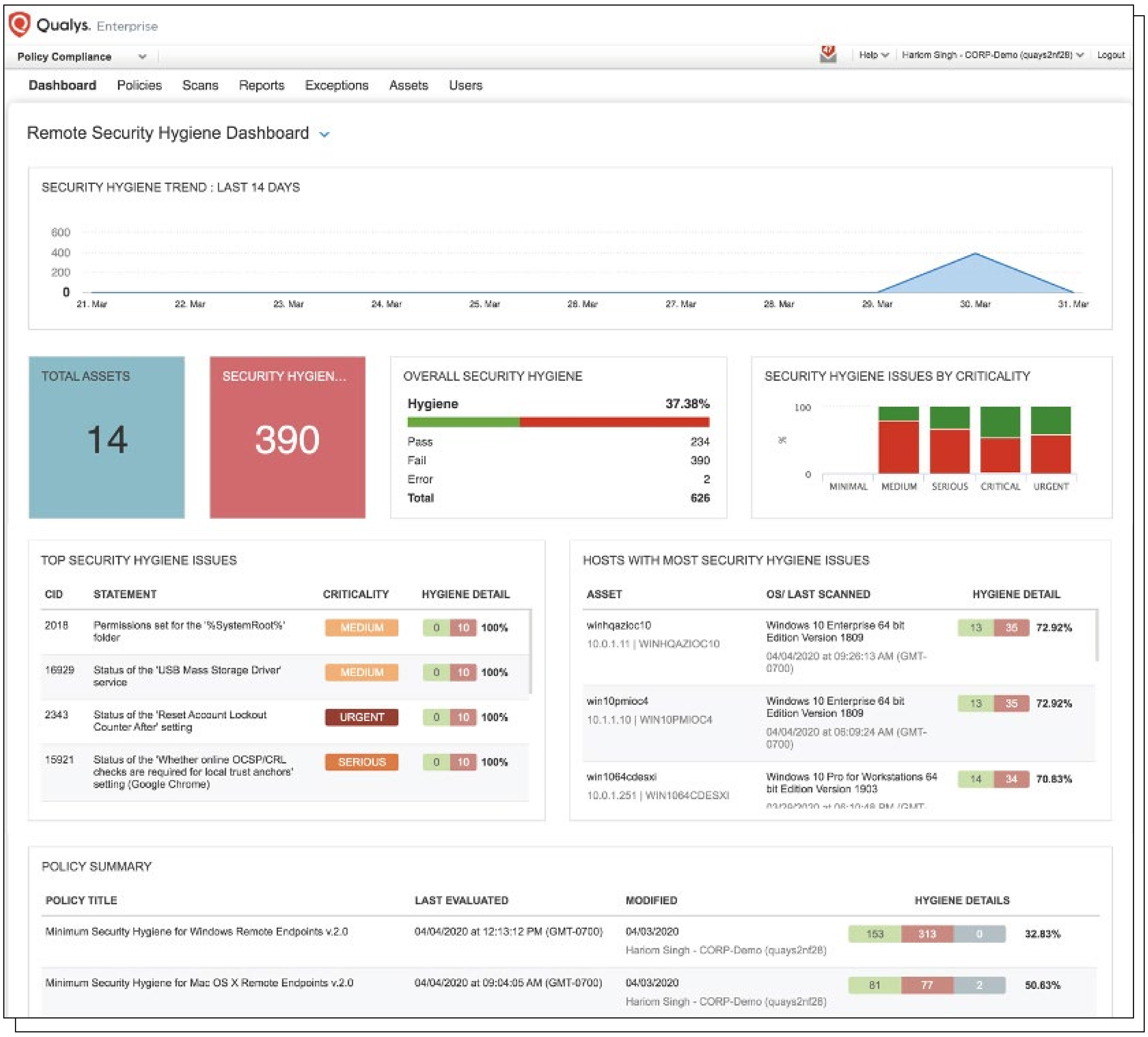

Qualys. Enterprise
Vulnerability Management ▾
DASHBOARD
VULNERABILITIES
SCANS
REPORTS
REMEDIATION
ASSETS
KNOWLEDGEBASE
USERS
BLOG: Zoom Client Multiple Vulns | Windows
TOP 10 | OPEN QID:372477 BY WINDOWS OS
Windows 10 Enterprise 64 bit Edit...
Windows 7 Ultimate
Windows 10 Pro 64 bit Edition Ver...
Windows Server 2012 R2 Datacen...
QID: 372477 | OPEN TREND
4
vs Total QID: 372477 Detections
4 (100%)
▼ 100.00%
showing last 1 day
6
4
2
0
Trend data not yet available
Today
QID: 372477 | BY STATUS
VULNERABILITY STATUS
COUNT
NEW
4
TOP 10 | OPEN PORTS ON HOSTS W/ OPEN QID:372477
5
4
3
2
1
0
4
4
4
4
4
4
4
3
3
1
135
137
138
139
445
500
3389
123
1900
49202

Enabling trending via the dashboard widgets allows users to track specific trends, such as the Zoom vulnerability in the example, in their environment by importing pre-configured Zoom Vulnerabilities Dashboard.

One of the other key aspects of securing remote computers is their configuration hygiene and that you harden security settings of the technologies you are using on the remote computers. Users can easily manage their security hygiene and configurations with the Remote Endpoint Protection service.

Qualys Malware Detection, integrated with the Remote Endpoint Protection offering and powered by the Qualys Platform and Cloud Agent, uses file reputation and threat classification to detect known malicious files on remote endpoints.

SECURITY HYGIENE



Remote Security Hygiene Dashboard

SECURITY HYGIENE TREND : LAST 14 DAYS

TOTAL ASSETS

14

SECURITY HYGIEN...

390

OVERALL SECURITY HYGIENE

Hygiene	37.38%
Pass	234
Fail	390
Error	2
Total	**626**

SECURITY HYGIENE ISSUES BY CRITICALITY

TOP SECURITY HYGIENE ISSUES

CID	STATEMENT	CRITICALITY	HYGIENE DETAIL	
2018	Permissions set for the '%SystemRoot%' folder	MEDIUM	0 10	100%
16929	Status of the 'USB Mass Storage Driver' service	MEDIUM	0 10	100%
2343	Status of the 'Reset Account Lockout Counter After' setting	URGENT	0 10	100%
15921	Status of the 'Whether online OCSP/CRL checks are required for local trust anchors' setting (Google Chrome)	SERIOUS	0 10	100%

HOSTS WITH MOST SECURITY HYGIENE ISSUES

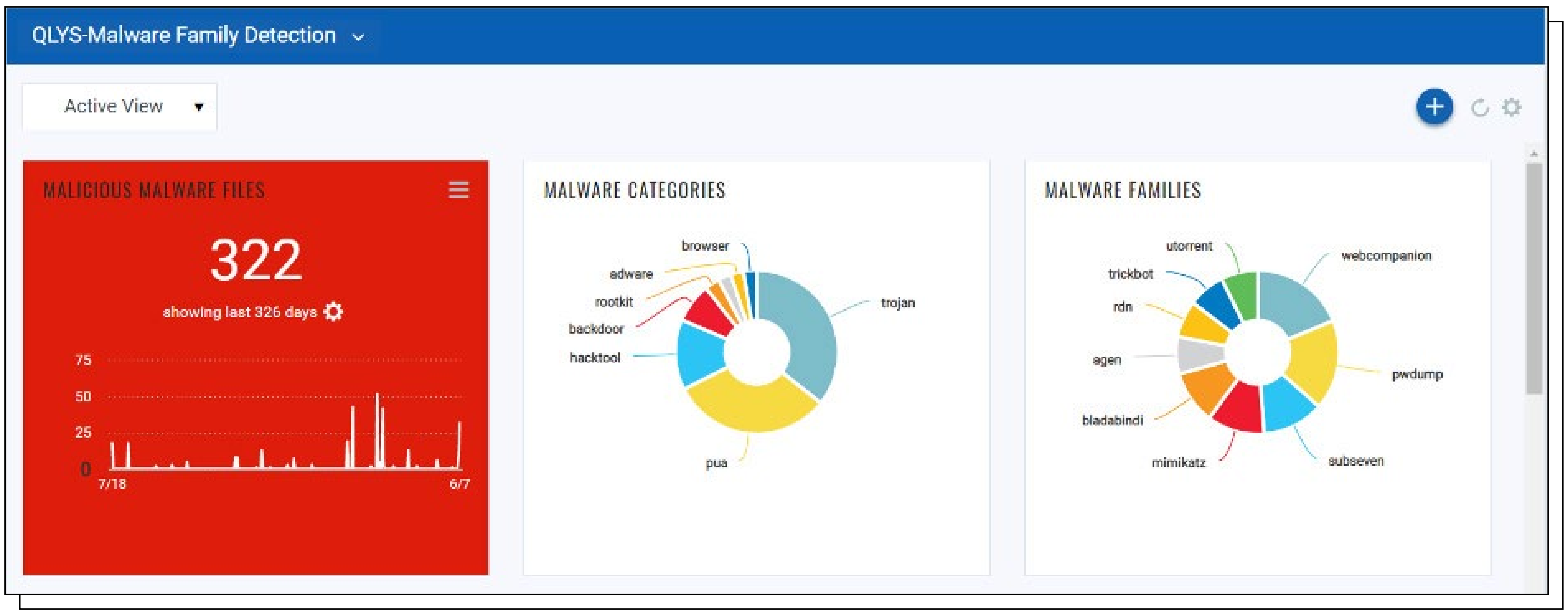
ASSET	OS/ LAST SCANNED	HYGIENE DETAIL	
winhqazioc10 10.0.1.11 | WINHQAZIOC10	Windows 10 Enterprise 64 bit Edition Version 1809 04/04/2020 at 09:26:13 AM (GMT-0700)	13 35	72.92%
win10pmioc4 10.1.1.10 | WIN10PMIOC4	Windows 10 Enterprise 64 bit Edition Version 1809 04/04/2020 at 05:09:24 AM (GMT-0700)	13 35	72.92%
win1064cdesxi 10.0.1.251 | WIN1064CDESXI	Windows 10 Pro for Workstations 64 bit Edition Version 1903 03/29/2020 at 08:10:48 PM (GMT-	14 34	70.83%

POLICY SUMMARY

POLICY TITLE	LAST EVALUATED	MODIFIED	HYGIENE DETAILS	
Minimum Security Hygiene for Windows Remote Endpoints v.2.0	04/04/2020 at 12:13:12 PM (GMT-0700)	04/03/2020 Hariom Singh - CORP-Demo (quays2nf28)	153 313 0	32.83%
Minimum Security Hygiene for Mac OS X Remote Endpoints v.2.0	04/04/2020 at 09:04:05 AM (GMT-0700)	04/03/2020 Hariom Singh - CORP-Demo (quays2nf28)	81 77 2	50.63%

Qualys Malware Detection, integrated with the Remote Endpoint Protection offering and powered by the Qualys Platform and Cloud Agent, uses file reputation and threat classification to detect known malicious files on remote endpoints. As a result, organizations can respond more quickly to malware ultimately increasing their overall security posture.

DETECTION



In summary, with recent remote endpoint surge, attack surface of the organizations has expanded beyond just "crown jewels", as weak remote hosts can compromise the security of the organizations and could result in a data breach.

Qualys Remote Endpoint Protection allows security teams to gain instant and continuous visibility of remote hosts in terms of their vulnerabilities, correlated patches, malware, security hygiene issues. Security teams will be able to prioritize missing patches for critical vulnerabilities and deploy them directly from the cloud.

The patches are delivered securely and directly from vendors' websites and content delivery networks to ensure there is little to no impact on internet connectivity or the bandwidth of the organization.

The Malware Detection capability integrated in remote endpoint protection detects malware missed by anti-virus and classifies malware into threat categories and malware families to prioritize incident response.

Healthcare delivery organizations have started demanding better security from medical device manufacturers (MDMs).

How to build up cybersecurity for medical devices

AUTHOR_Zeljka Zorz, Managing Editor, (IN)SECURE Magazine

Manufacturing medical devices with cybersecurity firmly in mind is an endeavor that, according to Christopher Gates, an increasing number of manufacturers is trying to get right.

Healthcare delivery organizations have started demanding better security from medical device manufacturers (MDMs), he says, and many have implemented secure procurement processes and contract language for MDMs that address the cybersecurity of the device itself, secure installation, cybersecurity support for the life of the product in the field, liability for breaches caused by a device not following current best practice, ongoing support for events in the field, and so on.

"For someone like myself who has been focused on cybersecurity at MDMs for over 12 years, this is excellent progress as it will force MDMs to take security seriously or be pushed out of the market by competitors who do take it seriously. Positive pressure from MDMs is driving cybersecurity forward more than any other activity," he told (IN)SECURE Magazine.

Gates is a principal security architect at Velentium and one of the authors of the recently released Medical Device Cybersecurity for Engineers and Manufacturers, a comprehensive guide to medical device secure lifecycle management, aimed at engineers, managers, and regulatory specialists.

In this interview, he shares his knowledge regarding the cybersecurity mistakes most often made by manufacturers, on who is targeting medical devices (and why), his view on medical device cybersecurity standards and initiatives, and more.

[Answers have been edited for clarity.]

_ *Are attackers targeting medical devices with a purpose other than to use them as a way into a healthcare organization's network?*

The easy answer to this is "yes," since many MDMs in the medical device industry perform "competitive analysis" on their competitors' products. It is much easier and cheaper for them to have a security researcher spend a few hours extracting an algorithm from a device for analysis than to spend months or even years of R&D work to pioneer a new algorithm from scratch.

No communications medium is inherently secure; it's what you do at the application level that makes it secure.

Also, there is a large, hundreds-of-millions-of-dollars industry of companies who "re-enable" consumed medical disposables. This usually requires some fairly sophisticated reverse-engineering to return the device to its factory default condition.

Lastly, the medical device industry, when grouped together with the healthcare delivery organizations, constitutes part of critical national infrastructure. Other industries in that class (such as nuclear power plants) have experienced very directed and sophisticated attacks targeting safety backups in their facilities. These attacks seem to be initial testing of a cyber weapon that may be used later.

While these are clearly nation-state level attacks, you have to wonder if these same actors have been exploring medical devices as a way to inhibit our medical response in an emergency. I'm speculating: we have no evidence that this has happened. But then again, if it has happened there likely wouldn't be any evidence, as we haven't been designing medical devices and infrastructure with the ability to detect potential cybersecurity events until very recently.

_ *What are the most often exploited vulnerabilities in medical devices?*

It won't come as a surprise to anyone in security when I say "the easiest vulnerabilities to exploit." An attacker is going to start with the obvious ones, and then increasingly get more sophisticated. Mistakes made by developers include:

Unsecured firmware updating

I personally always start with software updates in the field, as they are so frequently implemented incorrectly. An attacker's goal here is to gain access to the firmware with the intent of reverse-engineering it back into easily readable source code that will yield more widely exploitable vulnerabilities (e.g., one impacting every device in the world). All firmware update methods have at least three very common potential design vulnerabilities. They are:

- Exposure of the binary executable (i.e., it isn't encrypted)
- Corrupting the binary executable with added code (i.e., there isn't an integrity check)
- A rollback attack which downgrades the version of firmware to a version with known exploitable vulnerabilities (there isn't metadata conveying the version information).

Overlooking physical attacks

Physical attack can be mounted:

- Through an unsecured JTAG/SWD debugging port
- Via side-channel (power monitoring, timing, etc.) exploits to expose the values of cryptographic keys
- By sniffing internal busses, such as SPI and I2C
- Exploiting flash memory external to the microcontroller (a $20 cable can get it to dump all of its contents)

Manufacturing support left enabled

Almost every medical device needs certain functions to be available during manufacturing. These are usually for testing and calibration, and none of them should be functional once the device is fully deployed. Manufacturing commands are frequently documented in PDF files used for maintenance, and often only have minor changes across product/model lines inside the same manufacturer, so a little experimentation goes a long way in letting an attacker get access to all kinds of unintended functionality.

No communication authentication

Just because a communications medium connects two devices doesn't mean that the device being connected to is the device that the manufacturer or end-user expects it to be. No communications medium is inherently secure; it's what you do at the application level that makes it secure.

Bluetooth Low Energy (BLE) is an excellent example of this. Immediately following a pairing (or re-pairing), a device should always, always perform a challenge-response process (which utilizes cryptographic primitives) to confirm it has paired with the correct device.

I remember attending an on-stage presentation of a new class II medical device with a BLE interface. From the audience, I immediately started to explore the device with my smartphone. This device had no authentication (or authorization), so I was able to perform all operations exposed on the BLE connection. I was engrossed in this interface when I suddenly realized there was some commotion on stage as they couldn't get their demonstration to work: I had accidentally taken over the only connection the device supported. (I then quickly terminated the connection to let them continue with the presentation.)

> *Probably the most important thing that a majority of MDMs need to understand and accept is that their developers have probably never been trained in cybersecurity.*

_ *What things must medical device manufacturers keep in mind if they want to produce secure products?*

There are many aspects to incorporating security into your development culture. These can be broadly lumped into activities that promote security in your products, versus activities that convey a false sense of security and are actually a waste of time.

Probably the most important thing that a majority of MDMs need to understand and accept is that their developers have probably never been trained in cybersecurity. Most developers have limited knowledge of how to incorporate cybersecurity into the development lifecycle, where to invest time and effort into securing a device, what artifacts are needed for premarket submission, and how to proper utilize cryptography. Without knowing the details, many managers assume that security is being adequately included somewhere in their company's development lifecycle; most are wrong.

To produce secure products, MDMs must follow a secure "total product life cycle," which starts on the first day of development and ends years after the product's end of life or end of support.

> *Security is about protecting the business model of an MDM. This includes the device's safety and efficacy for the patient, which is what the regulations address, but it also includes public opinion, loss of business, counterfeit accessories, theft of intellectual property, and so forth.*

They need to:

- Know the three areas where vulnerabilities are frequently introduced during development (design, implementation, and through third-party software components), and how to identify, prevent, or mitigate them
- Know how to securely transfer a device to production and securely manage it once in production
- Recognize an MDM's place in the device's supply chain: not at the end, but in the middle. An MDM's cybersecurity responsibilities extend up and down the chain. They have to contractually enforce cybersecurity controls on their suppliers, and they have to provide postmarket support for their devices in the field, up through and after end-of-life
- Create and maintain Software Bills of Materials (SBOMs) for all products, including legacy products. Doing this work now will help them stay ahead of regulation and save them money in the long run.

> *Until very recently, cybersecurity was not part of traditional engineering or software development curriculum. Most developers need additional training in cybersecurity.*

They must avoid mistakes like:

- Not thinking that a medical device needs to be secured
- Assuming their development team 'can' and 'is' securing their product
- Not designing-in the ability to update the device in the field
- Assuming that all vulnerabilities can be mitigated by a field update
- Only considering the security of one aspect of your design (e.g., its wireless communication protocol). Security is a chain: for the device to be secure, all the links of the chain need to be secure. Attackers are not going to consider certain parts of the target device 'out of bounds' for exploiting.

Ultimately, security is about protecting the business model of an MDM. This includes the device's safety and efficacy for the patient, which is what the regulations address, but it also includes public opinion, loss of business, counterfeit accessories, theft of intellectual property, and so forth. One mistake I see companies frequently make is doing the minimum on security to gain regulatory approval but neglecting to protect their other business interests along the way – and those can be very expensive to overlook.

_ What about the developers? Any advice on skills they should acquire or brush up on?

First, I'd like to take some pressure off developers by saying that it's unreasonable to expect that they have some intrinsic knowledge of how to implement cybersecurity in a product. Until very recently, cybersecurity was not part of traditional engineering or software development curriculum. Most developers need additional training in cybersecurity.

And it's not only the developers. More than likely, project management has done them a huge disservice by creating a system-level security requirement that says something like, "Prevent ransomware attacks." What is the development team supposed to do with that requirement? How is it actionable?

> *While all of these regulations have the same goal of securing medical devices, how they get there is anything but harmonized among them.*

At the same time, involving the company's network or IT cybersecurity team is not going to be an automatic fix either. IT Cybersecurity diverges from Embedded Cybersecurity in many respects, from detection to implementation of mitigations. No MDM is going to be putting a firewall on a device that is powered by a CR2032 battery anytime soon; yet there are ways to secure such a low-resource device.

In addition to the how-to book we wrote, Velentium will soon offer training available specifically for the embedded device domain, geared toward creating a culture of cybersecurity in development teams. My audacious goal is that within 5 years every medical device developer I talk to will be able to converse intelligently on all aspects of securing a medical device.

_ What cybersecurity legislation/regulation must companies manufacturing medical devices abide by?

It depends on the markets you intend to sell into. While the US has had the Food and Drug Administration (FDA) refining its medical device cybersecurity position since 2005, others are more recent entrants into this type of regulation, including Japan, China, Germany, Singapore, South Korea, Australia, Canada, France, Saudi Arabia, and the greater EU.

While all of these regulations have the same goal of securing medical devices, how they get there is anything but harmonized among them. Even the level of abstraction varies, with some focused on processes while others on technical activities.

But there are some common concepts represented in all these regulations, such as:

- Risk management
- Software bill of materials (SBOM)
- Monitoring
- Communication
- "Total Product Lifecycle"
- Testing

But if you plan on marketing in the US, the two most important document should be FDA's:

- 2018 – Draft Guidance: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
- 2016 – Final Guidance: Postmarket Management of Cybersecurity in Medical Devices (The 2014 version of the guidance on premarket submissions can be largely ignored, as it no longer represents the FDA's current expectations for cybersecurity in new medical devices).

_ What are some good standards for manufacturers to follow if they want to get cybersecurity right?

The Association for the Advancement of Medical Instrumentation's standards are excellent.
I recommend AAMI TIR57: 2016 and AAMI TIR97: 2019.

Also very good is the Healthcare & Public Health Sector Coordinating Council's (HPH SCC) Joint Security Plan. And, to a lesser extent, the NIST Cyber Security Framework.

The work being done at the US Department of Commerce / NTIA on SBOM definition for vulnerability management and postmarket surveillance is very good as well, and worth following.

_ What initiatives exist to promote medical device cybersecurity?

Notable initiatives I'm familiar with include, first, the aforementioned NTIA work on SBOMs, now in its second year. There are also several excellent working groups at HSCC, including the Legacy Medical Device group and the Security Contract Language for Healthcare Delivery Organizations group. I'd also point to numerous working groups in the H-ISAC Information Sharing and Analysis Organization (ISAO), including the Securing the Medical Device Lifecycle group.

And I have to include the FDA itself here, which is in the process of revising its 2018 premarket draft guidance; we hope to see the results of that effort in early 2021.

_ What changes do you expect to see in the medical devices cybersecurity field in the next 3-5 years?

So much is happening at high and low levels. For instance, I hope to see the FDA get more of a direct mandate from Congress to enforce security in medical devices.

Also, many working groups of highly talented people are working on ways to improve the security posture of devices, such as the NTIA SBOM effort to improve the transparency of software "ingredients" in a medical device, allowing end-users to quickly assess their risk level when new vulnerabilities are discovered.

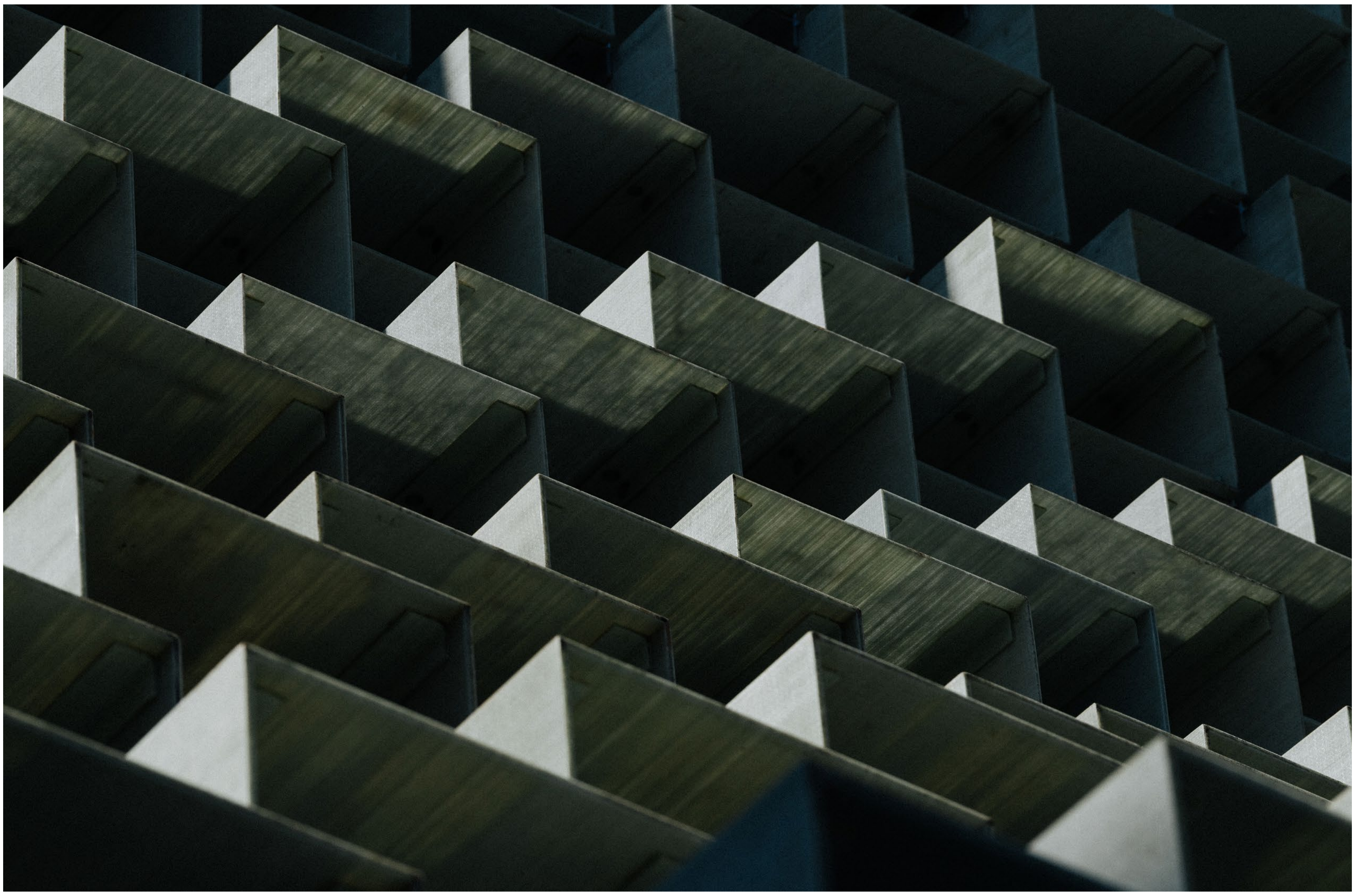
Semiconductor manufacturers continue to give us great mitigation tools in hardware, such as side-channel protections, cryptographic accelerators, virtualized security cores. Trustzone is a great example.

And at the application level, we'll continue to see more and better packaged tools, such as cryptographic libraries and processes, to help developers avoid cryptography mistakes. Also, we'll see more and better process tools to automate the application of security controls to a design.
HDOs and other medical device purchasers are better informed than ever before about embedded cybersecurity features and best practices. That trend will continue and will further accelerate demand for better-secured products.

I hope to see some effort at harmonization between all the federal, state, and foreign regulations that have been recently released with those currently under consideration.

One thing is certain: legacy medical devices that can't be secured will only go away when we can replace them with new medical devices that are secure by design. Bringing new devices to market takes a long time. There's lots of great innovation underway, but really, we're just getting started!

KILL PROCESS
QUARANTINE
UNINSTALL
PATCH OR REMEDIATE



State-backed hacking, cyber deterrence, and the need for international norms

AUTHOR_Zeljka Zorz, Managing Editor, (IN)SECURE Magazine

As time passes, state-backed hacking is becoming an increasingly bigger problem, with the attackers stealing money, information, credit card data, intellectual property, state secrets, and probing critical infrastructure.

While Chinese, Russian, North Korean and Iranian state-backed APT groups get most of the spotlight (at least in the Western world), other nations are beginning to join in the "fun."

It's a free for all, it seems, as the world has yet to decide on laws and norms regulating cyber attacks and cyber espionage in peacetime and find a way to make nation-states abide by them.

There is so far one international treaty on cybercrime (The Council of Europe Convention on Cybercrime) that is accepted by the nations of the European Union, United States, and other likeminded allies, notes Dr. Panayotis Yannakogeorgos, and it's contested by Russia and China, so it is not global and only applies to the signatories.

> *States are left to their own devices when it comes to devising a cyber deterrence strategy.*

Dr. Yannakogeorgos, who's a professor and faculty lead for a graduate degree program in Global Security, Conflict, and Cybercrime at the NYU School of Professional Studies Center for Global Affairs, believes this treaty could be both a good model text on which nations around the world can harmonize their own domestic criminal codes, as well as the means to begin the lengthy diplomatic negotiations with Russia and China to develop an international criminal law for cyber.

Cyber deterrence strategies

In the meantime, states are left to their own devices when it comes to devising a cyber deterrence strategy.

The US has been publicly attributing cyber espionage campaigns to state-backed APTs and regularly releasing technical information related to those campaigns, its legislators have been introducing legislation that would lead to sanctions for foreign individuals engaging in hacking activity that compromises economic and national security or public health, and its Department of Justice has been steadily pushing out indictments against state-backed cyber attackers and spies.

But while, for example, indictments by the US Department of Justice cannot reasonably be expected to result in the extradition of a hacker who has been accused of stealing corporate or national security secrets, the indictments and other forms of public attribution of cyber enabled malicious activities serve several purposes beyond public optics, Dr. Yannakogeorgos notes.

"First, they send a clear signal to China and the world on where the United States stands in terms of how governmental resources in cyberspace should be used by responsible state actors. That is, in order to maintain fair and free trade in a global competitive environment, a nation's intelligence services should not be engaged in stealing corporate secrets and then handing those secrets over to companies for their competitive advantage in global trade," he explained.

"Second, making clear attribution statements helps build a framework within which the United States can work with our partners and allies on countering threats. This includes joint declarations with allies or multilateral declarations where the sources of threats and the technical nature of the infrastructure used in cyber espionage are declared."

Finally, when public attribution is made, technical indicators of compromise, toolsets used, and other aspects are typically released as well.

"These technical releases have a very practical impact in that they 'burn' the infrastructure that a threat actor took time, money, and talent to develop and requires them to rebuild or retool. Certainly, the malware and other infrastructure can still be used against targets that have not calibrated their cyber defenses to block known pathways for attack. Defense is hard, and there is a complex temporal dimension to going from public indicators of compromise in attribution reports; however, once the world knows it begins to also increase the cost on the attacker to successfully hack a target," he added.

"In general, a strategy that is focused on shaping the behavior of a threat needs to include actively dismantling infrastructure where it is known. Within the US context, this has been articulated as persistently engaging adversaries through a strategy of 'defending forward.'"

The problem of attack attribution

The issue of how cyber attack attribution should be handled and confirmed also deserves to be addressed.

Dr. Yannakogeorgos says that, while attribution of cyber attacks is definitely not as clear-cut as seeing smoke coming out of a gun in the real world, with the robust law enforcement, public private partnerships, cyber threat intelligence firms, and information sharing via ISACs, the US has come a long way in terms of not only figuring out who conducted criminal activity in cyberspace, but arresting global networks of cyber criminals as well.

Granted, things get trickier when these actors are working for or on behalf of a nation-state. "If these activities are part of a covert operation, then by definition the government will have done all it can for its actions to be 'plausibly deniable.' This is true for activities outside of cyberspace as well. Nations can point fingers at each other, and present evidence. The accused can deny and say the accusations are based on fabrications," he explained.

> *In the realm of nation-state use of cyber, there have been dialogues within the United Nations for nearly two decades.*

"However, at least within the United States, we've developed a very robust analytic framework for attribution that can eliminate reasonable doubt amongst friends and allies and can send a clear signal to planners on the opposing side. Such analytic frameworks could become norms themselves to help raise the evidentiary standard for attribution of cyber activities to specific nation states."

A few years ago, Paul Nicholas (at the time the director of Microsoft's Global Security Strategy) and various researchers proposed the creation of an independent, global organization that would investigate and publicly attribute major cyber attacks – though they admitted that, in some cases, decisive attribution may be impossible.

More recently, Kristen Eichensehr, a Professor of Law at the University of Virginia School of Law with expertise in cybersecurity issues and cyber law, argued that "states should establish an international law requirement that public attributions must include sufficient evidence to enable crosschecking or corroboration of the accusations" – and not just by allies.

"In the realm of nation-state use of cyber, there have been dialogues within the United Nations for nearly two decades. The most recent manifestation is the UN Group of Governmental Experts that have discussed norms of responsible state behavior and issued non-binding statements to guide nations as they develop cyber capabilities," Dr. Yannakogeorgos pointed out.

"Additionally, private sector actors, such as the coalition declaring the need for a Geneva Convention for cyberspace, also have a voice in the articulation of norms. Academic groups such as the group of individuals involved in the research, debating, and writing of the Tallinn Manuals 1.0 and 2.0 are also examples of scholars who are articulating norms."

And while articulating and agreeing to specific norms will no doubt be a difficult task, he says that their implementation by signatories will be even harder.

"It's one thing to say that 'states will not target each other's critical infrastructure in cyberspace during peacetime' and another to not have a public reaction to states that are alleged to have not only targeted critical infrastructure but actually caused digital damage as a result of that targeting," he concluded.

WATERFALL
Stronger Than Firewalls
Unidirectional Security for Power Generation: Advanced Topics

The COVID-19 pandemic and online shift has brought to light the need for robust cybersecurity strategies and technology that facilitates safe practices

DaaS, BYOD, leasing and buying: Which is better for cybersecurity?

AUTHOR_Apu Pavithran, CEO, Hexnode

In the digital age, staff expect employers to provide hardware, and companies need hardware that allows employees to work efficiently and securely. There are already a number of models to choose from to purchase and manage hardware, however, with remote work policies becoming more popular, enterprises have to prioritize cybersecurity when making their selection.

The COVID-19 pandemic and online shift has brought to light the need for robust cybersecurity strategies and technology that facilitates safe practices. Since the pandemic started, the FBI has reported a 300 percent increase in cybercrime.

As more businesses are forced to operate at a distance, hackers are taking advantage of weak links in their networks. At the same time, the crisis has meant many enterprises have had to cut their budgets, and so risk compromising cybersecurity when opting for more cost-effective measures.

> *For many enterprises, DaaS is attractive because it allows them to acquire technology without having to outright buy, set up, and manage it*

Currently, Device-as-Service (DaaS), Bring-Your-Own-Device (BYOD) and leasing/buying are some of the most popular hardware options. To determine which is most appropriate for your business cybersecurity needs, here are the pros and cons of each:

Device-as-a-Service (DaaS)

DaaS models are when an organization distributes hardware like computers, tablets, and phones to employees with preconfigured and customized services and software. For many enterprises, DaaS is attractive because it allows them to acquire technology without having to outright buy, set up, and manage it – therefore saving time and money in the long run. Because of DaaS' growing popularity, 65 percent of major PC manufacturers now offer DaaS capabilities, including Apple and HP.

When it comes to cybersecurity, DaaS is favorable because providers are typically experts in the field. In the configuration phase, they are responsible for ensuring that all devices have the latest security protections installed as standard, and they are also responsible for maintaining such protections. Once the hardware is in use, DaaS models allow providers to monitor the company's entire fleet – checking that all devices adhere to security policies, including protocols around passwords, approved apps, and accessing sensitive data.

Another bonus is that DaaS can offer analytical insights about hardware, such as device location and condition. With this information, enterprises can be alerted if tech is stolen, missing or outdated and a threat to overall cybersecurity. Not to mention, a smart way to boost the level of protection given by DaaS models is to integrate it with Unified Endpoint Management (UEM). UEM helps businesses organize and control internet-enabled devices from a single interface and uses mobile threat detection to identify and thwart vulnerabilities or attacks among devices.

Nonetheless, to effectively utilize DaaS, enterprises have to determine their own relevant security principles before adopting the model. They then need to have an in-depth understanding of how these principles are applied throughout DaaS services and how the level of assurance enacts them. Assuming that DaaS completely removes enterprises from being involved in device cybersecurity would be unwise.

> *Although BYOD is favorable among employees – who can use devices that they are more familiar with – enterprises essentially lose control and visibility of how data is transmitted, stored, and processed.*

Bring-Your-Own-Device (BYOD)

BYOD is when employees use their own mobile, laptops, PCs, and tablets for work. In this scenario, companies have greater flexibility and can make significant cost savings, but there are many more risks associated with personal devices compared to corporate-issued devices. Although BYOD is favorable among employees – who can use devices that they are more familiar with – enterprises essentially lose control and visibility of how data is transmitted, stored, and processed.

Personal devices are dangerous because hackers can create a sense of trust via personal apps on the hardware and more easily coerce users into sharing business details or download malicious content. Plus, with BYOD, companies are dependent on employees keeping all their personal devices updated with the most current protective services. One employee forgetting to do so could negate the cybersecurity for the overall network.

Similar to DaaS, UEM can also help companies that have adopted BYOD take a more centralized approach to manage the risk of exposing their data to malicious actors. For example, UEM can block websites or content from personal devices, as well as implement passcodes, and device and disk encryption. Alternatively, VPNs are common to enhance cybersecurity in companies that allow BYOD. In the COVID-19 pandemic, 68 percent of employees claim their company has expanded VPN usage as a direct result of the crisis. It's worthwhile noting though, that VPNs only encrypt data accessed via the internet and cloud-based services.

When moving forward with BYOD models, enterprises must host regular training and education sessions around safe practices on devices, including recognizing threats, avoiding harmful websites, and the importance of upgrading. They also need to have documented and tested computer security incident response plans, so if any attacks do occur, they are contained as soon as possible.

Leasing / buying

Leasing hardware is when enterprises obtain equipment on a rental basis, in order to retain working capital that can be invested in other areas. In the past, as many as 80 percent of businesses chose to lease their hardware. The trend is less popular today, as SaaS products have proven to be more tailored and scalable.

Still, leasing is beneficial because rather than jeopardizing cybersecurity to purchase large volumes of hardware, enterprises can rent fully covered devices. Likewise, because the latest software typically requires the latest hardware, companies can rent the most recent tech at a fraction of the retail cost.

Purchasing hardware outright means companies have complete control over devices and can cherry-pick cybersecurity features to include

Comparable to DaaS providers, leasing companies are responsible for device maintenance and have to ensure that every laptop, phone, and tablet has the appropriate security software. Again, however, this does not absolve enterprises from taking an active role in cybersecurity implementation and surveillance.

Unlike leasing, where there can be uncertainty over who owns the cybersecurity strategy, buying is more straightforward. Purchasing hardware outright means companies have complete control over devices and can cherry-pick cybersecurity features to include. It also means they can be more flexible with cybersecurity partners, running trials with different solutions to evaluate which is the best fit.

That said, buying hardware has a noticeable downside where equipment becomes obsolete once new versions are released. 73 percent of senior leaders from enterprises actually agree that an abundance of outdated equipment leaves companies vulnerable to data security breaches. Considering that, on average, a product cycle takes only 12 to 24 months, and there are thousands of hardware manufacturers at work, devices can swiftly become outdated.

> *Despite all the perks, it has to be acknowledged that BYOD and leasing pose the biggest obstacles for enterprises because they take cybersecurity monitoring and control out of companies' hands.*

Additionally, because buying is a more permanent action, enterprises run the risk of being stuck with hardware that has been compromised. As opposed to software which can be relatively easily patched to fix, hardware often has to be sent off-site for repairs. This may result in enterprises with limited hardware continuing to use damaged or unprotected devices to avoid downtime in workflows.

> *Businesses should never underestimate the power of a transparent, well-researched, and constantly evolving security framework – one which a hardware model complements, not solely creates.*

If and when a company does decide to dispose of hardware, there are complications around guaranteeing that systems are totally blocked, and databases or networks cannot be accessed afterwards. In contrast, providers from DaaS and leasing models expertly wipe devices at the end of contracts or when disposing of them, so enterprises don't have to be concerned about unauthorized access.

Putting cybersecurity front-and-center

DaaS, BYOD, and leasing/buying all have their own unique benefits when it comes to cybersecurity. Despite all the perks, it has to be acknowledged that BYOD and leasing pose the biggest obstacles for enterprises because they take cybersecurity monitoring and control out of companies' hands.

Nevertheless, for all the options mentioned, UEM is a valuable way to bridge gaps and empower businesses to be in control of cybersecurity, while still being agile.

Ultimately, the most impactful cybersecurity measures are the ones that enterprises are firmly vested in, whatever hardware model they adopt.

Businesses should never underestimate the power of a transparent, well-researched, and constantly evolving security framework – one which a hardware model complements, not solely creates.