[+] (IN)SECUREMagazine

06 | 2020
ISSUE 66

Cybersecurity is a board level issue

CISSP®

Certified Information Systems Security Professional

An (ISC)² Certification

FREE CISSP WEBCAST SERIES

Get a Look Inside the CISSP Domains.

Watch Now

(ISC)²® Inspiring a Safe and Secure Cyber World

Table of contents

Featured experts

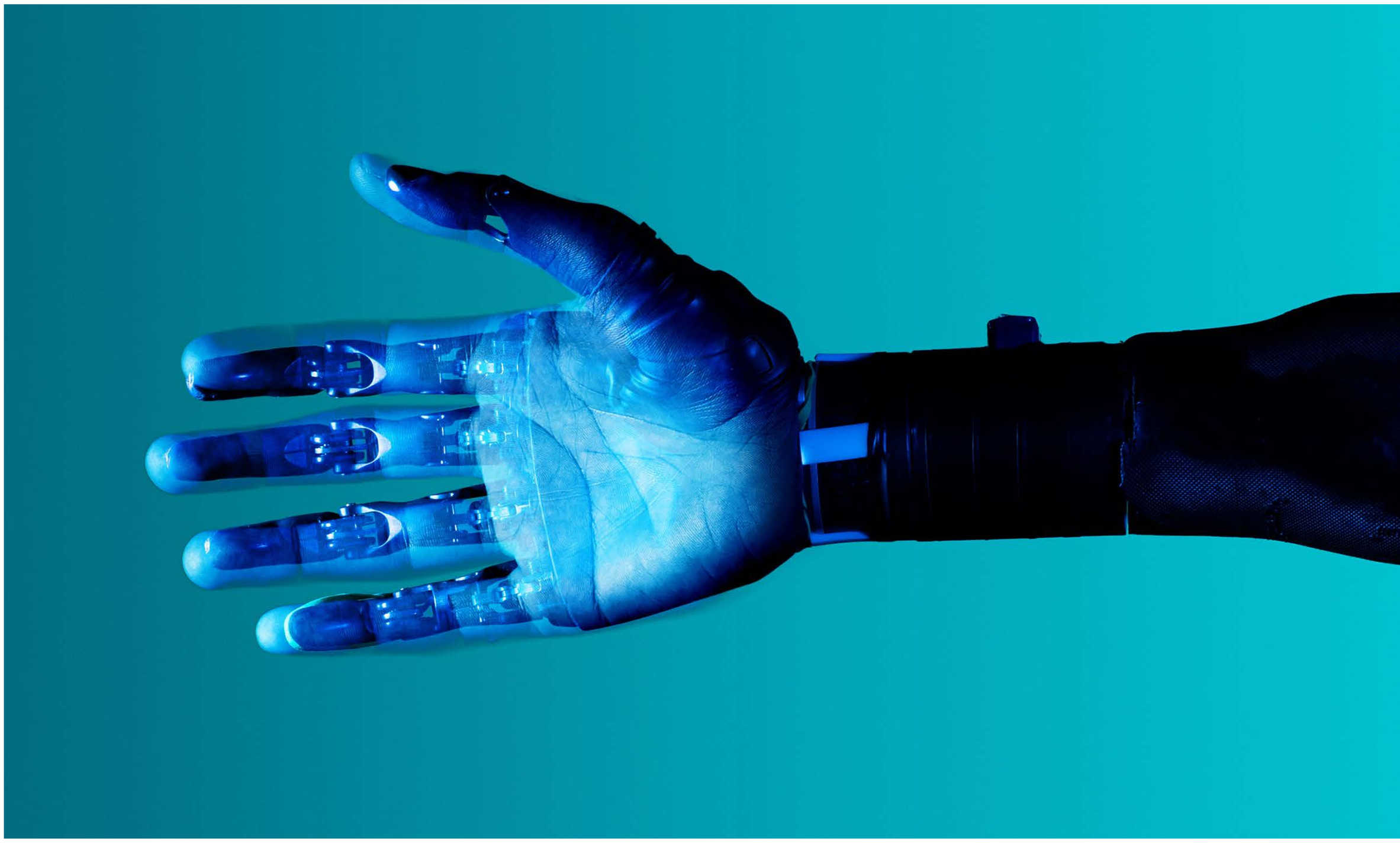
MICHAEL GREENE, CEO, Enzoic
ALEX HAYNES, CISO, CDL
TONIMIR KISASONDI, Founder, Oru
CHRISTIAN LEES, CTO and CIO, Vigilante
MICHAEL MORRISON, CEO, CoreView
OREN YUNGER, Venture Capital Investor, GGV Capital
BEN ZIOMEK, CPO, Actuate

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



Let’s be realistic about our expectations of AI

AUTHOR_ Ben Ziomek, CPO, Actuate

Pop culture contains no shortage of intelligent robots. When the tool became viable and widely available in real life, people brought a number of enthusiastic but unrealistic expectations to the table. Unfortunately, Amazon’s Alexa isn’t as smart as HAL 9000, and a Roomba can’t clean your home like the Jetsons’ metallic maid, Rosie.

People rely on the stories, both fictional and nonfictional, to inform their perceptions.

Media narratives often form public perceptions. This is especially true for technological themes because the general public doesn’t have an in-depth understanding of the science and technology behind them. People rely on the stories, both fictional and nonfictional, to inform their perceptions.

A study by the Royal Society outlines how narratives — or the way things are portrayed and perceived — have affected public discourse around scientific areas such as nuclear power, genetic modification, and climate change. We can use these lessons from history to inform how we shape the narratives around artificial intelligence.

Many nontechnical observers today think of AI as a sci-fi technology with human-level performance, but AI is still only as smart as the data that scientists feed to it.

Media misrepresentations of AI may seem harmless when we think about animated robots on "The Jetsons," but the consequences of portrayals both in entertainment and other media reporting can be significant when it comes to AI research and development. Many nontechnical observers today think of AI as a sci-fi technology with human-level performance, but AI is still only as smart as the data that scientists feed to it.

For example, running is an action that can be clearly defined. Scientists can train machines to detect that someone is running by feeding them datasets that clearly represent this motion. But the same can't be said for something like suspicious action. Whether someone is acting suspiciously or not is something that can't even be clearly defined by a human. Therefore, it would be impossible for scientists to train a machine to detect if someone is acting suspiciously.

How can today's (or even tomorrow's) AI tell the difference between an intruder with real malicious intent and a technician authorized to be on-site? How about the difference between someone walking in a confident way and a suspicious way?

Instead of assuming AI's inability to complete such tasks is a failure of the technology, consumers need to shift their understanding and realize that it's simply the reality of AI. Members of the public need to shift their expectations away from sensationalized accounts and toward the true capabilities of machines.

As enterprises and individuals flock to AI, they must realize that effective, and often impressive, technologies aren't always capable in the same ways they would expect.

Leveraging AI in security for realistic results

In security, specifically, providers have a lot to gain from the advent and implementation of AI. Automating the work of monitoring surveillance cameras and identifying potential threats promises to make the industry far more efficient and cost-effective while also improving security. Contrary to what some may believe, however, security can't be fully automated. The human element will always be essential.

Consider our hypothetical suspicious person. How can today's (or even tomorrow's) AI tell the difference between an intruder with real malicious intent and a technician authorized to be on-site? How about the difference between someone walking in a confident way and a suspicious way?

These determinations depend on understanding subjective context based on superficial data — a trait that is, so far, only human. It will take years before AI achieves that level of understanding. That's not because it is underpowered now, but because analyzing thousands of variables in real time takes significant computing power.

That's important to keep in mind when considering emotion recognition algorithms developed by tech titans. Each of them might offer impressive

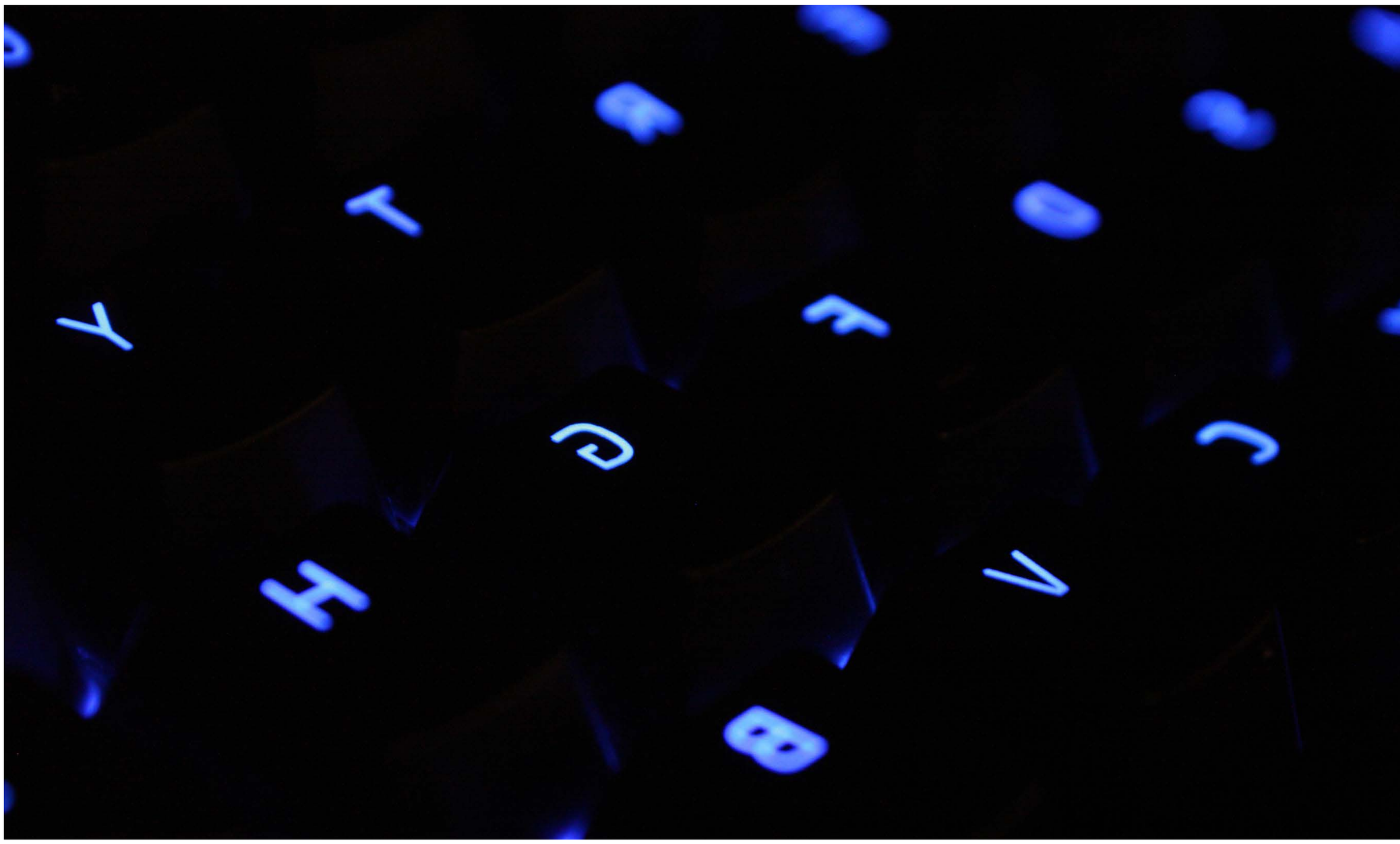
capabilities that can strategically supplement the work security teams already do — but none of them can replace the human members of those teams.

Worse than overestimating what AI can do, we tend to see it as a full replacement for human labor. This idea contributes to the perception of a binary humans-versus-robots scenario. But that perspective fails to see the fundamental difference between the two: AI offers high levels of precision and specialization, while humans have common sense and contextual knowledge. In that context, we see that man and machine must complement one another to work effectively.

Security companies hoping to leverage AI for real impact need to acknowledge the realistic capabilities of their technology. Current AI can detect specific actions and items, but there's no AI in development that is even close to being able to make clear evaluations of security decisions.

If an AI-enabled camera sees someone loitering outside, for instance, a human will still need to evaluate the situation to determine whether that human is a threat. AI can say something looks like a weapon or that someone is loitering, but it can't understand the context around situations. Maybe that weapon is only a realistic toy, or perhaps the "loiterer" is actually a contractor who's on-site for the day.

These are simple situations, but AI isn't yet capable of answering them. It requires the contextual knowledge only humans possess. In order for technology to be effective, both vendors and consumers must think about the capabilities of AI realistically. It can be a helpful security tool, but every piece of tech still needs to rely on highly trained humans to evaluate potential threats.



Being a bug hunter who discloses their discoveries to vendors (as opposed to selling the information to the highest bidder) has been and is an ambition of many ethical hackers.

Before vendors started paying for the info, the best they could hope for was a lucrative job offer, though an entry in the company's Hall of Fame was a good enough incentive for most.

Full-time bug hunting: Pros and cons of an emerging career

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

These days many vendors and service providers have an official vulnerability disclosure program, either run internally or managed by a third party, and offer bug bounties for quality reports about newly discovered security vulnerabilities in their offerings.

The sheer number of bug bounty programs in existence and the fact that the bounties occasionally reach tens or hundreds of thousands dollars has, as a result, lead many a bug hunter to concentrate on searching for vulnerabilities as their only occupation.

Those who have yet to make that transition but would like to are wondering whether they are cut out for this kind of life/work.

Full-time bug hunting is not for everybody

For someone who already has a consistent, well paying job and maybe a couple of kids, bug hunting as a full-time occupation wouldn't be the best thing to just jump into, says **Tommy DeVoss**, a hacker from Virginia (U.S.A.).

> *Each of these three full-time hacker/bug hunters we interviewed for this feature has had a different route to their current work position.*

One of the reasons is that searching for bugs involves a lot of effort (learning) and time. But if you are ready for this you will succeed, says **Cosmin**, a 30-year-old Romanian hacker who lives in Osnabrück, Germany (and prefers not to share his last name).

"Read the documentation, learn to write your own tools, read security articles, invest time in research, learn to write reports and always approach your target tactically and with the strategy that fits you well," he advised.

"It's also very important to realize that you and your mindset are unique, so don't follow what this or that person says. Try to grab little bits of knowledge and skill from everybody, analyze them and then integrate them in your workflow only if they suit you."

Santiago Lopez, a young man from Argentina who a year ago became the first bug hunter to earn over $1 million in bounty awards through the HackerOne bug bounty platform, pointed out that "wasted time" is also something that a would-be full-time bug hunter has to take into account.

What he means is that sometimes a bug you worked long and hard to discover, document and report has been flagged by another hacker days or mere hours before – and those who come second are rarely awarded anything.

Being able to deal with this fact of life is essential for aspiring bug hunters, he says, just as much as having unrelenting curiosity and a desire to play around with stuff and break it.

Getting into bug hunting

Each of these three full-time hacker/bug hunters we interviewed for this feature has had a different route to their current work position.

Lopez's path was the most straight-forward: he started hacking when he was 15 and earned his first bug bounty when he was 16. Since then, he has reported over 1,600 security flaws. Bug hunting is, effectively, his first job.

DeVoss also started hacking as a kid, but his life has had way more twists and turns.

> *Let's not beat around the bush: the money is good if you're good.*

"At school I would finish my work in ten minutes and spend the rest of the lesson playing on the computer. I was 10 or 11 when I stumbled across a chat room whose members taught me how to hack," he told us.

"I was just a bored kid doing it for fun. I first got into trouble for it in high school and was ordered to stay away from computers, but I didn't. With others, I broke into secure government systems and was caught again and spent 4 years in prison. I was told that if I got caught again, the next time I wouldn't get out."

For him, bug bounty programs were a blessing, as he could continue with the hobby he loved while remaining on the right side of the law.

Before becoming a bug hunter, Cosmin was working as a software developer.

During that time, he and his colleagues were allowed to choose an event or course to attend for skill development. He picked a practical hacking seminar in Hamburg and there he found out about the existence of bug bounty platforms.

“Soon after I made an account. I was miserable at first, but slowly, slowly gained more experience and now I have been doing it full-time for almost 2 years,” he shared.

The pros and cons of full-time bug hunting

Let’s not beat around the bush: the money is good if you’re good.

“If someone actually works 40 hours a week and is really good, they can easily make 7 figures a year,” DeVoss opined. “I work about 10-40 hours a month right now and have brought in $903,000 last year. My highest bounty for a single bug has been about $28,000 and my highest single day payout, I believe, is around $180,000.”

There is no upper limit on how much a dedicated, full-time bug hunter can earn in a year, says Cosmin, but the final amount will depend on luck, timing and experience.

For him, though, the most important advantage of working as a bug hunter under a platform like HackerOne is the possibility of working when he wants and as much (or little) as he wants.

“This allows me to try and stay on my peak level and if I am feeling down or frustrated, I don’t persist because usually I gain nothing except more frustration,” he noted.

“Another advantage is that I can take as many vacations as I want and when I want. I can attend a live hacking event when I’m invited and meet people from all over the world.”

There are cons, as well. “You don’t have a fixed salary, so some months can be worse than others. Social isolation can be an issue. Finally, you really need to know when to stop or change your working schedule to avoid potential burnouts.”

Perhaps unsurprisingly, for De Voss one of the most important advantages of reporting vulnerabilities via bug bounty platforms is the protection they offer (meaning: they make sure the bounties are run in a way that protects the researchers legally).

Personal preferences

Each of the three hackers have predilections when it comes to bug bounty programs and vulnerabilities.

Lopez likes searching for IDOR (Insecure Direct Object Reference) bugs, mainly because it’s a type of vulnerability that is easy to find and companies pay big bounties for.

“I had the opportunity to find a lot of interesting IDORs in my career. The most interesting ones allowed me to delete any user created by the affected company or edit critical settings without authorization,” he explained.

> *“Hacking will always be a good opportunity for people that don’t want to follow a traditional corporate career path and want the flexibility that comes with the territory,” Lopez noted.good if you’re good.*

Other than that, he likes bug bounty programs that pay well and that have a wide scope to allow him to explore and research new things.

Cosmin searches mostly for improper access control bugs, misconfigurations in cloud instances, self privilege escalation flaws, information disclosure bugs or issues in the login process.

"I don't spend that much time searching for rXSS (the reflector plugin for Burp does this) and I do not search for SQL injection flaws at all. I mainly just use Burp as it fits all my needs and there are a lot of really good plugins, but I also have some custom-built tools," he noted.

DeVoss is another Burp user, and he also likes Sublist3r and dnscan.

"I spend most of my hacking time in Verizon Media because I'm most familiar with it, but I also like to check out new private bug bounty programs. My favorite bug was the one for which I received the highest single day pay out on the HackerOne platform: I was able to bypass the protections of Verizon Media's blacklist, which allowed me to redo all the bugs I'd submitted from the previous months," he shared.

The future of bug hunting

"Hacking will always be a good opportunity for people that don't want to follow a traditional corporate career path and want the flexibility that comes with the territory," Lopez noted.

"As public understanding about hacking grows, it will certainly become less niche and there will be more competition for us."

All three have noticed an increased influx of hackers on the HackerOne platform and they welcome the competition.

"I already see more professional programs, a larger attack surface and higher rewards. I also see more competition from both programs and hackers and this is a very healthy trend as it leads to the constant improvement of both sides," Cosmin said.

The fact that more and more smart things are connected to the internet and that companies building IoT devices are still not prioritizing security is creating a vast threat surface and anyone who wants to help secure it is welcome.

"I like to think the defenders will win this fight, simply because there are so many of us now," DeVoss opined, but noted that cybercrime will continue to proliferate until we start taking security more seriously.

Some final advice

Lopez pointed out that the hacking community is welcoming and supportive so following hackers on social media or joining hacking forums is a great way for aspiring ethical hackers to learn and swap ideas and information.

Still, it might be a good idea not to choose to become a full-time bug hunter from the get-go.

"First make sure you know what you are doing, as hacking has a very very steep learning curve and it is overwhelming in the beginning," Cosim advised.

"Before making the switch to a full-time bug hunting job, it's important to have at least half a year or a year of experience as a part-time bug bounty hunter. You should also be in a financially solid position or be a young person that does not have many expenses."

Is crowdsourced security really a panacea to the ills of traditional pentesting or does it create more issues?

Crowdsourced pentesting is not without its issues

AUTHOR_ Alex Haynes, CISO, CDL

Crowdsourced security isn't new anymore, having existed in one form or another as a consumable enterprise service since 2013 with the launch of the main crowdsourced platforms (HackerOne, Bugcrowd and Synack). Slowly but surely, these platforms challenged traditional pentesting practices and started to eat away at their market share. Further platforms and competitors have since launched within the crowdsourced space to compete for a part of this growing market share.

But is crowdsourced security really a panacea to the ills of traditional pentesting or does it create more issues? Before we tackle this let's cover what the issues of traditional pentesting actually are.

Development cycles and continuous delivery

For companies that utilise pentesting, it is usually a once-a-year exercise. Sadly, this doesn't keep pace with the speed of development today. Many organizations deploy weekly, daily or are in a continuous delivery methodology, constantly changing their environments and applications and hence potentially introducing vulnerabilities and configuration issues at a constant pace.

A pentest performed on this kind of environment will only produce a snapshot of a security posture at a specific point in time (the generally accepted definition of pentesting). Add to this the time it takes for a report to be drafted, go through QA and delivered to the customer (usually several weeks) and a pentesting report is out of date as soon as it's delivered to the customer. In that time the customer environment has changed multiple times and is no longer representative of what was tested in the first place.

Time-limit

A commercially imposed limitation but a very important one. Pentesters don't have the luxury of time, and tests are usually time-limited. A website engagement may typically be assigned 5 days, one day of which is reserved for report writing. This means a pentester doesn't have time to deep dive into every nook and cranny of the application and will constantly have to make decisions on what to pursue and what to ignore in the time they have allotted.

> *Pentester syndrome is making things appear worse than they actually are.*

Skillset

There is a variance in skillset, even among pentesters. Some are better at testing mobile apps, others at testing API security and web applications. Still, the technologies are so varied that you will find variations in skillset even in a small population of specialized pentesters.

Add to this the difficulties in hiring skilled staff today (a theme that's not new in infosec) and you'll often run into the problem of two different pentesters testing the same application and finding different vulnerabilities. A tactical solution to this has been to "cycle" pentesting suppliers each year but - the pentesting pool of talent being so small and specialized - I've witnessed companies ending up with the same pentester two years in a row, but now working for a different company!

Pentester syndrome

Pentester syndrome is making things appear worse than they actually are. A common practice in pentesting reports is to "talk up" issues you've found, especially if you couldn't find anything critical. This is also why no-one's ever read a pentesting report which says "everything's ok" - I've seen even informational things like a missing Strict Transport Security Header appear as a "medium" vulnerability. This generates unnecessary work chasing down "junk risk", which will remediate issues in a pentesting report, but not improve your security posture one bit.

Business model

Lastly, there's a business model disadvantage to having to keep a roster of pentesters on your payroll. You have to pay them a competitive salary, provide them with the licenses for all the equipment they need (e.g., Burpsuite Pro licenses, etc.), as well as sponsor their ongoing training

and skillset, send them to conferences and all the baggage associated with full time employees. In a workforce where there is already scarcity, this is expensive and weighs on the bottom line.

How does crowdsourced security solve these issues?

Crowdsourced business models took aim at these issues by adopting a flexible approach to pentesting. There are no dedicated pentesters but a "crowd" of volunteer security researchers that sign up and attempt to find vulnerabilities in an asset. If they find one, they are paid. If they find nothing, they are paid nothing.

> *Crowdsourced security tests aren't suited to testing inside a company perimeter.*

The first problem this solves is the "time-limited" aspect of pentesting. No longer do you have just 5 days to try and pick at an application – crowdsourced pentests are typically open-ended, meaning you can spend weeks if not months hunting down elusive, critical vulnerabilities, and this has played out to great effect.

I have my own personal experience with this: as part of a crowdsourced program I once found a critical vulnerability in a multi-billion dollar, Nasdaq-listed company after looking for vulnerabilities for several weeks. This vulnerability allowed the total ownership of all 100 million + customer details (effectively owning all their data). Due to the complexity of the vulnerability, there was no chance any pentester would have had the time to investigate this properly (they relied on traditional pentests in the past, which proved this point).

The second problem about continuous delivery and point-in-time tests is also remediated by this open-ended approach and by having researchers dip in and out of the programs. This has its own issues, which I'll get into later, but also ensures that despite a constantly changing infrastructure, it is constantly being tested (providing you have a wide and deep enough pool of researchers to draw from).

This leads to the third pentesting issue – skillset and business model. Crowdsourced companies have a huge business model advantage in not having full-time employees. They don't pay them a salary or even need to pay their material costs. To compensate for skillset issues, they just throw as many bodies at an application as possible, and this will cover all known profiles of the technology stack by sheer numbers. The more eyeballs you have looking at something, the more issues you will find.

Finally, the pentester syndrome issue is resolved by the reward system. If you submit an issue that isn't really a vulnerability and you don't provide a proof of concept, then it's ignored. Worse, your profile will have points deducted for wasting time and/or (in extreme scenarios) be kicked off the platform entirely. The customer gets only actionable vulnerabilities with exploits, not pentesting reports filled with junk risk.

The issues with crowdsourced security today

Taking the above into account, crowdsourced security is not a like-for-like replacement for pentesting today. It still has many issues, some of them intractable due to their business model.

> *Crowdsourced security, while alleviating this somewhat by expanding the potential pool of testers to an international level, has still hit a brick wall, as there is no endless pool of talent to draw from.*

Internal vs external testing

Crowdsourced security tests aren't suited to testing inside a company perimeter. In a pentest, a consultant physically turns up to the organization's premises and just plugs his laptop in to begin his tests. In a crowdsourced scenario this isn't possible since it requires a complex mixtures of VPNs and/or proxies to be set up, and the network has to be able to maintain the load of dozens if not hundreds of users testing at once. This is why the majority of crowdsourced engagements so far have been for web applications, since these can be accessed from anywhere with relatively little cost or complexity.

This extends to any physical testing or testing of IoT devices. While I have participated in crowdsourced engagements where you were sent a physical item (a fitness track for example), this requires investment since every tester involved requires a copy. Add to this that testers are spread out all over the globe and your upfront costs can quickly spiral before you've even started the test.

The resource pool is finite

Offensive security suffers from a skills shortage just like every other facet of the information security workforce today. Crowdsourced security, while alleviating this somewhat by expanding the potential pool of testers to an international level, has still hit a brick wall, as there is no endless pool of talent to draw from.

Visit the leaderboard of the main crowdsourced platforms and you'll find one striking similarity – they're almost the same. The majority of the testing on all platforms is done by a select group of super-researchers, some of which do it full time. This means the majority of vulnerabilities are actually handled by the same group each time.

While you may read marketing references to having "thousands" of researchers, the reality is that two dozen researchers account for most of the vulnerabilities found on platforms today. This creates a resource problem where crowdsourced companies, many backed by venture capital, require constant growth, and so more customers, and therefore more programs are open for testing.

These programs need a corresponding growth in testers, which just isn't there. Everyone today who wants to participate in a crowdsourced pentest is already doing it. As it's entirely voluntary, you can see the problem this causes – you cannot force a voluntary workforce to test your new asset when they simply don't have the bandwidth to do it.

Cost

Despite what crowdsourced security companies say, crowdsourced pentesting is not cheap by any standard. A pentest for an external website today will set you back the number of days, multiplied by the daily rate of the consultant.

Despite what crowdsourced security companies say, crowdsourced pentesting is not cheap by any standard. A pentest for an external website today will set you back the number of days, multiplied by the daily rate of the consultant.

Let's take an average and say this is $1200 USD (this can be more or less depending on the pentesting company). For a five day pentest (common for a website) this gives you an average of $6000 USD to test an asset. To get a crowdsourced test first you need a platform fee which is many times that - the fee to actually advertize your pentest on the various crowdsourced platforms. Add to this that you also have to pay out a reward for every vulnerability

that's found so the more vulnerabilities that are discovered the more you pay out, and this means your costs can quickly spiral out of control.

The gig economy today is more commonly associated with the likes of Uber and Deliveroo - workers forego traditional benefits like pensions and sick pay to choose when and how much they work.

A couple of caveats here: Synack's (one of the platforms) approach is slightly differently - they only charge a platform fee and all reward payouts are from their own pocket. This cost premium effectively rules out crowdsourced testing for smaller companies due to the barriers for entry being so high.

Federacy is, for now, the only alternative for small/medium businesses. They cater to them by lowering the platform and payouts, but the problem is that the lower the payouts, the less researchers will be attracted to the plaftom.

The gig economy

Need a copy of Burp Suite Pro? You need to buy the license yourself. You're sick? Too bad. Pension? What's that?

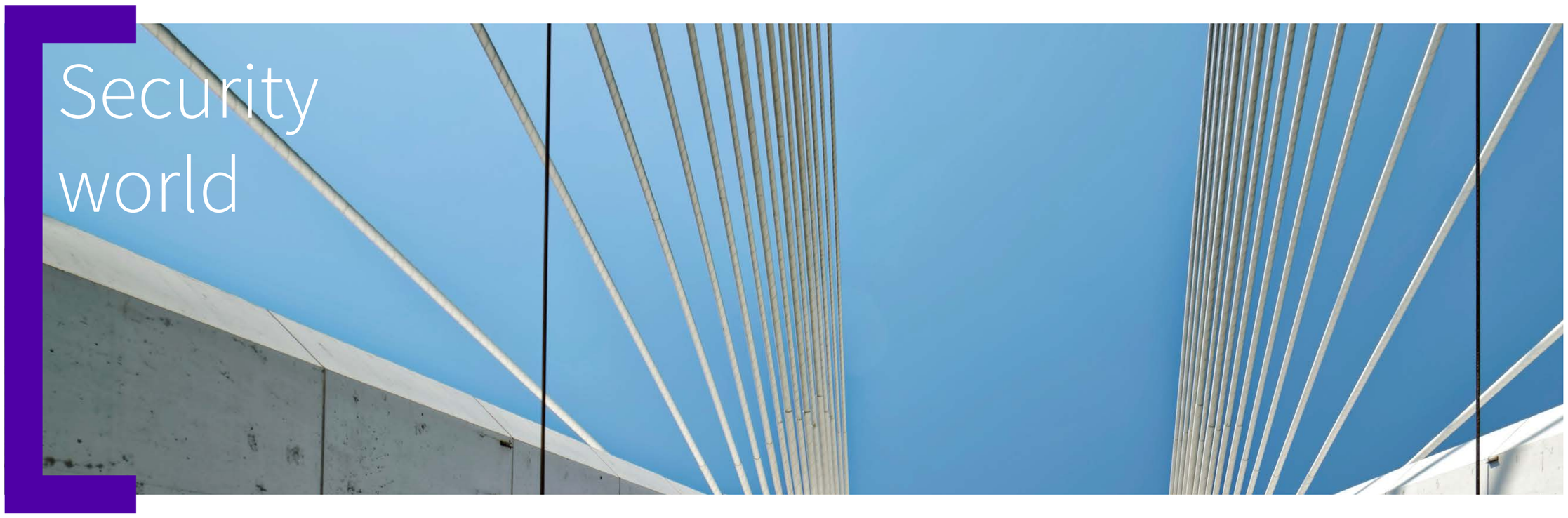
Probably the most insidious issue is that crowdsourced security effectively propagates an Orwellian version of the gig economy. The gig economy today is more commonly associated with the likes of Uber and Deliveroo - workers forego traditional benefits like pensions and sick pay to choose when and how much they work.

There is one crucial difference though: gig economy workers are actually paid for their labor. If you choose to work as an uber driver for 10 hours, you will be able to calculate a certain amount of take-home pay. Security researchers engaged in crowdsourced pentesting are not paid for the work, but per found vulnerability, and they can easily spend a day searching for vulnerabilities and find nothing. Finding no vulnerabilities is actually the default result for most security researchers today, and you are paid absolutely nothing for your time.

Not only this, but all the tools you use you must procure yourself. Need a jailbroken iPhone to test that mobile app? You need to provide it yourself. Need a copy of Burp Suite Pro? You need to buy the license yourself. You're sick? Too bad. Pension? What's that? This has huge costs savings for crowdsourced security companies since they effectively solve the business model issue pentesting companies struggle with, but introduce exploitation of a workforce as a result.

To conclude, note that both approaches can be complementary, despite their myriad of issues. There is no one solution for offensive security testing, and it's up to you decide which fits your environment best while keeping the above issues in mind.

Security world



Only 36% of critical infrastructures have a high level of cyber resilience

Greenbone Networks revealed the findings of a research assessing critical infrastructure providers' ability to operate during or in the wake of a cyberattack.

The research investigated the cyber resilience of organizations operating in the energy, finance, health, telecommunications, transport and water industries, located in the UK, US, Germany, France and Japan. Of the 370 companies surveyed, only 36 percent had achieved a high level of cyber resilience.

To benchmark the cyber resilience of these critical infrastructures, the researchers assessed a number of criteria. These included their ability to manage a major cyberattack, their ability to mitigate the impact of an attack, whether they had the necessary skills to recover after an incident, as well as their best practices, policies and corporate culture.

Infrastructure providers in the US were the most likely to score highly, with 50 percent of companies considered highly resilient. In Europe, the figure was lower at 36 percent. In Japan, is was just 22 percent.

Identity-related breaches on the rise, prevention still a work in progress

The number of workforce identities in the enterprise is growing dramatically, largely driven by DevOps, automation, and an increase in enterprise connected devices, which will only continue to accelerate identity growth, an IDSA survey of 502 IT security and identity decision makers has shown.

At the same time, compromised identities remain one of the leading causes of a data breach. According to the study, the vast majority of IT security and identity professionals have experienced an identity-related breach at their company within the past two years, with nearly all of them reporting that they believe these breaches were preventable.

"When approaching identity security, professionals must first consider a range of desired outcomes, or results they want to achieve, and then chart their paths accordingly," said Julie Smith, executive director of the IDSA.

Shifting responsibility is causing uncertainty and more security breaches

Data security is creating fear and trust issues for IT professionals, according to a new Oracle and KPMG report.

The study of 750 cybersecurity and IT professionals across the globe found that a patchwork approach to data security, misconfigured services and confusion around new cloud security models has created a crisis of confidence that will only be fixed by organizations making security part of the culture of their business.

Demonstrating the fear and trust issues experienced by IT professionals, the study found that IT professionals are more concerned about the security of their company's data than the security of their own home.

Eye-opening statistics about open source security, license compliance, and code quality risk

99% of commercial codebases contain at least one open source component, with open source comprising 70% of the code overall, according to Synopsys.

More notable is the continued widespread use of aging or abandoned open source components, with 91% of the codebases containing components that either were more than four years out of date or had seen no development activity in the last two years.

The most concerning trend in this year's analysis is the mounting security risk posed by unmanaged open source, with 75% of audited codebases containing open source components with known security vulnerabilities, up from 60% the previous year. Similarly, nearly half (49%) of the codebases contained high-risk vulnerabilities, compared to 40% just 12 months prior.

COVID-19 is driving diverging perspectives as enterprises decide which technologies to focus on

TACTICAL CHANGES	USA	CHINA
Re-skilling	84%	79%
Accelerating new business models	83%	89%
More agile app development	82%	86%
Refocus around customers	82%	89%
Real-time data and feedback	80%	89%
Changing the way we design apps	75%	88%
Getting more DX focus	71%	85%
How to look at 5G as an accelerator	69%	85%

With COVID-19–related challenges creating new pressures, enterprises are rapidly falling into the categories of simply surviving, pivoting to adapt to new realities, or doing nothing, Wind River has revealed.

While the U.S. and China are in different phases of the pandemic, in several aspects the responses from each country split in similar ways. More than 1 in 3 executives—39% of U.S. and 43% of Chinese leaders—are focusing on surviving this crisis, while 35% in the U.S. and 33% in China are spurred to make a transformation due to COVID-19.

The enterprises focused on transforming have a much higher propensity to accelerate key technology investments compared to those who are merely surviving. Those with a desire to digitally transform are placing 50%+ extra focus on key investment areas such as 5G, containers, and cloud native.

With the threat landscape continuously changing, businesses must be ready for anything

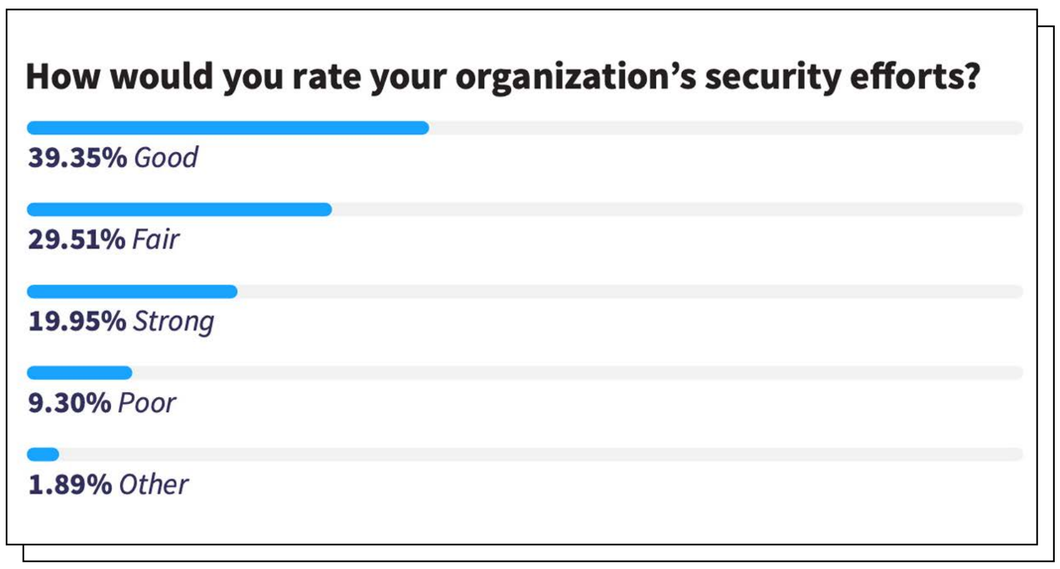
Despite efforts by organizations to layer up their cyber defenses, the threat landscape is changing, attackers are innovating and automating their attacks, NTT reveals.

Referencing the COVID-19 pandemic, the report highlights the challenges that businesses face as cyber criminals look to gain from the global crisis and the importance of secure-by-design and cyber-resilience.

The attack data indicates that 55% of all attacks in 2019 were a combination of web-application and application-specific attacks, up from 32% the year before, while 20% of attacks targeted CMS suites and more than 28% targeted technologies that support websites.

Organizations that are relying more on their web presence during COVID-19, such as customer portals, retail sites, and supported web applications, risk exposing themselves through systems and applications that cyber criminals are already targeting heavily.

With increased DevOps adoption, roles in software development teams are changing



Roles across software development teams have changed as more teams adopt DevOps, according to GitLab.

The survey of over 3,650 respondents from 21 countries worldwide found that rising rates of DevOps adoption and implementation of new tools has led to sweeping changes in job functions, tool choices and organization charts within developer, security and operations teams.

“This year’s Global DevSecOps Survey shows that there are more successful DevOps practitioners than ever before and they report dramatically faster release times, truly continuous integration/deployment, and progress made toward shifting both test and security left,” said Sid Sijbrandij, CEO at GitLab. “That said, there is still significant work to be done, particularly in the areas of testing and security. We look forward to seeing improvements in collaboration and testing across teams as they adjust to utilizing new technologies and job roles become more fluid.”

CEOs and CISOs disagree on cyber strategies

There are growing disparities in how CEOs and CISOs view the most effective cybersecurity path forward, according to Forcepoint.

The global survey of 200 CEOs and CISOs from across industries including healthcare, finance and retail, among others, uncovered prominent cybersecurity stressors and areas of disconnect for business and security leaders, including the lack of an ongoing cybersecurity strategy for less than half of all CEO respondents.

The research also identified disparities between geographic regions on data protection as well as a digital transformation dichotomy battle between increased risk and increased technology capability.

Key findings:

- Most leaders (76%) are losing sleep over the prospect of becoming the next headline-grabbing security breach
- This is despite a high percentage (87%) believing that their security team is consistently ahead of cybersecurity threats
- This disparity is compounded by a belief that senior leadership is cyber-aware and data-literate (89%) and focused on cybersecurity as a top organizational priority (93%)
- Cybersecurity strategies are seen by 85% of executives as a major driver for digital transformation, yet 66% recognize the increased organizational exposure to cyber threats because of digitization
- Only 46% of leaders regularly review their cybersecurity strategies

Unexpected downtime is crippling businesses, causing revenue losses

Unexpected downtime is a major challenge for SMBs today. The IT systems of nearly a quarter of SMBs have gone offline in the past year, according to a research from Infrascale.

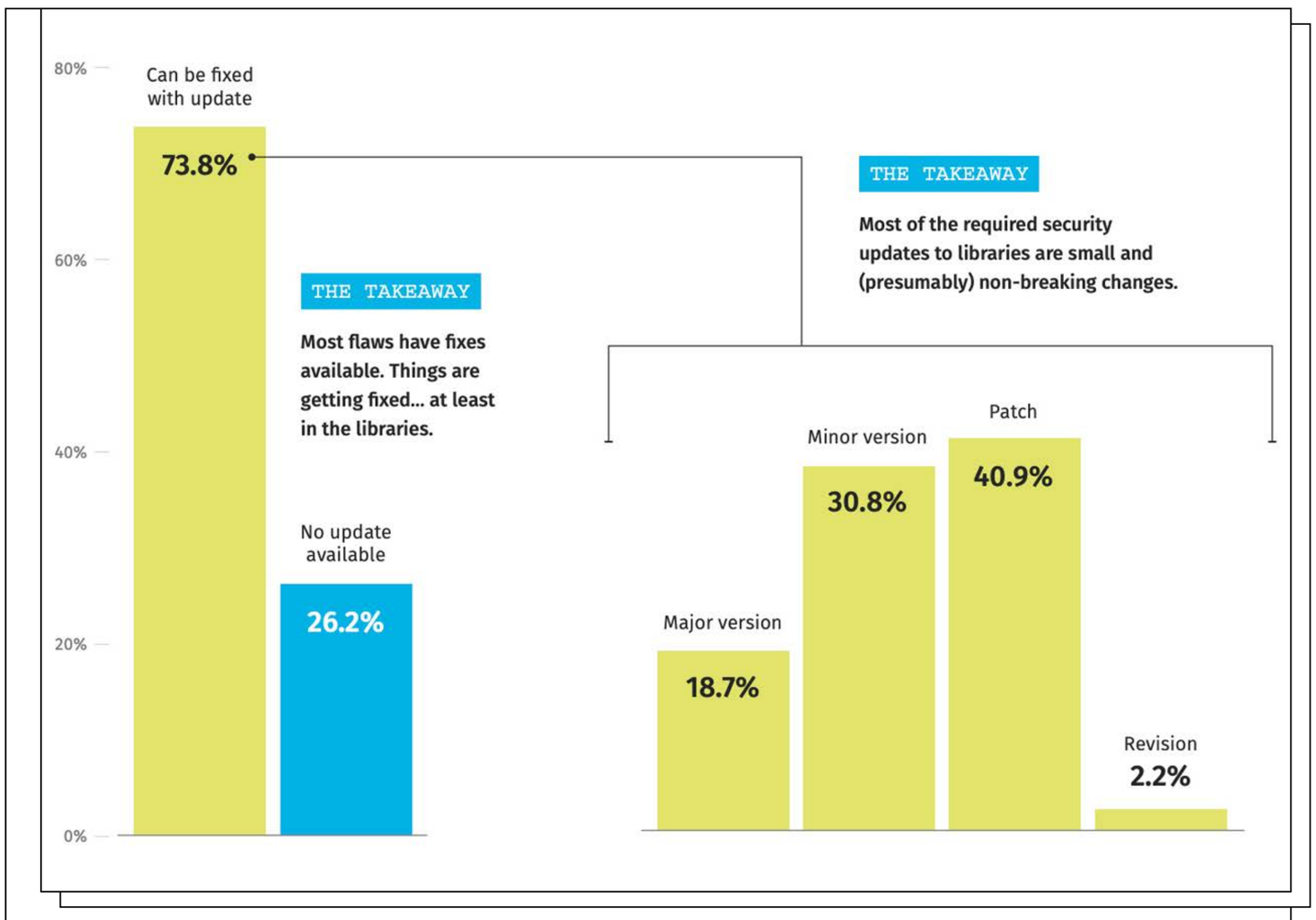
SMBs said the downtime creates business disruption and decreases employee productivity. 37% of SMBs in the survey group said they have lost customers and 17% have lost revenue due to downtime.

“Customer retention is essential for business success,” said Russell P. Reeder, CEO of Infrascale. “It can cost up to five times more to attract a new customer than to retain an existing one, and when customers leave, businesses lose out on vital profit and operational efficiencies. Especially in today’s competitive environment, it’s challenging enough to retain customers. With all the cost-effective solutions available, downtime shouldn’t be a reason for concern.”

19% of SMBs admit that they do not feel their businesses are adequately prepared to address and prevent unexpected downtime. Of those SMBs that said they feel unprepared for unexpected downtime, 13% said they do not feel their business is prepared for unexpected downtime because they have limited time to research solutions to prevent downtime.

28% attributed not feeling prepared for unexpected downtime due to IT teams at their organization being stretched. The same share (28%) said they don’t think their business is at risk from unexpected downtime. Yet 38% of SMBs said they don’t know what the cost of one hour of downtime is for their businesses.

The research is based on a survey of more than 500 C-level executives at SMBs. CEOs represented 87% of the group. Most of the remainder was split between CIOs and CTOs.



How secure are open source libraries?

Seven in 10 applications have a security flaw in an open source library, highlighting how use of open source can introduce flaws, increase risk, and add to security debt, a Veracode research has revealed.

Nearly all modern applications, including those sold commercially, are built using some open source components. A single flaw in one library can cascade to all applications that leverage that code.

According to Chris Eng, Chief Research Officer at Veracode, “Open source software has a surprising variety of flaws. An application’s attack surface is not limited to its own code and the code of explicitly included libraries, because those libraries have their own dependencies.”

Most flawed libraries end up in code indirectly: 47% of those flawed libraries in applications are transitive – in other words, not pulled in directly by developers, but are being pulled in by upstream libraries. Library-introduced flaws in most applications can be fixed with only a minor version update; major library upgrades are not usually required.

Businesses vulnerable to emerging risks have a gap in their insurance coverage

The majority of business decision makers are insured against traditional cyber risks, such as breaches of personal information, but most were vulnerable to emerging risks, such as malware and ransomware, revealing a potential insurance coverage gap, according to the Hanover Insurance Group.

Most businesses surveyed indicated they had purchased cyber insurance, and more than 70% reported purchasing a policy on the recommendation of an independent insurance agent.

Purchasing decisions also were heavily influenced by media coverage and prior attack experience. Nearly 90% of study respondents reported experiencing a cyberattack during the past year and recognized a cyberattack could have a disastrous impact on their businesses.

CISOs today have the opportunity to help enable the organization to grow by delivering a digital experience that delights customers while mitigating digital risk. This requires the CISO to advise the business about when and where cyber risks could manifest

Changing the mindset of the CISO: From enforcer to enabler

AUTHOR_ Michael Greene, CEO, Enzoic

With digital transformation investments expected to reach a staggering $7.4T before 2023, organizations realize that they must disrupt their markets or risk being disrupted themselves. However, with digital transformation comes a multitude of cybersecurity-related challenges to overcome, and it's up to the CISO to help businesses navigate the associated risks.

Security leaders can no longer adopt the role of enforcer, but rather need to pivot to a new role: the enabler. CISOs today have the opportunity to

help enable the organization to grow by delivering a digital experience that delights customers while mitigating digital risk. This requires the CISO to advise the business about when and where cyber risks could manifest. Security leaders must now be able to transform their security practices in lockstep with all the other changes wrought by business-wide digital transformation.

The successful CISO must collaborate with the business and find a way to balance the appropriate controls for any given scenario in order to maximize protection and minimize security friction.

Today's CISO needs to be able to provide advice to the business to help it understand the risk landscape so that it can then make informed decisions about which risks are tolerable and which ones to avoid at all costs. In addition to providing this counsel, security leaders must be able to implement the technology to mitigate risks and protect the business as it continues on the path to digitally transform.

As part of this change in mindset, security leadership needs to take into account the impact of friction on the user experience as it can "break or make" security initiatives. The CISO must now focus on reducing unnecessary friction where appropriate in support of digital transformation objectives.

How to reduce security friction

As a rule, security friction increases or decreases proportionally to the severity of security restrictions put in place. The successful CISO must collaborate with the business and find a way to balance the appropriate controls for any given scenario in order to maximize protection and minimize security friction.

To achieve this balance, the CISO needs to home in on these seven variables:

1_How much is at risk if no controls are in place?
2_How could controls interrupt revenue streams?
3_Could the aggravation of the control cost the company many customers?
4_Must the business stop using or restrict innovative business processes or technology for the controls to work?
5_Will the level of friction from controls cause a revolt among users that could hamper implementation or induce unsafe workarounds?
6_How much will controls slow down technology delivery or innovation?
7_Are there any other alternative controls that could offer significantly less friction without compromising all of the risk reduction benefits?

By reviewing this checklist, CISOs will be able to advise the business of the different options available and, most critically, the path forward to mitigate risk and minimize friction. Security leaders need to outline the options available that will help reduce risk in the context of the business operating environment.

The successful CISO in the digital era needs to help the business understand all the different variables. To achieve this requires a mindset shift from that of an enforcer to that of a collaborative and flexible partner. Security teams need to recognize that they now provide a valuable service to the business in the quest to mitigate digital risk and minimize security friction.

Here are three examples of ways to achieve this balance in a digital-first world.

Payment processing

Online and mobile transactions are increasingly becoming the lifeblood of commerce for every type

of organization, and digital transformation spurs this on further. While fraud protection is essential, transaction speed is tantamount. Effective security teams are managing that through behavioral indicators that increase security measures based on risky behavior. That paired with compromised credential screening during authentication can generally keep friction low for the average transaction, while at the same time mitigating the risk of account takeover and the corresponding associated financial costs and impact on reputation.

Security leaders reduce friction here by tailoring the controls to the development process rather than making developers jump through multiple time-consuming security hoops.

Software supply chain

Software development teams increasingly depend upon third-party code and open source libraries to quickly develop software. This underpins the DevOps and Agile practices that fuel the rapid software delivery necessary for digital transformation. But third-party code also accelerates the introduction of new vulnerabilities into enterprise software.

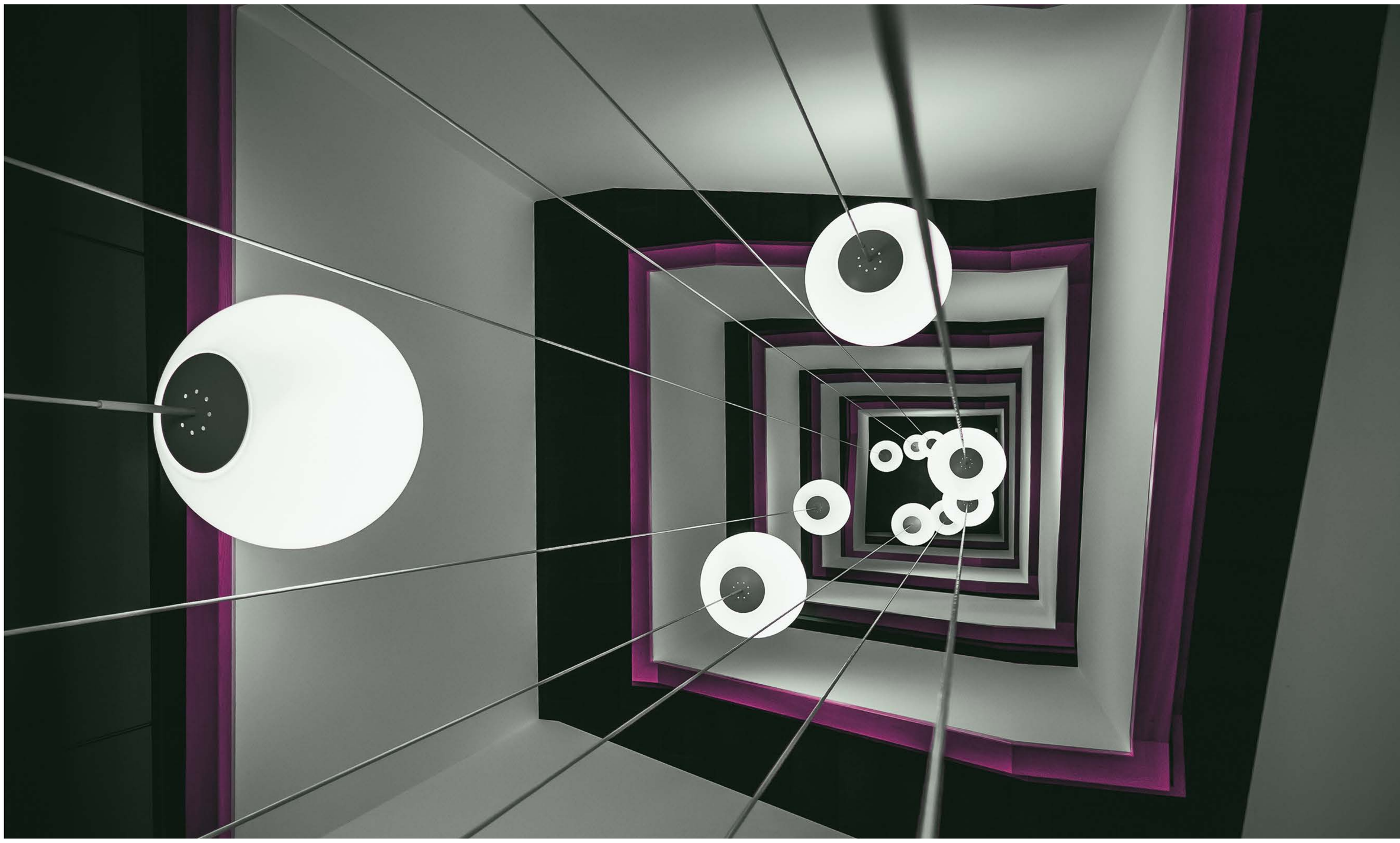
Rather than banning the use of the transformative practice of leaning on third-party code, successful security teams are finding ways to track and manage the use of these tools while making it easier for developers to source them. Security leaders reduce friction here by tailoring the controls to the development process rather than making developers jump through multiple time-consuming security hoops.

Data sharing

The most impactful frictionless security efforts are those that smooth ease of access and integration.

Data sharing through cloud services and API connections between applications is crucial to digital transformation efforts. So many innovations today rest on complex digital ecosystems and integrations. The most impactful frictionless security efforts are those that smooth ease of access and integration. At the business user level, that means allowing the use of common platforms such as Box, while increasingly tying data access policies and visibility into data use to identities and roles. At the application level, it means designing security mechanisms and APIs that work seamlessly in an ecosystem and help facilitate data controls. The security tools must work without breaking integrations or degrading service levels.

Digital transformation is changing every aspect of how we operate, including the role of the CISO. The successful CISO in the 2020s and beyond needs to take a risk-based approach that consistently views security reasoning through the lens of user experience, business profitability, and viability.



Mobile device use continues to grow, while an increasingly mobile and remote workforce depends heavily on laptops. To secure those devices, organizations need to implement client-side security controls.

What happens when one of your users forgets their full disk encryption passphrase, or if this hasn't been set up, simply plugs in new hardware that triggers a BitLocker Recovery Mode?

Review: Specops Key Recovery

AUTHOR_Tonimir Kisasondi, Founder, Oru

One of the more pressing risks linked to the use of mobile devices is the possibility of device loss or theft. If a device is lost, sensitive data (e.g., documents, account passwords) might get extracted and exposed.

One solution for this problem is full disk encryption, and one of the most popular systems is

Microsoft BitLocker, which is part of every Windows 10 installation.

What happens when one of your users forgets their full disk encryption passphrase, or if this hasn't been set up, simply plugs in new hardware that triggers a BitLocker Recovery Mode? If your organization uses Microsoft Active Directory and has set up the environment to store the recovery keys in AD, a system administrator can restore that machine.

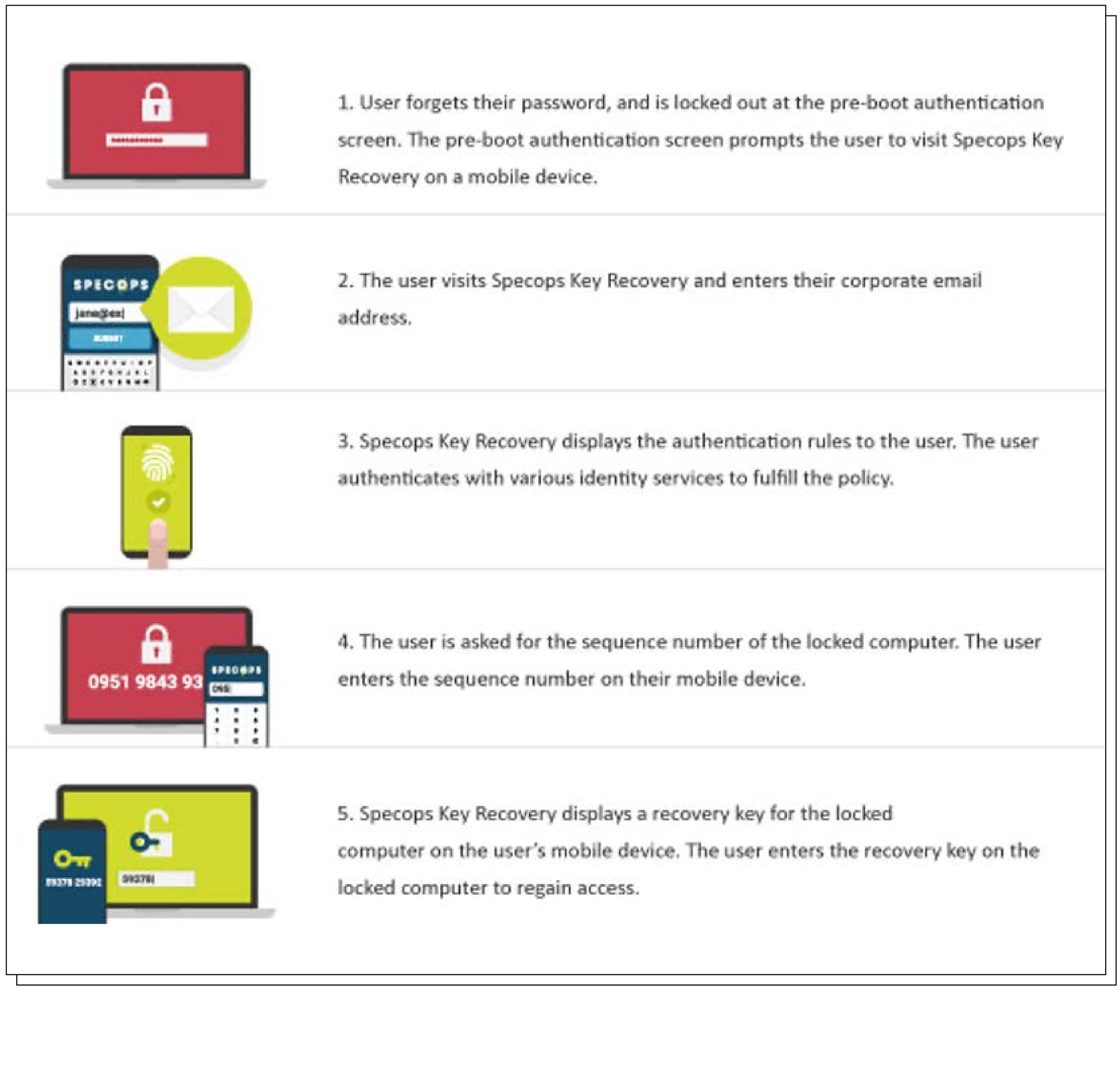
Of course, the user will still need to contact their organization's helpdesk, which will need to verify their identity in order to share the recovery key. Common problems with this scenario are issues with verifying the identity of the user and increased workload for the system administrators/helpdesk personnel.

Introducing Specops Key Recovery

Specops Software realized these problems and offers an interesting solution: Specops Key Recovery, a self-service tool for recovering BitLocker recovery keys.

Instead of contacting the helpdesk, which needs a way to verify the identity of a person over the phone (a hard problem to solve with high confidence given the lack of physical presence), Specops Key Recovery offers a cloud centric self-service portal.

An infographic from Specops illustrates the concept:



The user's perspective (enrollment)

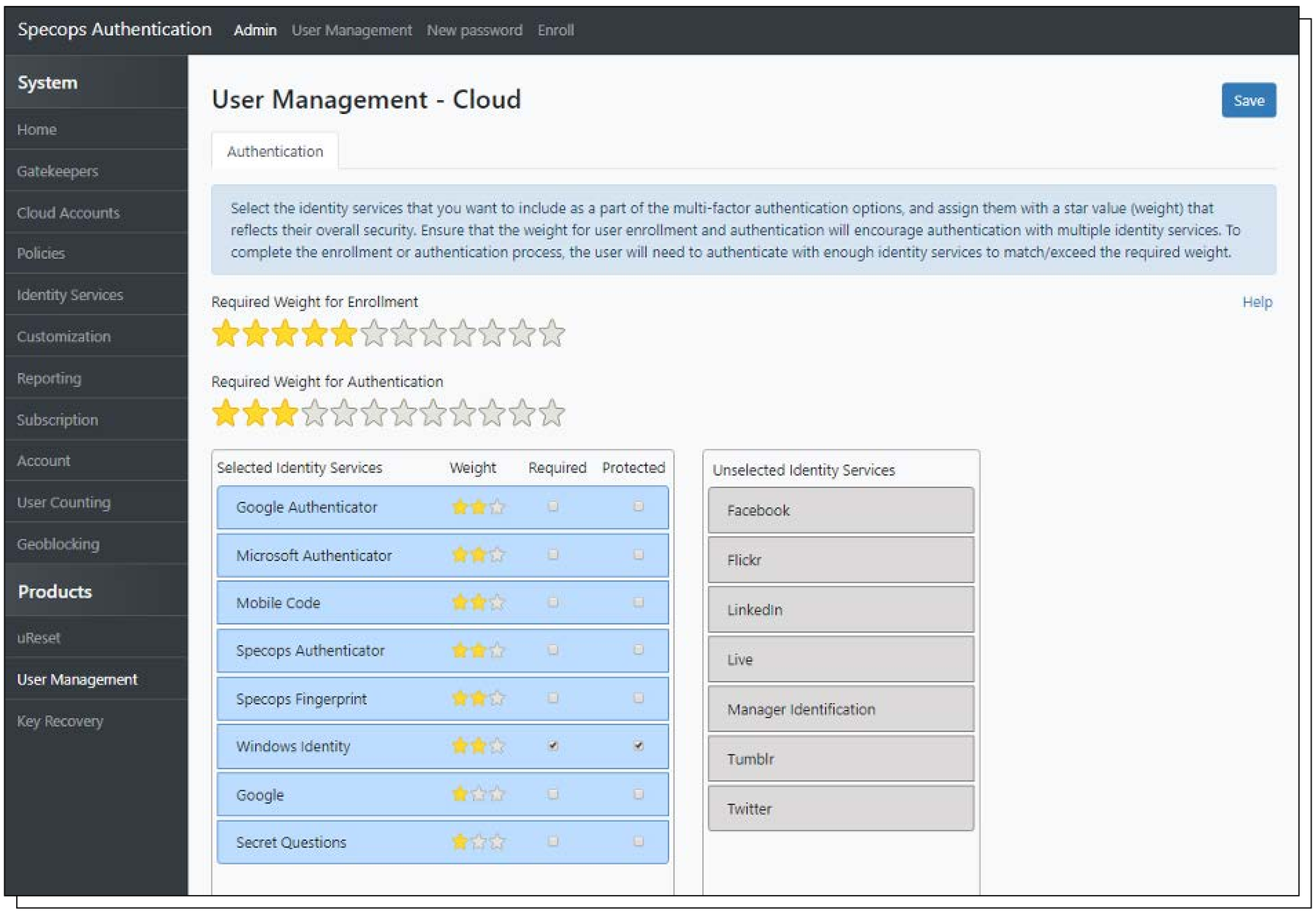
The user enrolls or can be pre-enrolled into the service. Pre-enrollment is achieved when an administrator selects identity services that leverage existing Active Directory details. When a user is pre-enrolled this means that he/she does not have to enroll but rather when a lock out occurs can utilize the system to authenticate identity and retrieve a recovery key.

However, it's best practice to extend additional identity services to users to minimize failure for example if an identity service is unavailable. Enrollment will require the user to successfully login and enroll with any combination of identity services extended to them by their system admin. The solution supports a number of identity services that can serve as multi-factor authentication options, depending on the authentication policy set by the administrator. These include:

a. SMS (mobile code)
b. Windows Identity
c. Authenticators: Google, Microsoft, Specops
d. Service logins: Google, Facebook, LinkedIn, Live, Tumblr, Twitter
e. Other: Specops Fingerprint, Secret questions, Manager Identification

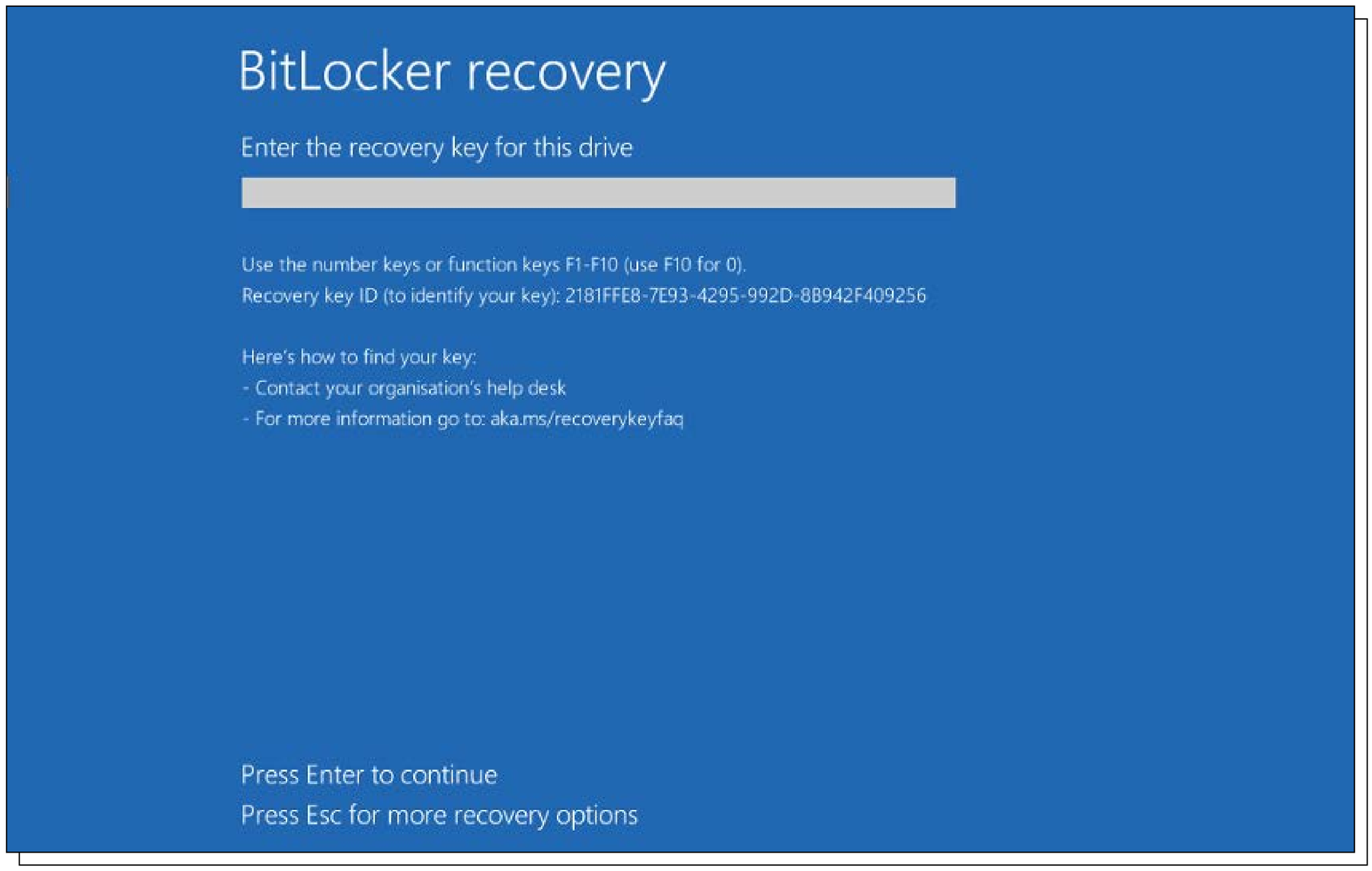
Administrators can vary the enrollment policy from the authentication policy to ensure that users have additional options when authenticating. Each service can be assigned a security weight reflected by stars. This depicts the security assurance level assigned to each service for example the screenshot below depicts Mobile Code as having a weight of two stars versus Security Questions which has a weight of one. Weights ensure that users are provided with options but that the alternatives are not sacrificing security as the required authentication weight will still have to be satisfied.

This screenshot of the administration interface illustrates the choices/flexibility:

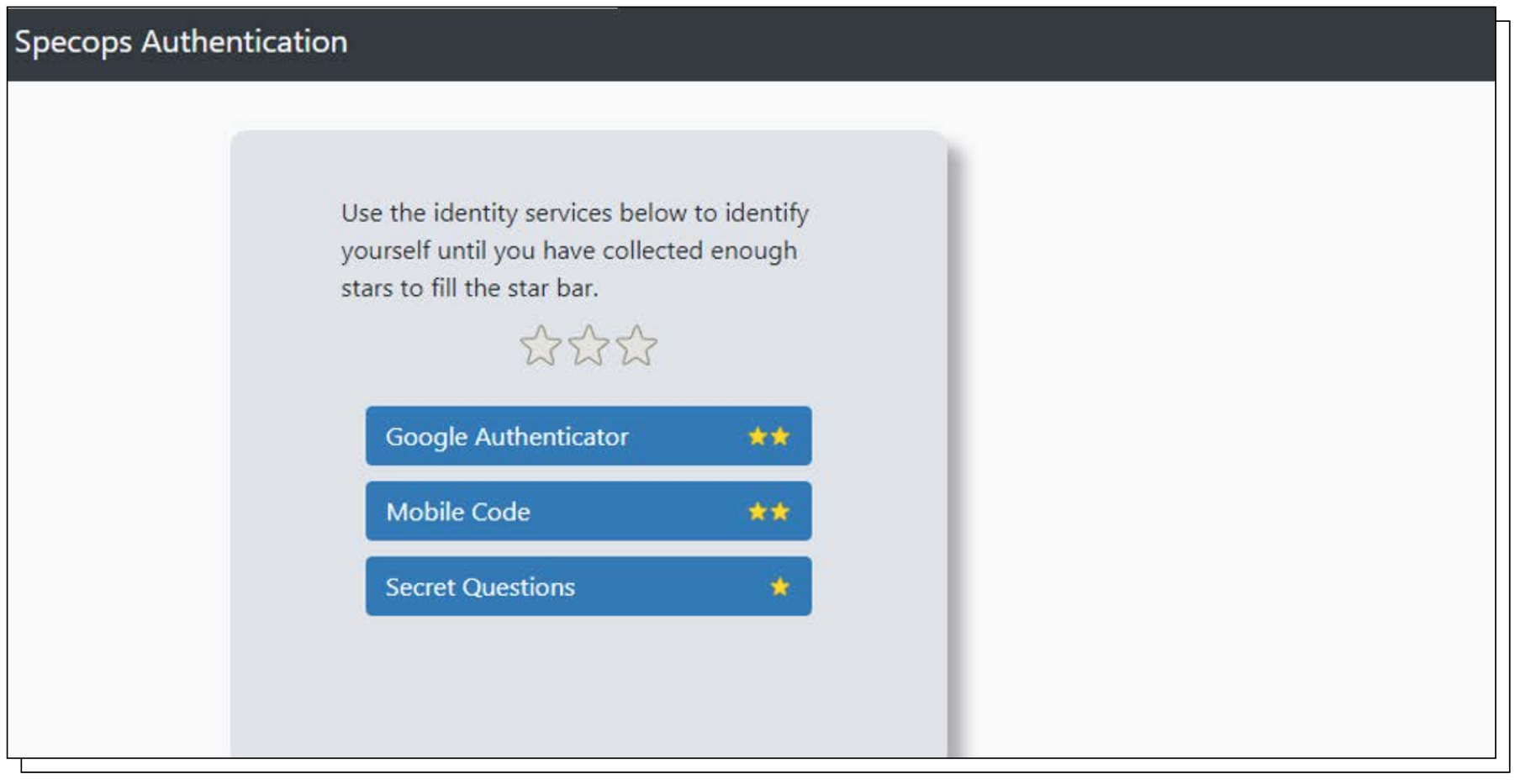


The user's perspective (use)

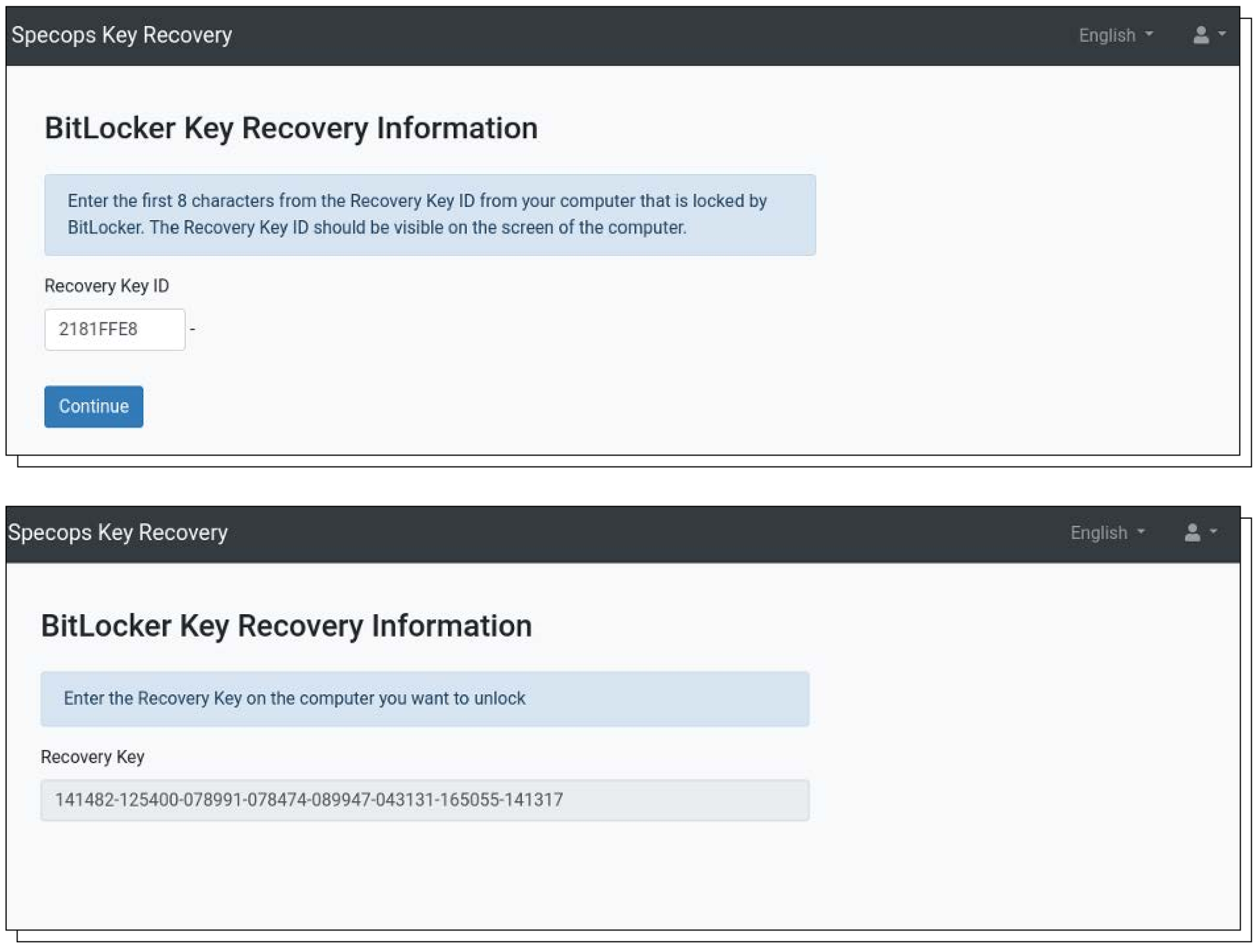
In the event of an encryption lock out, users are greeted with the infamous BitLocker Recovery screen:



Specops Key Recovery makes it possible for the user to visit a self-service portal via another device (e.g., a mobile phone) and verify their identity using a number of authentication factors provided by the previously enrolled identity services.



After proving their identity, they can enter the first 8 characters from the recovery key ID, press “Continue” and get the Bitlocker recovery key:



So, in a nutshell: enrolled users can recover access to their machine without having to ask the helpdesk for assistance. This is a cost savings but at the same time does not sacrifice security as users have to verify their identity before recovering access. This is what Specops Key Recovery does very well.

The sysadmin’s perspective (installation, setup, management)

To operate Specops Key Recovery, a sysadmin needs to set up multiple elements:

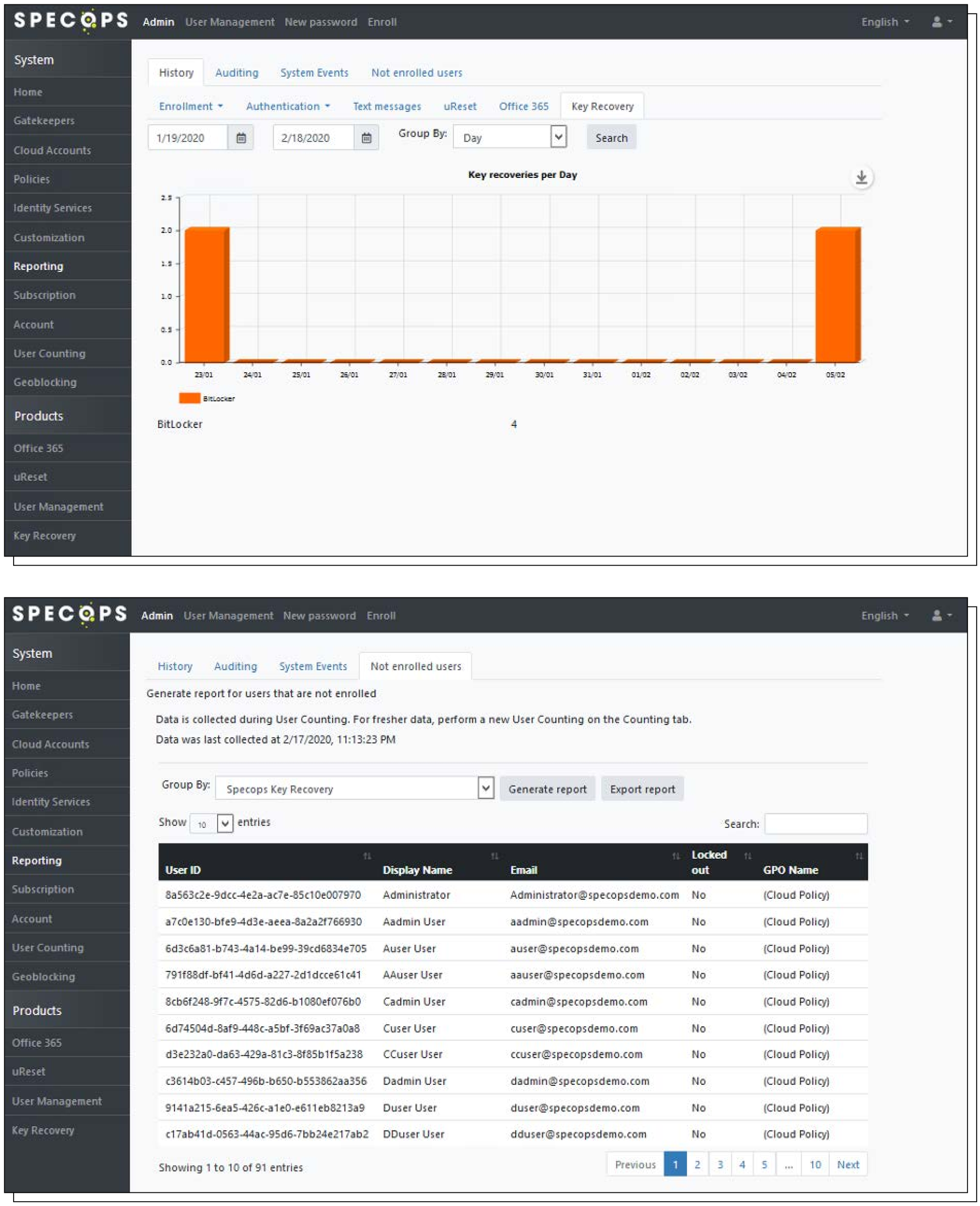
1_Register an account on the Specops cloud service.

2_Install the Specops Authentication Gatekeeper Administration tool on their Domain Controller (DC).

3_Set up the group policy to store the recovery passwords and key packages in the Active Directory Domain Services (AD DS).

4_Configure the service according to their required policies.

We particularly liked the fact that during account registration Specops Key Recovery insists on enabling 2-factor authentication (2FA). It’s SMS-based 2FA, but that’s still better than no 2FA, and you can swap it with something else later on. It’s also great that the system checks for common blacklisted passwords, adds a reCAPTCHA to curb automated attacks (which can be enforced or disabled), and has a default level logging and reports.



Customers will appreciate the fact that the web interface can be customized and the self-service portal can be integrated with the specific visual style of an organization.

The cloud user management component is the solutions service desk. It allows the IT helpdesk to verify users' identities using the same MFA factors they enrolled with before performing sensitive tasks such as recovering keys or resetting passwords. The interface also presents helpdesk users with details such as enrollment and authentication information. For example:

testuser

User info | Enrollment | Password info | Key Recovery | User identification | Reset password | History | Unlock Computer

Symantec Endpoint Encryption	
Enabled	No

BitLocker	
Enabled	Yes

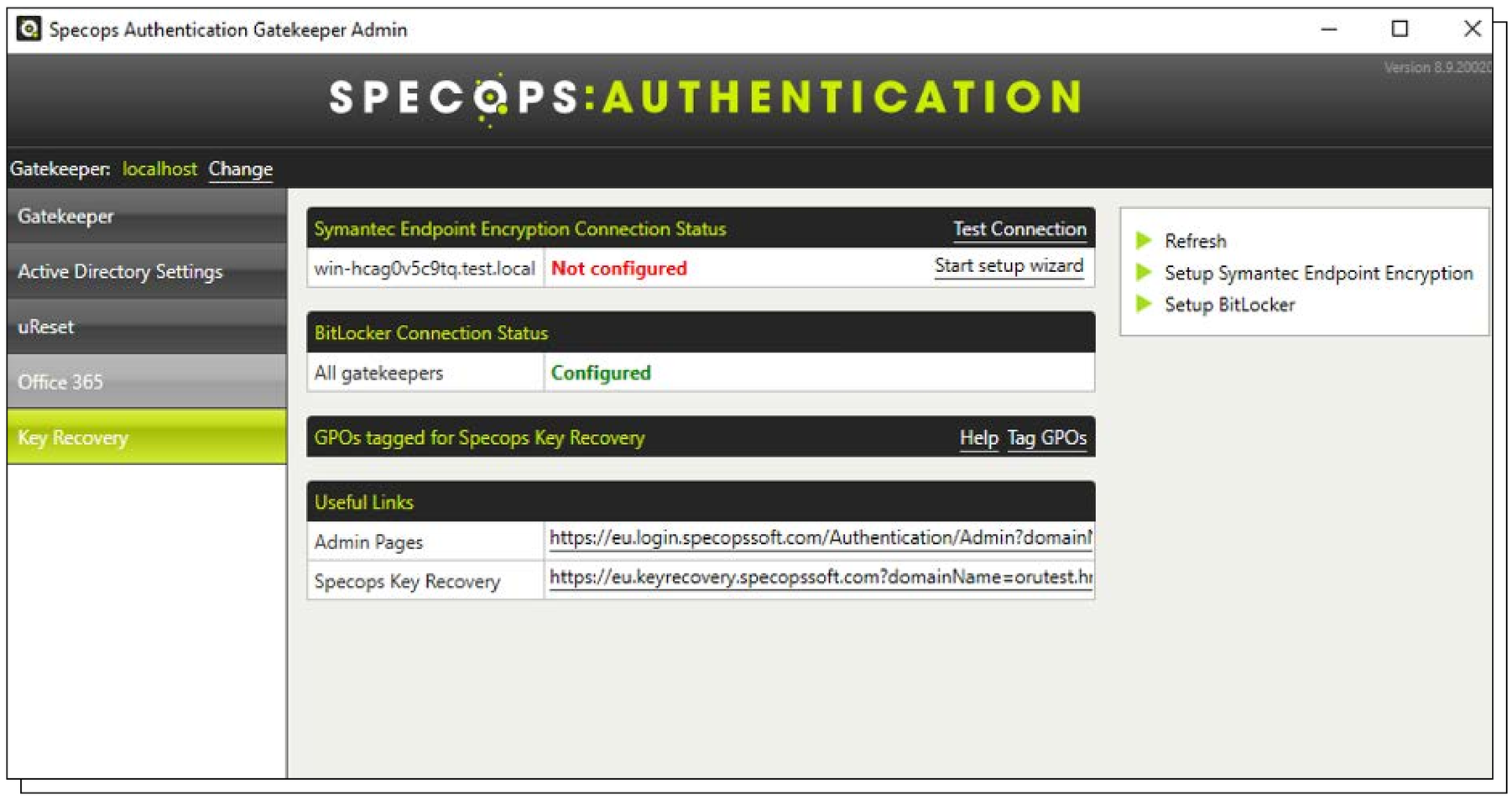
Enrollment Information	
Affected by authentication policy	Yes
Enrolled with authentication policy	Yes
Required number of stars	★★★★★
Current number of stars	★★★★★
Affected by Default Cloud Policy	Yes

Not Enrolled Identity Services	
Specops Authenticator	★★
Microsoft Authenticator	★★
Google	★
Specops Fingerprint	★★

Enrolled Identity Services	
Google Authenticator	★★
Secret Questions	★
Mobile Code	★★

From the AD-tooling side of things, installation is straightforward and the documentation covers the entire process in enough detail that any junior system administrator could set the system up.

If we really wanted to nitpick, we could suggest that the documentation or the tool itself could help admins set up the group policy to store the recovery passwords and key packages in the AD DS.



Final verdict

If you have a large, distributed and remote workforce, you will benefit from the increased security and convenience offered by the solution. Although we only illustrated the key recovery option, the Specops Authentication platform also offers additional account management features like password reset, change, and account unlocking – all utilizing the same multi-factor authentication engine. One important feature that stands out for those with a global workforce is geo-blocking, which may prove to be helpful in a number of situations.

From a diagnostics standpoint, it's easy enough to see if your Gatekeeper software is working on the DC, and the variety of supported identity services provides enough freedom/ flexibility for anyone to specify which service or method they trust and how much.

Customers will appreciate the fact that the web interface can be customized and the self-service portal can be integrated with the specific visual style of an organization.

By default, the application logs privileged events like key recovery to Windows events. Reporting is also available through a dashboard, where one can search for specific events. One thing I would love to see is the actual information about user logins to the cloud service in the event logs.

Specops Key Recovery helps system administrators and users: it removes complexity and successfully solves a common problem.

Is the future of information security and tech conferences virtual?

AUTHOR_Zeljka Zorz, Managing Editor, (IN)SECURE Magazine

The COVID-19 pandemic has brought about many changes to our personal and work lives. Among the latter are the forced work from home shift and the inability to travel far and attend in-person meetings, industry-specific workshops, events and conventions.

And while RSA Conference USA – the largest information security conference in the world – managed to take place mere weeks before the World Health Organization declared COVID-19 a pandemic, European countries started closing borders and airlines started suspending routes and grounding planes, most infosec and tech events scheduled to take place after it were doomed.

One by one, they were postponed, canceled or went virtual. While it's still impossible to tell whether the conferences postponed until the already-crowded (northern hemisphere) fall season will actually take place, we've asked some people

who are involved in organizing them to give their opinion on the future of large information security and tech gatherings.

> *While virtual events are – currently and generally – the most effective way of gathering people who are otherwise restricted from traveling, they will not become the only (or even predominant) method of conferencing.*

Smaller, more local in-person events

Jack Daniel, one of the co-founders of Security BSides, thinks that, long term, a lot of events will not resume and others will be scaled back.

"The economic fallout from the pandemic will limit funding for events large and small, and caution over transmission of illness will continue for a while," he told us.

When it comes to events that are organized under the BSides banner by different organizers in various corners of the world, he expects their number to diminish and those that do take place to be smaller.

"I think this will be true for events in general, but for BSides my hope is that it will drive focus to local events, local communities, and local opportunities – places where BSides have the most profound impact," he added.

> *Twitter discussions on what kind of virtual conferences eager attendees would prefer have brought to light disparate needs, wants and limitations.*

Michael Hiskey, Chief Strategy Officer at Data Connectors, a company that has been conducting cybersecurity conferences in cities across the US and Canada for the last 20 years or so, says they believe that, post-pandemic, conferences and trade shows will be far more "down to business."

"Regional relationship teams, meeting directly with accounts in their area, is where the action will increasingly be," he opined.

"For the purposes of educating cybersecurity professionals and connecting them with solutions with a presence in their region, smaller conferences will grow in their importance. They cost less, which will appeal to the bottom-line professionals, they will connect regional account executives with prospects (ask any account executive who's had to hand off a prospect at a big trade show to the appropriate regional connection, and you'll see the frustration), and will enable the 20% of job seekers who attend any conference to focus on the next opportunity in their area."

The pros and cons of virtual events

While virtual events are – currently and generally – the most effective way of gathering people who are otherwise restricted from traveling, they will not become the only (or even predominant) method of conferencing, Hiskey says.

"Replacing an all-day conference with an hours-long webinar will not meet the needs of conference-goers," he noted.

"We have found that immersive, live virtual event platforms, offer the opportunity for interacting with exhibitors, solution providers and peer-to-peer networking. Surprisingly, with respect to otherwise introverted attendees, we've found they're more likely to reach out for networking than at a physical event. While the 'happy hour' might not be quite the

same, virtual event platforms have thought through almost every facet of the physical event experience."

Twitter discussions on what kind of virtual conferences eager attendees would prefer have brought to light disparate needs, wants and limitations.

Many say that, while working from home, attending a whole-day virtual event is nearly impossible due to more immediate and pressing obligations – both work-related and personal.

And while those who would otherwise be prevented from attending a specific conference – whether due to the lack of a visa, funds, free time, physical mobility or psychological/social capacity – have mostly welcomed the diversity of virtual event offerings, most say that the networking aspect on in-person conferences is difficult to recreate.

For one, it is difficult to replicate the serendipitous aspect of real-life introductions that happen just because someone is sitting/standing physically beside you at an after-conference party or while waiting for a talk to start.

While some organizers keep hoping the situation will return to normal soon and they will be able to reboot their events, others have decided to cut their losses here and now.

Secondly, even if there is a virtual space ("hallway") that simulates an informal gathering, chit-chatting and discussing things there – whether over Zoom, Twitch, Slack or chat rooms – is far more tasking than in-person.

All in all, most agree that virtual "conferences" are a good enough option when there is no other option, but that they prefer the offline versions.

As Daniel noted, people attend and participate in events for a lot of reasons, and virtual events satisfy some, but come up short for many things.

"Virtual events will never have the same impact as far as connecting people, whether for community building, or for sales and support. Virtual events also don't have the social bonds that in-person events have," he opined.

Things to keep in mind when switching to a virtual venue

While some organizers keep hoping the situation will return to normal soon and they will be able to reboot their events, others have decided to cut their losses here and now.

O'Reilly Media is one of the latter. In late March 2020, after having previously postponed or cancelled some of their Strata conferences, the company announced they would be closing down the live conferences portion of their business.

"Without understanding when this global health emergency may come to an end, we can't plan for or execute on a business that will be forever changed as a result of this crisis," **Laura Baldwin, President at O'Reilly Media**, explained at the time, and said that they will concentrate their efforts on delivering quality on-line events.

"We believe that global tech events are going to be permanently changed because of COVID-19. We were already seeing a trend towards larger user events for specific tools or platforms, instead of conferences that represented the full ecosystem within a technology practice area," she told Help Net Security.

"At our own events, the fastest-growing, most popular portion of our conferences had been the two training days ahead of the events themselves.

Additionally, O'Reilly started delivering on-line training events in 2016, and has worked hard to perfect the delivery and efficacy of our live-trainers. The attendance at these events has proven that this type of focused learning can be delivered online and made even better with easy access to our interactive learning platform. This has been bolstered by the accelerated rate of technology over the past few years, which means attendees find it more difficult to be out the office for a week to attend an event. People who had traditionally attended our in-person events started showing up more at our live trainings and other interactive learning events on our platform."

Organizers of online events must not make the mistake of switching the "venue" but not the form.

As **open source developer and community manager Michael Hall** recently explained, there are a number of problems that have to be solved for a newly virtual event to be successful in the long run. His opinions based on experiences while helping Canonical turn the Ubuntu Developer Summit into an online affair should be required reading for organizators looking to make the switch.

Baldwin also agrees that virtual events are going to be different – and that's ok.

"While networking may be made more difficult, there are so many aspects of in-person events that can be improved upon and we're already starting to see that," she noted.

"Within 10 days of cancelling our Strata Data & AI conference, we had recreated it as a two-day virtual event through our learning platform and had 4,600 registered attendees. That in itself is a huge benefit because rather than planning an event a year out to secure venue space and give speakers time to travel, we can produce more nimble, timely and relevant events. The audience can register with little lead time because there's no need to clear their calendars for a week, organize time away from the office and families, and book travel."

She also says that they were ultimately impressed with the audience engagement: in just the first hour of the virtual conference, they had more than 160 questions asked of the initial presenter. "There's no opportunity for that level of engagement during an in-person session," she added.

Lastly, she says, shorter, more focused online events should also be taken into consideration.

"We've been doing live events that we call 'Meet the Experts' through our platform long before COVID-19 was ever an issue and had great results. It's about 15 minutes of presentation and then 45 minutes of Q&A. While not necessarily networking, it does connect technology practitioners with innovators to get a better understanding of timely topics," she concluded.

Industry news

ProcessUnity incorporates industry risk intelligence into third-party risk processes

ProcessUnity extended its Vendor Risk Management automation platform with new capabilities to incorporate industry risk intelligence into third-party risk processes.

The ProcessUnity Vendor Intelligence Suite uses program automation to seamlessly integrate cyber ratings, financial health data, watchlist ratings and more into ProcessUnity Vendor Risk Management to provide organizations with a comprehensive view into the health of their vendor ecosystem.

FireEye enables orgs to respond to security incidents faster with flexible and customizable modules

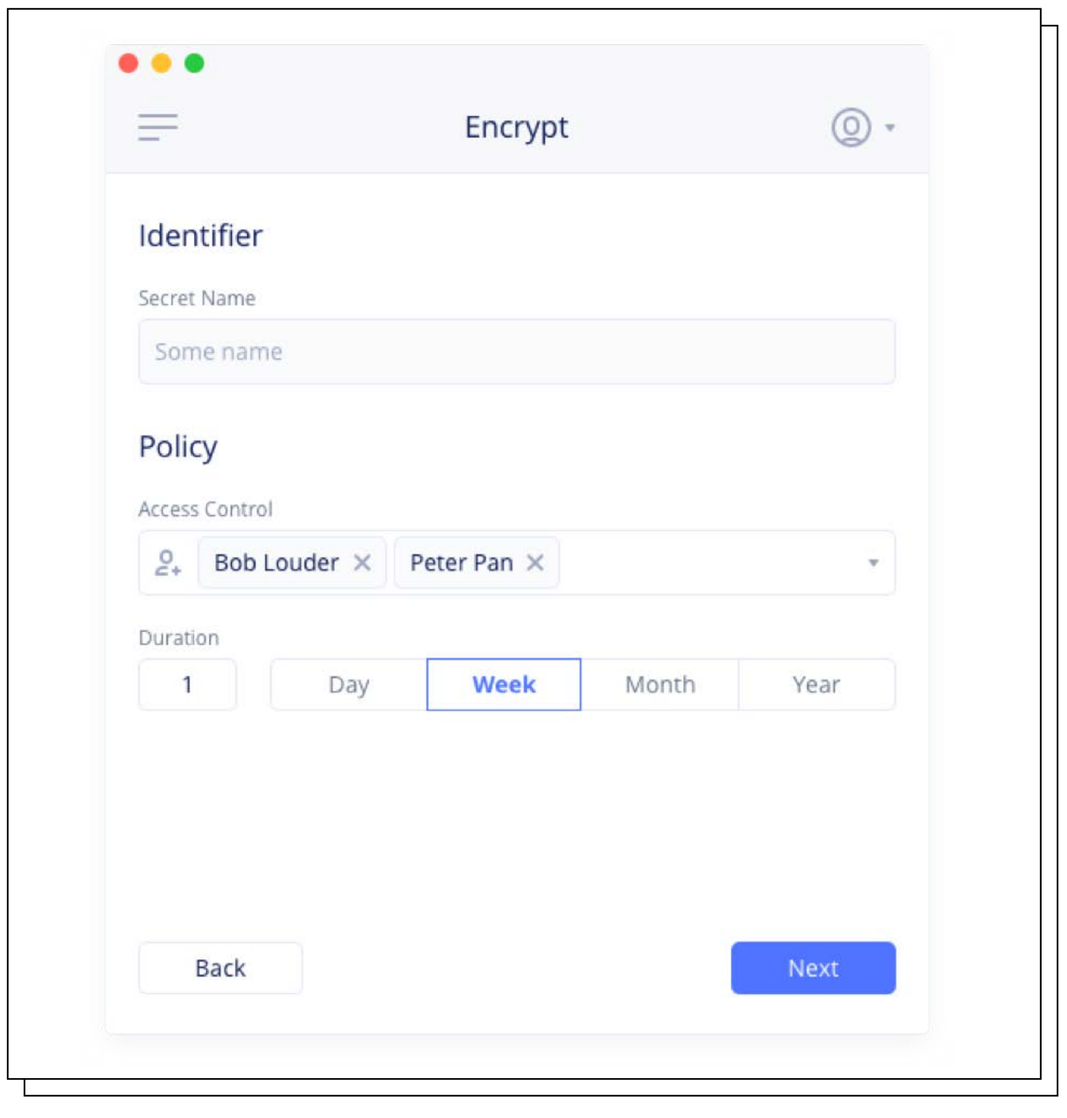
Unlike traditional endpoint security vendors that provide one-size-fits-all solutions to every customer, FireEye Endpoint Security is designed to deliver comprehensive defense using fully customizable protection modules.

The module creation is supported by the world's leading frontline responders at Mandiant, to block malware and exploits, detect advanced attacks, and provide the response tools and techniques that fit an organization's unique risk profile and security posture.

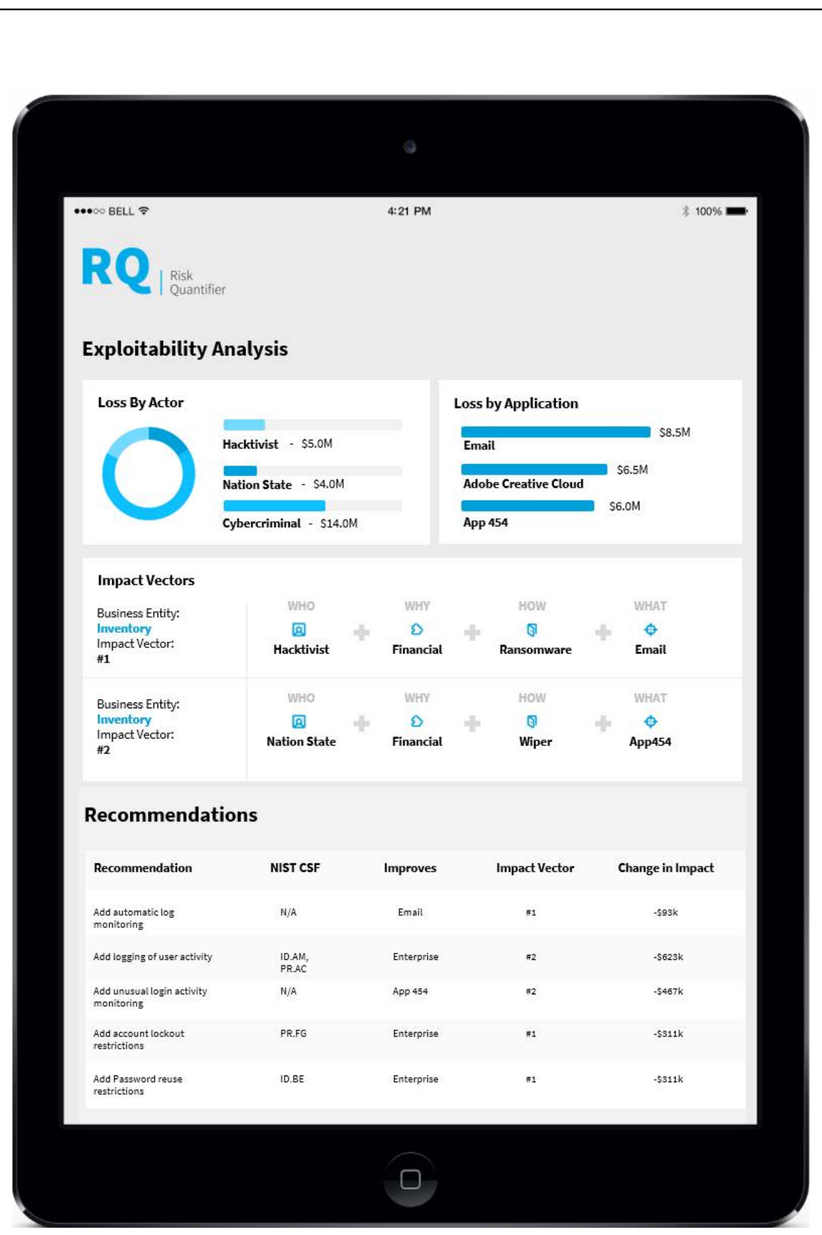
Volterra launches VoltShare to simplify the process of securely encrypting confidential data end-to-end

VoltShare is available as downloadable software (or an API and SDK) that operates locally on a laptop or mobile device to easily encrypt sensitive data for sharing with target recipients through email or existing collaboration platforms such as Slack, Teams, Dropbox, etc.

It is a simpler and more secure approach than traditional file sharing and encryption solutions since it does not require sending passwords or managing complex public-key cryptography.



Nehemiah Security Risk Quantifier 4.0: Modeling shared risks across business lines



Nehemiah Security recently released version 4.0 of Risk Quantifier (RQ), which provides enhanced ability to quantify, communicate, and manage risk across an enterprise's various lines of business.

For large enterprises (those with multiple subsidiary companies, business units, or legal entities), understanding how risk may affect different areas of the business or cascade throughout the organization has been a very labor intensive and time-consuming exercise to quantify and manage.

Version 4.0 builds on earlier versions, automating risk quantification, with enhancements to model shared risks across business lines or cascade risk down from corporate to subsidiaries or lines of business. This provides a more comprehensive view of the risk and the ability to measure its full value.

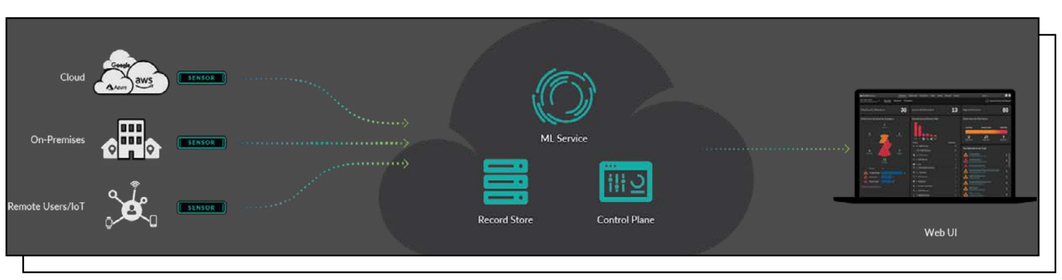
Sony releases two models of intelligent vision sensors with AI processing functionality

Sony announced the upcoming release of two models of intelligent vision sensors, the first image sensors in the world to be equipped with AI processing functionality.

Including AI processing functionality on the image sensor itself enables high-speed edge AI processing and extraction of only the necessary data, which, when using cloud services, reduces data transmission latency, minimizes any privacy concerns, and reduces power consumption and communication costs.

These products expand the opportunities to develop AI-equipped cameras, enabling a diverse range of applications in the retail and industrial equipment industries and contributing to building optimal systems that link with the cloud.

ExtraHop Reveal(x) 360: Improving security posture without compromising availability



ExtraHop announced the general availability of Reveal(x) 360, the first SaaS-based network detection and response (NDR) solution providing on-demand, unified visibility across multi-cloud and hybrid workloads, as well as distributed workforces and operations.

With ExtraHop Reveal(x) 360, security operations teams can harness the power of the cloud to improve security posture without compromising availability or core business objectives.

$(ISC)^2$ CISSP certification recognized as equal to a Master's by UK NARIC

$(ISC)^2$ – the world's largest nonprofit association of certified cybersecurity professionals – announced that the Certified Information Systems Security Professional (CISSP) certification has been found comparable to Level 7 of the Regulated Qualifications Framework (RQF) in the UK, denoting that the certification is comparable to Master's degree standard.

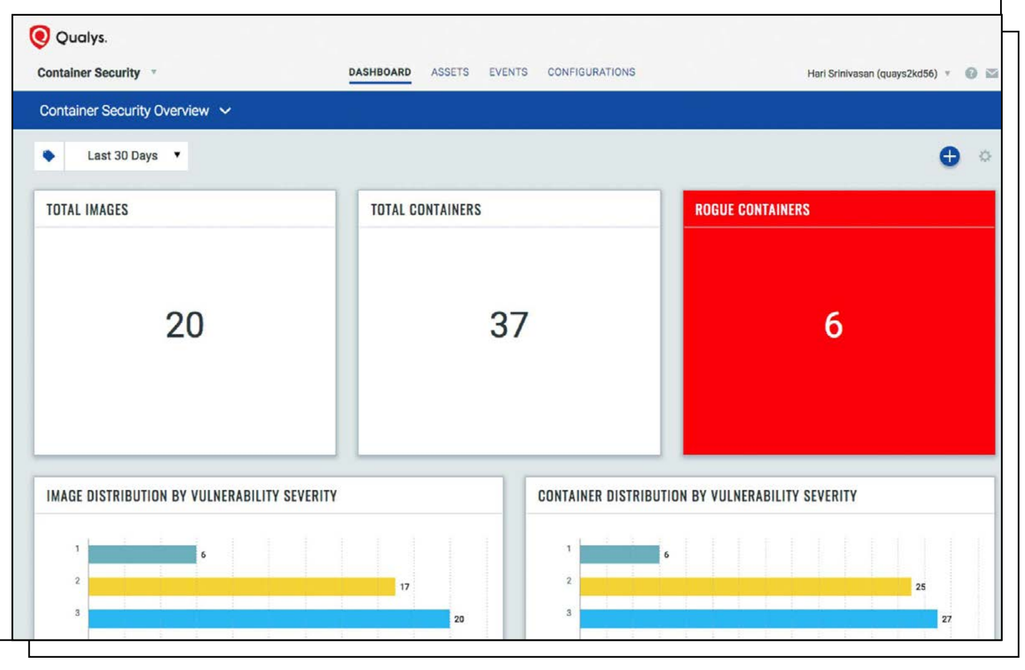
This further validates the achievement of CISSP-certified professionals in their ongoing career and qualification progression and supports educational institutions looking to determine weighting of a relevant certification to award course credits. It follows the American Council on Education's College Credit Recommendation Service (ACE CREDIT) recognizing six $(ISC)^2$ certifications as eligible for college credit.

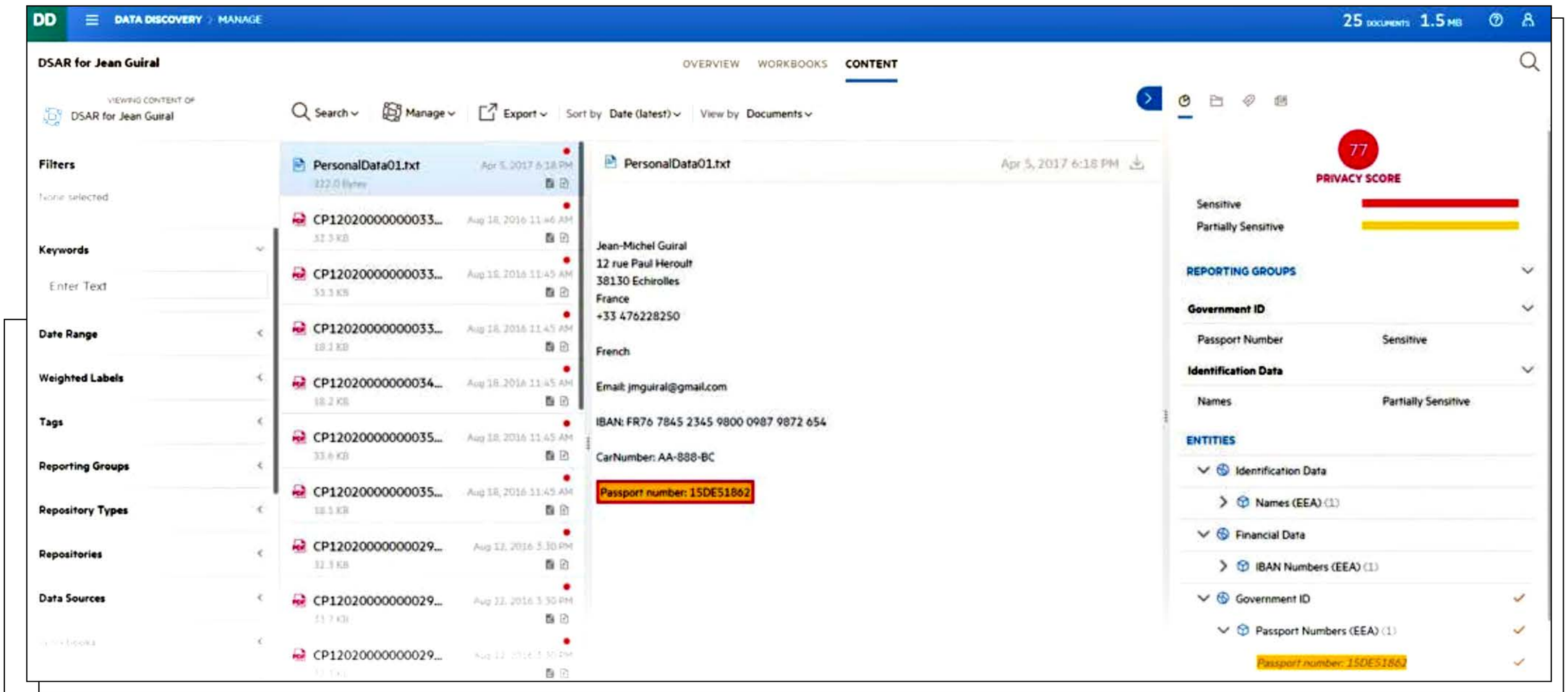
Qualys provides vulnerability management for customers of Azure Security Center

Qualys announced that Qualys Container Security is immediately available, and Qualys Vulnerability Management will be available within a month in Microsoft Azure Security Center.

This solution leverages the embedded Qualys Cloud Agent and Qualys Container Sensors to build Vulnerability Management automation into the CI/CD pipeline as well as real-time visibility into running virtual instances.

The solution automatically analyzes virtual machines and container images in Azure, providing customers visibility into vulnerabilities and configuration issues. Any discovered vulnerabilities are reported to Azure Security Center as recommendations, including the ability to create playbooks for one-click remediation with no software to deploy or update.





Micro Focus File Analysis Suite: Helping IT admins identify, manage and secure sensitive information

Micro Focus announced the release of Micro Focus File Analysis Suite, offering IT administrators a comprehensive data lifecycle management solution for identifying, managing and securing sensitive information across the enterprise.

As organizations implement protocols to meet national and international data regulations, the Micro Focus File Analysis Suite lowers the total cost of compliance, reduces risk and provides analytical insight and value across high-value and sensitive data assets.

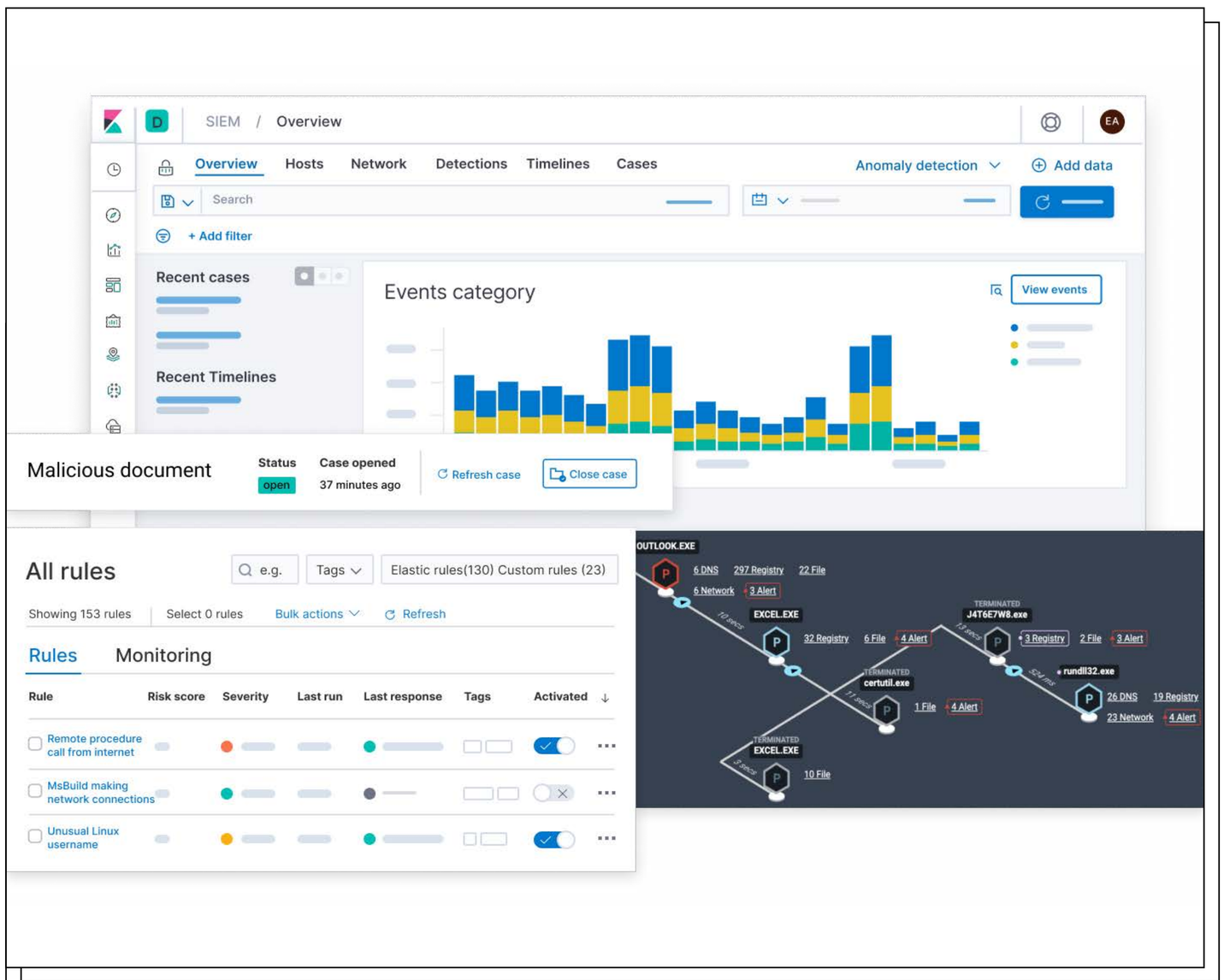
“With Micro Focus File Analysis Suite customers no longer need to choose between traditional platforms that are limited to only offering storage optimization or data access and governance,” said Rick Carlson, Vice President, Information Management & Governance Solutions at Micro Focus.

TransUnion announces the Global Fraud & Identity Solutions Group

TransUnion announced the creation of its Global Fraud & Identity Solutions Group, a move focused on uniting all aspects of the company’s fraud risk offerings, and the hiring of industry veteran, Shai Cohen, to lead the group.

“For years TransUnion has been a leading force in fraud prevention with a steady stream of high-profile acquisitions, product innovations and industry hires,” said Tim Martin, executive vice president and chief global solutions officer at TransUnion.

“We’re excited to bring in a proven leader from some of the world’s most respected cybersecurity and technology companies to unite these efforts and take our fraud prevention solutions to the next level.”



Elastic Stack 7.7.0: Major updates for Enterprise Search, Observability, and Security

Elastic announced major updates across the Elastic solution portfolio with dozens of advances to bring efficiency, flexibility, and integrated workflows to teams of every size and across every use case.

Case management introduces case management features built into Elastic Security, along with direct integration into ServiceNow ITSM.

- Provides security operations teams more control over detection and response workflows allowing analysts to open, update, tag, comment on, close, and integrate cases with external systems.
- Integrates case management with ServiceNow ITSM, allowing analysts to forward information from Elastic SIEM to the ServiceNow platform for cross-org ticket tracking and remediation.

Swimlane Analyst Hub: Increasing access to educational content and open-source tools

The Swimlane Analyst Hub is a way to aggregate its open-source and developer tools and content for security analysts. Free resources and tools include thought leadership on understanding APIs, enhancing digital forensics and incident response (DFIR) processes with PowerShell, and how to make the MITRE ATT&CK framework actionable with pyattck.

Two of the primary open-source tools introduced in the Analyst Hub are pyattck 2.0 and an equivalent PowerShell version called PSAttck.

These new releases provide security operations centers, defenders, and offensive security teams with external data points to enrich MITRE ATT&CK by providing potential commands, queries, and even detections for specific techniques. Swimlane's Deep Dive team will continue to enhance and add additional open-source tools on the Analyst Hub.

"As InfoSec professionals, it's our responsibility to mentor, educate and guide newcomers so they can one day do the same—simple recursion," said Josh Rickard, Swimlane Deep Dive team member.

Cyber security is a board level issue: 3 CISOs tell why

AUTHOR_ Oren Yunger, Venture Capital Investor, GGV Capital

As a venture capital investor who was previously a Chief Information Security Officer, I have noticed an interesting phenomenon: although cybersecurity makes the news often and is top of mind for consumers and business customers, it doesn't always get the attention it deserves by the board of directors.

> *How can boards dive deeper into the world of security and overcome the entry barriers to collaboration?*

Misconceptions and knowledge gaps increase this distance between security and oversight. How can boards dive deeper into the world of security and overcome the entry barriers to collaboration? Seeking advice, I reached out to prominent security leaders: **Joel Fulton**, the former CISO of Splunk; **Jeff Trudeau**, the CSO of Credit Karma; and **Yassir Abousselham**, the former CSO of Okta and the newly appointed CISO of Splunk. Here are their tips for board members:

Recognize security as both a business risk and an opportunity

First and foremost, it is imperative for the board to appreciate the impact that information security can have on the business. Boards should treat security as a top business risk as well as a top business opportunity. Major security events can have a significant impact on revenue, brand, and even lead to catastrophic results. **Abousselham** elaborates: "In an era where organizations are handling large amounts of sensitive information and governments are actively pushing more stringent privacy laws, data breaches have serious ramifications for the organization, its customers, and partners".

Contrary to popular belief, the security leaders believe that domain expertise is not a prerequisite to making smart security decisions.

Bridge the technical gaps

Contrary to popular belief, the security leaders believe that domain expertise is not a prerequisite to making smart security decisions. Instead of focusing on every technical bit and byte, **Trudeau** suggests the conversation should concentrate on understanding the risks and ensuring they are properly addressed. Yet, even on a macro level, security concepts might be difficult to fully understand, so a short and dedicated security training for the board can come in handy. It's also key to remember that it's not only the board members who may feel like fish out of water. The CISO, too, can get intimidated and might over-rely on the comfort and familiarity of technical details.

The board's questions should also serve as a vehicle for both the CISO and Directors to think more strategically about security.

To mitigate the differences, **Abousselham** offers to foster a synergic discussion by framing risks and mitigations in business terms. **Fulton** proposes focusing on the Venn overlap of the security program's weaknesses and the board's strengths (like governance and strategy). This enables the board to interact with security as they do with other domains, empowering the CISO with wise counsel, and letting both view clearly the current situation and the paths to success.

Ask the right questions

The board should operate on the notion that absolute security does not exist. The best way to assess your security program is often by focusing on and drilling down into the economic trade-offs. **Fulton's** suggested economic questions include: *Are you applying your scarce resources, people, and time to the correct problems? Next, drill deep to understand the security leader's rationale and thinking: How do you know you're right? What evidence would indicate you're wrong? and How can we find that evidence?*

The board's questions should also serve as a vehicle for both the CISO and Directors to think more strategically about security. As the technological environment has evolved tremendously in recent years, it is important to step outside the traditional realm of compliance and assess the potential catastrophic consequences of security deficiencies. For example, **Trudeau** proposes including questions like: *Could what happened at this other company happen to us? What would be the damages from such threat materializing in our company?*

Evaluate the effectiveness of the security program

The group offers structured approaches to synthetizing information and reaching conclusions about the security program. **Abousselham** recommends a top-down method: "Confirm that the CISO has a good grasp of security and compliance risks. Then validate that the CISO's vision and strategies support the direction of the company and desired risk posture. Further, get comfortable with the CISO's ability to execute, including the adequacy of the organizational structure, technical capabilities, funding, and ability to hire and retain talent. Lastly, because incidents are bound to happen, evaluate the ability to detect and respond to security compromises". Fulton advocates that

the board seek to help the CISO with possible blind spots, looking to validate the security strategy and initiatives with questions like: *Where are you intentionally reducing focus? Why is that decision the best decision in this company, environment, and vertical? In your areas of highest investment, what does "secure enough" look like?*

Certainly, no evaluation will be complete without metrics that measure the progress and maturity of the security program. Fulton suggest boards inquire on how the program is measured and how the CISO knows the measures are valid and reliable. **Abousselham** offers focusing on objective risk measures with metrics to show progress against a baseline such as NIST CSF; and adopting no more than ten key metrics that summarize the state of the security program and its business influence.

> *When measuring the security program's effectiveness, it is crucial to consider that it is tied to the CISO's ability to influence the organization. The security leader's ability to execute is very much dependent on the reporting structure.*

When measuring the security program's effectiveness, it is crucial to consider that it is tied to the CISO's ability to influence the organization. The security leader's ability to execute is very much dependent on the reporting structure. According to **Trudeau**, reporting to the wrong executive could pose challenges for the security program and hinder its effectiveness. In addition, it is important to validate the CISO's cross-functional operation. Most security practices and controls are implemented, operated, and maintained by employees without "security" in their title. Consequently, a CISO must be respected and influential outside her own organization.

Communicate in the right format and cadence

A good rule of thumb is for boards to meet the CISO at least once a year. **Abousselham** explains that some companies adopt a cadence of two updates per year, to the board and the audit committee. Boards might also ask the CISO for more frequent or ad hoc updates if the perceived risk is higher than the acceptable threshold. Additionally, informal and off-schedule meetings improve relationships and information sharing simply by the reduction in formality. **Fulton** believes these keep strategy aligned and could be invaluable during actual or tabletop incident walk-throughs. However, boards should be careful to not overdo it as too frequent meetings can be inefficient, **Trudeau** warns.

With security becoming increasingly important, some organizations have created security committees to ensure independent oversight of security risk. The security leaders don't believe it's necessary in most cases, since it might be distracting. If a company is forming a security committee, **Abousselham** explains that committee members should be independent and with proper domain expertise to formulate and report an accurate opinion of the security risk posture to the board.

Conclusion

Fostering collaboration between the board and the CISO benefits both groups and the company as a whole. However, it's not always easy and growing pains are to be expected. While everyone may share the same objective of seeing the company succeed, they often differ in their agendas and approaches. The good news is that asking the right questions, conquering communication gaps, measuring progress and treating security as a business risk will set the board up for success in improving the company's security standing.

(ISC)²®

Expert Instruction.
Online Convenience.
New Great Price.

CISSP® SSCP® CCSP® CAP® CSSLP® HCISPP®

Get the Best of Both Worlds
Expert Instructor-led Classes & Online Convenience

(ISC)² is here to help you stay on track with your certification.
Our Official Online Instructor-Led training is now at a **NEW LOWER PRICE**.

These trainings give you…

- The flexibility to train over consecutive days or weeks
- Continued access to course content for 6 months
- 1-year access to courseware materials
- Live support from an (ISC)² Authorized Instructor
- Official (ISC)² Student Training Guide (electronic)
- Collaboration with classmates
- And more

GET NEW PRICING

With the zero trust model, an organization only allows access between IT entities that have to communicate with each other.

The top four Office 365 security pain points

AUTHOR_Michael Morrison, CEO, CoreView

Many novice Office 365 (O365) shops do not know where platform-specific security vulnerabilities lie, or even that they exist. The threats that you are unaware exist do not cause pain until they rise up and bite – then the agony is fierce.

Companies get themselves into trouble when they do not fully understand the way data moves through O365 or they apply on-premise security practices to their cloud strategy. While the O365 platform comes with some security features and configuration options – that all customers should take advantage of – native or built-on tools do not address many vulnerabilities or other security issues.

In this article you will find four common areas that enterprises neglect when they adopt O365.

1. Impossible to implement zero trust with native tools

Enterprises are increasingly relying on zero trust cybersecurity strategies to mitigate risk and prevent data breaches. With the zero trust model, an organization only allows access between IT entities that have to communicate with each other. IT and security teams secure every communication channel and remove generic access to prevent malicious parties from eavesdropping or obtaining critical data or personally identifiable information (PII).

Under the O365 centralized admin model, all administrators have global credentials, which means they have access to/can see each and every user. Not only is this deeply inefficient, it also creates huge security problems.

One problem with using a zero trust strategy is that implementing it in Azure Active Directory (Azure AD) is highly complicated. For instance, IT and security teams can label an employee an "Application Administrator," which gives them and anyone else with that label the ability to perform/change 71 different attributes. The problem with these cookie-cutter roles is that organizations do not know precisely what all of the corresponding admin-controlled attributes mean nor do they know what functionally they are granted.

2. Difficult to manage privileged permissions

Under the O365 centralized admin model, all administrators have global credentials, which means they have access to/can see each and every user. Not only is this deeply inefficient, it also creates huge security problems. Did you know that 80% of SaaS breaches involve privileged permissions? And that admins have the most privileges of all? In O365, user identity must be treated as the security perimeter.

The native O365 admin center focuses on providing global admin rights, giving admins who tend to work locally too much power and privileges they do not need. This centralized management model of setting privileges with O365 entirely relies on granting "global admin rights" – including regional, local, or business unit administrators. The native O365 Admin Center does not enable you to easily set up rights based on business unit or country, or for remote or satellite offices. In addition, you cannot easily limit an admin's rights granularly, so they can only perform limited and specific functions, such as changing passwords when requested.

So, how do you mitigate the risk related to O365's operator rights? Some IT veterans may answer with role-based access control (RBAC) as it allows organizations to partition permissions based on job roles, resulting in far fewer, truly trusted global administrators. These global admins are augmented by a set of local, or business unit focused admins with no global access, all leading to far better protection for your O365 environment.

When used strategically, logs provide valuable forensics that not only help detect a breach, but also identify cybercriminals that may still reside on the network.

3. Difficult to set up log and audit functions

O365 collects millions of bits of information on even the smallest implementation. Unfortunately, from a security standpoint, these data points do not exist for long and far too few are ever used for protection or forensics. Microsoft historically offers logs for only the last 30 days (though that is being increased to a year soon, but only for high-end E5 licenses), but businesses must ask themselves:

- Why do they need to collect data logs?
- How do logs impact regulatory compliance?
- What happens if the logs aren't saved or otherwise mined and audited?
- What business value do these logs offer?

When used strategically, logs provide valuable forensics that not only help detect a breach, but also identify cybercriminals that may still reside on the network. Before businesses can even think about leveraging audits, IT and security teams have to turn on logging and implement a process to save log data far longer than Microsoft's standard 30 days. It's also important to know that even when logging is set up, event tracking is not an O365 default setting so businesses must turn that on.

Real-time monitoring and alerts for security compliance issues is the engine that drives much of the data that forms the logs. Smart IT shops now enable real-time monitoring and alerts for potential security compliance issues in their O365 environment.

4. The "right to be forgotten" challenge

Compliance is a big security and economic issue. There are almost daily incidents of fines occurring due to GDPR and other privacy regulations like CCPA. There is a lot involved in being compliant with GDPR, foremost among its statutes is the "right to be forgotten." This statute states that individuals have the right to ask organizations to delete their personal data.

Organizations must be able to track and audit individual user accounts to make sure that they not only comply with this request but have processes in place to differentiate between users with similar (or even identical) usernames, even if one of them exercises their right to be forgotten.

However, as many businesses have learned, it is difficult to fulfill this requirement if the IT or security team cannot locate personal information or know how it was used. Organizations must be able to track and audit individual user accounts to make sure that they not only comply with this request but have processes in place to differentiate between users with similar (or even identical) usernames, even if one of them exercises their right to be forgotten.

At their core, each of these challenges is centered around a general lack of visibility into the O365 infrastructure. Microsoft's SaaS platform introduces a number of important business benefits and capabilities but requires enterprises to take proactive measures to account for their data and how it is accessed and shared externally. Organizations need to fulfill their end of the shared responsibility model to maintain a solid organizational security posture.

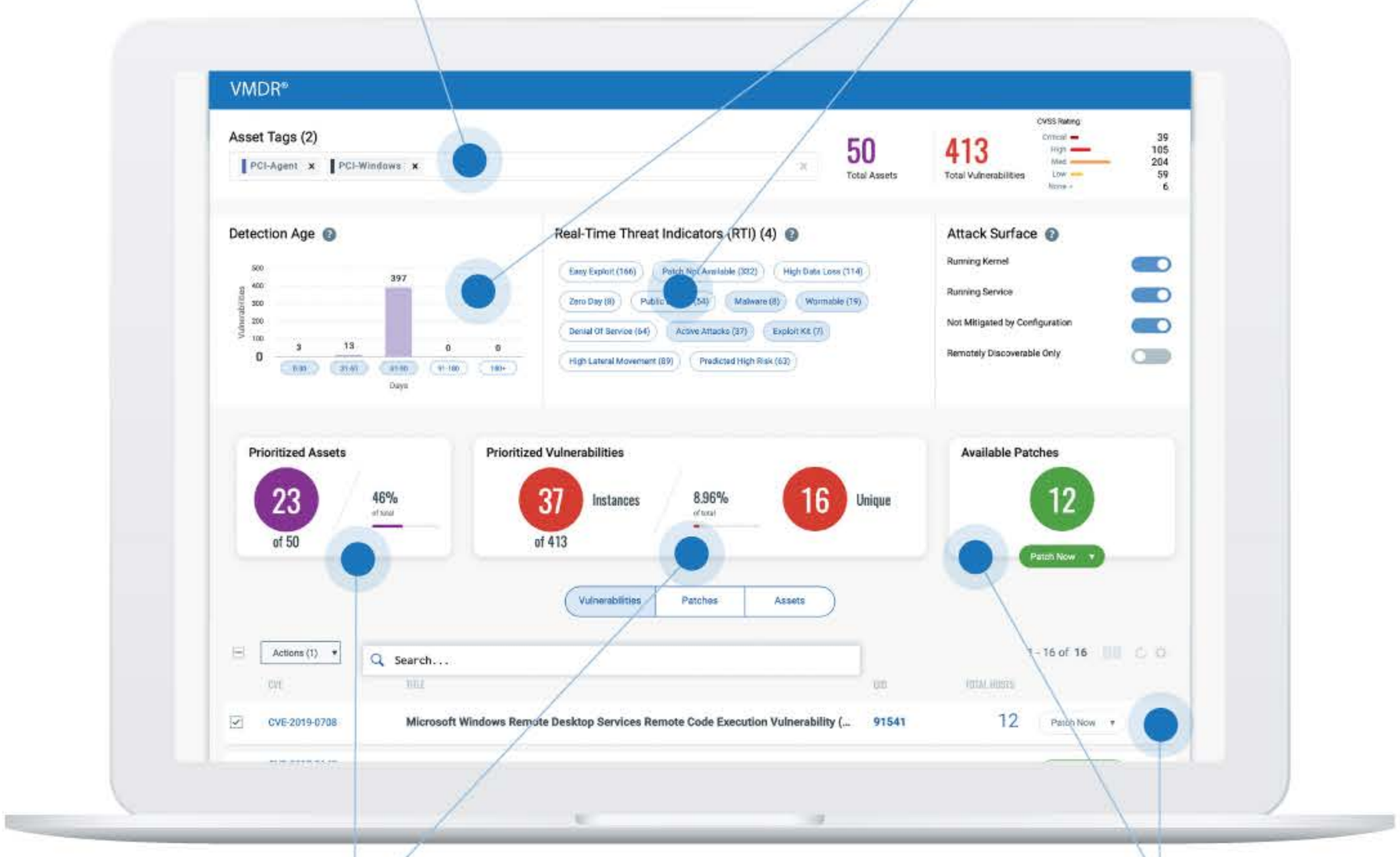
Bringing Vulnerability Management to the Next Level

Introducing **Qualys VMDR® – Vulnerability Management, Detection and Response.** An all-in-one cloud-based app for a true risked-based vulnerability management program.

qualys.com/tryVMDR

Identify and inventory all known and unknown assets, and add custom tags

Identify vulnerabilities and misconfigurations in real time



Automatically prioritize the vulnerabilities posing the greatest risk using advanced correlation and machine learning

With a single click, globally deploy the most relevant superseding patch

Qualys®

During this extended period of social distancing filled with increased online activity, I can't help but reflect on all the user data that has been created, stored, hacked, exposed, bought, shared and sold over the last 10 years. What's known as the black market is built on this immeasurable and personally identifiable data – information both believed to be secured and known to be exposed – and frankly, it is entirely of our own creation.

On my mind: Transitioning to third party cloud services

AUTHOR_ Christian Lees, CTO and CIO, Vigilante

> *Adversaries today do not have to spend nearly as much time or effort exploiting an organization – it's a no brainer for them to suck down improperly secured data from the cloud.*

The transition from traditional onsite data colocation to the use of third-party cloud shared tenant services should be on everyone's minds. With this growing shift, everyone from individuals

to enterprises will continue to fuel threat actors by improperly storing information in the cloud. Adversaries today do not have to spend nearly as much time or effort exploiting an organization – it's a no brainer for them to suck down improperly secured data from the cloud. In fact, I would argue that the amount of data exposed by misconfigured S3 buckets and or third-party vendors (for example misconfigured Mongo databases, Elastic Search Engines or other applications) far exceeds exposure by any other threat actor activity.

Major factors contributing to improperly secured data include a misconception that the cloud is inherently more secure than storing data on-premise, the struggle to define the scope of an enterprise environment and a lack of visibility into threat actor environments, the perpetual selling of security solutions as if they are a silver bullet, and a shortage of security professionals.

Because the cloud is often utilized by organizations who do not have robust security teams, this maintenance and security hygiene often goes unchecked.

The cloud is only as secure as we make it

I regularly hear people say the cloud is so much more secure, but when asked, "Why is it more secure?" the responses are not reassuring. Larger organizations are likely to have highly skilled teams to secure their own infrastructure, but the cloud model is designed for ease of use, and reduced friction and complexity – a ripe combinations for folks with less technical skills to launch data into the cloud. In fact, placing the data you govern into a shared tenant service is as easy as putting in a valid credit card.

However, many companies move to virtual servers in cloud services and simply duplicate traditional on-site services. They do not consider that in order to remain secure, these servers require the exact attention that an on-site server requires, continuous backporting and patching, network services firewall and identity access management. Because the cloud is often utilized by organizations who do not have robust security teams, this maintenance and security hygiene often goes unchecked.

You can't protect unknown data from unknown attackers

It's well understood by now that organizations are challenged by defining the boundaries and scope of their environments, and knowing where web applications ingress and egress, whether an environment has adequate segmentation or if it's a flat network. But it bears repeating that in order to protect data, you have to know everywhere it is and what it means.

Conducting tabletop exercises that leverage modern threat vectors such as Stride, Trike or other frameworks is one way to track the most likely ways a threat actor could gain access or circumvent intended security controls, but many organizations are unprepared to complete these exercises or internally discuss the technical issues surrounding the results. In other words, they lack the language and ability to quantify threat risks to the organization which prevents the brand from defining their appetite for risk.

The industry is still selling silver bullets and alert fatigue

Enterprise security solutions are being sold as silver bullets. Many of these solutions are generally syslog tools marked up with hot words like "AI" and "Next Generation", but really should be noted as "Lipstick on a Pig". These solutions are often the cause of

alert fatigue and companies quickly losing sight of the forest for the trees.

> *Companies that lack robust IT teams, understandably, seek out flexible options to keep their business operations streamlined and continue supporting growth.*

It doesn't matter how easy to use a tool is or how positive the intended outcome is – an organization must be able to remediate their identified risk and have a plan to determine whether the risk is greater than the technical debt. Often times this looks like delaying a product rollout and ultimately delaying revenue, or working in haste by dumping data into a new and easy to use product through cloud services that creates unaccounted for risk.

A lack of "highly seasoned" IT professionals

At the crux of the issues surrounding improperly secured information in the cloud is the lack of IT professionals available in the market today. Companies that lack robust IT teams, understandably, seek out flexible options to keep their business operations streamlined and continue supporting growth.

While organizations are hyper-focused on alert fatigue, underfunded security teams or those who simply cannot find the needed talent will be at greater risk of having their data stolen. Hiring managers should consider expanding their search radius for filling these roles, as there are many talented job seekers that could get up to speed quickly if time is allotted for training.

> *Data has overtaken the materials of old as the currency that drives the world.*

The transition to third party cloud environments as an enabler… eventually

I do believe third party cloud environments will eventually be the enabler we prop them up to be.

For larger organizations it may be an enabler to have more control over environments by creating actual CI/CD heavily security, controlled environments such as sanitized development environments with actual sanitized quality control and testing environments.

After all, it's easy to quickly duplicate and/or burn down environments in the cloud. However, many traditional security controls are often bypassed by decisions to quickly adapt to modern third-party platforms.

Data has overtaken the materials of old as the currency that drives the world. As we move further into this decade, it behooves organizations large and small to consider what data they actually need to collect or store; how and where they are securing it; and the role they may play in fueling the underground economy.

Assessing how data loss will affect a company (and a company's tolerance for such loss) is certainly complex but is imperative. I implore organizations to leverage threat vectoring frameworks and avoid the pitfalls of believing the cloud is inherently more secure.