2018

SECURITY REPORT

ixia

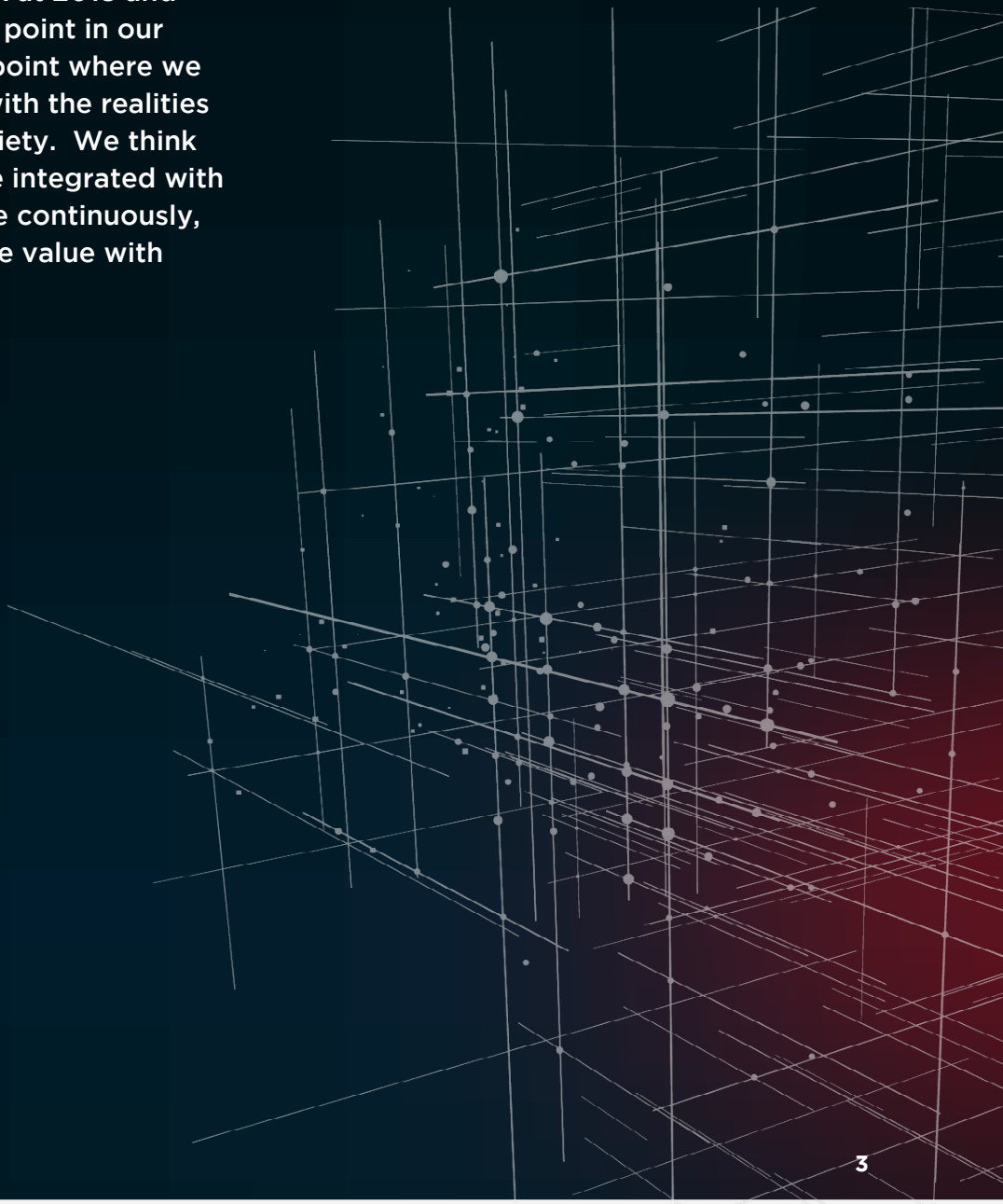
A Keysight Business

TABLE OF **CONTENTS**

SECTION
01

INTRODUCTION

Someday, we may look back at 2018 and recognize it as an inflection point in our approach to IT security - a point where we shifted to be more in step with the realities of our always-on digital society. We think this new model will be more integrated with network operations, operate continuously, and give us more of what we value with fewer trade-offs.



2018 is the year many IT organizations shift their focus from cloud migration to cloud operations. Many of those organizations expect cloud infrastructure will bring improved security[1]. But recent research from the Ixia Application Threat Intelligence (ATI) Research Center and third parties suggests a darker truth hiding behind the silver lining of the cloud: data breaches are up nearly 45% year over year[2], and one survey found that nearly three quarters of companies studied had one or more serious security misconfigurations on AWS[3]. The bottom line? The evolution of security practices is trailing behind the mainstream adoption of cloud operations.

An expanding attack surface is a well-understood trend driven by the cloud, mobility, and IoT. In 2018, new cloud-scale solutions are emerging which address the challenges of visibility, multi-layer security, and management of public, private, and hybrid cloud resources. In this report, we'll look at how the security ecosystem is evolving to tackle the scope of challenges inherent in a world of many clouds.

> The evolution of security practices is trailing behind mainstream adoption of cloud resources.

1 "Cisco 2018 Annual Cybersecurity Report Reveals Security Leaders Rely on and Invest in Automation, Machine Learning and Artificial Intelligence to Defend Against Threats," Cisco press release, 21 February 2018.

2 "Data Breaches Up Nearly 45 percent according to Annual Review by Identity Theft Resource Center and CyberScout," Identity Theft Resource Center press release, 25 January 25 2018.

3 "Threat Stack Analysis Reveals 73% of Companies Have Critical AWS Cloud Security Misconfigurations," Threat Stack press release, 18 April 2017.

We also look at the changing motivations and behaviors of threat actors. The payoff remains the primary motivator, and while ransomware remains a potent threat, crypto-jacking joined the main stage. In 2017, threat actors cashed in on the explosive growth of the crypto-currency market. Using infiltration techniques similar to ransomware attacks, hackers marshalled millions of devices to turn a quick profit using stolen CPU and electrical resources. Our report takes a deeper look at the techniques hackers use, and how you can protect yourself.

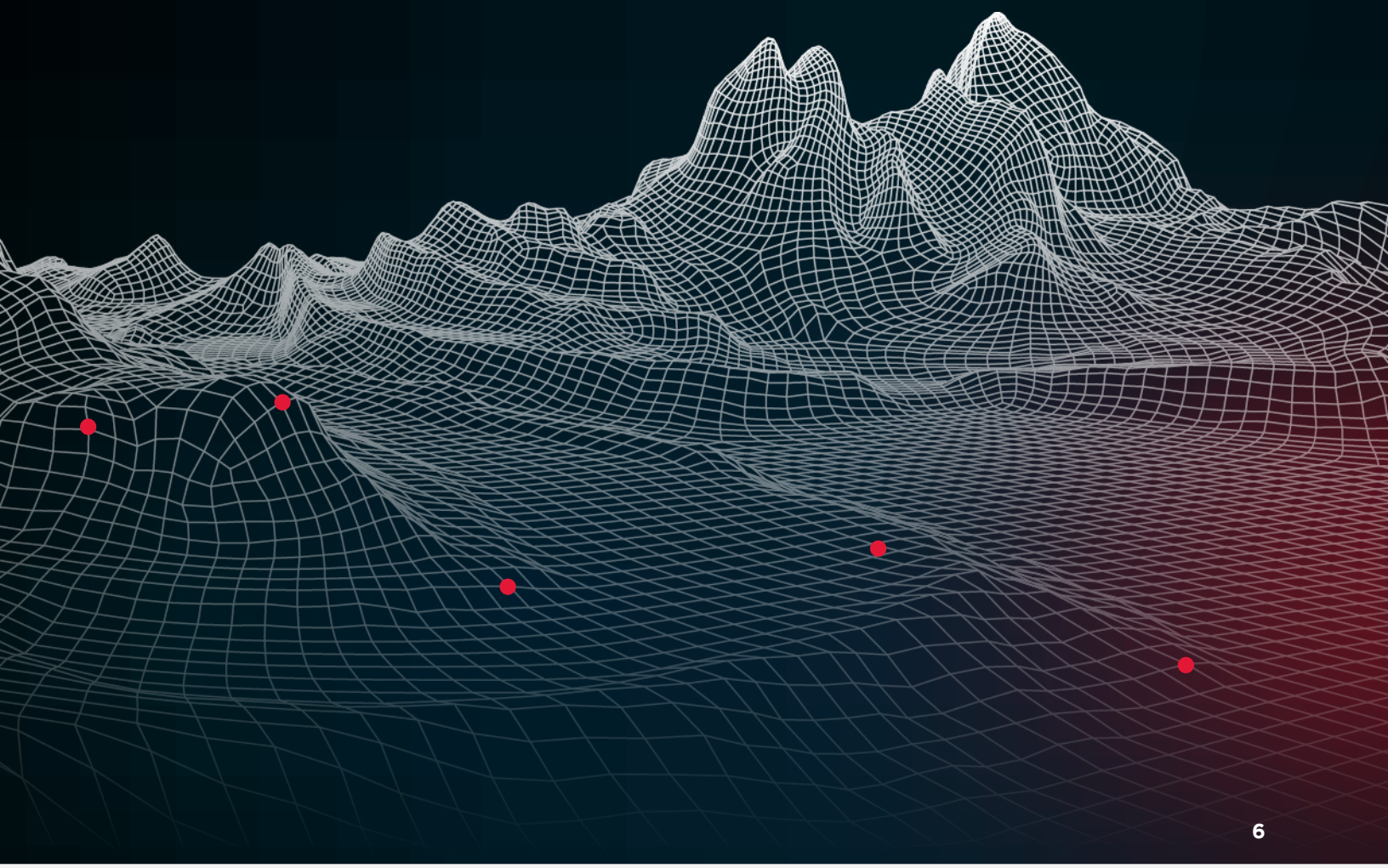
Finally, we look at the privacy landscape. Becoming secure and compliant was the top priority of IT professionals in Ixia's 2018 survey. May 25, 2018 marks the start of enforcement of the European Union's General Data Protection Regulation (GDPR), a regulation affecting any company doing business in the EU. With data and privacy stories making headlines so far in 2018, we expect privacy to be a hot-button issue throughout the year.

This year's report explores five key trends that are shaping IT security practices, with findings from the Ixia ATI Research Center that offer unique insights into customer challenges, threat actor behavior, and the global threat landscape. Taken together, these insights underscore the urgent need for continuous visibility and layered security to address the most urgent priorities of security and privacy in our cloud-dominated world.

SECTION

02

2018 KEY FINDINGS



1 Cloud security and compliance are top priorities in 2018

The dominance of cloud will significantly impact security teams as they strive to deliver effective security in a hybrid, dynamically changing, on-demand environment. An Ixia and Dimensions Research survey revealed that securing data and applications and satisfying compliance requirements overtook deploying and migrating applications as top public cloud priorities in 2018. Customers have become acutely aware of the visibility gap introduced with deployments in public cloud environments, with 88% experiencing issues related to a lack of visibility into public cloud data traffic.

2 The gap between cloud operations and security operations is growing

The number of US data breaches tracked in 2017 hit a new all-time high of 1,579, up 44.7% over 2016[2]. In addition, one study found nearly 73% of public cloud instances had one or more serious security misconfigurations[3]. The combination of cloud growth and a high number of security misconfigurations suggests we will see more breaches where cloud is a factor in 2018. Many IT leaders are turning to a multi-layer security approach[1] to combat the challenges of an ever-expanding attack surface.

3 As cyberattacks evolve, more focus should be on visibility and detection

Though critical, firewalls and intrusion prevention are not adequate to protect an organization from advanced attacks that are designed to sidestep such systems. To reduce the risk of business disruption and potential data breach, companies need to deploy security analysis and threat detection solutions that use granular, network packet data to identify multi-layer exploits and contain attackers.

4 Cyber-crime is good business (for cyber-criminals)

Where 2017 was the year of ransomware, 2018 is primed to be the year of crypto-jacking. Mining crypto-currencies using devices without the owners' consent provides hackers with a high-profit return that is far stealthier than a ransom attack. Code has even been found on compromised websites that can be secretly transfered to users and melt down their battery powered devices[4]. More damage is on the horizon, with critical internet of things (IoT) infrastructure already being targeted to mine digital currency[5].

5 Encryption is making business more secure for customers, and for hackers, too

In 2017, over half of all web traffic was encrypted[6]. Hackers are exploiting this trend, hiding malicious traffic in encrypted streams, often to legitimate IP addresses on compromised systems. This makes detection via traditional means impossible, and demands a complete visibility approach that combines continuous inspection with multi-layered security tailored to the application environment.

We end our report looking ahead to the challenges of 2018. We hope to give you food for thought and encourage you to reach out to us with questions and thoughts of your own.

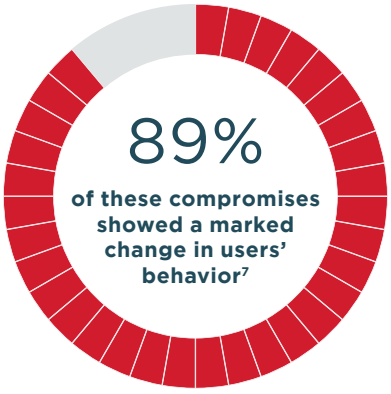
4 Francis Navarro, "This virus cryptojacks your phone and can literally melt it,"Komando.com, 27 December 2017.
5 Lily Hay Newman, "Now cryptojacking threatens critical infrastructure, too," Wired.com, 12 February 2018.
6 Gennie Gebhart, "We're Halfway to Encrypting the Entire Web," Electronic Frontier Foundation, 21 February 2017.

SECTION

03

CLOUD SECURITY IS A TOP PRIORITY

Spending on cloud computing is growing faster than ever before. Virtually all enterprises have workloads in one or more clouds and are all facing challenges with security and compliance in this hybrid environment. In fact, security and compliance have overtaken cloud migration as a top priority in Ixia's recent survey of cloud adopters.



7 Cloud Security Trends, Redlock Security Defense, October 2017, page 9, accessed online.

Lack of Visibility Drives Public Cloud Security Risk

Ixia recently commissioned Dimensional Research to conduct a survey among cloud adopters[8] to understand their security challenges. The survey found that more than 90 percent of IT professionals responsible for their company's public and private cloud environments are concerned about data and applications security in the cloud.

With nearly uniform concern around security and data privacy in the public and private cloud, the results make it clear that a better process for achieving cloud security is not just a trend of the moment, but is a must-have for organizations of all sizes.

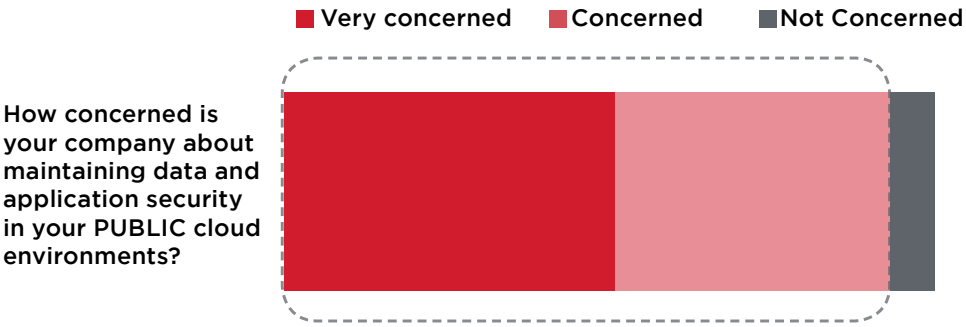


Figure 1 - 93% concerned about data and application security in public clouds.

8 Ixia Research Report: "Lack of Visibility Drives Public Cloud Security Risk," October 2017, available online.

Nearly All Companies are Concerned About Security in the Cloud

The security concerns these companies are facing are well founded. Nearly 9 out of 10 respondents indicated their companies have at some point seen a direct business impact from a lack of visibility into cloud traffic. Companies experience delays in troubleshooting application and network performance, as well as delays in resolving security alerts. These problems can result in a missed security threat or attack - making a lack of visibility the heart of the cybersecurity problem.

Which of the following issues has your company experienced from lack of visibility into PUBLIC cloud data traffic?

Select top three

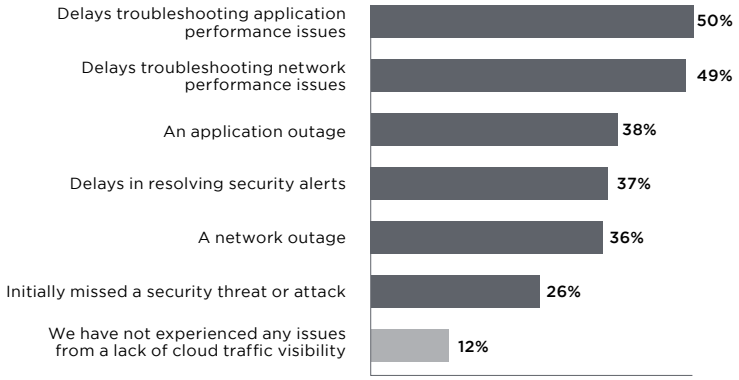


Figure 2 - 88% experienced issues from a lack of visibility into public cloud data traffic.

These concerns are rooted in the fear of becoming the next security breach headline. Unfortunately, few IT administrators have an accurate picture of what's going on inside the network, and lack the automated visibility and analytics tools that can quickly identify and act on threats. Network visibility tools help these professionals discover network vulnerabilities and user behaviors and in turn help to bolster security policies.

The security breaches that result from lack of visibility into clouds can cause customers to avoid or mistrust cloud-based services and applications. Total cloud visibility and constant monitoring can restore customer confidence and even become a differentiator for companies that go the extra mile to protect customer data and transactions.

What are your company's top priorities related to your PUBLIC cloud environments over the next 12 months?

Choose up to three

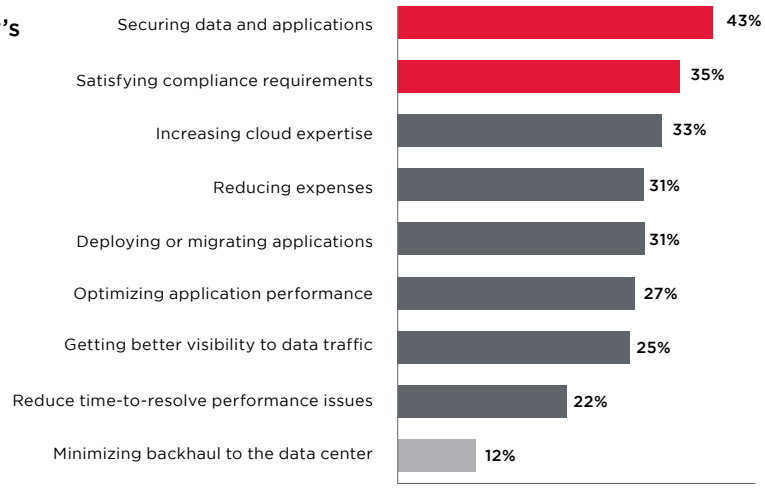


Figure 3 - Security and compliance top public cloud priorities.

Finding the Right Balance for Your Cloud Environment

Cloud computing is not a simple IT initiative – the move to a cloud environment brings with it a loss of control over the underlying infrastructure and introduces risk to the information being stored there. Reflecting this reality, the top priorities of public cloud users are security focused.

While securing data and applications may take precedence, with 43 percent of respondents stating this as a top priority, satisfying compliance requirements is not far behind, with 36 percent of respondents stating this as a top priority in the cloud. Compliance is a large area of focus for companies in highly-regulated industries such as financial services and healthcare, partially in wake of the long-awaited General Data Protection Regulation (GDPR) coming into force on May 25, 2018.

Organizations must take control of their data to align with this focus on security and compliance, as there is no other way to be more accountable to your customers than through full visibility.

Security and compliance are the top two concerns of public cloud users.

Take Steps to Strengthen Your Cloud Security

Once an enterprise begins using public cloud infrastructure, the potential attack surface expands to include attacks on the cloud provider, as well as the provider's other clients. Most providers employ strong security measures, but they still face the same threats as traditional networks—the only difference is that, as a customer, you do not have as much control over what is done to safeguard against these threats.

The scope and monetary value of a successful attack on shared infrastructure can be extremely attractive to hackers and cyber terrorists.

The most serious attacks include:

- **Data breaches:** If your cloud provider suffers a data breach, you may suffer exposure of sensitive customer information that could lead to serious financial or legal consequences, as well as damage to your brand.
- **Denial of service:** These attacks take advantage of vulnerabilities in Web servers, databases, or other resources to disrupt a cloud service, sometimes as a distraction while another attack is taking place.
- **Insecure interfaces:** The connectors of digital services are the most exposed part of any system and are frequently targeted. If the mechanisms used to manage systems, move data, and conduct admin tasks are compromised, an attacker can get access to almost anything or incur considerable unauthorized charges the company would be legally liable for.
- **System vulnerabilities:** In multitenant computing, vulnerabilities in one environment can lead to an attack on an adjacent tenant with shared resources. The source is often poorly implemented or unpatched software.

TOP CLOUD THREATS

1. Data breach
2. Weak access management
3. Insecure interfaces
4. System & app vulnerabilities
5. Account hijacking
6. Malicious insiders
7. Advanced persistent threats
8. Data loss
9. Insufficient due diligence
10. Abuse of cloud services
11. Denial of service
12. Shared technology issues
13. Hardware flaws

Source: Computer Security Alliance, update to The Treacherous Twelve, October 10, 2017, accessed online.

Accept Responsibility for Monitoring Your Data and Applications

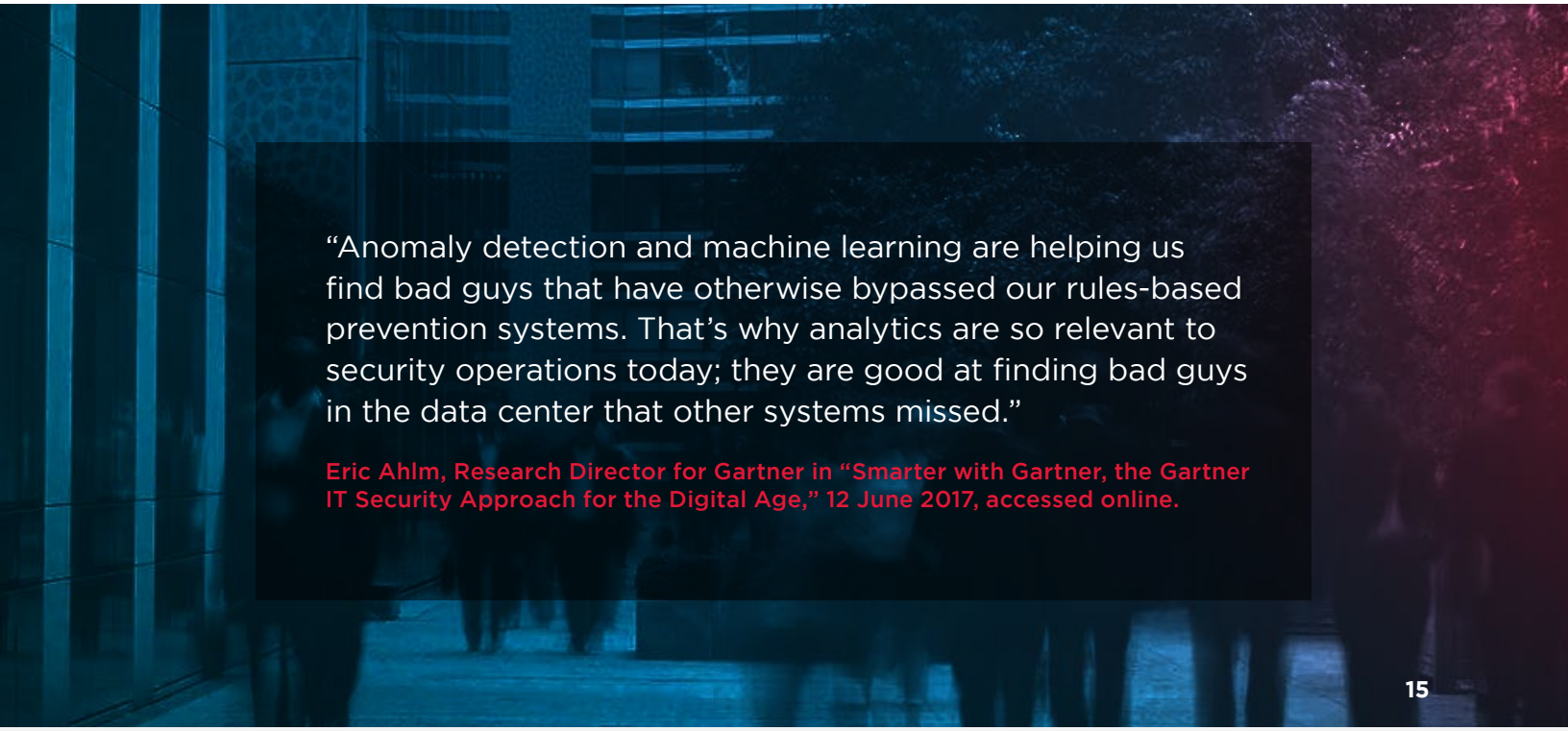
Moving to public cloud eliminates the burden of operating the infrastructure, but organizations are still responsible for the security, availability, and performance of their services, no matter whose equipment they run on. Therefore, cloud adopters must make sure their security solutions have all the data and metadata they require to defend against security breaches, data loss, and business disruption.

In some organizations, the pressure to achieve cost advantages and speed associated with cloud deployments or having a "cloud first" mandate can divert attention away from the basics of security enforcement. For example, data breaches reported in 2017 at Dow Jones and Verizon were attributed to faulty implementation of Amazon Web Service (AWS) security options[9]. Persistent, multi-layered security is, therefore, the best way to defend enterprises against security breaches, data loss, and business disruption.

Visibility is the Foundation of Security

Most organizations invest considerable time and money implementing sophisticated and advanced security solutions to examine data packets and identify threat signatures or suspicious behavior. Unfortunately, they do not always ensure these critical security solutions have all the data they need to perform effectively. Traffic in the cloud is not as easily observed as traffic moving between physical devices in the data center. To be effective, your security systems must have full transparency to every data packet that flows in your organization, including metadata about that packet. This type of data is not readily available from cloud providers, and organizations need alternative methods to fully expose data in the cloud. This is the role of a cloud visibility platform.

9 Conner Forrest: "Massive Amazon S3 leaks highlight user blind spots," Tech Republic, 18 July2017.



"Anomaly detection and machine learning are helping us find bad guys that have otherwise bypassed our rules-based prevention systems. That's why analytics are so relevant to security operations today; they are good at finding bad guys in the data center that other systems missed."

Eric Ahlm, Research Director for Gartner in "Smarter with Gartner, the Gartner IT Security Approach for the Digital Age," 12 June 2017, accessed online.

Deploy Every Cloud with Visibility

The most straight-forward way to get complete transparency to cloud data is to include visibility automatically as a component of each cloud instance or virtual machine deployed. A cloud visibility platform gets access to data in public clouds by embedding an agent or container-based traffic sensor inside each cloud instance the user deploys. The sensor makes copies of all the data passing through the cloud instance. In private clouds, a virtual network tap inside the hypervisor performs a similar function. In both cases, visibility scales automatically every time a new cloud instance or virtual machine is deployed.

The mirrored traffic can be filtered and sent to a cloud visibility platform that aggregates packets from multiple sources, processes as necessary to remove duplicates and unnecessary packet data, pinpoints traffic of interest, and delivers it to security solutions located in the cloud or on-premises. A centralized, Web-based interface is used to manage the visibility platform across the entire enterprise (see Figure 4). The Ixia CloudLens visibility platform can aggregate data from multiple cloud providers to simplify visibility management. Filtering policies are configured using simple drag-and-drop technology; no programming or training is needed to get the solution up and running.

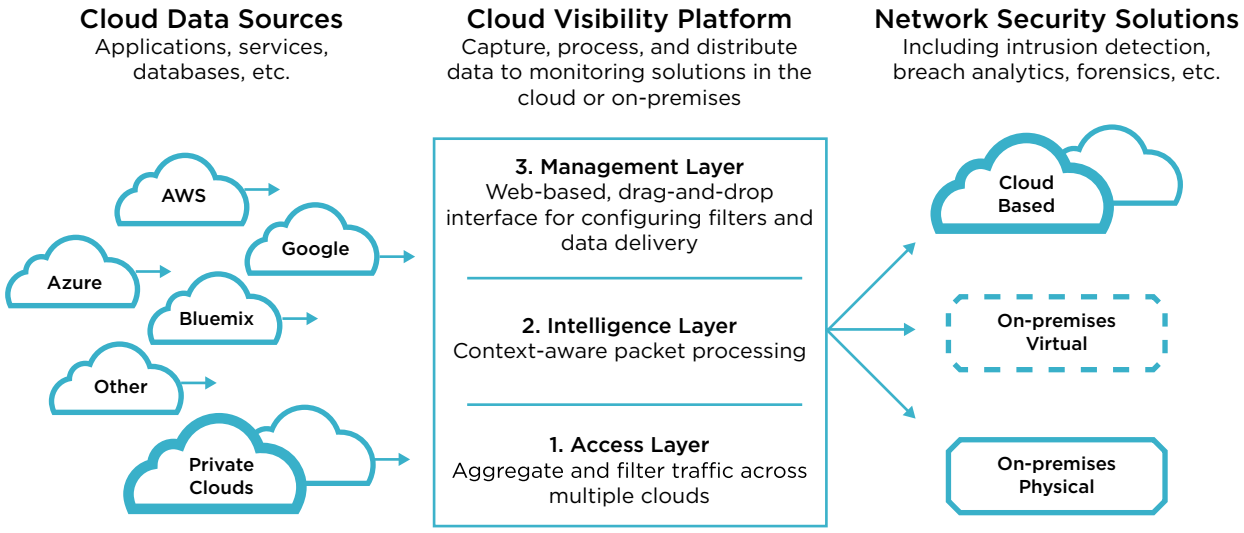


Figure 4 - Visibility platforms with a cloud-based management interface can provide access across multiple cloud environments.

Ensure Visibility is Scalable and Resilient

Deploy visibility that is as flexible as your clouds

Once deployed, your cloud visibility platform becomes a key component of your security system. It must scale along with your clouds, so there are no blind spots that are unexamined by your security solutions. This can be achieved using a cloud-native and container-based solution that is completely distributed, so it scales without limit, just like your clouds. Integration and pre-validation with popular cloud security solutions means that data begins flowing to your tools automatically, with no need for manual intervention or the risk of configuration mistakes.

Your visibility platform must also be resilient, so there are no disruptions in monitoring that give intruders an opportunity to act. This means there can be no single point of failure in the components that collect, filter, and distribute data to your security solutions. A visibility platform that relies on a single, monolithic processing engine—common in data center solutions retrofitted for the cloud—is dependent on that component to provide data access and is limited by the capacity of that engine. With a centralized processing engine, resiliency requires having an expensive backup system available to take over in case of an outage. In contrast, a cloud-native visibility platform is naturally resilient, since processing is spread among all the cloud and virtual machine instances. If any component stops working and sending data, another is automatically spun up to replace it, while all other images are unaffected.

Monitor with Efficiency

In both public and private clouds, a visibility platform makes monitoring more efficient and cost-effective by sorting and filtering the large volume of raw traffic, stripping away unnecessary data, and pinpointing the information that is relevant to each of your security solutions. Intelligent filtering decreases overall workload, reduces the potential for congestion, and can delay the need to increase security tool capacity.

Application layer filtering

While filtering packets based on ports, Internet Protocol (IP) addresses, or protocols is common, there is additional value in being able to filter and load-balance data on the basis of Layer 7 characteristics, such as application type, access device, operating system, geography, or other customized parameters (see Figure 5). The more granular the data provided, the more the security algorithms have to work with.

Single hybrid view

Hybrid cloud environments, where data may move between public and on-premises infrastructure, can be more complex to monitor. A cloud visibility platform gathers data from both environments, filters it, and delivers it to security solutions, whether they are located in the cloud, are software-based and running on-premises, or are highly specialized hardware appliances in the data center. The cloud-based interface of Ixia CloudLens, for example, provides a single pane of glass for managing filters across both environments and any public cloud.

All-cloud without backhaul

Cloud computing is cost effective until you want to take data out of the cloud and transport it back to the data center. Providers generally charge a steep price for what they call data exfiltration. To save money, enterprises may choose to use cloud-based security monitoring solutions. It can be less expensive and faster to deliver filtered data to a solution hosted by the same cloud provider. In fact, many leading security vendors now offer cloud-native options which deliver levels of scale and performance not possible or affordable in a private/on-premises installation. 2018 will be the year that many security customers will find cloud-native security solutions that rival their traditional data center based security solutions.

Future flexibility

A visibility platform filters traffic from multiple sources using consistent rules and provides the flexibility to support a wide variety of security monitoring solutions. This consistent platform means you can maximize the tools you have today, and maintain that performance advantage even as new tools are introduced to your security stack.

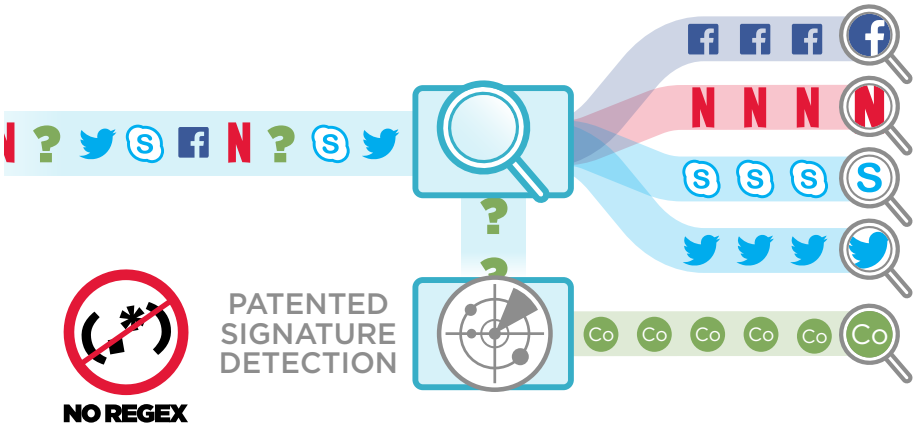


Figure 5 - Application layer filtering isolates traffic types.

SECTION
04

CLOUDS CHANGE SECURITY OPERATIONS

Not a day went by in 2017 where there wasn't at least one report of a cyberattack, data breach, or other malicious activity by threat actors. In fact, on average there were over 4.3 new data breaches per day in 2017.[10]

10 "Data Breaches Up Nearly 45 percent according to Annual Review by Identity Theft Resource Center and CyberScout," Identity Theft Resource Center press release, 25 January 25 2018.

Many of the attacks in 2017 had common root causes, such as:

- Security misconfigurations allowing access to sensitive data
- Unpatched vulnerabilities allowing threat actors to compromise remote systems
- Overly permissive security policies between entities in a supply chain

While these issues have always been present, there has been an increase in frequency of all three trends as the result of the mainstream adoption of public cloud. A 2017 study of enterprise cloud deployments found that nearly 73% had one or more security misconfigurations that could leave customers vulnerable to a data breach.[11]

These two trends – mainstream cloud adoption and high incidences of cloud security misconfigurations – suggest we are likely to see more security incidents attributed to cloud security in 2018. To combat this, organizations must evolve their cloud security operations with a security architecture that can encompass on-premises, private, and public clouds.

There is a small silver lining in 2017 cloud security trends. While the absolute number of misconfigurations continues to rise, cloud security misconfiguration rates finally peaked in 2017.[12] The availability of cloud-based visibility solutions and cloud-based security tools will help close the gap as IT develops best practices for mainstream cloud operations. We expect the gap between cloud operations and security to significantly improve as IT leaders bring greater visibility and analysis into their cloud operations.

11 "Threat Stack Analysis Reveals 73% of Companies Have Critical AWS Cloud Security Misconfigurations," Threat Stack press release, 18 April 2017.

12 Cloud Security Trends, Redlock Inc., February 2018, page 10.

Reduce Risks with Proactive Security Testing

Companies focused on risk reduction use testing to validate their security solutions are working as intended and not diminishing network and application availability. Testing simulates network traffic across protocols and applications, using production-level volume with similar bursts of activity, to let you observe the behavior of your most trusted security devices. Test results help you understand if your security solutions are scaling with your clouds and working as effectively as they do in the data center. Simulations measure what level of service is provided during an attack and how long it takes to recover. Some companies run these tests routinely when evaluating any new security solution.

Security test platforms

An integrated test platform gives users more granular control over test scenarios to more accurately reflect real-world network conditions. Advanced testing features will increase the insight you get from testing.

- **Hardware-based load modules** allow multi-terabit emulation of complex traffic, including SSL-encrypted traffic and high-volume bursts of cloud activity to observe how congestion affects latency, throughput, and concurrent processing.
- **Flexible, user-controlled simulations** let you specify a customized mix of traffic with hundreds of real-world application protocols from a single port to validate the stability, accuracy, and quality of your cloud environments.
- **Integrated threat intelligence** injects thousands of actual attacks, malware, and botnet activity into the testing mix. Some platforms provide specific DDoS attack simulations to prepare for one of the biggest and most common threats to any organization.
- **Integrated traffic recording** lets you include copies of production network traffic in your simulations to further increase the relevancy of testing results.
- **Pay-as-you-go option** matches the needs of today's networks by eliminating the need for capital investments in testing infrastructure.

> Be proactive about validating your security infrastructure using the most realistic simulations possible.

SECTION

05

FOCUS ON ANALYSIS AND DETECTION

As daily news stories continue to document, enterprises are struggling with how to prevent security breaches. Not only do breaches affect the company brand, but they continue to cause economic losses, as well.

In the current business climate, it is not a matter of if your network will be attacked, but when. The focus of security has turned to how quickly you can detect, respond, and recover from a threat.

In 2018, intrusions and breaches are the two issues most likely to keep chief information officers (CIOs) and chief information security officers (CISOs) up at night.

Not so long ago, the problem of securing the network was largely seen purely as an on-premises challenge. Mobility pushed and stretched IT, driving adoption of more security platforms and monitoring systems. Public cloud is forcing a wholesale shift in security architecture to one that must encompass both public and private clouds concurrently.

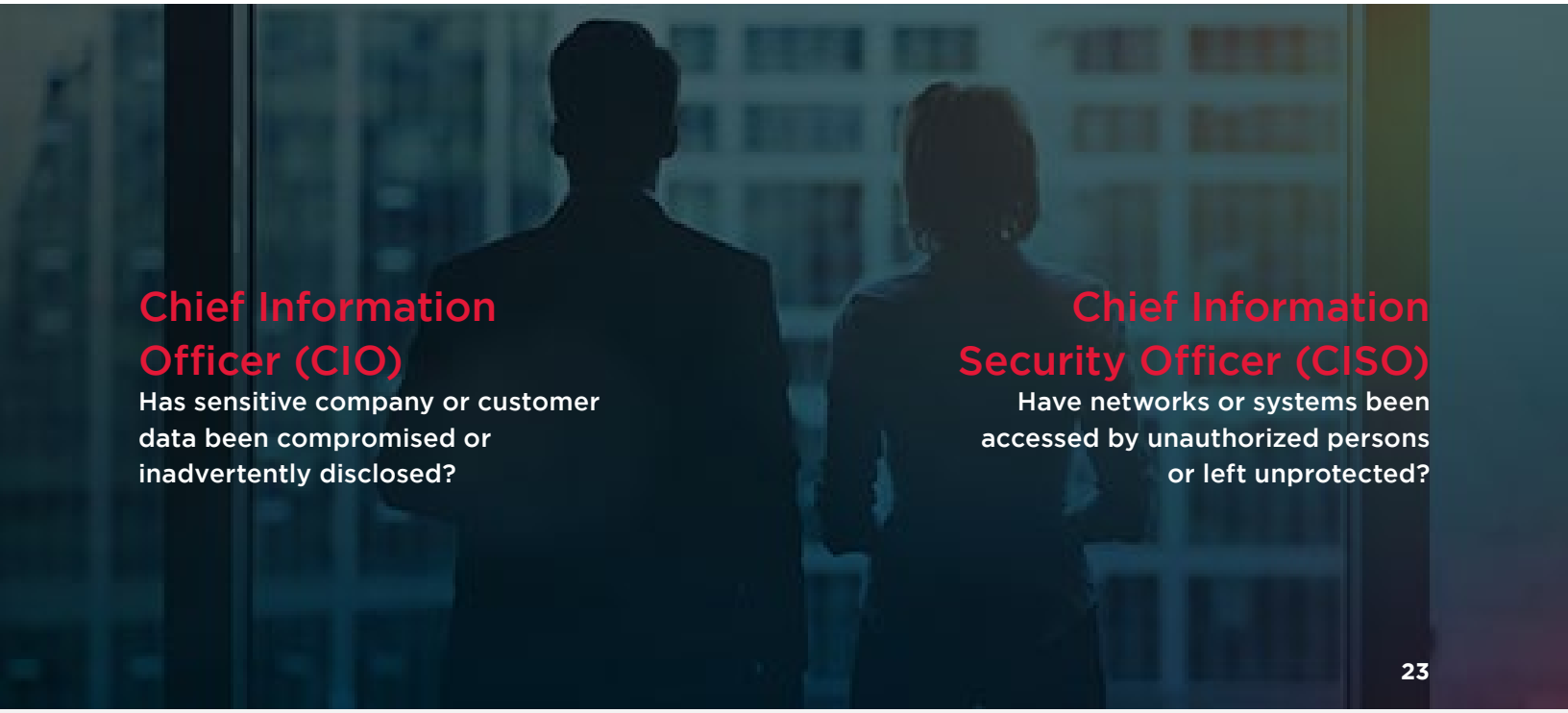
The response in the last several years has been to throw more and more technology at the problem. One report found that over 45% of CISO respondents were using 11 or more security solutions, up from 28% in 2016, and nearly 75% found it challenging to orchestrate activities across those solutions[13].

Another disturbing trend called out in the same study is that 44% of alerts are not investigated[13]. The volume of threats and diversity of threat types can quickly overwhelm any one tool, dashboard, or security professional.

This is where a wholesale shift in the mindset surrounding enterprise security is needed, to understand that security is intrinsically linked with achieving total network visibility. Robust security starts with a visibility and monitoring solution that can inspect all traffic flows across the enterprise, including modern data center and cloud architectures. Building on that is a layered security approach. Here, an intelligent packet broker can filter and feed relevant traffic flows to specific security, compliance, and monitoring systems, as required. Continuous testing and validation against the most current threats is a strong safeguard in the ever-changing threat landscape. Given 73% of security violations are rooted in misconfiguration[14], it is crucial to vigilantly test and assess both your application environment and your security stack for proper operations.

13 Cisco 2018 Annual Cybersecurity Report, page 48, available online.

14 "Threat Stack Analysis Reveals 73% of Companies Have Critical AWS Cloud Security Misconfigurations," Threat Stack press release, 18 April 2017.



HOW DO YOU GO ABOUT ENSURING YOUR SECURITY IS RESILIENT?

Think of security as **a three-tier approach:**

Tier 3:
Continuous testing and assessment

Tier 2:
Multi-layer security, compliance, and monitoring solutions

Tier 1:
Integrated visibility to data in on-premises data centers and private, public, and hybrid clouds

Resilient Security in a Hybrid IT Environment

Integrating Security and Visibility Architectures

One of the biggest challenges for security professionals today is to get the network information they need, when they need it, so they can make informed decisions about network security and problem resolution. Adequate network visibility is the solution. If you cannot see some segments of your network or certain types of traffic, how do you know that your network has not been breached? If your network has been breached, how can you tell exactly what was affected? Achieving full visibility helps address the fundamental concerns that CIOs and CISOs have.

With the proper visibility architecture in place, you will be able to see what is, and what is not, happening on your network. Having the proper data offers huge value for managing network security. When you integrate your security architecture with your visibility architecture, you will equip yourself with the necessary tools to properly visualize and diagnose the problems on your network.

When private and public cloud operations are added to the mix, traditional network taps are not sufficient to provide visibility. In the data center, critical "east-west" traffic is often invisible to normal security tools. In the public cloud, instances are ephemeral and mobile, and not tied to any specific hardware. In these cases, virtual taps used in conjunction with a network packet broker or SaaS visibility management platform deliver the relevant, filtered packets to the appropriate security solutions. With infrastructure that scales on demand, visibility needs to be established just as easily and quickly to ensure every packet is available for inspection and monitoring.

53%
of compromised victims did not detect the breach themselves[15]

191
average days from intrusion to identification[16]

66
average days from identification to containment[16]

15 M-Trends 2017: A View From the Front Lines, Mandiant: A FireEye Company, page 7, accessed online.

16 Ponemon Institute: 2017 Cost of Data Breach Study, conducted in the U.S and sponsored by IBM Security, page 3, accessed online.

Multi-Layer Security, Compliance, and Monitoring

Building on an integrated security and visibility architecture gives the enterprise a powerful tool to improve its security posture, maximize the performance of its existing security stack, and improve tool efficiency. Pre-filtering to eliminate known bad traffic so it doesn't flow through your firewalls and other solutions reduces the number of security alerts that can cause alert fatigue and data overload. This frees human and machine resources to focus on suspicious traffic and potential threats. Similarly, tools that help monitor and visualize your data can be a powerful addition to quickly spot unusual behavior on the network.

Whether in the enterprise or cloud environment, the ability to dig deep into the traffic is crucial in a layered security approach. Decrypting SSL to unmask both legitimate and malicious traffic ensures security devices can do their job optimally. Removing personally identifiable information from data streams is required for compliance.

Organizations may wish to be selective about which traffic they send through their layered security stack. For example, many organizations may wish to skip or truncate the large volume of inbound streaming traffic from Netflix. Advanced filtering makes it easy to deliver only the most relevant traffic to your security stack.

Finally, an increasing number of security tools are now available natively in the cloud. Whether available as a virtual machine or as a native cloud-scale offering, the ability to consume data loss prevention (DLP), intrusion prevention (IPS), and application performance management (APM) functions from the cloud is changing the way the CIO and CISO approach security.

75%

of respondents rate the maturity of their vulnerability indentification as very low to moderate

12%

have no breach detection program in place

35%

describe their data protection policies as ad-hoc or non-existent

38%

have no identity and access program or have not formally agreed such a program

Source: EY Global Information Security Survey 2017, conducted with 1200 worldwide leaders of security management.

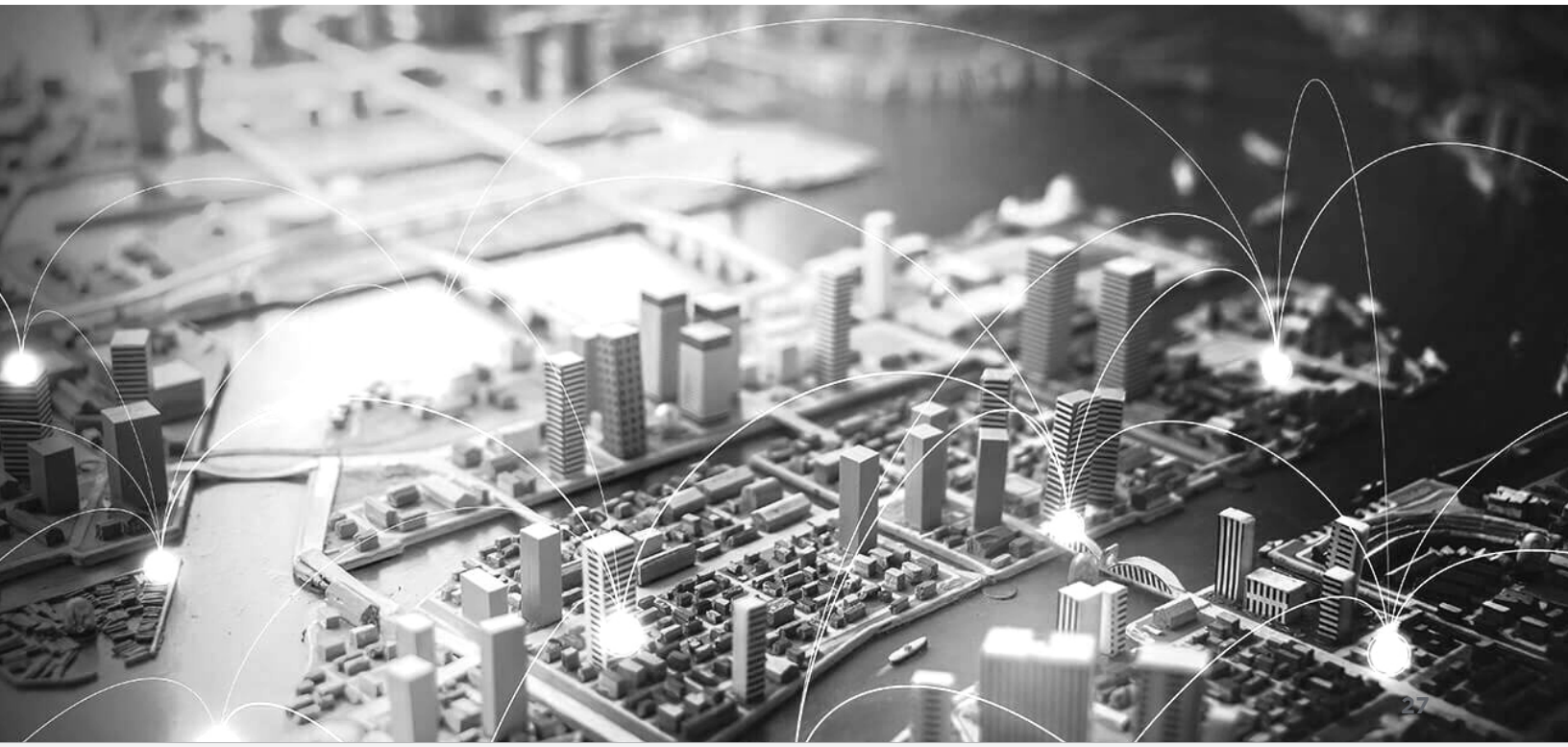
Continuous Testing and Assessment

Validating your application and security infrastructure using a realistic mix of traffic types, at cloud-scale volume through traffic simulations provides multiple benefits. It acts as a safeguard against misconfiguration and logic errors, validating that your visibility layer is performing optimally, and also validating that your security tools are operating and performing as intended.

Using traffic captured from your production environment increases confidence that the systems will perform as expected in a live environment. Mixing in the latest threats and transaction models ensures the performance and resiliency of your entire environment. This is particularly valuable when the latest security updates include newly discovered threats, which may reveal areas in your infrastructure that require attention before a malicious actor discovers them.

As environments become more complex with more interdependencies, more clouds, and more specialized security solutions, continuous security assessments can provide faster feedback. Armed with relevant and timely metrics, security teams can focus on the areas of greatest risk and limit the cost of security incidents.

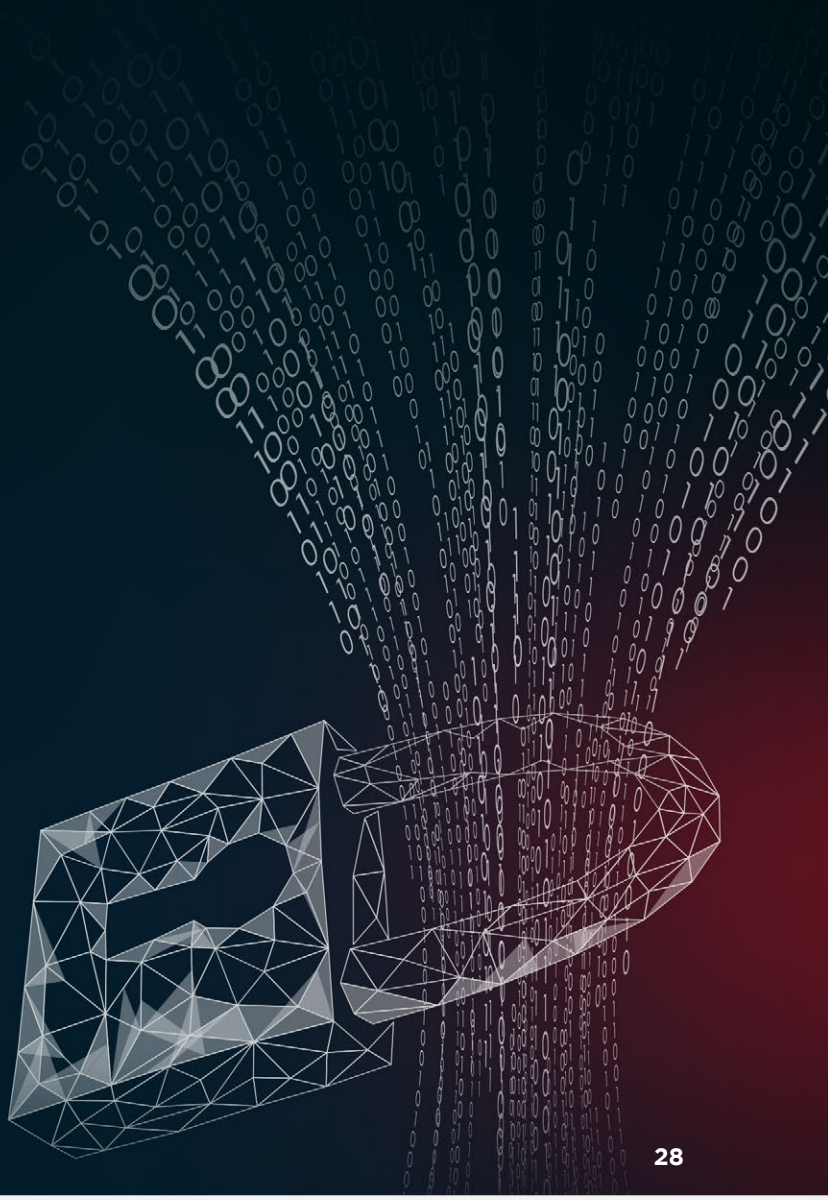
Active testing offers training and process benefits as well. Simulating attack environments gives your team valuable experience in dealing with a live threat. Simulation allows you to assess how long it takes to respond, how long it takes to recover, and lets you drive continuous improvement and learning within your organization. You will know precisely how your systems will respond, build team confidence, and identify process improvements -- before a breach occurs.



SECTION
06

CYBERCRIME IS GOOD BUSINESS

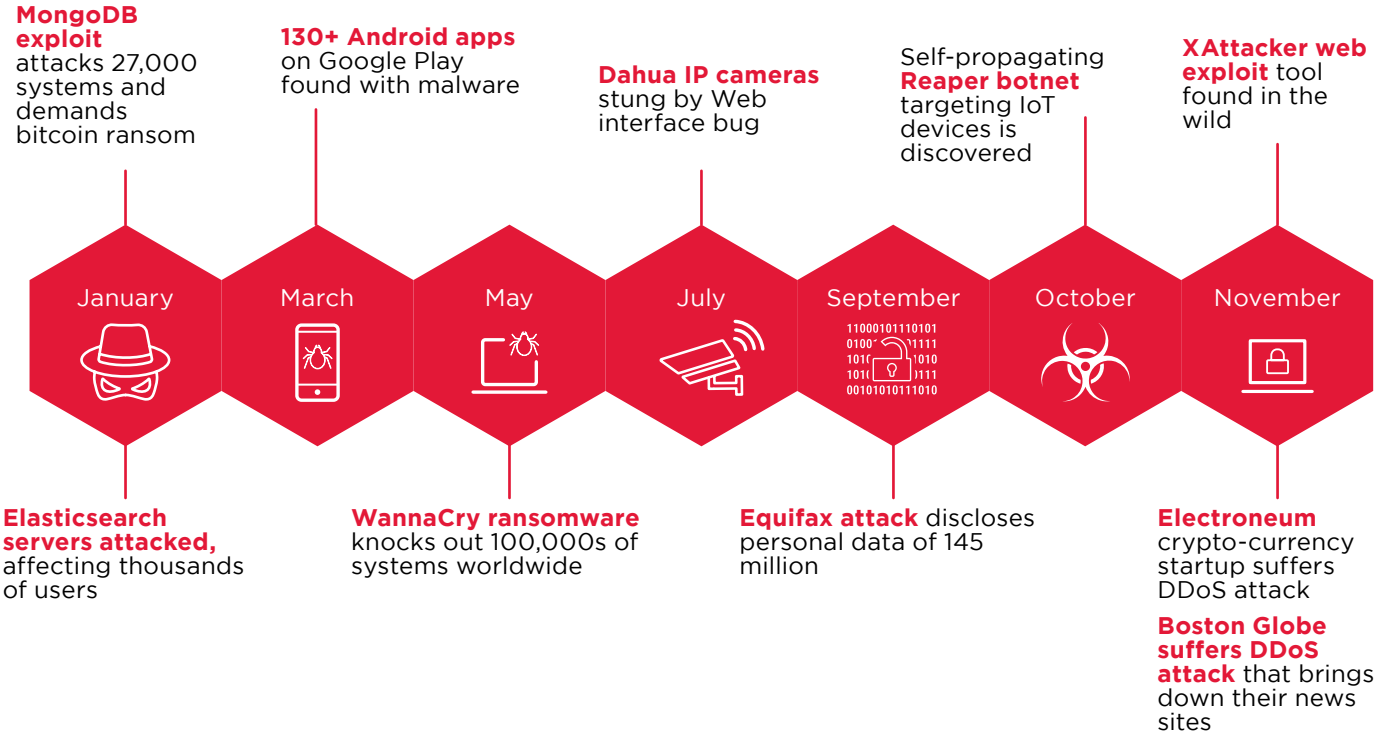
Cyberattacks linked to the U.S. presidential election made news throughout 2017 and similar attacks are being seen in other regions as well in 2018. As we finalize this report, Facebook is now admitting they need to do a better job protecting their customers' personal data. Cybersecurity is now a topic being raised in the general news directed at average citizens, not just technical professionals.



Another major news-making topic in 2017 was the breach of credit reporting agency Equifax. The breach could have been prevented if a solid patch policy had been implemented at Equifax. What is not in dispute is that this single event led to the compromise of confidential information for 143.5 million US citizens[17].

For IT security professionals, 2017 was the year of ransomware. Although not so visible in the general news media, ransomware attacks were a major source of lost time and money for many companies. In its 2017 Ransomware Damage Report, Cybersecurity Ventures estimated global ransomware damages to cost $5 billion in 2017, up from $325 million in 2015 — a 15X increase in just two years. They further predict that global ransomware damages will double and exceed $11.5 billion annually by 2019[18].

Security Headlines of 2017



17 Lily Hay Newman, "Equifax Officially Has No Excuse," Wired.com, 14 September 2017.

18 2017 Ransomware Damage Report, Cybersecurity Ventures, 14 November 2017, accessed online.

Ransomware

morphed in 2017 into a more malicious type of threat. The WannaCry and NotPetya outbreaks caused global panic and caught many organizations off-guard. According to trackers, the number of infections has continued to increase, but the number of new ransomware families appears to have slowed in the second half of 2017. This may be because the market is now dominated by professional gangs that have driven out the opportunists.

Our month by month "threatrospective" shows the dominance of ransomware throughout the year.

JANUARY

THREATS

Sage Ransomware: Variant of CryLocker ransomware with engaging user interface is distributed by the Sundown and RIG exploit kits.

IXIA INSIGHTS

Defend yourself by knowing where ransomware comes from. Read our blog: Protect yourself from ransomware.

FEBRUARY

THREATS

Spora Ransomware: A solid encryption routine, ability to work offline, and a very well put together ransom payment site.

IXIA INSIGHTS

Prepare for another year of ransomware. View our webinar: Ransomware – Not the What, but the How.

143.5 million
U.S. residents were affected by Equifax breach[17].

15x increase
in ransomware damages paid over the past year[18].

MARCH

THREATS

DNS Amplification Attack: Generates responses 10 or more times larger than the query sent. For every 1 megabit of traffic sent, 10 megabits is sent to the victim.

IXIA INSIGHTS

Protect yourself from vulnerabilities and weaknesses. Read our blog: Root DNAME Query Responses in DNS-BIND.

APRIL

THREATS

Dahua Vulnerability to DDoS: Password disclosure vulnerability can turn a Dahua IP camera into a DDoS attack.

IXIA INSIGHTS

Ixia researcher identifies DDoS flaw. Read our blog: How I Made My Camera into a DDoS Cannon.

Ransomware costs include damage and destruction of data, lost productivity, disruption to the normal course of doing business, forensic investigation, restoration and deletion of hostage data and systems, reputational harm, and employee training in direct response to an attack, in addition to the actual ransom payouts.

MAY

THREATS

Drive-by Downloads: Malware delivery through an exploit in the user's browser without the user's consent or knowledge.

IXIA INSIGHTS

Protect yourself from vulnerabilities and weaknesses. An Ixia researcher deconstructs this exploit in the blog: Deconstructing the Crash and Burn.

JUNE

THREATS

Wannacry (EternalBlue) Ransomware: Cryptoworm encrypts data and demands ransom payments in Bitcoin cryptocurrency.

IXIA INSIGHTS

Ixia BreakingPoint identified the underlying vulnerability and researchers posted cleanup script. Find out more in the blog: EternalBlue Exploitation in the Wild.

Failure to manage your digital risks can sabotage your digital business and expose your organization to impact well beyond a simple lost sale.

JULY

THREATS

Cerber ransomware family: This trojan on Microsoft Windows that is spread via spam emails currently has five versions.

IXIA INSIGHTS

Ixia researchers share their insight in the blog: Understand details about Cerber, what it does, and how to detect it.

AUGUST

THREATS

Equifax and Apache Struts: The Equifax data breach was totally preventable.

IXIA INSIGHTS

Check your system for vulnerabilities using the information in our blog: Learn from the Equifax breach and implement proper patching process.

Reaper

While the Reaper malware is partly based on the Mirai source code, it is much more dangerous and efficient in spreading from one compromised IoT device to another. Reaper doesn't brute-force for default SSH or telnet credentials like Mirai. Instead, this new botnet is attacking IoT devices, especially DVRs and routers, by exploiting publicly disclosed vulnerabilities that have not yet been patched.

SEPTEMBER

THREATS

Command injections: If successful, they damage a website beyond repair and possibly exfiltrate data or install a backdoor.

IXIA INSIGHTS

BreakingPoint security testing can validate your ability to detect, patch, and block vulnerabilities. Read more at: Supervisord command injection caught in wild and tamed.

OCTOBER

THREATS

Reaper botnet: Attacks IoT devices, especially routers, using publicly disclosed vulnerabilities. expected to target more devices in the future.

IXIA INSIGHTS

Keep your IoT devices safe. Don't overlook firmware updates. Learn more in: IoT Security: Strategies to Protect Your "Things" and Networks.

Ransomware aimed at cloud services is likely to be a significant threat in 2018, according to the Massachusetts Institute of Technology's annual Technology Review. Cloud providers are likely targets because they typically store huge amounts of data for customers. While the biggest and most established providers have the resources and experience to make it difficult for attackers, smaller cloud providers are likely to be more vulnerable.

NOVEMBER

THREATS

XAttacker: Website vulnerability scanner & auto exploiter can install attacks on browers that just visit a site.

IXIA INSIGHTS

ATI honeypot investigation identifies new threat. Read more: New web exploit tool found in the wild.

DECEMBER

THREATS

Crypto-mining malware: Coins being mined from thousands of malware-infected and unsuspecting web browsers and Android mobile phones.

IXIA INSIGHTS

Beware malware masquerading as mobile apps. Leverage threat subscription service to stay ahead of attacks. Read more: Everything's Better with Blockchain.

Crypto-Mining Malware Hits the Big Time

Ransomware took the digital world by storm by creating an easy way to monetize vulnerabilities in the infrastructure and applications we rely on. Many ransomware authors demanded ransom in crypto-currency such as Bitcoin, a digital currency which can be traded on the open market. The ability to easily exchange crypto-currency for other national currencies fueled explosive growth of over a dozen digital currencies in 2017.

Cryptocurrency mining—the process of confirming cryptocurrency transactions and generating new units of digital currency – is a legal and essential part of the cryptocurrency model. The model assumes an individual will use computing resources they own to "mine" the digital currency, especially when that resource is otherwise idle. However, as we have seen with command and control botnets, hackers can leverage exploits to seize control of millions of endpoints without their owner's knowledge or permission. When the power of those endpoints is turned towards mining digital currency, a hacker may be able to turn a substantial profit at the expense of others. This is not legal and is known as cryptojacking.

Research shows half a billion devices are unknowingly being used to mine cryptocurrency for others[19].

19 Anthony Cuthbertson, "Over 500 Million PCs Are Secretly Mining Cryptocurrency, Researchers Reveal," Newsweek, 13 October 2017, accessed online.

Cryptojacking here to stay, and it is shaping up to become as pervasive as ransomware. Cryptojacking used to be confined to victims unknowingly installing crypto-mining malware that secretly used their processing resources to do mining for hackers. Recently an even stealthier variant has emerged referred to as 'in-browser crypto-jacking.' This activity gains control of the victim's CPU through their web browser, which is infected by JavaScript embedded on a website they visit. No application needs to be downloaded and no action on the part of the victim is required—other than visiting a web page.

Some developers and web site owners are actively using these techniques to "leverage" their customers' processing power for crypto-mining. They see crypto-mining as a supplement to ad revenues and flagging application sales. Other web sites may be unwitting participants if hackers can embed mining malware on their web sites without them knowing.

There is evidence showing hackers using older vulnerabilities to embed mining malware after initial attempts to extort bitcoins from victims fail. As with ransomware, without a robust visibility, security, and monitoring strategy to protect applications and computers, you should not be surprised to become the next victim of cryptojacking.

CRYPTOCURRENCY MINING FEVER

220 WEBSITES
Had mining malware running, out of top 10,0000 websites

500 MILLION
Have been unknowingly mining crytocurrencies

50% FROM 4 COUNTRIES
Mining activity is most prevalent in the US 19%, India 13%, Russia 12%, and Brazil 8%

$9.5 MILLION
Potencial earnings at average of $43,000 per site over the period observed

Source: Research conducted by AdGuard over a three-week period in October 2017.

Mining Malware for the Mobile Era

With literally millions of somewhat easily-accessible and increasingly powerful mobile devices, it is no surprise that mining malware designed for mobile browsers and applications is flourishing. We have also witnessed the use of mining malware embedded in legitimate applications available on the Android store, which are used to extract value from people's phones during times when their devices are not in use.

Late last year, security firm Trend Micro discovered three Android apps on Google Play that hijack device resources without the owner's permission[20]. Google Play has since deleted those apps. And, in recent months, researchers have identified malware that continues to keep mining after the browser appears closed by hiding another browser window on the device[21].

Other methods that hackers are using to deploy cryptocurrency miners include using Telnet/SSH brute forcers attempting to install miners, along with SQL injection and direct installation of miners. Crypto-mining in browsers and mobile applications will continue to persist, so concerned companies should improve their security performance, bringing application-level visibility and context to their monitoring tools.

Top Website Categories Involved in Crypto-Mining

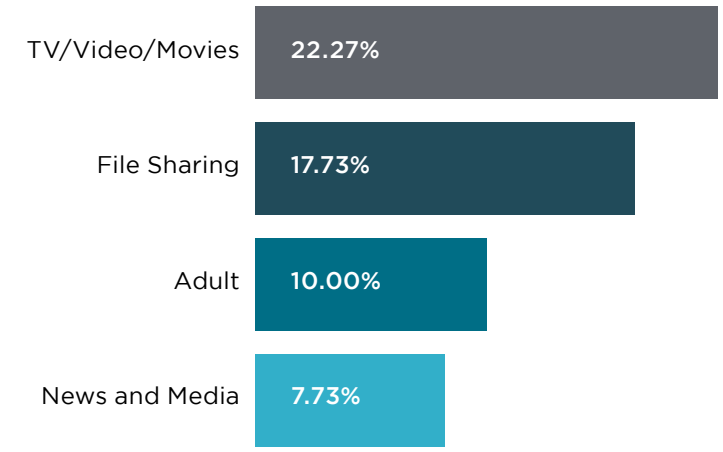


Figure 6 - Research by AdGuard in October 2017 shows over 57% of the websites involved in crypto-currency mining belong to four categories.

20 Liam Tung, "Android Security: Coin miners show up in apps and sites to wear out your CPU," ZDNet.com, 31 October 2017.
21 Nicholas Fearn, "Warning over explosion in web browser-based crypto-mining," Computing, 30 November 2017.

More Devices, More Mining

Perhaps the most disturbing target for crypto mining malware is IoT devices. A quick glance at shodan.io, the IoT search engine, shows how millions of devices, from webcams to SCADA systems, are openly discoverable and potentially exploitable. At least one report of crypto-currency mining on critical control systems was reported in February 2018[22]. And while crypto-jacking may seem like more of an annoyance than a threat, it can have disastrous effects on critical infrastructure, causing system failures which can cascade and cause loss of service and even loss of life.

Most crypto-mining attacks occur at the edge of the network. One of the more common attacks that attempts to install crypto-miners is the EternalBlue vulnerability released this past summer, which was at the center of ransomware outbreaks like WannaCry and Not-Petya. Here's the worst part: hackers are not using new tools or advanced methods to deploy these cryptocurrency miners, but they are still successful. To avoid becoming a victim, companies need to have a responsive patch management strategy, make sure their IPS rules are up to date, test to make sure they can detect the vulnerabilities that cannot be patched immediately, and finally, monitor network traffic for peer-to-peer mining and command and control traffic. We are likely to see more hybrid attacks that combine ransomware and crypto-mining in the future, as criminals attempt to cash in twice on the same computer.

> Application intelligence goes beyond threat tracking, to monitor the behavior of applications in action.

22 Lily Hay Newman, "Now cryptojacking threatens critical infrastructure, too," Wired.com, 12 February 2018.

SECTION
07

ENCRYPTION HELPS HACKERS, TOO

Encryption Can Break or Make Your Business

Last year we passed a significant milestone when, in February, Mozilla reported that approximately half of Internet traffic was protected by HTTPS[23]. The shift towards encryption continues with Google recently reporting that 81 of the top 100 sites on the web default to HTTPS[24]. You might think these trends would increase security, but some observers predict encrypted traffic will carry more than 70% of web malware by 2020[25].

On top of the increasing risk associated with encrypted traffic. IDC found in 2016 that only 25 percent of organizations were decrypting network traffic in order to inspect[26].That may not be a good strategy, since the average cost of a data breach in the U.S. is now estimated at a record high of $7.35 million[27]. To complicate matters further, the compute power needed to decrypt secure packets and peer inside is sapping the resources of the expensive and sophisticated security tools we use to keep our networks safe. Overloaded tools can start dropping packets or fail altogether. The bottom line is that if you are not decrypting and inspecting secure traffic, you are putting your data and resources at risk.

50%

of internet traffic is encrypted

81

of top 100 sites default to HTTPS

70%

of malware will be carried by encrypted traffic

75%

of organizations fail to decrypt

23 Gennie Gebhart, “We’re Halfway to Encrypting the Entire Web,” Electronic Frontier Foundation, 21 February 2017.

24 Russell Brandom, “Chrome will mark all HTTP sites as ‘not secure’ starting in July,” The Verge, 08 February 2018.

25 Jason Deign, “Seeing threats hidden in encrypted traffic,” on Cisco blog, 20 June 2017, accessed online.

26 IDC: “The Blind State of Rising SSL Traffic,” July 2016, page 1, accessed online.

27 Ponemon Institute: “2017 Cost of Data Breach Study,” page 8, June 2017.

The Type of Encryption Matters

Since the early days of the web, SSL and its descendent TLS 1.3 have governed the encryption used to secure Internet transactions. Hidden inside SSL and TLS 1.3 are two very different encryption key systems. The keys generate the ciphers that are used to scramble and unscramble data.

SSL is the older of the two and relies on static encryption keys. This makes SSL somewhat easier to implement, but also provides a fixed target for hackers, who can learn from their repeated attempts.

TLS 1.3 is more recent and relies on temporal or ephemeral keys, which are newly generated for each use. For hackers, ephemeral keys are like shooting at a moving target: difficult to hit, quick to disappear, and different each and every time.

In October 2017, Ixia published a report called, "Encryption--What's Hiding in Plain Sight,"[28] on the key preferences of major client browsers and popular web sites (servers) to observe any trends that could indicate the direction of encryption generally. The findings were clear that a major changing of the guard was taking place.

The results of the study showed that the major client browsers exhibit a preference for ephemeral encryption keys (report pages 12-14). The first 19 encryption keys preferred by browsers were of the ephemeral type. It is not until the 20th rank that a static key appears (report page 8). Trend analysis from 2011 to the present showed that out of all the browsers, Chrome appears to adapt to newer ciphers first, followed closely by Mozilla (report page 15). It's also notable that once Chrome and Mozilla decide to adopt and prefer a new key, other browsers follow.

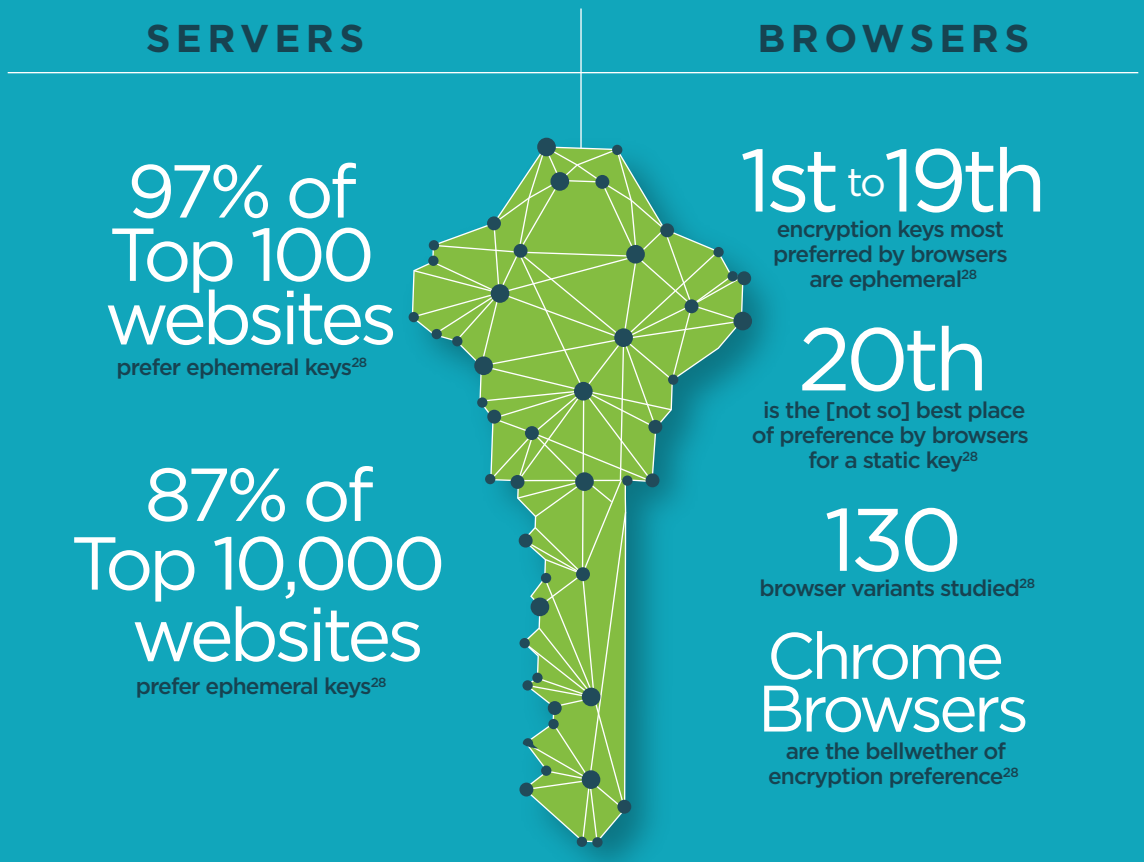
Similarly, Ixia studied the server side of the encryption equation and found that servers also prefer ephemeral encryption keys. Ninety-seven percent of top 100 websites prefer ephemeral keys (report page 17) and 87% of top 10,000 websites prefer ephemeral keys (report page 18).

> The world is getting encrypted and the encryptions themselves have changed. You need to update your infrastructure to keep up with the changes.

28 Ixia Research Report: "Encryption—What's Hiding in Plain Sight," October 2017, available online.

Ephemeral Encryption

Keys Prefered by



Use Ephemeral Encryption Keys

Design your infrastructure to support ephemeral keys

Chose vendors who optimize hardware and software for ephemeral keys

Best Practices for Encryption Optimization

Now why would anyone not use ephemeral keys over static ones? Fear of change, inertia, or older infrastructure are the most likely culprits. However, not only are ephemeral keys more secure, they don't have to require a huge change if handled according to best practices.

The main principles are to standardize on ephemeral encryption keys, design your visibility infrastructure to support ephemeral keys, and chose vendors who optimize hardware and software for ephemeral keys.

But a great visibility infrastructure based on active SSL goes even further by decrypting traffic once, and then using it many times. By deploying an active SSL visibility architecture and decrypting SSL using intelligent network packet brokers, you can provide optimized clear text data to your monitoring and security systems.

Staying Ahead of the Hackers

It takes highly skilled, experienced professionals to investigate and remediate after security incidents. Last year, ESG surveyed 412 cybersecurity and IT professionals and asked them about the size and skill set of their organization's cybersecurity team. Fifty-four percent of survey respondents said the skill level of their team is inappropriate for an organization of their size and 57% said the staff size is inappropriate[29]. Given this situation, how can organizations develop the elite cyber warriors they need to protect their business and customers?

54%
say cybersecurity skills are inadequate[29]

57%
say staff size is inadequate[29]

29 ESG: "Cybersecurity Skills Shortage: Profound Impact on Security Analytics and Operations," Jon Oltsik blog, 24 July 2017, accessed online.

HIRING CHALLENGES PERSIST

Indicate that open positions in cybersecurity take at least **THREE MONTHS** to fill.

32% of Enterprises report that the time to fill cyber security and information security positions is **SIX MONTHS OR MORE.**

More than 1 in 5 organizations get **Fewer Than Five Applicants** for an open cyber security position.

Few organizations get 20 or more applications.

Source: ISACA's State of Cyber Security 2017: Current Trends in Workforce Development

Lessons from Conventional Warfare

Attracting or developing the right skills for your organization is as important as the technology and process pieces of your cyber-security plan. Just because warfare is moving to the cyber realm, does not mean that lessons from real battlegrounds have lost their relevance and significance. The main rule from Sun Tzu's Art Of War, the ancient treatise that has provided inspiration for generations of warriors, still very much applies: if you know the enemy and know yourself, you need not fear the results of a hundred battles.

To know the enemy, aspiring cyber warriors can leverage the knowledge of security experts focused entirely on observing and characterizing today's attacks. The Ixia ATI Research Center, for example, offers information on to 6,000+ live attacks and 35,000+ malware, plus 330+ application signature families, DDoS and botnet attack simulations. To stay current, the Center continuously updates its database with the latest application profiles and threat characteristics by analyzing billions of IP addresses and URLs and millions of pieces of spam.

To know themselves, the cyber defense team needs to be tested in realistic conditions. Computer based training can only take learning so far. To help the team gain actual experience, enterprises can give trainees the chance to react to realistic simulations in a multi-vendor production-like environment. Integrating a traffic recording solution lets you incorporate several days worth of actual traffic from your production network to create your test simulation.

The Best Warriors Train, Train, Train

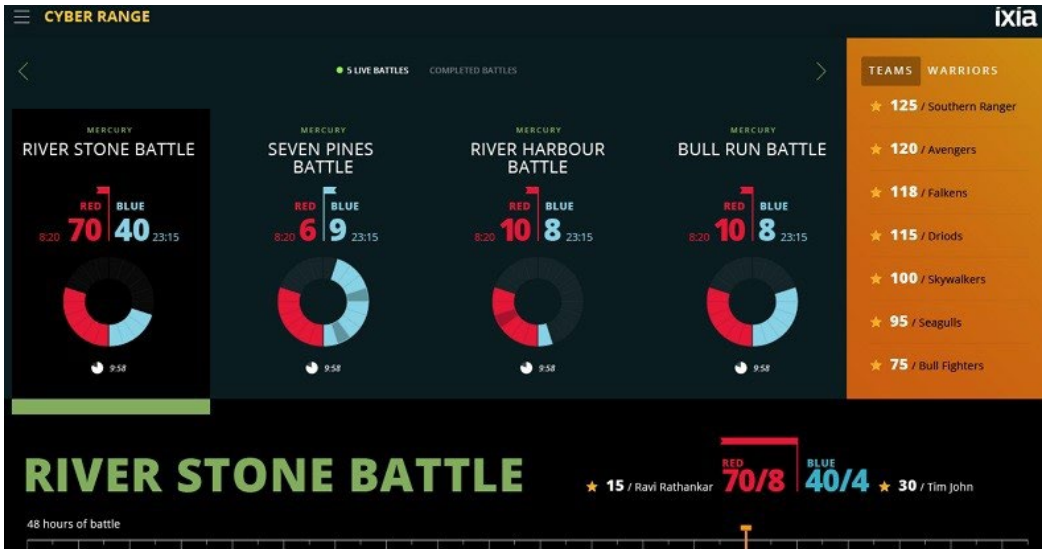
The renowned Spartans trained as soldiers continually from age 7 to age 60. The Roman gladiators trained to be combat-ready by using a wooden weapon called a palus that was double the weight of an actual combat weapon. And modern day elite warriors--US Navy seals--train to the breaking point during Hell Week.

Similarly, the best cyber warriors need to train continually to be combat-ready by testing themselves in simultaneous scenarios and against multiple enemies. They need training environments that feature scalable real-world traffic and current attacks. Finally, a high-performance cyber training program needs to constantly integrate new scenarios and attack elements to build up the level of adaptability elite cyber warriors need in real-life situations. As the US Marines say: "Improvise, Adapt, Overcome." Your threat intelligence solution should regularly feed new live attacks, malware, and application signatures to your simulations, so your cyber cadets face new situations every time they practice.

Track Progress With Metrics

Training is meaningless without the ability to assess the acquired skills and drive for results. Capturing and reporting key performance indicators in a dashboard gives individuals and their managers measurable goals to assess progress. A dashboard like Ixia's Cyber Range, shown below, reports scenario success rates, red team performance, blue team performance, and individual cyber warrior performance.

A fully-calibrated system of training helps cybersecurity warriors know themselves by giving them the information they need to focus on building strength through continued practice at the cyber range.



Example of Cyber Training Dashboard (Ixia Cyber Range)

SECTION

08

CONCLUSION

In our increasingly digital and connected world, security is an ever-present challenge. Human ingenuity and creativity drive both the solutions we develop and the threats we face. For that reason, we must continue to push forward and implement solutions that are continuous and resilient, stress detection and response, and seek to shrink our attack surface and risk profile.

We hope the 2018 Security Report will help you open new dialogues in your organization and help you tackle the challenges ahead.

Here are some final takeaways:

- **Security is dependent on total network visibility.** Do not lose sight of the foundation of security monitoring: "You can't protect what you cannot see." As network complexity grows, simple traffic visibility needs to keep pace. Work to understand how blind spots develop and how to eliminate them.
- **Make resilient security your goal.** The focus of security has shifted to from a single pre-deployment event to a continuous practice, designed to detect threats as fast as possible and limit the damage. Make sure your detection and analysis solutions have the real-time packet data *they* need to deliver the results *you* need. Use automation between your visibility platform and security solutions to enable near real-time reactions.
- **Deploy every cloud with total visibility.** Cloud environments can be attractive to hackers and bad actors and cloud providers are only responsible for securing the physical infrastructure. Take responsibility for securing your cloud data and applications with visibility to packet-level data and realistic testing of all your cloud environments.
- **Reduce risk with proactive security testing.** Testing gives you the insight you need to understand how your security infrastructure reacts under attack, so you can address weaknesses and accelerate recovery. As we rely more on software-defined resources and data centers, we need to verify that the architectures we build and integrate actually perform as expected.
- **Ensure your visibility platform supports ephemeral key decryption.** Secure traffic is the de facto standard for internet communication and transactions. Keep up with evolving encryption standards by ensuring you can decrypt and inspect secure traffic encrypted with ephemeral keys.
- **Vigorously train your cyber defense team.** Effective cyber warriors must have access to a rigorous training and practice environment. Make sure your team is prepared for battle using cyber range training.

Let us know how we can help you secure your network, data, and applications. Contact us at www.ixiacom.com. Ask for a demo and we will show you what is possible.

Learn more at: www.ixiacom.com

For more information on Ixia products, applications or services, please contact your local Ixia or Keysight Technologies office. The complete list is available at: www.ixiacom.com/contact/info

Find us at www.ixiacom.com

915-8260-01-5081 Rev A |