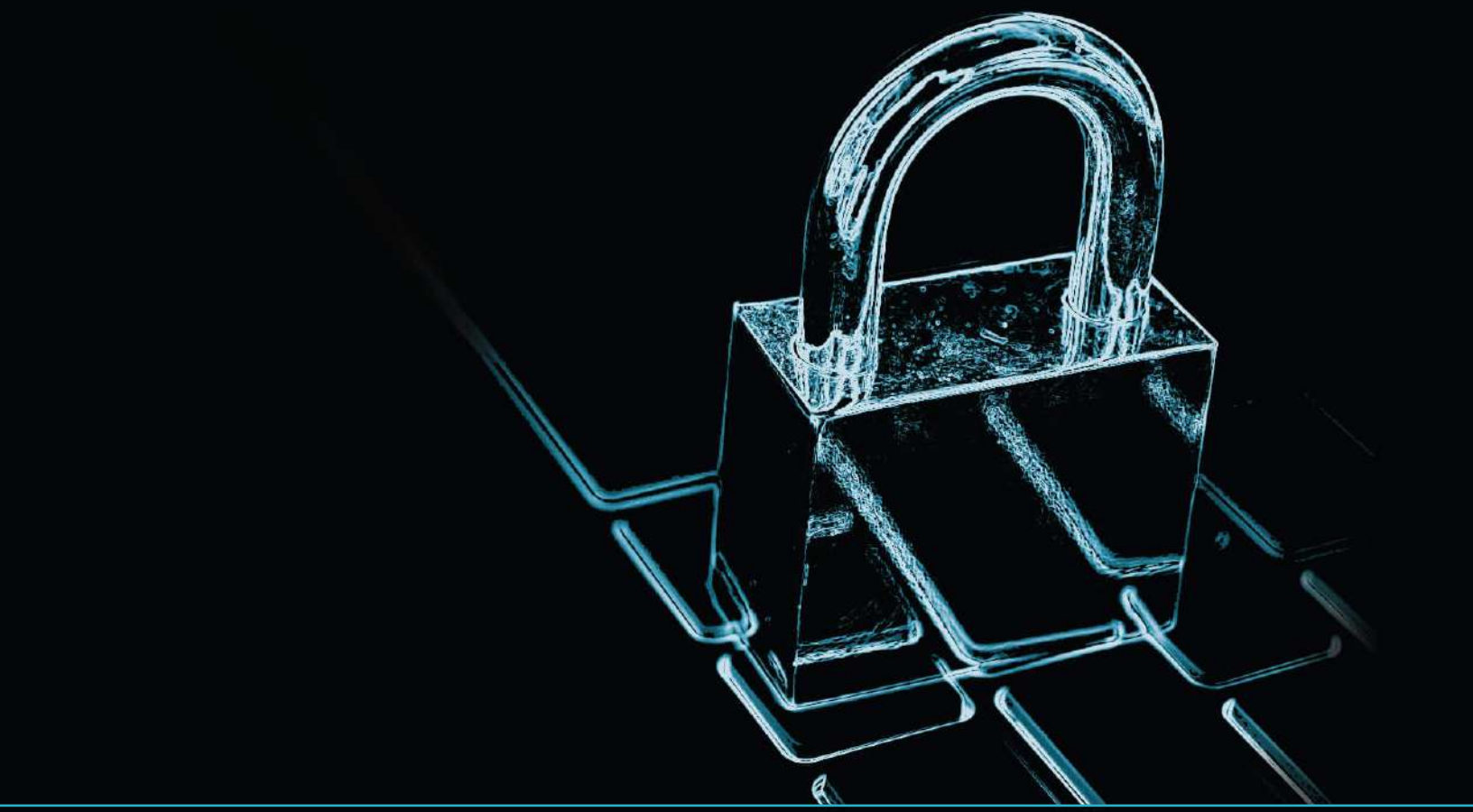
SECURITY REPORT

2017



ixia

SEE INSIDE

915-8136-01 Rev A

TABLE OF **CONTENTS**

01 Introduction
PAGE 3

02 The Shifting Environment of Network Security
PAGE 6

03 Dimensions of Security Expansion
PAGE 17

04 New Environments, New Threats
PAGE 25

05 Looking Ahead
PAGE 40

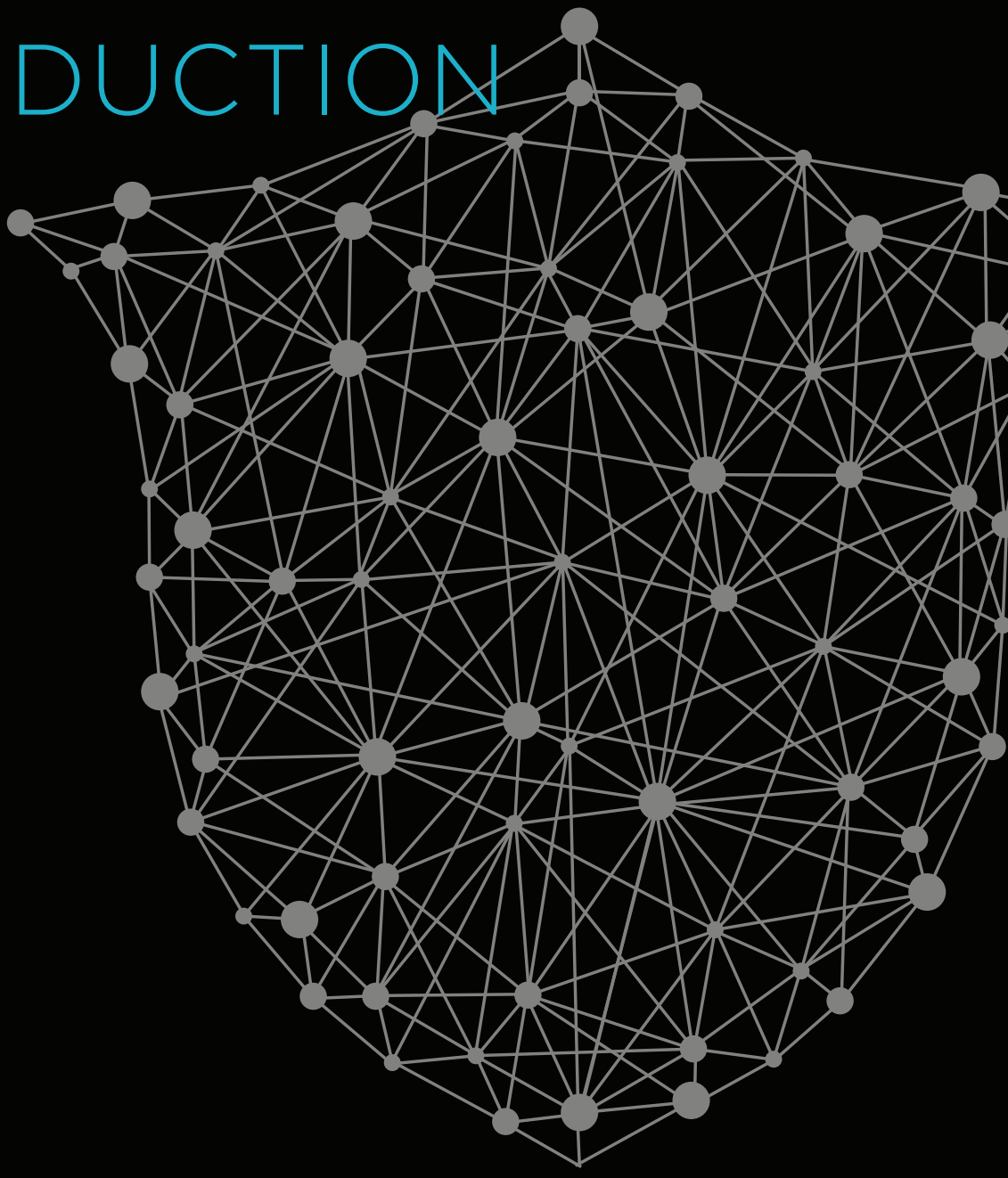
06 Identifying Vulnerable Areas
PAGE 46

07 Conclusion
PAGE 53

SECTION

01

INTRODUCTION



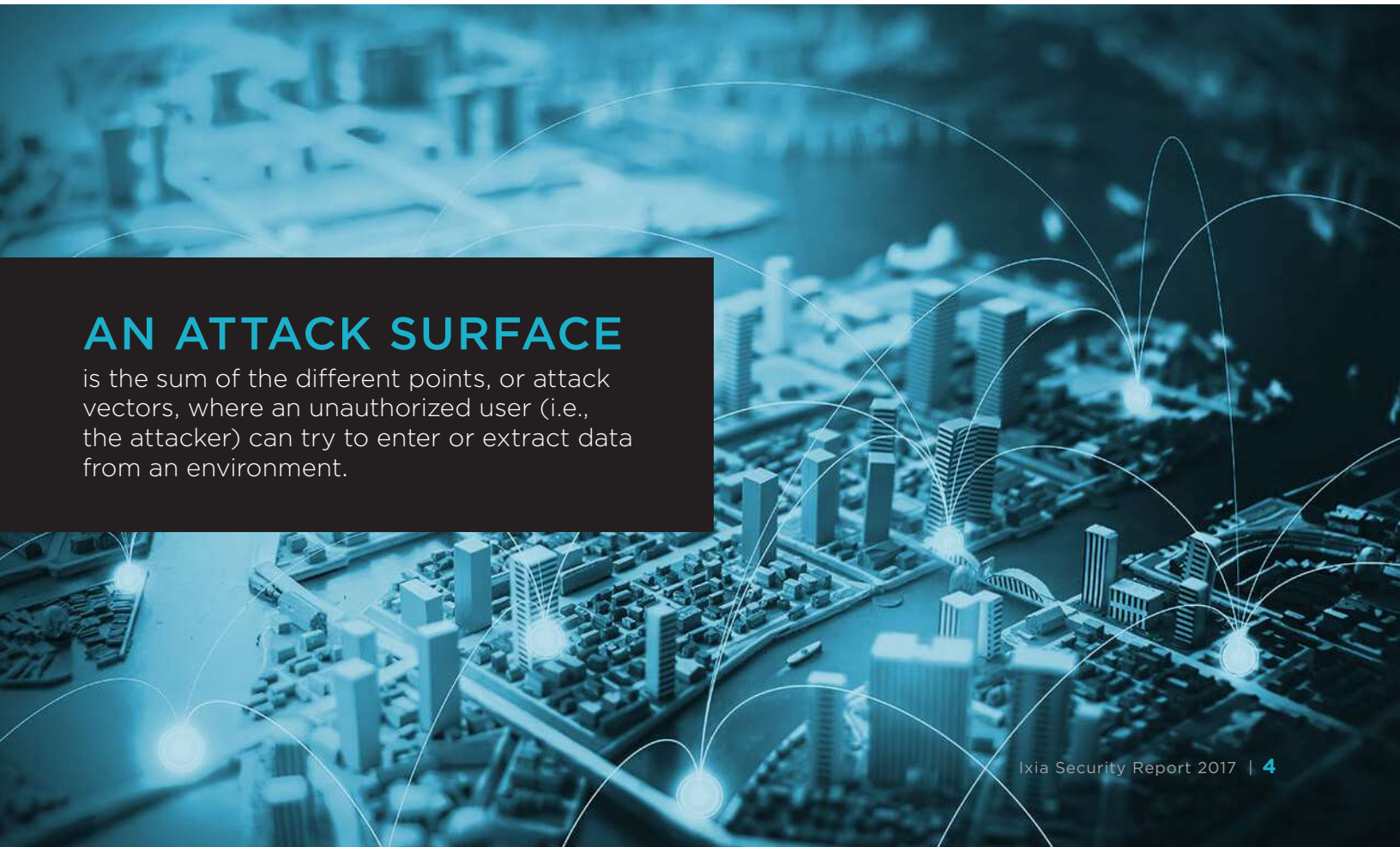
INTRODUCTION

In 2017, Ixia will celebrate its 20th year in business as a trusted source for comprehensive testing in the networking industry. Over these two decades, Ixia tests have been used to validate network routers, switches, servers, and firewalls. In addition, Ixia tests have validated cellular and Wi-Fi infrastructures, as well as a who's who of network security appliances, analytics appliances, compliance systems, storage systems, and network performance improvement solutions. Network Equipment Manufacturers, called NEMs, rely on Ixia tests to validate their latest appliances before shipping them to customers.

Our test business wrestles with a few constant trends. We simulate ever-increasing load environments for individual appliances—as well as end-to-end networks—with our test products.

Every year, data rates increase. Every year, network protocols expand and become more capable. Every year, a wider array of appliances enter the market and must be managed, optimized, and secured. This complexity has become its own vulnerability within many organizations, dramatically increasing attack surfaces. As a result, the information technology (IT) community has grown dramatically.

All IT organizations are conscious of their networks' attack surface. Enterprises, service providers, and data centers alike worry about every new device they insert into their networks, because they understand that any of these devices could create a vulnerability. But the attack surface is not just about growth in threats. It increases with the growth in IT complexity in three specific dimensions: (1) the number of data locations where data resides, (2) data throughput, and (3) IT tool complexity.

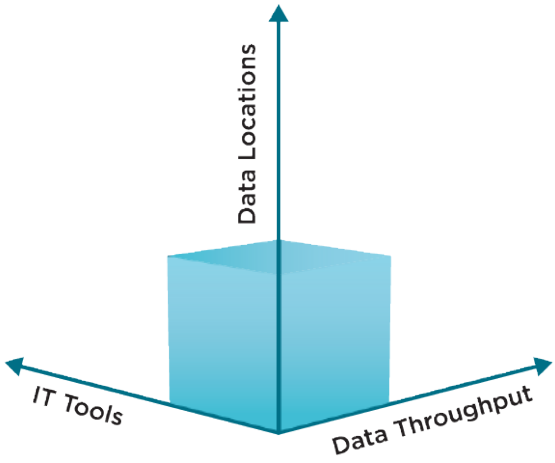


AN ATTACK SURFACE

is the sum of the different points, or attack vectors, where an unauthorized user (i.e., the attacker) can try to enter or extract data from an environment.

THE ATTACK SURFACE IS NOT JUST ABOUT GROWTH IN THREATS. It increases with the growth in IT complexity in three specific dimensions: (1) the number of data locations where data resides, (2) data throughput, and (3) IT tool complexity.

The more organizations grow along these dimensions, the more their overall attack surface increases. Five years ago, Ixia began work on a set of products aimed at enabling IT to manage these issues more effectively while in operation and discovered the same attack surface trends held true. Put simply, the continuous growth in data throughput capacity and distributed physical and cloud operations provide many more breach entry points. Combine this with the increase in the number of security, analytics, and compliance tools, each requiring access to the same incoming data streams, and it is likely that some sort of vulnerability will be exposed.



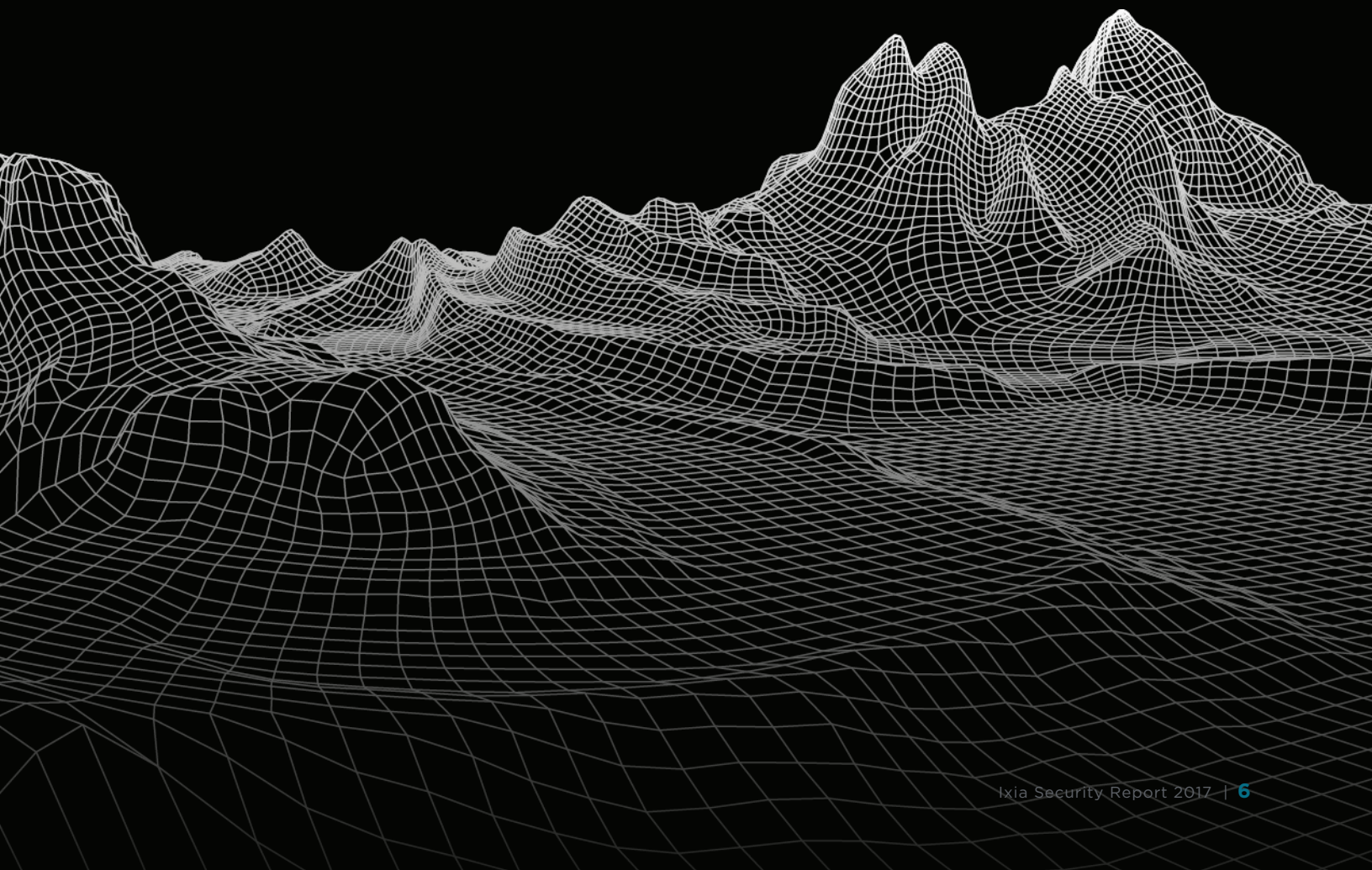
For instance, testing networks at average versus peak loads makes a big difference in performance, as can using multiple clouds with their own security processes. Making copies of the same data for multiple analytics tools—the fundamental job of a Network Visibility System—requires flawless operation if the tools are expected to be effective. This report looks at networks from both a pre-deployment (i.e., how they are tested before they go live) and production (i.e., how they operate in practice) perspective.

Below, we will look at how networking security has shifted.

SECTION

02

THE SHIFTING ENVIRONMENT OF NETWORK SECURITY



THE SHIFTING ENVIRONMENT OF NETWORK SECURITY

The world of threats expanded dramatically in 2016—and not just because of an increase in the amount of malware. Organizations are dealing with larger attack surfaces. Exploits of Internet of Things (IoT) devices have transitioned from speculation to reality. Users and organizations got direct experience with ransomware as attacks targeted nearly every mobile and desktop operating system (OS)—and the ransomware moved from the hands of elite programmers into the hands of novice hackers. State-sponsored cyberattacks had a larger impact than ever, as Russian cyberattacks were linked to U.S. presidential election results. That was a lot to take in one year.

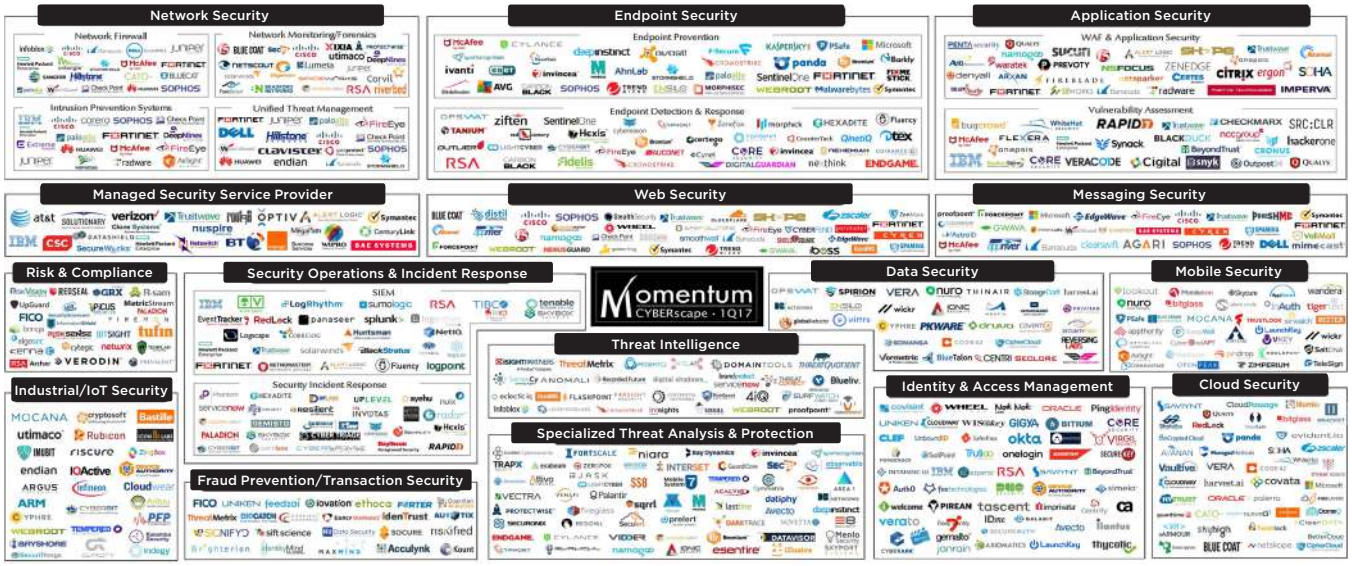
At the same time, the role of the chief information security officer (CISO), chief information officer (CIO), or SecDevOps is becoming more multifaceted. This role is no longer solely responsible for "inside the firewall" initiatives. The affordability and elasticity of the cloud has made movement to public and hybrid cloud deployments too cost effective to pass up. And as more on-premises software moves to software-as-a-service (SaaS)–based cloud services, a landslide migration to the cloud has commenced.

Just like end-consumers, who rarely read the software end-user license agreement (EULA) on their smart phone applications, many in IT have little, if any, knowledge of the security practices of their cloud and SaaS providers. As a result, the complexity and responsibility of the CISO role is potentially magnified 10-fold.

The security landscape graphic from Momentum Partners, below, highlights the issue well. There are a lot of vendors offering a lot of help. Sifting out which products are critical versus which are nice to have requires analysis and scrutiny. Once equipment and applications are selected, integration can create its own unintended vulnerabilities. As a result, vendor selection and integration has become a skill of its own.

The typical enterprise performs only limited testing before deploying new devices and has no way of independently validating their performance in operation. The net result? Every new device adds to an organization's potential attack surface: multi-site offices, physical and cloud, and all devices connecting to the network become potential entry points.

The Vendors of Network Security



Source: Momentum Partners

Securing the expanding network, and the intricate network of vendor devices designed to protect it, has taken on its own complexity. You have heard of the fog of war and the fog of networking; this is the *fog of security*.

Automation and sophisticated real-time monitoring provide critical insight into the fog. The good news is that the tools and techniques to test and monitor these environments are mature and deployable. The bad news is most enterprises have yet to leverage them.

In 2016, "shadow IT" became a bigger issue, getting worse as the concept of "shadow cloud"—describing employees' use of cloud-based services unknown to and unmanaged by IT—emerged. In a 2016 survey conducted by the analyst firm EMA, respondents said that for every controlled cloud application, five or more non-controlled SaaS applications were in use by individuals or departments. 36% enterprises using three or more cloud services do not use security tools to monitor or protect their environment.

Most of these were engaged with no assessment of the SaaS' risk or the security of the SaaS vendor in question. In fact, when IT professionals were questioned as to whether they believed their employees were adequately trained to avoid risky behavior that could lead to a data breach, less than 20% answered "yes."

The net result is that while more critical and confidential workloads and data are moving to the cloud, individuals performing this movement are unprepared for the security implications. Once again, the need for better testing and automated monitoring becomes more critical to protect corporate assets.

THE NEED FOR BETTER TESTING AND AUTOMATED MONITORING BECOMES MORE CRITICAL TO PROTECT CORPORATE ASSETS.

THE CONCERNS OF IT PROFESSIONALS

Do you feel that your employees are **adequately trained** to avoid risky behavior that could lead to a data breach?

81.2% **No** **18.7%** **Yes**

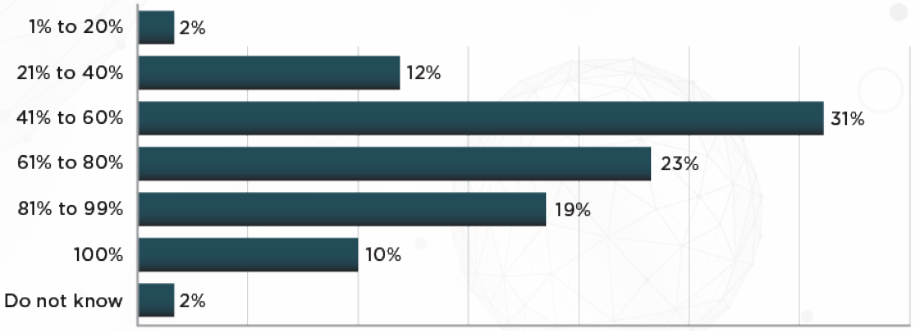
54% of companies surveyed operate more than 6 or more network segments but monitor only half of them.

47% leave half of their network segments unmonitored.

65% of companies do not protect their firewalls with a bypass switch.

An EMA survey of enterprises shows that 47% of enterprises surveyed recognize that they are leaving nearly half of their network segments unmonitored. Network monitoring has become its own issue, as network security needs to address both internal physical resources, and multi-site, mobile, and virtual environments.

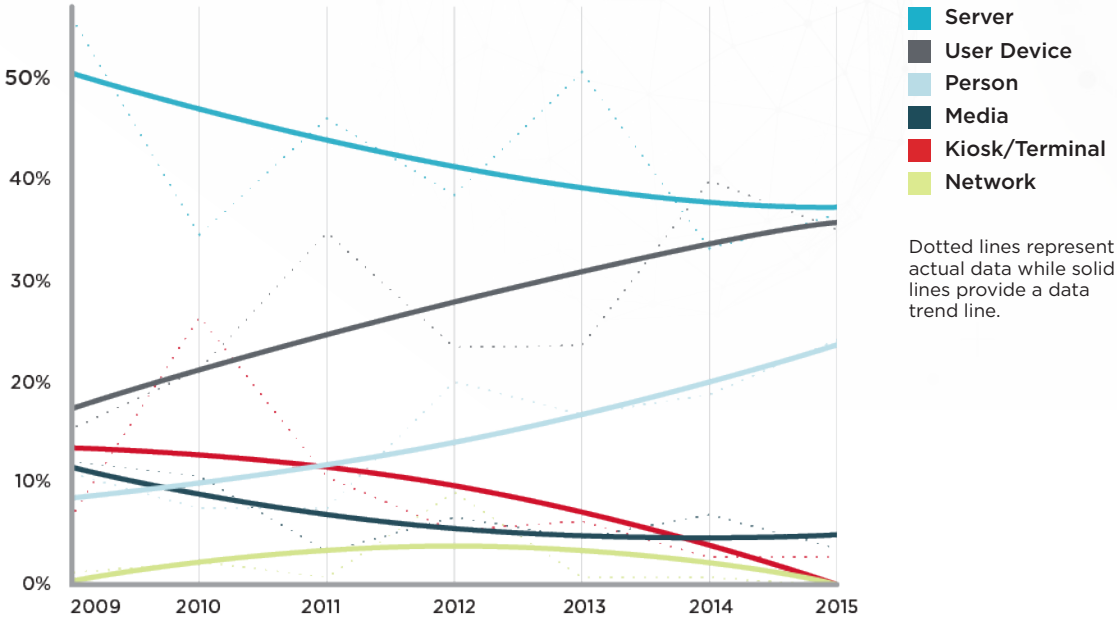
Percentage of Your Network Segments Currently Being Actively Monitored



Source: Ixia Survey of 242 Enterprises

As the emphasis in 2016 on hardening infrastructure increased, attacks against servers, hardened terminals, and the network itself are trending down, as expected. Servers remain the top attack vector, per Verizon's Data Breach Investigations Report findings, but have been on the decline for several years. The human element, however, from shadow cloud SaaS usage to casual use of laptop or smartphone devices not managed 24/7 by IT, continues to rise. In 2016, the terms *network validation testing* and *network monitoring* are increasingly being used in security marketing.

Percent of Breaches Per Asset Category

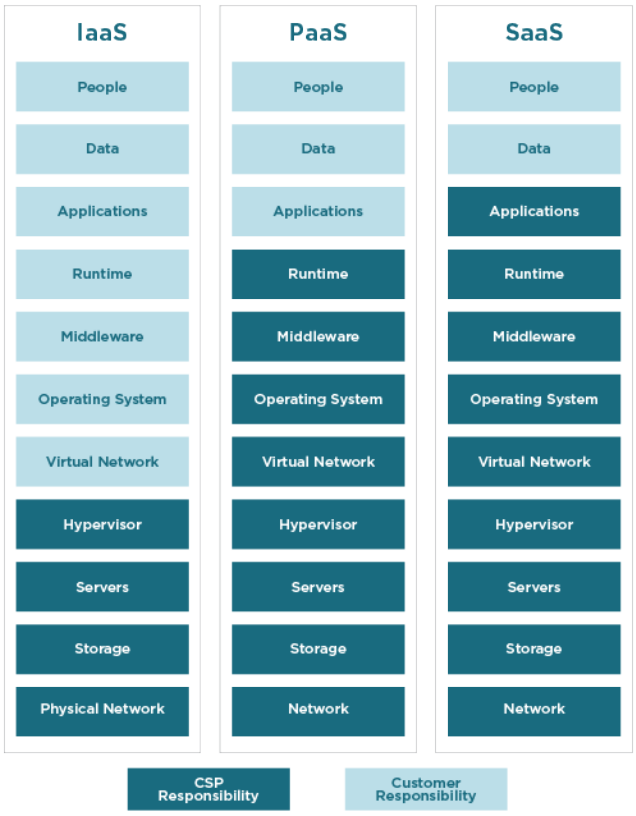


Source: Verizon Data Breach Investigations Report, 2016, page 9

SHARED SECURITY MODEL

Cloud usage is on the rise, which raises its own security issues. Service level agreements (SLAs) from the main Cloud Service Providers (CSPs) can vary and are not always closely monitored. Worse, the implications of multi-cloud implementations in the enterprise are not always evident. CSPs, including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud implement a shared-responsibility model whereby the provider ensures that the cloud infrastructure itself is secure, while securing the actual services running on top of it is the responsibility of the customer. And this varies a great deal depending on whether the service is Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or SaaS. It is vital to understand where your provider's performance and security responsibilities stop and your organization's start.

Looking closer at the responsibilities' split for cloud security and management, you can see from the Gartner analysis that IaaS customers take on a large share of responsibility to maintain the integrity of their platforms, applications, and of course, data. In the case of PaaS, the customer is responsible for applications but not the underlying OS. Only under an SaaS model is the CSP responsible for the service (application) itself.



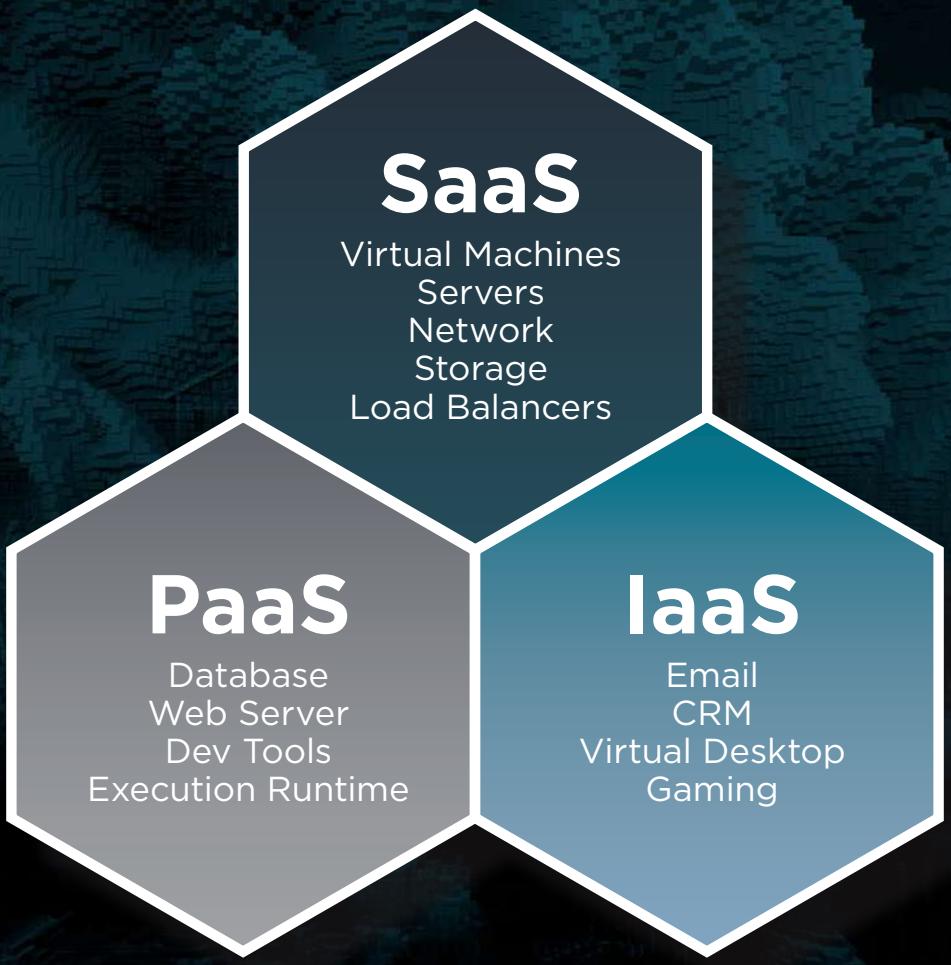
Source: Gartner, Staying Secure in the Cloud Is a Shared Responsibility, April 2016 Report.

ACCORDING TO THE 2016 STATE OF THE CLOUD SURVEY BY RIGHTSCALE,

82% of enterprises
have a multi-cloud strategy.

Software as a Service (SaaS)

Software application



Platform as a Service (PaaS)

Pre-configured application building tools to host your own web-based services

Infrastructure as a Service (IaaS)

Infrastructure (hardware/software) delivered over the web as an on-demand lease

Interestingly, SaaS is potentially the riskiest, because any employee can easily authorize use without the knowledge or oversight of IT, versus IaaS and PaaS solutions that typically require IT configuration and management.

The cloud by no means eliminates the need for strong, independent security and compliance practices at the application level. Quite the opposite is true. According to Gartner, "by 2018, the 60% of enterprises that implement appropriate cloud visibility and control tools will experience one-third fewer security failures."

Security should no longer deter organizations from using cloud services, but ensuring secure operation does require study and training. There are cloud security tests and certifications, such as the Cloud Security Alliance's (CSA) Certificate of Cloud Security Knowledge (CCSK) and the (ISC)^2 Certified Cloud Security Practitioner (CCSP), to ensure cloud services are more secure.

These resources, while helpful, typically address how to secure operation on a single cloud. On average, organizations are employing at least six clouds, evenly mixed between public and private. In the event of a breach, how can an enterprise assess who is at fault? What safeguards should you consider if your enterprise is deploying a multi-cloud approach?

MULTI-CLOUD DEPLOYMENTS AND SECURITY

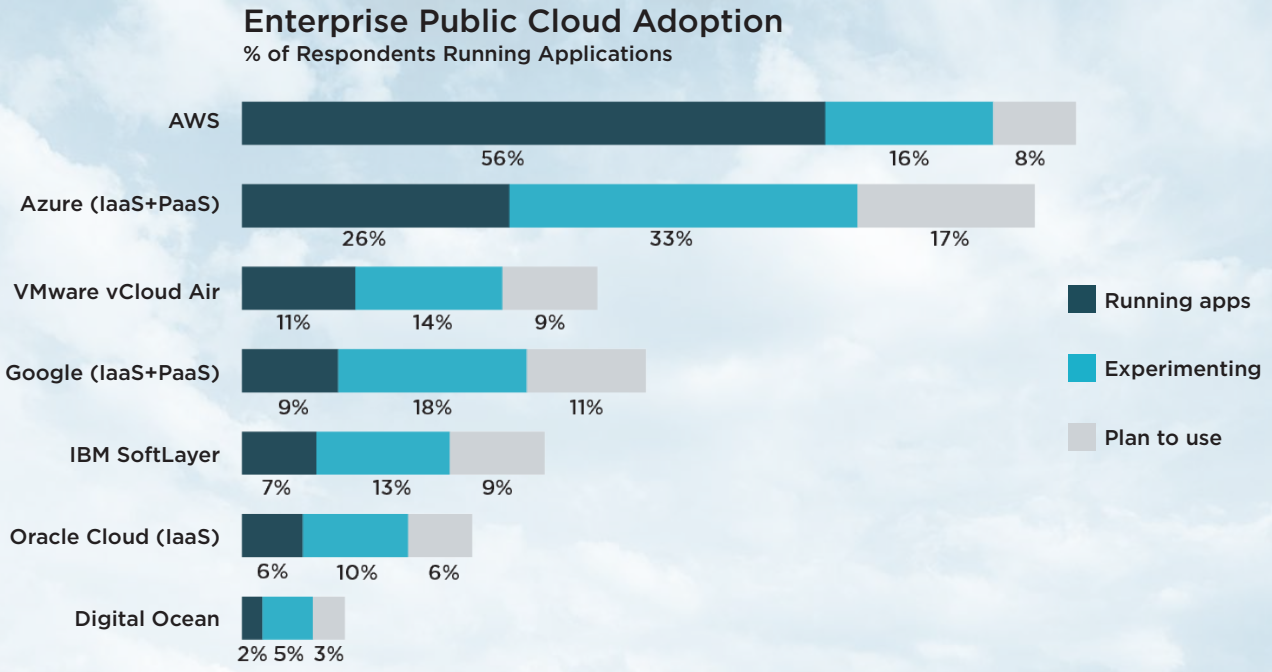
Although in 2016, AWS currently holds a commanding lead, it is by no means the only game in town, and enterprises must plan accordingly. In fact, a sizable number of enterprises have deployed or are planning to deploy on Azure and Google Cloud, especially for IaaS and PaaS. And depending on the region, a more localized CSP, such as Alibaba Cloud, may also host key applications.

The CISO must understand the security model of each cloud and plan accordingly. For example, Microsoft Azure may have better capabilities in some areas, such as those relating to Office applications, while Google Cloud may appeal more to developers.

If both are being used, then the SLAs and security offerings of both must be considered and monitored. They must also be included as part of your enterprise network test strategy.

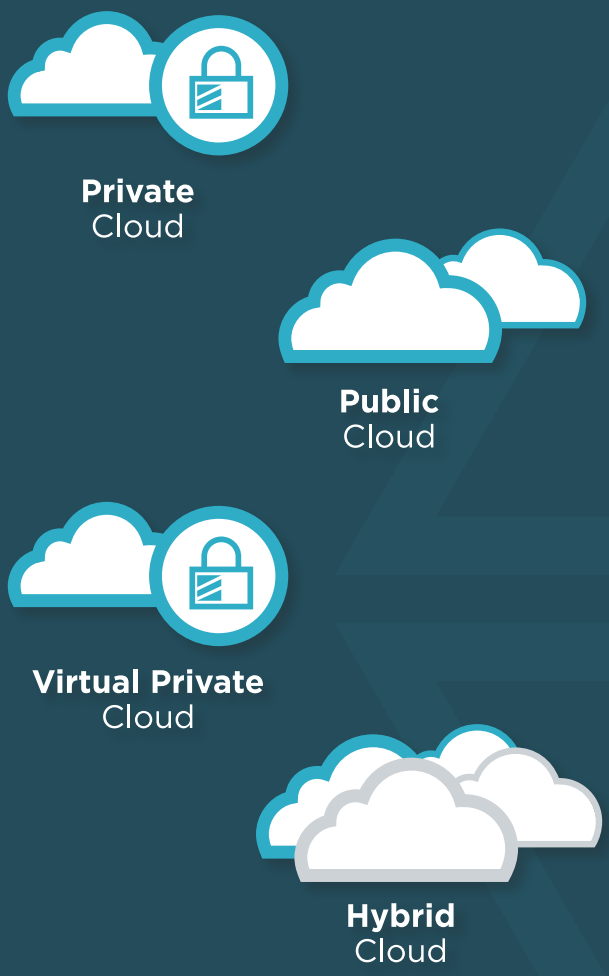
The strong growth of public, hybrid, and virtual private clouds, on top of the traditional enterprise private cloud, increases the size of the attack surface dramatically. Effective testing of new cloud-based applications requires simulation of cloud-scale applications and attacks. Effective monitoring in these multi-tenant environments, where usage is elastic and access is limited, requires its own type of visibility.

It is advisable to use a common set of visibility tools to tap into your data in these different virtual and physical networking environments. Because the raw data can be overwhelming, it is advisable to look beyond simple data access, integrating a sophisticated security fabric to get to the right data and make sure you are not clogging your security, analytics, and compliance tools with duplicate data.



Source: RightScale 2016 State of the Cloud Report.
https://www.rightscale.com/lp/state-of-the-cloud

Different Cloud Environments Each Require Visibility



There are four types of clouds where visibility is needed, each with different characteristics:

- **Private Cloud**: Deployed and managed by the enterprise, private clouds rely on dedicated resources that are easily accessible and controlled.
- **Public Cloud**: Services like Amazon Web Services (AWS), Google Cloud, Microsoft Azure, and others offer much less expensive multi-tenant services on shared infrastructure with elastic compute and storage capabilities.
- **Virtual Private Cloud (VPC)**: A set of partitioned public cloud resources that look much like a private cloud. They use public cloud infrastructure but are not multi-tenant.
- **Hybrid Cloud**: A combination of the first two with orchestration tying them together. This is useful for hosting more sensitive data and applications.

IXIA HAS A RANGE OF PRODUCTS THAT TEST AND MONITOR AT EVERY SCALE OF BUSINESS. Organizations invest heavily in their network designs. They should be able to expect high-quality performance in live operation. The only way to know for sure is to test their networks under realistic load, then monitor them in operation to make sure they exhibit the same behavior.

CloudStorm™

TEST AT CLOUD SCALE—When it comes to testing cloud-based applications, the only way to know it works is to simulate large volumes of traffic and attacks. Ixia CloudStorm is the first multi-terabit network security test platform designed to validate the increased capacity, efficiency, and resilience of hyper-scale cloud data centers. CloudStorm enables users to simulate a data center's capacity of cloud-scale applications, measure performance impacts of secure sockets layer (SSL) traffic, and assess Distributed Denial of Service (DDoS) mitigation techniques for terabit attacks. Simulate up to 2.4 terabits of mixed applications, as well as malicious traffic, to validate applications, storage, and network security devices.

CloudLens™

VISIBILITY INTO VIRTUAL AND CLOUD DATA—Ixia CloudLens provides visibility into public and private clouds. CloudLens Public enables you to tap into public cloud data via sensors installed in the cloud source instance and analyze them via tool connectors within the tool instance. A centralized management platform enables you to control and operate the sensors and connectors installed in the source and tool instances. The management platform creates a secure visibility path, which transfers packet data from the source to the tool connectors. This provides a serverless architecture that scales with distributed software systems built for cloud scale and delivers intelligent, resilient, and proactive public cloud visibility. In addition, for private clouds, CloudLens Private supports virtual taps and virtual packet broker (vPB). The vPB is a visibility packet processor that can be deployed in a virtual infrastructure to aggregate, filter, and distribute virtual traffic to security and performance monitoring tools—such as an intrusion protection, detection, or data loss prevention system. This level of processing power typically requires a physical network packet broker (NPB) appliance, but CloudLens vPB offers these capabilities as a virtual appliance, providing customers with flexibility and ease of deployment in dynamic virtual environments.

Vision ONE™

NPB FOR PHYSICAL AND VIRTUAL DATA—Vision ONE is an NPB that enables organizations to maintain security and identify and resolve performance problems across physical and virtual infrastructures from a single platform. Whether fighting against threats hidden in encrypted traffic or feeding the right data to the right forensic solution, Vision ONE boosts network protection without impacting performance.

SECTION

03

DIMENSIONS OF SECURITY EXPANSION

DIMENSIONS OF SECURITY EXPANSION

With an ever-increasing attack surface, more sophisticated attacks, and more specialized forms of response, industry analysts predict continued strong security investment. The challenge becomes choosing the necessary security elements for your specific network configuration. Every enterprise CISO must make choices about the best allocation of their limited security budgets, as well as what rules and policies to put in place.

For example, multifactor authentication is only as strong as the password rules in place. Complex passwords that change often are better for security but more complicated to remember, resulting in increased password reset requests. These requests can be automated, but they open the system to man-in-the-middle hijacks. Every network architecture and security choice has advantages and disadvantages.

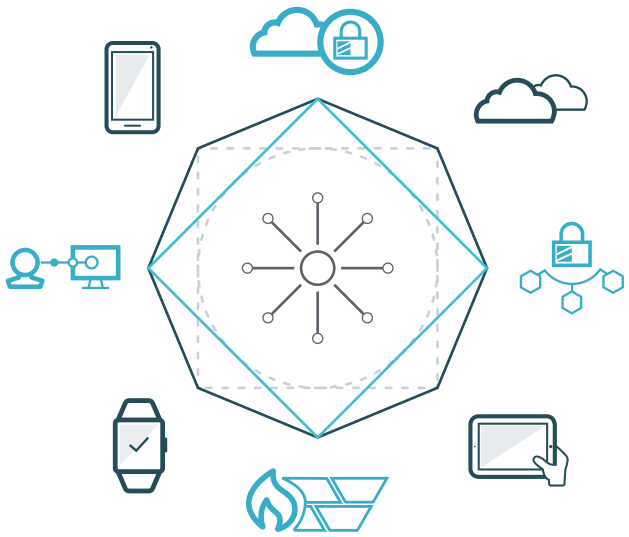
The human element is therefore critical. Per research from Gartner, "Through 2020, 80% of cloud breaches will be due to customer misconfiguration, mismanaged credentials or insider theft, and not cloud provider vulnerabilities."[1] With so many physical appliances and SaaS systems to manage, the chance for mistakes is much higher.

[1] Gartner, "Magic Quadrant for Public Cloud Storage Services," Worldwide, 26 July 2016

THE THREAT SURFACE

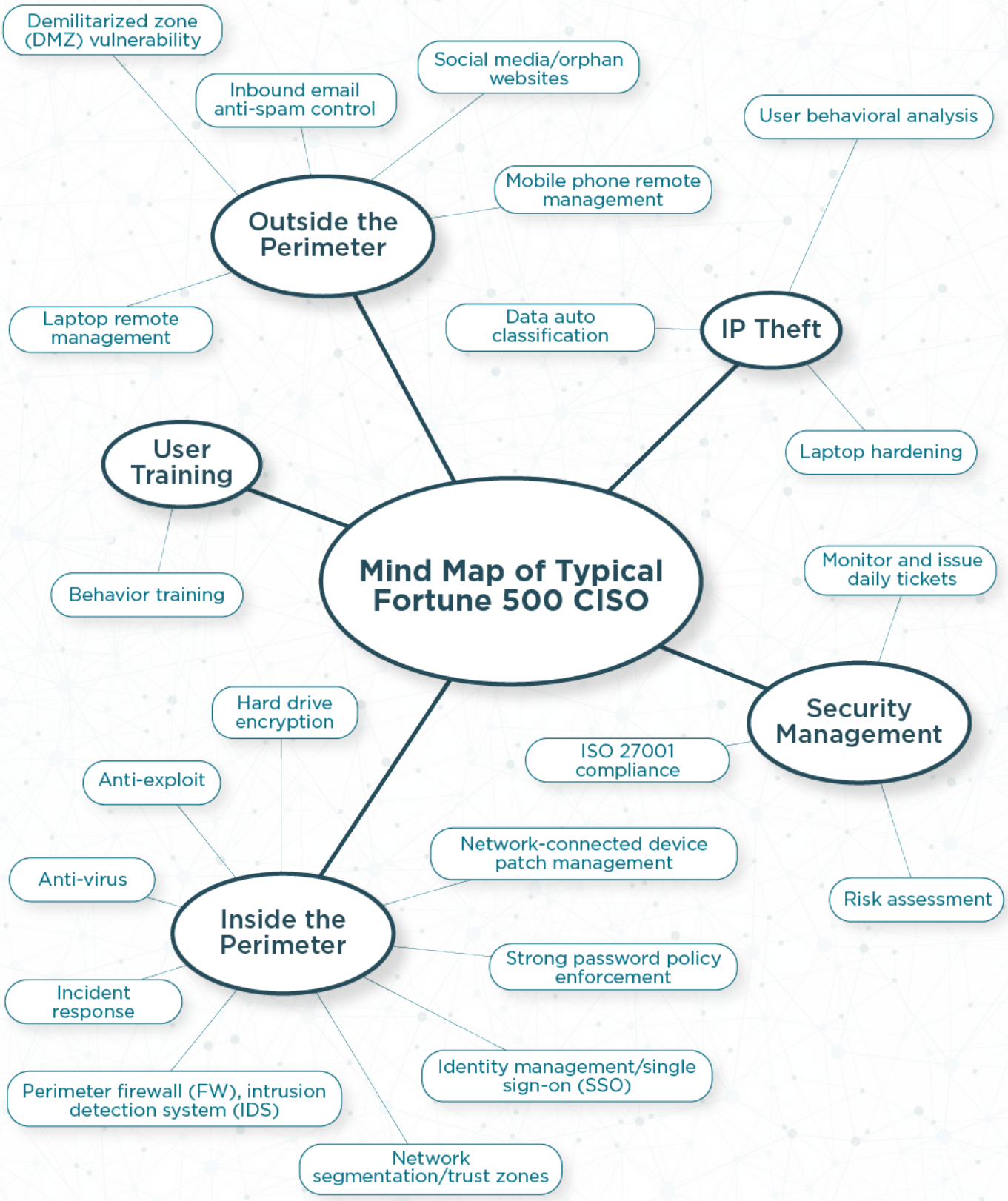
To gain an appreciation for the scope of the task at hand, a typical enterprise may engage upwards of 15 vendors for various aspects of outside- and inside-the-perimeter security, IP protection, user training, and risk assessment. Here are the zones of security that each require testing in your network and monitoring during operation:

- Inside the perimeter: private cloud, firewalls, antivirus software, encryption, directory and authentication services, and network segmentation
- Outside the traditional perimeter: public cloud services, SaaS services, smartphones, laptops, and typically most IoT
- Areas not always emphasized: IP protection actions, such as data classification, behavior analysis, incident response, user testing, and user training
- Other areas that need attention: security management, mobile applications that go directly to the cloud, bypassing internal security, IoT, security, and alert management



Vendors Used by One Fortune 500 Enterprise*	
OUTSIDE THE PERIMETER	
Demilitarized zone (DMZ) vulnerability	Tenable Nessus
Inbound email anti-spam control	Proofpoint
Social media/orphan websites	RiskIQ Enterprise Digital Footprint
Mobile phone remote management	VMware AirWatch
Laptop remote management	Palo Alto Global Protect
INSIDE THE PERIMETER	
Anti-virus	Symantec Endpoint Protection
Anti-exploit	Palo Alto Traps
Hard drive encryption	Symantec Endpoint Encryption
Network-connected device patch management	Quest KACE
Strong password policy enforcement	Microsoft Active Directory
Identity management/single sign-on (SSO)	Okta SSO
Network segmentation/trust zones	ForeScout CounterACT
Perimeter firewall (FW), intrusion detection system (IDS)	Palo Alto Next-Generation
Incident response	LogRhythm SmartResponse
IP THEFT	
User behavioral analysis	Securonix User and Entity Behavior
Data auto classification	McAfee Data Loss Prevention (DLP)
Laptop hardening	Quest One Identity
USER TRAINING	
Behavior training	PhishMe
SECURITY MANAGEMENT	
ISO 27001 compliance	Paladion
Risk assessment	Optiv
Monitor and issue daily tickets	ForeScout CounterACT

*Excludes cloud vendors and their integrated cloud monitoring/security


Mind Map of Typical Fortune 500 CISO
Outside the Perimeter
Demilitarized zone (DMZ) vulnerability
Inbound email anti-spam control
Social media/orphan websites
Mobile phone remote management
Laptop remote management
IP Theft
User behavioral analysis
Data auto classification
Laptop hardening
User Training
Behavior training
Security Management
Monitor and issue daily tickets
ISO 27001 compliance
Risk assessment
Inside the Perimeter
Hard drive encryption
Anti-exploit
Anti-virus
Network-connected device patch management
Strong password policy enforcement
Incident response
Identity management/single sign-on (SSO)
Perimeter firewall (FW), intrusion detection system (IDS)
Network segmentation/trust zones

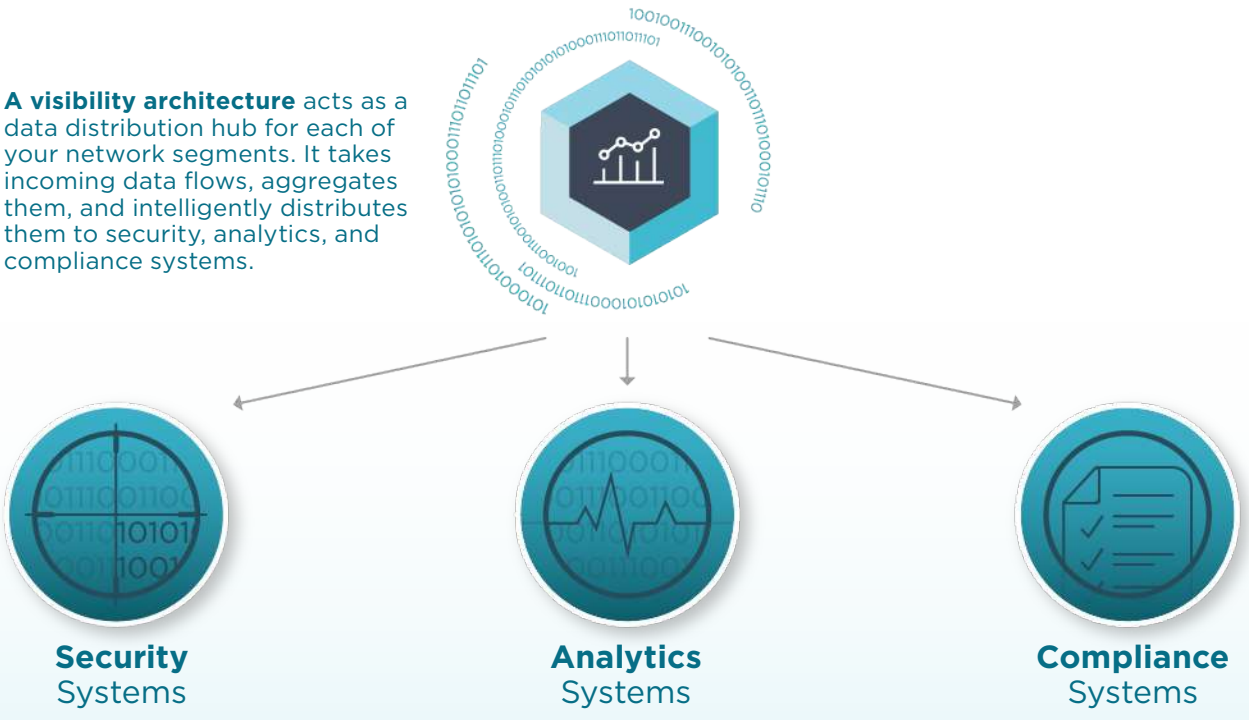
VISIBILITY ARCHITECTURE DEFINED

A visibility architecture is the end-to-end infrastructure that enables monitoring of physical and virtual networks, applications, and security. While it is possible to connect security, analytics, and compliance tools directly to a network's incoming data stream, it is very risky and not readily scalable.

A visibility architecture acts as a data distribution hub for each of your network segments. It takes incoming data flows, aggregates them, and intelligently distributes them to security, analytics, and compliance systems. Every organization's network architecture is different and will change and grow as a function of time. The visibility architecture is an abstraction layer, allowing network security, monitoring, and analysis growth to occur with minimal incidents, disruption, or downtime.

A Network Tool can be any device that IT uses to secure, monitor, or improve performance. The term *tool* encompasses security, analytics, compliance, and monitoring software/ appliances.

A visibility architecture acts as a data distribution hub for each of your network segments. It takes incoming data flows, aggregates them, and intelligently distributes them to security, analytics, and compliance systems.



To the CISO who is managing and monitoring enterprise security, the attacks highlight something they already know: even well-protected systems can be hacked. The CISO needs to constantly monitor, constantly test, and constantly shift security tactics to keep ahead of attackers. It starts with studying how data flows in and out of the new network environment and how to gather and direct all those data flows.

The more distributed security environment of 2016 saw an increase in the number of network segments needing to be monitored and managed. In addition, increases in data throughput often resulted in data distribution issues and blind spots in larger-scale networks.

APPLICATION INTELLIGENCE—rich data about the behavior and location of users and applications can be created and exported in any format needed.

THREAT INTELLIGENCE—organized, analyzed, and refined information about potential or current attacks that threaten an organization.

Ixia Application and Threat Intelligence (ATI) Research Center

Studying how hackers exploit vulnerabilities is one of the top mandates that the ATI Research Center focuses on. This is critical for Ixia's test business—helping organizations stress their products before they introduce them to the market. It is equally important for Ixia's visibility business, which sits at the foundation of large scale networks.

The ATI Research Center leverages 800+ engineers and researchers to operate a worldwide, distributed network of honeypots and web crawlers that actively identify known and unknown malware, attack vectors, and application exposures. It has deployed over five dozen honeypots, each recording thousands of attacks a day and detonating tens of thousands of malicious binaries in security sandboxes. Among these, the team regularly finds and discloses zero-day vulnerabilities. It correlates this data with real-world events and validates reported findings, in addition to partnering with leading developers, monitoring alerts at every layer of the Open Systems Interconnection (OSI) stack, and actively researching threats around the globe to keep application and threat intelligence feeds up to date. It then uses continuous updates to push this actionable intelligence to customers.

FACTORING IN THE COST OF DATA BREACHES

Today's threats pull the CISO in multiple directions: the increasing sophistication of threats, the different types of solutions and their proper deployment, the expected cost of a given attack, and the available budget.

The different security tools available and their use within the enterprise are critical, since the cost of a typical breach continues to increase. One report (Ponemon Cost of Data Breach 2016) finds that the average breach costs over $4 million, a 29% increase from 2013. More alarming is the time to discovery, averaging over 200 days and compounded by a further 70 days to achieve containment. If there is any redeeming factor, less than half (48%) are due to malicious intent. The other 52% are due to human error (25%) and IT or business process failures (27%).

CONTINUED GROWTH IN CYBERSECURITY

According to BCC Research, the global cybersecurity market was expected to reach $85.3 billion in 2016 and could grow to $187.1 billion by 2021. This is a 5-year compound annual growth rate (CAGR) of 17%, impressive for such a large market. The U.S. market alone will grow from $39.5 billion in 2016 to $78 billion by 2021, a projected five-year CAGR of 14.6%. The cloud component of this market is expected to have a 27.2% five-year CAGR, attributed to increasing adoption of cloud-based services. One analyst firm, Infonetics, estimates this at $9.2 billion in 2017.

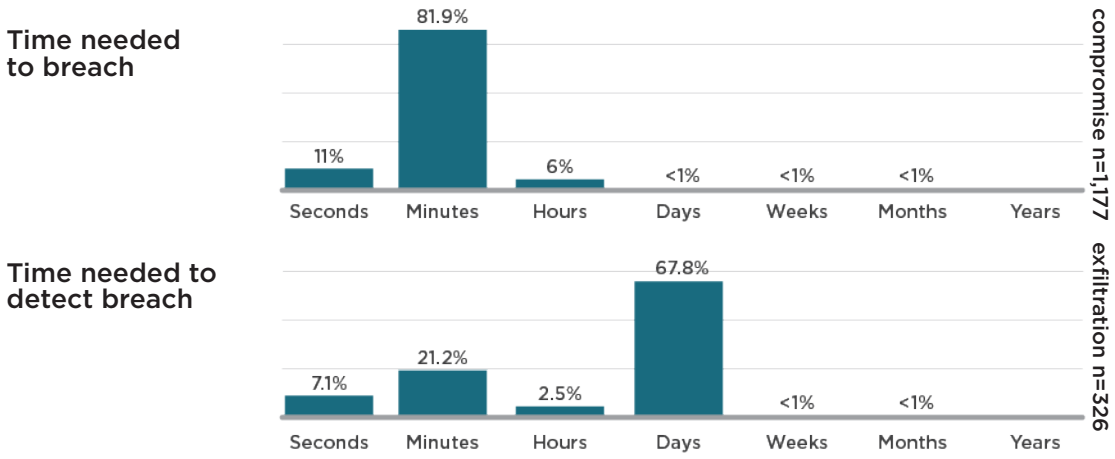
With all the investment and tools available, one issue is top-of-mind—the accuracy of threat reporting. CISOs walk a fine line between an approach that is too intrusive, resulting in false positives, and one that is too lenient, resulting in ineffective control. In addition, some tools may wrongly categorize a given IP address or cloud application as safe or unsafe. The real issue is how quickly a network may be compromised from any one of several vectors. There is a short window of entry—typically measured in minutes—so the proper visibility and automation must be in place to identify a breach before exfiltration begins.

CISOs must err on the side of caution. An issue with a customer relationship management (CRM) or marketing automation system may not result in sustained damage to the corporation or shareholder lawsuits. A major security breach will for sure. Now, let us look a little deeper into what 2016 was like.

Visibility is Key to Security

Time needed to breach: Minutes

Time needed to detect breach: Days

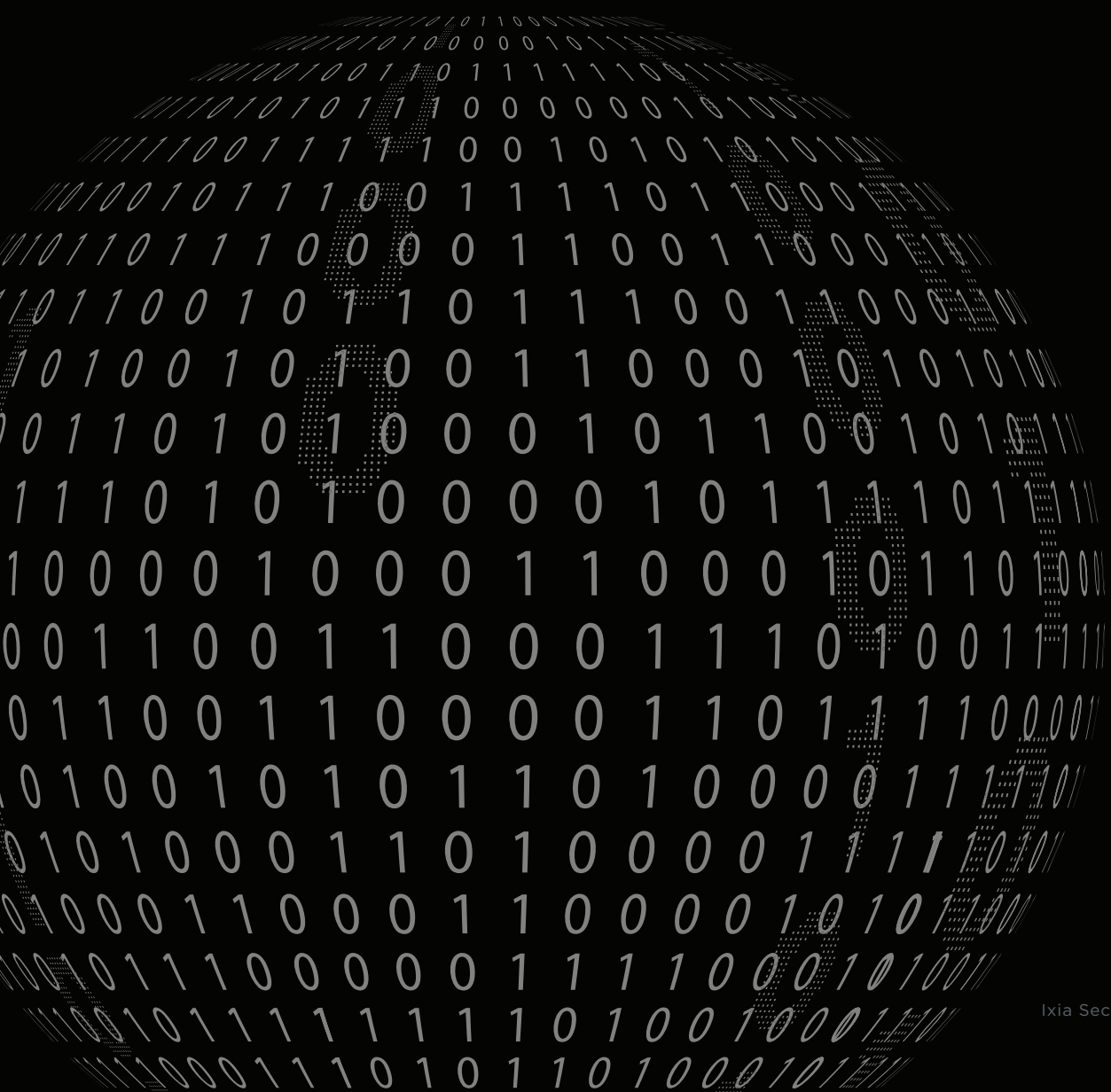


Source: Verizon DIBR, 2016, page 10

SECTION

04

NEW ENVIRONMENTS, NEW THREATS



NEW ENVIRONMENTS, NEW THREATS

Time magazine selected "the hackers" as their 3rd choice for their 2016 person of the year (after Donald Trump and Hilary Clinton, who coincidently were each personally affected by cybersecurity incidents). IoT and critical infrastructure risks, attacks against the Internet itself, state-sponsored hacks against voter records, and ransomware all entered our consciousness.

Consumers do not even bat an eyelid when their credit cards are compromised, and if the $300,000 asking price for the 1 billion Yahoo email records said to be compromised is true, your identity on the Internet is worth 3/100th's of a cent. One of the most disturbing trends was awareness that data may not only be ex-filtrated, but altered as well, calling into question what is real and what is not. Whether this results in better diligence by both organizations and individuals is yet to be seen.

As the industry leader in network security testing at large scale, Ixia researchers have to stay on top of the latest threats and trends. Shifts in attack methods and vectors require rapid re-creation in our lab, so we can create realistic—and current—test packs. We track the security headlines each year. Below are some of the noteworthy security headlines from 2016.

Security Headlines of 2016

Ransomware

is computer malware that installs covertly on a victim's computer, executes a cryptoviral attack and demands a ransom payment to decrypt it or not publish it. The severity of the attack may range from locking the system to encrypting the entire drive. Ransomware attacks are typically carried out using a Trojan that has a payload disguised as a legitimate file.

JANUARY

THREATS

BlackEnergy (reappears) and attacks Ukraine power grid. A threat group has been using the Russia-linked BlackEnergy malware family in attacks aimed at news media and electrical power organizations in Ukraine.

IXIA INSIGHTS

ModPOS: The most complex malware targeting point-of-sale systems to date is observed in action. Read our blog.

FEBRUARY

THREATS

Mazar Android Attack: The mobile malware gives attackers full control over your mobile phone.

Locky ransomware: Hits 100k+ PCs/day and encrypts local files and unmapped network shares.

IXIA INSIGHTS

IoT: Medical devices and hospital networks becoming a risk—how to counter? Read our blog.

Ixia introduces Vision ONE for end-to-end network visibility.

PowerShell is a task automation and configuration management framework from Microsoft, consisting of a command-line shell and associated scripting language built on the .NET Framework. PowerShell provides full access to COM and WMI, enabling administrators to perform administrative tasks on both local and remote Windows systems, as well as WS-Management and CIM enabling management of remote Linux systems and network devices. Initially a Windows component, PowerShell was open-sourced and made available across a number of platforms on August 18, 2016.

MARCH

THREATS

KeRanger: One of the first documented ransomwares to target Mac users, now packaged with BitTorrent.

Triada: Yet another Android malware, with a modular architecture that provides full access to an infected system and is hard to detect.

SamSam: The doctor will see you, after you pay the ransom.

IXIA INSIGHTS

Announcing simplified DDoS testing at scale via Ixia BreakingPoint Labs, including reflection attacks. Read our blog.

APRIL

THREATS

Major hacking campaigns spreading **CryptXXX Ransomware via Angler**.

Microsoft PowerShell vulnerabilities: Data from 1,100 security investigations shows PowerShell was used in 38 percent of cyberattacks.

Bangladesh SWIFT attack: Bank network flaw helped hackers steal $80 million.

IXIA INSIGHTS

Is your network or security tool blocking Ransomware? It pays to validate early. Read our blog.

Ixia introduces Hawkeye to automatically test and verify performance SLAs.

Angler Exploit Kit

is a hacking tool that is produced to search for Java and Flash Player vulnerabilities on the attacked PC and use them to distribute malware infections.

MAY

THREATS

Ixia ATI Research Center discovers **Zero-Day IBM Statistical Package for the Social Sciences (SPSS) Statistics Vulnerability**. Leverage subscription service to stay ahead!

IXIA INSIGHTS

ImageMagick vulnerabilities enable an attacker to exploit them without the user knowing. Read our blog.

Zero-day attacks are still real. What can you do to prevent IBM SPSS vulnerability from impacting you? Read our blog.

JUNE

THREATS

Resurgence of **MS Office macro malware**. For almost a decade the warnings have been neutered. This is now changing.

IXIA INSIGHTS

How to combat the latest threats including TorrentLocker and RAA that leverage JavaScript? Keep your OS current! Read our blog.

Protect against Angler Exploit Kit evolution with ATI. Read our blog.

ShadowBroker—Though the leaks dealt with networking equipment and exploits that were a few years old, one needs to assume that more recent NSA work is targeting the latest generation of hardware.

JULY

THREATS

Retefe Trojan targeting banks now supports HTTPS certificates.

Furtim malware now targets energy companies and others with both software and physical security systems.

IXIA INSIGHTS

Ixia's ATI Research Center protects customers from macro-based Zero-Day Ransomware that avoids discovery from intrusion prevention system (IPS) and anti-virus (AV). Read our blog.

Malware uses increasingly sophisticated means to stay hidden and they even detect if running in a sandbox. Read our blog.

AUGUST

THREATS

Pokeman GO, remember that? Be aware of the threat posed to your enterprise network by this or any other game.

IXIA INSIGHTS

Shadow Brokers release internal NSA hacking tools. Update your vulnerability lists! Read our blog.

Ixia IoT is available to help test IoT devices for medical usage and other sensitive environments.

MIRAI (JAPANESE FOR "THE FUTURE") is malware that turns computer systems running Linux into remotely controlled "bots," which can be used as part of a botnet in large-scale network attacks.

SEPTEMBER

THREATS

Mirai: Krebs of krebsonsecurity.com fame, had his website taken down by one of the largest DDoS attacks ever. The attack clocked in at over 600Gbps, removing the website from the Internet for multiple days.

Next level of Ransomware, **HDDCryptor**, now targets files and locks the drive as well.

IXIA INSIGHTS

Bring DDoS emulation into the lab and model the attacks in a controlled environment. Read our blog.

Dissecting the most complex DDoS test challenge in the world—DDoS evolves with IoT, tablets, and phones. Read our blog or watch the video.

OCTOBER

THREATS

Mirai IoT took down Dyn DNS and many popular Internet sites. It is the canary in the coal mine for future large-scale attacks against the Internet infrastructure.

IXIA INSIGHTS

The Equation Group's Firewall Exploit Chain and the ShadowBroker release: Understanding this better equips you to handle other threats to your security infrastructure. Read our blog.

What can enterprises learn from the massive Dyn DDoS attack that crippled the Internet? The next DDoS attack could strike anywhere at any time. Read our blog.

Security is a chain;
it is only as secure
as the weakest link.

—BRUCE SCHNEIER
in his new book, "Secrets and Lies"

NOVEMBER

THREATS

Another **Android hack** with more accounts compromised. Eighty-six apps available in third-party marketplaces can root 74 percent of Android phones.

Deutsche Telecom outage due to **Mirai botnet**.

German Election: Russian Fancy Bear hackers allegedly target political parties using spear-phishing attacks.

SF Muni hacked: Ransomware delivers free rides.

IXIA INSIGHTS

Defend against Ransomware and do not pay. Identify the source via known malicious IP addresses via Ixia's ThreatARMOR™. Read our blog.

DECEMBER

THREATS

Obama orders investigation into **election hacks**.

NGOs and Think Tanks targeted by hackers post-election.

Yahoo 1 billion more accounts hacked.

Russia Methbot YouTube zombies are a new high-tech enterprise fraud of showing real ads to fake people.

Social engineering revisited with hackers targeting lawyers handling **insider events**.

IXIA INSIGHTS

Tis the season to be wary. Find out about the most prevalent malware to watch out for. Read our blog.

As 2016 ended, there were still more unknowns than knowns regarding election impacts due to malicious hacking. What was known was the following: CrowdStrike, on behalf of the Democratic National Convention (DNC), identified two groups, Fancy Bear and Cozy Bear, as the culprits. Fancy Bear was said to be affiliated with Russia's Main Intelligence Agency (GRU—Glavnoye Razvedyvatel'noye Upravleniye), the military's foreign-intelligence agency, while Cozy Bear was linked to the Russian Federal Security Service (FSB), the current equivalent of the Komitet Gosudarstvennoy Bezopasnosti (KGB). Based on this and other indications, the U.S. government formally linked Russia to the attack and stated that Russia was attempting to interfere with the presidential election—a very serious allegation.

SECURITY FINDINGS

The ATI Research Center saw the following findings as part of its ongoing threat research. Of note is how much the old, tried brute force hacking methods still work. The main theme seen was the prevalence of low-hanging fruit for attackers to exploit. Across different services, OSs, and deployments, attackers are looking for the easiest way to gain entry. Despite the extensive media coverage of advanced persistent threats (APTs), most attackers were not APTs. Some were looking for one mistake among many targets. We saw that the most extensive breaches were through brute force, checking for passwords that are 14 years old, probing for vulnerabilities that are over 10 years old, and serving up malware that has not changed in years.

Despite the extensive media coverage of APTs, most attackers were not APTs.

Campaigns targeting large groups of users and popular services, such as Facebook, AOL, Google, Dropbox, and PayPal, resulted in a significant increase in the amount of ransomware delivered by phishing attacks. Content management systems (CMS) for websites offer many vulnerabilities for exploitation, and WordPress leads all CMSs in the number of vulnerabilities and breaches. The number one programming language exploited was PHP with the associated assumption that most targets are running out-of-date Linux/Apache/MySQL/PHP (LAMP) installations.

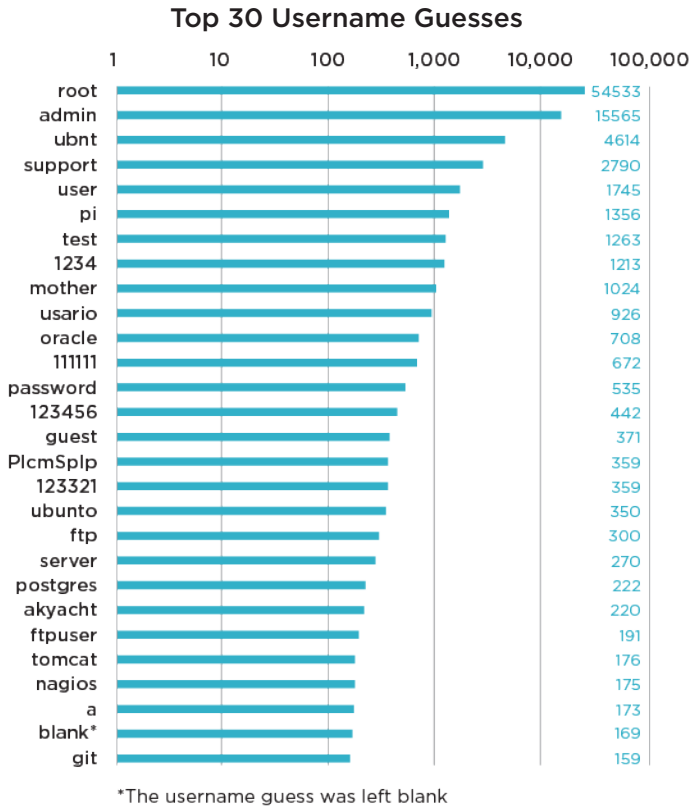
Evidence confirms what most of us already know. Easily exploitable systems will be exploited. Easily exploitable people will be exploited. IT and security need to eliminate the easy targets through ongoing training of their organizations and, more importantly, by setting an example of changing default passwords on any equipment or servers they place in their networks.

LAZINESS LEADS TO EXPLOITATION

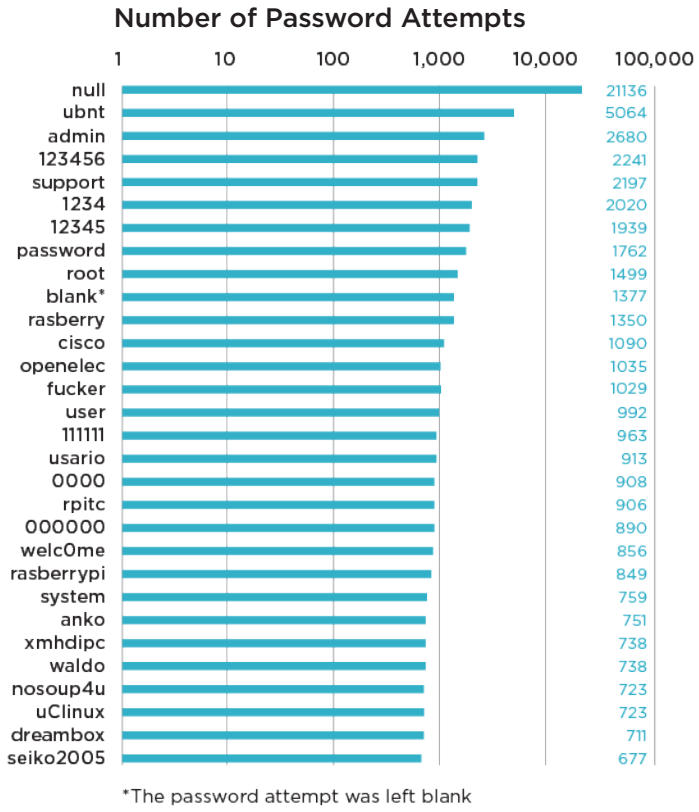
Gaining access to accounts is often done the old-fashioned way—brute force guessing starting with the obvious. It is shocking how many network accounts and devices contain default user names and passwords.

Username and Password Guesses

Below were the top 30 guesses seen over a year of secure shell (SSH) user names and passwords. At the top of the list were predictable user names like **root** and **admin**, but then we also saw **ubnt**, the default username for Ubuntu offered in AWS and other cloud services. Of course, old friends like **user**, **1234**, **Ubuntu**, **ftp**, **server**, and **guest** were prominent.



*The username guess was left blank



*The password attempt was left blank

IoT systems were favorite targets. The default user name for the Raspberry Pi, a hobbyist IoT platform often used for production systems, was **pi**. **PlcmSplp**, which also fell under device targeting, was an attempt seen to find Polycom session initiation protocol (SIP) phones. Also seen was **usuario**, Spanish for "user" and the full array of Linux and Berkeley Software Distribution (BSD) default user names: **oracle**, **nagios**, **postgres**, **ftpuser**, **tomcat**, and **git**. A favorite was the **blank** user name, which still showed up in the top 30 for the year.

Like usernames, topping the list of passwords were obvious guesses like **admin**, **123456**, **support**, **password**, and **root**. The first password is **null**. This is not an actual password, but the presence of no password, although **blank** is also a top ranked password. **Raspberry** might seem like a strange guess, but not surprising for Raspberry Pi. **Openelec** is a reference to an open source media server. **Cisco** is the default password for most Cisco brand routers, switches, and firewalls. Unfortunately, we saw that it sometimes did not get changed by the teams deploying the networking products. Mirai, yet another malware, was very visible this past year, and **anko**, **dreambox**, **xmhdipc**, **system**, **111111**, **000000**, **123456**, and **12345** were all botnet password guesses.

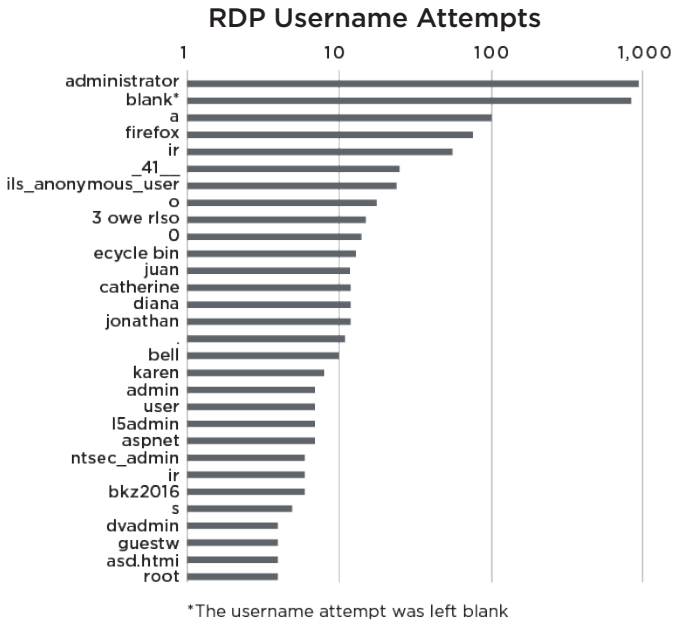
IoT Systems
Were Favorite Targets

RDP Username and Password Attempts

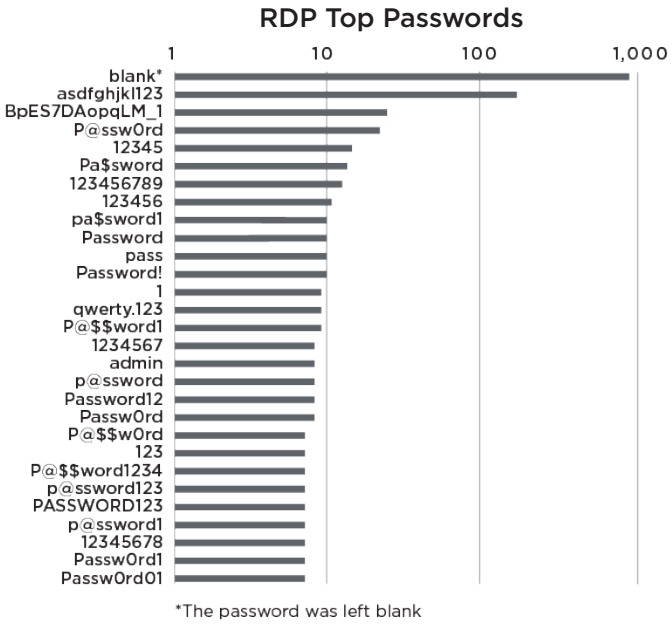
Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft that provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software. The ATI Research Center saw these brute force username and password attempts on RDP over the last year.

What was disappointing to see was the overwhelming use of the username **administrator**, considering that the default account created on Windows is the account **administrator**. Despite all education attempts, RDP accounts still seem to slip through the cracks of vigilance. Of interest, also, was **ils_anonymous_user**, an advisory released by Rain Forest Puppy in 2002, where Microsoft Site Server 3.0 contained a hardcoded username/password pair—indicating that no patches or updates were applied to these servers since 2002. **BpES7DAopqLM01**, as a password, belonged in the same advisory, yet still provides enough successful hits to be included in brute force password collections.

Since Windows deployments are less uniform than most UNIX/LINUX systems, the long tail of username guesses and passwords appear much more frequently.



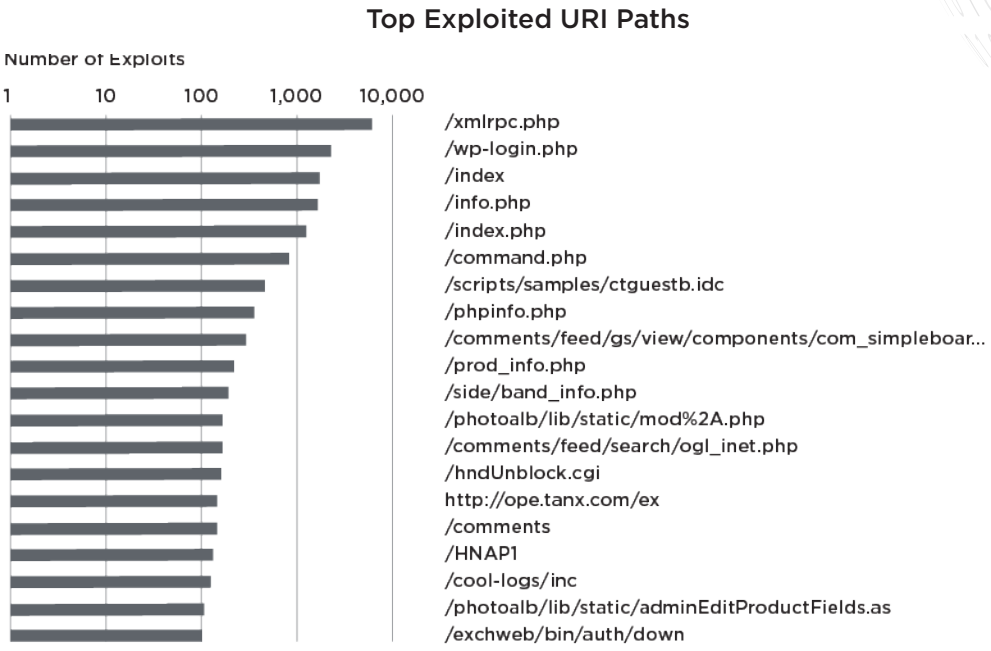
*The username attempt was left blank

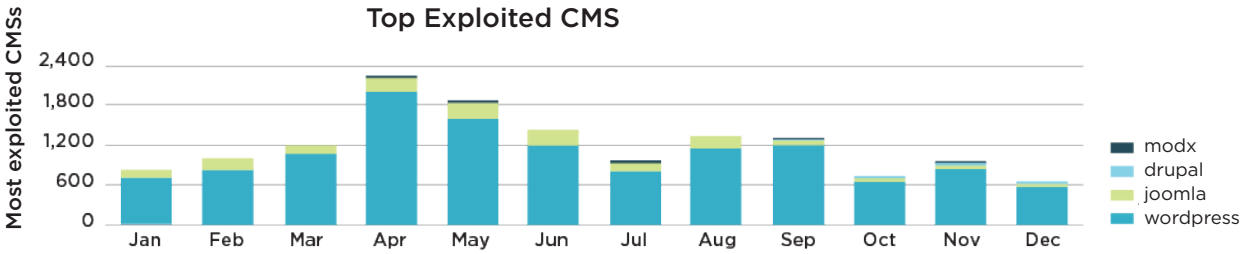


*The password was left blank

Top Exploited URI Paths and CMS

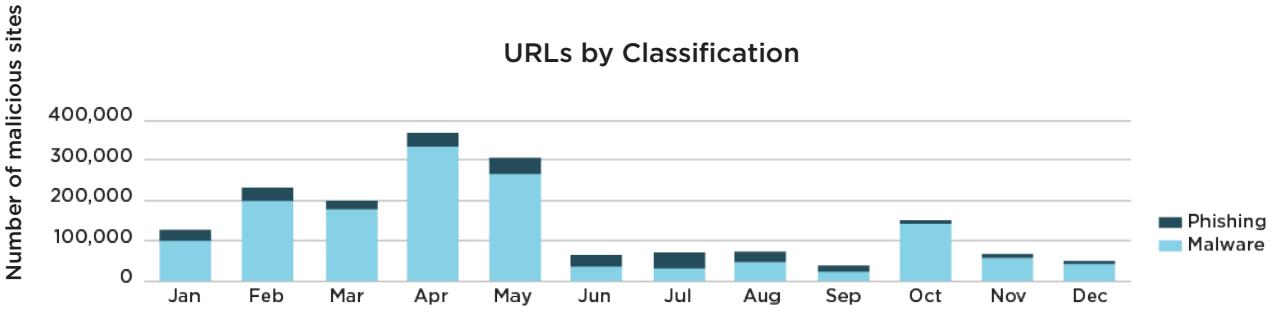
In computing, a uniform resource identifier (URI) is a string of characters used to identify a name of a resource. Such identification enables interaction with representations of the resource over a network, typically the World Wide Web, using specific protocols. The top attacked URI paths were **/xmlrpc.php** and **/wp-login.php**, both of which belong to the popular blogging platform WordPress, and were targets of brute forcing attempts. We also saw many scans for the **phpinfo()** function as a means of fingerprinting servers. Most URIs indicated that attackers were searching for PHP based targets and vulnerabilities. Many of the URIs seen are on the public lists for known Structured Query Language (SQL) inject attacks, including **ogl_inet.php** and **adminEditProductFields.asp**. Supporting this data was a view of the top exploited CMSs hosting malicious content. The overwhelming number ran WordPress, followed by Joomla as a distant second.

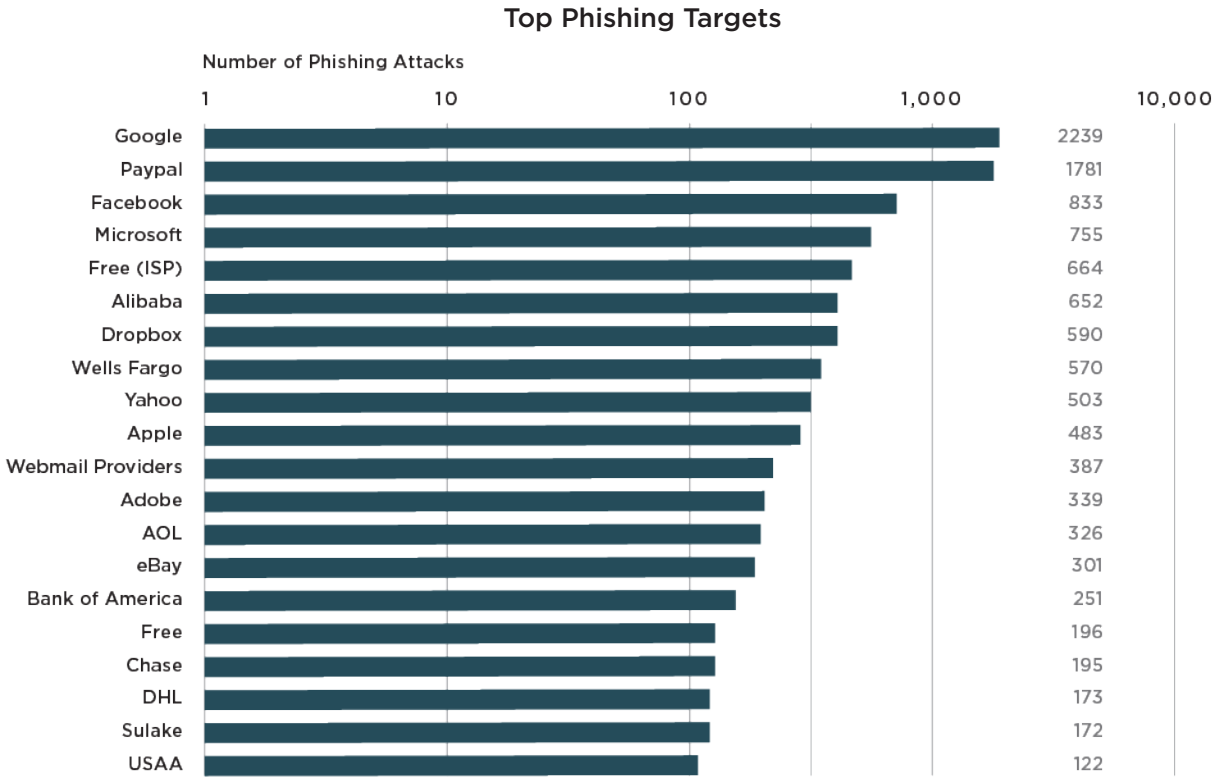




Malware or Phishing?

Malware continued to dominate over 2016, as seen in the diagram entitled "URLs by Classification." However, there were a few months, namely June, July, and August, during which ransomware phishing looked like it may outpace malware. The top phishing target sites are shown in the diagram entitled "Top Phishing Targets." Top targets included Facebook, Adobe, Yahoo, and AOL logins. Adobe updates were the most prevalent drive-by updates for delivering malware or phishing attacks. Toward the end of the year, the more typical malware–phishing distribution was seen.

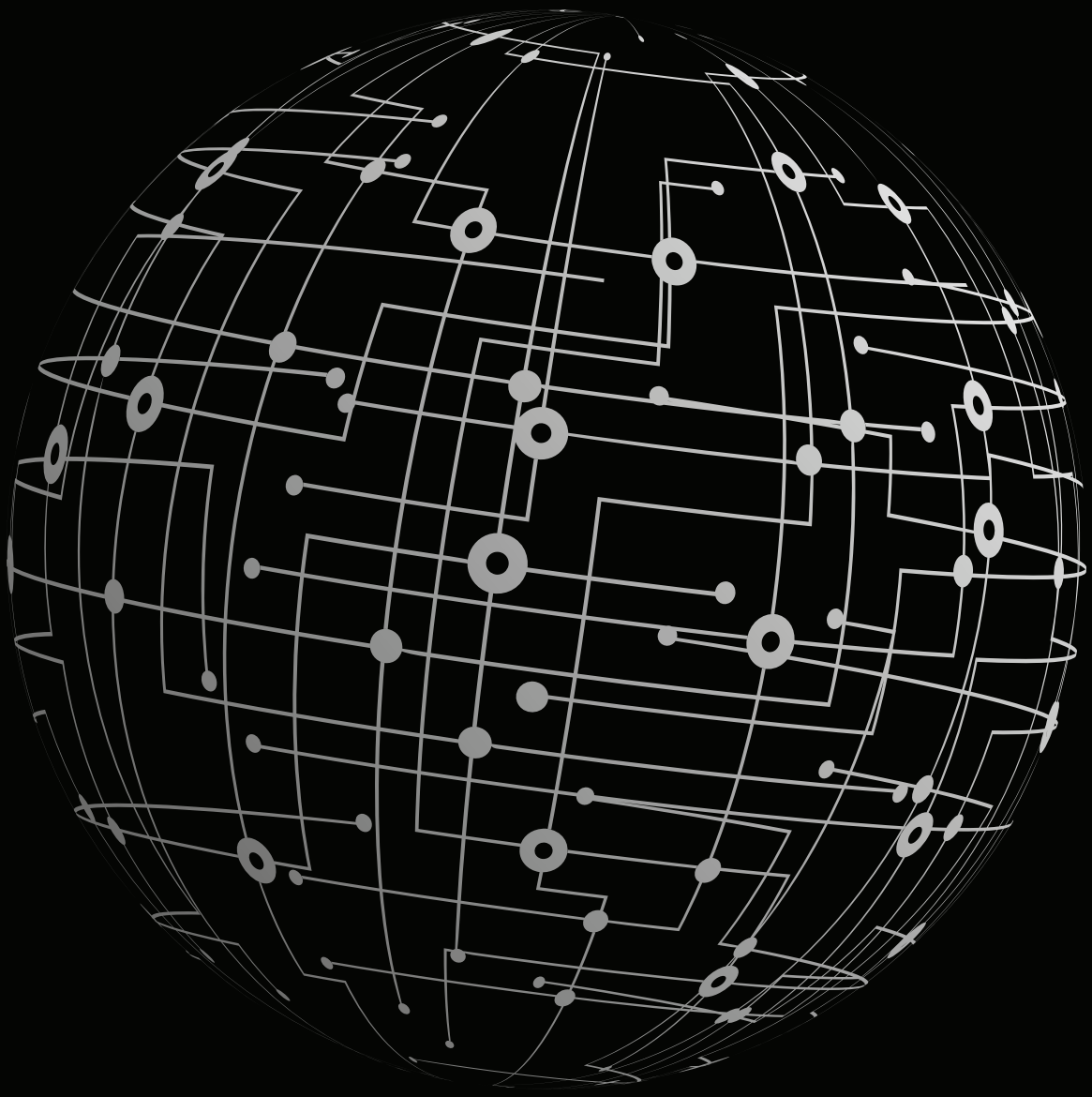




SECTION

05

LOOKING AHEAD

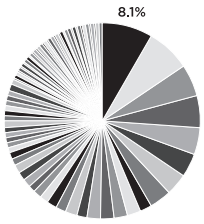


LOOKING AHEAD

Looking ahead to 2017, the threats that made the news in 2016 will not go away, if December was any indication. But, even more dangerous and harder-to-contain attacks will come into play. Some of these include:

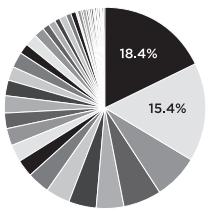
- Increasing focus on attacking the supply chain of a protected enterprise. Countering this will require dedicated efforts by enterprises to ensure the security of their vendors, contractors, and business partners. As enterprises become increasingly interconnected, the threat surface continues to grow.
- The risk to critical infrastructure has been reported time and time again, and this is good. With all the emphasis, as well as investment in countering any threat, the overall impact should be minimal, notwithstanding any state-sponsored attacks, such as Ukraine Power. "Soft targets" that do not receive the same level of investment will be less secure. And, given that the Internet is now critical, the intensity of DDoS attacks will only increase, which in turn, will spur investment in protection.
- As the social media footprint of an enterprise increases, so also does the potential damage to the corporation and to key individuals. Many enterprises have not instituted rigorous social posting policies.
- Ensure employees have a keen understanding that the Web is a very dangerous place. A Menlo Security study labels almost half (46%) of the top million websites as "risky" due to vulnerable software on the servers or the ad networks to which users are directed. This is difficult for the typical user to track due to the sheer volume of background Web browser requests, outnumbering actual user requests by 25 to 1. Even a site as well known as CNN results in over 250 content requests, some to domains that, at first glance, could be suspicious.
- Though in most cases not intended to be malicious, misbehaving algorithms and software can create equal or more damage than a dedicated hacker. There will be increased emphasis on tools that can quickly react to abnormal behavior, no different than a firewall.
- With continued deployment of IoT and devices within the smart home, the appeal to hackers will only increase. To counter this, leverage user training and implement controls on the supplier end, as well as better lockdown of open source code that is used in many of these devices. Security benchmarks need to be applied against any hardware, OSs, and applications. This will be a critical step in helping slow (but not eliminate) the proliferation of botnets.

Requests



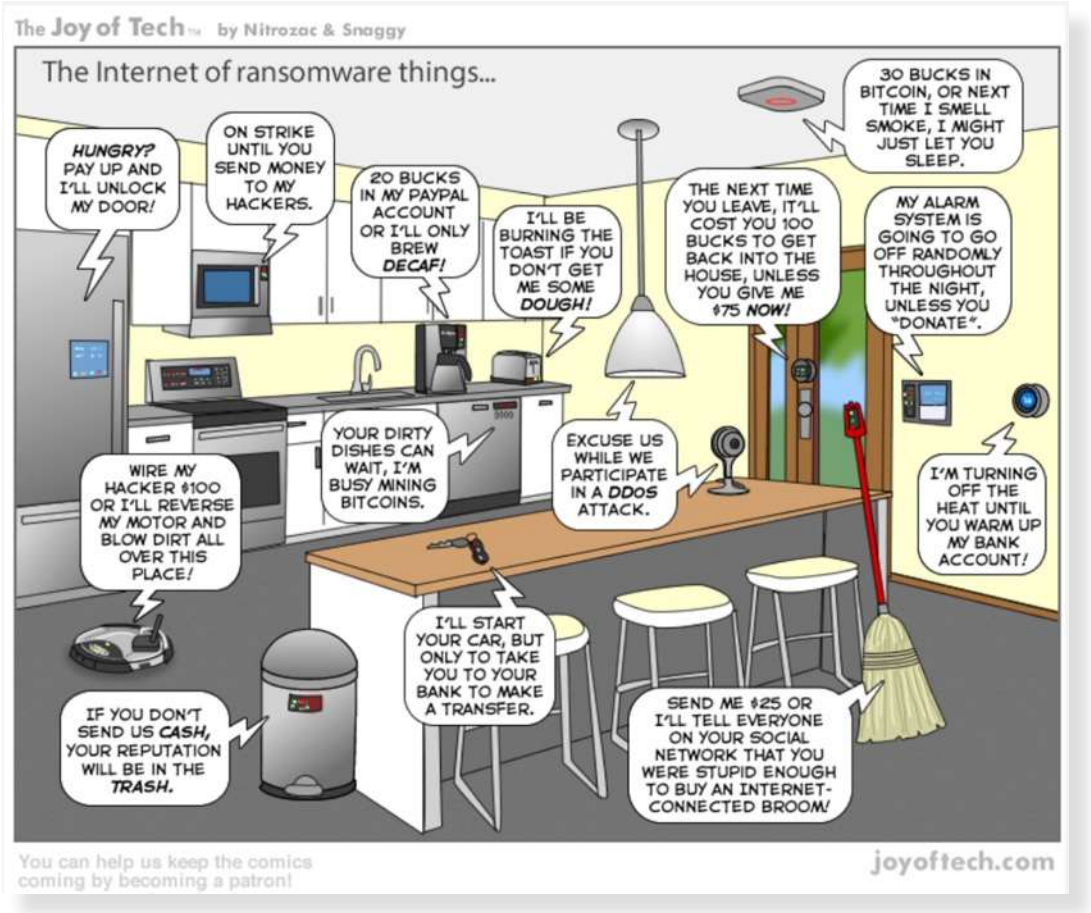
Domain	Requests
www.i.cdn.cnn.com	19
i2.cdn.cnn.com	17
www.cnn.com	12
beacon.krxd.net	12
logx.optimizely.com	10
log.outbrain.com	9
i.cdn.cnn.com	8
securepubads.g.doubleclick.net	8
images.outbrain.com	5
pagead2.googlesyndication.co	5
tpc.googlesyndication.com	5
i.cdn.turner.com	5
cdn.krxd.net	5
b.scorecardresearch.com	4
storage.outbrain.com	4
hpr.outbrain.com	4
optimized-by.rubiconproject.com	4
ml314.com	3
cdn.livefyre.com	3
www.facebook.com	3
widgets.outbrain.com	3
z.cdn.cnn.com	3
geo.moatads.com	3
ad.doubleclick.net	3
0914.global.ssl.fastly.net	3
r.nexac.com	2
secure-us.imrworldwide.com	2
www.google.com	2
staticxx.facebook.com	2
aax.amazon-adsystem.com	2
data.cnn.com	2
metrics.cnn.com	2
js.moatads.com	2
bs.serving-sys.com	2
secure-ds.serving-sys.com	2
static.chartbeat.com	2
cnn.stream1.fyre.co	2
cnn.bootstrap.fyre.co	2
googleads.g.doubleclick.net	2
connect.facebook.net	2
w.usabilla.com	1

Bytes



Domain	Bytes
www.i.cdn.cnn.com	512,388
i2.cdn.cnn.com	447,676
www.cnn.com	207,242
zor.fyre.co	170,245
js.moatads.com	134,501
secure-ds.serving-sys.com	124,606
cdn.krxd.net	111,245
cdn.optimizely.com	102,210
images.outbrain.com	80,611
dynaimage.cdn.cnn.com	78,974
securepubads.g.doubleclick.net	76,474
storage.outbrain.com	74,794
z.cdn.turner.com	74,517
i.cdn.cnn.com	69,501
connect.facebook.net	68,442
pagead2.googlesyndication.com	64,726
tpc.googlesyndication.com	52,499
cdn.livefyre.com	50,604
cdn.gigya.com	47,768
s1.2mdn.net	32,602
d2lv4zbk7v5f93.cloudfront.net	31,083
staticxx.facebook.com	29,617
ads.rubiconproject.com	28,448
widgets.outbrain.com	25,848
static.chartbeat.com	19,800
img.bleacherreport.net	13,772
ml314.com	12,868
w.usabilla.com	10,999
i.cdn.turner.com	9,638
hpr.outbrain.com	8,717
ad.doubleclick.net	8,478
bs.serving-sys.com	7,974
beacon.krxd.net	7,236
cnn.bootstrap.fyre.co	6,118
optimized-by.rubiconproject.com	4,930
z.cdn.cnn.com	2,915
logx.optimizely.com	2,572
metrics.cnn.com	2,504
b.scorecardresearch.com	2,372
log.outbrain.com	2,187
0914.global.ssl.fastly.net	2,085

Source: webpagetest.org test of cnn.com



- Not covered in detail here, the smartphone and tablet are still at risk, and there seems to be a trend of placing too much confidence in the underlying OS. After a great deal of emphasis on securing devices during the early days of the iPhone and Android, many enterprises have backed off. The decline of Blackberry, a very secure platform, contributed to the overall decline in mobile safety. This is not for the better, as many OS-level threats are not known until after the fact.
- Data residency, though not a threat per-se, will also be top-of-mind in how cloud services are utilized and applications are deployed. The European Union General Data Protection Regulation and the Network Information Security Directive mandate that organizations conducting business in Europe, or those planning to do so, must get an immediate handle on what data they are collecting on European individuals. They must know where it is coming from, what it is being used for, where and how it is being stored, who is responsible for it, and who has access to it. Lack of careful planning and rushed implementations could put enterprises at risk, and potential damages due to the compromise of confidential user data may be greater than expected.
- The increasing deployment within the cloud of virtualized infrastructures, be they VMware, KVM, OpenStack, or containers, open additional avenues of attack. Many enterprises do not fully understand the implications of the shared security model described earlier.

All of these concerns should give you pause and help you to create a framework for planning, but the next three items are downright scary.

- Much of the emphasis has been on the exfiltration and misuse of data, but more concerning is the undetected manipulation of data in place. This could call into question the validity of key financial, legal, and medical records.
- Security companies are heavily invested in artificial intelligence (AI), as are the hackers. Attacks are increasing in sophistication, with advanced techniques used to defeat traditional safeguards. Think of Spy vs. Spy from M.A.D. magazine, only security-style.
- With the proliferation of hacking tools, what was originally limited to more skilled hacking communities becomes available to the mass market. Without the skill set to ensure "safe" behavior (if safe or expected behavior of an attack could ever be considered good), hacks could cause unexpected collateral damage. Consider the example in ransomware, where less skilled programmers are locking up data, and even after you pay the bitcoin ransom, your files are non-recoverable. This is happening now and is expected to grow.

The year 2017 should see an increasing emphasis (and budget) on user training and awareness. Every employee needs to have the discipline to comply with corporate policies, coupled with tests and training and an awareness of potential risks to the company. Enterprises should implement Service Organization Control (SOC) 2 and multi-factor authentication. Periodic training exercises, such as random phishing simulations are essential to learning. Insider threats can be both malicious and accidental, with both capable of doing grave damage to the enterprise. To the CISO's defense, automated security assurance tools must be placed spanning the servers, storage, networking infrastructure, and end-points and extending from the on-premises data center to the cloud.

Finally, though headlines about drone-jacking, connected homes, quantum encryption, and connected cars make for good press, they likely will not impact the typical end-user over the coming year.

Best Practice
Safety Actions

SECURITY IS A

Verb

Remember that security is an ongoing process and not static. Enterprise lifecycle security management is observing, assessing, mitigating, auditing, and repeating.

ARE YOU(R TESTS)

Smarter Than a 5th Grader?

Testing can also be measured against the STRIDE model, first developed by Microsoft, which provides an initial framework for threat modeling. STRIDE stands for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. How good your test system is determines how ready you are to operate in real conditions.

THINK LIKE A

Crook

End-user discipline and education with awareness is key. You think everyone knows what to do, but you might be surprised. Think about how to optimize your three Ps—products, people, and processes.

PRODUCTS

Covers specific product features, system commands, or compliance issues, which hackers can identify and exploit. Think how you would exploit them and assume hackers know just as much.

PEOPLE

Covers both human error and malicious intent from inside an organization. Employees might leave passwords in obvious places or fall victim to social engineering attacks. IT teams might inadvertently leave a port to the network open for maintenance.

PROCESSES

Covers issues, such as how products or services are installed or configured, and even the method and timing of deployments of patches and upgrades.

BE A DRILL SERGEANT

Eliminate routine by reallocating tasks and emphasizing training to eliminate alert fatigue. There is a reason that the military runs constant drills. This is covered in the article "Is Failure in Security a Good Thing?"[2]

SANS Institute research into the incident response capabilities of companies worldwide found that

43%

of respondents did not have a formalized incident response plan

55%

did not even have an incident response team

MONITOR YOUR SOFT SPOTS

Implement the newer generation of vulnerability, compliance, social, behavior analysis, user training, cloud application usage, mobile security, and IP tools. Visibility across every device, user, application, and piece of data is of the essence, with the watchwords "Security through Visibility" replacing "Security through Obscurity." Some examples include forbidding use of cloud applications not sanctioned by IT, mandating strong passwords, and using multifactor authentication.

KNOW YOUR SUPPLIERS

Ensure that any supply chain partners and vendors implement good security practices—especially those who supply critical software or need access to your internal systems.

FIX WHAT IS BROKEN

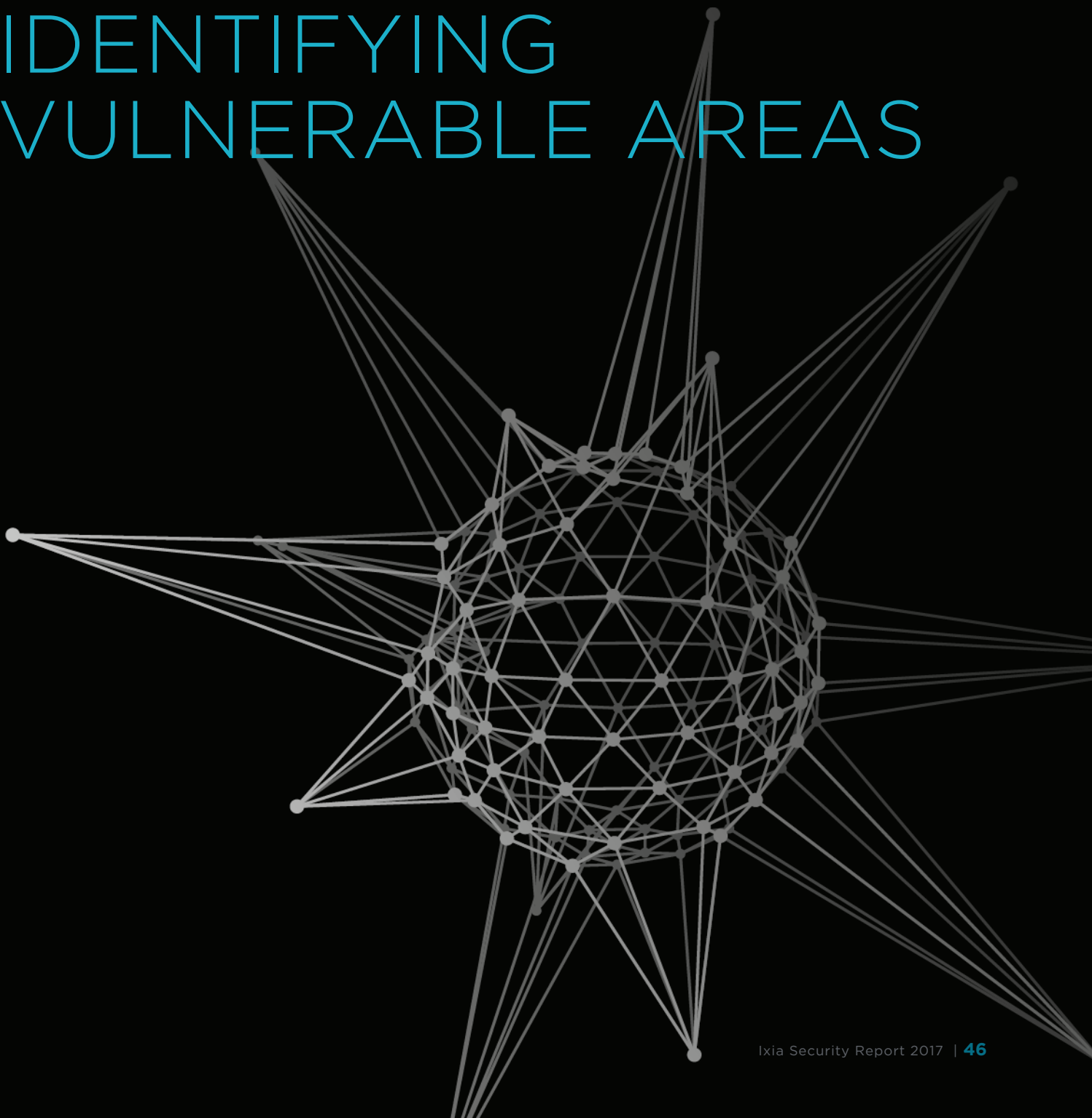
Finally, address known vulnerabilities. They may slip through priorities, but it is a given that it is easier and more inexpensive to fix before, rather than after, a breach. Gartner has stated that "through 2020, 99% of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year."[3]

[2] LinkedIn article, "Is Failure in Security a Good Thing?" April 2016
[3] Gartner, Smarter with Gartner, "Gartner's Top 10 Security Predictions 2016," June 2016

SECTION

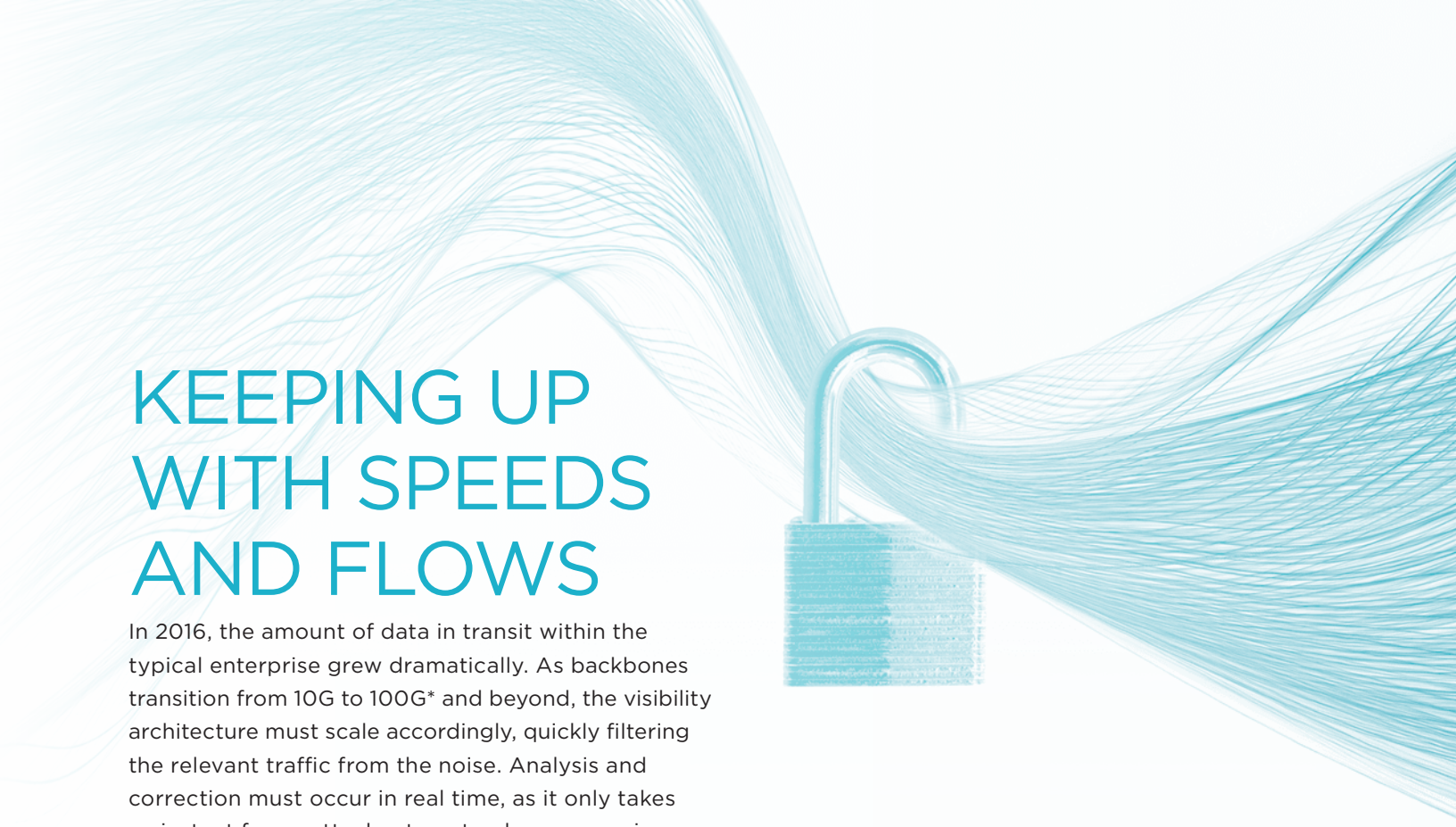
06

IDENTIFYING VULNERABLE AREAS



IDENTIFYING VULNERABLE AREAS

In 2016, the typical organization's attack surface increased in size due to increases in the number of physical and virtual network segments, volume of traffic, and number of IT appliances in use. Within these, there are certain areas that tend to have more vulnerabilities. Two areas we saw overlooked by many in the industry were (1) validating whether portions of your data were not even reaching your security, analytics, and compliance tools, and (2) considering whether threat and application intelligence could benefit you outside its typical uses.



KEEPING UP WITH SPEEDS AND FLOWS

In 2016, the amount of data in transit within the typical enterprise grew dramatically. As backbones transition from 10G to 100G* and beyond, the visibility architecture must scale accordingly, quickly filtering the relevant traffic from the noise. Analysis and correction must occur in real time, as it only takes an instant for an attacker to not only compromise an enterprise network but also hide his or her tracks.

An analogy to growth is typical server connection speed. This averaged 1G in 2009, transitioning to 10G by 2015. By 2020, a noticeable percent should see 100G connectivity, and even 400G is now on the horizon.

(Source: TE Connectivity Estimates http://www.networkcomputing.com/data-centers/100-gbps-headed-data-center/407619707)

As network traffic increases, dropped packets resulting in blind spots begin at the network switch points. Port mirroring, also known as Switched Port Analyzer (SPAN), is a typical method for monitoring network traffic. With port mirroring enabled, the switch sends a copy of all network packets seen on one port (or an entire virtual local area network (VLAN)) to another port, such as an NPB, where the packet can be analyzed. Integrated SPAN ports are convenient but create a scaling limitation.

- Performance: SPAN ports mirror traffic, but the SPAN port is prioritized lower by the network switch. At high-volume burst traffic, the switch will temporarily drop the SPAN process, and that data will never reach the analysis or compliance tools.
- Availability: Many new analytics, compliance, and security tools rely on getting copies of data. When you run out of SPAN ports, your network configuration gets more complicated quickly. The growth in IT tools is creating a severe SPAN port shortage.

Network Taps—physical and virtual—do not suffer from the scaling limitations of SPANs. Regardless of whether you choose to use SPAN ports, taps, or a combination, awareness of your organization's depth of network visibility in each segment will be key in 2017.

After the SPAN or tap, the major contributor to dropped packets is found in the visibility layer, where less-capable NPBs cannot keep up with larger network demands. Most NPBs have single processors with limited ability to manage multiple features simultaneously. Turn on just simple deduplication, for instance, and the performance between the two top vendors can differ by four times. Make sure you evaluate your choices carefully and look for the solution with the best scalability and growth. Some typical areas to consider are:

- Look for a hardware co-processor: Having a hardware-based accelerator can make a huge difference in NPB performance, especially at higher operating speeds.
- Test to ensure no dropped packets: Most NPBs function well at average traffic volumes. Make sure you test at peak volumes to see how your top contenders perform.
- Make sure you ask about simultaneous features: Your NPB may offer deduplication, NetFlow, SSL decryption, and more. Just make sure you can turn on the ones you want at once. Not all of them can support multiple simultaneous features.
- Make sure your NPB is easy to program: This may seem like common sense, but the easier, faster, and more intuitive something is to use, the fewer hours you need to dedicate to it and the fewer mistakes will be made.

Trust but verify. Make sure your network configurations are working the way you think. The best way is to run periodic tests over them to see if they react the way you believe they will. Doing this dramatically reduces your attack vulnerability.

Some companies may be tempted to take shortcuts, such as using internally generated attacks or crowdsourced probes to attack their networks. Just as bad, some have their development teams create and run their own test scenarios. While this can give the illusion that your network is secure, it creates a false sense of security—a single scenario only protects you from one type of attack, and the strength of a product or application is that of its weakest link.

Large American Insurance Company Case Study

A large American insurance company saw attacks on its network that its intrusion detection system (IDS) was not catching. The company changed the IDS system but then noticed that the new system was also missing attacks. It could not diagnose why the platform was not performing in the live network when it caught the attacks in the lab. The company asked Ixia to help. Ixia leveraged its BreakingPoint® with PerfectStorm™ product to launch traffic mixed with malware at the network and to monitor what occurred. The results showed that the IDS performed as per specification but it simply was not seeing the traffic, because the NPB was dropping packets under heavy load. The monitoring tools did not capture attacks, because they did not see all the traffic. The insurance company replaced its legacy packet brokers with high-performance Ixia Vision ONE packet brokers, and it improved its overall security posture, as its IDS received all the necessary data.

LEVERAGING APPLICATION AND THREAT INTELLIGENCE

Every day, hundreds of new applications and millions of new attacks are unleashed on the Internet. Tracking the new and emerging threats—the payload—is threat intelligence. Tracking changes and evolutions in applications—the delivery mechanisms carrying many of the threat payloads—is application intelligence. Many security providers offer threat intelligence—the tracking of attacker profiles, methods, and attack vectors. Some vendors offer application intelligence—the monitoring of applications in action. Both are critical to your operation and are more intertwined than they may appear on the surface.

The modern application is complex. Few understand this as much as those of us at Ixia, since we have tested equipment, networks, and applications for decades. That is why we created the ATI Research Center, collaborating with top application and security researchers from around the globe. The ATI Researchers expertise spans software development, reverse engineering, vulnerability assessment and remediation, malware investigation, and intelligence gathering.

Ixia's ATI Research Center combines proficiency in cybersecurity threats and application protocol behavior. We use this combination of application and threat intelligence across test, visibility, and security solutions to:

- Create realistic application attacks—from protocols through loading and threats
- Block malicious inbound and outbound communications
- Collect ongoing intelligence on new threats
- Identify unknown applications
- Detect traffic geo-location

An application and threat intelligence feed needs to extend far beyond simple signature recognition. It needs to proactively defend against attack patterns to reduce an organization's overall attack surface. Ixia uses aspects of its ATI feeds in several of its product offerings—from security and network visibility to network and equipment testing. Below are just a few of the ways an ATI feed can be leveraged to better secure networks.

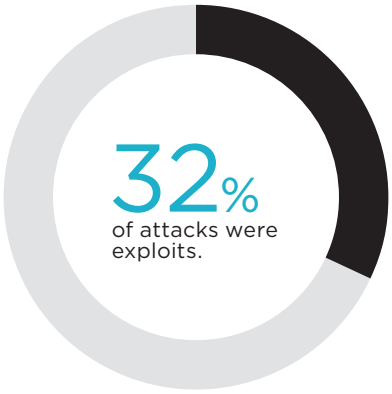
Product	ATI Leverage
ThreatARMOR™ Security appliance blocks traffic from known bad Internet Protocol (IP) addresses before it hits the security infrastructure	Continuously updated threat intelligence identifies, tracks, and individually validates every IP address on the Internet. It identifies malicious sites and unregistered and hijacked IP addresses and blocks them—both from entering or being communicated to from inside your network.
Vision ONE NPB aggregates data from multiple sources and distributes it to security, analytics, and compliance tools	An advanced form of NetFlow data provides deep knowledge of applications, including application bandwidth, device and browser type, and geo-location of application traffic. It can validate that an application feed is genuine and can dynamically detect new applications without signatures.
BreakingPoint Test system provides realistic, Internet-scale simulations of application traffic and attacks to validate network performance and security	Simulating realistic attacks and attack conditions with over 300 application protocols and 36,000+ security attacks (exploits, malware, DoS and DDoS). Mixes these attacks with various combinations of application flows, encryption schemas, and user loads to truly stress test entire networks or network equipment.
IxLoad®, IxNetwork®, and IxChariot™ Test application and network traffic and protocols to validate quality of service and performance of apps, networks, and devices	AppLibrary is a simplified workflow and framework that enables users to emulate realistic application mixes from a library of application flows. AppLibrary is used by IxNetwork, IxLoad, and IxChariot applications to simulate large volumes of protocols, applications, and network traffic for testing networking equipment and configurations.

Ixia utilizes this threat and application intelligence feed to actively protect customers from malicious attack attempts. The importance of being able to identify malicious IP addresses in various attacks cannot be overstated, as it can be one of the simplest and fastest ways to ensure a stronger security posture. Although the attribution of a cyberattack to a group or person is tenuous at best, we can understand the routes hackers took to reach their targets. Across 2016 and through our ThreatARMOR appliance deployments with various customers around the globe, we saw trends of where the cyberattacks originated and who they targeted.

36%
sourced from
the U.S.

4%
sourced from
Russia

12%
sourced from
China/Hong Kong



14%
sourced from
the U.S.

14%
sourced from
China

9%
sourced from
Vietnam

6%
sourced from
Brazil

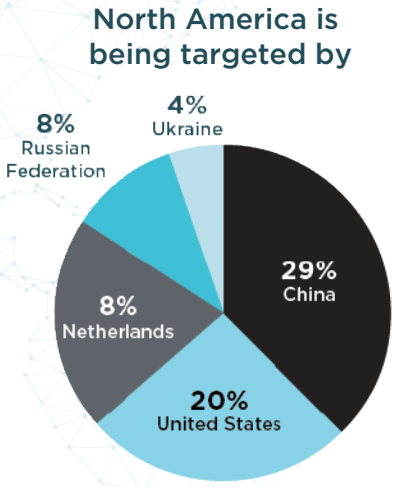
54%
sourced from
the U.S.

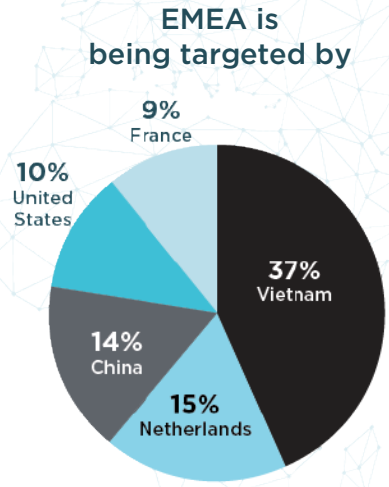
4%
sourced from
the UK

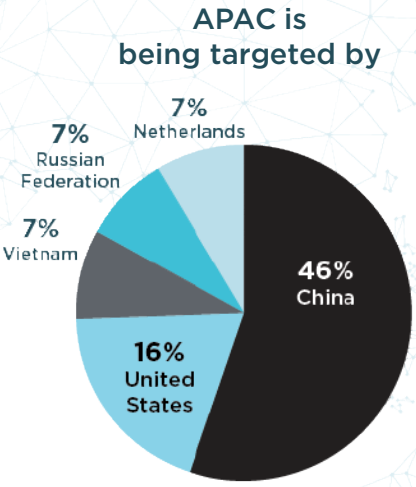
4%
sourced from
Germany

3%
sourced from
Russia

Ixia research revealed insights into which countries tend to attack which regions of the world, based on our worldwide deployments of security devices. Location determines who is most likely to launch attacks against you. For instance, if you have offices in Europe, those offices are more likely to be attacked by IP addresses located in Vietnam than from IP addresses located in China. If your office is in the U.S., attacks originating from Vietnamese IP addresses are much rarer, and China would be the primary origination point for attacks.







The Ixia ThreatARMOR product is highly effective in blocking these known malicious IP addresses. It can also quickly and simply block IP addresses from entire countries that have no business being inside your network. A sample of a ThreatARMOR user display tracks attacks being blocked and the location from which they were sourced. It not only blocks these addresses from entering your network, it provides proof, in the form of a Rap Sheet, with screen shots capturing why the malicious IP is being blocked.

SECTION

07

CONCLUSION

CONCLUSION

In 2016, expansion into more clouds, the addition of industrial IoT, and marked increases in virtual deployments resulted in more devices, more locations, and more environments to monitor and protect. Every new device could create a vulnerability—either on its own or when communicating with other devices in the network. The network attack surface continued to grow.

The roles of the CISO and CIO are becoming more multi-faceted. They are being pushed to look beyond simply "inside the firewall" protection or perimeter defenses. As the perimeter continues to extend and blur, the methods of monitoring and protection must evolve as well. As the number of analytics, compliance, and security tools being used continues to grow, this creates its own vulnerabilities.

We all want to believe that every new device we integrate includes consideration for security in their design; that the data sheet tells us the entire story, and that integrating devices from multiple vendors into a single network will simply work. The only way to ensure this is to test it at scale and to monitor it in operation. Testing each device would be advisable, but we all recognize that would be expensive and time consuming for most.

Here are some key takeaways:

- **Protect the simple stuff**. Most modern firewall and security tools will protect you adequately from the latest security threats. But most attackers lack the resources to create advanced zero-day malware. Most attackers reuse simple methods, including DDoS distractions, older malware/exploits, admin password guessing, or phishing. Start with user name and password hygiene, as it is the first place an attacker will look.

- **Challenge your security architecture**. We are constantly surprised at how many networks are not exposed to large-scale testing before deployment. Always challenge your defenses not with average data flows, but drive them to capacity to see how or if they fail. After all, attackers are doing this every day.

- **Validate provisioning**. Every time a new security or performance monitoring product is added, a new cloud is connected, or a network segment is established, there is provisioning. The vast array of command line interface connections that need programming leads to more complexity. And, complexity typically leads to mistakes or vulnerability.

- **Adopt a Zero Trust model**. Never trust. Always verify. Every new device, every new network update, and every provision should trigger validation testing. One error can create an opening.

- **Inspect encrypted traffic**. Many organizations do not decrypt encrypted traffic like SSL and SSH or leave it to individual security and performance monitoring tools to accomplish. This becomes a major blind spot that attackers are using to hide malware.

- **Limit your attack surface**. The more you can limit your network environment, the easier it will be to protect.

Constantly questioning, challenging, and most importantly, testing your network's ability to withstand attacks is wise. The difference between being "in decent shape" and "Olympic-ready" comes down to training intensity. Test to your network's throughput and loading limits using realistic test environments. Get total visibility into your physical and virtual data no matter where it resides.

When you are ready to test and monitor your networks using the best in the industry, contact us at www.ixiacom.com. Ask for a demo, and we will show you what is possible.

SEE
INSIDE

IXIA WORLDWIDE HEADQUARTERS

26601 W. AGOURA ROAD
CALABASAS, CA 91302

(TOLL FREE NORTH AMERICA)
1.877.367.4942

(OUTSIDE NORTH AMERICA)
+1.818.871.1800
(FAX) 1.818.871.1805
www.ixiacom.com

IXIA EUROPEAN HEADQUARTERS

IXIA TECHNOLOGIES EUROPE LTD
CLARION HOUSE, NORREYS DRIVE
MAIDENHEAD SL6 4FL
UNITED KINGDOM

SALES +44.1628.408750
(FAX) +44.1628.639916

IXIA ASIA PACIFIC HEADQUARTERS

101 THOMSON ROAD,
#29-04/05 UNITED SQUARE,
SINGAPORE 307591

SALES +65.6332.0125
(FAX) +65.6332.0127

© 2017 Ixia. All rights reserved | 915-8136-01 Rev A