

[+] (IN)SECURE Magazine

03 | 2018

ISSUE 57

Security best
practices

A deep dive into blockchain
and Bitcoin

Achieving zero false positives with
intelligent deception

Testing machine learning products
requires a new approach

REPLACE YOUR AV WITH STRONGER, SMARTER PROTECTION

Malware attacks are evolving. Traditional antivirus can't.

Modern attacks commonly evade antivirus by using fileless delivery techniques that are 10x more likely to succeed.

The Barkly Endpoint Protection Platform™ is the full antivirus replacement that protects you from evolving modern attacks.



EXPLOITS



ZERO-DAY
ATTACKS



RANSOMWARE



FILELESS
MALWARE



MALICIOUS
SCRIPTS



PRIVILEGE
ESCALATION

barkly.com/replaceAV

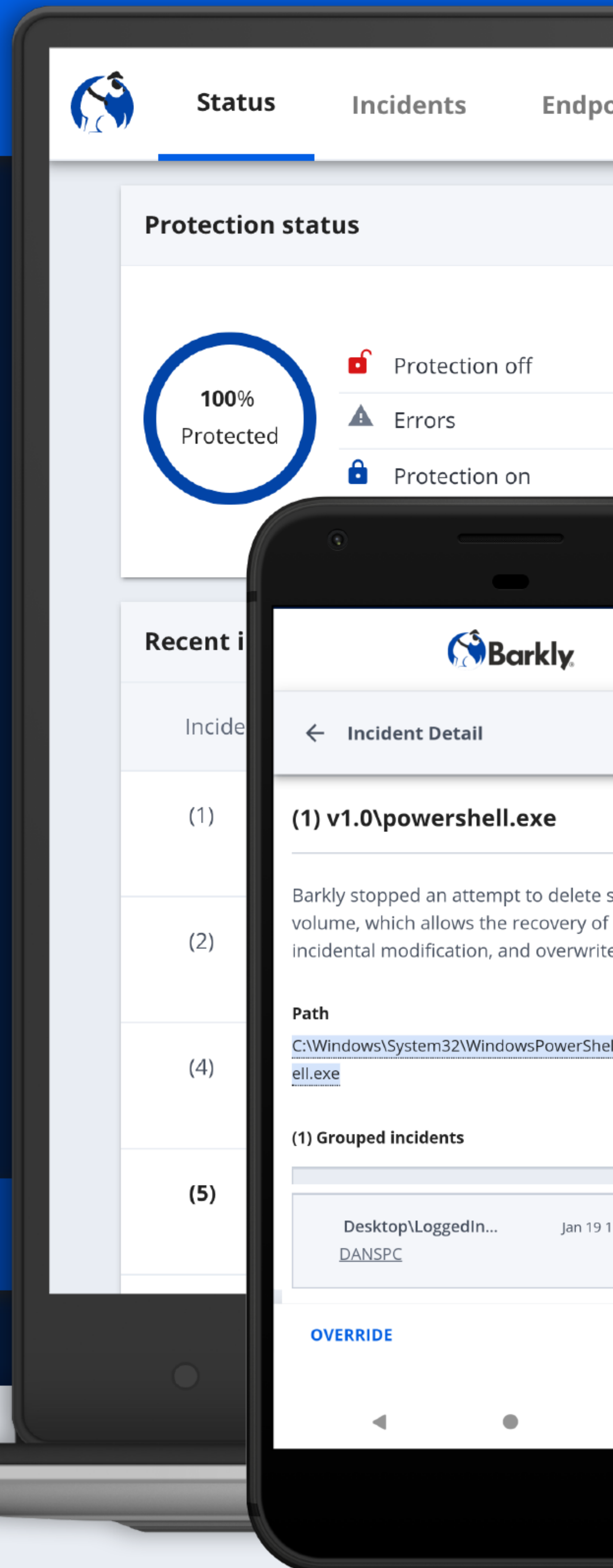


Table of contents

PAGE 04	Achieving zero false positives with intelligent deception
PAGE 07	SECURITY WORLD
PAGE 20	Expected changes in IT/OT convergence and industrial security
PAGE 23	Testing machine learning products requires a new approach
PAGE 27	MALWARE WORLD
PAGE 32	Why do we need a risk-based approach to authentication?
PAGE 35	Healthcare organizations and the cloud: Benefits, risks, and security best practices
PAGE 38	EVENTS
PAGE 39	A deep dive into blockchain and Bitcoin

Contributors

- ANUP GHOSH**, Chief Strategist, Next Gen Endpoint, Sophos

DAVID HATCHELL, Vice President of Industrial Security, ProtectWise

DORON KOLTON, Chief Strategy Officer - Emerging Technologies, Fidelis Cybersecurity
- ZORAN LALIC**, Enterprise Security Architect at a software company

RUOTING SUN, Head of Technology Partnerships, Duo Security

BRAD TAYLOR, CEO, Proficio

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 Operations
bkucan@helpnetsecurity.com

Achieving zero false positives with intelligent deception

AUTHOR_ Doron Kolton, Chief Strategy Officer - Emerging Technologies, Fidelis Cybersecurity

Cyber attacks are processes that compromise, spread and exploit multiple systems across an organization. They're not single events. When attackers compromise an asset, they don't know which asset it is; they must determine where they are in the network, the network structure and where they can find valuable information. That means attackers carefully try to find out as much as possible about the organization, and this is precisely the behavior that intelligent deception technology can exploit.

Four kinds of intelligent deception breadcrumbs

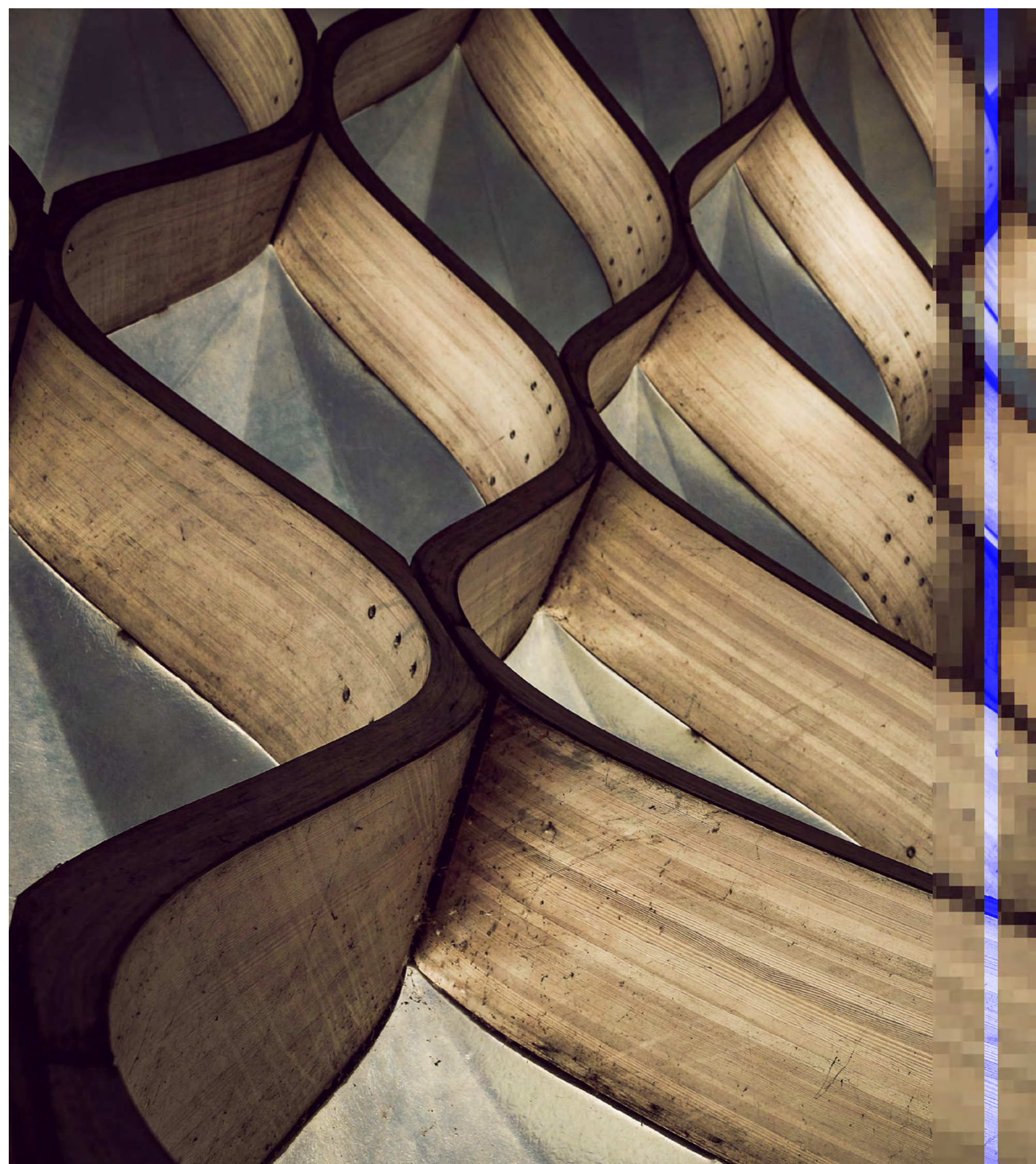
Intelligent deception systems interact with the surrounding organization's environment in ways that appear real and tempting to would-be attackers. They create a trail of breadcrumbs on endpoints, in the registry and in other places attackers look into, to lead them toward the

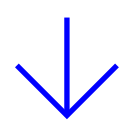
decoys and away from protected systems and sensitive information.

The intelligent deception components – a.k.a breadcrumbs – can be registered to Active Directory and DNS servers as regular users and assets of the organization. They can be referenced in files and emails and in the browser history of legitimate assets (servers and endpoints). They can point to shared folders (residing on decoys), as well as applications, files, and database entries.



Breadcrumbs are clues for a potential attacker that an intelligent deception platform intentionally leaves behind on organizational systems. For breadcrumbs to be effective, they must look and feel like real information and credentials, and must create a persuasive false trail back to deception decoys and traps.





There are four types of breadcrumbs, and they can be combined to thwart attackers:

- ▣ Credential and Active Directory breadcrumbs
- ▣ File and data breadcrumbs
- ▣ Network breadcrumbs
- ▣ Application breadcrumbs

Credential and Active Directory breadcrumbs

As part of their reconnaissance, attackers try to find credentials that will give them access to high-value systems in your organization. This presents a pivotal opportunity to create and store fake user credentials and permissions in your Active Directory system.

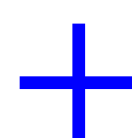
The AD Deception model uses fake users in Active Directory. Those users run on the decoys spread throughout the organization and periodically access the AD as would regular users with different permission levels in the organization. This creates the impression of legitimacy and furthers the persuasiveness of the deception. When a decoy associated with a particular fake user appears in the AD as a regular user of the organization, it presents a tempting target for an attacker who is trying to locate an account that might be used, for example, to reset a user's password.

When an attacker accesses a decoy based on the breadcrumbs in the AD, a validated decoy alert is automatically triggered and prompts an immediate response by the administrator and security operations teams.

Beyond fake Active Directory credentials and false information, these kinds of breadcrumbs can also include elements like passwords in registry keys for decoy services and SPN (service principal name) entries. If an attacker uses a decoy

credential, validated detections are enabled even for Man-In-The-Middle style attacks prompting rapid escalation and response.

File and data breadcrumbs



File-based breadcrumbs are some of the most straightforward and most versatile deception elements available. File and data breadcrumbs can include deception elements such as documents, emails, database entries and links to recent file lists that point to shared folders on the decoy systems.

Documents that are created and placed on real machines can include information about decoy systems, and contain passwords and credentials for servers and accounts in the organization.

Common examples include:

- ▣ A text file of an application's configuration that contains a username and password
- ▣ A technical document common to every organization, such as instructions on how to connect to the corporate VPN
- ▣ IT/corporate documents (TXT, DOC, XLS, PDF, etc.)

It is ideal for these file and data breadcrumbs to appear as real as any other organizational content. Since each organization is different, documents, naming conventions, and templates should be

customized with the organization's logos and usernames.

When an attacker accesses documents, emails or other data contained in these kinds of breadcrumbs, they are directed toward decoys and away from protected systems. This has a double effect: it increases the attackers' activity footprint and thwarts their attempts to locate sensitive information.

A word about emails

Emails are used extensively to transmit sensitive data from one person to another and are, therefore, often high on attackers' reconnaissance wish list. Emails are also more often perused by the attackers themselves (and not by automatic malware they have deployed), so the information contained in them is often considered to be very credible and actionable. All of this makes emails excellent deception breadcrumbs.

Network breadcrumbs

There are many ways for decoys to create network noise to lure attackers.

They can communicate with assets in the organization and with the DNS server. They can "advertise" themselves using different protocols to inform the environment about their existence or to look for certain services. This deception behavior is an effective lure for attackers that aim to conduct MITM (man-in-the-middle) attacks.

Entries to the ARP (address resolution protocol) cache are added based on the decoys' traffic and show connections to the decoys. Attackers investigating the ARP cache for interesting IPs and MAC addresses spot the decoy information and pursue that false trail, or intervene with the protocols to attempt MITM interception (and

simultaneously trigger automated and validated alerts to the security team).

Application breadcrumbs

Application breadcrumbs should ideally be broad and varied. Session application breadcrumbs drop tempting SSH, FTD, RDP credentials for would-be attackers. Web browser breadcrumbs create a trail that leads to decoys through history, cookies, stored passwords, and bookmarks. The deceptive illusion comes alive when attackers see expected data.

Conclusion

Intelligent deception takes advantage of the attacker's initial hunt for credentials and connections by creating deceptive breadcrumbs that lead to decoys. Breadcrumbs can take many forms. From cookies to registry values, to emails to files, to ARP table values and beyond – all with fake credentials and fake data that attackers find irresistible.


+ Breadcrumbs must be strategically placed to be effective.

An intelligent deception solution passively scans network traffic and analyzes the applications used on each asset, the communication graphs in the organization, the behavior of assets including internet communication habits, and much more. Using all of this data, intelligent deception solutions can deliver better and automated detection and response with fewer false positives.

Deception solutions are an excellent source for threat intelligence and detecting infected assets inside the organization. Because they interact with attackers, they can monitor attacker activity and track the patterns of the attackers' advance.



Security world



The economic impact of cybercrime? Almost \$600 billion

Cybercrime costs businesses close to \$600 billion, or 0.8 percent of global GDP, which is up from a 2014 study that put global losses at about \$445 billion, according to a report by McAfee, in partnership with the Center for Strategic and International Studies (CSIS).

Adopting new technologies

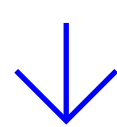
The report attributes the growth over three years to cybercriminals quickly adopting new technologies, the ease of engaging in cybercrime – including an expanding number of cybercrime centers – and the growing financial sophistication of top-tier cybercriminals.

“The digital world has transformed almost every aspect of our lives, including risk and crime, so that crime is more efficient, less risky, more profitable and has never been easier to execute,” said Steve Grobman, CTO for McAfee.

“Consider the use of ransomware, where criminals can outsource much of their work to skilled contractors. Ransomware-as-a-service cloud providers efficiently scale attacks to target millions of systems, and attacks are automated to require minimal human involvement. Add to these factors cryptocurrencies that ease rapid monetization, while minimizing the risk of arrest, and you must sadly conclude that the \$600 billion cybercrime figure reflects the extent to which our technological accomplishments have transformed the criminal economy as dramatically as they have every other portion of our economy,” Grobman added.

Leaders in cybercrime

Banks remain the favorite target of cybercriminals, and nation states are the most dangerous source of cybercrime, the report



finds. Russia, North Korea and Iran are the most active in hacking financial institutions, while China is the most active in cyber espionage.

“Our research bore out the fact that Russia is the leader in cybercrime, reflecting the skill of its hacker community and its disdain for western law enforcement,” said James Lewis, senior VP at CSIS. “North Korea is second in line, as the nation uses cryptocurrency theft to help fund its regime, and we’re now seeing an expanding number of cybercrime centers, including not only North Korea but also Brazil, India and Vietnam.”

Cybercrime around the world

The “Economic Impact of Cybercrime – No Slowing Down” report measures cybercrime in

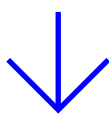
North America, Europe and Central Asia, East Asia and the Pacific, South Asia, Latin America and the Caribbean, Sub-Saharan Africa, and the Middle East and North Africa. Not surprisingly, cybercrime losses are greater in richer countries. However, the countries with the greatest losses (as a percentage of national income) are mid-tier nations that are digitized but not yet fully capable in cybersecurity.

CYBERCRIME	ESTIMATED DAILY ACTIVITY
Malicious scans	80 billion
New malware	300,000
Phishing	33,000
Ransomware	4,000
Records lots of hacking	780,000

What if defenders could see the future? Many clues are out there

Malware sophistication is increasing as adversaries begin to weaponize cloud services and evade detection through encryption, used as a tool to conceal command-and-control activity. To reduce adversaries’ time to operate, security professionals said they will increasingly leverage and spend more on tools that use AI and machine learning, reported in the 11th Cisco 2018 Annual Cybersecurity Report (ACR).

While encryption is meant to enhance security, the expanded volume of encrypted web traffic (50 percent as of October 2017) — both legitimate and malicious — has created more challenges for



defenders trying to identify and monitor potential threats. Cisco threat researchers observed more than a threefold increase in encrypted network communication used by inspected malware samples over a 12-month period.

Applying machine learning can help enhance network security defenses and, over time, “learn” how to automatically detect unusual patterns in encrypted web traffic, cloud, and IoT environments. Some of the 3,600 security professionals interviewed for the Cisco 2018 Security Capabilities Benchmark Study report, stated they were reliant and eager to add tools like machine learning and AI, but were frustrated by the number of false positives such systems generate. While still in its infancy, machine learning and AI technologies over time will mature and learn what is “normal” activity in the network environments they are monitoring.

“Last year’s evolution of malware demonstrates that our adversaries continue to learn,” said John N. Stewart, Senior Vice President and Chief Security and Trust Officer, Cisco. “We have to raise the bar now – top down leadership, business led, technology investments, and practice effective security – there is too much risk, and it is up to us to reduce it.”

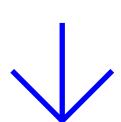
The financial cost of attacks is no longer a hypothetical number

According to study respondents, more than half of all attacks resulted in financial damages of more than US\$500,000, including, but not limited to, lost revenue, customers, opportunities, and out-of-pocket costs.

Supply chain attacks are increasing in velocity, complexity

These attacks can impact computers on a massive scale and can persist for months or even years. Defenders should be aware of the potential risk of using software or hardware from organizations that do not appear to have a responsible security posture.

- Two such attacks in 2017, Nyetya and Ccleaner, infected users by attacking trusted software.
- Defenders should review third-party efficacy testing of security technologies to help reduce the risk of supply chain attacks.



Security is getting more complex, scope of breaches is expanding

Defenders are implementing a complex mix of products from a cross-section of vendors to protect against breaches. This complexity and growth in breaches have many downstream effects on an organization’s ability to defend against attacks, such as increased risk of losses.

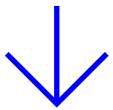
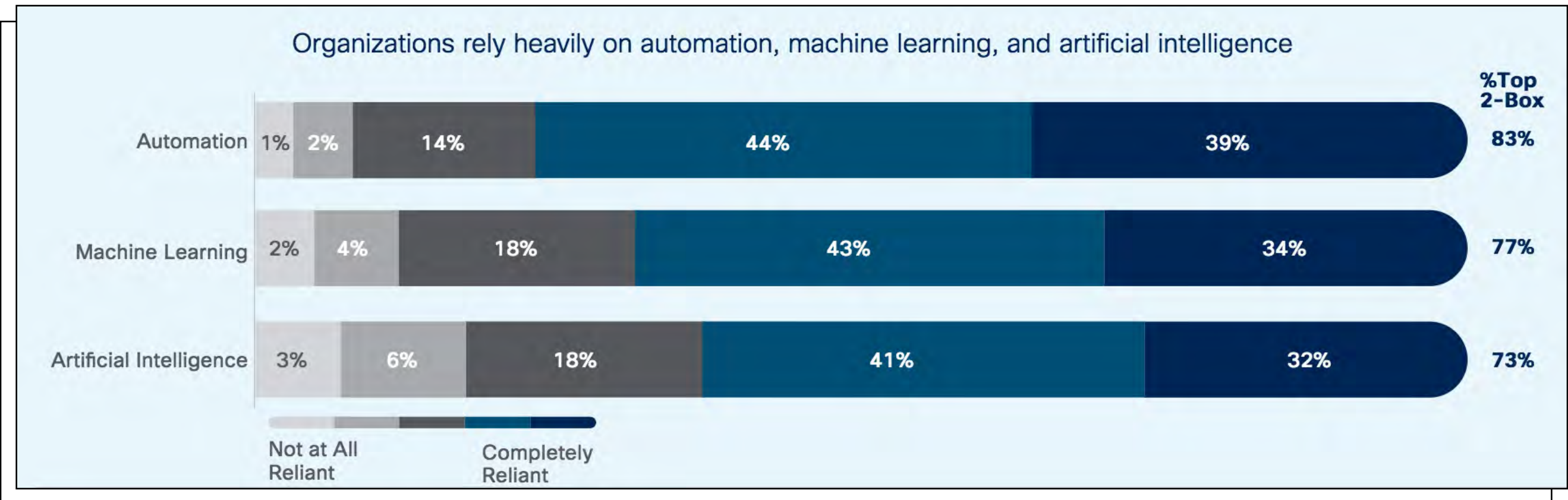
- In 2017, 25% of security professionals said they used products from 11 to 20 vendors, compared with 18 percent of security professionals in 2016.
- Security professionals said 32% of breaches affected more than half of their systems, compared with 15% in 2016

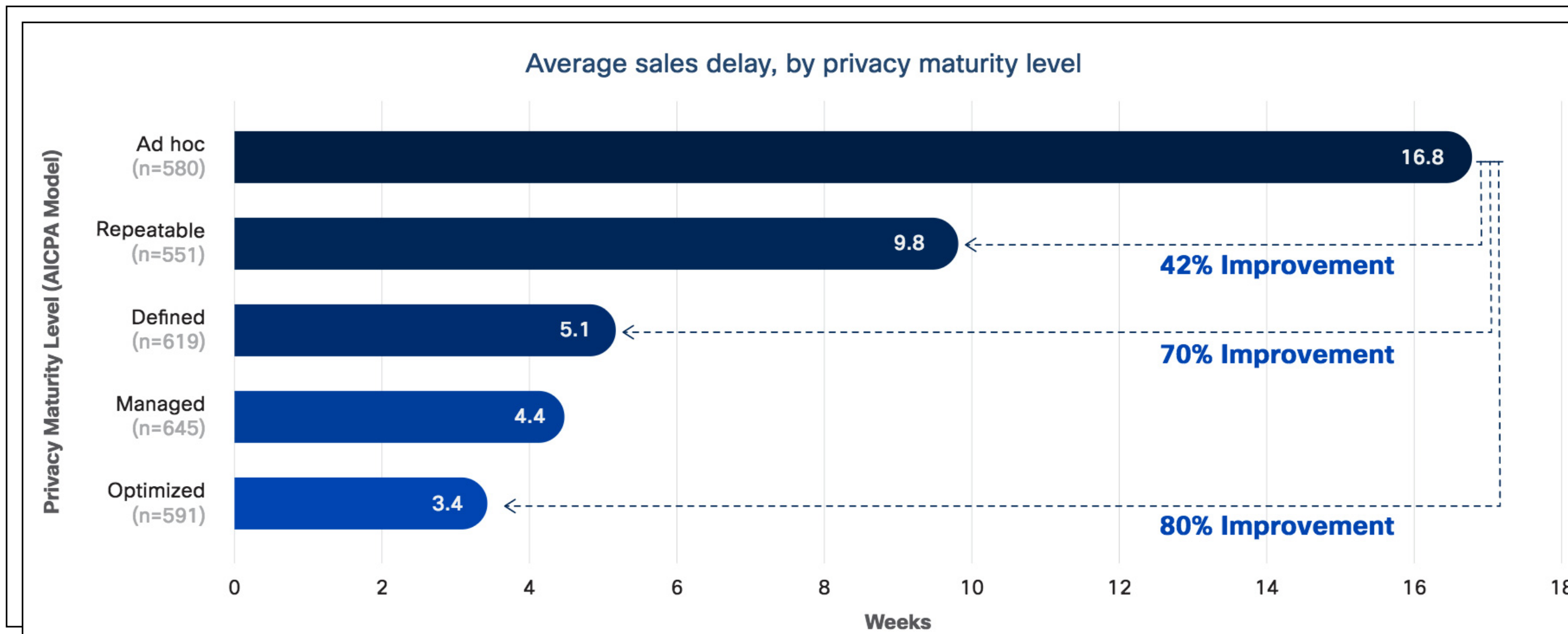
Security pros see value in behavioral analytics tools

92% of security professionals said behavior analytics tools work well. Two-thirds of the healthcare sector, followed by financial services, found behavior analytics to work extremely well to identify malicious actors.

Use of cloud is growing: Attackers taking advantage of the lack of advanced security

- In this year’s study, 27% of security professionals said they are using off-premises private clouds, compared with 20% in 2016
- Among them, 57% said they host networks in the cloud because of better data security; 48%, because of scalability; and 46%, because of ease of use.
- While cloud offers better data security, attackers are taking advantage of the fact that security teams are having difficulty defending evolving and expanding cloud environments. The combination of best practices, advanced security technologies like machine learning, and first-line-of-defense tools like cloud security platforms can help protect this environment.





Trends in malware volume have an impact on defenders' time to detection (TTD)

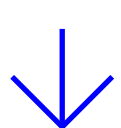
- The Cisco median TTD of about 4.6 hours for the period from November 2016 to October 2017 — well below the 39-hour median TTD reported in November 2015, and the 14-hour median reported in the Cisco 2017 Annual Cybersecurity Report for the period from November 2015 to October 2016.
- The use of cloud-based security technology has been a key factor in helping Cisco to drive and keep its median TTD to a low level. Faster TTD helps defenders move sooner to resolving breaches.

How organizations are confronting escalating third-party cyber risk

Based on in-depth interviews with security executives from 30 participating organizations across multiple industries, RiskRecon revealed how companies are managing the security risks of their complex digital supply chains and sensitive business partnerships.

Researchers identified vendor-neutral capability sets comprising common, emerging, and pioneering practices that firms have implemented to manage third-party security risk.

“Enterprise risk officers are waking up to the reality that their information risk increasingly resides in the systems of their third-



parties, beyond the bounds of their own network. You can outsource your systems and operations to third-parties, but you cannot outsource your risk,” said RiskRecon CEO Kelly White.

The financial services industry is the clear leader

Financial services firms have been actively managing third-party security risk for an average of six and a half years, nearly four years longer than firms in other industries. Financial services firms also are the drivers behind more than 60 percent of the pioneering practices observed in the study.

Third-party security risk management is rapidly innovating

Thirty-two percent of the third-party risk management practices the study identified are implemented by fewer than 25 percent of the study participants. In all cases, these pioneering practices were recently implemented by the adopting firms. The practices leverage objective security data to better understand third-party risk performance and more intelligently allocate and engage risk analysts in assessments.

Pioneering firms are hunting for dangerous conditions in their third-party systems

Twenty-three percent of respondent companies are proactively identifying severe vulnerabilities in their vendors’ systems and working collaboratively with their vendors to quickly address the issues.

Fourth-party awareness is peaking over the horizon

While only seven percent of respondent firms are actively tracking fourth-parties (the third-parties used by their vendors), an additional 33 percent stated that they intend to implement capabilities to better manage fourth-party risk within two years, citing regulatory requirements as the primary driver.

Brian Johnson, a CISO consultant, said, “CISOs know that effective third-party security risk management is essential for protecting their enterprise, yet many lack the data necessary to appropriately understand and prioritize third-party risk exposure. The best thinking on solving risk lies within industry, where practitioners are solving real enterprise risk problems every day.”

Poor communication between CEOs and technical officers leads to misalignment

A misalignment between CEOs and technical officers is weakening enterprise cybersecurity postures, according to Centrify.

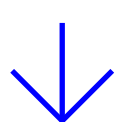
CEOs are incorrectly focused on malware, creating misalignment within the C-suite, which results in undue risk exposure and prevents organizations from effectively stopping breaches. Technical officers (CIOs, CTOs and CISOs) on the front lines of cybersecurity point to identity breaches – including privileged user identity attacks and default, stolen or weak passwords – as the biggest threat, not malware.

As a result, cybersecurity strategies, project priorities, and budget allocations don't always match up with the primary threats nor prepare companies to stop most breaches.

The study – a survey of 800 enterprise executives including CEOs, technical officers, and CFOs – highlights that:

- ▣ 62 percent of CEOs cite malware as the primary threat to cybersecurity, compared with only 35 percent of technical officers.
- ▣ Only 8 percent of all executives stated that anti-malware endpoint security would have prevented the “significant breaches with serious consequences” that they experienced.
- ▣ 68 percent of executives whose companies experienced significant breaches indicate it would most likely have been prevented by either privileged user identity and access management or user identity assurance.

“While the vast majority of CEOs view themselves as the primary owners of their cybersecurity strategies, this report makes a strong argument that companies need to listen more closely to their technical officers,” said Tom Kemp, CEO of Centrify. “It’s clear that the status quo isn’t working. Business leaders need to rethink security with a Zero Trust Security approach that verifies every user, validates their devices, and limits access and privilege.”



Investing in the wrong cybersecurity solutions

The 2017 Data Breach Investigation Report released by Verizon indicates that 81 percent of breaches involve weak, default, or stolen passwords. Identity is the primary attack vector, not malware, yet the report reveals that malware is still the focus point for most CEOs:

- ▣ 60 percent of CEOs invest the most in malware prevention and 93 percent indicate they already feel “well-prepared” for malware risk.
- ▣ 49 percent of CEOs say their companies will substantially reduce malware threats over the next two years, yet only 28 percent of CTOs agree with this statement.

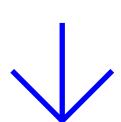
These investment decisions are frequently caused by misplaced confidence in the ability to protect against breaches, putting organizations at significant risk. While technical officers are more aware of the real risks, they are also frustrated by inadequate security budgets, as spending is typically strongly aligned with CEO priorities rather than with actual threats.

Poor communication leads to misalignment

The study also exposed that the disconnect between CEOs and technical officers leads to misaligned security strategies, and tension among executives.

- ▣ 81 percent of CEOs say they are most accountable for their organizations’ cybersecurity strategies, while 78 percent of technical officers make the same ownership claim.
- ▣ Only 55 percent of CEOs say their organization has experienced a breach, whereas 79 percent of CTOs acknowledge they’ve been breached. This indicates that 24 percent of CEOs are not aware that they have experienced a breach.

“The traditional security model of using well-defined perimeters between ‘trusted’ corporate insiders and ‘untrusted outsiders’ to protect assets has evolved with the advent of cloud, mobile and IoT. Yet most enterprises continue to prioritize spending on traditional security tools and approaches,” said Garrett Bekker, Principal Security Analyst at 451 Research. “Centrify’s research reveals that a primary reason for conflicting cybersecurity strategies and spending is that C-level executives and technical managers don’t always see eye-to-eye regarding security priorities, and a misaligned C-Suite can put



the organization at risk. Modern organizations need to rethink their approach and adopt a framework that relies on verifying identity rather than location as the primary means of controlling access to applications, endpoints and infrastructure.”

Outdated thinking results in higher risk

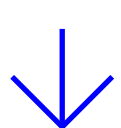
CEOs also expressed frustration with security technologies that have a poor user experience and cause their employees to lose productivity. 62 percent of CEOs state that multi-factor authentication (MFA) is difficult to manage and is not user-friendly, while only 41 percent of technical officers agree with this assessment.

This outdated perception has been resolved by significant innovation by identity security vendors in areas such as machine learning. These advances have substantially reduced the burden of deploying and managing authentication solutions and improved the user experience for a range of security technologies.

Still relying solely on CVE and NVD for vulnerability tracking? Bad idea

2017 broke the previous all-time record for the highest number of reported vulnerabilities. The 20,832 vulnerabilities cataloged during 2017 by Risk Based Security (VulnDB) eclipsed the total covered by MITRE’s Common Vulnerability Enumeration (CVE) and the National Vulnerability Database (NVD) by more than 7,900.

“Incredibly, we see too many companies still relying on CVE and NVD for vulnerability tracking, despite the US government funded organization falling short year after year. While some argue that the CVE/NVD solution is ‘good enough’, that simply isn’t the case. Just look at the number of web and computer hacking data breaches reported on a regular basis. In addition to a false sense of security, the ‘good enough’ mindset often leads some to believe that the



important vulnerabilities are covered, and that isn't the case either", said Brian Martin, VP of Vulnerability Intelligence for Risk Based Security.

In fact, the 7,900 vulnerabilities published by VulnDB in 2017 that are not found in CVE/NVD, impact prevalent products that are used in all sizes of organizations. While the number of CVE assignments continue to rise, the actual coverage still lags behind.

Of the more than 18,000 CVE IDs that were assigned or allotted to CVE Numbering Authorities (CNAs), almost seven thousand were in RESERVED status despite 1,342 of them having a public disclosure. This seems to indicate that MITRE is more focused on assigning and increasing the number of IDs, and not ensuring the quality of data.

39.3% of reported vulnerabilities received CVSS scores above 7.0. This means that not only has the number of vulnerabilities been increasing, but the

CVSS scores are also trending higher over the last five years. In 2017, web-related issues accounted for over half of all vulnerabilities disclosed, 31.5% had public exploits, and 24.1% had no solution at the time of the report.

While relationships between researchers and vendors can at times appear strained, they are continuing to attempt to work together. Vulnerabilities disclosed in a coordinated fashion with vendors was relatively consistent at 44.8%, compared to 45.6% in 2016.

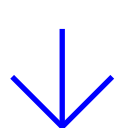
"From operating systems and software installed on client and server systems to IoT and SCADA devices, vulnerabilities continue to be a major concern. Using metrics to help determine which vendors and products are putting your organization at risk needs to be a key part of your vendor risk management and procurement process.", says Carsten Eiram, Chief Research Officer.

Global cyber risk perception: Highest management priorities

Few organizations are highly confident in their ability to manage the risk of a cyber-attack, despite viewing cybersecurity as a top risk management priority, according to a survey conducted by Marsh and Microsoft.

Cybersecurity confidence

In the global survey of more than 1,300 senior executives, two-thirds ranked cybersecurity among their organizations' top five risk management priorities – approximately double the response to a similar question Marsh asked in 2016.



The survey also found that a vast majority – 75% – identified business interruption as the cyber loss scenario with the greatest potential to impact their organization. This compares to 55% who cited breach of customer information, which has historically been the focus for organizations.

Despite this growing awareness and rising concern, only 19% of respondents said they are highly confident in their organization's ability to mitigate and respond to a cyber event. Moreover, only 30% said they have developed a plan to respond to cyber-attacks.

“Cyber risk is an escalating management priority as the use of technology in business increases and the threat environment gets more complex,” said John Drzik, president Global Risk and Digital, Marsh. “It’s time for organizations to adopt a more comprehensive approach to cyber resilience, which engages the full executive team and spans risk prevention, response, mitigation and transfer.”

Risk quantification

An important step toward this goal is risk quantification. According to the survey, fewer than 50% of respondents said their organization estimates financial losses from a potential cyber event and, of those that do, only 11% make their estimates in economic terms. Such calculations are a key step in helping boards and others develop strategic plans and investment decisions, including those related to cyber insurance purchase, the report notes.

At the same time, responsibility for cyber risk management continues to lie primarily with the IT department, with inconsistent involvement of other stakeholders across the enterprise. According to the survey, 70% of respondents pointed to IT as a primary owner and decision-maker for cyber risk management, compared to just 37% who cited the president/CEO or the board of directors, and 32% who cited the risk management function.

“While technology is the foundation of any good cybersecurity strategy, companies can benefit from investing in non-technology solutions like risk management as part of a holistic approach,” said Matt Penarczyk, vice president and deputy general counsel, Microsoft. “Through advanced technology, tools and training, for example, companies can better protect the data in their networks and be ready for the business interruptions and reputational risks associated with cyberattacks.”

Financial services firms most adept at making balanced security investments

Cyber attacks cost financial services firms more to address and contain than in any other industry, and the rate of breaches in the industry has tripled over the past five years, according to a study conducted by the Ponemon Institute.

Cost of cyber crime

The report, Cost of Cyber Crime Study, examines the costs that organizations incur when responding to cybercrime incidents and applies a costing methodology that allows year-over-year comparisons.

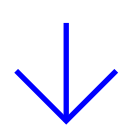
It found that the average cost of cybercrime for financial services companies globally has increased by more than 40 percent over the past three years, from \$12.97 million per firm in 2014 to \$18.28 million in 2017 – significantly higher than the average cost of \$11.7 million per firm across all industries included in the study. The analysis focuses on the direct costs of the incidents and does not include the longer-term costs of remediation.

Spending on advanced solutions

The report also notes while cyberattacks have a greater financial impact on the financial services industry than on any other industry, financial services firms continue to make prudent and sophisticated security technology investments that contribute to reducing the cost of breaches significantly.

The greatest proportion of financial services firms' cyberdefense spending is for more advanced solutions like security intelligence systems, followed by automation, orchestration and machine-learning technologies.

"While the cost of cybercrime for financial services companies continues to rise, our research found that these companies have considerably more balanced and appropriate spending levels on key security technologies to combat sophisticated attacks than do those in other industries," said Chris Thompson, a senior managing



director at Accenture who leads financial services security and resilience in the company's Security practice. "This is particularly true with regard to the use of automation, artificial intelligence and machine learning technologies, which could be critical to future cybersecurity efforts."

Key findings for the financial services industry

- The average number of breaches per company has more than tripled over the past five years, from 40 in 2012 to 125 in 2017; that is slightly below the global average of 130 across all industries.
- Nearly two-thirds (60 percent) of financial services companies' total security costs is spent on containment and detection of breaches.
- The greatest impact of cyberbreaches on financial services firms are business disruption and information loss, which together account for 87 percent of the cost to respond to cybercrime incidents, with revenue loss accounting for only 13 percent

The insider threat

More can be done with regards to security technologies deployed in financial services. Only one-quarter (26 percent) of financial services companies have actually deployed AI security technologies, and fewer than one-third (31 percent) use advanced analytics to fight cybercrime.

At the same time, financial services firms appear to be less affected than other industries by more-common forms of cyberattacks. While 2017 saw a string of malware attacks – including the WannaCry and Petya attacks, which cost several global firms hundreds of millions of dollars in lost revenues – malware attacks were among the least costly types of cyberattacks for financial services companies.

The costliest types of attacks for banks and insurers are denial of services, phishing and social engineering, and malicious insiders.

"Banks and other financial services firms have implemented advanced solutions for malware, reducing the susceptibility to such attacks, so the cybercrimes they're currently grappling with are largely different from those affecting other industries," Thompson said. "One such threat is identifying bad actors within their own organization and figuring out the right combination of human effort with technologies to combat this growing issue. One thing is certain, however: When it comes to fighting cybercrime, organizations can't hire their way out of this issue, as there simply aren't enough talented cyber professionals out there."

Expected changes in IT/OT convergence and industrial security

AUTHOR_ David Hatchell, Vice President of Industrial Security, ProtectWise

Ten years ago, I was brought into the industrial security arena by a top company executive in who was convinced that we needed traditional endpoint protection on smart meters. I had spent fifteen years before that in enterprise security, so it took a while to shape my focus around the nature of the problem of IT/OT convergence and industrial security.

I have had the pleasure of being on both sides of the fence — from a major IT security provider building major partnerships with automation vendors, to specifically working at an automation networking company developing a major security practice.

+ I'm a firm believer that we can have a world with basic security hygiene across all verticals within critical infrastructure.

Over the past year, we have seen a continued cross-pollination: IT security staff trying to step



on the plant floor and plant teams trying to understand IT security. At an oil and gas security conference I attended last fall, a full 40 percent of the people were from the OT side, and a full 50 percent of those people were involved in running the operations of a plant. This shift means that IT security has become imperative for ICS environments, and that we can expect a lot of change. Here are four areas in which I believe we'll see most of it:

Unified visibility, detection and response across industrial environments

Over the past few years, we have witnessed the second wave of industrial security companies advancing visibility in industrial environments above the traditional detective controls of patching, endpoint security and so forth. Pressured by the Board, CISOs and CIOs are rushing to deploy SOMETHING to provide visibility, while

pushing their plan to “do no harm” to operational environments and avoiding impacting production.

We will see more industry testing of these approaches, further validation of claims from these solution providers, and companies sharing their success stories about large global deployments. One of the key issues to monitor is how a company sets up its IT security operations center (SOC) and process control network (PCN) teams to rapidly collect information from the plants, visualize the traffic, and provide meaningful analysis back to the plant operators.

Increased intentional and unintentional attacks impacting ICS

We started out 2018 with Trisis/Triton, which demonstrated the unintentional exploit of a safety system. Last year WannaCry exposed one of the core problems in industrial environments — legacy unpatched servers — with a full-fledged ransomware attack.

CrashOverride showed how a sophisticated attacker can build a modular malware framework for substation environments, to thoroughly disrupt an industrial process by exploiting the critical industrial protocols used between the control and operational functions of a plant. Despite our heightened awareness, this combination of sophistication, exposure of basic defenses, and reliance on security by obscurity will continue throughout 2018.

Security offerings and support of security solutions will continue to increase

Since Stuxnet, automation vendors have struggled to fix their product vulnerabilities. They provide their customers a security offering which will protect not just their systems, but also protect a heterogeneous plant environment. IIoT Services like GE Predix and Siemens MindSphere, which are

based on cloud-connected data-driven services, further compound this issue.

End users are trying to rely on manufacturers to provide security controls or some level of testing and assurance that their security solutions will not impact plant uptime. In 2018, I see automation vendors combining security service offerings with cloud offerings to help address these issues. Furthermore, due to customer demand for network visibility, some forward-thinking vendors will provide visibility into their networks and configurations to better allow security tools to monitor their environments properly.

The need for an IT/OT security specific skill set will become a significant issue

The cybersecurity industry is projected to reach 1.8 million unfilled roles by 2020. The added complexities of a converged IT/OT security environment could amplify perceived barriers to entry, as organizations struggle to manage the aging workforce of their plant teams with the Millennial generation of new cybersecurity talent.

+ The industry will be forced to find solutions for tapping talent by leveraging technologies that make it possible to attract, upskill and retain the next generation of security staff.

One approach is to introduce highly immersive tools including 4-D imagery, virtual reality, and augmented or mixed reality — much like the environments in which the Minecraft generation grew up. The good news is that the ICS industry already uses immersive data visualization to discover oil in the subsurface, so adoption on the security side of the house is not far-fetched. Organizations who leverage their talent pool and industry education to build security leaders of tomorrow will be in a good position to address the problem.

HITBSecConf2018 - Amsterdam

April 9th - 13th <https://conference.hitb.org/>

9th, 10th & 11th April: Hands-On Technical Trainings

TRAINING 1 – The ARM Exploit Laboratory

TRAINING 2 – Modern Malware Warfare: Basics, Delivery, and Advanced Analysis

TRAINING 3 – Making & Breaking Machine Learning Systems

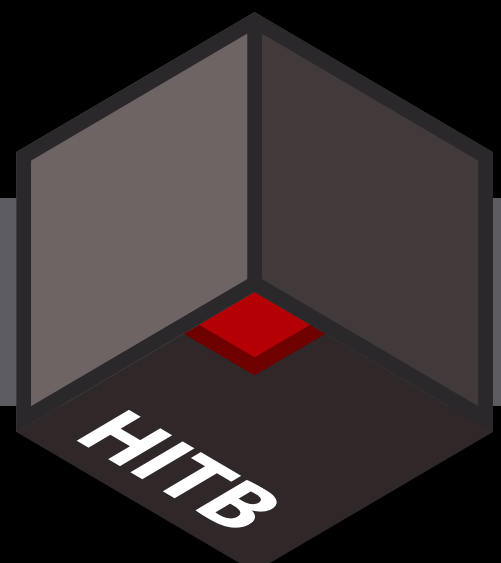
TRAINING 4 – Source Code Auditing Like a Ninja

TRAINING 5 – Pentesting & Exploiting Highly Secured Enterprise Networks

TRAINING 6 – Out Of The Blue: Attacking BLE, NFC, HCE and More

TRAINING 7 – Mastering Burp Suite Pro: 100% Hands-On

12th & 13th April: Quad Track Conference + Industry Exhibition



The 9th Annual HITB Security Conference in The Netherlands



Let's face it – artificial intelligence (AI) and machine learning (ML) have become two more buzzwords in the cybersecurity industry.

This isn't to say that these technologies aren't valuable. There's little doubt that machine learning is having a significant impact in many industries, and is recognizable in virtual assistants such as Amazon's Alexa and Apple's Siri and in-car driving automation features already in production. Facebook also does a pretty good job of recognizing people in photos by using machine learning algorithms.

The same technology is now being embedded in security products to detect previously unknown or undetectable threats. This is a noble goal and unquestionably the right direction for the industry.

List-based detection techniques, i.e., those that depend on the continuous cataloging of known threats, have had a long run in protecting computers

Testing machine learning products requires a new approach

AUTHOR_Anup Ghosh, Chief Strategist,
Next Gen Endpoint, Sophos

and networks. As good as they are at detecting threats, and as powerfully as cloud-based sharing of known threats among subscriber devices has scaled this approach, we know they are fundamentally limited by changes in the adversarial model where cyber adversaries no longer re-use their malware.

+ Today malware factory kits churn out effectively infinite permutations of malware to defeat list-based approaches.

One side effect of this is that the resulting malware tends to share the same “malware DNA,” and it is largely distinct from that of benign programs. This combination of massive data sets and strong similarity among malware variants makes machine learning techniques a good solution for the problem of malware detection.

On the other hand, in cases where this combination of large data sets and regular data does not exist, machine learning technology is not that helpful.

Unfortunately, the marketing machine makes it difficult to separate the wheat from the chaff, to identify the real deal from the pretenders. This is where third-party test organizations come in: they can produce fair test results that reflect real-world performance of products.

Don't try this at home

Many enterprises test the security products they intend to purchase. While this sounds like a reasonable buyer's due diligence strategy, most organizations don't have the resources or expertise to do it properly. The result is inadequate testing that leads to poor decision-making.

Testing security products requires not only software testing expertise with a scientific background (as opposed to only IT networking), but also special

test harnesses, malware safety controls and sandboxes, large data sets of malware (known and new), exploits, and benign software. These requirements are typically beyond the reach of most organizations and, to fill this expertise gap, third-party test organizations have emerged as a viable business segment.

Vendors often find themselves at odds with these test companies, particularly when their product results are less than stellar. In part, this conflict drove the development of testing standards and test standard organizations as a cooperative venture of test organizations, which typically represent the interests of both the security buyers and vendors.

+ The Anti-Malware Test Standards Organization (AMTSO) today sets standards for adequate testing of anti-malware products, to be adopted by third-party test organizations or anyone who aspires to test well.

The organization's work is important to ensure test practices are standardized across testing organizations, as well as for maintaining quality and consistency to assure the integrity of their work. In theory, if a test organization follows AMTSO's methodology guidance, the test results can be trusted.

Specialized knowledge required

While testing standards and test bodies are a welcome development for all concerned, testing parties and their standards bodies need to keep pace with the continued march of technology.

Security test organizations were born in the era of list-based antivirus products. Not surprisingly, today's test standards reflect traditional AV testing.

To many professionals, testing is a black box exercise: give me a box with a set of claims, provide

a set of test cases, and measure the outputs. The tests are agnostic as to what technology powers the box. This view represents the most basic needs of buyers, i.e., does the product work?

However, the basic input/output black box view of testing falls short when it comes to highlighting and differentiating fundamental attributes of machine learning.

For instance:

- ▣ Can a solution detect known threats but also generalize or “learn” to identify new threats?
- ▣ How do tunable thresholds in a machine learning product affect its performance in terms of true detections versus false positives?
- ▣ How well does the model age, i.e., how often must it be updated?
- ▣ What are the characteristics of the data sets on which an ML implementation was trained on and, by extension, how robust will that trained model be to different real-world data sets? Not only how sizeable is the training data, but how was it sourced/curated, and how diversified is it?
- ▣ “Time to learn” is a crucial metric in today’s ML-based products. Should this be evaluated and reported on? Is learning conducted on customer premises or in a lab?
- ▣ Should “time to detect/protect against threats” be metrics that enterprises look for in these security products?
- ▣ What are the hardware and network footprint requirements of a solution? Must it be connected to a network? Can it be run in memory on a standard machine or is cloud-based look-up required?
- ▣ How much manual configuration (or human footprint) is required to configure and manage a solution?
- ▣ Are tests manual or automated?
- ▣ Are test cases numbered in the tens or hundreds or millions?

In machine learning, the data sets on which a model is trained are as important as the model itself. To test the ability of a model to generalize from what it’s trained on, a solution must be subjected to test cases it has not seen before (on a device or in the cloud). Likewise, if an ML model needs updating on a daily or near-daily basis, then there is little benefit to that over-fitted model compared to list-based techniques.

Finally, for a test to be statistically valid, it must have a sufficient sample size - cases should number in the millions.

An outlier in a sample of 100 test cases can have a disproportionate impact on results, and that would not be the case in a sample size of 1 million.

Effective measures of performance

Data scientists have developed protocols to test their solutions out of the necessity to measure and improve their algorithms. One common testing protocol involves separating data sets into training data and a reserve set for testing. The performance is then measured and the training/testing process is repeated with different training and reserve sets. The process is repeated multiple times, to average out anomalies between testing and training data.

Likewise, time-based testing (aka time-splitting) is essential to measure the ability of a model to generalize to real-world threats, and also to measure its decay function. This involves freezing a trained model at a point in time (e.g., March 1), testing it against real-world test cases at that time, then continuing to test the model frozen in time at future points in time (e.g., April 1, May 1, June 1, and so on).

Different organizations have different operational requirements when it comes to sensors and detectors, and therefore most ML algorithms are tunable. By changing a threshold parameter,

an ML algorithm can achieve very high rates of detection (with potentially high false positive rates) or can minimize false positives to negligible with a commensurate reduction in detections.

The data science research community often uses Receiver Operating Characteristic (ROC) curves to measure the performance of a detector as a function of correct detections versus false positives across a range of operating points.

This is perhaps the best measure of detection performance for a given solution. It allows buyers to specify things like “If I can tolerate five false positives a day, which may translate to 0.01% false positive rate, what is the level of detection I can expect?” Another enterprise may be willing to tolerate a 0.1% false positive rate to achieve much higher detection rates. In comparing solutions, these curves (superimposed on the same graph) provide the most scientific and objective measure of detection and false positive performance, which matters in the real world.

Building on previous work

Standards bodies like AMTSO have done much to standardize and improve testing in what is still a nascent industry. Also, the representation from industry and test organizations on the governing body will ensure it continues to update its testing standards as technology advances.

To be clear: many ML products today can be tested with existing and legacy testing regimes, i.e., the black box input/output approach to testing. But you cannot obtain a valid measure of machine learning-based approaches with traditional testing regimes.

To underscore what differentiates ML-based products from traditional list-based techniques we need to incorporate testing approaches for ML that are well established from data science.

This will allow us to separate companies that can innovate via machine learning from those that are re-packaging old technology in a new ML wrapper. It will also provide buyers scientific evidence of how well an ML-based product can address real-world threats given adequate data sets and a scientific approach to testing.

A visual metaphor would be a low-resolution image compared to an HD image: you cannot get a high fidelity view of machine learning with a traditional approach to testing. For example, testing with small sample sizes (e.g., hundreds of URLs/PEs instead of millions) - as is often the case in traditional testing - simply cannot provide a statistically valid estimate of the actual detection capabilities of an ML solution.

Likewise, a discussion of detection performance without its corresponding false positive rate is nonsensical and a sure sign of lack of scientific rigor. Additionally, to understand an ML algorithm’s performance, a ROC curve analysis is essential for buyers to understand how a solution will likely perform in their network according to their operational requirements.

+ Finally, one point almost all vendors, buyers, and test organizations agree on is that testing should reflect real-world performance.

Testing procedures need more than just large data sets: they need ones that are curated from real-world threats (as opposed to manufactured/mutated).

Time-based testing can address not this requirement, but can also be used to measure the decay rate of models over time - a real-world concern in many cases.



Malware world

When crypto-mining malware hits a SCADA network

Stealthy crypto-mining is on track to surpass ransomware as cybercriminals' most favorite money-making option, and companies with computers and servers that run all day and night long are the preferred targets.

Industrial cybersecurity vendor Radiflow company has recently discovered Monero-mining malware on five servers of a water utility company located in Europe. These servers included the HMI (Human Machine Interface), which was also the control server of the physical processes of the company.

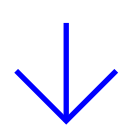
"These PCs had some indirect connectivity to the Internet for remote monitoring," Yehonatan Kfir, CTO at Radiflow, explained. "It seems that one of these was wrongly used for browsing to a site with the malware and from there it was spread to the internal network to several other servers."

The company discovered the attack as part of a routine and ongoing monitoring of the OT network of the water utility customer.

Its industrial intrusion detection system raised the alarm after identifying several abnormalities, including unexpected HTTP communication attempts with suspicious IP addresses and changes to the topology of the customer's OT network (from a tree-like topology that is typical for SCADA networks to a more star-like topology where several servers communicating with many external IP addresses of crypto miner pools).

"As an immediate mitigation, the entire site was disconnected from the Internet," Kfir shared. "We will design the improved setup in a few days, but it will likely include improved firewalling on the Internet link and better segmentation inside the site."

Luckily, the operation of the utility wasn't affected but had the



malware been ransomware the attack could likely have had more of a negative impact on business operations.

Crypto-mining malware attacks are a serious problem

“Cryptocurrency malware attacks involve extremely high CPU processing and network bandwidth consumption, which can threaten the stability and availability of the physical processes of a critical infrastructure operator,” Kfir noted.

“While it is known that ransomware attacks have been launched on OT networks, this new case of a cryptocurrency malware attack on an OT network poses a new threat as it runs in stealth mode and can remain undetected over time.”

This particular instance of crypto-mining malware was also designed to disable security tools on the target systems to operate undetected. But, in general, PCs in an OT network run sensitive HMI and SCADA applications that cannot get the latest Windows, antivirus and other critical updates and will always be vulnerable to malware attacks, Kir pointed out.

Radiflow CEO Ilan Barda said that given the attractiveness of cryptocurrency mining and its increasing need for processing power, they would not be surprised to see such attacks on other OT networks.

“This case emphasizes the need for a holistic cybersecurity solution for OT networks, including access control, intrusion detection and analytics services with the relevant expertise,” he added.

For the moment, this seems like a non-targeted attack that hit as part of a broader search for online resources. Still, the company’s research team is still in the middle of a more in-depth analysis of the overall site activity, and they might change their assumption about the specific targeting.

They are also still investigating the cause of the infection, to discover which vulnerability (if any) was exploited to install the crypto-mining malware. Local regulatory authorities have also been informed of the incident and are cooperating in the investigation.

Thousands of government, orgs' websites found serving crypto mining script

On a weekend in early February, over 4,200 websites around the world started hijacking visitors' browsers to mine the Monero crypto currency.

Among the compromised websites were that of UK's Information Commissioner's Office and the Financial Ombudsman Service, the US Courts information portal, Manchester's city council, the City University of New York, the Indiana state government, the Swedish Police, and so on.

The problem was first noticed by security researcher Scott Helme, and it didn't take him long to pinpoint the source of the compromise: Browsealoud, a service run by a UK-based firm Texthelp.

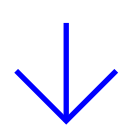
The company serves a JavaScript that "adds speech, reading, and translation to websites facilitating access and participation for people with Dyslexia, Low Literacy, English as a Second Language, and those with mild visual impairments."

Apparently, the company's script server was hacked, and the attackers added another obfuscated script to the Browsealoud one. Its sole aim was to exploit visitors' computers' processing power, and the hackers tried to keep the crypto-mining operation unnoticeable by limiting the amount of processing power that the crypto mining effort used.

Texthelp reacts

Texthelp CTO and Data Security Officer Martin McKay confirmed the breach later that same day, as well as that the script was only meant to mine crypto coins, not steal user data.

"In light of other recent cyber attacks all over the world, we have been preparing for such an incident for the last year and our data security action plan was actioned straight away," he said.



“Texthelp has in place continuous automated security tests for Browsealoud, and these detected the modified file and as a result, the product was taken offline. This removed Browsealoud from all our customer sites immediately, addressing the security risk without our customers having to take any action.”

The Browsealoud service was temporarily taken offline so that Texthelp customers would notice and learn about the issue and the company’s response plan.

Victims’ browsers were “set free” as soon as they closed the windows or tabs in which one of the compromised sites was opened.

Protection against future attacks

For sites depending on third party scripts for some of their functionalities, Helme advised using a technique called SRI (Subresource Integrity), which allows websites to instruct the browser to perform an integrity check on an asset loaded from a 3rd party.

Texthelp ultimately heeded the advice.

Two weeks after the breach, McKay announced that no customer data was accessed or lost as a result of it, and that they have redesigned their threat response process to be faster.

He also shared that the company:

- ▣ Performed an internal security review on all AWS resources
- ▣ Engaged a 3rd party to perform a penetration test to provide independent validation of the security status of Browsealoud
- ▣ Has deployed an improved threat detection script with an automated take down facility if the Browsealoud script has been tampered with
- ▣ Has implemented a second factor authentication to prevent any script changes being published without two Texthelp staff members separately approving the update, and
- ▣ Has implemented versioning with Subresource Integrity.

Dridex gang follows trends, also created FriedEx ransomware

The gang behind the infamous banking Trojan Dridex has also created the FriedEx (aka BitPaymer) ransomware, ESET researchers confidently claim.

The similarities between Dridex and FriedEx

- By analyzing and comparing the code of both threats, the researchers discovered a handful of similarities:
- Both malware use the same function for generating UserID (i.e., that generates a unique string from several attributes of the victim’s machine)
- Most of the other functions that correspond to the specific malware functionalities are the same and are listed in the same order in the binaries
- The two threats use the same malware packer
- The PDB (Program Database) paths included in the analyzed malware binaries are the same (and unique to the Dridex and FriedEx projects).
- Several Dridex and FriedEx samples have the same date of compilation (with time differences of several minutes at most) and consistent randomly generated constants (which means that the samples were probably built during the same compilation session).
- Malware binaries of both threats are compiled in Visual Studio 2015.

An active group

This discovery points to the group being active on multiple fronts: they consistently update the banking malware (a new code injection technique that makes it easier to avoid AV detection, a new MS Word zero-day exploit to help the malware spread), but also follow the latest malware trends and participate in them (they created their own ransomware).

FriedEx was first detected in July 2017, concentrates on higher profile targets (companies), and is usually delivered via an RDP brute force attack. Dridex first appeared in 2014. The Dridex botnet has had its ups and downs during the years, but continues to chug along.

Dridex loader 2017-09-07

```

int __fastcall GetAPIByHash(LIB_HASHES a1, FUNC_HASHES a2)
{
    FUNC_HASHES v2; // edi
    LIB_HASHES v3; // esi
    int result; // eax
    int v5; // eax

    v2 = a2;
    v3 = a1;
    result = GetAPIByHash_Fast(a2);
    if ( !result )
    {
        if ( v3 != 0xA8A28E83 )
            && ((v5 = FindDLLByHash(v3)) != 0 )
            || LoadDLLByHash(v3)
            && (v5 = FindDLLByHash(v3)) != 0 )
        {
            result = GetProcByHash(v5, v2);
        }
        else
        {
            result = 0;
        }
    }
    return result;
}
Machine Intel1386
Thu Sep 07 17:57:41 2017
Magic optional header 0100

```

FriedEx 2017-09-07

```

int __fastcall GetAPIByHash(LIB_HASHES a1, FUNC_HASHES a2)
{
    FUNC_HASHES v2; // edi
    LIB_HASHES v3; // esi
    int result; // eax
    int v5; // eax

    v2 = a2;
    v3 = a1;
    result = GetAPIByHash_Fast(a2);
    if ( !result )
    {
        if ( v3 != 0xA8A28E83 )
            && ((v5 = FindDLLByHash(v3)) != 0 )
            || LoadDLLByHash(v3)
            && (v5 = FindDLLByHash(v3)) != 0 )
        {
            result = GetProcByHash(v5, v2);
        }
        else
        {
            result = 0;
        }
    }
    return result;
}
Machine Intel1386
Thu Sep 07 17:59:17 2017
Magic optional header 0100

```

“With all this evidence, we confidently claim that FriedEx is indeed the work of the Dridex developers,” the researchers noted.

Why do we need a risk-based approach to authentication?

AUTHOR Ruoting Sun, Head of Technology Partnerships, Duo Security

20 years ago, everyone worked at a desktop workstation hardwired into an office building. This made network security simple and organizations felt they could depend on the time-tested method of the trusted perimeter. Firewalls were relied on to keep out external threats, and anything within the network was considered secure and safe.

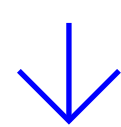
Today, however, the number of variables has skyrocketed. The move to the cloud, BYOD, and increased use of outside contractors means a legitimate user could now be logging into the network from anywhere in the world, at any time, and from a vast array of devices.

The idea of the trusted perimeter has become increasingly untenable and users routinely bypass the corporate network altogether with cloud-based applications. This has been further complicated by most users having two or three devices, as well as the increasing presence of IoT-

enabled devices on the network. It's also clear that cyber attackers have long since moved beyond the secure perimeter; if they gain access to the network through an employee's credentials they can often move about unrestricted.

+ But where there are challenges, there is also tremendous opportunity.

On the leading edge of the "zero trust" movement is Google's BeyondCorp framework. This is a security model designed to grant access to applications based on the trustworthiness of the user and the device. The user needs to have an endpoint that has been inspected for security vulnerabilities and then must pass authentication requests.



Accounting for risk

The biggest challenge for an enterprise seeking to adopt a more nuanced approach to authentication is the sheer number of variables that must be accounted for in each and every request. As a result, we've seen a shift in demand towards risk-based, adaptive authentication, which is able to account for all these variables and apply a customised access policy based on each situation.

In some cases, risk levels and the resulting access policies are obvious: an access request for customer records outside of business hours made by an unknown device in Jakarta (where the enterprise doesn't operate) is clearly suspicious and should be presented with very strict policies.

This means that the older static, rules-based approach to authentication is no longer feasible, and organizations cannot simply work in absolutes of allowing access or blocking the user entirely.

Instead, we need to look at the attributes of the user; what system they're accessing and device they're using, and what they're doing, and make an authentication decision based on these attributes.

Depending on the risk profile, organizations could add an additional authentication method, or a more secure one, before allowing access.

Balancing automation and control

+ The biggest challenge for an enterprise seeking to take on adaptive authentication is from an administrative perspective.

Enterprises need to be able to ensure that all the disparate policies are applied and enforced

accurately and smoothly if they are to make a BeyondCorp-style perimeter-less strategy work.

As with many other areas of IT security, automation provides a solution to the problem here. Having a system that is able to create a unique access policy for each user profile based on their specific attributes and presents appropriate authentication requirements will ensure that legitimate users are able to fulfil their needs quickly and won't be needlessly locked out.

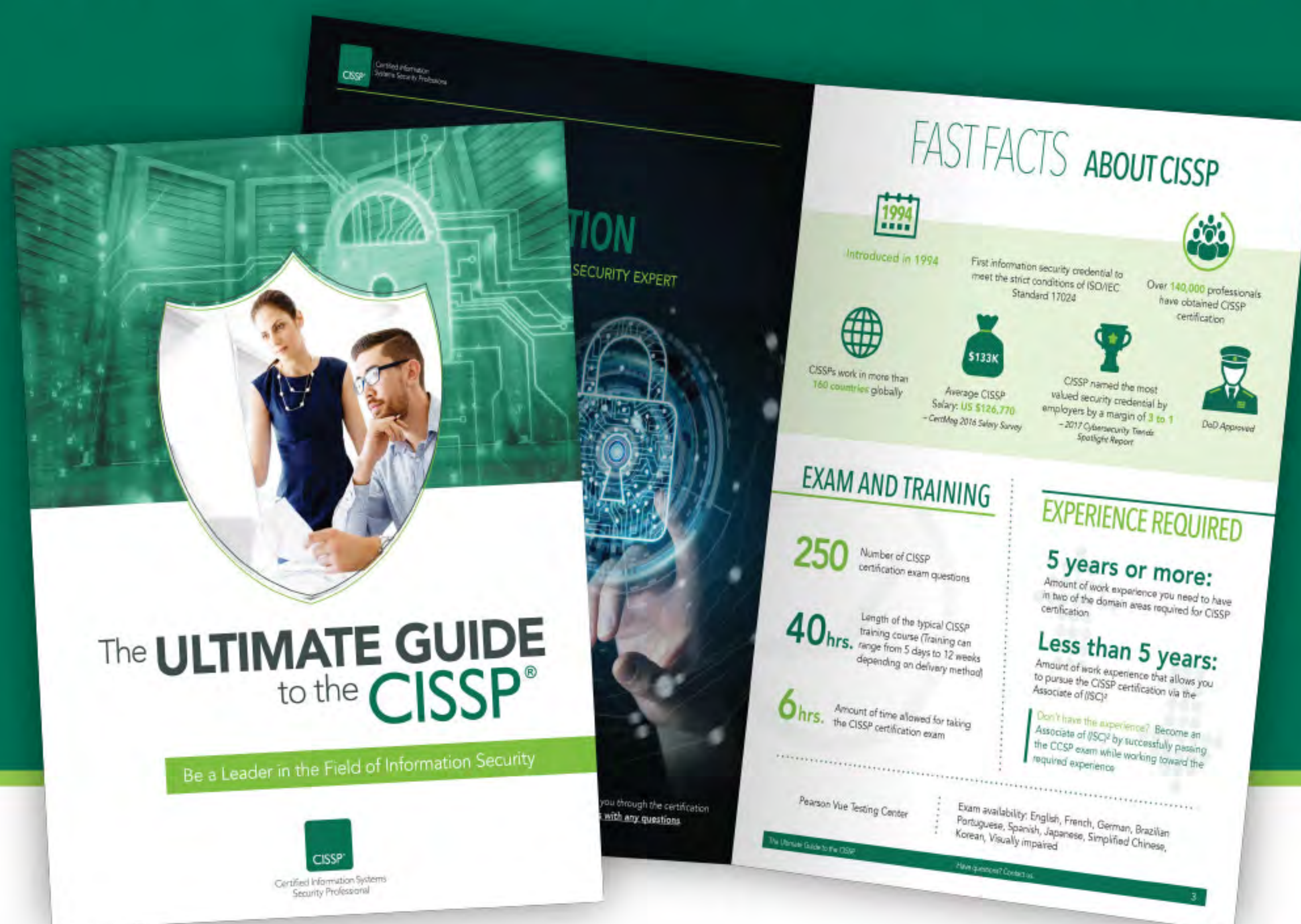
However, there is a tendency to rely too heavily on the automated approach, which can be risky because it takes the ability to make granular decisions away from the administrator. Reducing accessibility for admins can make them less likely to use the tools, because they don't have the chance to get to grips with how they work. Similarly, if end users feel too restricted by an automated system they will be more likely to find workarounds, which increases the risk of a security incident.

Instead, we believe there needs to be a balance between automation, granular control for admins, and usability for end users. Also, providing the right level of granularity for administrators while automating the simple mundane tasks means they can focus on higher value activities.

Authentication, and security more broadly, need to be designed for and managed by humans, but also smart enough to adapt to risk profiles automatically, empowering employees to use what they want and get on with their jobs.

By finding this equilibrium, enterprises can use advanced authentication to meet the growing demand for a perimeter-less workplace, without exposing their organization to a security breach. By taking this approach, cybersecurity will be seen as an ally to businesses rather than a barrier.

The ULTIMATE GUIDE to the CISSP®



Be a Leader in Information Security

Aspiring to be a CISSP?

Studying for the exam can seem over-whelming - but it doesn't have to be with The Ultimate Guide to the CISSP.

This guide is a must-have resource if you are planning to sit for the exam – and it was developed by (ISC)², the creator of the CISSP Common Body of Knowledge (CBK).

This guide includes:

- ✓ Fast facts about CISSP
- ✓ An overview of the CISSP exam
- ✓ Benefits of becoming a CISSP
- ✓ Setting yourself up for success
- ✓ Steps to getting certified

GET YOUR FREE ULTIMATE GUIDE



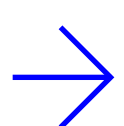
Healthcare organizations and the cloud: Benefits, risks, and security best practices

AUTHOR_Brad Taylor, CEO, Proficio

Healthcare organizations are moving their business-critical applications and workloads to the cloud, and while there are many benefits (lower costs, added flexibility and greater scalability), there are also inherent risks that cannot be overlooked. Ensuring that organizations' sensitive data is being monitored and protected 24/7 is key and having analysts who clearly understand security in the cloud is critical.

Hiring and staffing these roles can be quite difficult because of the skillset required.

+ Outsourcing cybersecurity to a managed security service provider (MSSP) is one viable solution for healthcare organizations that are in the process of migrating to the cloud.



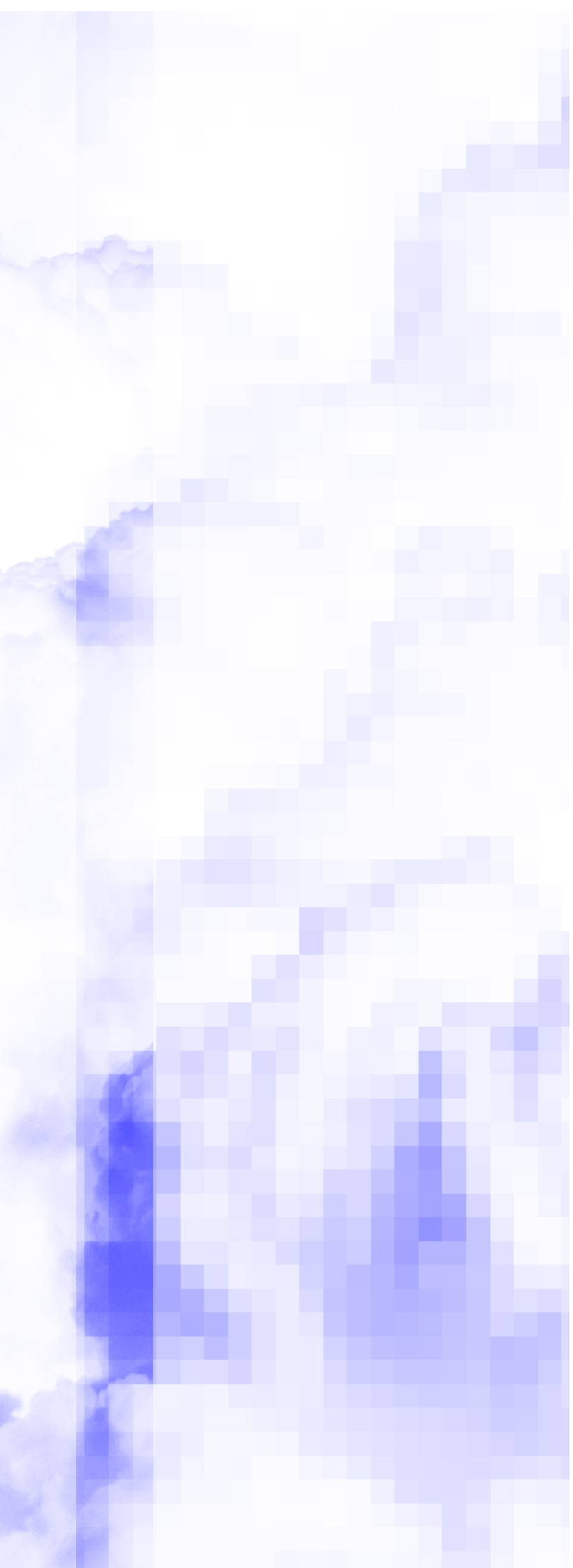
Why healthcare organizations are moving to the cloud

HIMSS Analytics conducted a survey of healthcare IT professionals about their views of cloud usage, with nearly two-thirds of respondents saying they are currently using the cloud or cloud services. So, why are healthcare organizations finally making the move?

Many have started to look at the cloud as a disaster recovery and backup option in the event of a ransomware attack, which affected the healthcare sector in 2017. The cloud also enables increased operational and storage flexibility as more healthcare companies use applications for things like precision medicine and population health.

Who's responsible for keeping the cloud secured?

With so much critical information being accessed and stored in the cloud, it's important to know who



is responsible for monitoring authentication, communication, and client access to devices as well as how they're securing it.

Cloud application vendors are motivated to secure their infrastructure against denial of service attacks, disruption to service delivery, and large backend infrastructure breaches to protect their business. However, control over data access, user credentials (in some cases the application servers themselves), and regulatory compliance rests on the user organization's IT team – not the cloud vendor. In short, cloud infrastructure providers are responsible for protecting their service, while IT teams must

ensure their organization's private data and critical applications are protected.

So, whether you are using cloud providers (such as AWS or Microsoft Azure) to host your sensitive applications and data, taking advantage of Microsoft Office 365, or leveraging the scalability of a cloud-based electronic health record (EHR) application, security is a shared responsibility between the IT security team and cloud provider. As more healthcare organizations turn to cloud services, it is becoming critical for IT and security teams to understand the delineation of responsibility.

Taking the right security measures in cloud infrastructures

Most of the same security risks that apply to data and applications residing within a traditional data center also apply to virtualized assets in cloud infrastructures like AWS, Azure, and others.

Virtual servers can be infected with malware or ransomware, credentials can be stolen, and cyber criminals can extract data which makes cyber protection even more important.

Web applications are one of the most significant sources of enterprise data breaches, and public-facing web applications are often hosted on cloud platforms. Because cloud platforms are designed for easy sharing, data runs the risk of becoming unintentionally shared or exposed. Misconfigured cloud-based data stores have resulted in many vulnerabilities and threats.

+ To address these risks, IT security teams are adopting security tools such as virtualized firewalls, web application firewalls, intrusion detection systems, and vulnerability scanning tools developed for cloud infrastructures.

These technologies are integrated using service provider application programming interfaces (APIs) that are designed to address the virtualized and dynamic nature of these environments.

Protecting Software as a Service applications in the cloud

Software as a service (SaaS) applications like EHR software, Office365, and Salesforce often store sensitive patient data and confidential business and operational information. A breach or inadvertent exposure of this data can result in compliance violations, revenue loss, significant recovery expense, and can damage irreparably the organization's reputation.

MSSPs and cloud access security brokers (CASBs) can collect and analyze authentication, access control, and cloud application transaction logs to identify suspicious behavior. Such logs include downloads, logins, usage, and application specific

behaviors that may be analyzed by an MSSP to determine indicators of compromise.

Importance of maintaining HIPAA compliance

For healthcare organizations, the Health Insurance Portability and Accountability Act (HIPAA) is an omnipresent reality. HIPAA requires patient data to be properly protected, no matter where it is being stored. Those who fail to protect patient data face fines and other regulatory penalties.

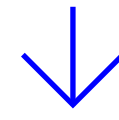
To meet HIPAA requirements, IT security teams should apply the same level of vigor to safeguarding their cloud-based data and applications as they would to on-premise applications and data. This can include deploying virtualized firewalls, scanning virtual servers for vulnerabilities, and monitoring and retaining log events from the public cloud.

How MSSPs can help implement stringent security in the cloud

When migrating to the cloud, many healthcare organizations consider implementing in-house security solutions. This means hiring security experts and around-the-clock staff to manage and respond to alerts. With the current cybersecurity skills shortage, finding and building the right team is not always easy. How can a healthcare organization maximize the rewards of cloud-based data and applications while minimizing the security risks? One approach is to outsource the security monitoring, investigations, and incident response to an MSSP.

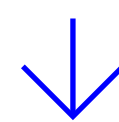
MSSPs have a service model that is well-suited for healthcare organizations with limited resources and strict compliance requirements. MSSPs can act as an extension of a healthcare organization's IT security team at a fraction of the cost associated

with hiring additional employees and operating a 24/7 security operations center (SOC).



When choosing an MSSP, it is important that healthcare organizations thoroughly evaluate providers and cross-reference their healthcare expertise to ensure a smooth transition to the cloud. Key questions organizations should ask an MSSP include:

- ▣ Are you experienced with helping healthcare organizations protect their data and applications in the cloud?
- ▣ Does your mix of security services include 24/7 monitoring, breach detection, and incident response?
- ▣ Can you monitor log events from my preferred cloud provider and cloud-based application vendor?
- ▣ How do you ensure we will receive accurate and relevant actionable alerts?
- ▣ Can you manage or co-manage vulnerability management tools, virtualized firewalls, and endpoint security in cloud environments?
- ▣ Do you have a single portal where we drill into security events and understand our security posture for both cloud-based and on-premise assets?
- ▣ Do you offer HIPAA reporting and services to prepare us in the event of an HHS audit?



By asking these questions, healthcare organizations should be able to determine if the MSSP is equipped to handle security needs. Especially for healthcare organizations with limited budgets and small IT teams, a qualified MSSP can serve as an extension of their team, help improve cybersecurity posture, and make the most of moving to the cloud.

Events



DoD Information Warfare Symposium 2018

March 28-29, 2018

Mary M. Gates Learning Center, Alexandria, VA, USA
<http://informationwarfare.dsigroup.org>

DSI's DoD Information Warfare Symposium will focus on the efforts to fight and win in an increasingly congested information battlespace. This year's event will focus on the convergence of Cyber, EW, and IA and the employment of these capabilities to win in the information environment.

HITB Security Conference 2018 – Amsterdam

April 9-13, 2018

NH Grand Krasnapolsky, Amsterdam, The Netherlands
<https://conference.hitb.org/hitbsecconf2018ams/>

The 9th annual HITB Security Conference features six 3-day technical training courses followed by a 2-day triple track conference, a CTF competition, technology exhibition covering AI and blockchain, a space for EU hackerspaces, a lock picking village, car hacking and hardware related exhibits, plus the CommSec track – a free-to-attend track of 30 and 60 min talks live streamed on Youtube!

RSA Conference 2018

April 16-20, 2018

San Francisco, CA, USA
<http://bit.ly/rsac2018hns>

At RSA Conference 2018, Now Matters. From emerging innovations to pressing threats, RSAC has everything you need to shut down cyber risk. As the world's leading cybersecurity event, RSAC brings together the field's brightest minds, CISOs to analysts, for an experience you can't find anywhere else. And when you register for RSAC 2018 in San Francisco, April 16-20, you'll have access to expert-led sessions, keynotes and more.



Blockchain technology promises to solve many complex problems across different business sectors and industries, and Bitcoin is breaking value records seemingly every hour. But many don't understand how the two really work, and use the two words interchangeably as if they were synonymous.

One important thing to remember is that blockchain can exist without Bitcoin, but Bitcoin cannot exist without a blockchain.

What is Bitcoin?

Bitcoin is a digital currency that was created in 2009. Only 21 million Bitcoins can ever be created (mined), and it is estimated that the last coin will be produced in 2140.

It is exchanged on a decentralized, peer-to-peer network, meaning that there is no central server or

A deep dive into blockchain and Bitcoin

AUTHOR_ Zoran Lalic, Enterprise Security Architect at a software company

authority (i.e., a central bank) that regulates it. In the beginning, the Bitcoin network was operated by volunteers who had a full Bitcoin protocol stack installed on their private computers. However, the network's operation has mostly been taken over by specialized data centers.

Bitcoin operates on a cryptographic protocol, is fully transparent and open source. As it's not backed by a real authority, the health of the system depends entirely on the trust people have in it. The value of Bitcoin is determined by the amount people are willing to pay for it.

To receive Bitcoins, store them, make payments, and send them to someone else, users need a cryptocurrency (digital) wallet. Think of this wallet as a bank account or a traditional wallet that you carry in your pocket. However, to be technically correct, Bitcoins are not stored in this wallet - effectively, they don't even exist. (I will get back to this statement later in the article.)

There are several types of cryptocurrency wallets:

1_Software wallet: You download it on your personal computer, it is physically stored on its hard drive, you have full control over it, and its protection is your responsibility (i.e., you have to keep your private keys in a secure place).

2_Online wallet: It's hosted in the cloud by a third party, you can access it from anywhere around the globe, but there's always the possibility that this third party will be breached and your currency stolen once your private keys are compromised.

3_Mobile app: You download an app on your mobile phone.

4_Hardware wallet: Stores your private keys in a secure hardware device.

5_Paper wallet: Your private key and corresponding Bitcoin address printed on a paper, which should be stored in a secure place. A Bitcoin wallet is a collection of public and private key pairs. Bitcoins are received into a Bitcoin address, which is public and can be shared with anyone to send Bitcoins to it (similar to an email address - you can provide your email address to anyone to send you emails). A Bitcoin address is not a public key, but rather a shorthand for a public key.

+ Your private key allows you to spend Bitcoins, and thus must be kept secret (like a password for your email account).

The wallet application randomly generates a private key along with its corresponding Bitcoin address when the wallet is created. Within a cryptocurrency wallet, you can easily generate as many Bitcoin addresses as you like. This is what happens in the background when you create a Bitcoin address in your wallet:

1_A public/private key pair is created.

2_The public key is put through multiple SHA-256 and RIPEMD-160 calculations.

- RIPEMD-160 produces a shorter hash, thus shorter Bitcoin addresses.
- Better security if one hashing algorithm is broken.

3_It is then converted into a Base58 format, which removes the possibility of having ambiguous characters in a Bitcoin address. (e.g. lowercase "l"/upper case "i"), and is ready to be used. *By the by, the reason Bitcoin uses a Bitcoin address (a hash of public key) instead of a public key is to increase the security of the system. If a vulnerability were to be discovered in the Elliptic Curve Digital Signature Algorithm (ECDSA), your Bitcoins would still be safe because the public key is not present anywhere on the network until you spend Bitcoins.*

4_ The generated pair will look like this:

- Bitcoin address:

1Jydra8thqJYSRC5Ykg2mVv3UdCV8fj3Q7

(That's the address you can publicly distribute to people to send you Bitcoins.)

- Private Key:

L5RMWUU8yFzqdZ5AzVG6VAXGTEYjiF72oVw2kN3E6zFeuV1sD4ww

(This key allows you to spend Bitcoins. If you lose it, you lose access to your Bitcoins forever. This is a private key that signs every transaction you authorize and allows you to spend the funds you received from others. If someone steals this key from you, they can access to your Bitcoins and spend them.)

What is blockchain?

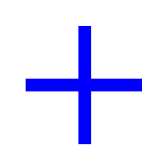
Blockchain is the technology that powers Bitcoin. It is a decentralized and distributed digital ledger that is run by a global network of computers and is used to record Bitcoin transactions securely. It is open and public: everyone knows about everyone's transactions, but can't readily determine the identity of a Bitcoin owner. A copy of the blockchain database (record of transactions) resides on each computer that is part of the blockchain network, thus ensuring that the record cannot be altered. The trust is placed in the mathematical functions that protect the entire system. The interesting point is that blockchain does not keep an account balance of Bitcoins, it just records the transactions from the beginning of Bitcoin creation. By linking to previous transactions, it determines if a person has sufficient funds to spend.

Do you recall me mentioning earlier that Bitcoin does not exist? So, what is it then? It is merely a

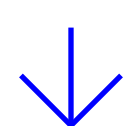
reference to a transaction, which is a way to move "Bitcoin value" from one owner to another in a chain of ownership. A transaction tells the Bitcoin network that the owner of a Bitcoin is authorizing a transfer to another owner. The new owner can then approve a transfer to another owner, and so on.

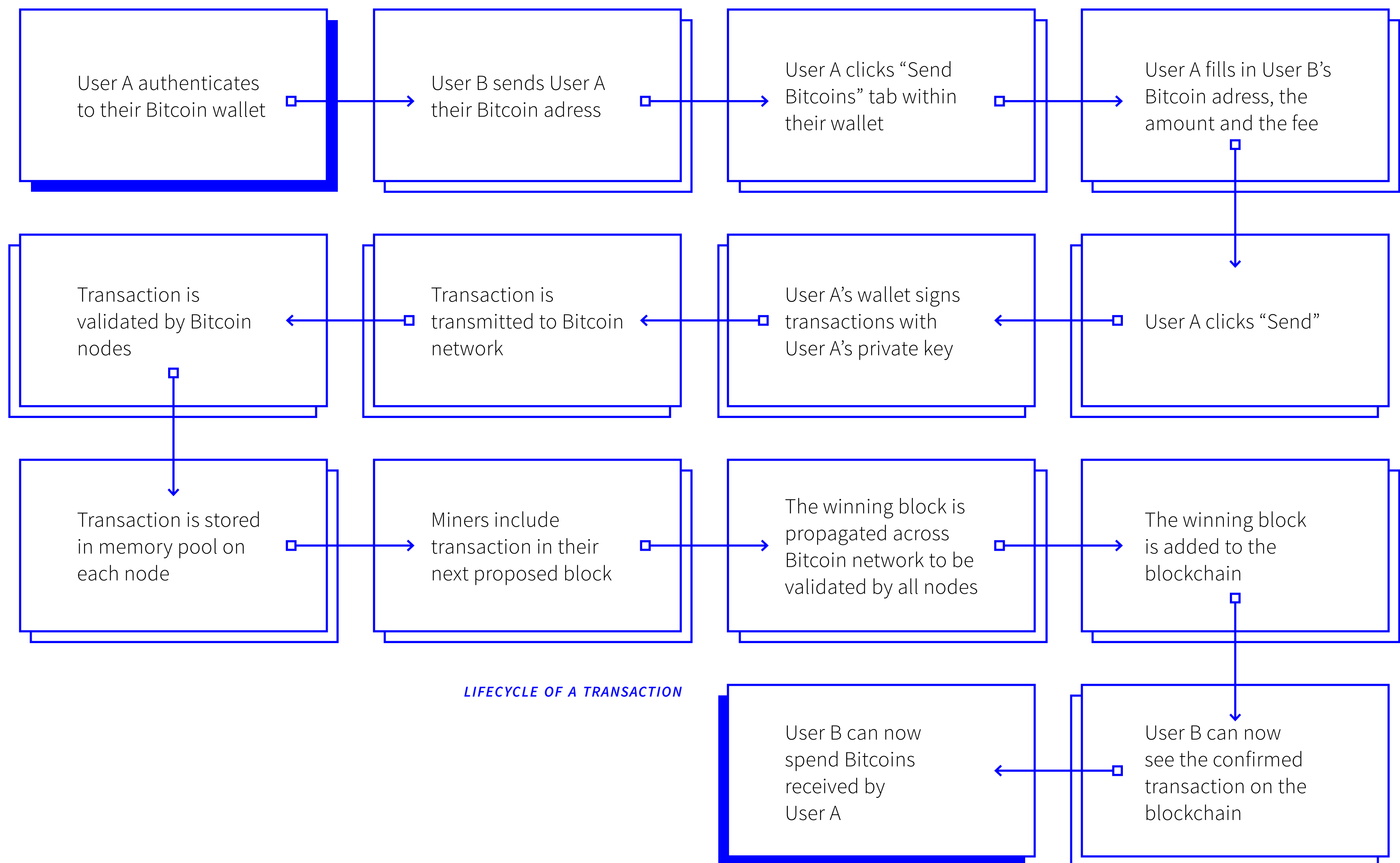
Each transaction contains one or multiple "inputs" and "outputs." An input, also known as "unspent transaction," holds a Bitcoin value (typically a previous transaction's output). Thus, the output becomes a new input. In other words, the input spends a previous output. The wallet uses the private key to sign the transaction.

What happens to the transaction once it leaves your wallet? The transaction is transmitted to the Bitcoin network for confirmation to become a part of the blockchain. Each node that is part of Bitcoin network will validate this transaction and send it to other nodes that are connected to it until the transaction propagates across the entire network (i.e., reaches all nodes). All valid transactions are sent to a local memory pool waiting to be included in a newly proposed block (each node has a local memory pool). If the transaction is invalid, the first node that received will reject it immediately, and will not broadcast it to other nodes on the network.



The criteria list to validate each transaction is very long. The transaction contains no sensitive or confidential data so that it can be transmitted over insecure networks.





Let's now try to understand "bitcoin mining" and "blockchain" a bit better, and then we will come back to transactions and transaction fees.

Bitcoin mining is a process by which new Bitcoins are created, and transaction records are confirmed and added to the blockchain. The same process also ensures that the Bitcoin system is secured against fraudulent transactions and double-spend transactions (when the same input is spent more than once). Mining is performed by miners, who provide processing power to the Bitcoin network.

Who are these miners and why would do they do this? Anyone can become a miner by downloading and running a full Bitcoin protocol stack on their computer. In the early days of Bitcoin, even a home computer was good enough for this process. However, today you need much processing power, specialized hardware, and cheap electricity to be in this business. Becoming a Bitcoin miner creates the opportunity to be awarded new Bitcoins.

Miners receive these rewards when they successfully mine a block, and they also collect transaction fees included in it. All miners around the globe compete to solve a challenging and complex mathematical problem that is based on a cryptographic hash algorithm. This mathematical problem is called the Proof-Of-Work algorithm, which is included in the newly created (mined) block to serve as a proof that the miner used significant processing power to solve it. The Bitcoin protocol adjusts the difficulty, resulting in a new block being produced, on average, every 10 minutes.

Miners are making millions and billions of guesses every second trying to solve this problem. When a miner finds the solution to a problem, they immediately broadcast their block to the rest of the network. If their block is accepted as a valid block, they are rewarded with the block reward and with all the transactions fees in it. The reward started with 50 Bitcoins for each block and has been halved every four years since then (currently

it’s 12.5 BTC per block). In addition to significant processing power, the miners also need luck to mine a block.

Each block is identified by a unique hash. Each block also contains a hash of a previous block,

which allows blocks to be linked together creating a chain all the way to the first block ever built (a.k.a. the genesis block).

Each block is made of two parts – a block header and transaction data.

THREE BLOCKS CHAINED TOGETHER

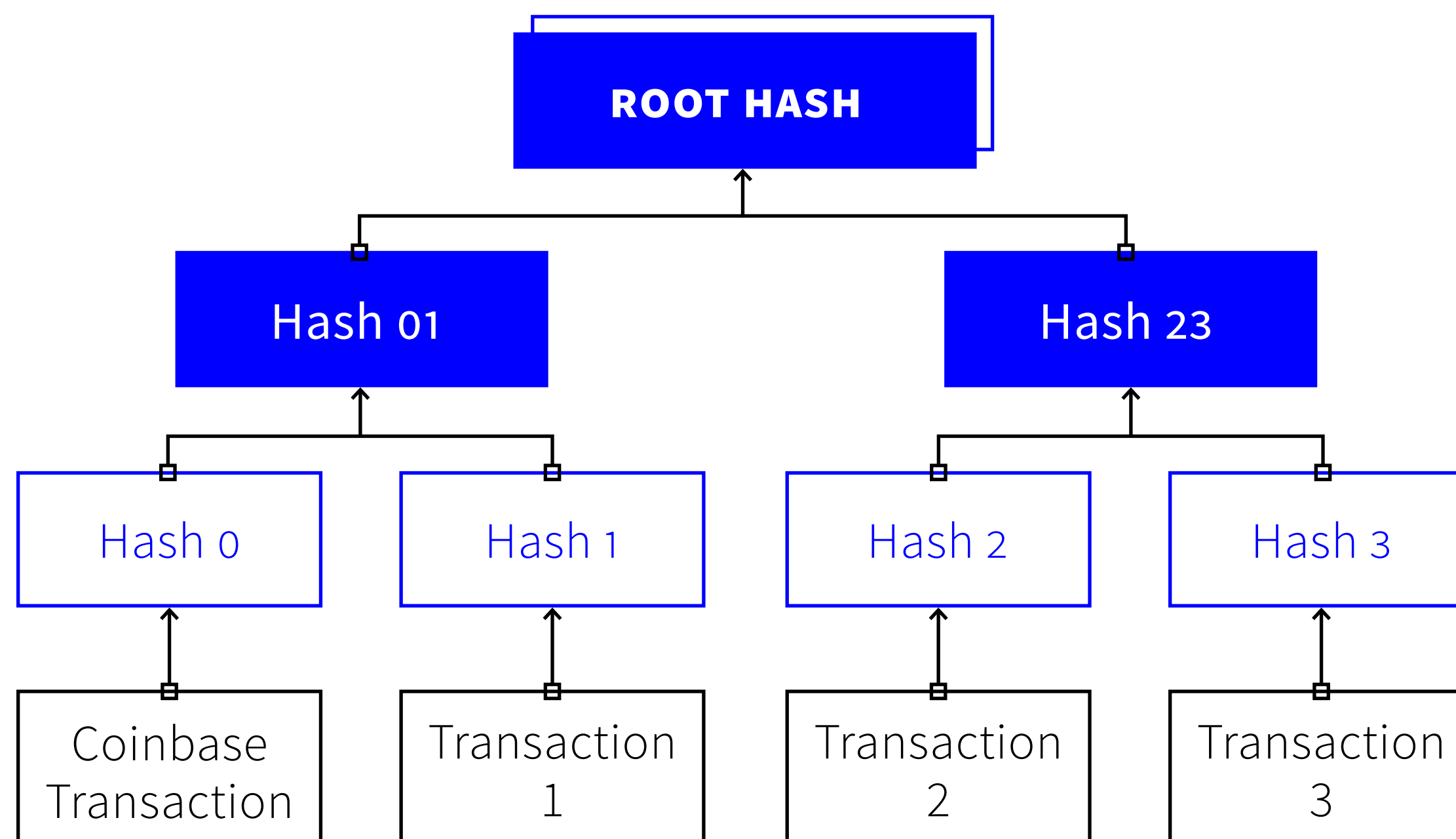
BLOCK 10,001	BLOCK 10,002	BLOCK 10,003
HEADER HASH 000000005vm56	HEADER HASH 000000005vm66	HEADER HASH 000000005vm76
BLOCK HEADER	BLOCK HEADER	BLOCK HEADER
Version 1	Version 1	Version 1
Previous Block Hash 000000005vm50	Previous Block Hash 000000005vm56	Previous Block Hash 000000005vm66
Merkle Block Hash a67vvc45re222	Merkle Block Hash b67vvc45re859	Merkle Block Hash c67vvc45re221
Time Stamp 2017-11-27 10:22:10	Time Stamp 2017-11-27 10:31:10	Time Stamp 2017-11-27 10:42:10
Difficulty 17554.29	Difficulty 17554.29	Difficulty 17554.29
Nonce - Proof of Work 7899433	Nonce - Proof of Work 8785437	Nonce - Proof of Work 4552432
TRANSACTIONS	TRANSACTIONS	TRANSACTIONS
Transaction 1 4v7hhr5g34	Transaction 1 5v7hhr5g88	Transaction 1 4v7hhr5gd4
Transaction 2 3v7utr5g34	Transaction 2 3v7utr5g55	Transaction 2 3v7utr5ge5
Transaction 3 2k8hhr5g22	Transaction 3 2k8hhr5g11	Transaction 3 2k8hhr5g21e

The block header consists of the following elements:

- ▣ Version number
 - ◆ This is just a tracking number for the protocol.
- ▣ The previous block hash (a.k.a. the parent hash)
 - ◆ Like I mentioned earlier, this is how blocks are linked together.
- ▣ The Merkle tree
 - ◆ A Merkle tree is a data structure that is used to hash a large number of pieces of data together. In Bitcoin, it is used to summarize all transactions in a block by producing an overall hash (root hash). It is used to verify that the set of transactions included in a block has not been tampered with.
- ▣ The timestamp
 - ◆ The time of hashing.
- ▣ The difficulty
 - ◆ Every two weeks, the Bitcoin network automatically readjusts the difficulty so that a new block is always produced every 10 minutes or so. It does so by creating the difficulty target. This target is a hash with a targeted number of zeros.
- ▣ The nonce
 - ◆ This is a 32-bit random number that miners vary to find an acceptable hash (a problem that they are solving) with the required number of leading zeros. They typically start with 0.
 - ◆ The 32-bit number ranges from 0 to 2^{32} .
 - ◆ You literally need to brute force all possible nonces to find an acceptable hash. However, you don't have to start with 0.
 - ◆ One important thing to mention is that 2^{32} = around 4 billion numbers. With the processing power some miners use, it might take only a several seconds to go through all 4 billion. But, most likely, an acceptable hash will not be discovered within this range. Miners vary the other pieces within the block to change the block hash allowing them to do billions of hashes per second. For example, when the nonce is exhausted, the miner might change the timestamp, and now they can run through the nonce (2^{32}) once again.

Note: The block hash is produced by hashing the block header and then hashing the hash (double SHA256 hash). The block header is 80 bytes. Each transaction is, on average, 300 bytes. The number of transactions in each block depends on the size of transactions. Each block can contain up to 1MB of data.

DIAGRAM: THE MERKLE TREE



Before tackling transaction fees, let's summarize what we just talked about:

The blocks are linked together using hashes to create a chain going back all the way to genesis block. This blockchain is a list of all transactions that have been confirmed by miners since the creation of Bitcoin.

Each received block is validated before being linked to the existing blockchain. For this system to work, each peer on the network must be in agreement who owns and how many Bitcoins at all times. Bitcoin uses a process called mining to accomplish this distributed consensus. The people who decide to participate in this distributed consensus are called miners.

Miners are rewarded with newly generated Bitcoins for their efforts (this is how new Bitcoins are created). The mining process uses the Proof-of-Work algorithm to ensure this consensus is true. The algorithm allows miners to perform trillions of calculations in the hope of finding the right hash. Each node in the Bitcoin network independently verifies each transaction and each block. This distributed consensus is how the trust is established in this untrusted network of thousands of nodes.

The main point is that there is no central blockchain list and no central authority. Each full node in the

Bitcoin network has the exact same copy of the blockchain, which is updated continuously with newly mined blocks.

Transactions

Transactions are nothing more than a "record" indicating the change of ownership of Bitcoins from one owner to another. *Transaction fees* are small fees collected by miners for including the transactions in a block. (Transaction fees are not mandatory.)

Each transaction is validated by all Bitcoin nodes, sent to the memory pool, included in a valid block, and will be confirmed once a block with the proper proof of work (an acceptable hash) is found. Then, it will be broadcasted to the rest of the network, validated by the Bitcoin network, and the block added to the blockchain. All transactions within this block are now confirmed, and anyone in the world can see them.

It's up to the miners to include or not to include transactions in their newly proposed block. There are empty blocks out there that are valid (miners that solve a block start mining a new block immediately, hoping they can buy some time by not including any transactions). However, there is one transaction that must be included in each proposed

block. This transaction is known as the coinbase transaction, and it can only be created by miners. It is used to reward a miner with newly created Bitcoins (currently 12.5 BTC) for discovering a new block.

One thing to note is that a wallet contains all the logic needed to build each transaction. As a user, you only need to specify the Bitcoin address to which you are sending Bitcoins to and the amount. Most wallets will automatically calculate and include

the transaction fee, while some will allow you to enter the fee amount manually. One occasion where you must be very careful is when you construct your transaction since there is no field for fees. In this situation, the fee is the difference between an input and output. In other words, if something costs you 2 Bitcoins to purchase and your input was 10 Bitcoins, the fee that is collected by a miner would be 8 Bitcoins. These fees are collected by miners as a reward for confirming and including transactions into the block.

I would like to drive this point home with this example:

- ▣ You received 10 BTC from someone. Now you have an unspent transaction of 10 BTC.
- ▣ You now want to send your friend 0.5 BTC.
- ▣ Your previous input of 10 BTC now becomes an output. You cannot just simply send 0.5 BTC. Therefore, your 10 BTC output is sent to the network.
- ▣ Now a new transaction will be created that will point to you. This new input will now be 9.5 BTC, which you can use again as output in the future. To summarize, you had an 10 BTC output that you received from someone, you paid your friend 0.5 BTC, and you got a change back of 9.5 BTC. This is all taken care of for you by your cryptocurrency wallet (fee excluded).

If all this still does not make sense, don't worry, just bear with me and I will walk you through a very simplified example that incorporates everything previously discussed.

The scenario

- ▣ 15 miners
 - ♦ Physically located all over the globe.
 - ♦ They all purchased hardware for this purpose.
 - ♦ All miners are peers. No centralized server.
 - ♦ They all downloaded and installed a full Bitcoin client.
 - » The Bitcoin client downloaded the entire blockchain locally – all of 10,001 blocks.
 - » All 15 miners have completed this step.

- ▣ 10,001 blocks in a blockchain
 - ♦ Up to this point, 10,001 blocks were successfully mined.
 - ♦ The first block is called a genesis block.
 - ♦ The plan is to mine blocks 10,002 and 10,003.
 - ♦ The hash for block 10,001:
 - » 00000000000000007811b6013a77914120217ef55c4f4dedd9d4fd99c5e3bd22
- ▣ 5 users involved in spending and/or receiving Bitcoins
 - ♦ All 5 users signed up for a hosted wallet.
 - ♦ All 5 users generated their Bitcoin address within the wallet.
 - ♦ User A sends User B 2 BTC
 - ♦ User A sends User C 3 BTC
 - ♦ User A sends User D 5 BTC
 - ♦ User D sends User E 2 BTC
 - » We will take a closer look at this last transaction
- ▣ Difficulty is 5.02
 - ♦ Bitcoin network adjusts it automatically every 2 weeks so that discovering a new block takes 10 minutes on average.
 - ♦ If it took less than 10 minutes on average to find each new block the previous two weeks, the difficulty would increase. If it took more than 10 minutes, the difficulty would decrease.
 - » The target hash is:
 - » 0000000043ad33aa5811b6013a2241412bd17ef55c4f4debd9d4fd99c5e3ba45
 - The solution must be equal or less than the target hash.
 - The more zeros, the harder it is to find the right solution.
 - The miner will be making millions and billions of guesses per second before they find a hash that is acceptable.
- ▣ The difficulty level determines what the minimum acceptable hash is.
 - ♦ As more miners join the network, the difficulty level increases. As the difficulty level increases, there are less and less acceptable hashes.
 - ♦ Current difficulty level (December 2017) is 1,590,896,927,258.08.
 - ♦ In the beginning, the difficulty level was 1.
 - ♦ As of December 2017, almost 500,000 blocks have been mined.
 - ♦ Blocks are stacked on top of one another.

Let's start

- ▣ All 15 miners compete to find an acceptable hash to mine block 10,002.
 - ◆ It is not just one hash that they are competing to find, but one of many that will be accepted by the network.
- ▣ They are all using a Proof-Of-Work algorithm to find an acceptable hash. They do it like this:
 - ◆ They all propose a new block. This proposed block contains the various pieces we talked about earlier: version number, the previous block hash, the Merkle root hash, the timestamp, the difficulty, the nonce, and the transactions.
- ▣ How did the transactions end up there?
 - ◆ We mentioned that User D sent User E 2 bitcoins.
 - ◆ User D signs into his hosted wallet.
 - ◆ He has one unspent transaction (5 BTC) as he received it from User A. Now he wants to transfer 2 BTC to User E. How can he do this?
 - ◆ User E sends a Bitcoin address to User D.
 - ◆ User D goes inside his wallet.
 - » He goes to the “Send” section of his wallet.
 - » Pay to: User E’s Bitcoin address
 - » Amount: 2 BTC
 - » Fee: Some wallets dynamically calculate the fee. Some require you to enter the amount manually. (Fees are not mandatory, but they are required if you want fast transaction processing. Miners decide which transactions they will include in their block. They might not include transactions with no fees attached to them. These fees are minimal. It’s important to note that transactions are prioritized - fees, age, etc. are taken into consideration.
- ▣ The miner will now calculate the hash of the block’s header and then hash the produced hash.
- ▣ Bitcoin uses modified “hashcash” as the mining function.
 - ◆ Bitcoin uses SHA256 instead of SHA1 as the original hashcash.
 - ◆ Double SHA256.
 - ◆ Fractional difficulty defined. The initial hashcash difficulty can only double or halve.
- ▣ Now the mining process (Proof of Work) is taking place by testing billions and trillions of “nonces.” It will start with number “0” and

- ▣ Whichever node receives a block from miner #1 will validate it and extend its local blockchain by adding this block.
 - ◆ Nodes closer to miner #1 will receive this block first.
- ▣ Whichever node receives a block from miner #15 will validate it and extend its local blockchain by adding this block.
 - ◆ Nodes closer to miner #15 will receive this block before they receive a block from miner #1.
- ▣ Now, this results in two different versions of the blockchain.
(Remember that both blocks are valid and mined properly. So, what happens now?)
- ▣ This kind of scenario is typically resolved within the next block. So, in this case, let's mine block 10,004 to resolve this issue.
- ▣ Let's say that miners 2 – 8 are building on top of block discovered by miner #1 and miners 9 -14 are building on top of block discovered by miner #15. Let's also say that the next block (10,004) has been discovered by miner #7. Now miners 1 – 8 will extend their existing blockchain by adding block 10,004.
- ▣ Miners 9 – 15 will now see two chains. They will set the blockchain used by miners 1-8 as the primary chain because it is longer (more blocks) and use their existing one as a secondary. They will immediately stop their current work and start using the longer chain.
- ▣ The transactions from blocks that were not added to the primary blockchain will go back to the memory pool.
- ▣ The entire Bitcoin network re-converges to use the same copy of blockchain.



Conclusion

I will conclude the article by giving you some additional information about blockchain and Bitcoin:

1_Blockchain is a technology that can solve other problems - cryptocurrency is just one of its use cases. Anything of value that needs to be tracked can exist on a blockchain. Additionally, smart contracts are becoming an important part of blockchain technology.



2_ You might have heard that a transaction is not truly valid until 6 confirmations. What does this mean? Each confirmation represents a block that has been accepted by the Bitcoin network since the block that included the transaction. Let's say you purchased a car with Bitcoins (5BTC). Let's also assume that this transaction has been included in block 10,001. Before the purchase is accepted by the seller, he or she will want to wait until 6 more blocks have been accepted by the blockchain on the top of block 10,001. We already know that it takes 10 minutes on average to mine each block, which means that the waiting period would be 60 minutes. (The seller would see a transaction in their digital wallet within seconds, but unconfirmed). The main reason for this is to prevent a double-spend attack. For small transactions (e.g., a cup of coffee) this is typically not required. Six confirmations represent that enough processing power was used to ensure the transaction is valid and will never be able to be changed.

3_ Proof-of-Work, also referred to as the consensus algorithm, requires massive amounts of computing power and energy. Estimates suggest that for processing a single transaction, the network consumes as much electricity as 8-10 average households for one entire day. This is one of the main reasons why you will often hear that blockchain is immutable.

4_ How hard or easy is it to tamper with blockchain? How secure is it? According to estimates, the electricity consumed to mine one block (all miners combined) is equal to the amount of electricity used by a city with a population of 200,000. Thus, it would require the same amount of energy to recalculate the block's hash (re-mine the block) to make it valid after it has been tampered with. Let's say, for example, a blockchain with 1,000 blocks is being tampered with. An attacker tampered with block #500 and successfully recalculated a new hash. What would happen in this situation? A blockchain would break, blocks 501 through 1,000 would no longer be valid because the "previous hash" in block 501 no longer matches the original hash. An attacker would now have to re-mine the entire blockchain from the block #501 onwards. They would have to re-write the history.

5_ What would happen if someone was in the position to control more than 50% of the network's mining power? This brings us to what is known as 51% attack. In theory, this person could manipulate the Bitcoin system to double-spend Bitcoins, prevent transaction confirmations, prevent anyone else on the network to mine the new blocks, etc.

6_ There are mining pools that individual miners can join to combine the mining power so that they have a higher chance to mine new blocks. The reward is split between all miners.

7_ Bitcoin can be broken down into one hundred-millionth of a Bitcoin – 0.00000001. This smallest unit of Bitcoin is called Satoshi.

8_ There could be several inputs and several outputs in one transaction. Let's say that, for example, you have received 2 BTC from User A (transaction 1), 3 BTC from User B (transaction 2), and 5 BTC from User C (transaction 3). Now you want to send 9 BTC to User D. Your wallet would aggregate transactions 1, 2 and 3 (altogether 10 BTC) as an input, and the output would contain the User D's Bitcoin address. Also, it would contain output back to you (a change) and a transaction fee. The output could have several recipients if your input is less or equal to all outputs combined. Remember that miners check the entire blockchain (all the way to genesis block) searching for unspent outputs that point to you. All unspent outputs combined must equal to or be less than what you are trying to spend.

9_ You will often hear that it is recommended to use a different Bitcoin address for every transaction. Why is that? The main reason for this is increased anonymity. It makes it very difficult to trace that the person who received a transaction A is the same person who received transaction B. There are 2^{160} possible Bitcoin addresses. In other words, it is near impossible to ever run out of them. To put that in perspective: there are 2^{128} possible IPv6 IP addresses.

10_ *Backup and encrypt your digital wallets!*

11_ It would be challenging for a blockchain to comply with the GDPR. GDPR gives people the right to request their data to be erased, but data

stored on a blockchain cannot be deleted.

12_ Bitcoin uses a scripting language called Script to validate transactions. This language uses two types of scripts to validate transactions:

- scriptPubKey (Output) – The sender creates it using the receiver's Bitcoin address.
- scriptSig (Input) – The receiver proves that they own the above Bitcoin address by providing their private key.

13_ Traditional Bitcoin addresses are also known as single-key addresses and begin with the number "1". A person can move funds knowing "one" private key. Bitcoin also has an alternative pay-to-script-hash (P2SH) address. These addresses begin with the number "3". These addresses require multiple keys (multiple signatures) to spend funds.

14_ There are different kinds of blockchains out there:

- Public (Bitcoin)
- Private (run on a private network)
- Open (Bitcoin)
- Permissioned (specific people adding data)

15_ You can use Blockchain.info to view all transactions ever recorded.

16_ To being able to understand blockchain and Bitcoin, one must understand cryptography, as it is at the heart of these technologies.

17_ Elliptic Curve Digital Signature Algorithm (ECDSA) is a cryptographic algorithm that Bitcoin uses to sign transactions (digital signature). A key pair (private/public) in Bitcoin is an ECDSA key pair. The private key is used to approve a transaction, and the public key is used to verify it.





HITBSecConf2018 - Amsterdam

The 9th Annual HITB Security Conference in The Netherlands

*Where ideas are exchanged,
talent discovered and genius celebrated.*

Michel van Eeten

Professor of Cybersecurity,
Delft University of Technology



Marion Marschalek

Reverse Engineer / Low-Level
Security Researcher,
Intel

Amber Baldet

Executive Director,
Blockchain Program Lead,
J.P. Morgan

REGISTER ONLINE

<https://conference.hitb.org/hitbsecconf2018ams/>