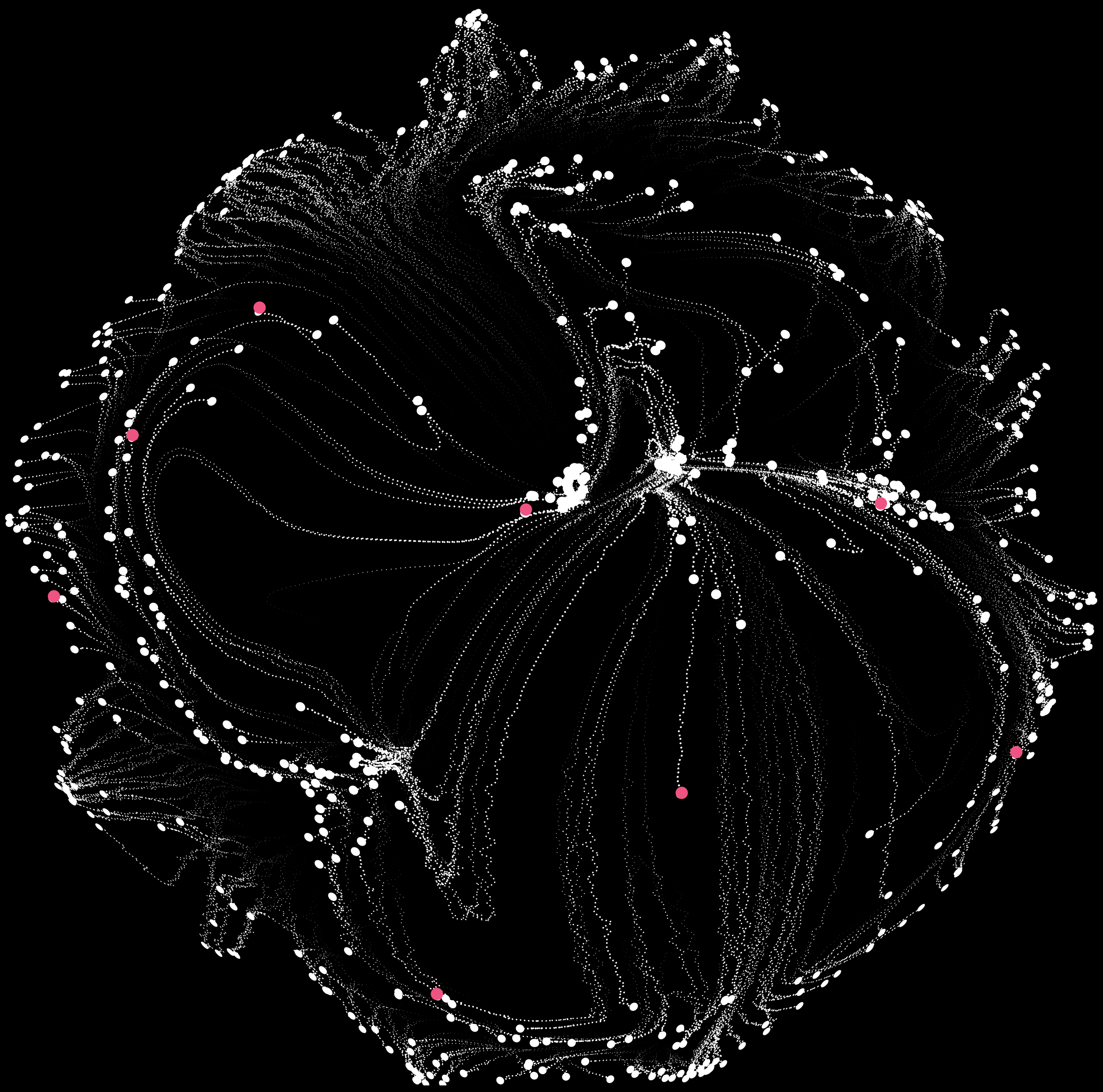
2016 SECURITY REPORT



Check Point® SOFTWARE TECHNOLOGIES LTD

ONE STEP > AHEAD

1. INTRODUCTION AND METHODOLOGY 04-11

2. THE ATTACK ARSENAL: KNOWN AND UNKNOWN MALWARE 12-19

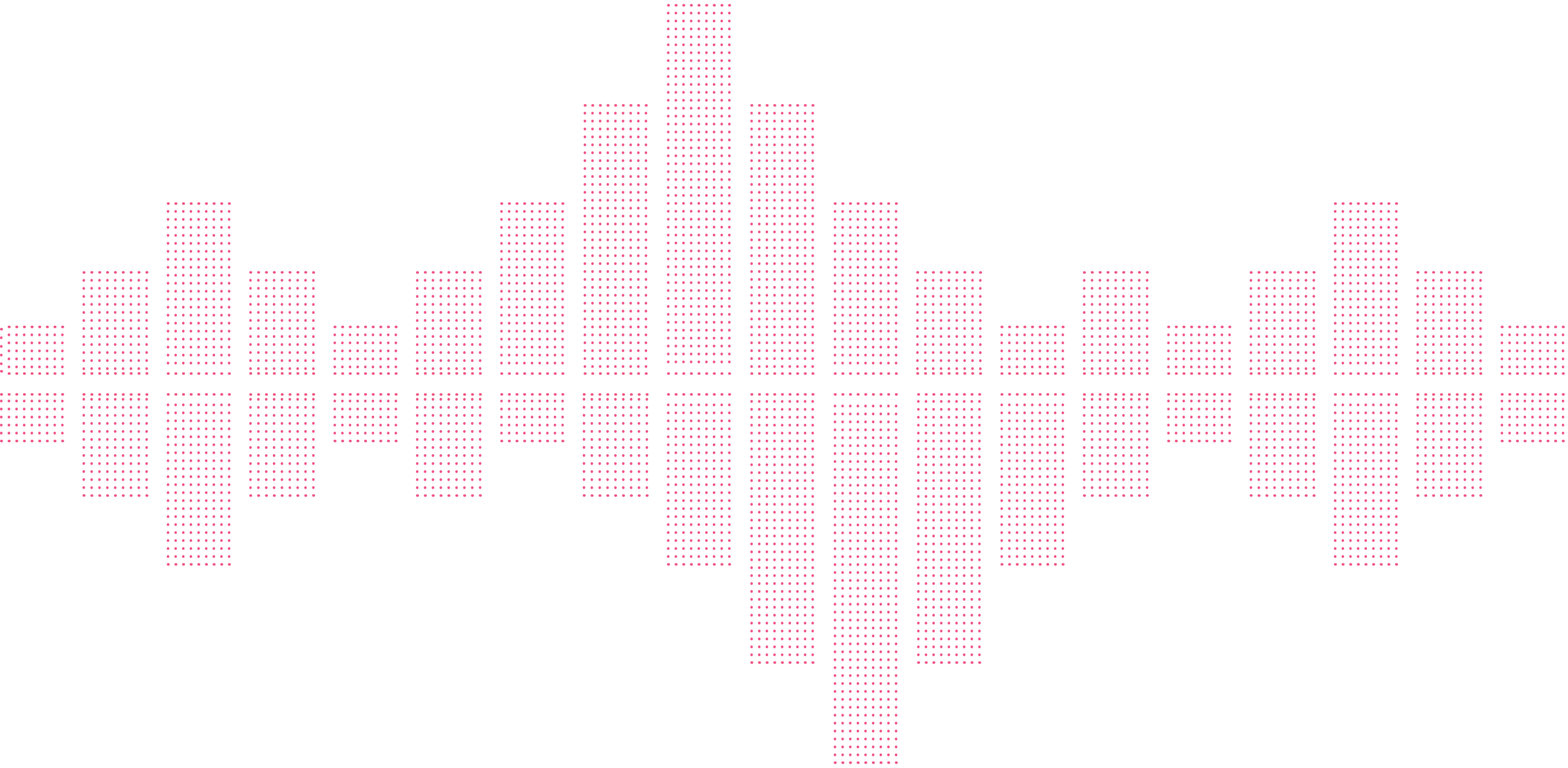
3. ONE DEVICE FOR PERSONAL AND BUSINESS 20-27

4. STUDYING ATTACK PATTERNS 28-37

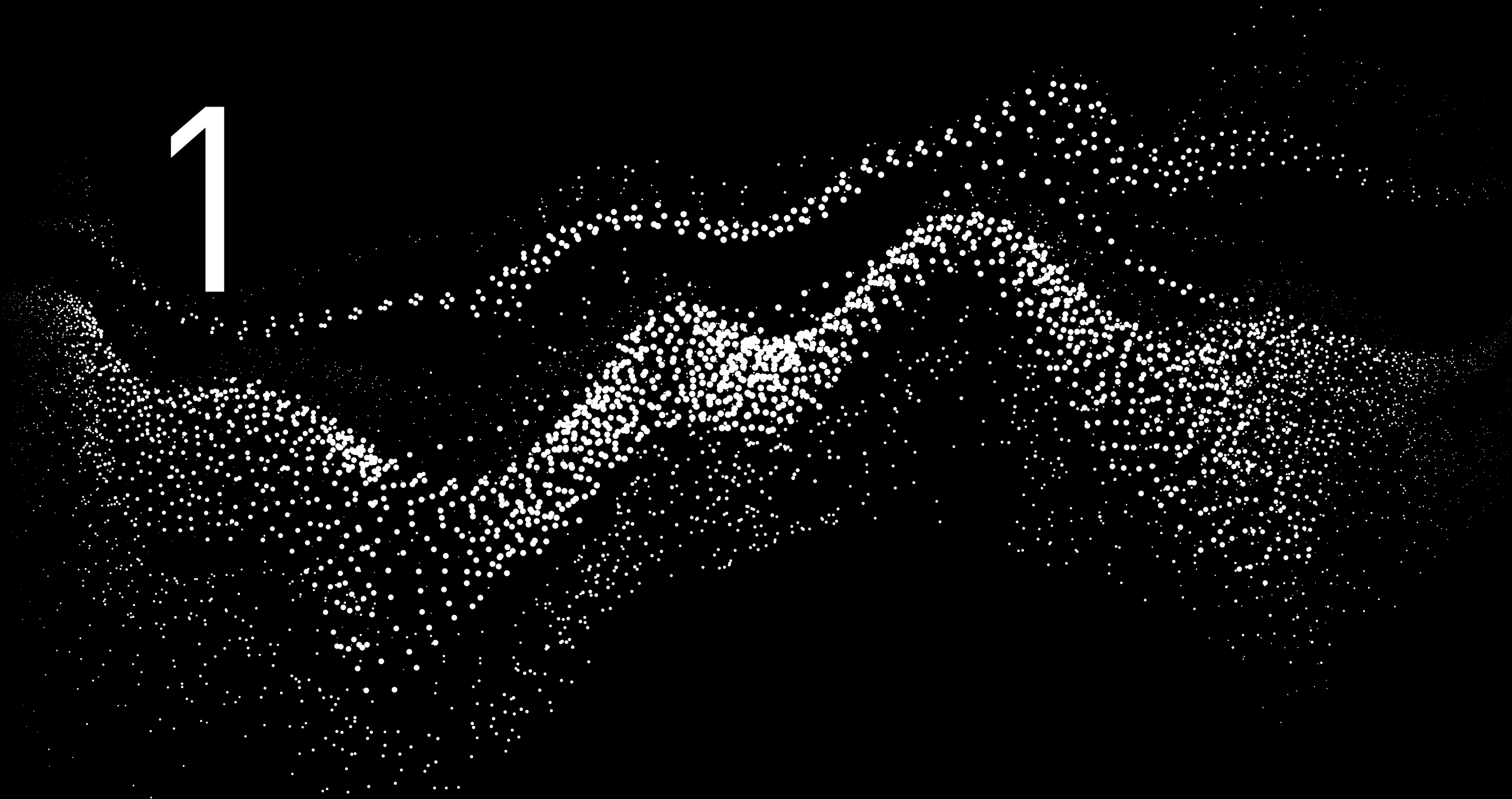
5. THE RIPPLE EFFECTS OF INSECURITY 38-47

6. STAYING ONE STEP AHEAD 48-55

REFERENCES 56-58



2016 SECURITY REPORT



1

INTRODUCTION AND METHODOLOGY

"We are stuck with technology when what we really want is just stuff that works."

Douglas Adams, author and satirist

> *The prize for the biggest hack of 2015 goes to OPM—the [U.S.] Federal Office of Personnel Management. The hackers, reportedly from China, maintained their stealth presence in OPM's networks for more than a year before being discovered. When the breach was finally uncovered, initial estimates placed the number of victims at four million. But that number soon ballooned to more than 21 million, including some 19 million people who had applied for government security clearances and undergone background investigations, as well as an additional 1.8 million spouses and live-in partners of these applicants. The hackers got their hands on a trove of sensitive data, including the SF-86 forms of people who applied for clearances. The forms can contain a wealth of sensitive data not only about the workers seeking a security clearance, but also about their friends, spouses, and other family members.*
>
> — **Wired Magazine**, December 23, 2015

While there were a number of notable breaches in 2015, the OPM breach garnered high levels of attention because it took more than a year to discover and the ripple effects of this particular breach are very far reaching. Reading this year's Security Report, it becomes clear that the protection model of security that reacts to threats is no longer sufficient to safeguard today's enterprises. Losing is a real possibility. This kind of breach can happen to anyone. To help you protect your organization, your data, and your customers, we have woven recommendations into each of the report's chapters. Every breach is a learning experience that inspires us to protect ourselves better. We can all learn from OPM's experience.

In April 2015, it was disclosed that as many as 21 million personnel records were stolen from the United States Office of Personnel Management, the central human resources repository for the U.S. Government.

These records included detailed security clearance application forms along with the fingerprints of 5.6 million employees. According to federal officials, it is one of the largest breaches of government data in the history of the United States.

According to U.S. Department of Homeland Security official Andy Ozment, the breach started nearly a year before it was discovered. The attackers initially gained valid user credentials to access the system, likely through social engineering. Once inside, they launched a malware package, establishing a backdoor for persistency. From there, they escalated their privileges, gaining access to a wider range of OPM systems.

This one incident highlights how a modest network entry-point breach can expand into a large-scale, multi-month data extraction. As networks grow and are segmented, then reconnected, it can be complicated just to keep up with the network resources map. The sheer volume of attacks targeting an increasingly blurry network edge complicates matters further. The OPM breach clearly shows the need for unified security architecture providing coverage of all server environments and all types of endpoints with real-time preventative security measures as well as measures that uniformly apply data loss prevention. Proactively scanning internal networks, segmenting network elements, and requiring multi-factor authentication also helps ensure security. These must be part of every organization's baseline security posture. When an attack is successful, analyzing breach methods tells a lot about an attacker, their motives, and how you can best protect against them in the future.

Prevention Call to Action

All organizations can learn from the OPM breach. Preventing attacks before they inflict damage and using a unified security architecture to simplify and harden security is a must in today's threat landscape.

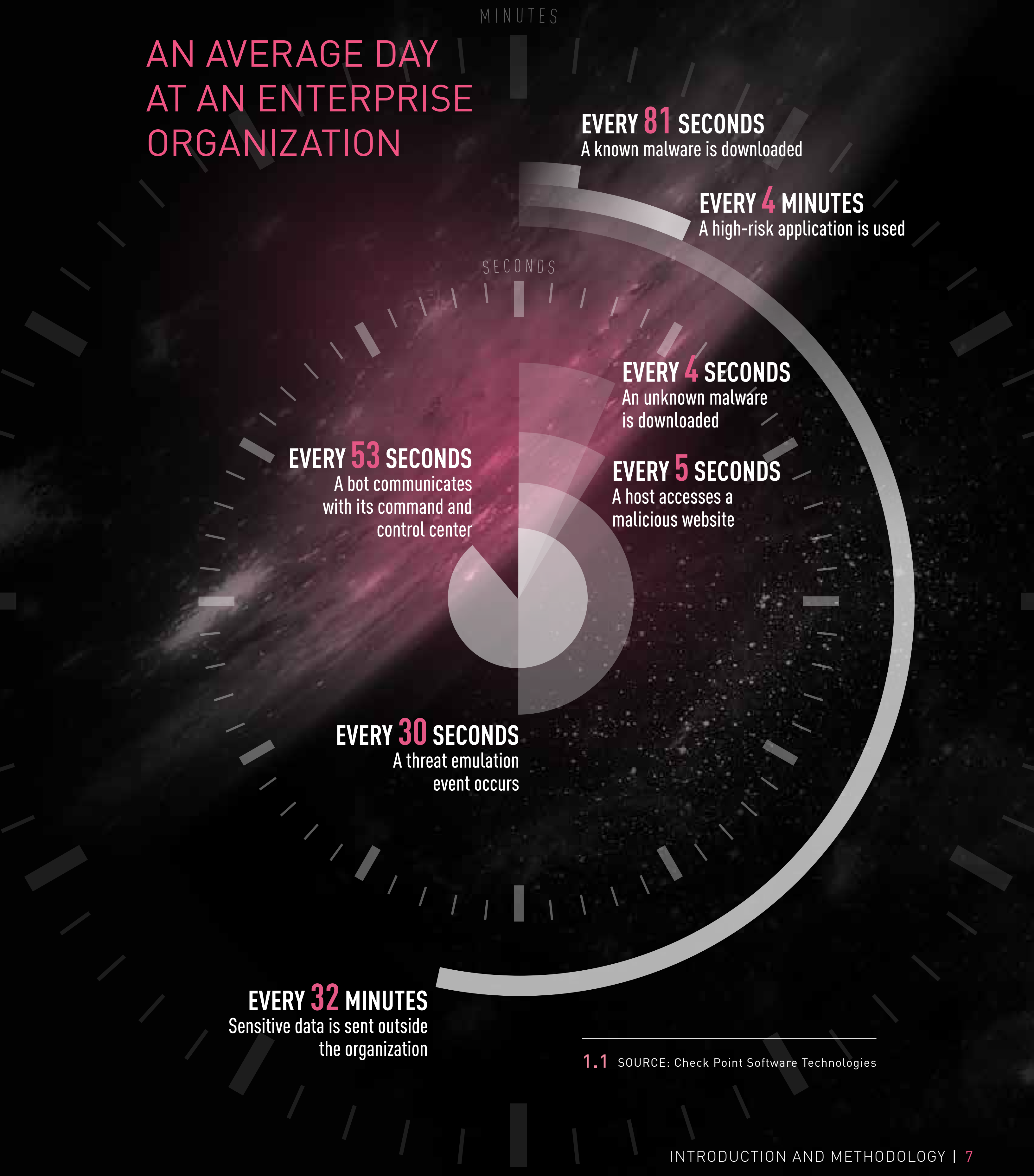
Segment your network and enforce uniform policies on all segments using unified security architecture.

Patching leaves gaps. Use IPS virtual patching for protection that spans periodic patch updates.

Prevent malware infections in real time with CPU and OS level threat prevention.

Monitor all network segments through a single pane of glass.

AN AVERAGE DAY AT AN ENTERPRISE ORGANIZATION



EVERY 81 SECONDS
A known malware is downloaded

EVERY 4 MINUTES
A high-risk application is used

EVERY 4 SECONDS
An unknown malware is downloaded

EVERY 53 SECONDS
A bot communicates with its command and control center

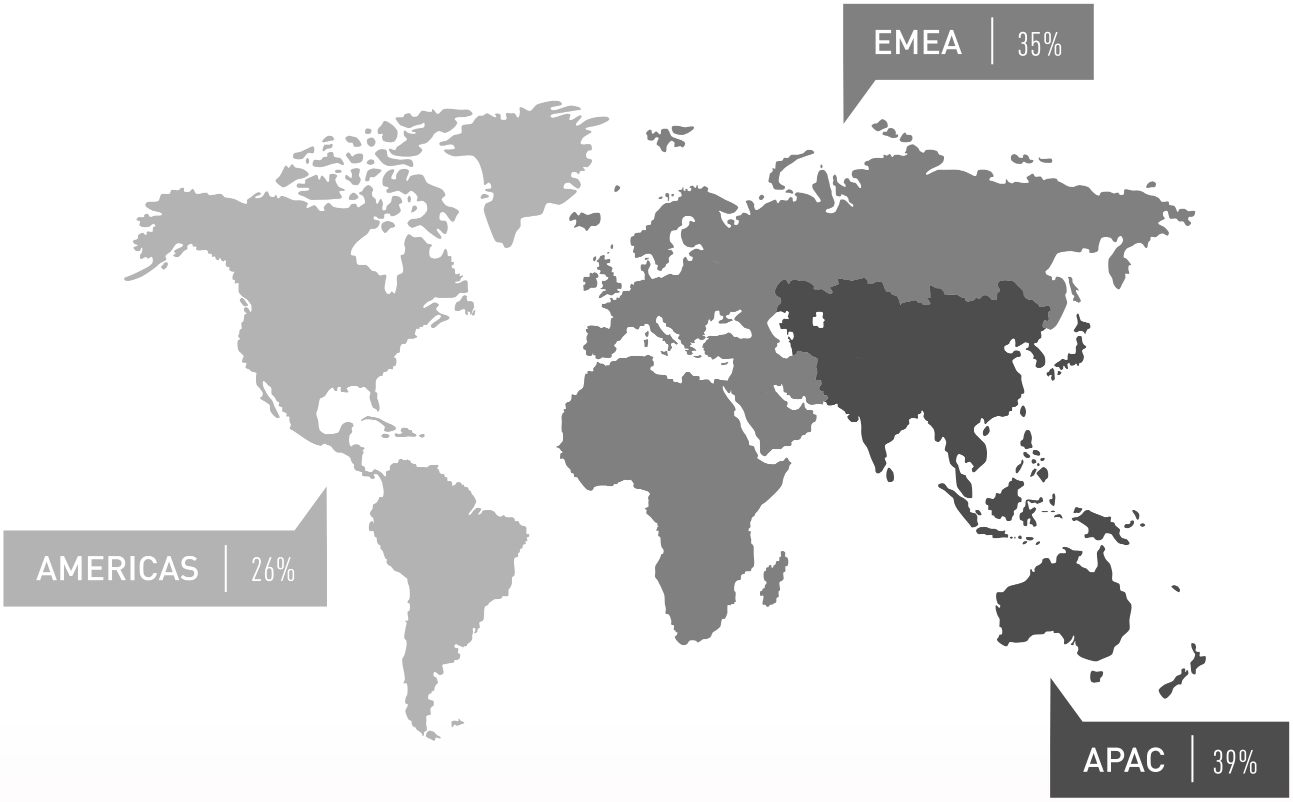
EVERY 5 SECONDS
A host accesses a malicious website

EVERY 30 SECONDS
A threat emulation event occurs

EVERY 32 MINUTES
Sensitive data is sent outside the organization

1.1 SOURCE: Check Point Software Technologies

ORGANIZATIONS BY GEOGRAPHY



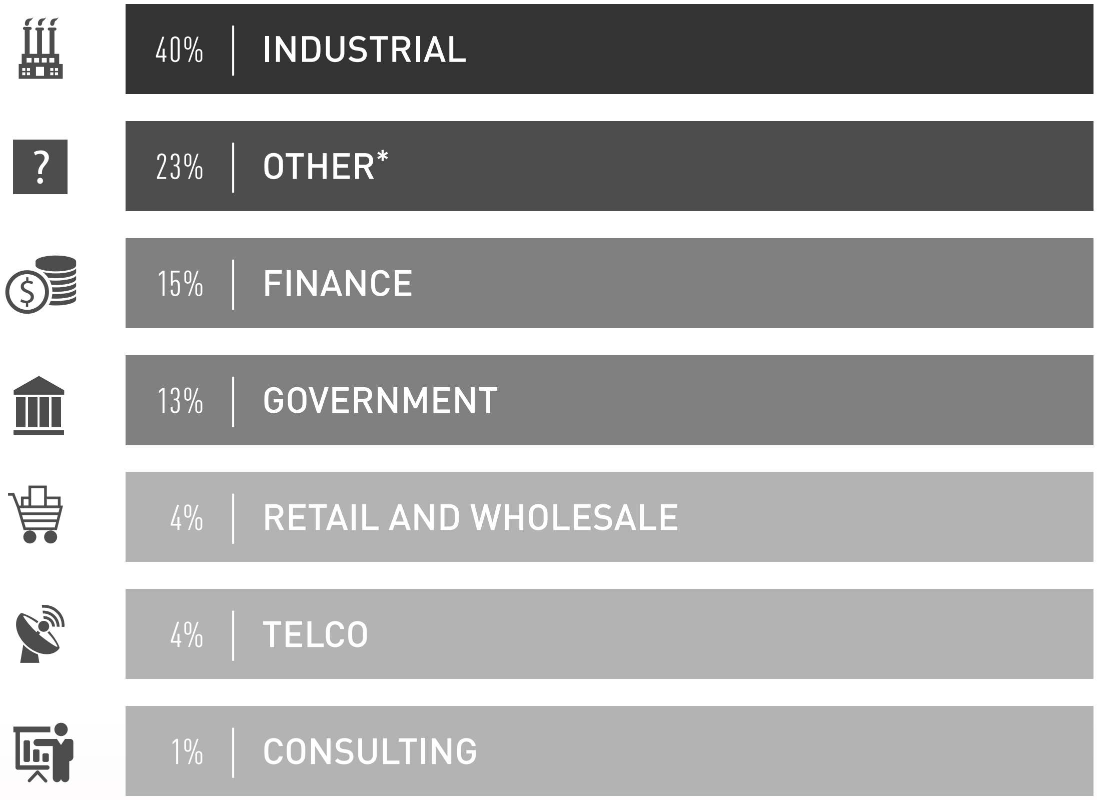
1.2 SOURCE: Check Point Software Technologies

SOURCES OF CHECK POINT RESEARCH

To stay one step ahead, we collected event data from different sources around the world throughout 2015.

This included research from more than 1,100 Security Checkups, events discovered through ThreatCloud (which is connected to more than 25,000 gateways worldwide), and more than 6,000 gateways reporting to our Threat Emulation Cloud. We combined that data with analysis of external trends and insights from our internal research team to develop each of our section recommendations.

ORGANIZATIONS BY INDUSTRY



*Legal, Leisure/Hospitality, Retail and Wholesale, Advertising/Media, Securities, Other

1.3 SOURCE: Check Point Software Technologies

STRUCTURE OF THE 2016 SECURITY REPORT

Our 2016 Security Report looks at what enterprises are encountering in known and unknown malware, attack trends, as well as the impact of more mobile devices in the enterprise. Additionally, we look at the impacts successful breaches have on organizations and their brands' added expenses that go well beyond the obvious cleanup costs.

Chapter 2 explores and analyzes different types of malware and how they take advantage of users' behavior. The majority of large scale

2015 BY THE NUMBERS

75% of organizations had existing bot infections

82% of organizations accessed a malicious site

88% of organizations suffered a data loss incident

89% of organizations downloaded a malicious file

94% of organizations used at least one high-risk application

400% increase in loss of business data records the past three years

1.5B files analyzed for this report

1.4 SOURCE: Check Point Software Technologies

breaches in 2015 were perpetrated using existing vulnerabilities, known malware and, of course, social engineering. While user attempts to access malicious sites is up, IT effectiveness to block them is improving slightly faster, making that attack vector slightly less effective. Meanwhile, bot infections are down, but the frequency of bot communications attempts per day is way up.

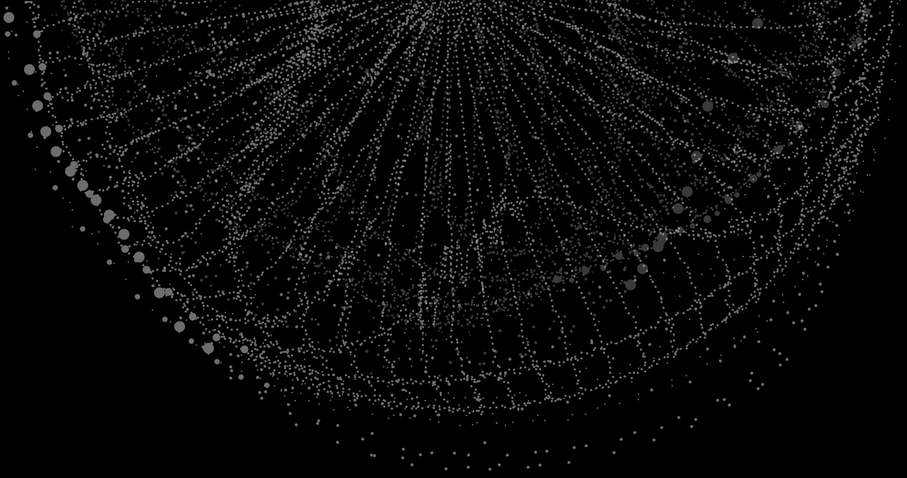
Chapter 3 explores how the mobile revolution continues to bring new attack opportunities as more mobile devices enter the enterprise largely unchecked. Organizations now realize they cannot easily stop employees from connecting their personal devices to corporate resources, because they have discovered that "bring your own device" (BYOD) greatly increases productivity. Unfortunately, the mobile platform is an attractive target for attackers as most organizations have not put in place controls to effectively protect them.

In Chapter 4, we look at the patterns of attacks by global region and by type. The U.S. still leads the world in malicious file and malicious website hosting, in large part due to the remarkably higher percentage of active users and abundance of resources. As for the attack vectors hackers prefer, code execution such as return-oriented programming (ROP) emerged as the most popular attack vector for hackers, as deployment of patches for buffer overrun vulnerabilities rendered 2014's most popular attack vector less attractive. Overall, vulnerabilities were down slightly in 2015, but vendors with the top vulnerabilities have shifted. Trends may change, but if organizations fail to implement vital patches, attack vectors will never truly be extinguished.

While initial costs of a breach are well documented, the overall financial impacts run much higher. In Chapter 5, we explore these ripple effects of insecurity, diving into examples across the finance, healthcare, and industrial sectors. Maintaining the speed of business while keeping it safe is your best financial move.

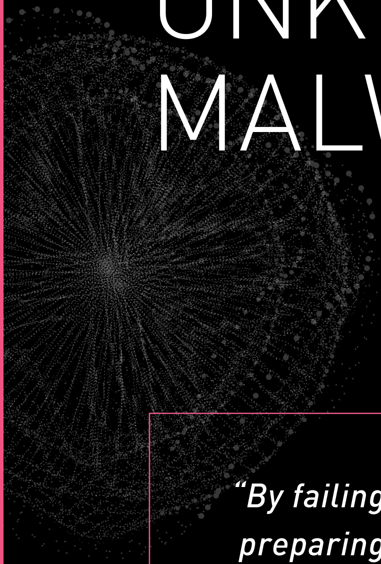
Staying one step ahead means staying on top of all areas: malware, attack trends, managing the mobile revolution, and being aware of the impact of missing something. In each chapter, you'll find our recommendations on how you can keep your organization a step ahead of cybercriminals.

> *"Any sufficiently advanced technology is indistinguishable from magic."*
>
> Arthur C. Clarke, science fiction writer



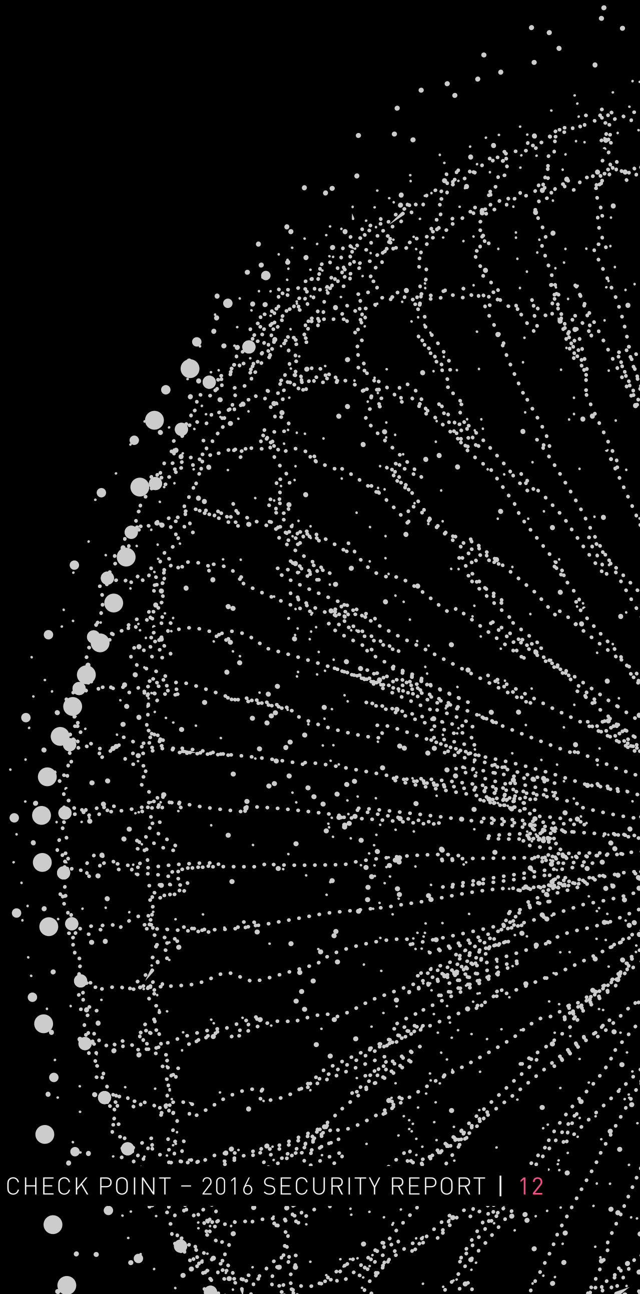
2

THE ATTACK ARSENAL: KNOWN AND UNKNOWN MALWARE



"By failing to prepare, you are preparing to fail."

Benjamin Franklin, politician, author



Known Malware

a piece of identified malicious software with a recognizable signature.

Many security tools use signature-based techniques when analyzing and making blocking decisions, but require users to keep their firewall and antivirus definitions up to date.

Unknown Malware

a piece of unidentified malicious software without a recognizable signature on file.

Creating unknown malware can be as simple as making a small modification to a known malware, or repackaging malware with a different payload. This new unknown version can then bypass signature-based defenses.

Zero-Day

exploits that take advantage of previously unknown security vulnerabilities where there are currently no protections in place.

The first step of an attack is getting the malware past the security barrier. In 2015, this was accomplished using a large volume and variety of attacks. Most malware hides in the form of legitimate looking traffic or attachments, or exploits legitimate network control or access functions. Whether hiding in a link, in a document, or exploiting a shell vulnerability, attackers use a range and mixture of ingress methods.

Regardless of the method of entrance, we can think of malware as one of three basic types: known, unknown and zero-day.

Nearly one million new pieces of malware are launched every day.[1] Verizon's 2015 Data Breach Investigations Report estimates that close to 90 percent of 2015 hacks used a vulnerability that has existed since 2002. HP's latest Cyber Risk Report[2] asserts that of the top ten vulnerabilities exploited in 2015, all of them were over a year old, and 29 percent of breaches used a 2010 infection vector with two different patches available. While unknown rates are on the rise, known vectors are still dominating the threat landscape.

EVERY 5 SECONDS, A USER ACCESSES A MALICIOUS SITE

Today's forecast for data centers is mostly cloudy. Cisco estimates cloud data centers will process over 86 percent of IT workloads by 2019.[3] According to RightScale, 95 percent of businesses already employ cloud platforms, using on average 3 public clouds and 3 private clouds.[4] Despite the rapid migration to the cloud, few IT professionals consider how running services in virtualized public and private cloud environments can cause turbulence for their security. What causes the turbulence is the pattern of data traffic changes from flowing north/south in traditional data centers to flowing east/west in public cloud environments, and as workloads move off-site to public cloud domains.

Clouded Thinking: Your Data Traffic Could be Headed the Wrong Way for Security

Say what you will about traditional data centers: they add months to new application deployments and aren't very scalable. In addition, they require a ton of manual intervention to operate. But for security, traditional data centers do pretty well with the right security gateway racked and connected where the fiber from the backbone comes through the raised floor. This is because in old-school data centers, traffic travels north from servers to the security gateway and south from the gateway back to servers. Traffic can even follow north/south "hairpin" turns that go up from a server to the gateway and back down to another server within the data center so internal traffic can be inspected for threats.

However, in virtualized or software-defined networks deployed in private cloud environments, up to 80 percent of the traffic travels east and west among virtualized applications and various network sectors. Furthermore, virtualized applications can migrate among host servers as resource usage changes. Under these conditions, the majority of traffic entirely bypasses the perimeter security gateway. Mobile apps, cloud apps, partner apps and even hosted customer apps can connect services to users outside the data center through various pathways not scanned by perimeter security controls. If attackers compromise even one of an organization's minor web services with malware, the entire network, including core services, are at risk.

Therefore, to maintain IT security in virtualized public and private clouds, it is helpful to think about segmenting your network and applications by using the same security capabilities as physical gateways, but with the addition of flexible support for software-defined micro-segmentation which can be centrally managed. High visibility of applications is also critical for securing cloud-based services traveling in new directions because of cloud platforms and domains.

MORE DEVICES, MORE WAYS IN

Today's enterprise must protect dramatic increases in the number of remote workers, organizations with multiple sites, cloud-based applications, and lots more devices. The number of network entry points requiring protection continues to increase. Every wired and wireless entry point, the servers and infrastructure that host enterprise applications, and signature-based threat prevention tools that protect them, need constant patches and updates.

Staying up-to-date with critical security patch management continued to be an issue in 2015, keeping known malware very relevant.

ORGANIZATIONAL DISCIPLINE: BETTER, BUT NOT YET GOOD

Our research shows that organizations are doing a slightly better job of preventing user access to malicious sites. In 2015, only 82% of organizations accessed a malicious site—lower than the 86% of 2014. Unfortunately, other metrics were not as positive.

In enterprise organizations, users accessed a malicious website five times more frequently in 2015—every 5 seconds compared to every 24 seconds the previous year.

With more frequent access comes more malware, affecting more enterprises. In 2015, 89% of organizations downloaded a malicious file, compared with 63% in 2014. In 2015, organizations downloaded malware four times more frequently—every 81 seconds compared to every 6 minutes in 2014.

A USER DOWNLOADS MALWARE EVERY 81 SECONDS

2.1 SOURCE: Check Point Software Technologies

What does this mean? While organizations do their best to prevent access to malicious sites and files, the sheer volume of attacks gives the advantage to the attacker. Organizations must evaluate and filter greater volumes of potentially malicious content while maintaining user productivity. They must instantly isolate malware in real time to prevent its spread and negative impact.

2015 RECOGNIZED BOT ATTACKS

FAMILY	DAMAGE	PERCENT
SALITY	Steals sensitive information	18.6%
CONFICKER	Disables system security services, gains attacker remote access	18.6%
ZEROACCESS	Allows remote operations and malware download	6.7%
CUTWAIL	Spreads spam	5.1%
GAMARUE	Opens a backdoor for attacks	3.0%
ZEUS	Steals banking credentials	2.7%
LDPINCH	Steals sensitive information	2.1%
DELF	Steals authentication credentials	1.1%
RAMNIT	Steals banking credentials	1.0%
GRAFTOR	Downloads malicious files	0.9%

2.2 SOURCE: Check Point Software Technologies

BOT PROBLEMS PERSIST

Bots remain a significant attack methodology for attackers. Similar to a worm or Trojan, a bot executes a variety of automated tasks once inside a network and communicates out on a regular basis. Replicating themselves onto adjacent networks and devices, or projecting themselves outside their host network, they send spam or participate in denial of service and other types of attacks.

Some bots remain dormant until they are activated remotely through a predetermined victim computer action or at a specific future time. Despite differences, bots typically communicate back to a command and control (C&C) machine to provide activation status and receive instructions. Those communications can be isolated, tracked and blocked.

In 2015, a typical bot attempted to communicate with its command and control (C&C) server over 1,630 times per day, or once every 52.8 seconds. This speed and frequency continues to increase, jumping 12% from the previous year, and 95% more than in 2012.

While bot infection levels were down almost 10% in 2015 from 2014, the numbers are still troubling. Almost 75% of organizations studied were infected with bots in 2015, with 44% of those active for more than four weeks.

Bot attacks steal sensitive information such as authentication and banking credentials, disable system security services, and gain remote access for attacks. Bots also engage in remote operations and download additional malware.

An analysis of bot attack data show four specific bots: Sality, Conficker, ZeroAccess, and Cutwail were responsible for 50% of recognized bot attacks in 2015. Interestingly, these bots all originate from well-known malware.

BOTS TRY TO COMMUNICATE WITH C&C OVER 1,630 TIMES PER DAY, OR EVERY 52.8 SECONDS

274 NEW, UNKNOWN MALWARE DISCOVERED EVERY MINUTE THROUGHOUT 2015

THE CONTINUED RISE IN UNKNOWN MALWARE

Overall, unknown malware usage by attackers remained at historically high levels, growing slightly in 2015 according to AV-TEST.[5] In 2015, almost 144 million new malware were found—274 new, unknown malware were produced and launched every minute of 2015.

During 2015, Check Point analyzed over 6,000 gateways, finding 52.7% of them downloaded at least one infected file with unknown malware. On average, 2,372 infected files were reported per gateway.

On the user side, attacks were more frequent and varied. With more than 971 unknown malware downloads per hour, over 9 times last year's 106 downloads per hour, many organizations found themselves struggling to keep up.

Most users know the risk of infection is higher for certain file types. As expected, .exe files represented nearly 30% of infected files, and archive formats such as .zip and .jar were more than 16% in 2015. The growth of malware continues to be in file types most users trust, such as PDF, Flash, or Microsoft Office files, as hackers take advantage of these less threatening file types. In 2015, Microsoft Office file formats accounted for more than 9% of malicious files seen, and PDF another 7.5%.

75%

OF THE ORGANIZATIONS STUDIED WERE INFECTED WITH BOTS

52%

OF GATEWAYS DOWNLOADED AT LEAST ONE INFECTED FILE WITH UNKNOWN MALWARE

971

UNKNOWN MALWARE HIT AN ORGANIZATION EVERY HOUR

28%

OF FILES INFECTED WITH MALWARE ARE SWF (SMALL WEB FORMAT FLASH) FILES

2.3 SOURCE: Check Point Software Technologies

Flash continued to grow as a malware delivery mechanism, representing 28% of files infected with unknown malware downloaded. When packaged as a Flash file, users are much less likely to be aware of an infection. Infections attributed to malvertising and drive-by exploits expose the user to more invasive malware without specific action required.

Using unknown malware in an attack increases the likelihood of success for cybercriminals. With unknown malware hackers work smarter, with fewer attempts yielding greater success. Creating unknown malware is easier than ever. With antivirus systems' blocking based on known signatures, even a slight modification to existing malware creates a new unknown variant.

With nearly 12 million new malware variants being discovered every month, more new malware has been discovered in the past two years than in the previous 29 years combined.[6]

THE STATE OF PROTECTION

While the rates of attack and infection in 2015 are not growing at the same exponential rate as from 2013 to 2014, growth remains steady. While infection rates decreased slightly due to better protection resources and education, the continued erosion of the network edge and increase in number of devices accessing internal networks continues to complicate protection.

In today's borderless landscape of cloud, mobile, IoT, and hybrid data centers, cybersecurity tools must provide granular control over all network segments and environments. Though shifting from an option to a necessity, traditional sandbox techniques all impose processing delays. For protections against today's attacks, the emphasis is on speed and prevention. Newer techniques analyze behavior at the OS and CPU level, using behavioral analysis to prevent malware at the exploit phase before it has an opportunity to deploy.

Defending against the large volume and combination of known, unknown, and zero-day attacks drives the necessity of a multi-layer approach to protecting enterprises. While no one technology or technique can hope to provide complete protection from all threat vectors, a well-designed approach combining multiple methods of protection and detection can minimize successful attacks. With additional protections at the post-infection stage, organizations can limit damage and lateral movement.

4X MORE MALWARE DOWNLOADS IN 2015

TAKE ACTION

RECOMMENDATIONS

As IT quickly evolves, the threat landscape changes with it. Keeping ahead of change requires multi-level security architecture that delivers real-time threat prevention and unified management that spans virtual, cloud and mobile environments.

PREVENTION

1 DEPLOY MULTILAYER CYBERSECURITY

Security should be implemented in multiple layers that automatically coordinate among different protections including: Advanced Threat Prevention, Security Gateway, Application Control, Anti-Bot, Antivirus, Identity Awareness, Anti-Spam and Email Security, Intrusion Prevention System, and URL Filtering.

2 PREVENT ZERO-DAY MALWARE

Unknown attacks render traditional sandboxes ineffective. Real-time threat prevention that stops malware on first contact is the new standard for threat prevention. However, even the best sandbox could miss a threat embedded in a document. Stripping active content out of documents prevents hidden threats and gives users timely access to safe content.

3 USE VIRTUAL PATCHING

Patching software is a necessary best practice, but is also insufficient to prevent threats. First, there are no patches for zero-day software vulnerabilities that have yet to be discovered by security researchers. Then, for discovered vulnerabilities, it can take considerable time for software providers to create and distribute patches, leaving networks open to attacks. Lastly, lean IT staffing can also extend the time before patches are deployed.

Virtual patching using an IPS protects against exploits that prey on zero-day and discovered vulnerabilities that cannot be patched or have not yet been patched.

ARCHITECTURE

1 SIMPLIFY SECURITY MANAGEMENT

Switching among consoles to manage security for each network segment is inefficient, promoting configuration errors and inconsistencies among security layers. Managing all security functions, segments and environments through one console helps reduce errors while coordinating policies for protection layers across network segments.

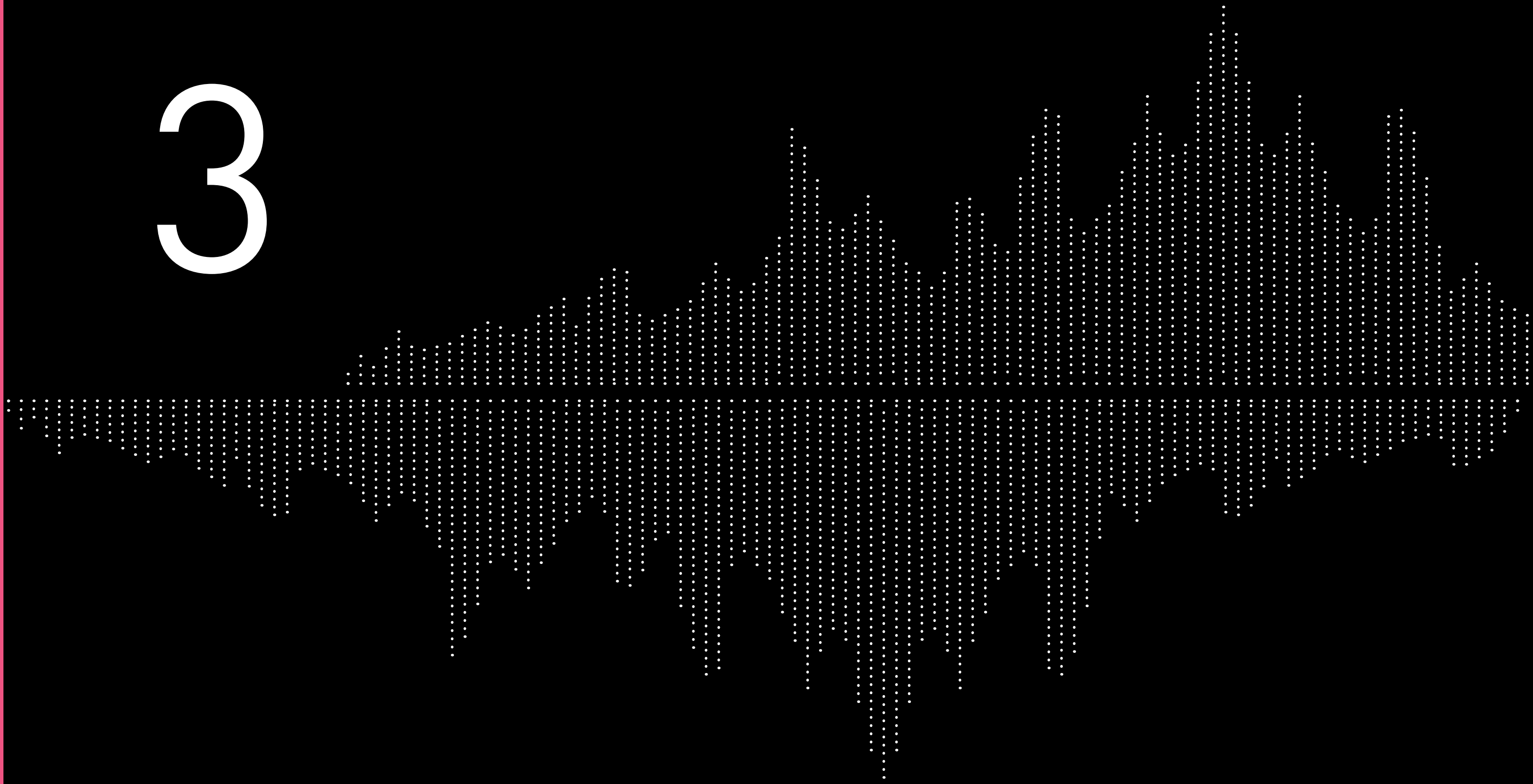
2 UNIFY CONTROLS

Implement unified controls that extend across all networks, systems, endpoints and environments including traditional, cloud, virtual, mobile, IoT, and hybrids.

LEARN MORE

checkpoint.com/sandblast

3

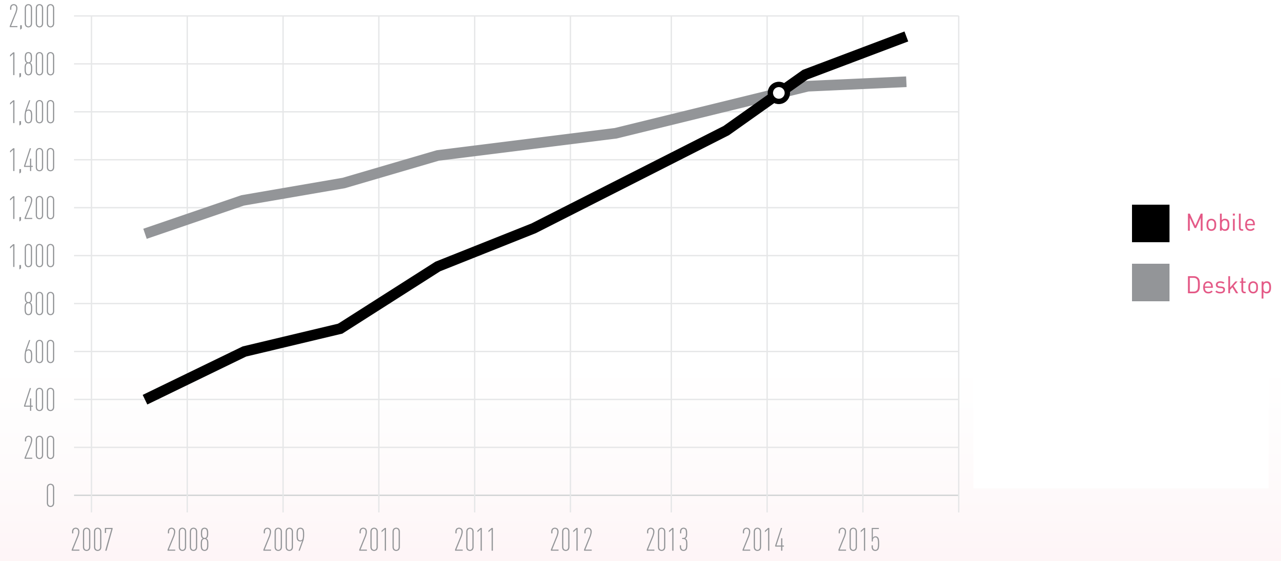


ONE DEVICE FOR PERSONAL AND BUSINESS

"I get mail; therefore I am."

Scott Adams, cartoonist, creator of *Dilbert*

NUMBER OF GLOBAL USERS (MILLIONS)



3.1 SOURCE: The U.S. Mobile App Report, comScore Whitepaper, August 2014

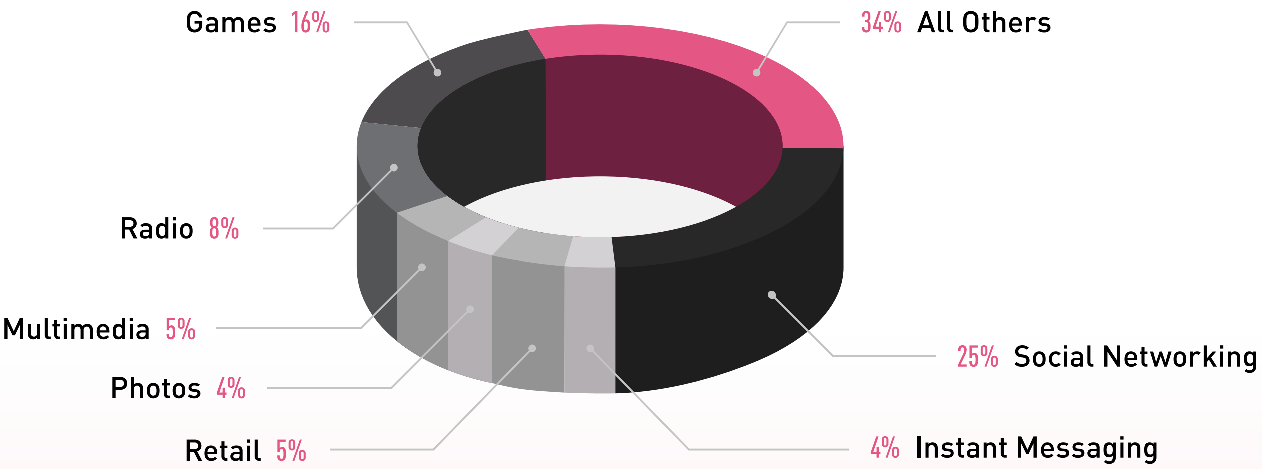
More powerful than ever, mobile devices continuously improve workers' accessibility and productivity. Increasingly affordable, most employees carry mobile devices throughout their work day whether they are using them for work or not. With such pervasiveness, mobile devices are integrating into the core fabric of businesses in ways we see and ways we may not.

As the number of mobile users increases, a tipping point in usage patterns emerges, as seen in a set of 2014 surveys by comScore. First, mobile overtook desktop for media and website access.[1] Along with this, users became comfortable blurring the lines between their work and personal usage on those devices. Whether sponsored by the company or not, employees conduct work on their personal devices, and access personal information on their work devices—not always thinking about the implications.

ALL IT TAKES IS ONE INFECTION ON A DEVICE TO IMPACT BOTH PERSONAL AND CORPORATE DATA AND NETWORKS

Smartphone usage is up 394% and tablet usage is up more than 1700% in the past four years. Together, these platforms account for 60% of digital media time spent.[2] A third study conducted by comScore and Yahoo Flurry Analytics shows that, on average, Americans spend 162 minutes per day using mobile devices for any variety of activities.[3] Together, these three trends highlight a growing desire for instant and continuous access to data, whether on a company or personally owned device.

SHARE OF MOBILE APP TIME SPENT



3.2 SOURCE: U.S. Mobile App Report, comScore, August 2014

WHERE SECURITY FITS

Like websites in the 1990s and remote access for laptops a decade later, mobile devices present both an access curse and a business productivity blessing. Similar to the access trends before them, mobile security lags behind mobile adoption as users discover new ways of engaging while on the go.

Mobile security is a difficult topic for enterprises. It remains a push-pull argument between productivity, protection, and privacy. Enterprises and users want both the increased productivity of mobile devices and protection while accessing company information, but no one likes the idea of unilateral restrictions, nor the thought that they are being watched.

Users expect access everywhere and the ability to use personal devices for work purposes. It is their employer's responsibility to figure out how to secure its own data—but not if that means enabling any monitoring rights over their online activities. The enterprise, on the other hand, must protect company data with the extra burden of adhering to different personal information privacy compliance regulations around the world. Mandatory personal identification requirements in one country could

ONE IN FIVE EMPLOYEES WILL BE THE CAUSE OF A COMPANY NETWORK BREACH THROUGH EITHER MALWARE OR MALICIOUS WI-FI

violate privacy laws in another, and the company must comply with both.

Malware, phishing, baited Wi-Fi access points, and other online dangers are worrisome for everyone. Employees do not want to be the cause of a company network breach. Yet one in five will in fact do so through either malware or malicious Wi-Fi.[4]

Mobile security must include several building blocks that address all the different aspects of the security challenge:

Secure Containers—preventing data leakage between business and personal applications hosted on the same device

Mobile Threat Prevention—protecting against malicious app behaviors and preventing known, unknown, and zero-day threats against iOS and Android devices in real time.

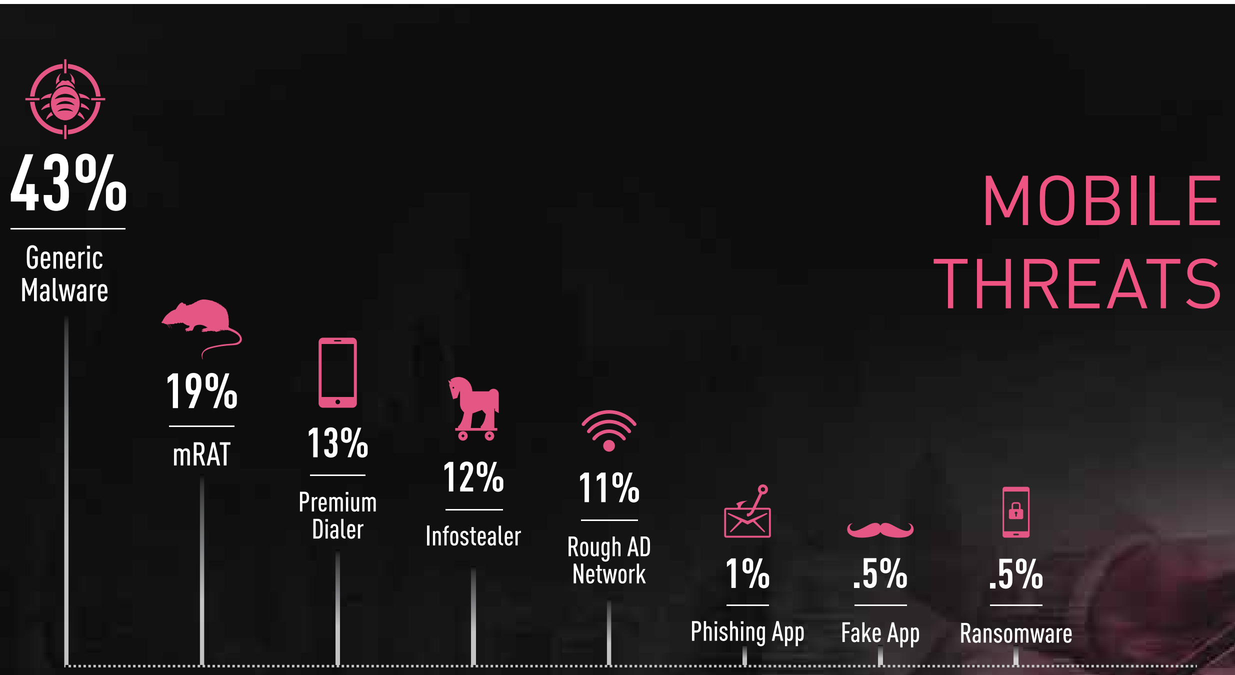
None of these on their own is sufficient, and of course IT groups do not need one more system to manage. Integrating all four into a single security console is a priority.

MOBILE ATTACK TRENDS

After analyzing the trends of 2015, we have a new perspective on the entry points of attack as well as the types of information stolen. The three main attack vectors used to target mobile devices are infected apps, network attacks, and operating system (OS) exploits. Once inside a mobile device, cybercriminals exfiltrate information through email, account login credentials, and access sensors like the microphone or camera, as well as tracking device location.

Between September 2014 and February 2015, Apple iOS was a more frequent target of cybercriminals with five different operating system attacks between XSSer, WireLurker, Masque, Pawn Storm, and Commercial mRATs. By the fall of 2015, the number of attacks increased nearly fivefold across both Apple iOS and Android.

MOBILE THREATS



3.3 SOURCE: Check Point Software Technologies

Mobility: Five New Trends in Android Malware

Android's domination of mobile computing has ushered in a new era of malware. Malware targeting Android devices has grown in sophistication in a few short years. Here are some of the latest Android threats Check Point's mobile security researchers have uncovered.

1. Obfuscation. As security vendors combat Android malware, cybercriminals evolve new ways to hide or "obfuscate" malware. By encrypting malware's malicious components, cybercriminals can bypass many security solutions including Google's Bouncer, which guards the Google Play app store. Some malware writers are even obfuscating the keys they use to uncover the malicious components, making malware even harder to detect.

2. Droppers. Malware writers are using "droppers" to infiltrate Google Play with malicious apps. Dropper schemes begin by uploading a seemingly benign app to Google Play. Google approves the app since it doesn't contain malicious code. After a user installs the app on a device, the app calls the attacker's server, downloading the malicious component to the user's device.

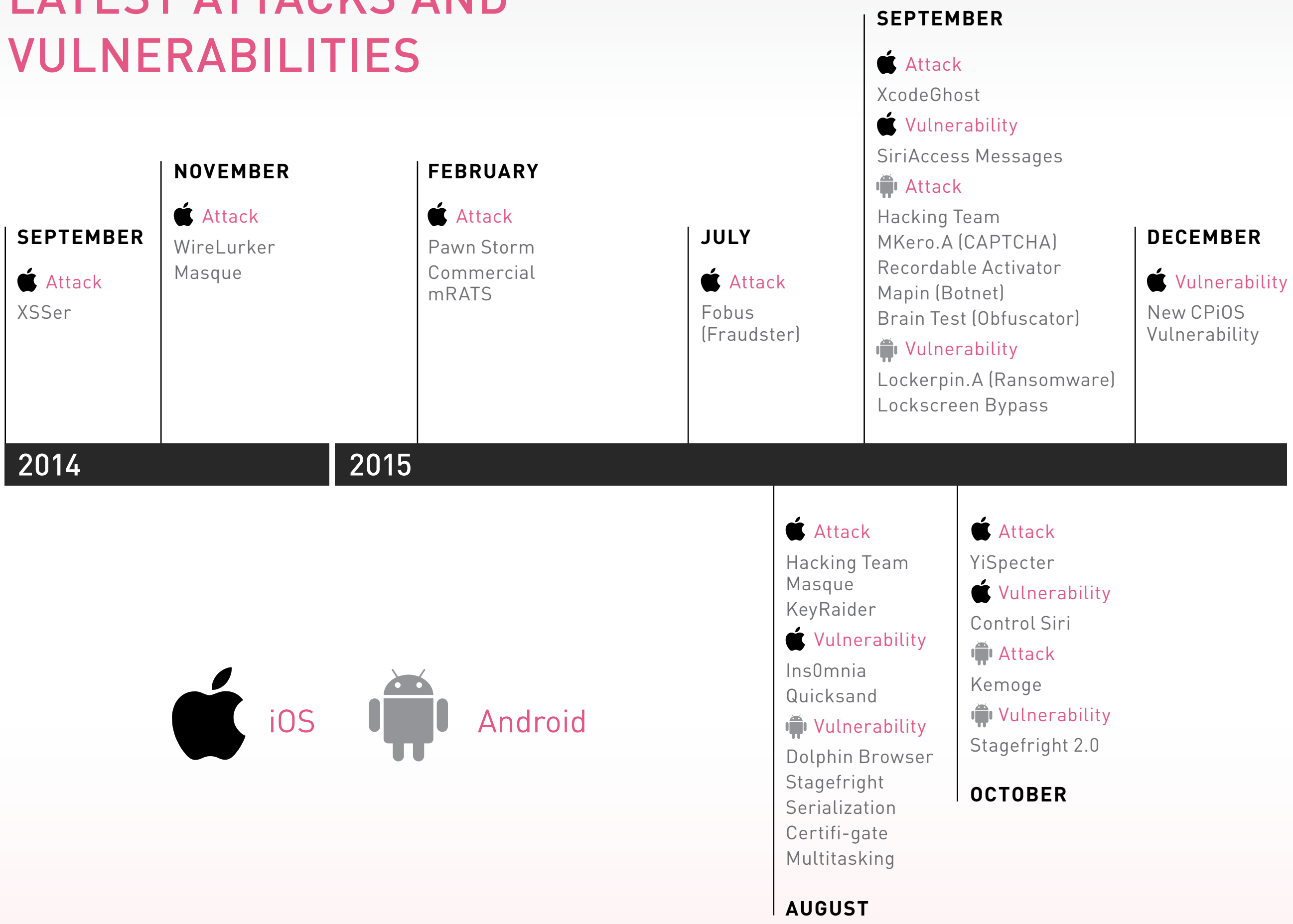
3. Redundancy. Often, malware has several components, each designed for a different malicious purpose. Two components can be designed to achieve the same objective from different directions. That way, if one malware component is detected and remediated, the attack can continue through the second component. Even if a critical component is disabled, it is easier for the attacker to change that portion than change the whole malware.

4. Persistency. Malware writers use several tactics to ensure their malware remains on the infected device. For example, they might hide the app's icon; delay malicious activity for weeks or months; masquerade as different apps; and gain elevated privileges to prevent users from uninstalling it. The main goal is the same: remaining on the device to complete a malicious objective.

5. Privilege Elevation. Recently, malware writers used social engineering to trick users into giving them elevated privileges. Other threat actors used exploits to gain privileged permissions. Because so many different versions of Android are in use, each with its own vulnerabilities, security patches can take months to arrive if they reach users at all. This leaves users vulnerable to known threats for long time periods. Malware writers use these delays to target users with exploit kits capable of abusing known flaws in Android devices.

Malware writers are as innovative and well-funded as they are persistent. Undoubtedly, they will continue to devise new techniques to achieve their goals. To stay one step ahead of evolving Android threats, businesses and users must use advanced solutions that prevent mobile threats.

LATEST ATTACKS AND VULNERABILITIES



2014

SEPTEMBER

🍎 Attack
XSSer

NOVEMBER

🍎 Attack
WireLurker
Masque

2015

FEBRUARY

🍎 Attack
Pawn Storm
Commercial
mRATS

JULY

🍎 Attack
Fobus
(Fraudster)

AUGUST

🍎 Attack
Hacking Team
Masque
KeyRaider
🍎 Vulnerability
InsOmnia
Quicksand
🤖 Vulnerability
Dolphin Browser
Stagefright
Serialization
Certifi-gate
Multitasking

SEPTEMBER

🍎 Attack
XcodeGhost
🍎 Vulnerability
SiriAccess Messages
🤖 Attack
Hacking Team
MKero.A (CAPTCHA)
Recordable Activator
Mapin (Botnet)
Brain Test (Obfuscator)
🤖 Vulnerability
Lockerpin.A (Ransomware)
Lockscreen Bypass

OCTOBER

🍎 Attack
YiSpecter
🍎 Vulnerability
Control Siri
🤖 Attack
Kemoge
🤖 Vulnerability
Stagefright 2.0

DECEMBER

🍎 Vulnerability
New CPiOS
Vulnerability

🍎 iOS 🤖 Android

3.4 SOURCE: Check Point Software Technologies

Overall, the five major categories of attacks and vulnerabilities challenging the mobile device space are:

1. System Vulnerabilities. Operating system variations increase attack vectors. Android is especially vulnerable, supporting over 24,000 types of smartphones and tablets. Security patches for each version can take weeks or months to develop and test, leaving users easy prey.

2. Root Access and Configuration Changes. Rooting or jailbreaking a phone not only gives enthusiasts more access—but cybercriminals as well. A series of attacks focused on bypassing policy limitations to change settings and configurations create subtle changes without users even knowing.

3. Repackaged or Fake Apps. Like phishing, fake apps look real but have unexpected features. Malicious applications that remotely control, turn on a device's microphone, camera or GPS tracking are becoming more widespread.

4. Trojans and Malware. Embedding malicious code in attachments and applications remains a large area of concern for mobile devices. Many do not have any kind of antivirus or threat prevention, and smaller screens make noticing details like inaccuracies in application graphics more difficult to spot.

5. Man-in-the-Middle Attacks. Free and public Wi-Fi hotspots are very easy to fake, making them more prevalent. Spoofing encryption security certificate credentials makes it easier to intercept, alter data in transit, or install Trojans.

Safe mobile computing requires user awareness and vigilance. While attack types vary, the enterprise target remains the same. Enterprise security teams must create a barrier between an employee's personal device and the company network. Accomplishing that requires multiple elements operating in parallel.

> *"Once you bring life into the world, you must protect it. We must protect it by changing the world."*
>
> Elie Wiesel, writer,
> political activist

CREATING A BARRIER

Mobile threat prevention creates a reliable barrier. It utilizes behavioral analysis to block threats before they enter mobile devices as well as offers visibility into attempted attacks.

At a higher level, integrating the device management and threat prevention with your next generation firewall and virtualized cloud security boosts both detection and blockage of attack attempts. Of course, all these resources require management, so integrating them into a unified management platform is essential to your mobile security barrier's effectiveness.

TAKE ACTION

BEST PRACTICES TO PROTECT YOUR MOBILE BUSINESS

1 EDUCATE YOUR WORKFORCE

We often underestimate how much privacy and security our smartphones and tablets provide. Make sure your employees understand threats like phishing scams and unsecured Wi-Fi hotspots. Falling victim to these doesn't just compromise the privacy of their personal data, it can jeopardize sensitive work information on their mobile devices too.

2 DEFINE YOUR RISK TOLERANCE

Not all businesses have the same mobile security needs, and not all employees require the same level of protection. It's also important to strike the right balance between threat defense and user experience. Consider a prescriptive approach to mobile security that can do both. Define policies based both on the roles of people who have access and the kinds of security that make sense for different types of sensitive data.

3 ENFORCE BASIC HYGIENE

A surprising number of people don't fully understand the basics of mobile security: Enable passwords or biometric locks, activate remote location and wiping capabilities, use device encryption if it's available. Ensure end users always upgrade to the latest operating system release. Taking even basic steps to keep mobile devices and data secure can make a big impact to your overall security efforts, and it keeps their personal data safe too.

4 SEPARATE WORK AND PERSONAL DATA

Creating a secure barrier between the sensitive work and personal data employees keep on their mobile devices is a great way to help ensure mistakes don't happen. Messages and files stored in secure containers can be protected and encrypted separately from the personal space on a device. And managing secure containers to manage data is faster and easier than managing devices and multiple policies.

5 INVEST FOR AN UNCERTAIN FUTURE

You can be sure that the threats you don't know about today are the ones that will catch you unprepared tomorrow. So it's important to invest in prevention technologies that are known for staying ahead of the threats. But these should also integrate with the solutions you have in place today to help them keep mobile devices safer while extending your return on investment.

LEARN MORE

checkpoint.com/mobilesecurity

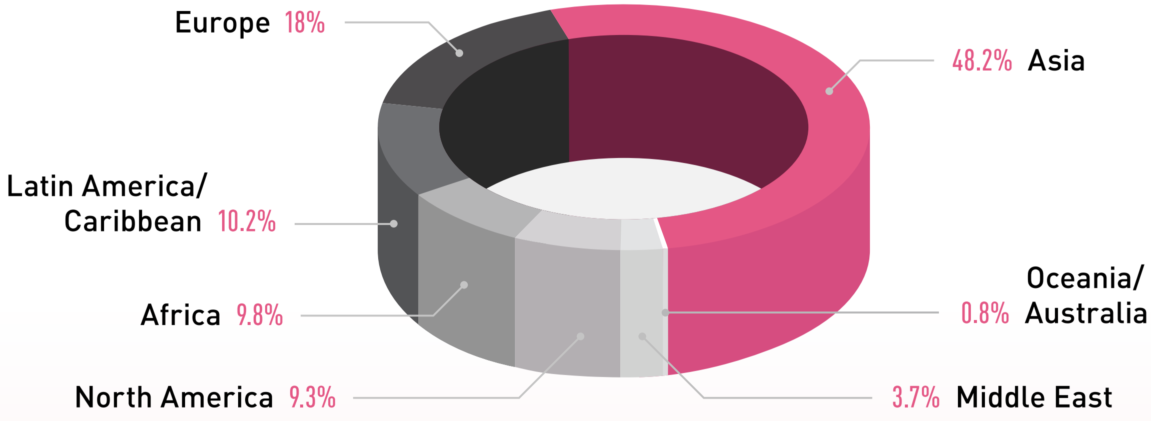
4

STUDYING ATTACK PATTERNS

"All technologies should be assumed guilty until proven innocent."

Jerry Mander, activist and author

INTERNET USERS IN THE WORLD BY REGION



4.1 SOURCE: Internet World Stats, www.internetworldstats.com/stats.htm, November 2015

Staying one step ahead of attackers requires understanding the methods they use, the pathways they follow, and where they have been successful. Studying attack patterns and trends tells a critical part of that story.

In 2015, ransomware emerged as a headline-grabbing attack methodology, as both businesses and individuals were willing to pay to regain access to files encrypted and locked by malware. Either the lack of a recent backup, or the time required to restore from backup led many organizations to opt to pay for the decryption key to their own content, while focusing on preventing the next attack. As quickly as solutions are found to combat one type of attack, new alternate techniques emerge in their place or the attack vectors shift to other methods.

Analysis uncovers distinct patterns in these emerging threats. For instance, while almost 50% of the world's Internet users are in Asia, they represent the smallest percentage of malicious behavior.[1] Meanwhile, the United States, representing less than 10% of the world's users, is home to 26% of the organizations hosting malicious content.

While it may seem as if attackers are constantly introducing new attacks, analysis shows that most often malware and attack techniques take advantage of prior attacks and known weaknesses. Leveraging known malware to create new unknown variants is relatively inexpensive and simple for even novice hackers. Exploit Kits (EKs) have evolved from just a packaging of hacking tool sets into Crimeware as a Service (CaaS) offerings. In these CaaS offerings, operators pay per use only when malware has been successfully installed on a victim machine. Hackers have an abundance of choices with

Ransomware: Steal Smarter, Not Harder

Like legitimate businesses, threat actors must occasionally retool when a "product" loses traction. Analyzing this year's intelligence data, Check Point caught criminals in the act of ramping up ransomware attacks while scaling back banking Trojans. There are several reasons we believe ransomware, which attacks by encrypting a user's files and demanding payment to decrypt them, is becoming the attack of choice for those who wish to "steal smarter, not harder."

Stealing Harder: Banking Malware

Raiding online bank accounts used to be as easy as 1, 2, 3: drive users to a deceptive mirror copy of a bank website, capture users' login credentials, and then log onto the real websites to transfer funds to a mule account. Now, attackers must contend with 2-factor authentication and connect to the bank's website from users' recognized desktops and devices.

Additionally, funds transfers can trigger fraud systems that block transfers and freeze accounts. Threat actors must also customize content to spoof each target bank's website.

Stealing Smarter: Ransomware

Ransomware can attack any user, not just banking customers, which vastly increases the pool of potential targets compared to banking malware. Ransomware makes victims pay quickly or lose access to vital content without the need for the user to sign in to capture login credentials. After encrypting the victim's data, a ransom note tells users how they can pay, or where to find their "owner" in the TOR anonymized underground. Recent data shows some ransomware arriving with a pre-held key so it doesn't even have to communicate with an external server to obtain encryption keys before initiating the attack. Without the need for multiple mirror sites, one ransomware approach works for all users. The only localization needed is for short ransom notes or attackers can direct victims to Google Translate to skip localizing content entirely.

For sure access to funds, ransomware payoffs typically use alternate payment methods like Bitcoin, enabling liquid funds transfers that users can't dispute and banks can't cancel. Bitcoin wallet shuffling prevents authorities from tracing transactions. In addition, it is easy to anonymously convert bitcoins to any currency.

Summary

Four factors are increasing ransomware attacks:

1. Ransomware targets many more potential victims.
2. Attacks have low overhead, as there is no need to host and maintain spoofed, customized mirror sites for each targeted base.
3. Attacks are simple to perform end-to-end.
4. Payments from victims are more certain to be received and untraceable.

Predictions

- With high returns and low overhead, we expect ransomware attacks will increase.
- As with banking malware, we expect advanced security will force ransomware to grow more complex and evasive.
- As fewer users fall victim to ransomware, threats will target larger organizations to increase revenue from each attack. We expect more cases like the Samsam APT attacks on hospitals and enterprises.
- Attacks will move laterally within organizations or to shared storage where data will be encrypted. This will increase payment amounts by involving multiple users.
- For the public sector, we predict the emergence of new forms of ransomware attacks such as blackmail involving threats to disclose embarrassing information which users will pay to prevent from being publicly exposed.

successful track records, leveraging known and unknown malware, and readily exploitable entry points in Android and Microsoft Windows.

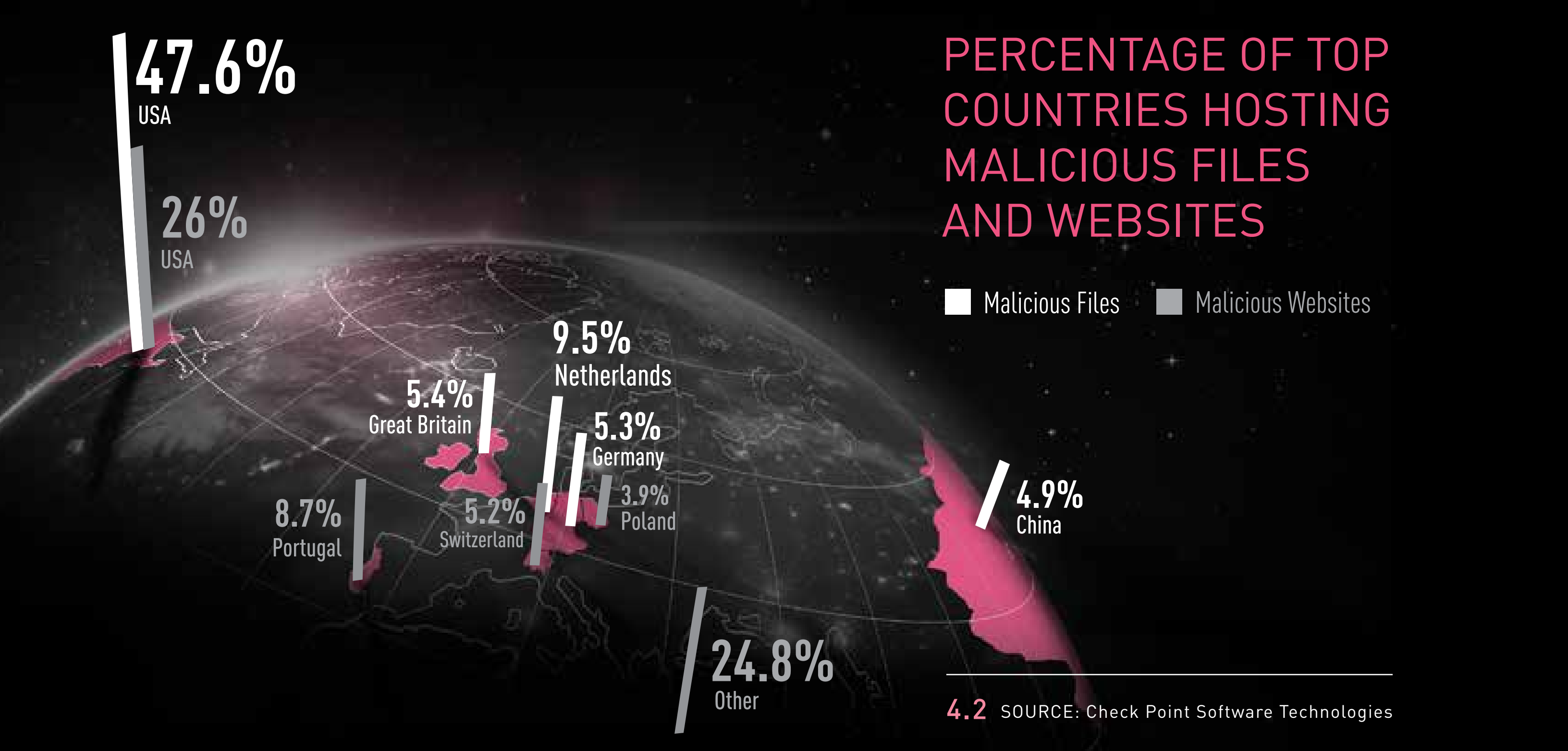
Staying one step ahead, our research team analyzes a wide range of these attack aspects and continuously improves defenses against unknown and zero-day threats. Some elements include:

- Where attacks originate
- Most popular types of attacks
- The biggest areas of vulnerability
- How the attacker gets in

This data, both individually and in combination, helps Check Point adjust and fine-tune our threat intelligence feeds. Understanding the trends in attack sources, destinations, and key methods shapes the best approaches for more impactful defense.

WHERE ATTACKS ORIGINATE

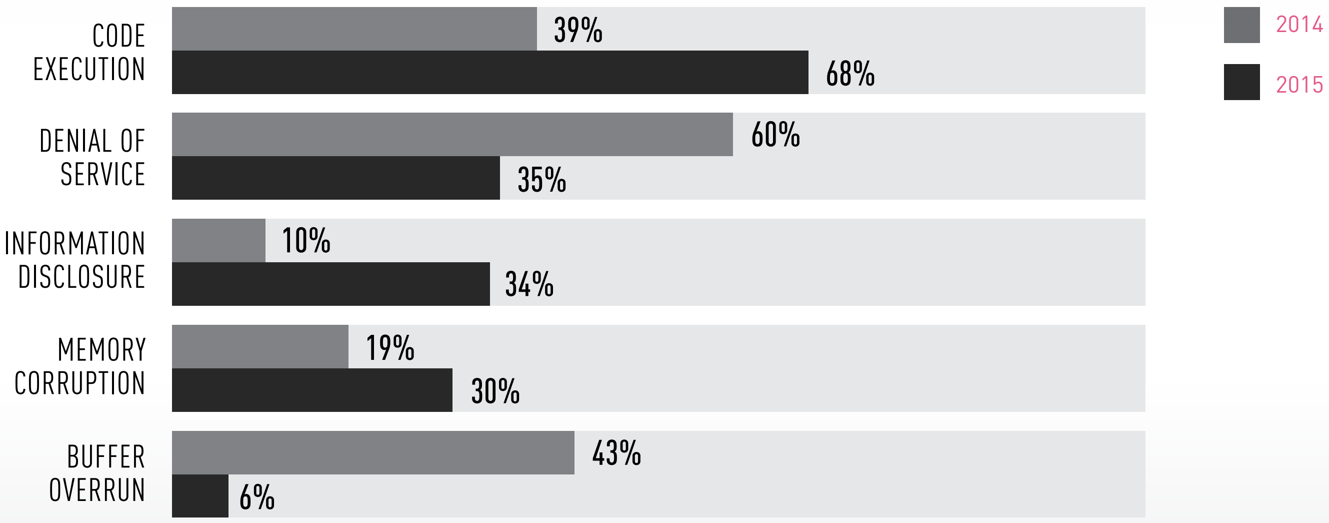
Of the 7.4 billion people on the planet, less than 5% live in the United States. Despite this, the U.S. leads the world in hosting malicious files and malicious websites. While this seems disproportionate, the U.S. hosts double the percentage of Internet users than the rest of the world, averaging 87.9% vs. the rest of the world averaging 44.2%.[2] The U.S. is also home to many of the world's pioneering Internet brands, making it an attractive target. A tech-savvy population creates more innovation—both useful and malicious.



PERCENTAGE OF TOP COUNTRIES HOSTING MALICIOUS FILES AND WEBSITES

4.2 SOURCE: Check Point Software Technologies

PERCENTAGE OF IPS TOP ATTACK VECTORS



4.3 SOURCE: Check Point Software Technologies

MOST POPULAR TYPES OF ATTACKS

Our Check Point Security gateways report the favored methods of attacks, or top attack vectors, of each year. In 2014, the three largest attack vectors were Denial of Service (DoS), buffer overrun, and code execution. In 2015, buffer overrun exploits suddenly dropped dramatically and code execution became the most popular vector.

The Heartbleed Bug made buffer overrun the big attack story and dominant attack method of 2014, with its name deriving from exploiting a buffer overread flaw in the heartbeat function of Transport Layer Security (TLS) protocol.

With this bug, attackers used vulnerable servers to repeatedly scrape up to 64 KB of sensitive information at a time from the computer's memory. Even more frightening, this was all done without a trace. For more information on this topic, check our Heartbleed blog on www.checkpoint.com.

As patches for this vulnerability became available, organizations implemented them and were protected, forcing attackers to shift to different attack vectors. Even years after Heartbleed patches were made available, though, the exploit[3] is still viable as not all organizations have installed the patches.

In 2015, attack patterns shifted—nearly 68% of organizations experienced at least one code execution attack. These attacks focus on having a system to execute code remotely.

Code executions can be launched even in the presence of security defenses, making them very attractive. One of the more popular code execution techniques is Return-Oriented

36 CODE EXECUTION ATTACKS HAPPENED EVERY DAY IN 2015

Programming (ROP). When opening an infected document, ROP hijacks small pieces of legitimate code, and redirects the CPU to load and execute the actual malware. Appearing legitimate to most security systems, detecting this manipulation at the CPU level is essential to stopping attacks before they even happen.

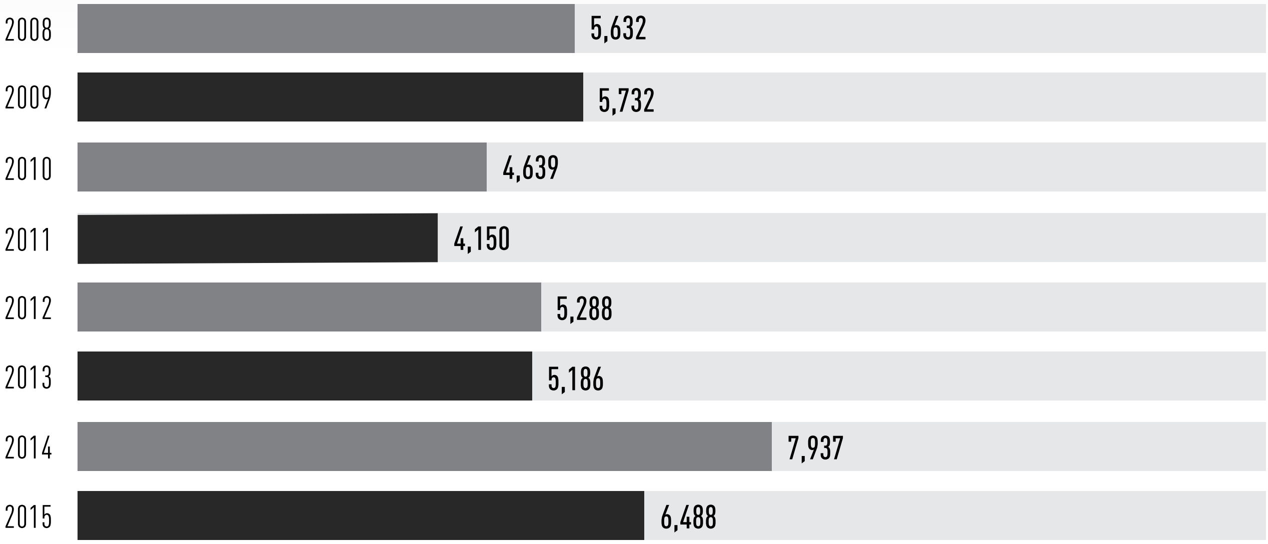
Denial of Service continues as an attractive means to attack and disrupt, with 35.1% of organizations being victims of at least one DDoS attack. In 2015, DDoS attacks rose to 73 events daily, up from the already staggering 48 events per day in 2014.

EVERY 20 MINUTES: A NEW DDOS ATTACK OCCURRED

THE BIGGEST AREAS OF VULNERABILITY

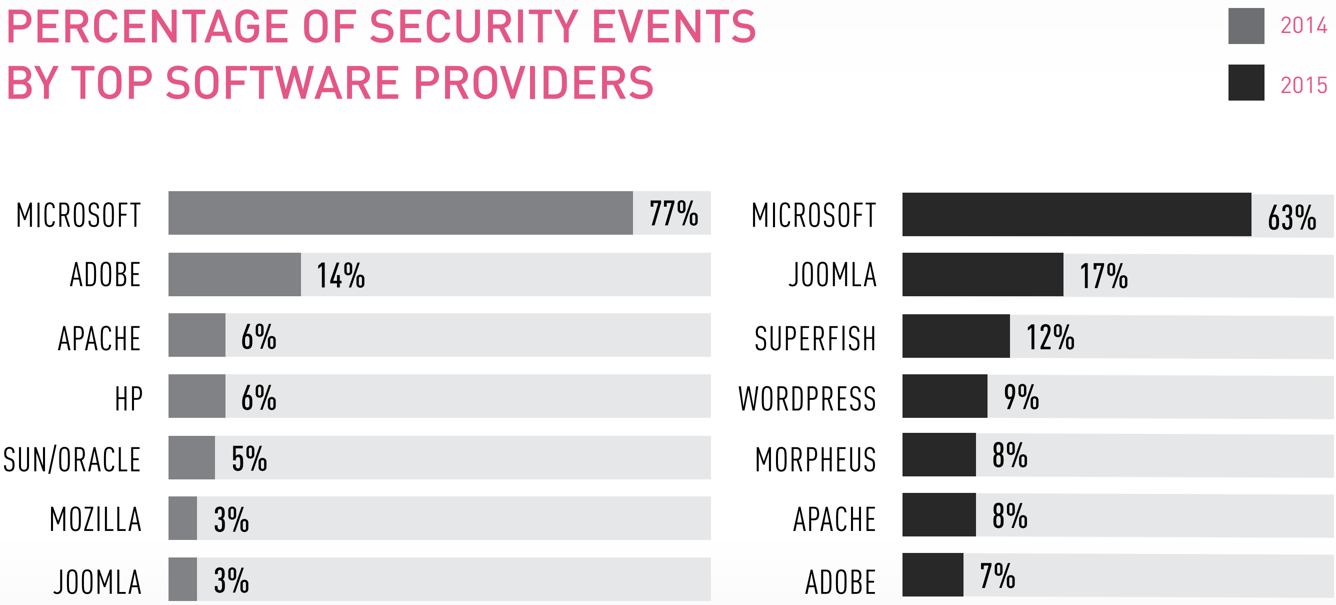
Vulnerabilities exist in most of the software we rely on across the enterprise. One of the largest repositories of organizations reporting known vulnerabilities, the Common Vulnerabilities and Exposures (CVE) database, reveals 2015's overall vulnerabilities were 15% higher on average when assessed over the past eight years. Malware that exploits known vulnerabilities remains a significant threat, making continuous patching and updates an essential effort across all software.

NUMBER OF COMMON VULNERABILITIES AND EXPOSURES



4.4 SOURCE: Common Vulnerabilities and Exposures Database (CVE)

PERCENTAGE OF SECURITY EVENTS BY TOP SOFTWARE PROVIDERS



4.5 SOURCE: Check Point Software Technologies

Breach entry points exist in many places. Combating known malware requires continuous application of patches and updates across an ever-widening array of hardware products. Servers, security tools, computers, wireless access points, and even network printers require regular patch updates. With so many devices and network entry points, it's easy to overlook some.

HOW HACKERS GET IN

Though down slightly from previous years, the tremendous install base of Microsoft solutions—from operating systems, to browsers, to productivity applications and more—has them continuing to lead in volume of software security events. Joomla and WordPress for web and ecommerce rose through the ranks this year. Open source and very common, content management system (CMS) applications like these are extremely attractive to cybercriminals as a means of spreading malware.

Jumping onto the scene and into a top spot in 2015 was SuperFish. This adware, discovered on many Lenovo PCs, went far beyond the simple intercept of web searches. Extending its reach to include encrypted searching, SuperFish installed a non-unique trusted root certification authority (CA) allowing itself, and savvy attackers, to spoof HTTPS traffic. This allowed attackers to perform a classic man-in-the-middle spoofing attack without alerting the browser. SuperFish became a popular attack vector, resulting in a warning from the U.S. government in February 2015 to Lenovo users[4] and Lenovo has discontinued its use in new PC shipments.

After two decades, phishing scams that convince users to give away sensitive information, such as credit-card numbers and banking login credentials, remain a popular source of revenue for cybercriminals. Since users have become more aware of the risks, and detection of spam and phishing traffic has improved, criminals have turned to several techniques for increasing their phishing success rates. However, these new approaches take more time and effort and yield relatively modest returns for each crime. To maximize their "take," we are seeing criminals retargeting phishing schemes from mass attacks on random users to highly focused attacks on high-value employees at enterprises.

Phishing: Baiting Bigger Hooks to Catch Enterprises

Phishing's Evolution

Spear phishing is the name given to highly-targeted attacks that use deception and social engineering to steal credentials and other valuable information from specific groups of users, a specific company, or even specific individuals. To conduct a successful spear phishing attack, the perpetrator invests much more time and effort performing reconnaissance to gather detailed information about the intended targets. For example, an attacker might conduct research into vendors used by the company, service providers such as accounting firms, or the company's business partners. The attacker then identifies specific individuals and their email addresses, sending them spoofed emails appearing to be legitimate in nearly every respect. The emails either encourage the user to open an attachment or send the recipient to a high-quality counterfeit website. The net effect of the increased social engineering is a much higher success rate. In addition, businesses typically have much deeper pockets than the average user, so the typical "take" from each spear-phishing scam is much higher.

Whaling

Spear phishing has further evolved into attacks referred to as "whaling." This elaborate form of spear phishing usually targets C-level executives, deriving its name from "phishing for the big fish." For example, a whaling perpetrator might send a spoofed email masquerading as a correspondence from the CEO to the CFO, requesting that the CFO transfer money to a specific bank account. With effective social-engineering research into what will sound credible to an executive, these approaches have convinced some very astute professionals to fall for the scam. By the time the truth is discovered, the money is long gone. To erase any traces, some attackers use mule accounts for only one attack. According to the FBI, over the last two-and-a-half years, whaling scams have bilked businesses out of $2.3 billion.

It is certain attackers will continue to develop innovative ways to deceive users into compromising their systems. A combination of ongoing awareness training and advanced technology is needed to prevent users from falling victim to these scams.

BEST PRACTICES

Enterprises need a unified threat prevention strategy. Known malware still remains a large threat. New techniques bring significant growth in unknown and zero-day malware, requiring solutions that can prevent known and unknown threats in real time including even the most evasive threats. Monitoring outgoing communications is also important to spot anomalous behavior before damages occur.

1 UNIFIED ARCHITECTURE

Protect your network from advanced malware and zero-day threats. Extend these protections to fixed and mobile endpoints, cloud services, and virtual environments to prevent threats across the organization.

2 PROTECT ALL ENVIRONMENTS

Use environment-agnostic security architecture to uniformly prevent threats against data centers, cloud platforms, software defined data centers, SaaS, hybrid, and mobile environments.

3 PREVENT ZERO-DAY MALWARE AND EXPLOITATION

Increases in code execution attacks, including advanced techniques such as Return-Oriented Programming (ROP), bypass traditional sandboxes. CPU-level Threat Emulation picks up malware at the exploit phase before hackers apply evasion techniques to bypass the sandbox.

4 MANAGE ALL SECURITY THROUGH A SINGLE PANE OF GLASS

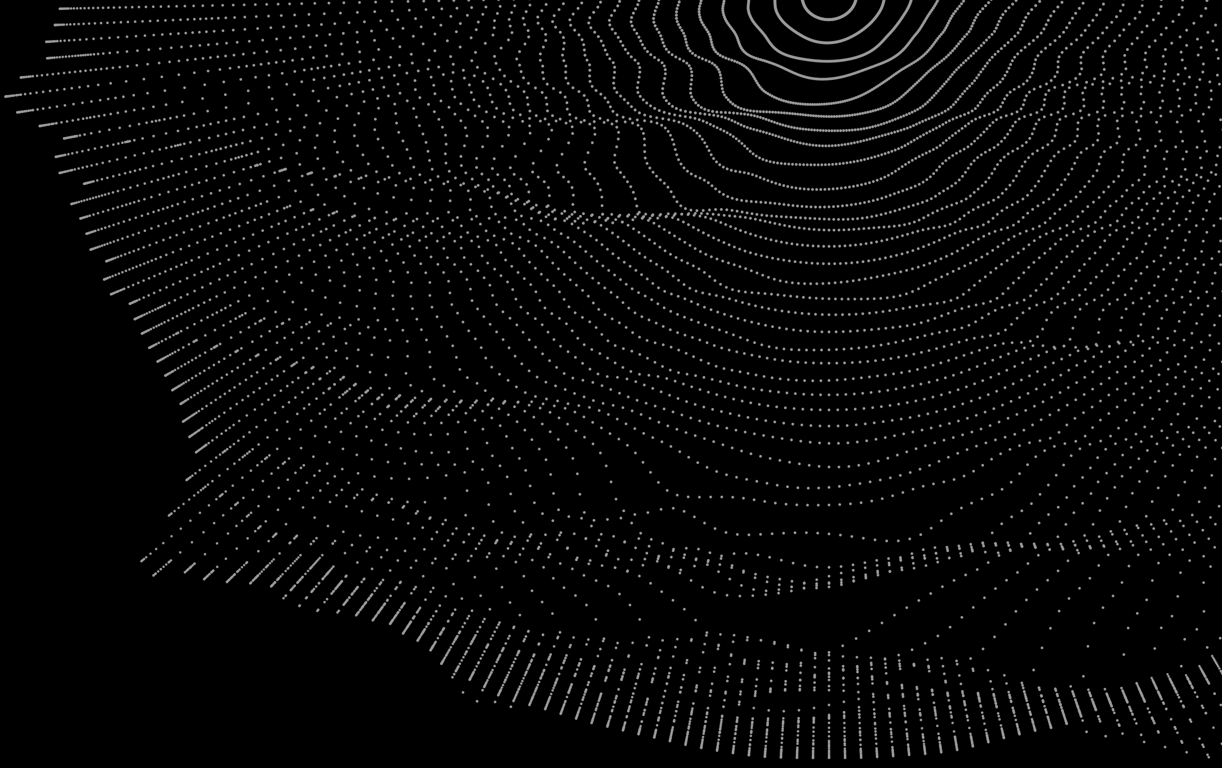
Unified security management improves the accuracy of security settings and visibility when monitoring logs.

5 HAVE A GAME PLAN FOR INCIDENT RESPONSE

Until you have unified real-time prevention, you need incident response. The Check Point Incident Response Team is available 24x7x365 to investigate and resolve malware attacks and other security events impacting your organization. Call 866-923-0907 or email emergency-response@checkpoint.com.

LEARN MORE

checkpoint.com/management



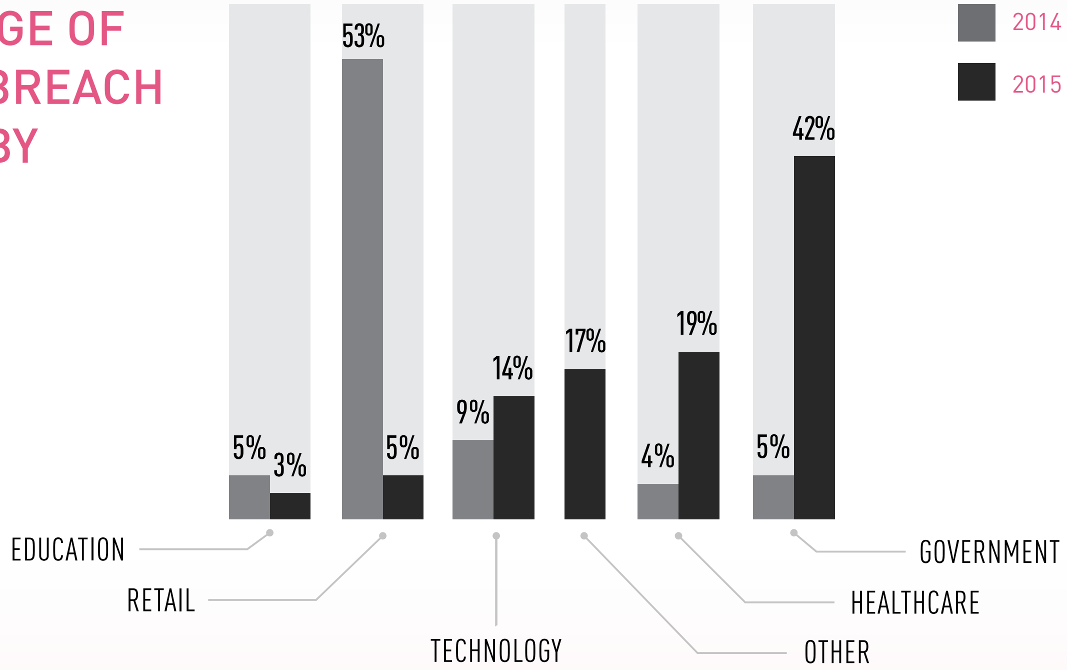
5

THE RIPPLE EFFECTS OF INSECURITY

“Everything we do, even the slightest thing we do, can have a ripple effect and repercussions that emanate. If you throw a pebble into the water on one side of the ocean, it can create a tidal wave on the other side.”

Victor Webster, actor

PERCENTAGE OF TOP DATA BREACH RECORDS BY INDUSTRY



5.1 SOURCE: Gemalto's Breach Level Index

The impact of cybercrime costs more than the value of the stolen information. The ripple effects are often more damaging than the actual theft. The loss of confidence—both from your company and your customers—make you overspend on remedies, feel obligated to pay impacted suppliers and partners, and at least for some amount of time, cause your customers to flee.

If someone broke into your home, you would feel violated. Your insurance company would reimburse you for the value of any items stolen, but the feeling of being safe cannot be replaced so easily. You would be cautious afterwards, perhaps over-investing in security system upgrades, or begin storing valuables off-site, or even going out less, all to feel safer. You would invest in changing your habits to not just be more secure, but to feel more secure—which can be costlier. Corporate breaches are no different. Here too the ripples can be more damaging than the initial splash.

Calculating the financial value of information is complex, though today there are several ways to estimate it. In 2013 and 2014, a wave of breaches attacked big industry names such as Anthem, Target, Home Depot, and Sony, in search of personal information. With the average cost of a data breach at $154 per record according to Ponemon Research, and many incidents involving thousands, or even millions of records, the average total cost of a single data breach rose twenty-three percent to $3.79 million in 2015.[1]

In 2015, the number of breaches decreased slightly from 1 billion records in 2014 to just over 700 million in 2015, according to research firm Gemalto.[2] While this seems promising, not all records have the same value.

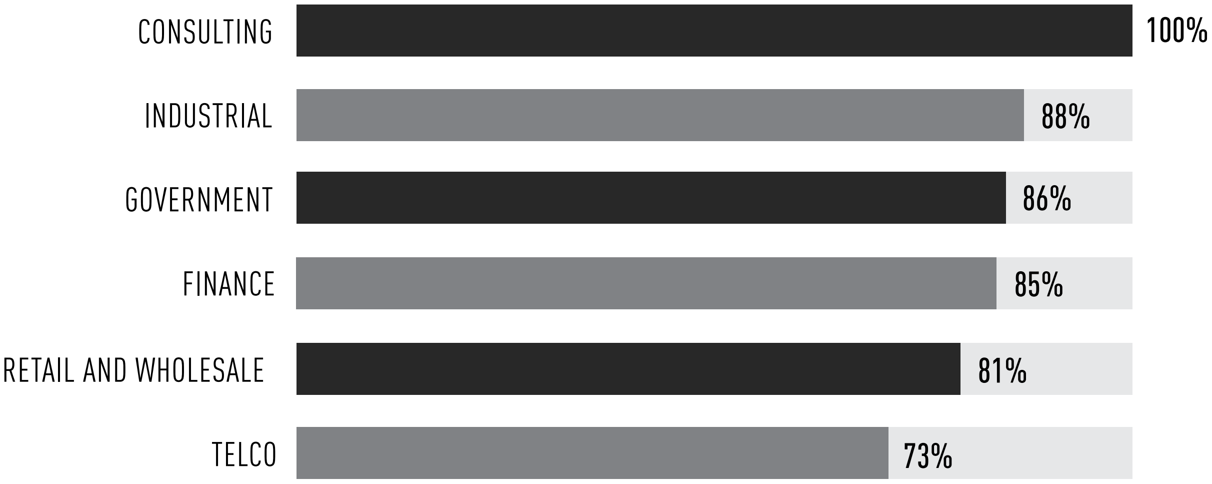
In 2014, the main target was credit card data which has a relatively short shelf life—credit card companies cancel charge accounts and reissue new cards quickly. In 2015, attackers shifted to data with a longer shelf life—personal information and identity theft. In addition, attackers went from focusing on mainly retail and financial targets in 2014 to government and healthcare targets in 2015. The longer the shelf life of a record, the more expensive the cleanup.

Calculating the initial splash costs of a breach includes several direct expenses:

- The value of stolen intellectual property
- Downtime analyzing, repairing, and refortifying all compromised systems
- Checking all company systems for additional lurking infections
- Restoring systems from backups, including checking those backups for vulnerabilities
- Changing security procedures and training personnel on new safeguards

The less obvious ripple costs, however, quickly overshadow these direct costs. In the case of the Target breach, the 40 million credit and debit cards stolen in late 2013 cost Target

PERCENTAGE OF COMPANIES WITH A DATA LOSS EVENT



5.2 SOURCE: Check Point Software Technologies

LOSS OF BUSINESS DATA RECORDS INCREASED MORE THAN 400% OVER THE PAST THREE YEARS

5.3 SOURCE: Check Point Software Technologies

$248 million in direct expenses the first two years, but that number continues to rise. Some sources estimate costs ultimately exceeding $2.2 billion when including losses from fraudulent charges, reimbursing suppliers, and penalties from class action lawsuits. Disaster recovery is expensive.

Security breaches typically steal information, and often smaller companies are easier to attack than larger ones. According to Trustwave research, 90 percent of data breaches impact small businesses, and those businesses have a much more difficult time surviving the impact. While smaller companies may not be in possession of large amounts of personal data, they often hold the access keys to those that do.

The ripple effects to company reputation are difficult to estimate, but very real. If a company has strong customer support and handles the situation carefully, customers may be shaken, but not leave. For smaller companies, however, any loss in customer confidence is devastating.

While government trust is a big issue in the aftermath of a breach, the financial impact is limited compared to a public or private business. Three private sector market segments experiencing the largest post-breach financial impacts are financial services, healthcare, and the industrial sector. As many people are in the bad habit of reusing passwords, losing a password for one site often has ripple effects. Attackers use one stolen password to access other sites and applications used by the victim resulting in multiple breaches.

FINANCIAL SERVICES

Our research shows financial institutions face much higher rates of attack than any other market sector. We are not alone in this conclusion. A report by Websense Security Labs in 2015 agrees, highlighting that financial institutions experience 300 percent more cyber-attacks than any other sector.[3] This volume of attacks exceeds all other sectors by 3:1.

Security Findings for the Financial Industry in 2015

Some of the most significant finance market pressures in 2015 included:

83% of financial service firm executives agree that the ability to combat cyber threats and protect personal data is one of the biggest issues in building reputation over the next 12 months[4]

24% increase of financial losses from incidents[5]

73% of U.S. consumers switch their financial services provider due to breach or theft of personal data[6]

61% of consumers do not trust financial institutions[7]

44% of financial services companies reported business loss of 20% or more in the last twelve months due to reputation and customer satisfaction issues; the average lost 17%—nearly double the 2014 average[8]

42% of U.S. consumers believe failing to protect personal and financial information is the biggest threat to their financial services firms' reputation[9]

68% of consumers report that negative news about their current financial services firms—regulatory issues, illegal activity, fines, etc.—will likely lead them to switch providers[10]

Financial companies make ideal targets because their data has the broadest appeal in the open market. Retail banks, commercial banks with branch offices scattered across the world, credit card processing companies, insurance companies, and trading companies all have data, and connect to others with more. Financial services did not top the list of attack targets in 2015, merely because their 2014 efforts to fortify their defenses made them a more difficult target to penetrate.

Financial cybersecurity is a profoundly complex and multifaceted ecosystem. Large financial institutions smartened up after 2014. They began investing in integrated solutions rather than point products. This further increases protection against the barrage of advanced persistent threats and zero-day attacks.

The volume of attacks and attack points requires complete visibility into operations and centralized security management, but not complete transparency. Like nations protecting their citizens, security officers at major financial institutions are cautious when exposing protection methods or discussing attack details. When cybercriminals see where attacks have an impact, and where they don't, they adapt their tactics or reprisals.

Perception of protection is as important, if not more, than the actual protection. Incidents where no account or personal data is lost shakes customer confidence. Because of this, financial institutions now share attack information through shared threat intelligence feeds. Our threat intelligence partner programs host several of these. Since most hackers use the same successful attack methods against multiple victims, it increases their costs if a hack method only works once. The more expensive hacking is, the lower the number of hackers, making everyone safer.

HEALTHCARE

Patient health records have the highest value on the black market—ten times more than credit cards or other financial data.[11] While a credit card number or bank login information can be quickly reissued, healthcare records cannot. They also expose much more information about an individual, including their sensitivities, vulnerabilities, and personal concerns, making them valuable for espionage. Healthcare companies are cybercriminals' prime targets.

9% OF HEALTHCARE/INSURANCE ORGANIZATIONS EXPERIENCED A HIPAA DATA LOSS

5.4 SOURCE: Check Point Software Technologies

In 2015 and the beginning of 2016, many healthcare organizations fell victim to a multitude of attacks, primarily ransomware. Traditionally, the healthcare industry has lagged behind more

Security Findings for the Healthcare Industry in 2015

60% increase in healthcare security incidents[12]

2% of U.S. healthcare organizations reported at least one case of medical identity theft[13]

282% jump in security breach costs in the healthcare industry over the prior 12 months[14]

89% of U.S. healthcare providers make patient data available to patients, surrogates and/or designated others[15]

11 types—the average number of technical-security tools that U.S. healthcare organizations have in place[16]

21% of U.S. healthcare organizations do not use disaster recovery (DR) technology, and 51.7% of these intend to purchase DR in the future[17]

54% of U.S. healthcare organizations do not have single sign-on (SSO) implemented, and 49.3% of them intend to purchase SSO in the future[18]

60% of U.S. healthcare organizations do not have two-factor authentication implemented[19]

19% of U.S. healthcare organizations report having a security breach in the last year[20]

Only 54% of U.S. healthcare providers' IT and IS professionals have tested their data breach response plan[21]

In U.S. healthcare, the top three perceived threat motivators were: (80%) of workers snooping on relatives/friends,
(66%) concerned with financial identity theft,
(51%) identity theft[22]

prime targets like the finance market in terms of security robustness but new regulations regarding personal information protection compliance has complicated upgrading further.

Programs like HIPAA set strict guidelines regarding the intentional or accidental release of personal information, but doing so may open up new vulnerabilities in the process. Healthcare providers of all sizes must comply with these regulations on personal information and its security. Personal information protection sometimes is prioritized over access control protections. The integration of Internet of Things (IoT) devices into healthcare environments dramatically increases this industry's attack surface, which does not scale with the size of the provider, making smaller providers prime targets. Making health care harder to protect is updating the software and OS of systems keeping people alive that can't be taken off line.

Healthcare compliance primarily focuses on internal controls rather than information protection. While compliance protections for doctors, nurses and administrators with access to data but limited knowledge of cybercrime techniques is certainly important, the focus needs to shift to IoT and access control protections.

INDUSTRIAL IoT

The Industrial Internet of Things (IIoT) continues on a significant upward trend in 2015 with important implications for the global economy. According to Oxford Economics,[23] this segment encompasses industries that contribute to 62 percent of the gross domestic product (GDP) among G20 nations, including utilities, oil and gas, agriculture, and manufacturing. Also included are organizations providing transportation, staging logistics and healthcare services for hospitals, power plants, and rail and seagoing shipping ports.

One of the biggest attractions to IIoT is the promise of operational efficiency. More automation and flexible production techniques result in productivity increases as much as 30 percent.[24] However, these devices are all connected, typically accessible and unattended, with little to no endpoint protections.

The ripple effects of IIoT breaches are difficult to measure, but mostly center around disruption. Critical infrastructure disruptions have enormous implications—one grid going off-line could impact hundreds or even thousands of businesses in ways not easily quantified.

Of all the current advancements in technology, IIoT has the potential to produce the biggest impact and cause the most disruption. For example, Google and Tesla producing autonomous cars is likely to disrupt a multitude of industries, including car manufacturing, car insurance and government licensing, and possibly over-the-air updates to software defined vehicles. Apple's HealthKit is another far-reaching IIoT example. If health sensors and health applications are suddenly accessible locally by patients, the healthcare data ecosystem now occupied by doctors, insurance organizations and pharmaceutical companies would shift to individuals.[25]

The benefits of increased efficiency will rapidly be overshadowed by the loss of those benefits in the instance of a breach.

88% OF ORGANIZATIONS SUFFERED A DATA LOSS INCIDENT

Top Ways to Secure the Industrial Internet of Things

Prevention. If malware protection can't be implemented on each device, it can reside at the point where IoT devices communicate.

Segment. IoT devices should talk to a central controller, not each other.

Protocols. Use security that supports ICS/ SCADA specific protocols.

Directional Commands. IoT systems should report out. However they shoulf receive few commands in.

TALLYING THE RIPPLE IMPACTS

Data breaches can cause short-term financial impacts but pale in comparison to the potentially long-lasting damage to an organization's market position. Brand value on average decreases 21% as a direct result of a security breach.[26] Recovering and restoring your reputation takes time and depends on how your post-breach disaster recovery is handled.

Take a holistic approach to security instead of patching together point solutions. Stress threat prevention, as opposed to threat detection and remediation.

To further reduce risk, include data loss prevention (DLP) in your security mix and use best practices when configuring security.

> *"Success does not consist in never making blunders, but in never making the same one a second time."*
>
> H. W. Shaw (Josh Billings),
> American humorist

The Check Point Incident Response Team is available to investigate and resolve complex security events that span from malware events, intrusions or denial of service attacks. The team is available 24x7x365 by contacting **emergency-response@checkpoint.com** or calling **866.923.0907**.

AS YOU THINK ABOUT YOUR CYBERSECURITY GOALS, ASK YOURSELF THESE QUESTIONS

1 UNDERSTAND THE SITUATION

How confident are we that our cybersecurity is effective against zero-day threats?

How well trained are my employees about cyberthreats and the potential consequences of their actions?

2 SEE WHAT'S COMING

Do we have clear visibility of log activity in all of our network segments or is monitoring too complex a task to be useful?

3 SECURE WORKLOADS NOT SERVERS

Do the workloads I run in virtual, cloud and software-defined environments receive the same protections as workloads run in my data center?

4 GET PREPARED

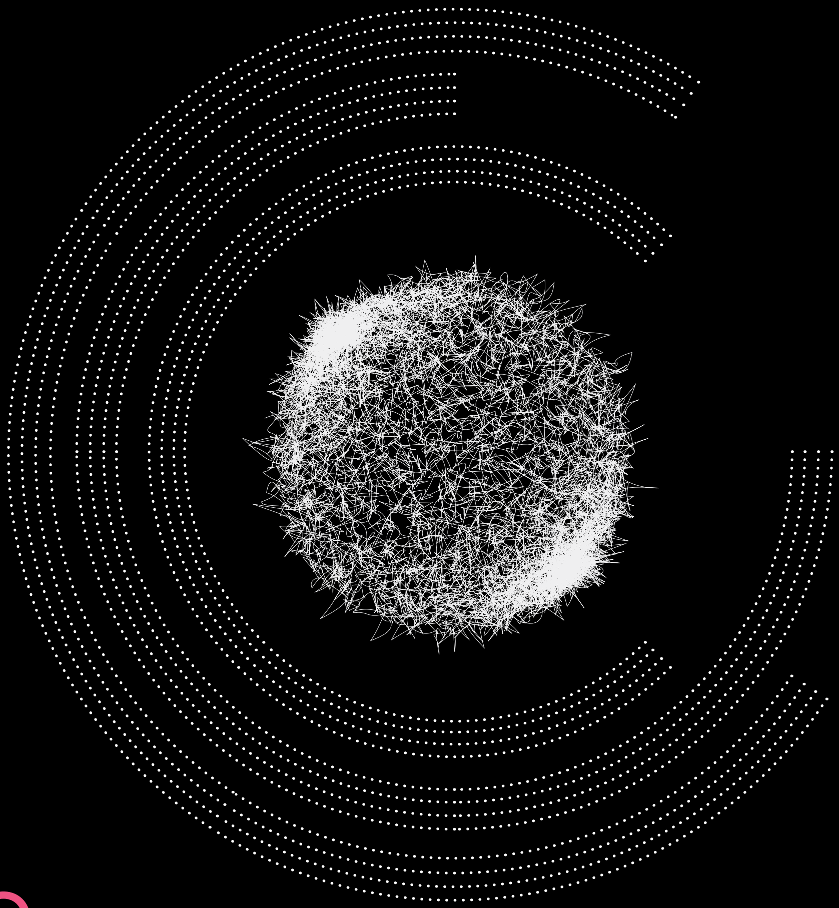
Do the company's policies protect information and resources in all environments?

How is the executive leadership informed about the current threat level and potential business impact of cyber-attacks on our company?

GET STARTED

Discover the active threats now running on your network and weak points in your security you can harden. Visit: checkpoint.com/resources/securitycheckup

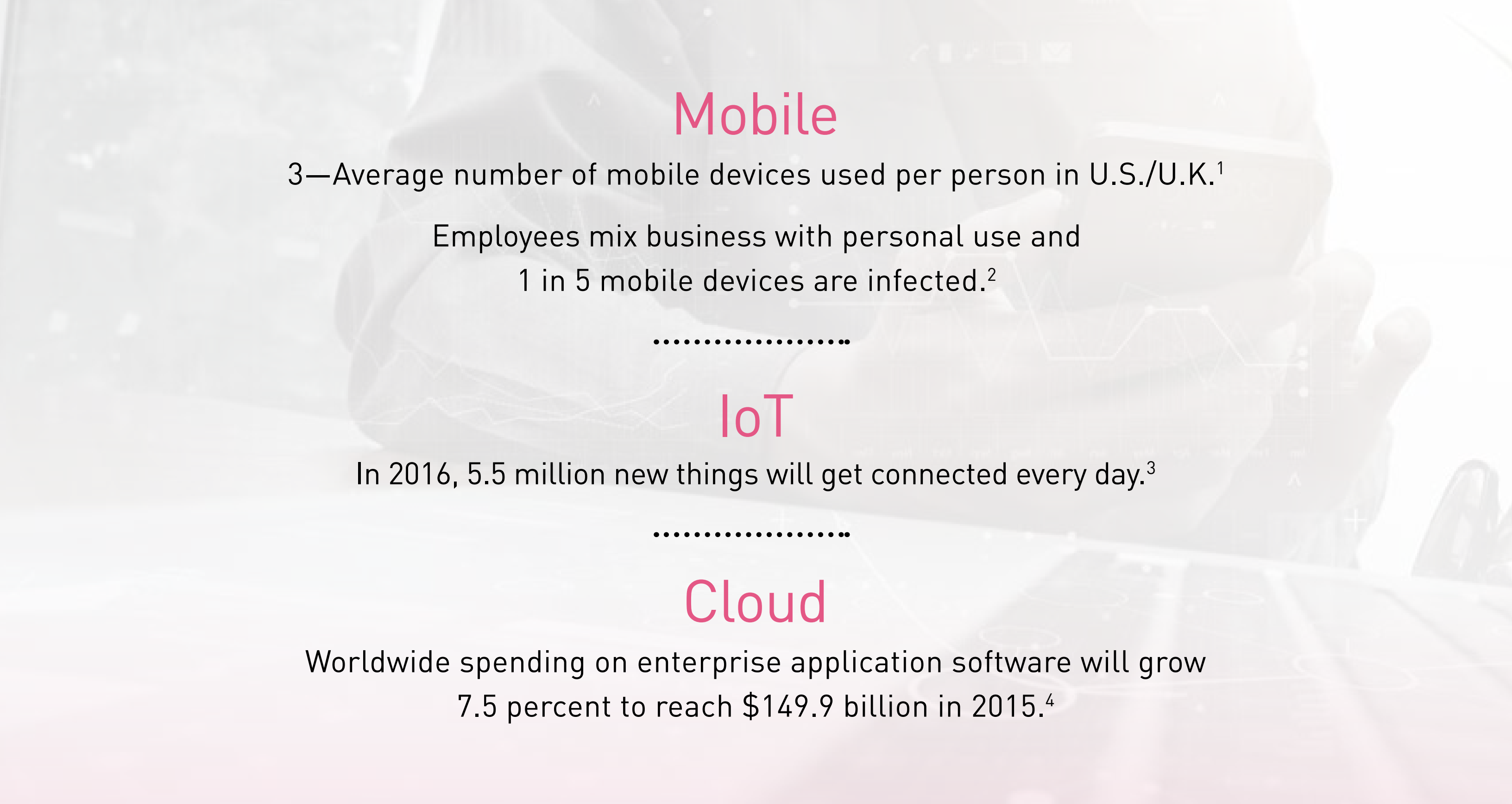
6



STAYING ONE STEP AHEAD

"Forewarned, forearmed; to be prepared is half the victory."

Miguel de Cervantes, writer



Mobile

3—Average number of mobile devices used per person in U.S./U.K.[1]

Employees mix business with personal use and 1 in 5 mobile devices are infected.[2]

IoT

In 2016, 5.5 million new things will get connected every day.[3]

Cloud

Worldwide spending on enterprise application software will grow 7.5 percent to reach $149.9 billion in 2015.[4]

To have an effective security strategy, you must understand attackers. This year's report shows that the threat environment continues to grow in complexity as malware is easier than ever to obtain and deploy. In 2005, one million new pieces of malware were launched. In 2015, that many were launched every day.[5] Malware continues to be easy to obtain and easier to launch Review successful attacks, the latest vulnerabilities, and attack trends to create the security strategy your organization needs.

Next, understand the breadth of your organization's attack surface. The enterprise boundary continues to stretch and blur, complicating security even more. Servers and corporate computers no longer define this boundary. Instead, it is pushed by record numbers of mobile devices, cloud-based applications, and a growing number of Internet of Things (IoT) devices that your IT department might not even know are connected. These tools increase productivity, but each extension of the enterprise boundary must be protected.

Mobile devices, IoT, and cloud applications provide great new freedoms, but these freedoms bring brand new security risks. For every disruptive business model there is an IT department scratching their heads thinking about how to protect it. For instance, the wireless communications of mobile devices used to scan inventory in the warehouse must not be compromised or intercepted. The IoT devices that automate medical readings, high voltage power distribution, or high-rise office building airflow must be properly secured against being disrupted by remote command. Cloud-based applications should not have unchecked open interfaces that unknowingly let hackers into your network.

Managing security for IoT as a separate entity will increase the complexity of security management. Ideally security for IoT, whether for consumer goods or industrial SCADA systems, can be instituted under a unified security architecture and managed through the same console as other network segments.

Compliance: The Best Reason for Best Practices

Did you know a group of jellyfish is called a "smack?" Although there isn't a name for groups of people who write cybersecurity regulations, like jellyfish, regulators seem to form groups. The evidence for group behavior shows up in the many common requirements regulators write into cybersecurity rules that emanate from industry organizations and the public sector. When faced with a complex web of regulations and laws, using best practices can help you leverage common requirements to simplify and improve compliance—and security.

By best practices, we mean guidelines for optimizing how to configure cybersecurity solutions. The main reason for using best practices is to eliminate human errors. According to Gartner, "Through 2020, 99% of firewall breaches will be caused by simple firewall misconfigurations, not flaws."[6] Writing for IT Governance, Lewis Morgan states, "Human error is the cause of most data breaches. It's no secret that the largest threat to an organization's data is its own employees—whether deliberate or not."[7]

Given the profound impact configuration errors can have on security and compliance, Check Point researchers were interested in learning how effectively organizations were using best practices and their impact on compliance. To find out, our researchers monitored the configurations of security controls such as firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), anti-virus, and others, and compiled metrics on compliance.

Our researchers were shocked to find only 53.3 percent of configuration settings were defined according to industry best practices. Compliance levels for different industries and regulatory standards are shown in the following table:

Compliance Levels for 4 Regulations by Industry

INDUSTRY	REGULATION	OVERALL COMPLIANCE STATUS
Healthcare	HIPAA Security	59%
General IT Security	ISO 27001	64%
Bulk Power Systems	NERC CIP	67%
Payment Cards	PCI DSS 3.1	60%

The image that has emerged from our research shows a large segment of IT professionals across a broad spectrum of industries are not optimizing their security configurations for security and compliance. To understand this in greater detail, Table 2 below shows compliance with best practices broken out for critical infrastructure companies and financial services organizations.

Compliance Levels by Configuration Standard by Industry

BEST PRACTICE	ALL INDUSTRIES	CRITICAL INFRASTRUCTURE	FINANCIAL SERVICES
Enabling Anti-Spoofing	70.0%	75.5%	65.0%
Ensuring Firewall rules are properly documented	28.0%	30.0%	30.0%
Defining the Track options for policy rules	20.0%	22.0%	30.0%
Blocking high-risk applications and websites	49.5%	54.0%	45.0%

It is interesting to see that 3 out of 10 businesses are not taking advantage of anti-spoofing technology and one out of two businesses do not restrict access to high-risk applications. Given the risks associated with these security techniques, these are explosive statistics. Another relevant finding is that three out of four firewall policies that were analyzed did not fully document the rule base.

Best Practices and Reporting

Best practices can also help you with the reporting and the continuous monitoring aspects of compliance in case you have to meet with an inquisition of auditors. PCI-DSS Rule 11,[8] HIPAA CFR 160-164,[9] FISMA,[10] FERPA 99.62,[11] FINRA Rule 4530 and many other regulations require monitoring security, and reporting security procedures. Once you have gotten ahead of configurations, citing best practices in reports is an effective way to structure content for audits.

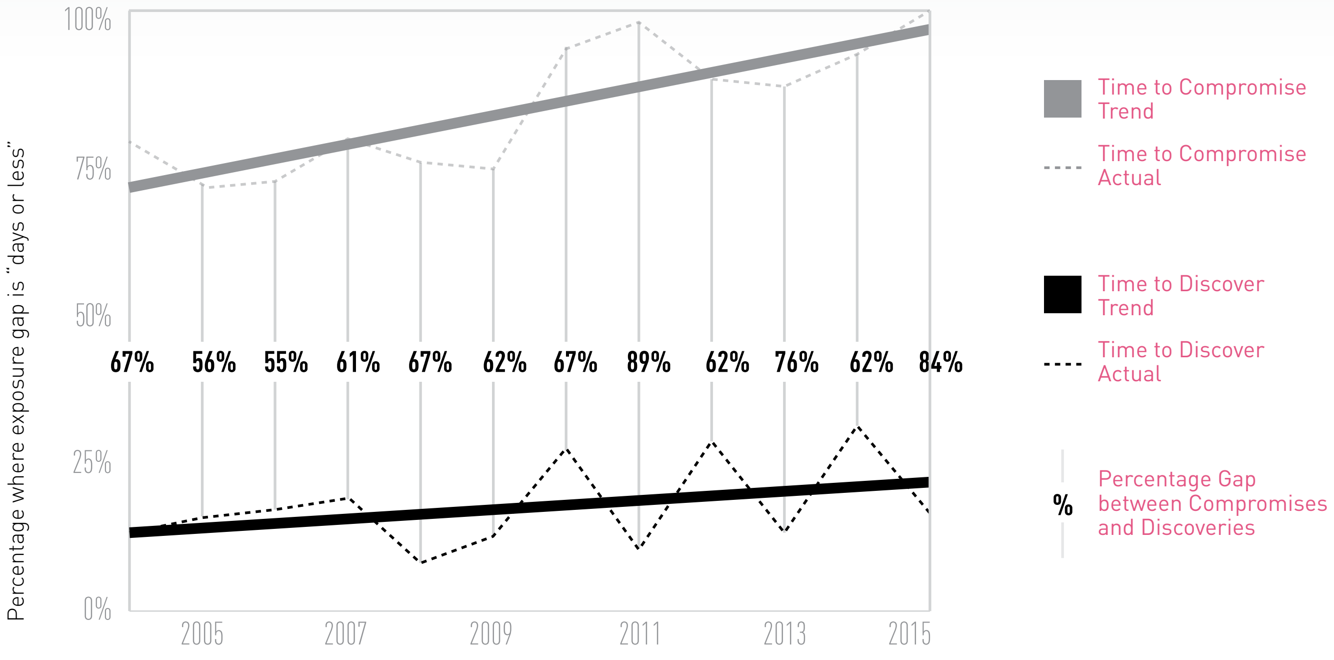
LOTS OF FIRES, VERY FEW FIREFIGHTERS

With so much malware, so many attack vectors, and so many devices to protect, no organization is immune—small, large, commercial, industrial, government. We are all at risk. As threats and attacks grow, so does the number of security devices and tools your IT department has to manage. Even if IT budgets were unlimited, there are only so many trained IT staff available.

There are not enough security IT professionals to support the growing demand for managing and monitoring IT systems. Those who are available must juggle combinations of routine requests mixed with urgent alerts. In addition, they are bogged down by manual processes and siloed systems. Advanced threat prevention tools across all points, along with centralized management and methodical execution, are key to their success. Management systems that increase efficiency are crucial.

Traditional approaches to security are no longer enough. To keep up with ever-expanding network perimeters, IT teams must fundamentally change their approach to security. Traditionally

EXPOSURE GAP FROM COMPROMISE TO DISCOVERY



6.1 SOURCE: 2016 Data Breach Investigations Report, Verizon, page 10 a series of individually managed, individually monitored components, security must now become a unified "best-of-breed" system. Today's security architecture must integrate security management for mobile devices, IoT, and cloud systems under one management architecture with the flexibility to support multiple distributed cloud environments. Today's security must be fast, open, integrated, and most importantly, managed from a single pane of glass.

It only takes minutes for a skilled attacker with an entry point to get inside your network. Attackers are more efficient at getting in and out with data, so it is vital to focus on prevention, not just detection. The latest data from Verizon's 2016 Breach Investigation Report shows that every minute counts, as every year attackers get better at compromising networks faster than they can be detected.

BE ORGANIZED IN YOUR EXECUTION

As you saw in Chapters 2 and 4, unknown malware is growing. However, the majority of attacks in 2015 were coming from known malware that is over a year old. Many of these attacks could have been avoided. Keeping up with the latest patches and making sure those patches propagate out to all devices and computers on the networks requires organization and good automation. Be organized and methodical. Augment a strong patching policy with solutions for preventing known attacks. These should include traditional Antivirus, Intrusion Prevention Systems, and a Next Generation Firewall, each updated continuously with the most recent threat intelligence.

As you saw in Chapter 3, mobile devices blur the lines between personal and business usage. One device harboring undetected malware puts the whole network at risk. So, it is vital to create a safe, protected business environment on any mobile device.

Chapter 4 provided a view into the continued growth of unknown malware—both true zero-day vulnerabilities and repackaged variants of prior malware. These attacks are more difficult to detect. In addition, many hackers are learning to bypass the first generation of sandboxes that were installed in recent years. Thankfully, more modern sandboxing solutions detect attacks before evasion code can deploy.

Forward-looking security starts with having a best-of-breed set of fundamental security tools. Advanced Threat Prevention, mobile device protection, and segmenting your network so it can be monitored closely are critical to fully protecting your organization. With costs always being carefully scrutinized, keep execution efficient to maximize the productivity of your IT team.

> *"The best way to predict the future is to invent it."*
>
> Alan Kay, computer scientist

Whether you do it yourself or command a force of minions, tasks like racking servers and tinkering with the server-room air conditioning are quickly becoming someone else's problems—someone working in a cloud-computing center. Cisco estimates that 83 percent of data center traffic will become cloud traffic by 2019.[12] The large-scale transformation to cloud computing signals a fundamental shift from hardware-centric infrastructures residing in enterprise data centers to software-centric infrastructures running on dynamic pools of compute and storage resources. Technology changeover to cloud computing makes this a good time to rethink the solutions you will need to protect your organization's IT assets and services when they originate from a cloud platform as well as what this means for your role as an IT professional.

Rethinking IT Security Roles

Cloud computing lets you provide extensible services cheaper and faster as cloud platforms like Microsoft Azure, Amazon Web Services and Google Cloud Platform are typically more resource efficient than their enterprise-data center counterparts. For example, cloud computing centers typically have higher densities of virtual guest machines in host servers than you typically find in enterprise virtual environments. In addition, cloud computing's burstable bandwidth can handle traffic spikes while on-demand computing resources can make services more reliable, scalable and cost efficient. Letting cloud Infrastructure as a Service (IaaS) and Software as a Service (SaaS) providers deal with hardware and bandwidth issues means you can focus more on the software aspects of your operations: deploying self-service application portals, architecting policies, instituting best practices, and monitoring and reporting on security.

The transition to public and hybrid cloud networking does not mean services and the security measures you need to protect them will be fundamentally different. In the cloud, you still need comprehensive threat prevention capabilities as well as email security, web security, application security; all the measures you currently use to protect your on-site network.

Despite security needs staying constant, moving to the cloud means roles will change. Instead of IT and security administrators calling the shots about what security controls are in scope and other infrastructure issues, application developers will be making these decisions. Administrators and application developers should explore ways to bridge the knowledge gap that separates IT administration, security administration, and application development.

To get the upper hand, you will need to start aligning security with application service workflows and orchestration processes that let you protect services and data and enforce policies regardless of where your services originate and wherever they terminate.

A server is a server regardless of whether it is in your data center or in a cloud-computing center. However, when the servers are mostly under someone else's roof, focusing your attention on the software aspects of networking and security become priorities you should start getting used to now.

TAKE ACTION

STAYING ONE STEP AHEAD IN SECURITY

Benjamin Franklin's axiom that "an ounce of prevention is worth a pound of cure" is especially apt in the era of unknown malware and zero-day vulnerabilities. Ideally, scarce IT resources are better invested in preventing threats than on chasing alerts and responding to security incidents.

PREVENTION

1 MULTILAYER CYBERSECURITY

Threats come in many shapes and sizes. Here are security technologies to layer in your security stack: Next Generation Threat Prevention, Firewall, Application Control, Anti-Bot, Antivirus, Identity Awareness, Anti-Spam and Email Security, Intrusion Prevention System, and URL Filtering.

2 PREVENT MALWARE ON FIRST CONTACT

Real-time threat prevention that disrupts malware on first contact is the new benchmark for security effectiveness.

3 VIRTUAL PATCHING

Virtual patching protects against exploits of unannounced vulnerabilities and bridges the gap until patches for known vulnerabilities are available and can be deployed.

ARCHITECTURE

1 SIMPLIFY SECURITY MANAGEMENT

Switching among consoles to manage security for each network segment is inefficient and promotes making configuration errors that degrade security. Managing all security functions, segments and environments through one console streamlines management for stronger security that is also easier to manage.

2 UNIFY CONTROLS

Implement unified controls across all networks, systems, endpoints and environments including traditional , cloud, virtual, mobile, IoT, and hybrids.

GET THE FACTS

Learn the results from third party independent testing about malware catch rates, real-time threat prevention, management scalability and more. Download Facts vs. Hype: checkpoint.com/facts

REFERENCES

Chapter 2

1 Harrison, Virginia and Pagliery, Jose. "Nearly 1 million new malware threats released every day." CNN Money, April 14, 2015. http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/

2 Chickowski, Ericka. "5 Exploit Trends Driving Attacks Today." Dark Reading, February 17, 2016. http://www.darkreading.com/perimeter/5-exploit-trends-driving-attacks-today/d/d-id/1324352

3 Cisco. "Cisco Global Cloud Index: Forecast and Methodology, 2014–2019 White Paper," April 21, 2016.

4 Weins, Kim. "Cloud Computing Trends: 2016 State of the Cloud Survey." RightScale, February 9, 2016. http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2016-state-cloud-survey

5 Malware Statistics. AV-TEST. https://www.av-test.org/en/statistics/malware/

6 Malware Statistics. AV-TEST. ibid.

Chapter 3

1 comScore Whitepaper. "The U.S. Mobile App Report." August, 2014. http://www.comscore.com/Insights/Presentations-and-Whitepapers/2014/The-US-Mobile-App-Report

2 comScore Whitepaper. "The U.S. Mobile App Report." August, 2014. ibid.

3 comScore Whitepaper. "The U.S. Mobile App Report." August, 2014. ibid.

4 Information Security. "2016 BYOD & Mobile Security Spotlight Report." Scribd. https://www.scribd.com/doc/309703246/BYOD-and-Mobile-Security-Report-2016

Chapter 4

1 Internet World Stats, "Internet Users in the World by Region 2015." http://www.internetworldstats.com/stats.htm

2 Internet World Stats, "Internet World Penetration Rates by Geographic Regions, November 2015 Update." http://www.internetworldstats.com/stats.htm

3 Kerner, Sean Michael. "Heartbleed Remains a Risk 2 Years After It Was Reported," eWeek, April 7, 2016. http://www.eweek.com/security/heartbleed-remains-a-risk-2-years-after-it-was-reported.html

4 US Cert Alert TA15-051A, "Lenovo Superfish Adware Vulnerable to HTTPS Spoofing." US-CERT, February 24, 2015. https://www.us-cert.gov/ncas/alerts/TA15-051A

Chapter 5

1 Korolov, Maria. “Ponemon: Data Breach Costs Now Average $154 per Record.” CSO, May 27, 2015. http://www.csoonline.com/article/2926727/data-protection/ponemon-data-breach-costs-now-average-154-per-record.html

2 Gemalto. "Gemalto releases findings of 2015 Breach Level Index," February 23, 2016. http://www.gemalto.com/press/Pages/Gemalto-releases-findings-of-2015-Breach-Level-Index.aspx

3 Raytheon Websense. "2015 Drill-Down Report – Financial Services," June, 2015.

4 Makovsky. "Data Breaches and Failure to Protect Personal Info Further Damage Wall Street's Reputation and Business," May 28, 2015. http://www.makovsky.com/news/data-breaches-and-failure-to-protect-personal-info-further-damage-wall-streets-reputation-and-business-2/

5 PwC. "The Global State of Information Security Survey 2015 - Managing cyber risks in an interconnected world," 2015. http://www.pwccn.com/home/eng/rcs_info_security_2015.html

6 Makovsky Wall Street Reputation Study op. cit.

7 Makovsky Wall Street Reputation Study ibid.

8 Makovsky Wall Street Reputation Study ibid.

9 Global State Information Security Survey op. cit.

10 Makovsky Wall Street Reputation Study op. cit.

11 Wagstaff, Jeremy. "Medical data, cybercriminals' holy grail, now espionage target," Reuters, June 2015. http://www.reuters.com/article/cybersecurity-usa-targets-idUSL3N0YR30R20150605

12 Global State of Information Security Survey op. cit.

13 6th Annual HIMSS Security Survey.
http://www.himss.org/2013-himss-security-survey?ItemNumber=28270

14 6th Annual HIMSS Security Survey ibid.

15 6th Annual HIMSS Security Survey ibid.

16 6th Annual HIMSS Security Survey ibid.

17 6th Annual HIMSS Security Survey ibid.

18 6th Annual HIMSS Security Survey ibid.

19 6th Annual HIMSS Security Survey ibid.

20 6th Annual HIMSS Security Survey ibid.

21 6th Annual HIMSS Security Survey ibid.

22 6th Annual HIMSS Security Survey ibid.

23 Copyright Oxford Economics, Ltd. Global Industry Databank. http://www.oxfordeconomics.com/forecasts-and-models/industries/data-and-forecasts/global-industry-databank/overview

24 Heng, Stefan. "Industry 4.0: Huge potential for value creation waiting to be tapped," Deutsche Bank Research, May, 2014. http://www.dbresearch.com/servlet/reweb2.ReWEB?rwsite=DBR_INTERNET_EN-PROD&rwobj=ReDisplay.Start.class&document=PROD

25 Boulton, Clint. "Apple's New Health Focus Comes at Propitious Time," The Wall Street Journal, June 10, 2014. http://blogs.wsj.com/cio/2014/06/10/apples-new-health-focus-comes-at-propitious-time/

26 Experian. "Reputation Impact of a Data Breach."
https://www.experian.com/assets/data-breach/white-papers/reputation-study.pdf

Chapter 6

1 Statista. "Average number of connected devices used per person in selected countries in 2014." http://www.statista.com/statistics/333861/connected-devices-per-person-in-selected-countries/

2 Information Security. "2016 BYOD & Mobile Security Spotlight Report." Scribd. https://www.scribd.com/doc/309703246/BYOD-and-Mobile-Security-Report-2016

3 Gartner. "Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015," November 10, 2015. http://www.gartner.com/newsroom/id/3165317

4 Gartner. "Gartner Says Modernization and Digital Transformation Projects Are Behind Growth in Enterprise Application Software Market," August 27, 2015. http://www.gartner.com/newsroom/id/3119717

5 AV-TEST. "Malware Statistics." https://www.av-test.org/en/statistics/malware/

6 Gartner. "One Brand of Firewall Is a Best Practice for Most Enterprises," February 18, 2016. https://www.gartner.com/doc/3215918?ref=SiteSearch&sthkw=One%20Brand%20of%20Firewall%20is%20a%20Best%20Practice%20for%20Most%20Enterprises&fnl=search&srcId=1-3478922254

7 Morgan, Lewis. "Five damanging data breaches caused by human error," IT Governance Blog, February 17, 2016. https://www.itgovernance.co.uk/blog/five-damaging-data-breaches-caused-by-human-error/

8 PCI Security Standards Council. "Maintaining Payment Security." https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

9 U.S. Department of Health & Human Services. "Summary of the HIPAA Security Rule." http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/

10 National Institute of Standards and Technology. "Federal Information Security Management Act (FISMA) Implementation Project." http://csrc.nist.gov/groups/SMA/fisma/

11 U.S. Department of Education. "Family Educational Rights and Privacy Act (FERPA)." http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

12 Cisco. "Cisco Global Cloud Index: Forecast and Methodology, 2014–2019 White Paper," page 5, April 21, 2016.

About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) is the largest network cyber security vendor globally, providing industry-leading solutions and protecting customers from cyber-attacks with an unmatched catch rate of malware and other types of threats. Check Point offers a complete security architecture defending enterprises—from networks to mobile devices—in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes.

Check Point®
SOFTWARE TECHNOLOGIES LTD

ONE STEP > AHEAD

WORLDWIDE HEADQUARTERS
5 Ha'Solelim Street, Tel Aviv 67897, Israel
Tel: 972-3-753-4555 | Fax: 972-3-624-1100
Email: info@checkpoint.com

U.S. HEADQUARTERS
959 Skyway Road, Suite 300, San Carlos, CA 94070
Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

checkpoint.com