

Cisco

2017 Annual Cybersecurity Report



Table of Contents

EXECUTIVE SUMMARY AND MAJOR FINDINGS	3
INTRODUCTION.....	8
THE EXPANSION OF THE ATTACK SURFACE	10
ATTACKER BEHAVIOR	13
The Reconnaissance Phase.....	13
Web Attack Methods: “Short Tail” Threats Help Adversaries Lay the Groundwork for Campaigns.....	13
The Weaponization Phase	15
Web Attack Vectors: Flash Is Fading, but Users Must Remain Vigilant	15
Application Security: Managing OAuth Connection Risk Amid an App Explosion	16
The Delivery Phase	20
Disappearance of Major Exploit Kits Presents Opportunities for Smaller Players and New Entrants.....	20
Malvertising: Adversaries Use Brokers to Increase Speed and Agility	22
Investigation Finds 75 Percent of Organizations Affected by Adware Infections.....	23
Global Spam Is Increasing—and So Is the Percentage of Malicious Attachments	25
The Installation Phase.....	30
Web Attack Methods: “Long Tail” Snapshot Reveals Threats That Users Can Easily Avoid	30
Vertical Risk of Malware Encounters: Attackers See Value Across the Board	31
Regional Overview of Web Block Activity.....	32
Time to Detection: An Essential Metric for Measuring Defenders’ Progress	33
Time to Evolve: For Some Threats, Change Is Constant	34
DEFENDER BEHAVIOR	42
Vulnerabilities on the Decline in 2016.....	42
Middleware: Adversaries See Opportunity in Unpatched Software.....	44
Time to Patch: Closing the Recovery Time Frame	45
CISCO 2017 SECURITY CAPABILITIES BENCHMARK STUDY.....	49
Perceptions: Security Professionals Confident in Tools, Less Sure They’re Using Them Effectively	49
Constraints: Time, Talent, and Money Affect the Ability to Respond to Threats	51
Impact: More Organizations Experiencing Losses from Breaches	55
Outcomes: Increased Scrutiny Will Play a Role in Security Improvements	58
Trust Versus Cost: What Drives Security Purchases?	61
Summary: What the Benchmark Study Reveals	62
INDUSTRY	64
Value Chain Security: Success in a Digital World Hinges on Mitigating Third-Party Risk.....	64
Geopolitical Update: Encryption, Trust, and a Call for Transparency.....	65
High-Speed Encryption: A Scalable Solution to Protecting Data in Transit.....	66
Network Performance and Adoption Versus Security Maturity	67
CONCLUSION.....	71
A Rapidly Expanding Attack Surface Requires an Interconnected and Integrated Approach to Security.....	71
The Key Goal: Reducing Adversaries’ Operational Space.....	73
ABOUT CISCO	74
Contributors to the Cisco 2017 Annual Cybersecurity Report.....	75
APPENDIX	78

Executive Summary

As the attack surface increases, defenders must focus on their most important goal: reducing their adversaries' operational space.

Adversaries have more tools at their disposal than ever before. They also have a keen sense of when to use each one for maximum effect. The explosive growth of mobile endpoints and online traffic works in their favor. They have more space in which to operate and more choices of targets and approaches.

Defenders can use an array of strategies to meet the challenges of an expanding threat landscape. They can purchase best-of-breed solutions that work separately to provide information and protection. And they can compete for personnel in a market where talent is in short supply and budgets are tight.

Stopping all attacks may not be possible. But you can minimize both the risk and the impact of threats by constraining your adversaries' operational space and, thus, their ability to compromise assets. One measure you can take is simplifying your collection of security tools into an interconnected and integrated security architecture.

Integrated security tools working together in an automated architecture can streamline the process of detecting and mitigating threats. You will then have time to address more complex and persistent issues. Many organizations use at least a half dozen solutions from just as many vendors ([page 53](#)). In many cases, their security teams can investigate only half the security alerts they receive on a given day.

The Cisco 2017 Annual Cybersecurity Report presents research, insights, and perspectives from Cisco Security Research. We highlight the relentless push-and-pull dynamic between adversaries trying to gain more time to operate and defenders working to close the windows

of opportunity that attackers try to exploit. We examine data compiled by Cisco threat researchers and other experts. Our research and insights are intended to help organizations respond effectively to today's rapidly evolving and sophisticated threats.

This report is divided into the following sections:

Attacker Behavior

In this section, we examine how attackers reconnoiter vulnerable networks and deliver malware. We explain how tools such as email, third-party cloud applications, and adware are weaponized. And we describe the methods that cybercriminals employ during the installation phase of an attack. This section also introduces our "time to evolve" (TTE) research, which shows how adversaries keep their tactics fresh and evade detection. We also give an update on our efforts to reduce our average median time to detection (TTD). In addition, we present the latest research from Cisco on malware risk for various industries and geographic regions.

Defender Behavior

We offer updates on vulnerabilities in this section. One focus is on the emerging weaknesses in middleware libraries that present opportunities for adversaries to use the same tools across many applications, reducing the time and cost needed to compromise users. We also share Cisco's research on patching trends. We note the benefit of presenting users with a regular cadence of updates to encourage the adoption of safer versions of common web browsers and productivity solutions.

Cisco 2017 Security Capabilities Benchmark Study

This section covers the results of our third Security Capabilities Benchmark study, which focuses on security professionals' perceptions of the state of security in their organizations. This year, security professionals seem confident in the tools they have on hand, but they are uncertain about whether these resources can help them reduce the operational space of adversaries. The study also shows that public security breaches are having a measurable impact on opportunities, revenue, and customers. At the same time, breaches are driving technology and process improvements in organizations. [For more in-depth analysis around the state of security in organizations, go to page 49.](#)

Industry

In this section, we explain the importance of ensuring value chain security. We examine the potential harm of governments stockpiling information about zero-day exploits and vulnerabilities in vendors' products. In addition, we discuss the use of rapid encryption as a solution for protecting data in high-speed environments. Finally, we outline the challenges of organizational security as global Internet traffic, and the potential attack surface, grow.

Conclusion

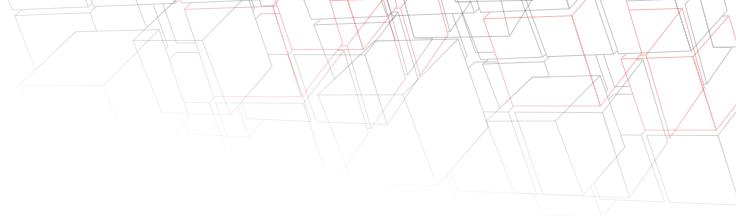
In the conclusion, we suggest that defenders adapt their security practices so they can better meet typical security challenges along the attack chain and reduce adversaries' operational space. This section also offers specific guidance on establishing an integrated and simplified approach to security: one that will connect executive leadership, policy, protocols, and tools to prevent, detect, and mitigate threats.

Major Findings

- Three leading exploit kits—Angler, Nuclear, and Neutrino—abruptly disappeared from the landscape in 2016, leaving room for smaller players and new entrants to make their mark.
- According to the Cisco 2017 Security Capabilities Benchmark Study, most companies use more than five security vendors and more than five security products in their environment. Fifty-five percent of the security professionals use at least six vendors; 45 percent use anywhere from one to five vendors; and 65 percent use six or more products.
- The top constraints to adopting advanced security products and solutions, according to the benchmark study, are budget (cited by 35 percent of the respondents), product compatibility (28 percent), certification (25 percent), and talent (25 percent).
- The Cisco 2017 Security Capabilities Benchmark Study found that, due to various constraints, organizations can investigate only 56 percent of the security alerts they receive on a given day. Half of the investigated alerts (28 percent) are deemed legitimate; less than half (46 percent) of legitimate alerts are remediated. In addition, 44 percent of security operations managers see more than 5000 security alerts per day.
- Twenty-seven percent of connected third-party cloud applications introduced by employees into enterprise environments in 2016 posed a high security risk. Open authentication (OAuth) connections touch the corporate infrastructure and can communicate freely with corporate cloud and software-as-a-service (SaaS) platforms after users grant access.
- An investigation by Cisco that included 130 organizations across verticals found that 75 percent of those companies are affected by adware infections. Adversaries can potentially use these infections to facilitate other malware attacks.
- Increasingly, the operators behind malvertising campaigns are using brokers (also referred to as “gates”). Brokers enable them to move with greater speed, maintain their operational space, and evade detection. These intermediary links allow adversaries to switch quickly from one malicious server to another without changing the initial redirection.
- Spam accounts for nearly two-thirds (65 percent) of total email volume, and our research suggests that global spam volume is growing due to large and thriving spam-sending botnets. According to Cisco threat researchers, about 8 percent to 10 percent of the global spam observed in 2016 could be classified as malicious. In addition, the percentage of spam with malicious email attachments is increasing, and adversaries appear to be experimenting with a wide range of file types to help their campaigns succeed.
- According to the Security Capabilities Benchmark Study, organizations that have not yet suffered a security breach may believe their networks are safe. This confidence is probably misplaced, considering that 49 percent of the security professionals surveyed said their organizations have had to manage public scrutiny following a security breach.

- The Cisco 2017 Security Capabilities Benchmark Study also found that nearly a quarter of the organizations that have suffered an attack lost business opportunities. Four in 10 said those losses are substantial. One in five organizations lost customers due to an attack, and nearly 30 percent lost revenue.
- When breaches occur, operations and finance were the functions most likely to be affected (36 percent and 30 percent, respectively), followed by brand reputation and customer retention (both at 26 percent), according to respondents to the benchmark study.
- Network outages that are caused by security breaches can often have a long-lasting impact. According to the benchmark study, 45 percent of the outages lasted from 1 to 8 hours; 15 percent lasted 9 to 16 hours, and 11 percent lasted 17 to 24 hours. Forty-one percent (see [page 55](#)) of these outages affected between 11 percent and 30 percent of systems.
- Vulnerabilities in middleware—software that serves as a bridge or connector between platforms or applications—are becoming more apparent, raising concerns that middleware is becoming a popular threat vector. Many enterprises rely on middleware, so the threat could affect every industry. During the course of a Cisco® project, our threat researchers discovered that a majority of new vulnerabilities examined were attributable to the use of middleware.
- The cadence of software updates can affect user behavior when it comes to installing patches and upgrades. According to our researchers, regular and predictable update schedules result in users upgrading their software sooner, reducing the time during which adversaries can take advantage of vulnerabilities.
- The 2017 Security Capabilities Benchmark Study found that most organizations rely on third-party vendors for at least 20 percent of their security, and those who rely most heavily on these resources are most likely to expand their use in the future.

Introduction



Introduction

Adversaries have a vast and varied portfolio of techniques for gaining access to organizational resources and for attaining unconstrained time to operate. Their strategies cover all the basics and include:

- Taking advantage of lapses in patching and updating
- Luring users into socially engineered traps
- Injecting malware into supposedly legitimate online content such as advertising

They have many other capabilities, as well, from exploiting middleware vulnerabilities to dropping malicious spam. And once they've achieved their goals, they can quickly and quietly shut down their operations.

Adversaries work nonstop to evolve their threats, move with even more speed, and find ways to widen their operational space. The explosive growth in Internet traffic—driven largely by faster mobile speeds and the proliferation of online devices—works in their favor by helping to expand the attack surface. As that happens, the stakes grow higher for enterprises. The Cisco 2017 Security Capabilities Benchmark Study found that more than one-third of organizations that have been subject to an attack lost 20 percent of revenue or more. Forty-nine percent of the respondents said their business had faced public scrutiny due to a security breach.

How many enterprises can suffer such damage to their bottom line and remain healthy? Defenders must focus their resources on reducing their adversaries' operational space. Attackers will then find it extremely difficult to gain access

to valuable enterprise resources and to conduct their activities without being detected.

Automation is essential to achieving this goal. It helps you understand what normal activity is in the network environment, so you can focus scarce resources on investigating and resolving true threats. Simplifying security operations also helps you become more effective at eliminating adversaries' unconstrained operational space. However, the benchmark study shows that most organizations are using more than five solutions from more than five vendors ([page 53](#)).

Such a complex web of technology, and the overwhelming number of security alerts, is a recipe for less, not more, protection. Adding more security talent can help, of course. With more experts on board, the logic goes, the better the organization's ability to manage technology and deliver better outcomes. However, scarce security talent and limited security budgets make hiring sprees unlikely. Instead, most organizations must make do with the talent they have. They rely on outsourced talent to add muscle to their security teams while also conserving budget.

The real answer to meeting these challenges, as we explain later in this report, is to operationalize people, processes, and technology in an integrated manner. To operationalize security is to truly understand what the enterprise needs to protect, as well as what measures should be used to protect those vital assets.

The Cisco 2017 Annual Cybersecurity Report presents our latest security industry advances designed to help organizations and users defend against attacks. We also look at the techniques and strategies that adversaries use to break through those defenses. The report also highlights major findings from the Cisco 2017 Security Capabilities Benchmark Study, which examines the security posture of enterprises and their perceptions of their preparedness to defend against attacks.

The Expansion of the Attack Surface

The Expansion of the Attack Surface

Mobile devices. Public cloud. Cloud infrastructure. User behavior. Security professionals who participated in Cisco's third annual Security Capabilities Benchmark Study cited all those elements as top sources of concern when they think about their organization's risk of exposure to a cyber attack (Figure 1). This is understandable: The proliferation of mobile devices creates more endpoints to protect. The cloud is expanding the security perimeter. And users are, and always will be, a weak link in the security chain.

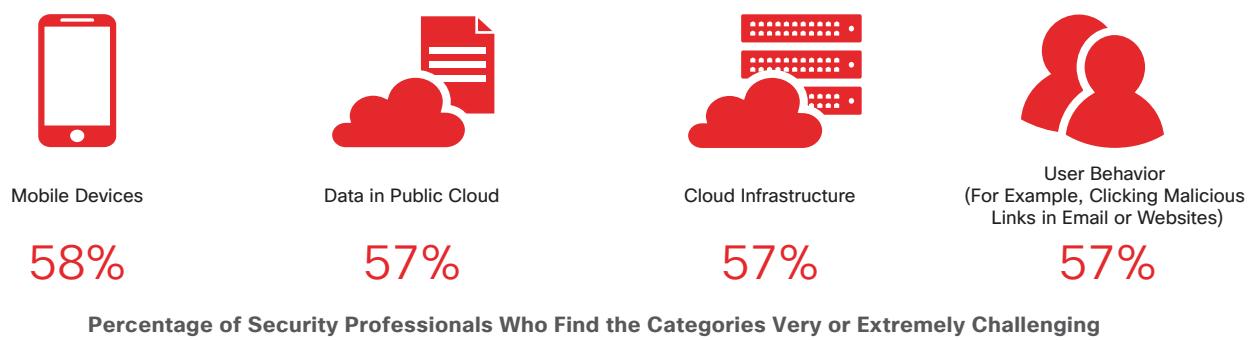
As businesses embrace digitization—and the Internet of Everything (IoE)¹ begins to take shape—defenders will have even more to worry about. The attack surface will only expand, giving adversaries more space to operate.

For more than a decade, the **Cisco® Visual Networking Index (VNI)** has provided global IP traffic forecasts and

analyzed the dynamic factors that facilitate network growth. Consider these statistics from the most recent report, *The Zettabyte Era—Trends and Analysis*:²

- Annual global IP traffic will pass the zettabyte (ZB) threshold by the end of 2016 and reach 2.3 ZB per year by 2020. (A zettabyte is 1000 exabytes, or 1 billion terabytes.) That represents a threefold increase in global IP traffic in the next 5 years.
- Traffic from wireless and mobile devices will account for two-thirds (66 percent) of total IP traffic by 2020. Wired devices will account for only 34 percent.
- From 2015 to 2020, average broadband speeds will nearly double.
- By 2020, 82 percent of all consumer Internet traffic globally will be IP video traffic, up from 70 percent in 2015.

Figure 1 Security Professionals' Biggest Sources of Concern Related to Cyber Attacks



Source: Cisco 2017 Security Capabilities Benchmark Study

 Download the 2017 graphics at: www.cisco.com/go/acr2017graphics

¹ "Internet of Everything FAQ," Cisco: <http://ioeassessment.cisco.com/learn/ioe-faq>.

² *The Zettabyte Era—Trends and Analysis*, Cisco VNI, 2016:

<http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html>.



In addition, the Cisco *VNI™ Forecast and Methodology, 2015–2020* white paper³ predicts that the volume of global Internet traffic in 2020 will be 95 times as great as it was in 2005.

Of course, opportunistic cybercriminals pay close attention to these trends, too. We are already seeing operators in the shadow economy taking steps to become more agile in this changing environment. They are creating highly targeted and varied attacks designed to succeed across the expanding attack surface. Meanwhile, security teams are in a constant firefighting mode, overwhelmed by alerts. They're having to rely on an array of security products in the network environment that only add more complexity and can even increase an organization's susceptibility to threats.

Organizations must:

- Integrate their security technology
- Simplify their security operations
- Rely more on automation

This approach will help reduce operational expenses, ease the burden on security personnel, and deliver better security outcomes. Most important, it will give defenders the ability to focus more of their time on eliminating the unconstrained space in which adversaries currently operate.

³ Cisco VNI Forecast and Methodology, 2015–2020, Cisco VNI, 2016:
<http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html>.

Attacker Behavior

Attacker Behavior

Reconnaissance

Weaponization

Delivery

Installation

Attackers research, identify, and select their targets.

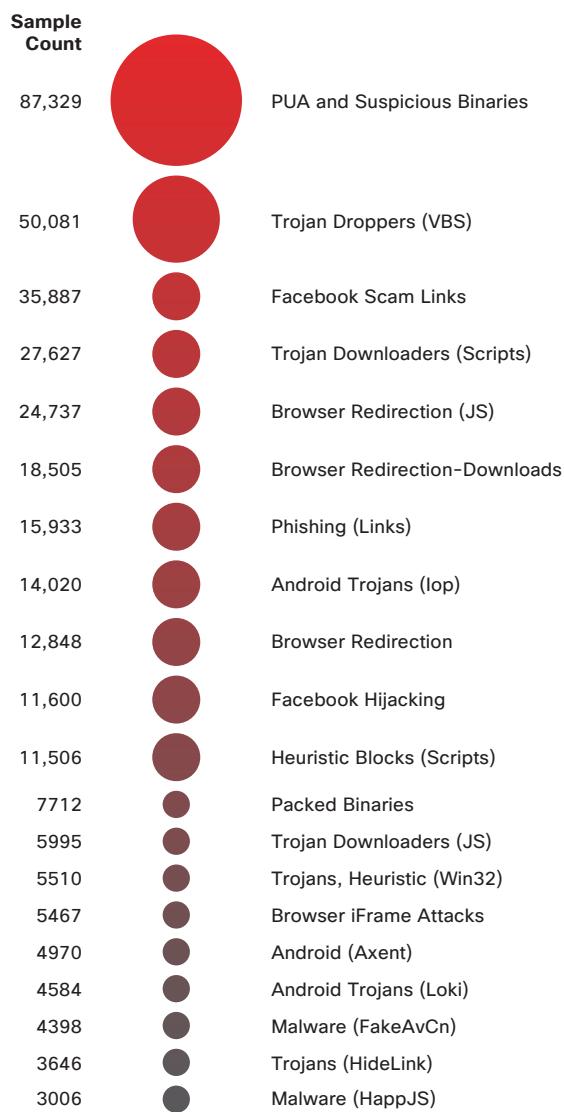
Web Attack Methods: “Short Tail” Threats Help Adversaries Lay the Groundwork for Campaigns

Reconnaissance is, of course, a foundational step for launching a cyber attack. In this phase, adversaries look for vulnerable Internet infrastructure or network weaknesses that will allow them to gain access to users’ computers and, ultimately, to infiltrate organizations.

Suspicious Windows binaries and potentially unwanted applications (PUAs) topped the list of web attack methods for 2016 by a significant margin (see Figure 2). Suspicious Windows binaries deliver threats such as spyware and adware. Malicious browser extensions are an example of PUAs.

Facebook scams, which include fake offers and media content along with survey scams, ranked third on our list. The continued prominence of Facebook scams on our annual and midyear lists of the most commonly observed malware highlights the foundational role of social engineering in many cyber attacks. Facebook has nearly 1.8 billion monthly active users worldwide.⁴ It is logical territory for cybercriminals and other actors looking to dupe users. One positive development is the company’s recent announcement that it is taking steps to eliminate fake news and hoaxes. Critics suggest such content may have influenced voters in the 2016 U.S. presidential election.⁵

Figure 2 Most Commonly Observed Malware



⁴ Facebook stats, September 2016: <http://newsroom.fb.com/company-info/>.

⁵ “Zuckerberg Vows to Weed Out Facebook ‘Fake News,’” by Jessica Guynn and Kevin McCoy, USA Today, November 14, 2016: <http://www.usatoday.com/story/tech/2016/11/13/zuckerberg-vows-weed-out-facebook-fake-news/93770512/>.

Source: Cisco Security Research

Browser redirection malware rounded out the top five most commonly observed malware types for 2016. As discussed in the *Cisco 2016 Midyear Cybersecurity Report*,⁶ browser infections can expose users to malicious advertising (malvertising), which adversaries use to set up ransomware and other malware campaigns. Cisco threat researchers warn that malicious adware, which includes ad injectors, browser-settings hijackers, utilities, and downloaders, is a growing problem. In fact, we have identified adware infections in 75 percent of the companies we recently investigated as part of our research into the adware problem. (For more on this topic, see “Investigation Finds 75 Percent of Organizations Affected by Adware Infections,” [page 23](#).)

Other malware types listed in Figure 3, such as browser JavaScript abuse malware and browser iFrame abuse malware, are also designed to facilitate browser infections. Trojans (droppers and downloaders) also appear among the top five most commonly observed malware types, which indicates that they remain popular tools for gaining initial access to users’ computers and to organizational networks.

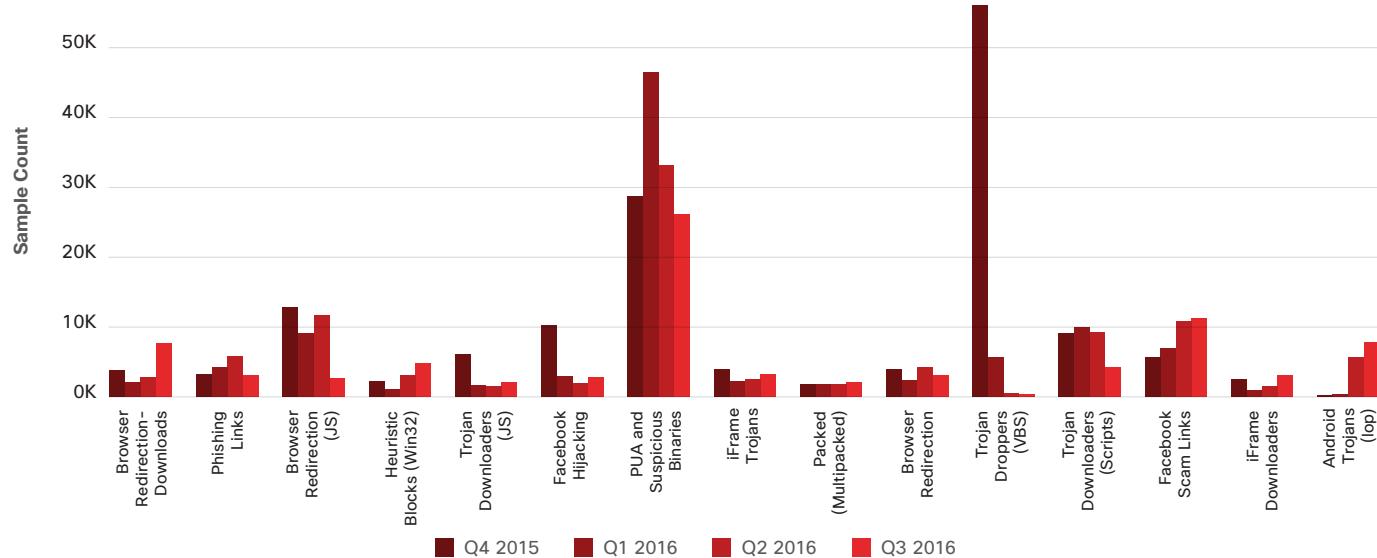
Another trend to watch: consistently high use of malware that targets users of the Android operating platform. Android Trojans have been moving steadily up the short-tail list over the past 2 years. They ranked among the top

10 most commonly seen types of malware in 2016. Loki malware, which appears toward the very end of the short tail shown in Figure 2 (see previous page), is particularly troublesome because it can replicate and infect other files and programs.

Figure 3 helps to illustrate malware trends that Cisco threat researchers have observed since late 2015. It shows that adversaries have made a definite shift in the reconnaissance phase of web-based attacks. More threats now specifically seek vulnerable browsers and plugins. This shift corresponds with adversaries’ growing reliance on malvertising, as it becomes more difficult to exploit large numbers of users through traditional web attack vectors. (See the next section, “Web Attack Vectors: Flash Is Fading, but Users Must Remain Vigilant,” [page 15](#).)

The message for individual users, security professionals, and enterprises is clear: Making sure that browsers are secure, and disabling or removing unnecessary browser plugins, can go a long way toward preventing malware infections. These infections can lead to more significant, disruptive, and costly attacks, such as ransomware campaigns. These simple steps can greatly reduce your exposure to common web-based threats and prevent adversaries from finding the operational space to carry out the next phase of the attack chain: weaponization.

Figure 3 Most Commonly Observed Malware, Q4 2015–Q3 2016



Source: Cisco Security Research

⁶ Cisco 2016 Midyear Cybersecurity Report: http://www.cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html.

Reconnaissance

Weaponization

Delivery

Installation

Attackers pair remote access malware with exploits in deliverable payloads.

Web Attack Vectors: Flash Is Fading, but Users Must Remain Vigilant

Adobe Flash has long been an attractive web attack vector for adversaries who want to exploit and compromise systems. However, as the amount of Adobe Flash content on the web continues to decline—and awareness about Flash vulnerabilities grows—it is becoming more difficult for cybercriminals to exploit users at the scale they once enjoyed.

Adobe itself is moving away from full development and support of the software platform and has encouraged developers to adopt newer standards such as HTML5.⁷ Providers of popular web browsers are also taking a strong position on Flash. For example, Google announced in 2016 that it will phase out full support for Adobe Flash on its Chrome browser.⁸ Firefox is continuing to support legacy Flash content, but it is blocking “certain Flash content that is not essential to the user experience.”⁹

Flash may be fading, but exploit kit developers are helping it endure as an attack vector. However, there are signs this may be changing. After three leading exploit kits—Angler, Nuclear, and Neutrino—abruptly disappeared from the threat landscape in 2016, our threat researchers observed a significant decline in Flash-related Internet traffic. (See “Disappearance of Major Exploit Kits Presents Opportunities for Smaller Players and New Entrants,” [page 20](#).) The actors behind the Angler exploit kit heavily targeted Flash vulnerabilities to compromise users. The Nuclear exploit kit had a similar focus on Flash. And Neutrino relied on Flash files to deliver exploits.

Users must remain cautious and should uninstall Flash unless they need it for business reasons. If they must use it, they must stay current with updates. Using web browsers that feature automatic patching capabilities can help. As noted in “Web Attack Methods: ‘Short Tail’ Threats Help Adversaries Lay the Groundwork for Campaigns” on [page 13](#), using secure browsers—and disabling or removing unnecessary browser plugins—will significantly reduce your exposure to web-based threats.

Java, PDF, and Silverlight

Both Java and PDF Internet traffic experienced notable declines in 2016. Silverlight traffic has already reached a level that is not worthwhile for threat researchers to track regularly.

Java, once the dominant web attack vector, has seen its security posture improve significantly in recent years. Oracle’s decision in early 2016 to eliminate its Java browser plugin has helped to make Java a less attractive web attack vector. PDF attacks are also increasingly rare. For that reason, they can be easier to detect, which is why many adversaries now use this strategy less often.

However, as with Flash, cybercriminals still use Java, PDF, and Silverlight to exploit users. Individual users, enterprises, and security professionals must be aware of these potential roads to compromise. To reduce their risk of exposure to these threats, they must:

- Download patches
- Use up-to-date web technology
- Avoid web content that might present risk

⁷ “Flash, HTML5 and Open Web Standards,” Adobe News, November 2015: <https://blogs.adobe.com/conversations/2015/11/flash-html5-and-open-web-standards.html>.

⁸ “Flash and Chrome,” by Anthony LaForge, The Keyword blog, Google, August 9, 2016: <https://blog.google/products/chrome/flash-and-chrome/>.

⁹ “Reducing Adobe Flash Usage in Firefox,” by Benjamin Smedberg, Future Release blog, Mozilla, July 20, 2016: <https://blog.mozilla.org/futurereleases/2016/07/20/reducing-adobe-flash-usage-in-firefox/>.

Application Security: Managing OAuth Connection Risk Amid an App Explosion

When enterprises shift to the cloud, their security perimeter extends into the virtual realm. However, that security perimeter quickly dissipates with each connected third-party cloud application that employees introduce into the environment.

Workers want to improve their productivity and stay connected while on the job. But these shadow IT applications create a risk for enterprises. They touch the corporate infrastructure and can communicate freely with the corporate cloud and software-as-a-service (SaaS) platforms as soon as users grant access through open authentication (OAuth). These apps can have extensive—and, at times, excessive—access scopes. They must be managed carefully because they can view, delete, externalize, and store corporate data, and even act on behalf of users.

The cloud security provider CloudLock, now part of Cisco, has been tracking the growth of connected third-party cloud applications across a sample group of 900 organizations representing a range of industries. As Figure 4 shows, there were about 129,000 unique applications observed at the beginning of 2016. By the end of October, that number had grown to 222,000.

The number of applications has increased approximately 11 times since 2014. (See Figure 5.)

Classifying the Riskiest Applications

To help security teams understand which connected third-party cloud applications in their environment present the most risk to network security, CloudLock developed the Cloud Application Risk Index (CARI). The process involves several evaluations:

- **Data-access requirements:** Organizations answer the following questions, among others: What permissions are required to authorize the application? Does granting data access mean that the application has programmatic (API) access to corporate SaaS platforms through OAuth connections? Can the application (and by extension, the vendor) act on behalf of users and take actions with corporate data, such as viewing and deleting?

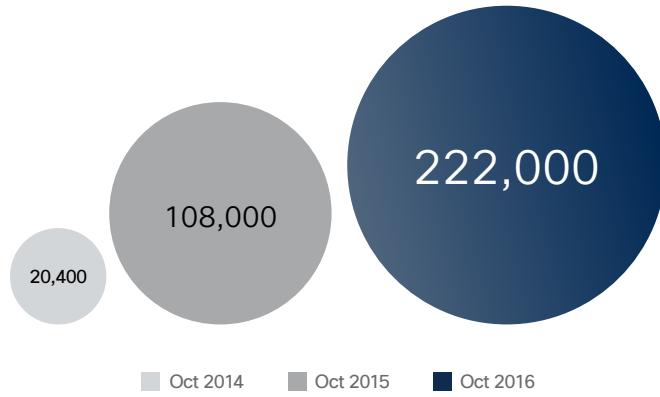
- **Community trust rating:** Peer-driven and crowd-sourced evaluations are used for this assessment.
- **Application threat intelligence:** This comprehensive background check by cybersecurity experts is based on an application's various security attributes, such as security certifications, breach history, and analyst reviews.

Figure 4 Explosive Growth of Connected Third-Party Cloud Applications, 2016



Source: Cisco CloudLock

Figure 5 Growth of Third-Party Cloud Applications, Year-Over-Year Comparison



Source: Cisco CloudLock

Download the 2017 graphics at: www.cisco.com/go/acr2017graphics



Risk Scores and Examples

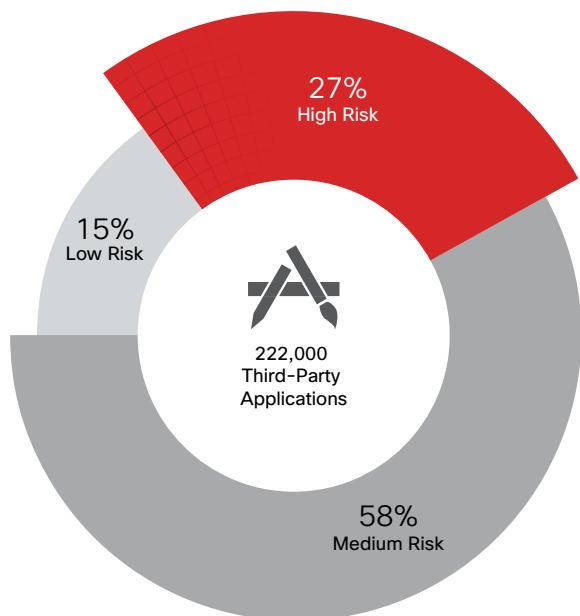
After categorizing third-party cloud applications using the CARI, CloudLock assigns a risk score for each app on a scale of 1 (lowest risk) to 5 (highest risk).

An app that would score 1 on the scale might have, for example, minimal access scopes (it can see email only), a 100 percent community trust rating, and no breach history.

An app that would score 5 on the scale might be one with full account access (it can see all emails, documents, navigation history, calendar, and more), an 8 percent trust rating (meaning, only 8 percent of administrators trust it), and no security certification.

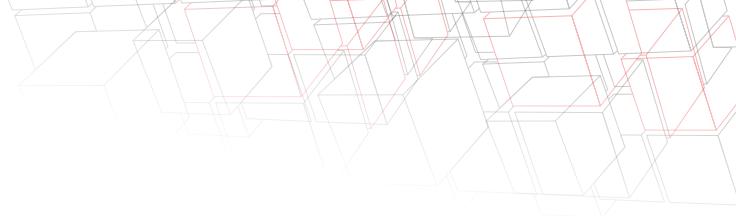
CloudLock used the CARI to categorize the 222,000 applications it had identified across the 900 organizations in its sample. Of those total applications, 27 percent were deemed to be high risk, while the majority fell into the medium-risk category. (See Figure 6.) Half of those organizations had OAuth connections related to a popular gaming application that was released in the summer of 2016.

Figure 6 Third-Party Applications Classified as High Risk



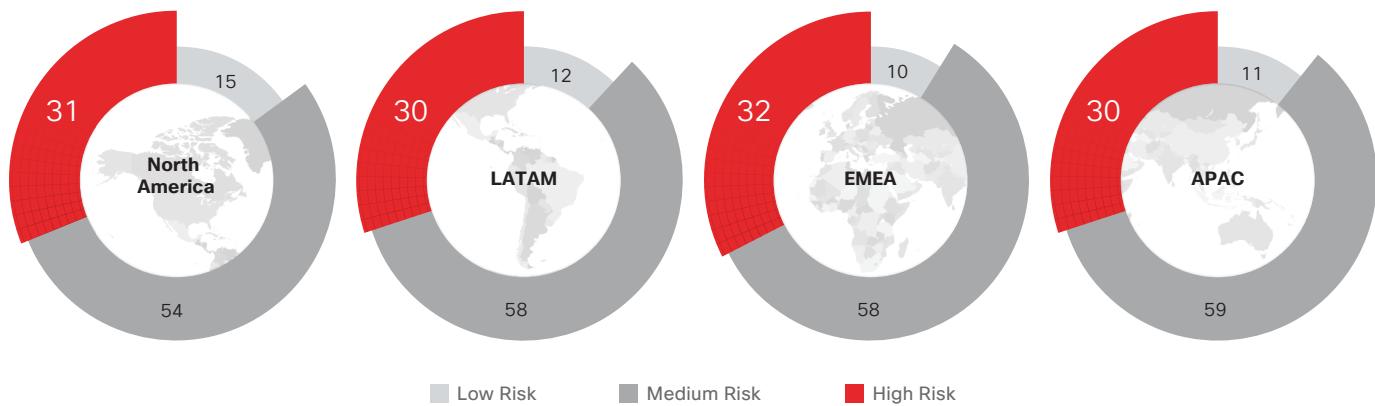
Source: Cisco CloudLock

SHARE [f](#) [t](#) [in](#) [em](#) [dl](#)



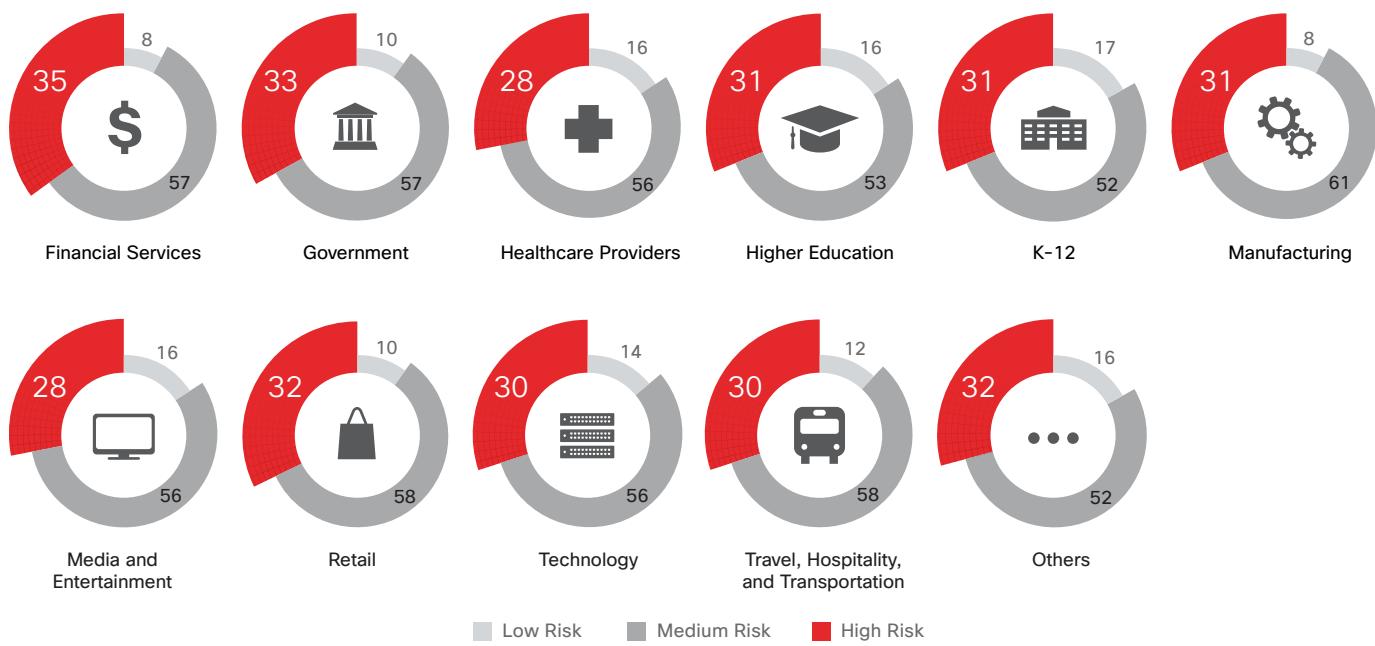
Through our analysis, we have found that all organizations, regardless of their size, industry, or region, have a relatively even distribution of low-, medium-, and high-risk applications (Figures 7 and 8).

Figure 7 Distribution of Low-, Medium-, and High-Risk Applications, by Region



Source: Cisco CloudLock

Figure 8 Distribution of Low-, Medium-, and High-Risk Applications, by Industry



Source: Cisco CloudLock



Download the 2017 graphics at: www.cisco.com/go/acr2017graphics

Cutting Through the Noise

To identify suspicious user and entity behavior in corporate SaaS platforms, including third-party cloud applications, security teams must sift through billions of user activities to define normal patterns of user behavior in their organization's environment. They must look for anomalies that fall outside those expected patterns. Then they need to correlate suspicious activities to determine what might be a true threat that requires investigation.

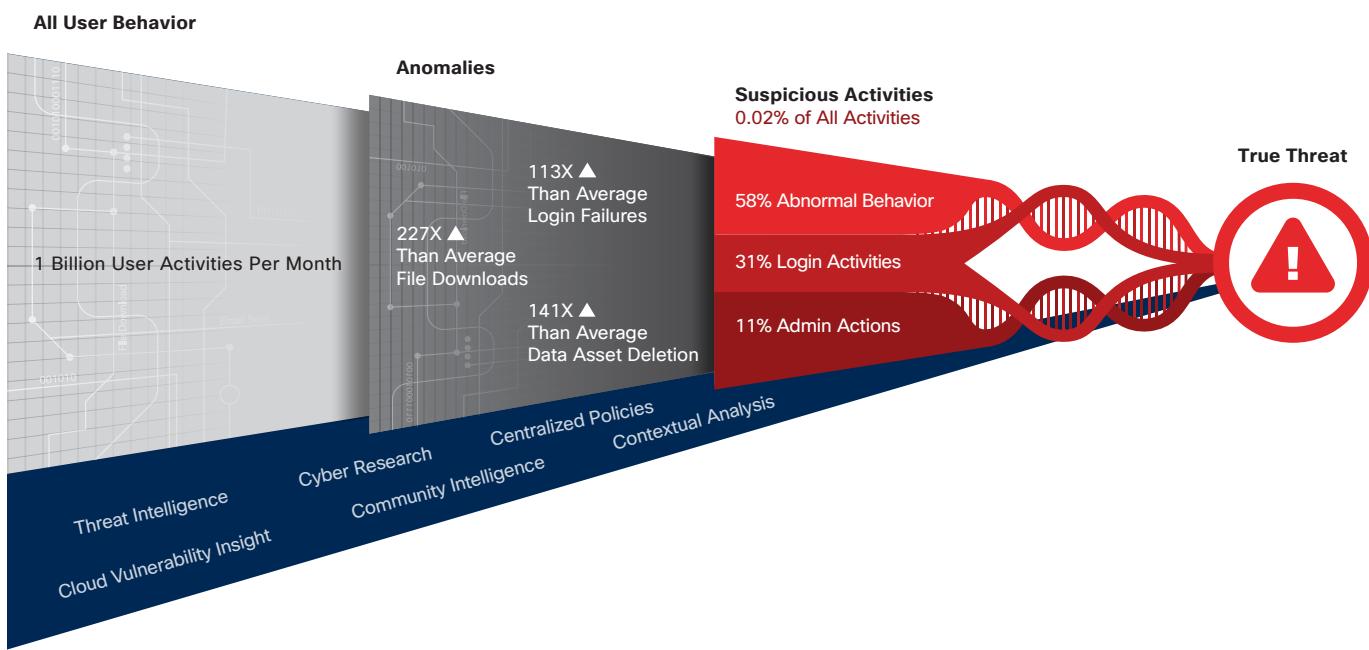
An example of suspicious activity is excessive login activity from several countries in a short period. Say that normal user behavior in a certain organization is for employees to log in to a specific application from no more than one or two countries per week. If one user starts logging in to that application from 68 countries over the course of one week,

a security team will want to investigate that activity to confirm that it is legitimate.

According to our analysis, only 1 in 5000 user activities—0.02 percent—that are associated with connected third-party cloud applications is suspicious. The challenge for security teams, of course, is pinpointing that one instance.

Only with automation can security teams cut through the “noise” of security alerts and focus their resources on investigating true threats. The multistage process of identifying normal and potentially suspicious user activities that is described above—and illustrated in Figure 9—hinges on the use of automation, with algorithms applied at every stage.

Figure 9 Identifying User Behavior Patterns with Automation (Process)



Source: Cisco CloudLock

SHARE

Reconnaissance

Weaponization

Delivery

Installation

Through the malicious use of email, file attachments, websites, and other tools, attackers transmit their cyberweapons to targets.

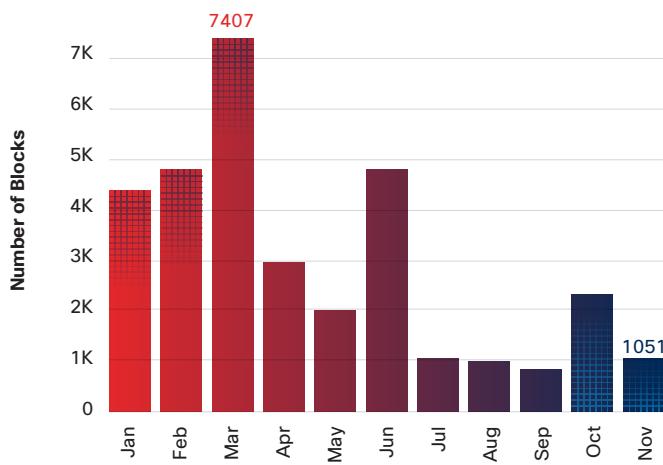
Disappearance of Major Exploit Kits Presents Opportunities for Smaller Players and New Entrants

2016 saw dramatic changes in the exploit kit environment. At the start of the year, Angler, Nuclear, Neutrino, and RIG were clear leaders among exploit kits. By November, RIG was the only one from that group still active. As Figure 10 shows, exploit kit activity dropped off significantly around June.

Nuclear was the first to disappear, suddenly ceasing operation in May. Why its authors abandoned it is a mystery. The Neutrino exploit kit, which also left the scene in 2016, relied on Flash files to deliver vulnerabilities. (See Figure 11 on next page for a list of top vulnerabilities in known exploit kits in 2016.)

Flash remains an attractive web attack vector for adversaries, but it is likely to become less so over time. Fewer sites and browsers are supporting Flash fully or at all, and there is generally greater awareness about Flash vulnerabilities. (For more on this topic, see “Web Attack Vectors: Flash Is Fading, but Users Must Remain Vigilant,” on [page 15](#).)

Figure 10 Exploit Kit Landing Page Blocks, January–November 2016



Source: Cisco Security Research



Download the 2017 graphics at: www.cisco.com/go/acr2017graphics

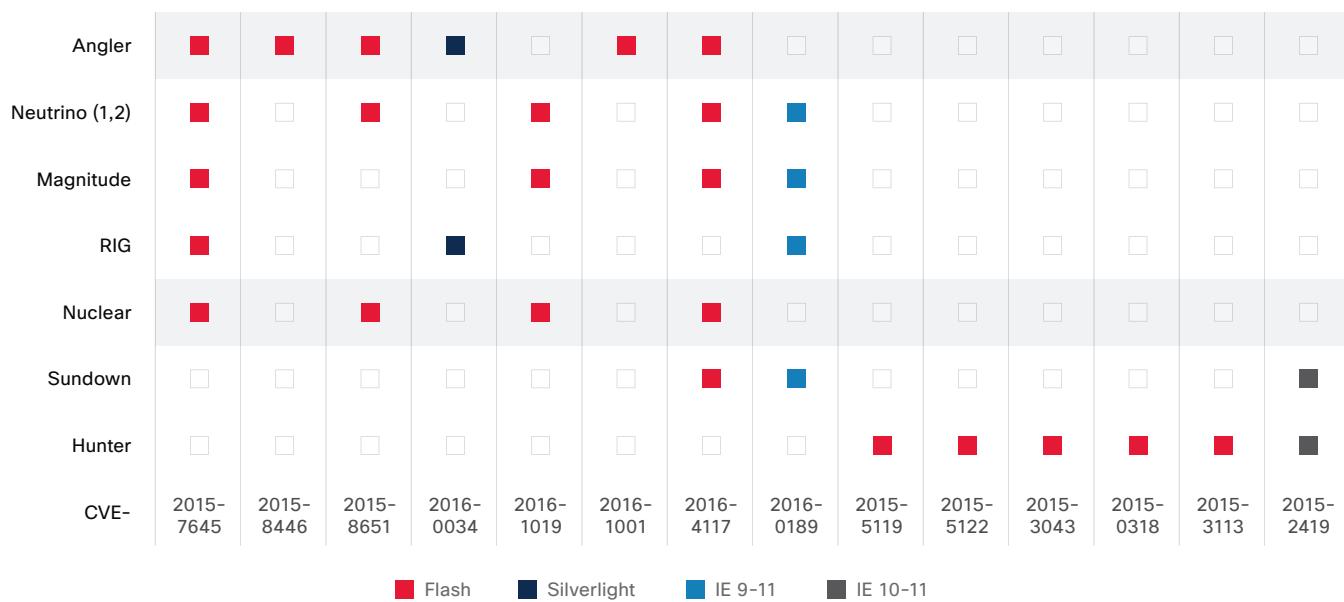
A Giant Goes Silent

Angler—the most advanced and largest among known exploit kits—also targeted Flash vulnerabilities and was linked to several high-profile malvertising and ransomware campaigns. However, unlike Nuclear and Neutrino’s disappearance, Angler’s departure in 2016 is not a mystery.

In late spring, about 50 hackers and cybercriminals were arrested in Russia; the group was linked to the Lurk malware, a banking Trojan that specifically targeted Russian banks.¹⁰ Cisco threat researchers identified clear connections between Lurk and Angler, including the fact that Lurk was being delivered largely through Angler to victims inside Russia. Following the arrests, Angler vanished from the exploit kit marketplace.¹¹

Now that three of the most dominant exploit kits have cleared the field, smaller players and new entrants can expand their market share. And they are becoming more sophisticated and agile. Exploit kits that appeared poised for growth in late 2016 were Sundown, Sweet Orange, and Magnitude. These kits, as well as RIG, are known to target Flash, Silverlight, and Microsoft Internet Explorer vulnerabilities. (See Figure 11.) Uninstalling Flash, and disabling or removing unnecessary browser plugins, will help users reduce the risk that they will be compromised by these threats.

Figure 11 Top Vulnerabilities in Exploit Kits



Source: Cisco Security Research

SHARE

¹⁰ “Russian Hacker Gang Arrested Over \$25M Theft,” BBC News, June 2, 2016: <http://www.bbc.com/news/technology-36434104>.

¹¹ For more on this topic, see the July 2016 Cisco Talos blog post, [Connecting the Dots Reveals Crimeware Shake-Up](#).



Malvertising: Adversaries Use Brokers to Increase Speed and Agility

Users are directed to exploit kits in two primary ways: compromised websites and malvertising. Adversaries will place a link to an exploit kit landing page into a malicious ad or a compromised website, or they will use an intermediate link, known as a broker. (These links, positioned between compromised websites and exploit kit servers, are also referred to as “gates.”) The broker serves as an intermediary between the initial redirection and the actual exploit kit that delivers the malware payload to users.

The latter tactic is becoming more popular as attackers find they must move faster to maintain their operational space and evade detection. Brokers allow adversaries to switch quickly from one malicious server to another without changing the initial redirection. Because they don’t need to constantly modify websites or malicious ads to start the infection chain, exploit kit operators can carry out longer campaigns.

ShadowGate: A Cost-Effective Campaign

As it becomes more difficult to compromise large numbers of users through traditional web attack vectors alone (see [page 15](#)), adversaries are relying more on malvertising to expose users to exploit kits. Our threat researchers dubbed a recent global malvertising campaign “ShadowGate.” This campaign illustrates how malicious ads are providing adversaries with more flexibility and opportunity to target users across geographic regions at scale.

ShadowGate involved websites ranging from popular culture to retail to pornography to news. It potentially

affected millions of users in North America, Europe, Asia-Pacific, and the Middle East. The campaign’s global reach and use of many languages are noteworthy.

ShadowGate, which used domain shadowing, was first seen in early 2015. It would go quiet at times and then randomly start up again to direct traffic to exploit kit landing pages. Initially, ShadowGate was used to direct users to the Angler exploit kit only. But after Angler disappeared in the summer of 2016, users were directed to the Neutrino exploit kit, until that vanished as well a few months later. (For more on this story, see “Disappearance of Major Exploit Kits Presents Opportunities for Smaller Players and New Entrants,” on [page 20](#).)

Even though ShadowGate saw a high volume of web traffic, only a tiny fraction of interactions led to a user being directed to an exploit kit. The malicious ads were mostly impressions—ads that render on the page and require no user interaction. This online advertising model allowed the actors responsible for ShadowGate to operate their campaign more cost-effectively.

Our research into ShadowGate led to a joint effort with a major web hosting company. We worked together to mitigate the threat by reclaiming registrant accounts that adversaries had used to host the activity. We then took down all applicable subdomains.

For more details on the ShadowGate campaign, see the September 2016 Cisco Talos blog post, [Talos ShadowGate Take Down: Global Malvertising Campaign Thwarted](#).

Investigation Finds 75 Percent of Organizations Affected by Adware Infections

Adware, when used for legitimate purposes, is software that downloads or displays advertising through redirections, pop-ups, and ad injections and generates revenue for its creators. However, cybercriminals are also using adware as a tool to help increase their revenue stream. They use malicious adware not only to profit from injecting advertising, but also as a first step to facilitate other malware campaigns, such as DNSChanger malware. Malicious adware is delivered through software bundles; publishers create one installer with a legitimate application along with dozens of malicious adware applications.

Bad actors use adware to:

- Inject advertising, which may lead to further infections or exposure to exploit kits
- Change browser and operating system settings to weaken security
- Break antivirus or other security products
- Gain full control of the host, so they can install other malicious software
- Track users by location, identity, services used, and sites commonly visited
- Exfiltrate information such as personal data, credentials, and infrastructure information (for example, a company's internal sales pages)

To assess the scope of the adware problem for enterprises, Cisco threat researchers examined 80 different adware variants. About 130 organizations across verticals were included in our investigation, which took place from November 2015 to November 2016.

We categorized the adware into four groups, based on the primary behavior of each component:

- **Ad injectors:** This adware usually resides in the browser and can affect all operating systems.
- **Browser-settings hijackers:** This adware component can change computer settings to make the browser less secure.
- **Utilities:** This is a large and growing category of adware. Utilities are web applications that offer a useful service to users, such as PC optimization. These applications can inject advertising, but their primary purpose is to convince users to pay for the service. However, in many cases, utilities are nothing more than scams and provide no benefits to users.
- **Downloaders:** This adware can deliver other software, such as a toolbar.

We determined that 75 percent of the organizations in our study were affected by adware infections.

Figure 12 Percentage of Organizations with Adware Infections



Source: Cisco Security Research

SHARE [f](#) [t](#) [in](#) [x](#) [d](#)

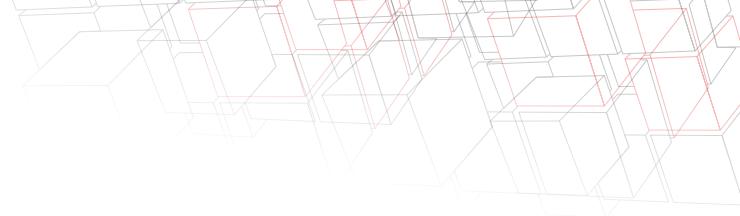
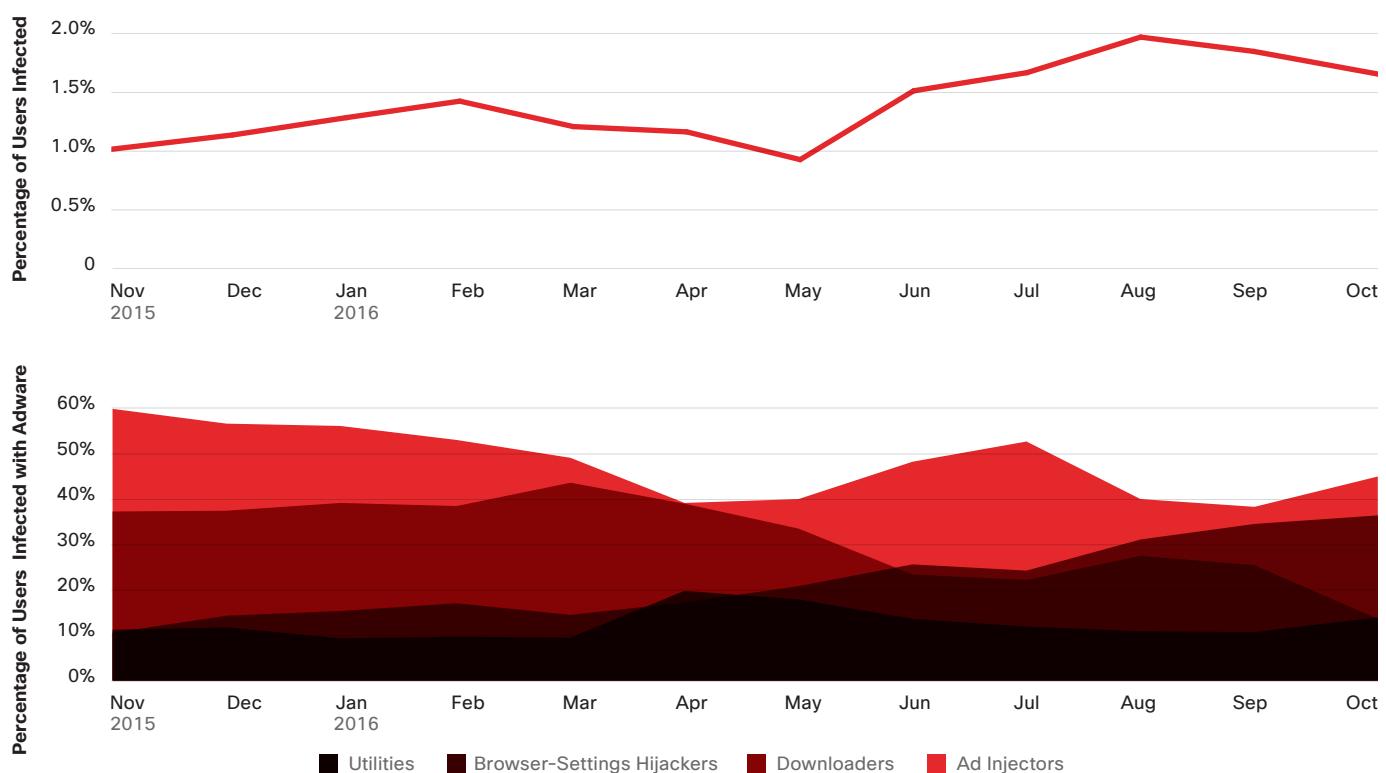


Figure 13 shows the types of incidents we observed in the organizations included in our investigation. Ad injectors were the primary source of infections. This finding indicates that most of these unwanted applications target web browsers. We have also seen an increase in browser-based infections during the last few years, which suggests adversaries are finding success with this strategy for compromising users.

All the adware components we identified during our investigation can place users and organizations at risk for malicious activity. Security teams must recognize the threat that adware infections pose and make sure that users in the organization are fully aware of the risks.

For additional information on this topic, see the February 2016 Cisco Security blog post, [DNSChanger Outbreak Linked to Adware Install Base](#).

Figure 13 Breakdown of Total Incidents by Adware Component



Source: Cisco Security Research

 Download the 2017 graphics at: www.cisco.com/go/acr2017graphics

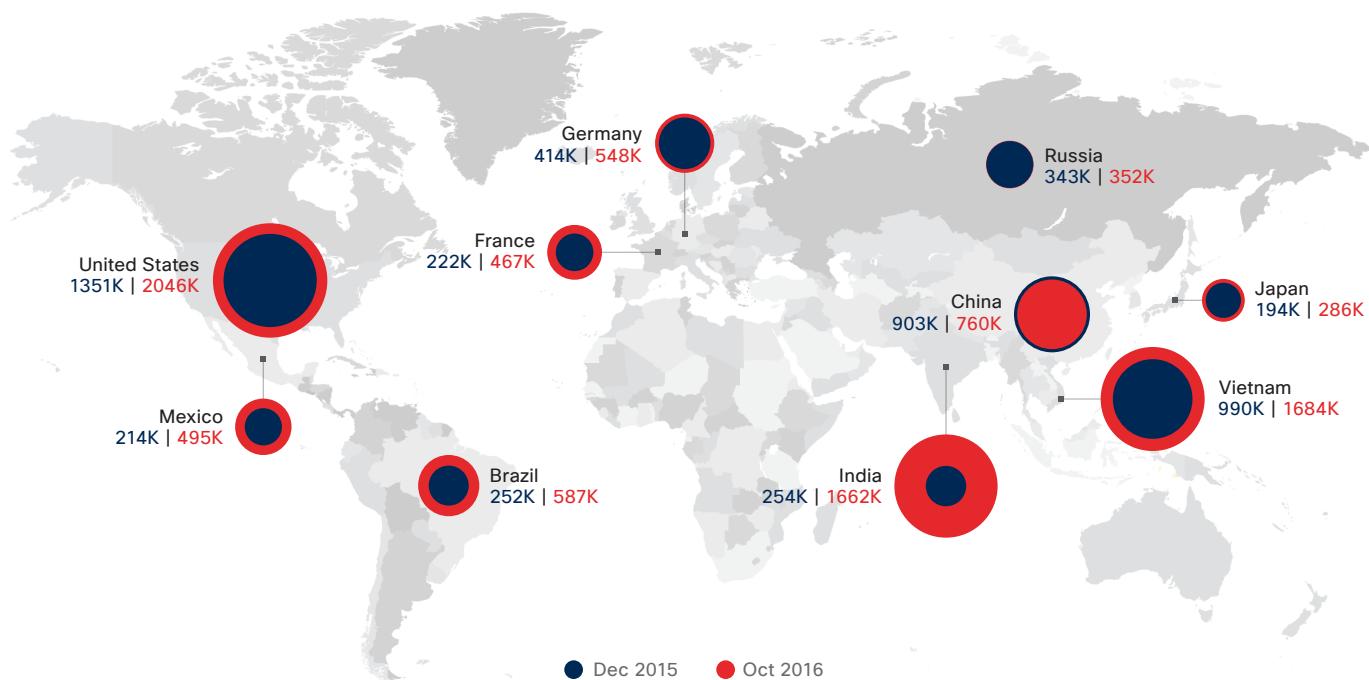
Global Spam Is Increasing—and So Is the Percentage of Malicious Attachments

Cisco threat researchers conducted two studies in 2016 using opt-in customer telemetry to estimate what percentage of total email volume is spam. We found that spam accounts for nearly two-thirds (65 percent) of total email volume. Our research also suggests that global spam volume is growing, due primarily to large and thriving spam-sending botnets like Necurs. In addition, we determined through our analysis that

about 8 percent to 10 percent of global spam observed in 2016 could be categorized as malicious.

From August to October 2016, there was a significant increase in the number of IP connection blocks (Figure 14).¹² This trend can be attributed to an overall rise in spam volume, as well as reputation systems adapting to information about spam senders.

Figure 14 IP Blocks by Country, December 2015–November 2016



Source: Cisco Security Research

SHARE

¹² IP connection blocks are spam messages that are blocked immediately by spam-detecting technology because the spam sender has a bad reputation score. Examples include messages that have originated from known spam-sending botnets or compromised networks that are known to participate in spam attacks.

The five-year graph from the Composite Blocking List (CBL), a DNS-based “blackhole list” of suspected spam-sending computer infections,¹³ also shows a dramatic increase in total spam volume during 2016 (Figure 15).

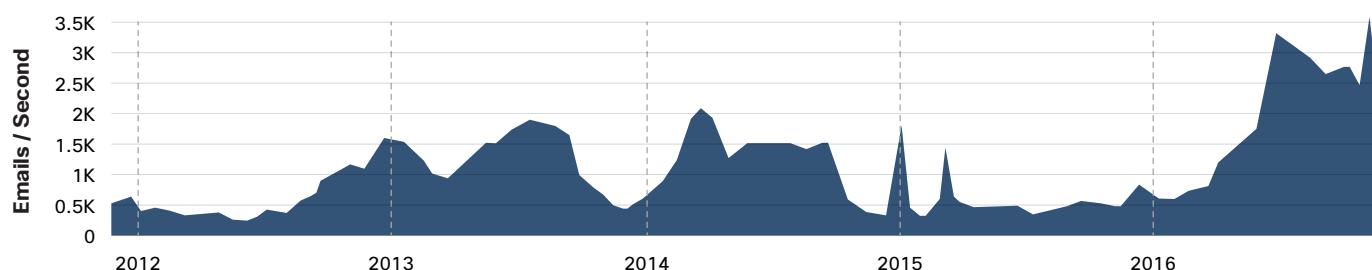
A review of 10-year data from CBL (not shown) suggests that 2016 spam volume is close to the record-high levels seen in 2010. New antispam technologies, and high-profile takedowns of spam-related botnets, have helped to keep spam levels low in recent years. Our threat researchers attribute the recent increase in global spam volume to the Necurs botnet. Necurs is a primary vector for Locky ransomware. It also distributes threats such as the Dridex banking Trojan.

Figure 16 is an internal graph generated by Cisco’s SpamCop service that illustrates the change in spam

volume observed in 2016. This graph shows the overall size of the SpamCop Block List (SCBL) from November 2015 to November 2016. Each row in the SCBL represents a distinct IP address.

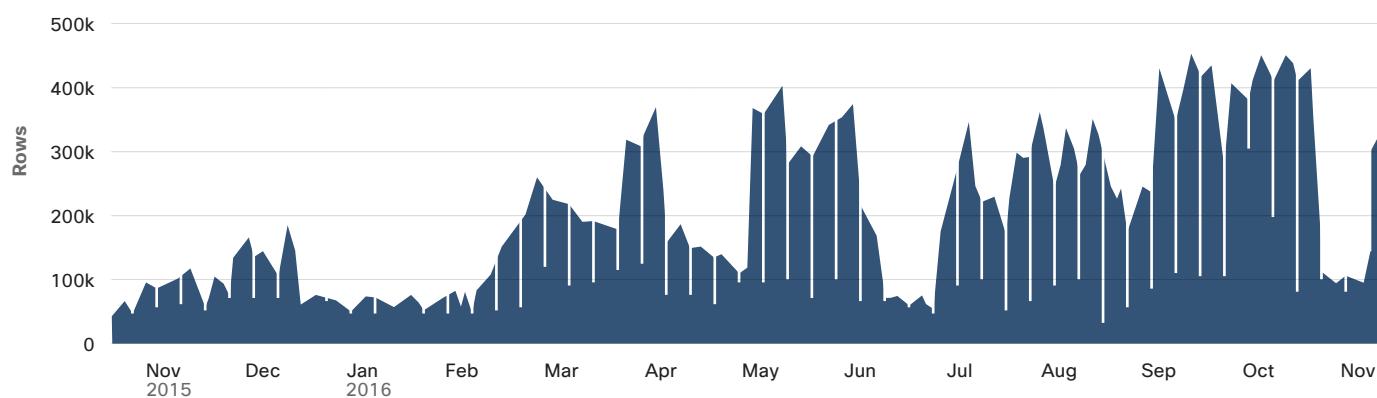
Between November 2015 and February 2016, SCBL size hovered below 200,000 IP addresses. In September and October, SCBL size exceeded 400,000 IP addresses before dropping off in October, which our threat researchers attribute to the operators of Necurs simply taking time off. Also note the significant decline in June. At the end of May, there were arrests in Russia related to the Lurk banking Trojan (see page 21). Subsequently, several high-profile threats, including Necurs, went silent. However, 3 weeks later, Necurs was back in action, adding more than 200,000 IP addresses to the SCBL in less than 2 hours.

Figure 15 Total Spam Volume



Source: CBL

Figure 16 Overall Size of SCBL



Source: SpamCop

SHARE

¹³ For more information about CBL, visit <http://www.abuseat.org/>.

Many of the host IPs sending Necurs spam have been infected for more than 2 years. To help keep the full scope of the botnet hidden, Necurs will send spam only from a subset of infected hosts. An infected host might be used for 2 to 3 days, and then sometimes not again for 2 to 3 weeks. This behavior complicates the job of security personnel who respond to spam attacks. They may believe they have found and successfully cleaned an infected host, but the actors behind Necurs are just biding their time until they launch another attack.

Seventy-five percent of total spam observed in October 2016 contained malicious attachments. Most of that spam was sent by the Necurs botnet. (See Figure 17.) Necurs sends malicious .zip attachments that include embedded executable files such as JavaScript, .hta, .wsf, and VBScript downloaders. In calculating the percentage of total spam containing malicious attachments, we count both the “container” file (.zip) and the “child” files within it (such as a JavaScript file) as individual malicious attachments.

Attackers Experiment with Attachment Types to Keep Malicious Spam Campaigns Fresh

Our threat researchers examined how adversaries use different types of file attachments to help prevent malicious spam from being detected. What we found is that they are continually evolving their strategies, experimenting with a wide range of file types, and quickly switching tactics when they don’t find success.

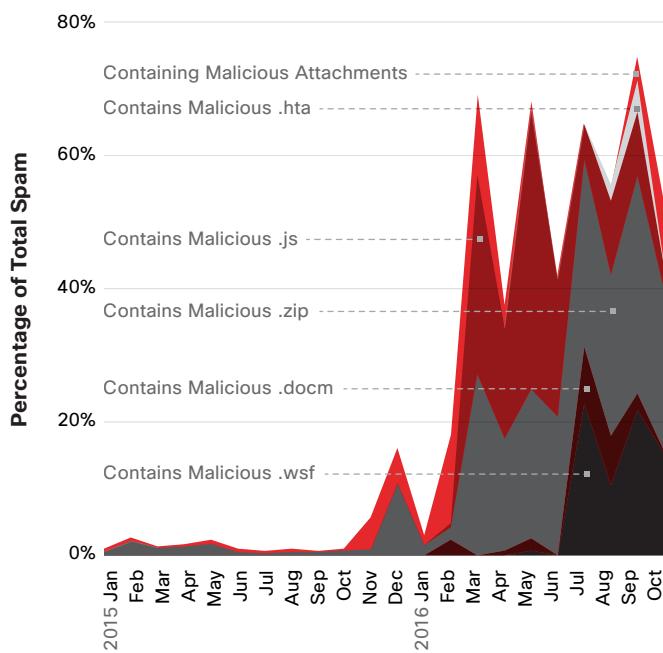
Figure 17 shows how malicious spam operators experimented with the use of .docm, JavaScript, .wsf, and .hta files during the period observed. As noted earlier, many of these file types are associated with spam sent by the Necurs botnet. (For research related to other file types we examined, see the Appendix on [page 78](#).)

The specific percentages for the different file types in a given month are derived using the percentage of total spam that contained malicious attachments seen in that month. So, for example, in July 2016, .docm files represented 8 percent of the total percentage of malicious attachments observed.

Patterns with .wsf files during 2016 (see Figure 17) provide an example of how adversaries will evolve malicious spam tactics over time. This file type was rarely used as a malicious attachment before February 2016. Then, the use of this file type begins to grow as the Necurs botnet becomes more active. By July, .wsf files accounted for 22 percent of all malicious spam attachments. This was also around the time that global spam activity increased dramatically (see previous section), an uptick that was due largely to the Necurs botnet.

Through August, September, and October, we saw fluctuations in the percentages of .wsf files. This indicates that adversaries were pulling back at times when the file type was being detected more frequently.

Figure 17 Percentage of Total Spam Containing Malicious Attachments



Source: Cisco Security Research

SHARE

Hailstorms and Snowshoes

Two types of malicious spam attacks are especially problematic for defenders: hailstorm attacks and snowshoe attacks. Both employ the elements of speed and targeting, and both are highly effective.

Hailstorm attacks target antispam systems. The operators behind these attacks take advantage of the very small window of time between the moment they launch their spam campaign and when antispam systems see it and push coverage out to antispam scanners. Adversaries typically have only seconds or minutes to operate before their campaigns are detected and blocked.

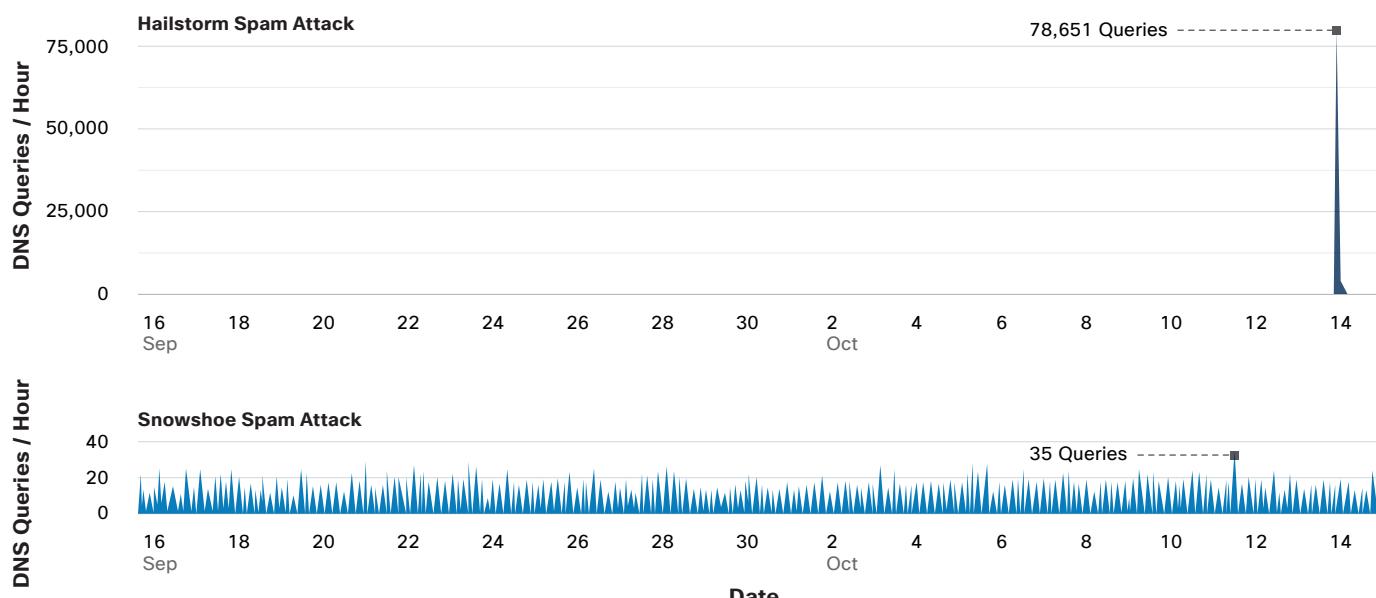
The spike in Figure 18 is a hailstorm attack. The activity is shown in the Cisco Investigate interface. Just before the attack, no one was resolving the IP address. Then, suddenly, the number of computers resolving the domain in DNS spiked to more than 78,000 before dropping back down to zero.

Contrast the hailstorm attack to a snowshoe spam campaign, also shown in Figure 18, where attackers attempt to fly under the radar of volume-based detection solutions. The number of DNS lookups is steady, but there are only about 25 queries per hour. These low-volume attacks allow adversaries to quietly distribute spam from a large swath of IP addresses.

Even though these spam attacks operate differently, they do have things in common. Through either approach, adversaries can:

- Evade a bad reputation by sending from clean IPs and domains
- Emulate marketing mail with professional content and subscription management
- Use well-configured email systems rather than sloppy scripts or spam bots
- Properly set up forward-confirmed reverse DNS and Send Policy Framework (SPF) records

Figure 18 Comparison of Hailstorm and Snowshoe Spam Attacks



Source: Cisco Investigate

SHARE

Adversaries can also impair content detection by mutating text and cycling through file types. (For more details on how cybercriminals evolve their threats to evade defenders, see the “Time to Evolve” section on [page 34](#).) For more information on how they experiment with malicious file attachments for spam, see the previous section.

Figure 19 shows top threat outbreak alerts; this is an overview of the spam and phishing messages that we observed adversaries frequently updating in 2016 in order to bypass email security checks and rules. It is important to know what types of email threats are the most prevalent so that you can avoid being duped by these malicious messages.

Figure 19 Top Threat Outbreak Alerts

Version	Publication Identifier	Publication Name and URL	Message Summary	Attachment File Type	Language	Last Publication Date
96 [REDACTED]	35656	RuleID4626	Invoice, Payment	.zip	German, English	04/25/16
87 [REDACTED]	34577	RuleID10277	Purchase Order	.zip	German, English	06/02/16
82 [REDACTED]	36916	RuleID4400KVR	Purchase Order	.zip	English	02/01/16
74 [REDACTED]	38971	RuleID15448	Purchase Order, Payment, Receipt	.zip, .gz	English	08/08/16
72 [REDACTED]	41513	RuleID18688	Order, Payment, Seminar	.zip	English	09/01/16
70 [REDACTED]	40056	RuleID6396	Purchase Order, Payment, Receipt	.rar	English	06/07/16
66 [REDACTED]	34796	RuleID5118	Product Order, Payment	.zip	German, English	09/29/16
64 [REDACTED]	39317	RuleID4626 (cont)	Invoice, Payment, Shipping	.zip	English, German, Spanish	01/28/16
64 [REDACTED]	36917	RuleID4961KVR	Confirmation, Payment/Transfer, Order, Shipping	.zip	English	07/08/16
63 [REDACTED]	37179	RuleID13288	Delivery Notice, Court Appearance, Ticket Invoice	.zip	English, Spanish	07/21/16
61 [REDACTED]	38095	RuleID858KVR	Shipping, Quote, Payment	.zip	English	08/01/16
58 [REDACTED]	39150	RuleID4961KVR	Quote Request, Product Order	.zip	English, German, Multiple Languages	01/25/16
47 [REDACTED]	41886	RuleID4961	Transfer, Shipping, Invoice	.zip	English, German, Spanish	02/22/16

Source: Cisco Security Research

 Download the 2017 graphics at: www.cisco.com/go/acr2017graphics

Reconnaissance

Weaponization

Delivery

Installation

Once the threat is in position, it installs a back door on a target's system, providing adversaries with persistent access.

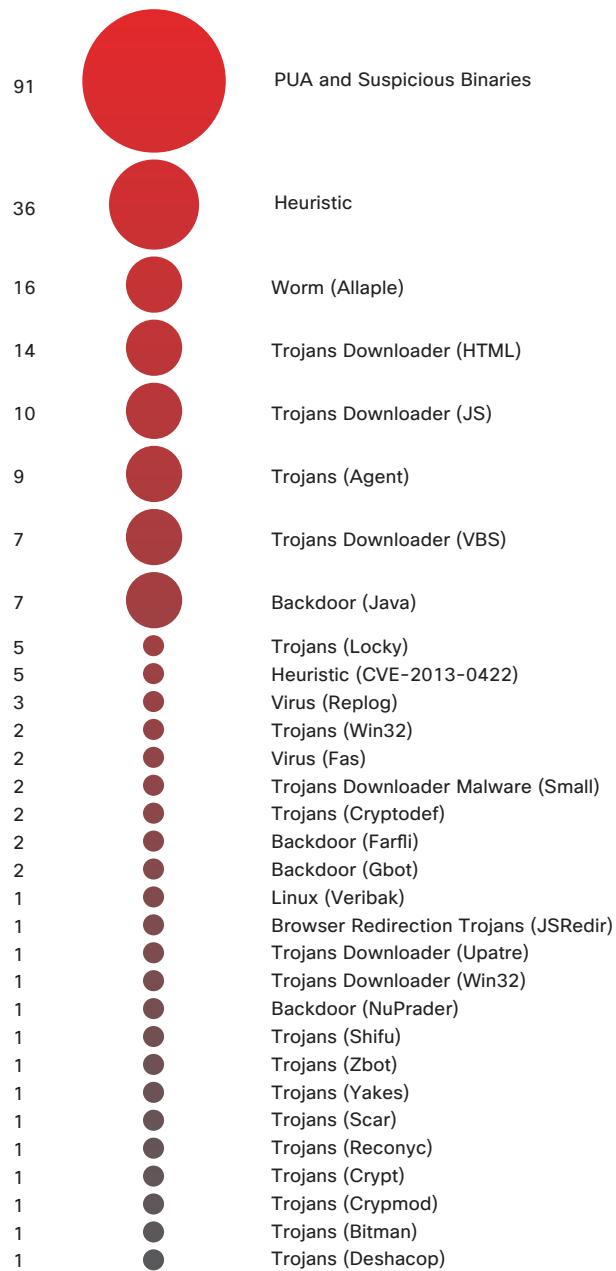
Web Attack Methods: “Long Tail” Snapshot Reveals Threats That Users Can Easily Avoid

The so-called long tail of the web attack methods spectrum (Figure 20) includes a collection of lower-volume malware types that are employed at a later stage in the attack chain: installation. In this phase, the threat that has been delivered—a banking Trojan, a virus, a downloader, or some other exploit—installs a back door in the target system, providing adversaries with persistent access and the opportunity to exfiltrate data, launch ransomware attacks, and engage in other mischief.

The threats listed in Figure 20 are samples of malware signatures found outside the top 50 most commonly observed malware types. The long tail of web attack methods is, essentially, a snapshot of threats that are quietly at work on a machine or system after a successful attack. Many of these infections were first spawned by an encounter with malicious adware or exposure to a well-crafted phishing scam. These are situations that users can often easily avoid or quickly remediate.

SHARE     

Figure 20 Sample of Observed Lower-Volume Malware



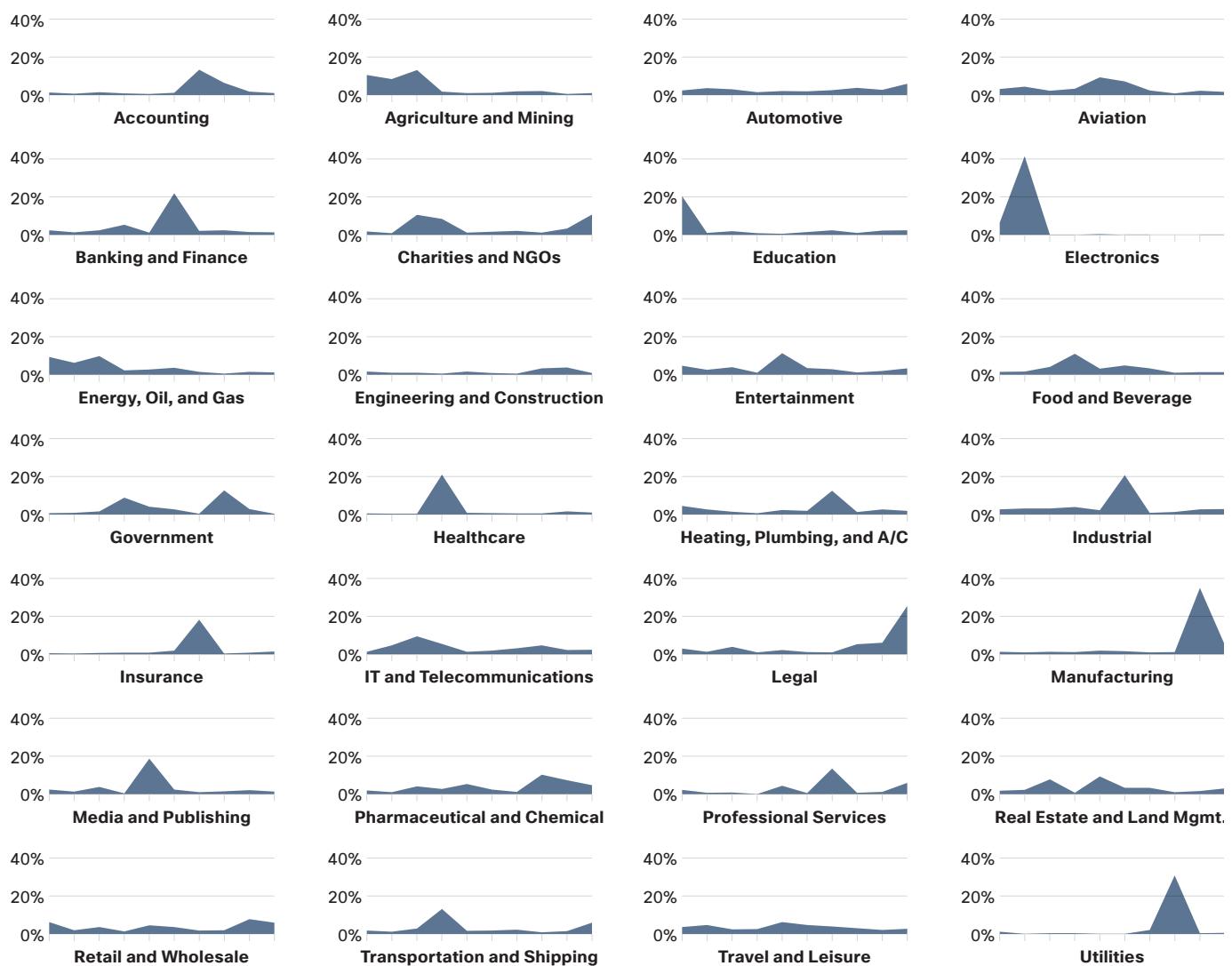
Source: Cisco Security Research

Vertical Risk of Malware Encounters: Attackers See Value Across the Board

In the *Cisco 2016 Midyear Cybersecurity Report*, a key message about the risk of malware was that “no vertical is safe.” Judging from our researchers’ periodic examination of attack traffic (“block rates”) and “normal” or expected traffic by industry, this message held true in the latter half of the year.

In looking at verticals and their block rates over time (Figure 21), we see that, at some point over the course of several months, every industry has been subject to attack traffic and at varying levels. It’s clear that as attacks rise and fall, they affect different verticals at different times—but none are spared.

Figure 21 Percentage of Monthly Vertical Block Rates



Source: Cisco Security Research

SHARE

Regional Overview of Web Block Activity

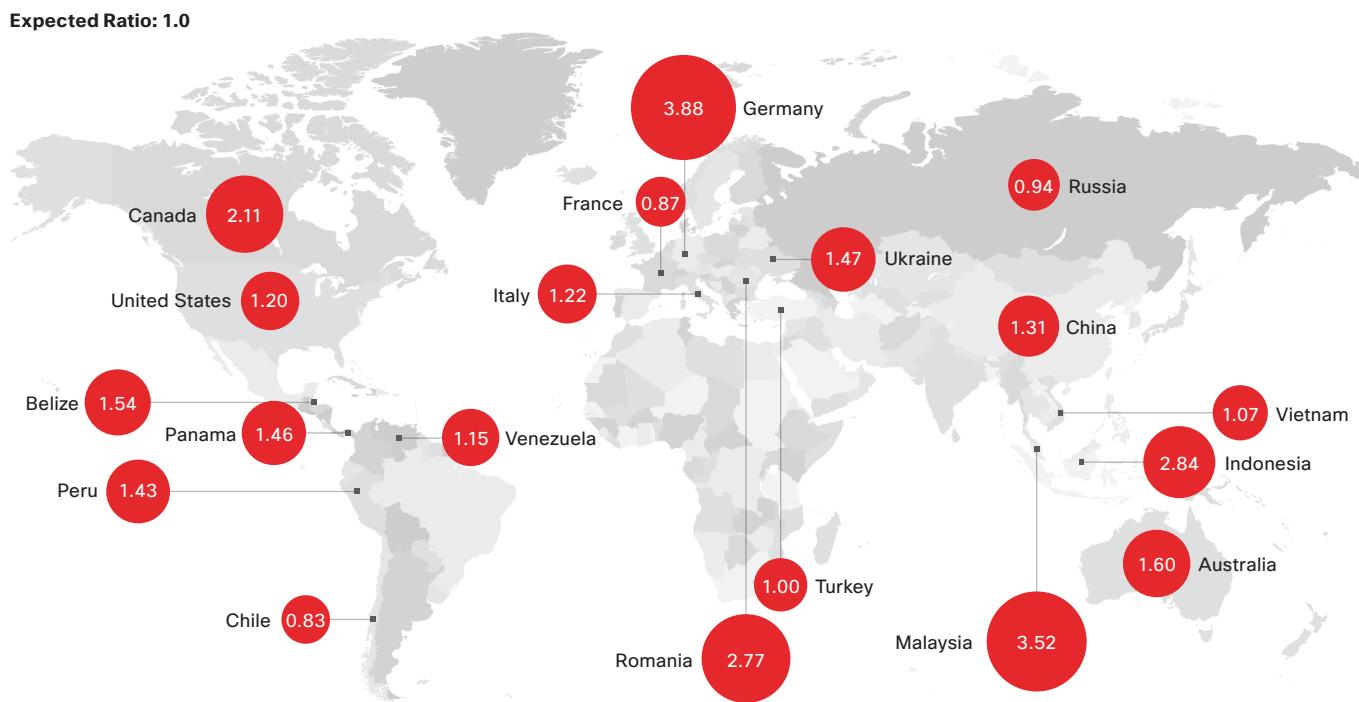
Adversaries frequently shift their base of operation, searching for weak infrastructure from which they can launch their campaigns. By examining overall Internet traffic volume and block activity, Cisco threat researchers can offer insight on where malware is originating.

As Figure 22 shows, traffic from the United States edged up slightly from the block rates seen in the *Cisco 2016 Midyear Cybersecurity Report*. The United States

houses the far greater share of blocks, but this should be considered a function of the country's far greater share of online traffic. In addition, the United States is one of the world's largest targets of malware attacks.

The takeaway for security professionals: Much like the vertical web block activity, the regional web block activity shows that malware traffic is a global problem.

Figure 22 Web Blocks by Country



Source: Cisco Security Research

SHARE

Time to Detection: An Essential Metric for Measuring Defenders' Progress

Cisco is continually refining our approach to measuring TTD so that we can ensure we are tracking and reporting the most accurate estimate of our median TTD. Recent adjustments to our approach have increased our visibility into files that were categorized as “unknown” when first seen and then later identified as “known bad” after continuous analysis and global observation. With a more holistic view of data, we are better able to pinpoint when a threat first emerged and exactly how long it took for security teams to determine that it was a threat.

This new insight helped us to determine that our median TTD was 39 hours in November 2015. (See Figure 23.) By January 2016, we had reduced the median TTD to 6.9 hours. After collecting and analyzing data for October 2016, our threat researchers determined that Cisco products had achieved a median TTD of 14 hours for the period from November 2015 to October 2016. (Note: The median TTD figure for 2016 is the average of the medians for the period observed.)

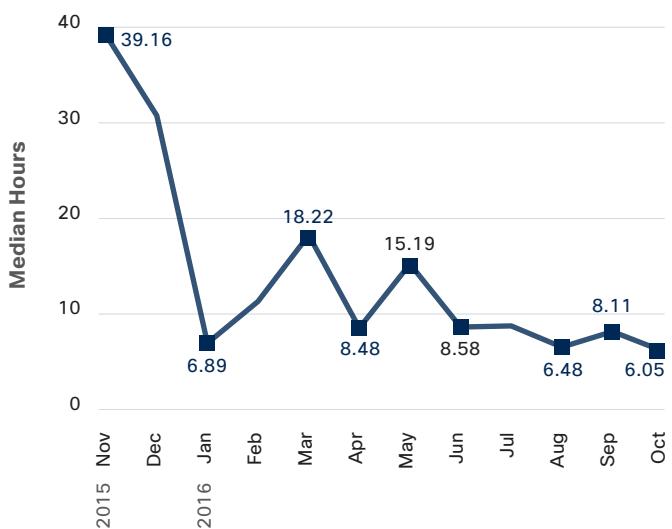
The median TTD fluctuated throughout 2016 but trended downward overall. Increases in the median TTD indicate times when adversaries launched a wave of new threats. The subsequent decreases reflect periods where defenders gained the upper hand and could identify known threats quickly.

Figure 23 also shows that the median TTD was about 15 hours by the end of April 2016, which is greater than the 13-hour figure we reported in the *Cisco 2016 Midyear Cybersecurity Report*.¹⁴ That 15-hour figure is based on data collected from November 2015 through April 2016. It was not derived using our modified approach to analyzing more detailed retrospective information about files. Using the new midyear TTD figure, we can report that TTD declined to about 9 hours for the period from May through October 2016.

Reviewing retrospective data is important not only for determining a more accurate measure of our median TTD, but also for studying how threats evolve over time. Numerous threats in the landscape are particularly evasive and can take a long time to identify even though they are known to the security community.

Adversaries will evolve certain malware families to avoid detection and increase their time to operate. This tactic hinders defenders’ progress in gaining, and then maintaining, an edge in detecting many types of known threats. (For more on this topic, see “Time to Evolve: For Some Threats, Change Is Constant,” [page 34](#)). However, the fact that cybercriminals are evolving their threats frequently and rapidly indicates that they are facing intense and constant pressure to find ways to keep their threats operating and profitable.

Figure 23 Median TTD by Month



Source: Cisco Security Research

Cisco defines “time to detection,” or TTD, as the window of time between a compromise and the detection of a threat. We determine this time window using opt-in security telemetry gathered from Cisco security products deployed around the globe. Using our global visibility and a continuous analytics model, we are able to measure from the moment malicious code runs on an endpoint to the time it is determined to be a threat for all malicious code that was unclassified at the time of encounter.

¹⁴ Cisco 2016 Midyear Cybersecurity Report: http://www.cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html.

Time to Evolve: For Some Threats, Change Is Constant

Cybercriminals use various obfuscation techniques to keep their malware strong and profitable. Two common methods they employ are evolving their payload delivery types and quickly generating new files (defeating hash-only detection methods). Our researchers closely examined how adversaries have used these two strategies to help six well-known malware families—Locky, Cerber, Nemucod, Adwind RAT, Kryptik, and Dridex—evade detection and continue compromising users and systems.

Through our analysis, we sought to measure the “time to evolve” (TTE): the time it takes adversaries to change the way specific malware is delivered and the length of time between each change in tactics. We analyzed web attack data from different Cisco sources—specifically, web proxy data, cloud and endpoint advanced malware products, and composite antimalware engines.

Our researchers looked for changes in file extensions delivering the malware and the file content (or MIME) type as defined by a user’s system. We determined that each malware family has a unique pattern of evolution. For each family, we examined the patterns in both web and email delivery methods. We also tracked the ages of unique hashes associated with each malware family to determine how quickly adversaries are creating new files (and thus, new hashes).

Through our research, we learned that:

- Ransomware families appear to have a similar rotation of new binaries. However, Locky uses more file extension and MIME combinations to deliver its payload.
- Some malware families employ only a handful of file delivery methods. Others use 10 or more. Adversaries tend to use effective binaries over long periods. In other cases, files pop up and then drop off quickly, indicating that the malware authors are under pressure to switch tactics.
- The Adwind RAT and Kryptik malware families have a higher median TTD. (For more on TTD, see [page 33](#).) We also see a greater mix of file ages for these families. This suggests that adversaries reuse effective binaries that they know are difficult to detect.
- Looking at the file ages for the Dridex malware family, it appears that the shadow economy may be abandoning use of this once-popular banking Trojan. In late 2016, detection volume for Dridex declined, as did the development of new binaries to deliver this malware. This trend suggests that the malware’s authors no longer see value in evolving this threat—or that they have found a new way to package the malware that has made it harder to detect.

TTE and TTD

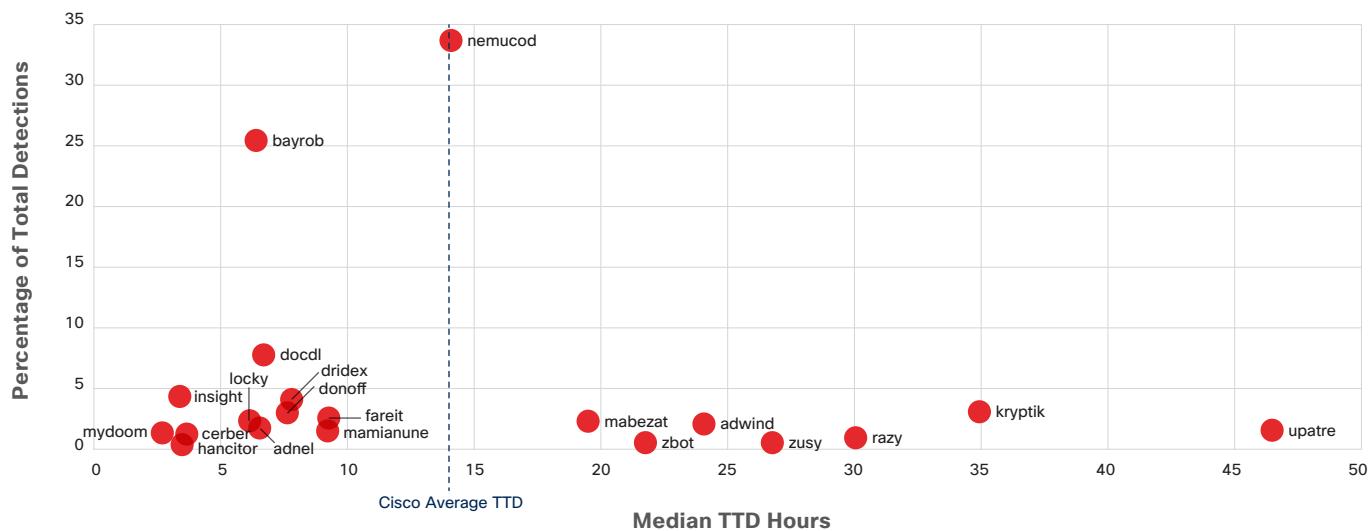
The six malware families we analyzed in our TTE study are listed in Figure 24. The chart depicts the median TTD for the top 20 malware families (by detection count) that our researchers observed from November 2015 to November 2016. Our average median TTD for that period was about 14 hours. (For details on how we calculate TTD, see [page 33](#).)

Many of the malware families that Cisco products are detecting within the median TTD are industrialized threats that spread quickly and are therefore more prevalent. Cerber and Locky, which are both types of ransomware, are examples.

Old and pervasive threats that adversaries don't bother to evolve much, or at all, are also typically detected below the median TTD. Examples include malware families like Bayrob (botnet malware), Mydoom (a computer worm that affects Microsoft Windows), and Dridex (the banking Trojan).

In the following sections, we present research highlights on TTE and TTD for the Locky, Nemucod, Adwind RAT, and Kryptik malware families. Detailed findings for Cerber and Dridex are included in the Appendix on [page 78](#).

Figure 24 TTD Medians of Top Malware Families (Top 20 Families by Detection Count)



Source: Cisco Security Research

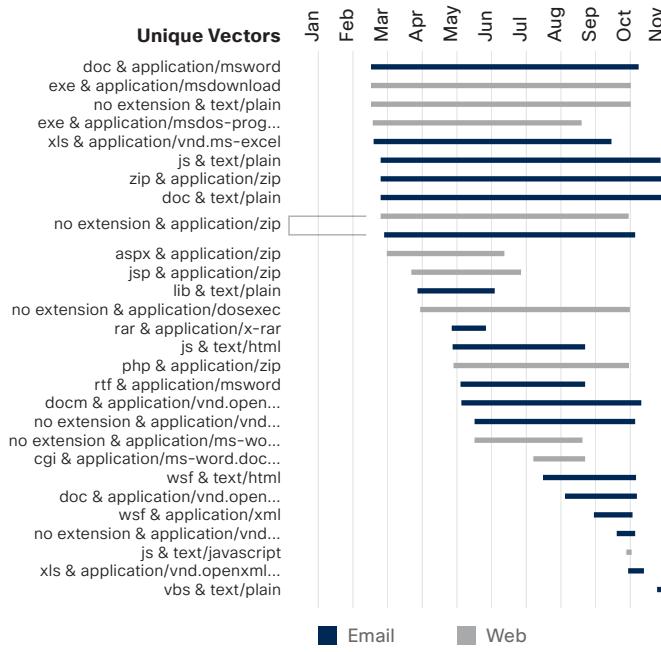
SHARE

TTE Analysis: Locky

Through our TTE research, we learned that Locky and Cerber employ a limited number of file extension and MIME combinations to deliver malware through the web or by email. (See Figure 25.) We observed several combinations that included file content types related to Microsoft Word (msdownload, ms-word). However, the associated file extensions (.exe and .cgi) did not point back to a Word file. We also identified content types that pointed to malicious .zip files.

Both Locky and Cerber also appear to use new binaries frequently as an attempt to evade file-based detection. File ages for the Locky malware family are shown in Figure 26.

Figure 25 File Extension and MIME Combinations for the Family of Threats and Indicators That Lead to and Include the Locky Payload (Web and Email Vectors)



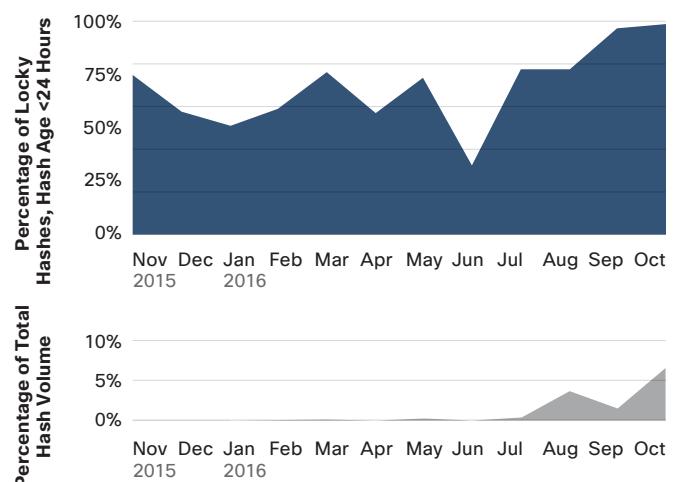
Source: Cisco Security Research

SHARE

The top half of the chart depicts the ages of files that were observed during a specific month. The bottom portion of the chart shows monthly changes in the volume of Locky-related hashes, both new and previously observed files.

In Figure 26, also note the decline in volume in June as well as the distribution of file ages. The Necurs botnet, which was known to deliver Locky, was taken down in June. This likely sidelined the malware authors' efforts to keep the malware fresh during that month. However, it's clear that they recovered quickly. By July, the malware had returned to its more standard mix of file ages with the majority (74 percent) being less than a day old when first detected.

Figure 26 Hash Ages for the Locky Malware Family and Percent of Total Hash Volume Observed Per Month

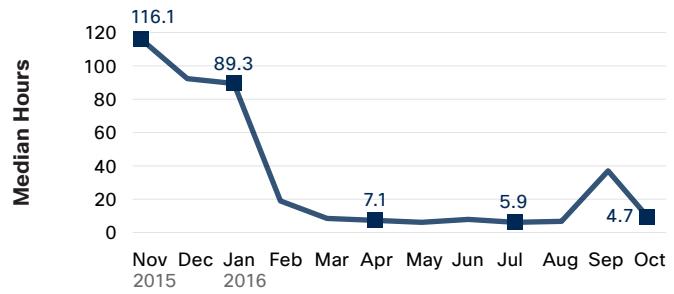


Source: Cisco Security Research

The rapid cycling of binaries for this ransomware is not surprising. Instances of Locky and Cerber are often detected either on the same day they are introduced or within 1 to 2 days after, making it imperative for adversaries to evolve these threats continually if they want them to remain active and effective. (Figure 24, discussed earlier, shows that Cisco products detected both Locky and Cerber ransomware within the median TTD in 2016.)

Figure 27 shows the median TTD for Locky ransomware, which declined dramatically from about 116 hours in November 2015 to just under 5 hours in October 2016.

Figure 27 TTD for the Locky Malware Family

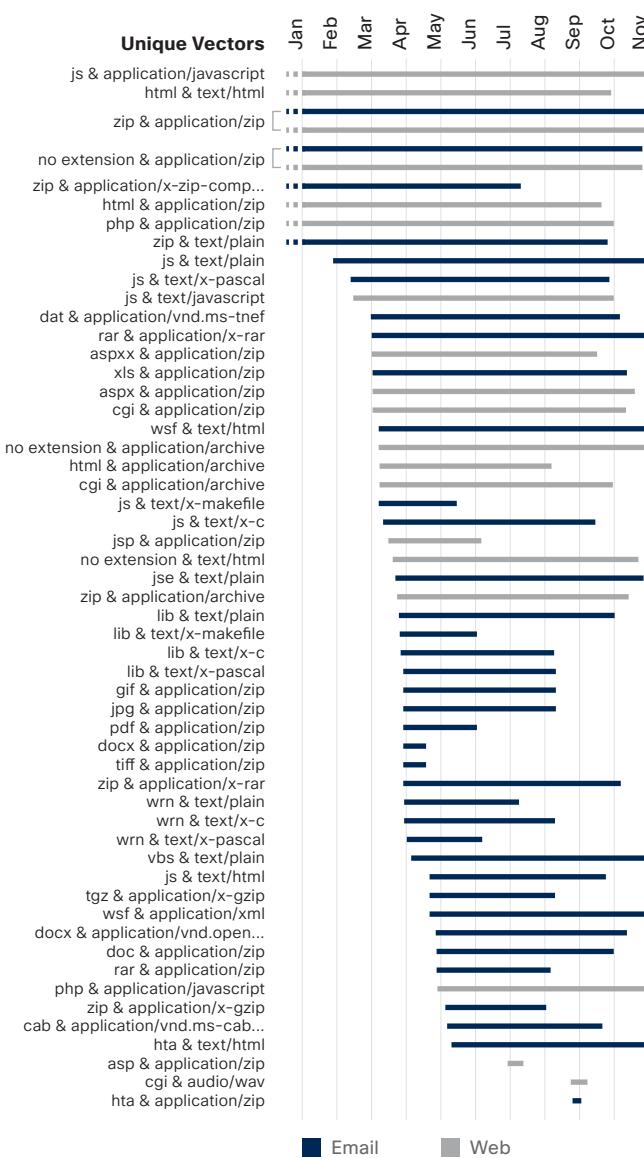


Source: Cisco Security Research

TTE Analysis: Nemucod

In 2016, Nemucod was the most frequently detected malware among the top 20 families shown in [Figure 24](#). Adversaries use this downloader malware to distribute ransomware and other threats, such as backdoor Trojans that facilitate click fraud. Some variants of Nemucod also serve as engines for delivering the Nemucod malware payload.

Figure 28 File Extension and MIME Combinations for Nemucod (Web and Email Vectors)



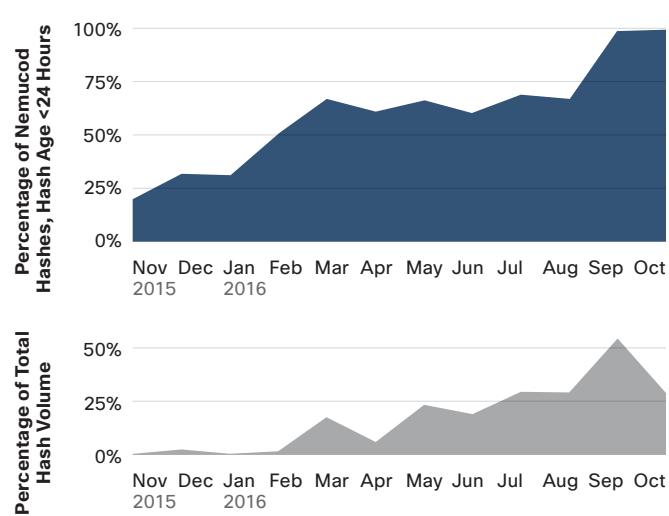
Source: Cisco Security Research

One reason Nemucod malware was so prevalent in 2016, according to our threat researchers, is that its authors frequently evolved this threat. Cisco identified more than 15 file extension and MIME combinations associated with the Nemucod family that were used to deliver malware through the web. Many more combinations were used to deliver the threat to users through email (Figure 28).

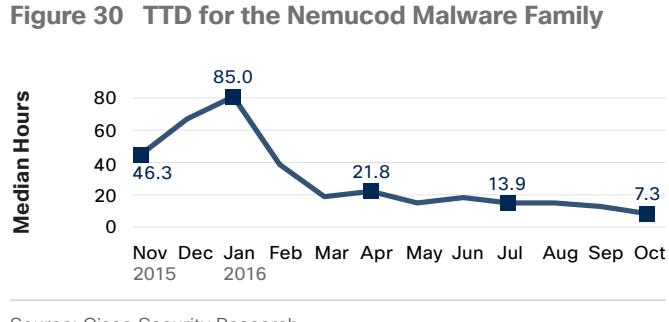
Several file extension and MIME combinations (web and email) were designed to point users to malicious .zip files or archives. Adversaries also reused many combinations during the months we observed.

As Figure 29 shows, many Nemucod hashes are less than 2 days old when they are detected. In September and October 2016, almost every binary related to the Nemucod family that was blocked was less than a day old.

Figure 29 Hash Ages for the Nemucod Malware Family and Percent of Total Hash Volume Observed Per Month



Source: Cisco Security Research



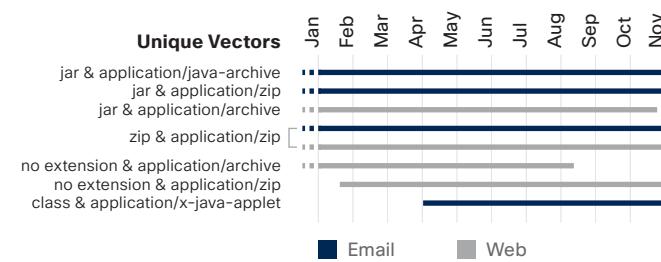
Attacker Behavior

TTE Analysis: Adwind RAT

Cisco threat researchers found that Adwind RAT (remote access Trojan) malware is delivered through file extension and MIME combinations that include .zip or .jar files. This is true whether the malware is being delivered through the email or web attack vector. (See Figure 31.)

Adwind RAT used a wide range of hash ages throughout most of the period observed in 2016, except during September and October, when most files seen were 1 to 2 days old (Figure 32).

Figure 31 File Extension and MIME Combinations for Adwind RAT (Web and Email Vectors)

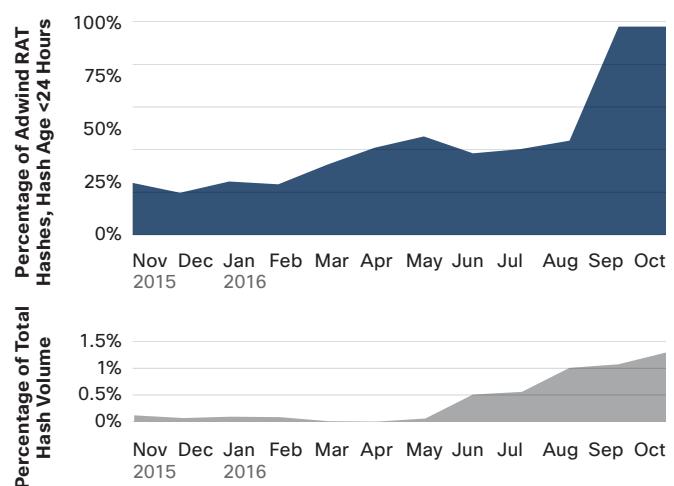


Source: Cisco Security Research

Download the 2017 graphics at: www.cisco.com/go/acr2017graphics

We also found that the median TTD for Adwind RAT is consistently higher than the median TTD for other malware families we analyzed (Figure 33). The malware's authors have apparently developed hard-to-detect delivery mechanisms that keep Adwind RAT successful. Therefore, they don't need to rotate through new hashes as frequently or as rapidly as the actors behind other malware families do. The Adwind Trojan is also known by other names, such as JSocket and AlienSpy.

Figure 32 Hash Ages for the Adwind RAT Malware Family and Percent of Total Hash Volume Observed Per Month



Source: Cisco Security Research

Figure 33 TTD for the Adwind RAT Malware Family



Source: Cisco Security Research

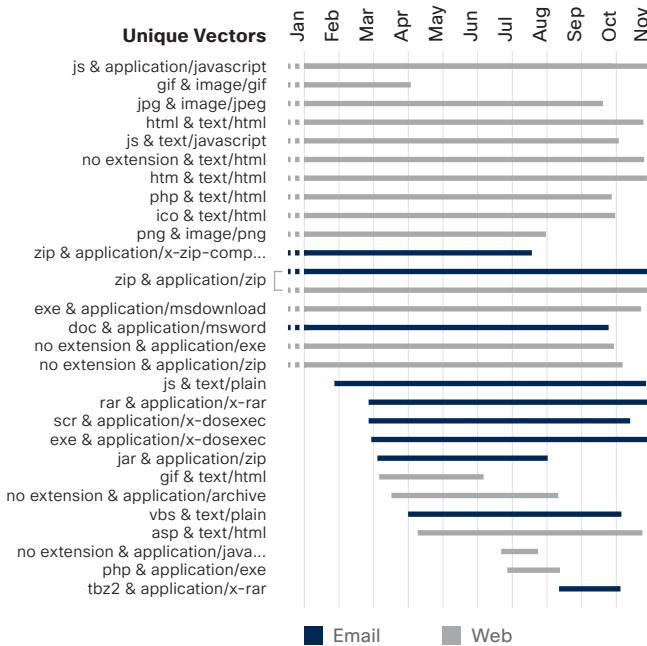
TTE Analysis: Kryptik

Kryptik, like Adwind RAT malware, had a median TTD that was consistently higher (about 20 hours) than other malware families Cisco analyzed for the TTE study from November 2015 through October 2016 (Figure 36). However, by October, Cisco products had reduced the median TTD window for Kryptik malware to less than 9 hours (Figure 36).

The Kryptik malware family also used a wider range of hash ages than the other malware families we analyzed, particularly during the first half of 2016. The ability of Kryptik's authors to rely on older hashes for so long indicates that defenders had trouble detecting this malware type.

During the period that we observed, Kryptik's authors employed a wide range of payload delivery methods through the web attack vector. The authors used JavaScript files and archive files such as .zip files in file extension and MIME combinations for both web and email. (See Figure 34.) Some of the combinations date back to 2011.

Figure 34 File Extension and MIME Combinations for Kryptik (Web and Email Vectors)



Source: Cisco Security Research

In our analysis of the six malware families, we find that adversaries must shift tactics frequently to take advantage of the small window of time during which their threats can operate successfully. These adjustments indicate that defenders are getting better at detecting known malware quickly, even after a threat has evolved. Attackers are under pressure to find new ways to avoid detection and keep their campaigns profitable.

In this complex landscape of rapid evolution, where all malware families behave differently, human expertise and point solutions are not enough to identify and respond quickly to threats. An integrated security architecture that provides real-time insight into threats, along with automated detection and defense, is essential for improving TTD and ensuring swift remediation when infections occur.

Figure 35 Hash Ages for the Kryptik Malware Family and Percent of Total Hash Volume Observed Per Month

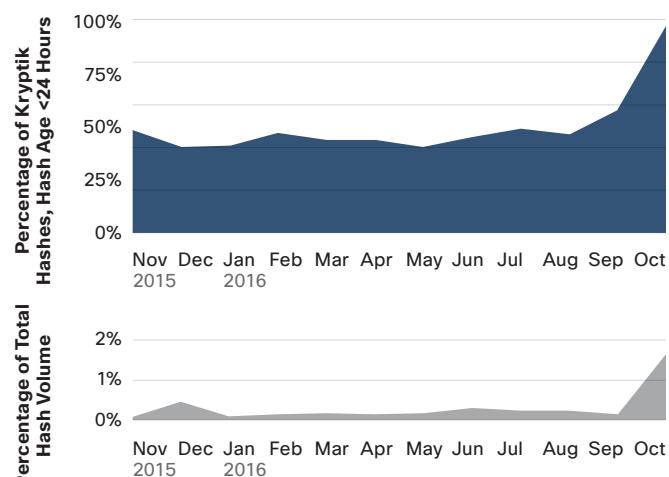
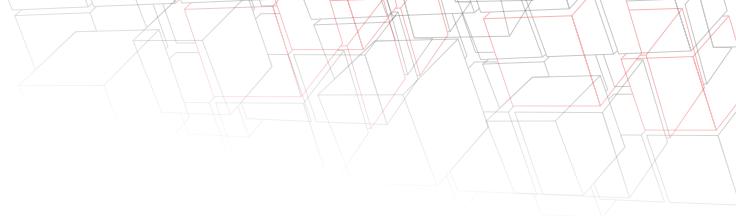


Figure 36 TTD for Kryptik Malware Family



Defender Behavior



Defender Behavior

Vulnerabilities on the Decline in 2016

In the second half of 2016, vendor-disclosed vulnerabilities dropped significantly from 2015, according to our research (Figure 37). The [National Vulnerability Database](#) shows a similar decline. The reasons for the drop in disclosed vulnerability advisories are not entirely clear.

It should be noted that 2015 was an unusually active year for vulnerabilities, so the 2016 numbers may reflect a normal pace of vulnerability advisories. From January to October 2015, total alerts reached 7602. During the same time period in 2016, total alerts reached 6380; during this period in 2014, total alerts were 6272.

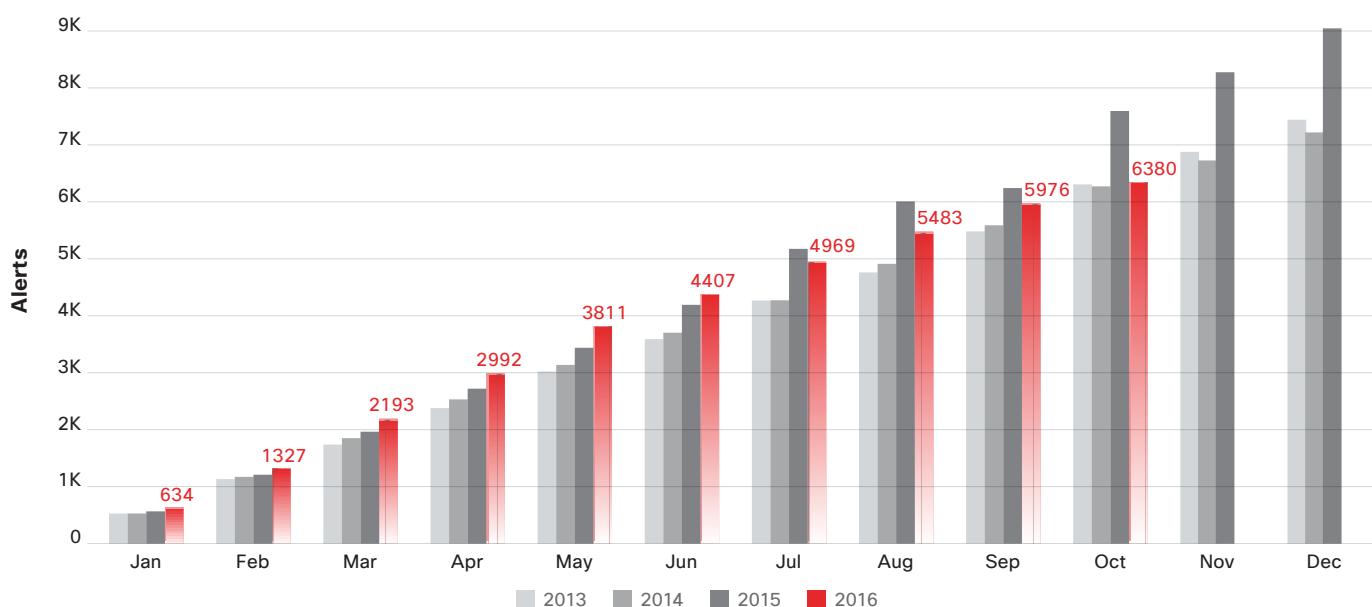
The high number of vulnerability reports in 2015 may indicate that vendors were looking more closely at existing products and code, more carefully implementing secure development lifecycle (SDL) practices, and identifying vulnerabilities and subsequently fixing them. The decline in reported vulnerabilities may indicate that these efforts are

paying off. That is, vendors are now focusing on identifying vulnerabilities and correcting them before products reach the market.

In 2016, Apple was the vendor showing the most dramatic decline in vulnerabilities: The company reported 705 vulnerabilities in 2015, and 324 vulnerabilities in 2016 (a 54 percent decline). Similarly, Cisco reported 488 vulnerabilities in 2015, and 310 in 2016 (a 36 percent decline).

A concern among security researchers is that “vulnerability fatigue” may be setting in among security professionals. In recent months, there has not been a major vulnerability announcement that sent shock waves through the industry, as Heartbleed did in 2014. In fact, the hype around “named” vulnerabilities such as Heartbleed and the increase in 2015 likely contributed to the level of fatigue—or, at least, to less interest in reporting vulnerabilities.

Figure 37 Cumulative Annual Alert Totals



Source: Cisco Security Research

Figure 38 Critical Vulnerability Advisories by Vendor and Type

Source: National Vulnerability Database (NVD)

Cisco is now using severity/impact ratings (SIRs), in which the rating levels are “critical,” “high,” “medium,” and “low.” The ratings reflect a simplified prioritization of scores from the Common Vulnerability Scoring System (CVSS). In addition, Cisco has adopted CVSS v3.0, the successor to CVSS v2.0. Because of this change, some vulnerabilities may have higher scores than before, so security professionals may see a small increase in vulnerabilities that are rated “critical” and “high,” instead of “medium” and “low.” For more information about this scoring change, read the Cisco Security blog post, [The Evolution of Scoring Security Vulnerabilities: The Sequel](#).

In the Cisco 2017 Security Capabilities Benchmark Study ([page 49](#)), security professionals indicated a slight decrease in their agreement about security operationalization. This decrease may be connected to “fatigue” about the need to continually implement upgrades and patches. For example, in 2016, 53 percent of security professionals said they strongly agreed that they review and improve security practices regularly, formally, and strategically; in 2014 and 2015, 56 percent strongly agreed.

Of course, a decline in vulnerabilities should not lead to overconfidence about the threat landscape: No one should adopt the mindset that attention to threats can lapse, even in the absence of high-profile vulnerabilities.

As we’ve advised in past reports, security professionals should make a concerted effort to prioritize patches. If a lack of staffing and other resources prevents the timely installation of all available patches, evaluate which ones are most critical to network safety, and place those at the top of the to-do list.

 Download the 2017 graphics at: www.cisco.com/go/acr2017graphics

Figure 39 Selected Critical Vulnerability Advisories

Advisory Title	Date Issued
Adobe Acrobat and Acrobat Reader memory corruption code execution vulnerability	Jul 28, 2016
Adobe Acrobat and Acrobat Reader memory corruption remote code execution vulnerability	Jul 28, 2016
Adobe Acrobat and Acrobat Reader memory corruption vulnerability	Jul 21, 2016
Adobe Acrobat and Acrobat Reader integer overflow vulnerability	May 23, 2016
Adobe Acrobat and Acrobat Reader memory corruption remote code execution vulnerability	Feb 08, 2016
Adobe Acrobat and Acrobat Reader memory corruption vulnerability	Jul 28, 2016
Adobe Acrobat and Acrobat Reader memory corruption vulnerability	Jul 18, 2016
Adobe Acrobat and Acrobat Reader memory corruption vulnerability	Jun 23, 2016
Adobe Acrobat and Acrobat Reader memory corruption vulnerability	May 24, 2016
Adobe Acrobat and Acrobat Reader memory corruption vulnerability	May 23, 2016

Source: Cisco Security Research

The advisories listed above are selected 2016 critical-rated vulnerabilities that were reported by multiple sources to have exploit code publicly available or to be actively exploited in the wild.

Server and Client Vulnerabilities

As discussed in the [Cisco 2016 Midyear Cybersecurity Report](#), adversaries are finding space and time to operate within server-side solutions. By launching attacks within server software, they can potentially gain control of more network resources, or move laterally among other critical solutions.

Cisco researchers have tracked client and server vulnerabilities by vendor (Figure 40).

Figure 40 Client-Server Vulnerabilities Breakdown, 2015–2016



Source: National Vulnerability Database

Figure 41 Vulnerabilities Found in Middleware Libraries



Source: Cisco Security Research

SHARE

Middleware: Adversaries See Opportunity in Unpatched Software

In the [Cisco 2016 Midyear Cybersecurity Report](#), we shared data about attacks against server-side systems. In 2017, middleware, which connects platforms or applications, is poised to attract attackers seeking places to operate where defenders are slow to react or recognize a threat.

Cisco researchers, while looking for vulnerabilities in third-party software, discovered an average of 14 new vulnerabilities in software per month. Most of those vulnerabilities (62) were attributable to the use of middleware. Of those 62 vulnerabilities, 20 were found within code that handles PDFs; 12 were found in code that handles images; 10 were found in code for common office productivity solutions; nine were found in code for compression; and 11 were found in other libraries (Figure 41).

Vulnerabilities in middleware pose a unique security threat because their libraries are not usually updated as rapidly as software that is more client-facing—that is, software that users interact with directly on a day-to-day basis, such as productivity solutions. Middleware libraries may be left out of software audits, so vulnerabilities remain in place.

Organizations may gamble on middleware being safe and may place greater attention on updating high-profile solutions. But they can lose the bet that adversaries won't seek entry to networks through these low-profile pathways. Middleware thus becomes a security blind spot for defenders and an opportunity for attackers.

The challenge of updating middleware libraries closely relates to the open-source software problem (discussed in the [Cisco 2015 Midyear Security Report](#)), since many middleware solutions come from open-source developers. (However, the problem at hand can affect both open-source and proprietary middleware developers.) Therefore, middleware libraries may rely on many developers to keep them updated. On the list of tasks that an overtaxed IT or security team needs to manage, middleware library updates may not be a top priority, but they should be given greater attention.

What is the potential impact of a middleware vulnerability that is exploited by adversaries? Given the connections between middleware and other crucial systems, such as email or messaging, an attacker could move laterally into these systems and send phishing messages or spam. Or attackers could masquerade as authorized users and abuse trust relationships between users to gain further access.

To avoid becoming the victim of an attack launched through a middleware vulnerability, you should:

- Actively maintain a list of known dependencies and libraries in the applications you use
- Actively monitor the security of these applications, and mitigate risks as much as possible
- Insert a service-level agreement in contracts with software vendors for providing patches in a timely manner
- Routinely audit and review software dependencies and library use
- Ask software vendors for details on how they maintain and test their products

In short: Delays in patching increase the operational space for attackers and allow them more time to gain control of critical systems. In the next section, we discuss this impact and trends in the patching of common productivity solutions such as web browsers.

Time to Patch: Closing the Recovery Time Frame

Many users do not download and install patches in a timely manner. Adversaries can use these unpatched vulnerabilities to gain entry to networks. In our latest research, we find that the key to encouraging users to download and install patches may rest in the cadence of software updates from vendors.

A security patch release is a clear indication to attackers that there is a vulnerability worth exploiting. Although sophisticated attackers have likely been exploiting the vulnerabilities for some time, the notification of a patch tells many others that it's open season on the earlier versions.

When software vendors release new versions on a regular schedule, users become conditioned to downloading and installing updates. Conversely, when vendor upgrade releases are erratic, users are less likely to install them. They will continue to operate outdated solutions that may contain exploitable vulnerabilities.

Other behaviors that affect the upgrade cycle include:

- How disruptive the reminder experience is
- How easy it is to opt out
- How often the software is used

There are varying windows of time in which users are likely to install an upgrade when it is released by the vendor. Our researchers looked at the installations of software on the endpoints used by our customers. Their software fell into three categories:

- **New versions:** The endpoint ran the newest available version of the software
- **Recent versions:** The endpoint ran one of the previous three versions of the software, but not the newest
- **Old versions:** The endpoint ran software that was more than three versions behind the current release

As an example, if a software vendor released version 28 on January 1, 2017, version 28 would be new; version 26 would be recent; and version 23 would be old. (The figures on the next page contain callouts of the weekly time periods where one or more versions of the software were released.)

In examining users of Adobe Flash (Figure 42), we found that, within the first week of an update release, nearly 80 percent of users install the software's latest version. In other words, it takes only about one week for the user population to get up to speed with the latest version. This one-week "recovery" period represents hackers' window of opportunity.

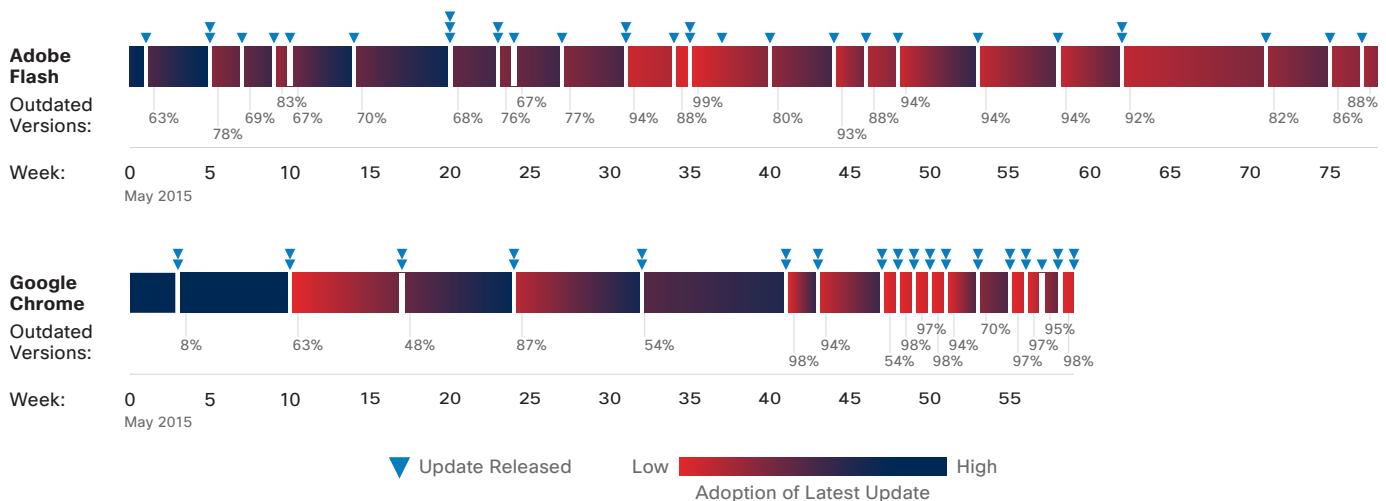
In looking at late Q4 2015 in the Adobe Flash graphic, we see a sharp drop in the number of users on the newest version of the solution. In the time period we examined, Adobe released five versions of Flash in quick succession, representing a mix of functionality additions, bug fixes, and security updates. Such a flurry of updates may confuse users. They may question whether they need to download so many updates; they can become fatigued by the number of upgrade notifications; and they may think they've already downloaded a crucial update and can ignore new notifications. No matter what drives their lack of interest in installing an update, it's bad news for defenders.

In examining upgrades for the Google Chrome web browser, we see a different pattern. It reflects a regular cadence of upgrades, as well as a strong opt-out policy that makes it difficult for users to ignore update notifications. As seen in Figure 42, endpoints running the newest version stay relatively steady over the course of many weeks.

The Chrome data shows that users recover relatively quickly. In the case of regular updates, one week is roughly the recovery timeline. In one span of 9 weeks running through Q2 and Q3 of 2016, however, there were seven updates. During this time the population recovered, but upgrade fatigue began to set in. The percentage of users staying with an older version steadily climbs despite the majority of the population recovering.

Mozilla's Firefox browser also offers updates on a regular schedule, but the recovery period after an update is released appears to take as long as a month. That is, users do not download and install updates as frequently as Chrome users do. One reason may be that some users might not use the browser regularly and therefore aren't seeing and downloading updates. (See Figure 43 on next page.)

Figure 42 Time to Patch for Adobe Flash and Google Chrome



Source: Cisco Security Research

SHARE

We found that Firefox updated its versions about every other week, with the frequency of updates increasing over the course of the observation period. This increase in frequency is reflected in the growth of old Firefox versions within the population. The recovery time is roughly 1.5 weeks, but the times overlap. The population that tries to stay current drops to as little as 30 percent of the user base. At some point, two-thirds of the users have resorted to simply running the browser more than four versions behind the most current one. So, although Firefox is rapidly addressing issues and fixing bugs, the user base is not updating and restarting on the same frequency.

For software, the level of use seems to also be an indicator of its vulnerability. When users do not access software often and therefore aren't aware of the need to patch and upgrade it, the ignored software provides space and time for attackers to operate.

We can see this in the research on Microsoft Silverlight, which shows a recovery period of as long as 2 months

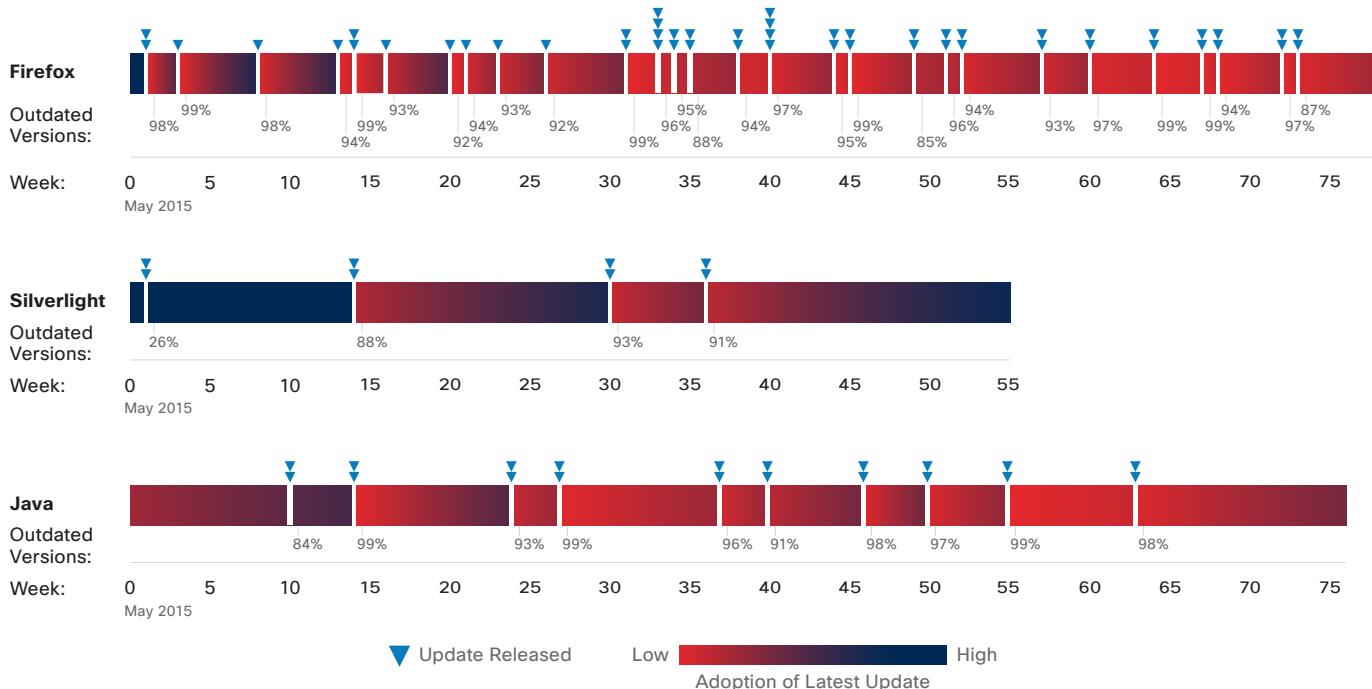
for users to install upgrades after a release. At one point, there were two releases within 5 weeks, which affected the user population for more than 3 months, as can be seen between Q4 of 2015 and Q1 of 2016.

Microsoft announced the end of life of Silverlight in 2012, although patches and bug fixes are still being released. However, it poses the same problem that Internet Explorer does: Outdated and unpatched software invites attackers to easily exploit it.

The recovery period for Java users shows that most are running versions of the software that are one to three versions behind the most recent release. The time to recovery is about 3 weeks. An unusual pattern with Java is that the dominant populations are those that use recent versions. The Java update cycle is from 1 to 2 months.

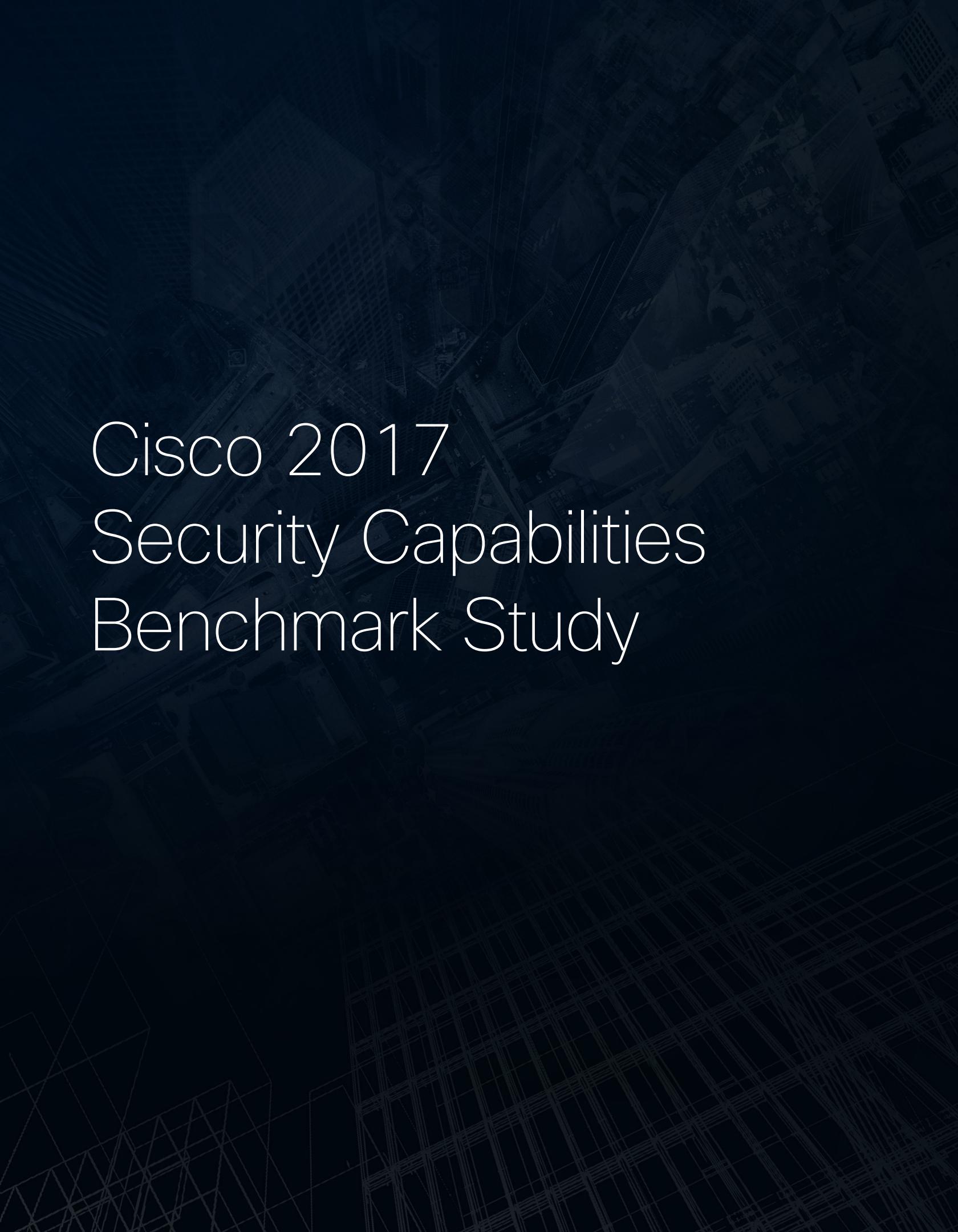
The overall lesson from time-to-patch cycles is that upgrade release patterns are a contributing factor in user security posture, which can place networks at risk.

Figure 43 Time to Patch for Firefox, Silverlight, and Java



Source: Cisco Security Research

Download the 2017 graphics at: www.cisco.com/go/acr2017graphics



Cisco 2017 Security Capabilities Benchmark Study

Cisco 2017 Security Capabilities Benchmark Study

To gauge the perceptions of security professionals on the state of security in their organizations, Cisco asked chief security officers (CSOs) and security operations (SecOps) managers in several countries and at organizations of various sizes about their perceptions of their own security resources and procedures. The Cisco 2017 Security Capabilities Benchmark Study offers insights on the maturity level of security operations and security practices currently in use, and also compares these results with those of the 2016 and 2015 reports. The study was conducted across 13 countries with more than 2900 respondents.

Security professionals want to make their organizations more secure, but in a way that responds to the complex attacker landscape and their adversaries' efforts to expand their operational space. Many organizations are relying on many solutions from many vendors. This tactic adds to the complexity and confusion of securing networks as the Internet continues to grow in terms of speed, connected devices, and traffic. Organizations need to aim for simplicity and integration if they are to protect themselves.

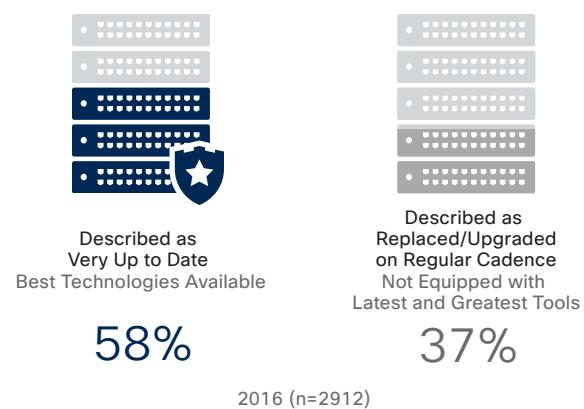
Perceptions: Security Professionals Confident in Tools, Less Sure They're Using Them Effectively

Most security professionals believe that they have adequate solutions on hand and that their security infrastructures are up to date. However, according to our study, this confidence comes with some uncertainty. These professionals are not always sure they can muster the budgets and brainpower to truly take advantage of the technology they have.

Threats to organizations are coming from every direction. Adversaries are nimble and creative, and they're able to outfox defenses. Even in this sobering environment, the majority of security professionals feel confident that their security

infrastructure is up to date, although that confidence appears to be waning a bit from previous years. In 2016, 58 percent of the respondents said their security infrastructure is very up to date and is constantly upgraded with the latest technologies. Thirty-seven percent said they replace or upgrade their security technologies on a regular basis but aren't equipped with the latest-and-greatest tools (Figure 44).

Figure 44 Percentages of Security Professionals Who Feel Their Security Infrastructure Is Up to Date



Source: Cisco 2017 Security Capabilities Benchmark Study

In addition, more than two-thirds of security professionals perceive their security tools as very effective or extremely effective. For example, 74 percent believe their tools are very or extremely effective in blocking known security threats, while 71 percent believe their tools are effective at detecting network anomalies and dynamically defending against shifts in adaptive threats (Figure 45).

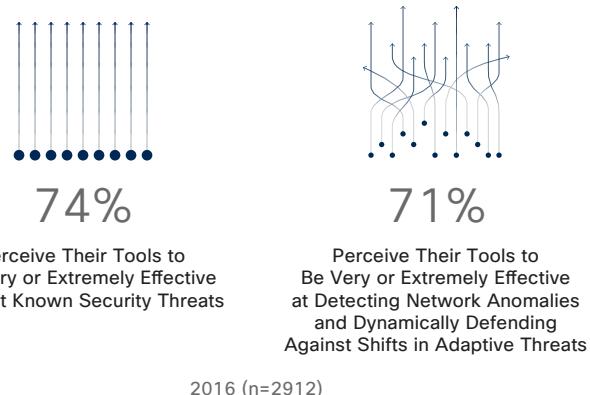
The problem: Confidence in tools does not necessarily transfer to effective security. As the study indicates, security departments are wrestling with complicated tools from many vendors, as well as a lack of in-house talent. This boils down to an “intent versus reality” problem. Security professionals want simple, effective security tools, but they don’t have the integrated approach they need to make this vision happen.

Security remains a high priority for the top levels of many organizations. And security professionals believe that executive teams keep security high on the list of key organizational goals. The challenge, of course, is to match executive support with the talent and technology that can affect security outcomes.

The number of security professionals strongly agreeing that their executive leadership considers security a high priority was 59 percent in 2016, down slightly from 61 percent in 2015 and 63 percent in 2014 (Figure 46). In 2016, 55 percent of security professionals agreed that security roles and responsibilities are clarified within their organization’s executive team; in 2015 and 2014, 58 percent agreed.

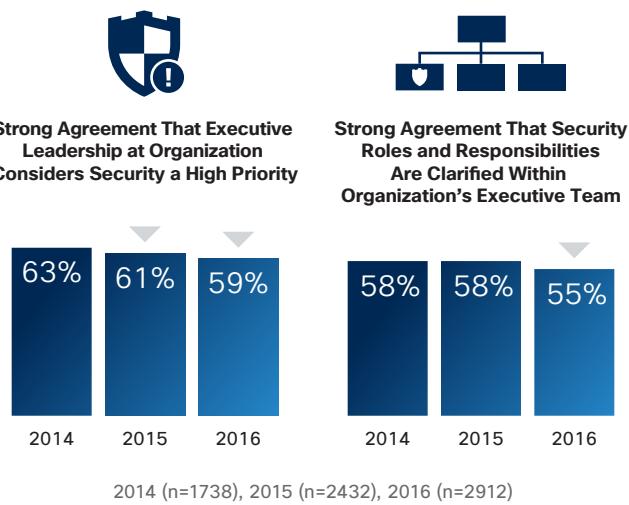
In summary, security professionals have confidence in the tools on hand, and they appear to have the ear of corporate leaders in addressing security issues. But that confidence is waning slightly. Security professionals are becoming aware of attacker successes and the unwieldiness of managing the growing attack surface.

Figure 45 Percentages of Security Professionals Who Perceive Various Security Tools to Be Highly Effective



Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 46 Percentages of Security Professionals Who Believe Security Is a High Priority at the Executive Level, 2014–2016



Source: Cisco 2017 Security Capabilities Benchmark Study

SHARE

Constraints: Time, Talent, and Money Affect the Ability to Respond to Threats

If security professionals are relatively confident that they have the tools needed to detect threats and mitigate damage, they also recognize that certain structural constraints stand in the way of their goals. A tight budget is a perennial challenge. But other constraints on effective security speak to the problems of simplifying and automating security.

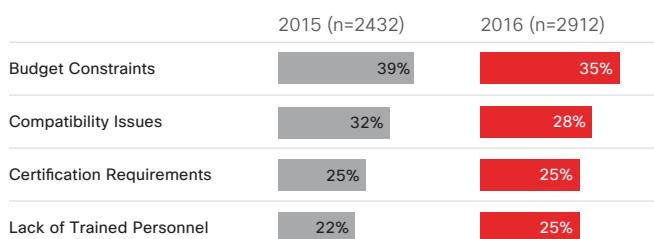
In 2016, 35 percent of security professionals said that budget was their biggest obstacle to adopting advanced security processes and technology (a slight decrease from 2015, when 39 percent said budget was the number one obstacle), as seen in Figure 47. As in 2015, compatibility issues with legacy systems was the second-most-common obstacle: 28 percent named compatibility in 2016, compared with 32 percent in 2015.

Money is only part of the problem. For example, compatibility issues speak to the problem of disconnected systems that don't integrate. And concerns about the lack of trained personnel highlight the problem of having the tools but not the talent to truly understand what is happening in the security environment.

The struggle to find talent is a concern, considering the expertise and decision-making abilities needed to fight targeted attacks and shifting adversary tactics. A well-resourced and expert IT security team, paired with the right tools, can make technology and policies work together and achieve better security outcomes.

The median number of security professionals at the surveyed organizations was 33, compared with 25 in 2015. In 2016, 19 percent of organizations had between 50 and 99 dedicated security professionals; 9 percent had 100 to 199 security professionals; and 12 percent had 200 or more (Figure 48).

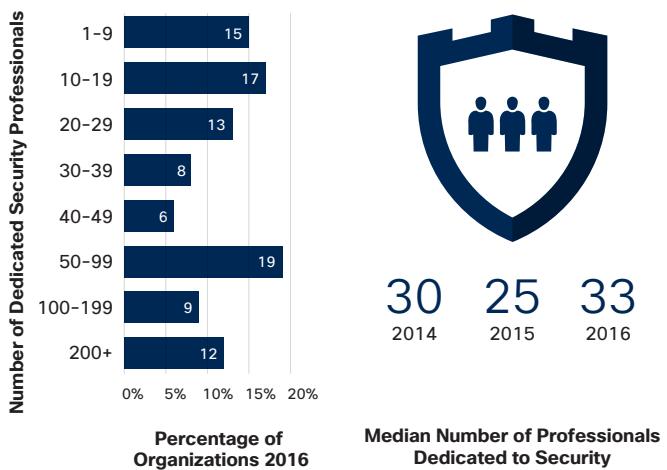
Figure 47 Biggest Obstacles to Security



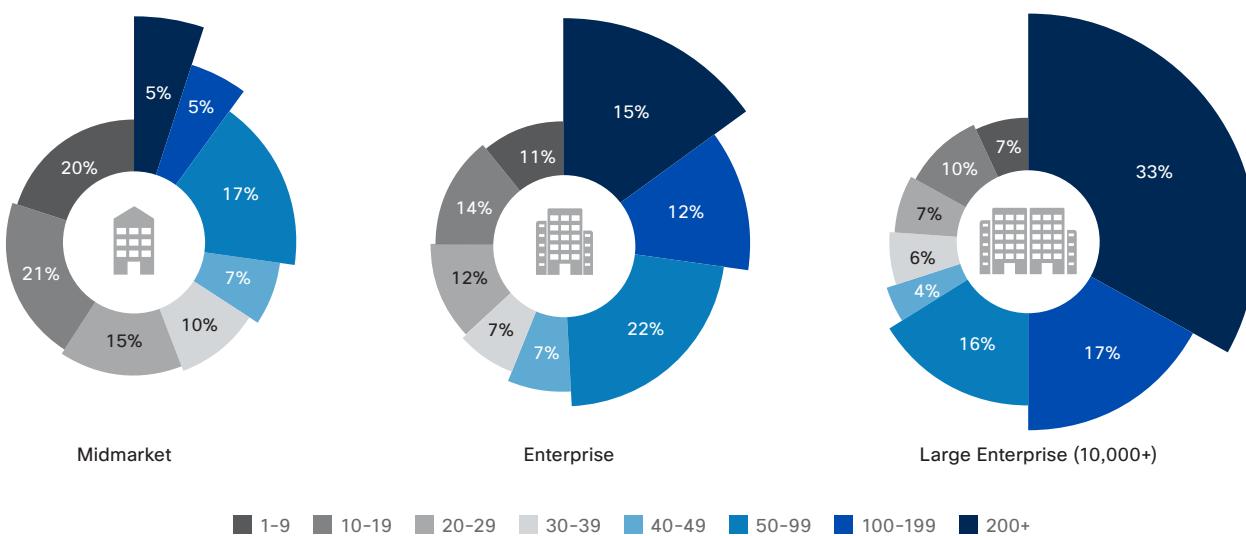
Source: Cisco 2017 Security Capabilities Benchmark Study

SHARE     

Figure 48 Number of Security Professionals Employed by Organizations



Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 49 Number of Security Professionals by Size of Organization

Source: Cisco 2017 Security Capabilities Benchmark Study

SHARE

The number of security professionals varies by organizational size. As shown in Figure 49, 33 percent of large enterprises with more than 10,000 employees had at least 200 security employees.

Whatever the constraints, security professionals need to ask hard questions about the barriers that limit their ability to face coming threats.

For example, when it comes to budget, how much is really enough? As survey respondents explained, security teams must compete against many other corporate priorities, even within the IT setting. If they can't secure funds for more tools, then the budget they do have must work harder. For example, automation can be used to offset limited manpower.

Similar questions should be asked about the software and hardware compatibility problem. As compatibility issues multiply, how many different versions of software and hardware—most of which may not be operating effectively—must be managed? And how will security teams handle the multiple certification requirements needed?



Outsourcing and the Cloud Help Stretch Budgets

Many security professionals participating in the benchmark study felt they were cash-strapped when making security purchases. They stretched their budget by outsourcing some tasks or using cloud solutions. They also relied on automation.

Aside from those limitations, security professionals are also placing slightly less emphasis on security operationalization. This trend may raise concerns that security professionals are building a suboptimal security infrastructure. Signs of a weakening focus on operationalization can indicate that organizations are not prepared to defend a widening attack landscape.

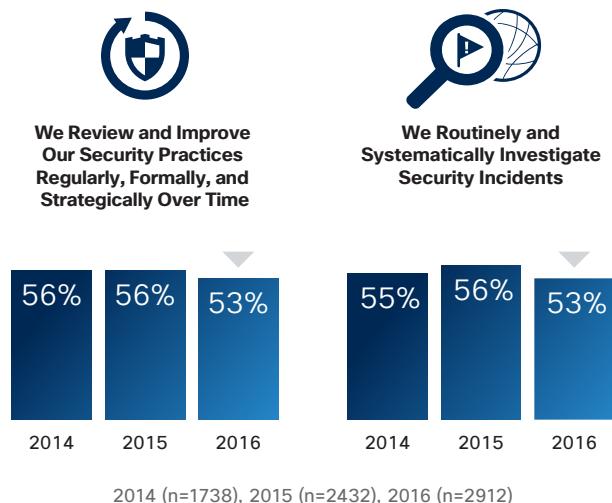
For example, in 2016, 53 percent of the respondents strongly agreed that they review and improve security practices regularly, formally, and strategically; in 2014 and 2015, 56 percent strongly agreed. Likewise, in 2016, 53 percent said they strongly agreed that they routinely and systematically investigate security incidents, compared with 55 percent in 2014 and 56 percent in 2015 (Figure 50).

If security professionals are slipping in their goals to put security into use, then it may not be a surprise that they can't effectively deploy the tools they have, much less add new tools. If, as study respondents told us, they cannot use the technology that they already have on hand, they need simpler streamlined tools that automate security processes. And those tools need to provide a holistic picture of what is going on in the network environment.

The lack of integration in security can allow gaps of time and space, where bad actors can launch attacks. The tendency of security professionals to juggle solutions and platforms from many vendors can complicate assembling a seamless defense. As seen in Figure 51, a majority of companies use more than five security vendors and more than five security products in their environment. Fifty-five percent of security professionals use at least six vendors; 45 percent use anywhere from one to five vendors; and 65 percent use six or more products.

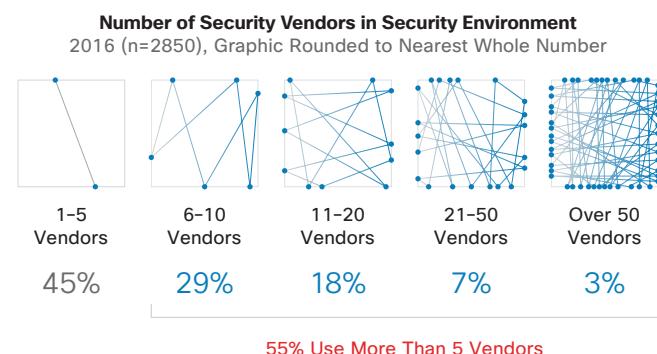
 Download the 2017 graphics at: www.cisco.com/go/acr2017graphics

Figure 50 Percentages of Respondents Who Strongly Agree with Security Operationalization Statements

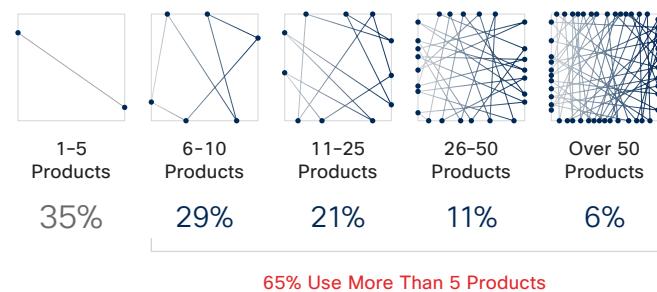


Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 51 Number of Security Vendors and Products Used by Organizations



Number of Security Products in Security Environment
2016 (n=2860), Graphic Rounded to Nearest Whole Number



Source: Cisco 2017 Security Capabilities Benchmark Study

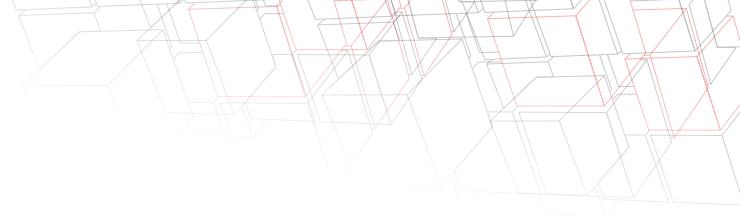
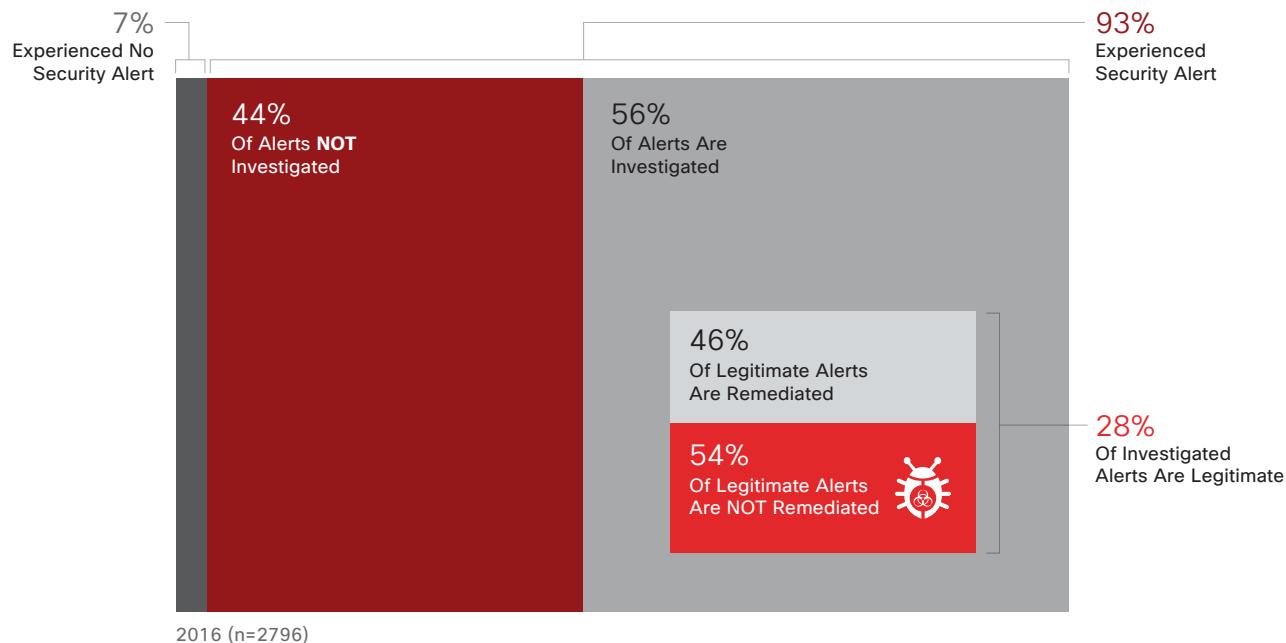


Figure 52 Percentages of Security Alerts That Are Not Investigated or Remediated



Source: Cisco 2017 Security Capabilities Benchmark Study

If operationalization goals are slipping, if tools are not used at their maximum effectiveness, and if manpower is not robust, the result is faltering security. Security professionals are forced to skip the investigation of alerts simply because they do not have the talent, tools, or automated solutions available to determine which ones are critical and why they are occurring.

Perhaps due to several factors—such as the lack of an integrated defense system or the lack of staff time—organizations are able to investigate a little more than half the security alerts they receive in a given day. As shown in Figure 52, 56 percent of alerts are investigated, and 44 percent are not investigated; of those alerts that are investigated, 28 percent are deemed legitimate alerts. Forty-six percent of legitimate alerts are then remediated.

To put the problem into more concrete terms, if an organization records 5000 alerts per day, this means:

- 2800 alerts (56 percent) are investigated, while 2200 (44 percent) are not
- Of those investigated, 784 alerts (28 percent) are legitimate, while 2016 (72 percent) are not
- Of the legitimate alerts, 360 (46 percent) are remediated, while 424 (54 percent) are not remediated

The fact that nearly half of alerts go uninvestigated should raise concern. What is in the group of alerts that is not being remediated: Are they low-level threats that might merely spread spam, or could they result in a ransomware attack or cripple a network? To investigate and understand a greater slice of the threat landscape, organizations need to rely on automation as well as properly integrated solutions. Automation can help stretch precious resources and remove the burden of detection and investigation from the security team.

The inability to view so many alerts raises questions about their impact on an organization's overall success. What could these uninvestigated threats do to productivity, customer satisfaction, and confidence in the enterprise? As respondents told us, even small network outages or security breaches can have long-term effects on the bottom line. Even when losses were relatively minor and the affected systems were fairly easy to identify and isolate, security leaders regard breaches as significant because of the stress they put on the organization.

SHARE [f](#) [t](#) [in](#) [x](#) [d](#)

The stresses can affect organizations in many ways. Security teams must devote time to managing network outages that occur after a security breach. Nearly half of these outages lasted as long as 8 hours. Forty-five percent of the outages lasted from 1 to 8 hours (Figure 53); 15 percent lasted 9 to 16 hours, and 11 percent lasted 17 to 24 hours. Forty-one percent of these outages affected between 11 percent and 30 percent of the organizations' systems.

Impact: More Organizations Experience Losses from Breaches

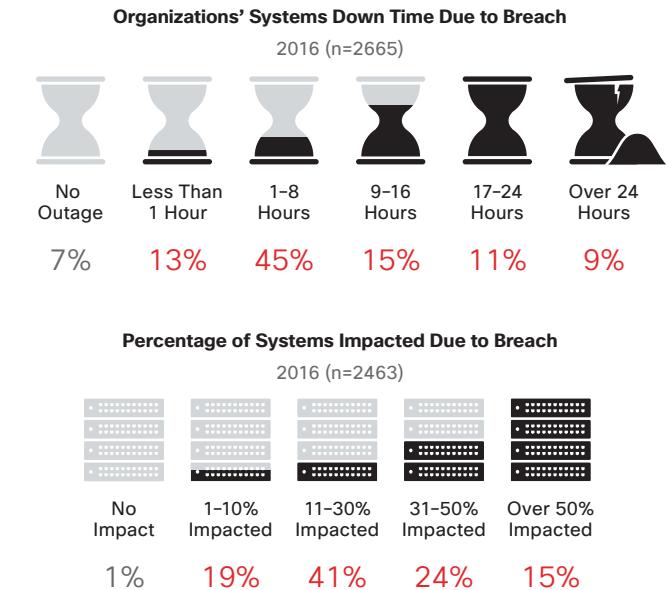
The effects of breaches aren't limited to outages. Breaches also mean the loss of money, time, and reputation. Security teams who believe they will dodge this bullet are ignoring the reality of the data. As our study shows, almost half of organizations have had to cope with public scrutiny following a security breach. Given the attackers' range of ability and tactics, the question isn't if a security breach will happen, but when.

As the benchmark study shows, security professionals are jarred into reality when breaches occur. They often change security strategies or bolster defenses. Organizations that have not yet suffered a breach of their networks due to attackers may be relieved they've escaped. However, this confidence is probably misplaced.

Forty-nine percent of the security professionals surveyed said their organization has had to manage public scrutiny of a security breach. Of those organizations, forty-nine percent disclosed the breach voluntarily, while 31 percent said the disclosure was made by a third-party (Figure 54). In other words, nearly one-third of the surveyed organizations were forced to deal with the involuntary disclosure of a breach. It's clear that the days of quietly dealing with breaches may be long gone. There are too many regulators, media, and social media users who will expose the news.

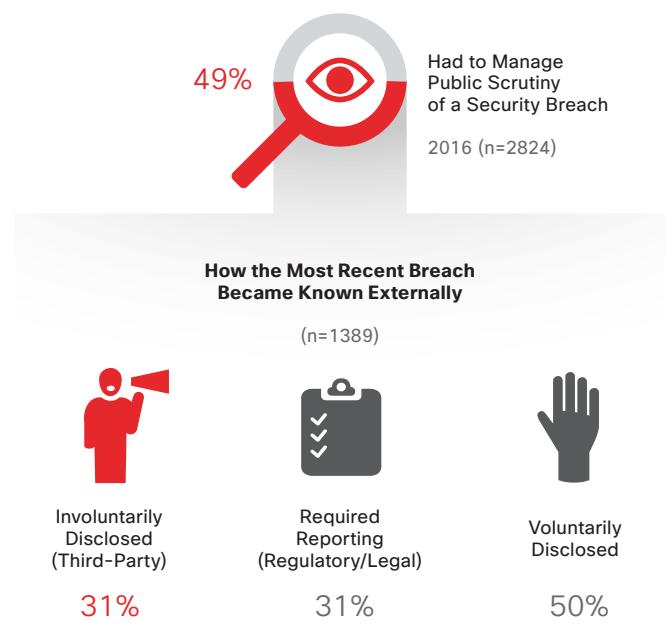
SHARE     

Figure 53 Length and Extent of Outages Caused by Security Breaches



Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 54 Percentage of Organizations Experiencing a Public Breach



Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 55 Functions Most Likely to Be Affected by a Public Breach

Source: Cisco Security Research

SHARE

The damage to organizations goes far beyond the time it takes to deal with a breach or outage. There are real and substantial impacts that enterprises should try mightily to avoid.

As seen in Figure 55, 36 percent of security professionals said that operations was the function most likely to be affected. This means that core systems of productivity, which affect industries from transportation to healthcare to manufacturing, can slow down or even grind to a halt.

After operations, finance was the function most likely to be affected (cited by 30 percent of the respondents), followed by brand reputation and customer retention (both at 26 percent).

No organization that plans to grow and achieve success wants to be in a position of having critical departments affected by security breaches. Security professionals should view the survey results with an eye toward their own organizations, and ask themselves: If my organization suffers this kind of loss from a breach, what happens to the business down the road?

The opportunity losses for companies suffering online attacks are daunting. Twenty-three percent of the surveyed security professionals said that in 2016, their organizations experienced a loss of opportunity due to attacks (Figure 56). Of that group, 58 percent said that the total opportunity lost was under 20 percent; 25 percent said the lost opportunity was 20 to 40 percent, and 9 percent said the lost opportunity amounted to 40 to 60 percent.

Many organizations can quantify the revenue losses they experience due to public breaches. As seen in Figure 57, 29 percent of security professionals said their organizations experienced a loss of revenue as a result of attacks. Of that group, 38 percent said that revenue loss was 20 percent or higher.

Online attacks also result in fewer customers. As shown in Figure 58, 22 percent of organizations said they lost customers as a result of attacks. Of that group, 39 percent said they lost 20 percent of their customers or more.



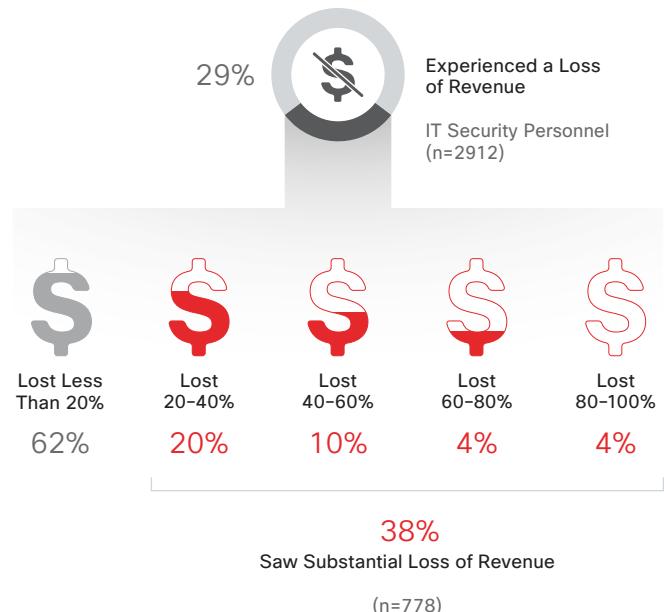
Download the 2017 graphics at: www.cisco.com/go/acr2017graphics

Figure 56 Percentage of Business Opportunity Lost as the Result from an Attack



Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 57 Percentage of Organizational Revenue Lost as the Result of an Attack



Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 58 Percentage of Customers Lost by Companies Due to Attacks



Source: Cisco 2017 Security Capabilities Benchmark Study

Outcomes: Increased Scrutiny Will Play a Role in Security Improvements

As the survey results show, the impact of breaches can be long-lasting and widespread. If one assumes an organization will be affected by a breach at some point, the question is, what happens next? Where should management shift their attention and resources so that breaches are less likely to occur?

The aftermath of a breach is a learning opportunity, an experience that should not go to waste in terms of investing in better approaches.

Ninety percent of the security professionals said that a security breach drove improvements in threat defense technologies and processes, as shown in Figure 59. Of those organizations affected by breaches, 38 percent said they responded by separating the security team from the IT department; 38 percent said they increased security awareness training among employees; and 37 percent said they increased their focus on risk analysis and mitigation.

SHARE

Figure 59 How Security Breaches Drive Improvements



Source: Cisco 2017 Security Capabilities Benchmark Study

Organizations recognize that they have to exercise creativity to move beyond the constraints of talent, technology compatibility, and budget. One strategy is to adopt outsourced services to strengthen the budget and also tap into talent that may not be in-house.

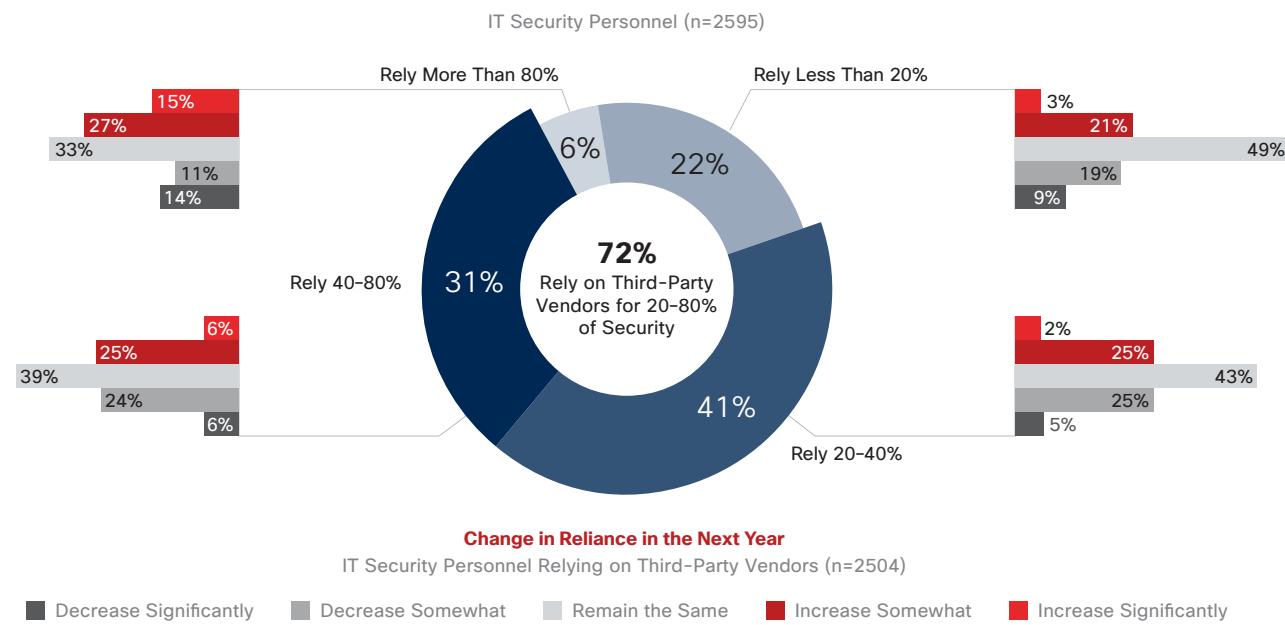
In 2016, 51 percent of security professionals outsourced advice and consulting, while 45 percent outsourced incident response (Figure 60). Fifty-two percent said they outsource services to save costs, while 48 percent said they do so to obtain unbiased insights.

As they do with outsourcing, organizations also rely on third-party vendors to augment their defense strategies. The security ecosystem provides them with ways to share the responsibility for security.

Seventy-two percent of the security professionals said that they rely on third-party vendors for 20 to 80 percent of their security, as seen in Figure 61. Those organizations that rely heavily on outside help for security were most likely to say that they will increase their use of third-party vendors in the future.

SHARE     

Figure 61 Percentage of Organizations' Reliance on Outsourcing



Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 60 Organizations' Reliance on Outsourcing



Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 62 Sources of Increased Scrutiny

Source: Cisco 2017 Security Capabilities Benchmark Study

As organizations take steps to strengthen their security posture, they can expect that more attention will be paid to their efforts. This scrutiny will come from influential audiences and therefore can't be ignored. How these audiences' concerns are addressed can have a significant impact on an organization's ability to defend itself.

Seventy-four percent of the security professionals said scrutiny will come from the executive leadership; 73 percent, from clients and customers; and 72 percent, from employees, as seen in Figure 62.

Figure 63 How Trust and Cost-Effectiveness Drive Security Decisions**Security Threat Defense Solution Purchasing**

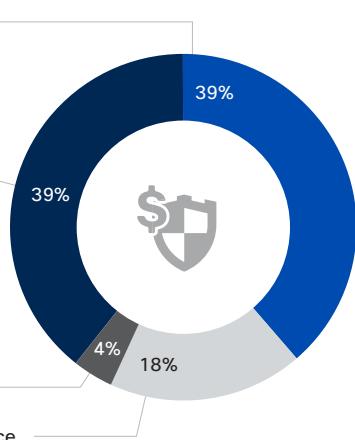
IT Security Personnel (n=2665)

Typically Follow Enterprise Architecture Approach

Typically Follow Project-Based Approach (For Example, Best-of-Breed Point Products)

Deploy Point Products as Needed

Only Deploy to Meet Compliance or Regulatory Requirements



Source: Cisco 2017 Security Capabilities Benchmark Study

Reasons for Favoring a Best-of-Breed Approach

Organization That Purchased Best-of-Breed Point Solutions

Trust More Than Enterprise Architecture Approach

Best-of-Breed Solutions Are More Cost-Effective

Best-of-Breed Solutions Are Easier to Implement

Best-of-Breed Solutions Are Faster to Implement

65%

41%

24%

13%

Reasons for Favoring an Enterprise Architecture Approach

Organizations That Typically Follow an Enterprise Architecture Approach

Trust More Than Best-of-Breed

Enterprise Architecture Approach Is More Cost-Effective

36%

59%

Enterprise Architecture Approach Is Easier to Implement

33%

Enterprise Architecture Approach Is Faster to Implement

10%

Trust Versus Cost: What Drives Security Purchases?

Security professionals want the very best solutions for protecting their organizations, but their perceptions differ on how to create the ideal secure environment. Do they purchase best-of-breed solutions from a variety of vendors because they trust these solutions will solve many different problems? Or do they turn to an integrated architecture, because they believe this approach is more cost-effective? Although there are many drivers for security investments, greater simplicity can benefit every organization.

As seen in Figure 63, the security professionals seem evenly split between trust and cost in choosing between best-of-breed and architected solutions. Sixty-five percent said they favor best-of-breed solutions because they trust them more than an enterprise architecture approach. On the other hand, 59 percent said they favor an architected approach because they believe it is more cost-effective.

This isn't an either/or dilemma. Organizations need both best-of-breed and integrated security solutions. Both approaches offer benefits and will simplify security while providing automated response tools (Figure 63).

By combining best-of-breed solutions with an integrated approach, security teams can take steps toward less complex yet more effective security. The integrated approach helps security professionals understand what's happening at every stage of defense. Such an approach reduces attackers' operational space. It is simple, allowing teams to deploy solutions at scale. It is open, allowing for best-of-breed solutions as needed. And it's automated for faster detection.

Summary: What the Benchmark Study Reveals

There is a world of difference between amassing security tools and actually having the capability to use those tools to reduce risk and close the operational space for adversaries. Respondents to the benchmark study believe they have the tools that will thwart attackers. But they also acknowledge that constraints such as a lack of manpower and poor product compatibility can render good tools much less effective than they'd hoped.

The sobering findings regarding the impact of breaches should provide security professionals with ample evidence of the need to improve processes and protocols. Faced with real and immediate effects like lost revenue and

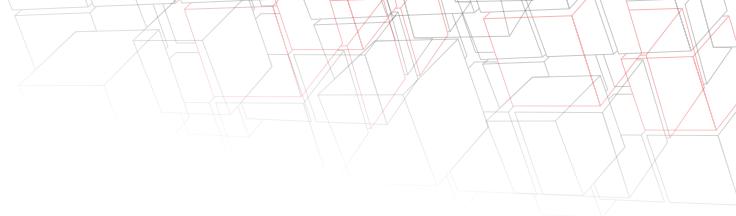
customers, organizations can no longer simply wish away gaps in security protection, because the question is not if a breach will happen, but when.

One takeaway from the benchmark study is that the constraints limiting agile and effective security will always be with us: There will never be as much budget and talent as security professionals believe they need. If we accept these constraints, then the idea of simplifying security and deploying automated solutions makes sense.

Simplifying security also makes use of best-of-breed solutions and an integrated architecture. Organizations need the benefits of both approaches.

The background of the image is a dark, high-angle aerial photograph of a city. The city's layout is characterized by a dense grid of streets and buildings, creating a pattern of numerous small, rectangular plots. The lighting is low, making the scene appear somber and industrial. In the center-left area, the word "Industry" is overlaid in a large, white, sans-serif font.

Industry



Industry

Value Chain Security: Success in a Digital World Hinges on Mitigating Third-Party Risk

Value chain security is an essential element of success in a connected economy. Ensuring that the right security is in the right place at the right time throughout the value chain—the end-to-end lifecycle for hardware, software, and services—is an imperative.

The eight stages of the value chain are shown in Figure 64.

Information technology and operations technology are converging in this digitized world. It is not enough for organizations to focus only on protecting their internal business models, offerings, and infrastructure. Organizations must look at their value chain holistically and consider whether each third-party that is involved in their business model or touching their offerings poses a risk to their security.

The short answer is that they likely do: Research by the SANS Institute found that 80 percent of data breaches originate from third parties.¹⁵ To reduce risk, organizations must foster a value chain where trust is not implicit and security is everyone's responsibility. As a foundational step toward achieving this goal, organizations should:

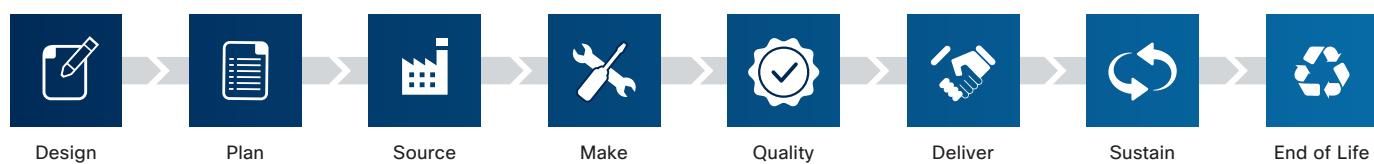
- Identify the key players in their third-party ecosystem and understand what those third parties deliver

- Develop a flexible security architecture that can be shared with and deployed across the variety of third parties in that ecosystem
- Assess whether those third parties are operating within the tolerance levels set by the organization's security architecture
- Be alert to new security risks that the ecosystem may present as digitization increases

Organizations must also think about security before introducing a new business model or an offering that requires involvement by, or that otherwise affects, their third-party ecosystem. Any potential value and productivity gains must be weighed against potential risks, particularly around data security and privacy.

Awareness of the importance of the value chain is growing both globally and in specific industry sectors. Recent U.S. IT procurement legislation mandated a 1-year assessment by the U.S. Department of Defense regarding open technology standards in procurements for information technology and cybersecurity acquisitions.¹⁶ In the highly converged energy sector, the North American Electric Reliability Corporation (NERC) is actively developing new requirements addressing its cyber value chain.¹⁷

Figure 64 The Stages of the Value Chain



Source: Cisco

SHARE

¹⁵ *Combating Cyber Risks in the Supply Chain*, SANS Institute, 2015: <https://www.sans.org/reading-room/whitepapers/analyst/combating-cyber-risks-supply-chain-36252>.

¹⁶ Public Law 114-92 §

¹⁷ NERC ordered to undertake this effort by United States Federal Energy Regulatory Commission 18 CFR Part 40 [Docket No. RM15-14-002; Order No. 829].

Organizations, together with their third parties, need to answer questions such as, "How will data be generated and by whom?" and, "Should the data be digitally mined?" Further clarity requires determining the answers to such questions as, "Who owns the digital assets we are collecting or creating?" and, "With whom must we share that information?" Another critical question to answer: "Who owns what liability and obligation when a breach occurs?"

This value chain-centric approach helps ensure that security considerations are built in at every stage of the solutions lifecycle. The right architecture, combined with adherence to the appropriate security standards, will help to drive pervasive security—and build trust—throughout the entire value chain.

Geopolitical Update: Encryption, Trust, and a Call for Transparency

In previous cybersecurity reports, Cisco geopolitical experts examined the uncertainty in the Internet governance landscape, the rights of the individual versus the rights of the state, and the ways that governments and private businesses might navigate the data-protection dilemma. One common topic across these discussions has been encryption. We believe that encryption will continue to permeate, perhaps even dominate, the cybersecurity debate for the foreseeable future.

The proliferation of national and regional data privacy laws has created unease among vendors and users attempting to navigate those laws. In this uncertain environment, issues such as data sovereignty and data localization have come to the fore, helping to fuel growth in cloud computing and localized data storage as businesses seek a creative solution to meeting complex and evolving privacy regulations.¹⁸

At the same time, the escalating number of data breaches and advanced persistent threats, and the publicity around hacks sponsored by nation-states—including those conducted during high-profile events such as the U.S. presidential election—are making users even less confident that their sensitive data and privacy will be protected.

Governments in the post-Snowden era have been increasingly strident in their desire to regulate digital communications and to access data when needed. However, users have been just as ardent in their demand for privacy. Events such as the recent head-butting between Apple and the FBI over an iPhone belonging to a terrorist have done nothing to assuage users' worries about privacy. If anything, it taught a generation of digital users, especially in the United States, about end-to-end encryption. Many users are now demanding end-to-end encryption from their technology providers, and they want to hold the encryption keys.

This marks a fundamental shift in the cybersecurity landscape as we have known it. Organizations are going to need to architect their environments so they can navigate and respond to competing agendas.

While this shift is taking place, more governments are giving themselves the legal right—often on a broad basis—to bypass or break encryption or technical protection measures, often without the knowledge of the manufacturer, communication provider, or the user. This is creating tension not only between authorities and technology firms but also between governments, who are not necessarily keen to see their citizens' data accessed by third-country authorities. Many governments collect information about zero-day exploits and vulnerabilities that they discover in vendor software; however, they are not always transparent with vendors about the information they possess, or sharing it in a timely manner.

Hoarding such valuable information prevents vendors from improving security in their products and providing users with better protection from threats. Even though governments may have good reason to hold some of this intelligence close, there is also a need for greater transparency and trust in the global cybersecurity landscape. Governments therefore should conduct a frank assessment of their current policies regarding the hoarding of zero-day exploits. They should start from the default position that sharing information with vendors can only lead to a far more secure digital environment for everyone.

¹⁸ For more on this topic, see "Data Localization Takes Off as Regulation Uncertainty Continues," by Stephen Dockery, June 6, 2016, *The Wall Street Journal*: <http://blogs.wsj.com/riskandcompliance/2016/06/06/data-localization-takes-off-as-regulation-uncertainty-continues/>.



High-Speed Encryption: A Scalable Solution to Protecting Data in Transit

As explained in the geopolitical section on [page 65](#), end-to-end encryption will remain a topic of much debate and consternation between governments and industry for the foreseeable future. Regardless of any tension stemming from this issue, however, user demand for end-to-end data encryption with customer-held keys is increasing.

Cisco geopolitical experts anticipate that some streams and pools of data will likely remain encrypted with vendor-managed keys at least for the short term, particularly in ad-driven business models. Elsewhere, however, we should expect to see the use of end-to-end encryption with customer-held keys gaining more traction, absent a legal mandate to the contrary.

Meanwhile, look for organizations to also seek more control over how they protect their data while it is in transit, particularly as it moves at high speed from one data center to another. This was once an arduous task for enterprises due to the limitations of legacy technologies and the impact on network performance. However, new approaches are making this process easier.

One solution is application-layer security, where applications are modified to encrypt data. Deploying this type of security can be very resource-intensive, complex to implement, and operationally expensive depending on how many applications an organization uses.

Another approach seeing increased traction is encryption capabilities built in to a network or cloud service to protect data in transit. This is an evolution of the traditional gateway VPN model, a solution that addresses the dynamic nature of networks and the high-speed transmission rates of data center traffic. Enterprises are using the operational and cost efficiencies provided by the new capabilities to protect data coming from any application in that environment as it travels at high speed to another location.

Network-based encryption is only one tool for protecting data, however. To ensure they are doing enough to protect their data while it is in transit or at rest, organizations should look at the challenge holistically. A good place to begin is by asking technology vendors basic but important questions such as:

- How is data protected when it's in transit?
- How is it protected when it's at rest?
- Who has access to the data?
- Where is the data stored?
- What is the policy for deleting data, when and if it must be deleted?

Again, these questions are only a starting point for a broader dialogue about data protection that should evolve to include a discussion of topics such as data resiliency and availability.

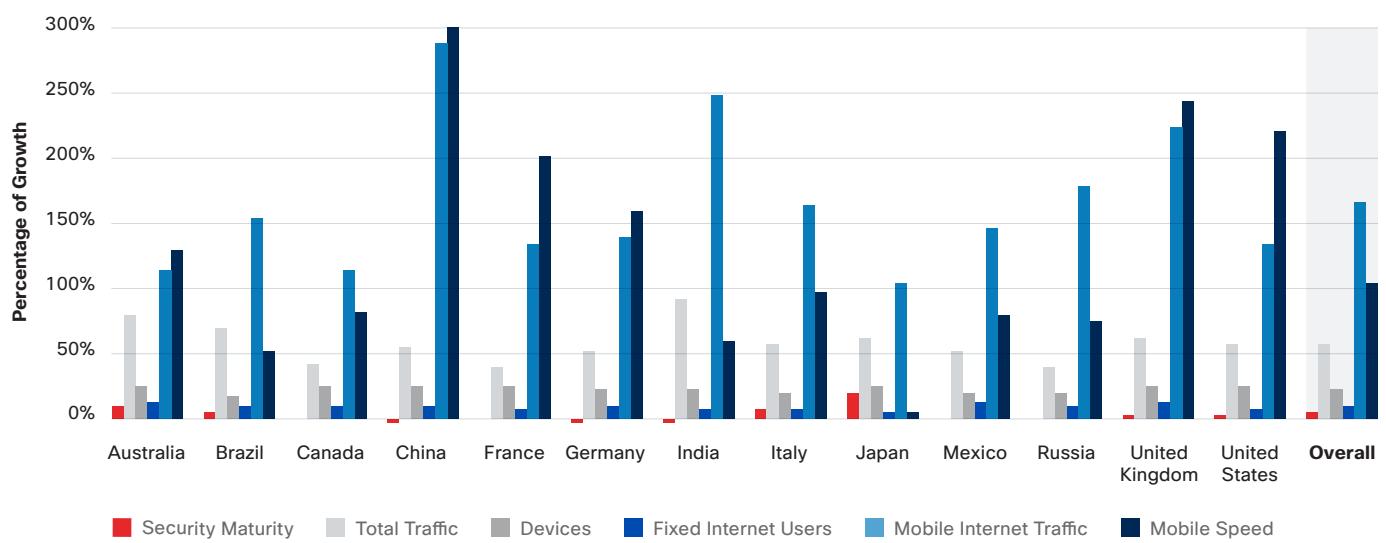
Network Performance and Adoption Versus Security Maturity: Online Speeds, Traffic, and Preparedness Are Not Growing at the Same Pace

Defenders want to stay ahead of their adversaries. To be behind them is to be in a potentially dangerous place. The worry is that defenders can't improve their security posture at the same pace that adversaries can gain space and time to operate. Given the pace of growth of fixed and mobile Internet traffic worldwide, defenders are obligated to match this growth with gains in the maturity of their security infrastructure.

The Cisco VNI Forecast examines global IP traffic annually, including mobile and Wi-Fi traffic. The forecasts provide 5-year projections for IP traffic, the number of Internet users, and the number of personal devices and machine-to-machine (M2M) connections that will be supported by IP networks. ([Visit here](#) for more details on the VNI Forecast.) For example, the forecast estimates that by 2020, smartphones will generate 30 percent of total IP traffic.

Cisco has matched the VNI Forecast to data about defender maturity, taken from Cisco's annual Security Capabilities Benchmark Study (see [page 49](#)). In examining maturity growth rates in the 2015, 2016, and 2017 benchmark reports, as seen in Figure 65, security maturity is underwhelming compared with the growth of Internet traffic. Some countries, such as China and Germany, actually show a slight decline in maturity over this time period. Broadband speeds, in particular, are improving and growing at a significantly greater rate than other networking variables shown in Figure 65. Faster speeds and more connected devices foster greater traffic growth, but organizations are struggling to bolster their security measures and infrastructures at similar rates.

Figure 65 Security Maturity and Growth Rates



Source: Cisco Security Research, Cisco VNI, and Cisco 2017 Security Capabilities Benchmark Study

SHARE

Certain industries also lag in terms of their security maturity compared with other industries, as seen in Figure 66. In particular, pharmaceuticals, healthcare, and transportation are behind other industries.

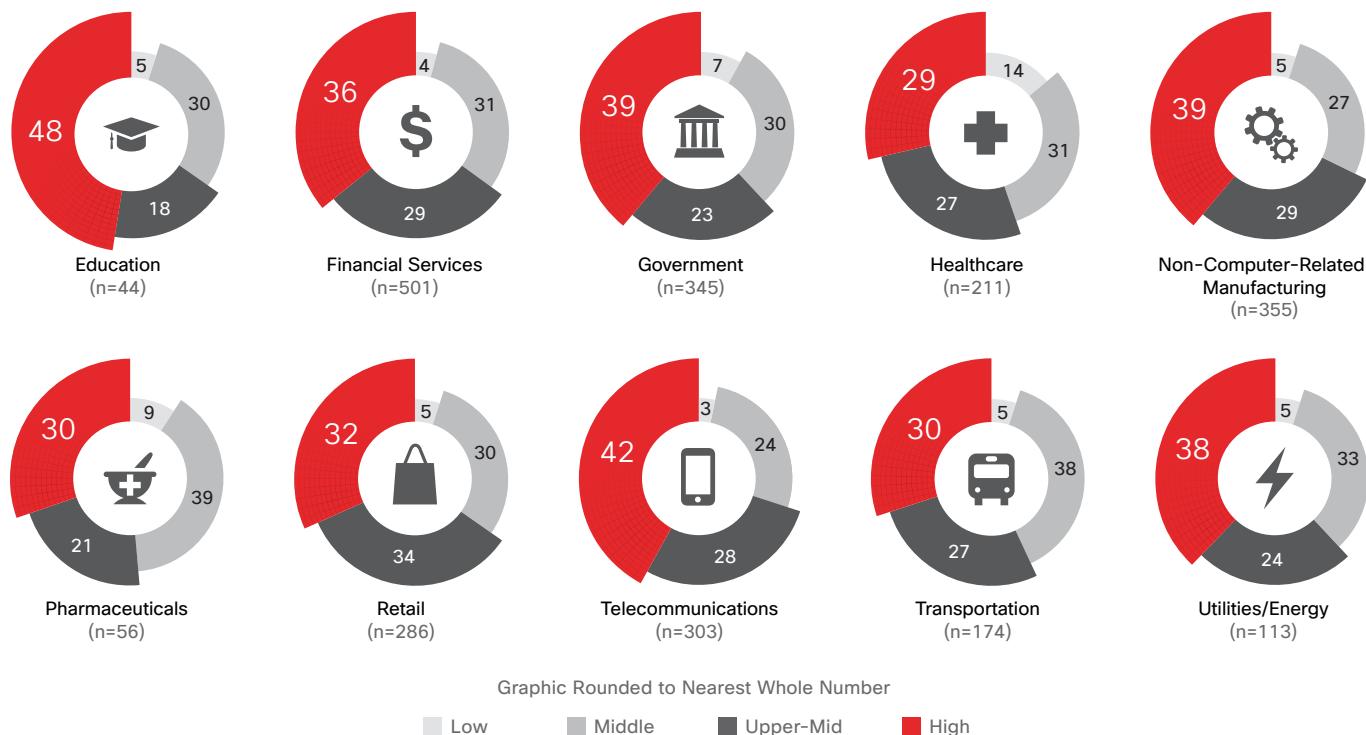
It's important to note that the dramatic rise in mobile speeds is an outcome of the broad adoption of 4G and LTE networks by telecommunications providers. When large-scale deployments of 5G networks become available toward the end of this decade, mobile speeds are expected to become comparable to fixed network speeds. According to the current Mobile VNI Forecast, global mobile traffic will likely gain a greater share of total IP traffic when 5G

is broadly adopted. Global mobile traffic was 5 percent of total IP traffic in 2015, according to the VNI Forecast; it is projected to be 16 percent of total IP traffic by 2020.

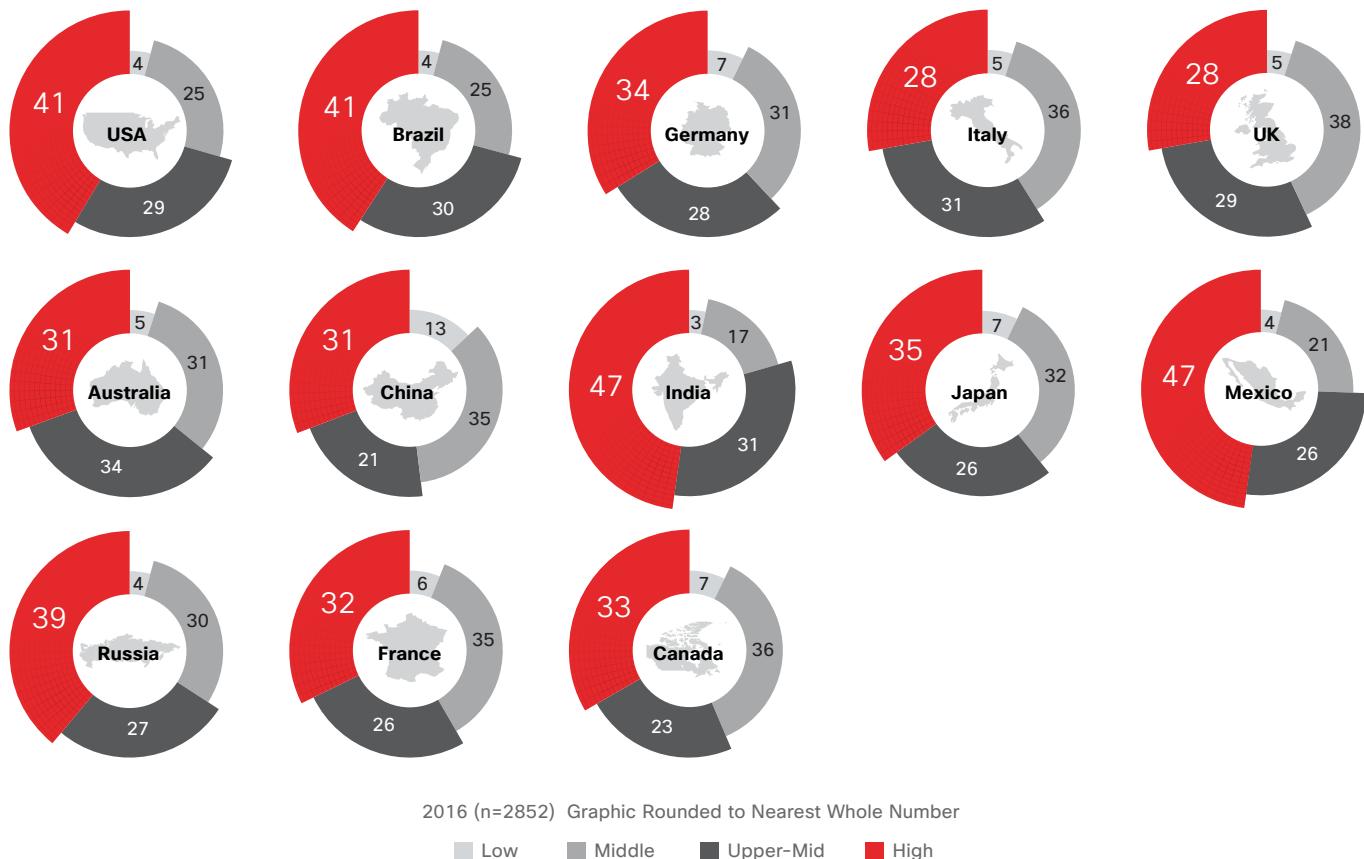
It's clear that security organizations must step up their maturity efforts, and quickly, if they are to match the growth in Internet traffic, which portends growth in the potential attack surface. In addition, organizations must respond to the growth in the use of endpoints that are not fixed or wired to corporate networks. They must also accommodate a more widespread use of personal devices from which workers access corporate data.

Figure 66 Security Maturity in Industry Verticals

Industry by Segment



Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 67 Security Maturity by Country

Source: Cisco 2017 Security Capabilities Benchmark Study

Faster speeds are not the only factor driving growth of Internet traffic. The IoT is accelerating the number of devices that are attached to the Internet, not only adding to the growth of traffic but also adding potential pathways for attackers.

For more information about the Cisco VNI Forecast, visit the [Cisco website](#) or read the Cisco blog post on the [annual VNI forecast for 2015 to 2020](#).

Conclusion

Conclusion

A Rapidly Expanding Attack Surface Requires an Interconnected and Integrated Approach to Security

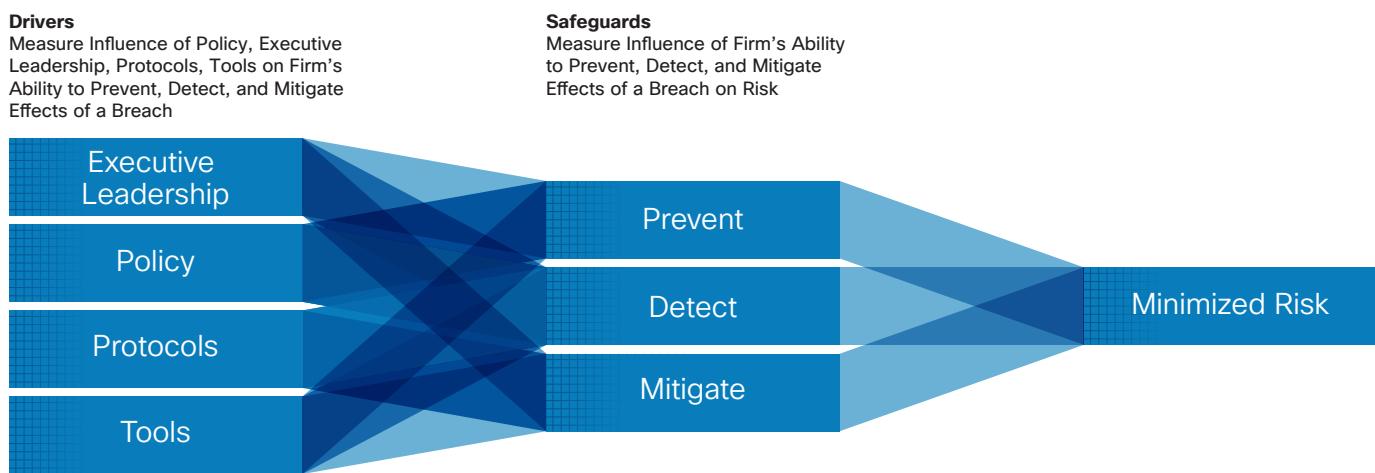
In analyzing data from Cisco's Security Capabilities Benchmark Study (see [page 49](#)), we are able to examine patterns and decisions that help organizations minimize risk. We can therefore see where they should make security investments that can lead to a significant difference in risk exposure. We measured risk by looking at the lengths of breaches as well as percentages of system outages (see [Figure 53 on page 55](#) regarding the length of breaches and the systems affected).

To understand how organizations create effective safeguards against risk, we need to examine what drivers affect their ability to prevent, detect, and mitigate risk. (See [Figure 68](#).) The drivers must include these elements:

- **Executive leadership:** The top leadership must prioritize security. This is critical for the mitigation of attacks, as well as their prevention. The executive team should also have clear and established metrics for assessing the effectiveness of a security program.

- **Policy:** Policy has strong ties to mitigation. Controlling access rights to networks, systems, applications, functions, and data will affect the ability to mitigate damage from security breaches. In addition, policies to ensure a regular review of security practices will help prevent attacks.
- **Protocols:** The right protocols can help prevent and detect breaches, but they also have a strong relationship to mitigation. In particular, regular reviews of connection activity on networks, to ensure that security measures are working, are key to both prevention and mitigation. It's also beneficial to review and improve security practices regularly, formally, and strategically over time.
- **Tools:** The judicious and appropriate application of tools has the strongest relationship with mitigation. With tools in place, users can review and provide feedback that is vital to detection and prevention as well as mitigation.

Figure 68 Drivers and Safeguards for Minimizing Risk



Source: Cisco 2017 Security Capabilities Benchmark Study

 Download the 2017 graphics at: www.cisco.com/go/acr2017graphics

The security safeguards that organizations use—prevention, detection, and mitigation—can be viewed as measures of influence on an organization’s ability to minimize risk. (See Figure 68.)

These safeguards must include the following elements:

- **Prevention:** To minimize the impact of security breaches, employees must report security failures and problems. It’s also crucial for security processes and procedures to be clear and well understood.
- **Detection:** The best detection methods for minimizing the impact of breaches are those that allow organizations to spot security weaknesses before they become full-blown incidents. To accomplish this, it’s vital to have a good system for categorizing incident-related information.

- **Mitigation:** Well-documented processes and procedures for incident response and tracking are key to effective breach mitigation. Organizations also need strong protocols to manage their response to crises.

All of these drivers and safeguards are interconnected and interdependent. Security professionals can’t simply cherry-pick a couple of drivers and one or two safeguards, and believe they have solved the security problem. They need every driver, and every safeguard. Security teams must analyze where their weaknesses are—for example, low levels of support from leaders, or a lack of tools to mitigate breaches—and calculate where investments in security must be made.

The Key Goal: Reducing Adversaries' Operational Space

Reducing—and ideally, eliminating—the unconstrained operational space of adversaries, and making attackers' presence known, must be top priorities for defenders. The reality is that no one can stop all attacks, or protect everything that can and should be protected. But if you focus on closing the operational space that cybercriminals must have for their campaigns to be effective and profitable, you can prevent them from reaching critical systems and data without entirely evading detection.

This report categorized different approaches that adversaries use to compromise and attack users and systems. We based our categories—reconnaissance, weaponization, delivery, and installation—on where the attacks are typically deployed in the attack chain. This exercise was meant to illustrate when, how, and where adversaries take advantage of vulnerabilities and other weaknesses to gain a foothold on a device or in a system, launch their campaign, and then reap the rewards they seek.

We suggest that defenders adapt their security approaches to stay ahead of attackers' basic processes. For example, to undermine adversaries during the reconnaissance phase, security teams should be:

- Gathering information about the latest threats and vulnerabilities
- Ensuring they are controlling access to their networks
- Limiting the organization's exposure in an expanding attack surface
- Managing configurations
- Developing consistent response practices and procedures that are informed by this work

When weaponized threats are delivered, defenders must apply every tool in their arsenal to prevent them from spreading and worsening. This is where an integrated security architecture becomes critical. It will provide real-time insight into threats as well as automated detection and defense, which are essential for improving threat detection.

At the installation phase, security teams must stay informed about the state of the environment as they respond to and investigate the compromise. If that environment is simple, open, and automated, and if defenders have taken the other proactive steps outlined above, they can then focus their resources on helping the business to answer critical questions such as:

- What did the attackers access?
- Why were they able to get to it?
- Where did they go?
- Are they still operating in our network?

The answers to these questions will allow security teams not only to take appropriate actions to prevent further attacks, but also to inform management and the board about possible exposures and necessary disclosures. Then, the business can begin the process of ensuring that it has comprehensive controls and mitigations in place to address any security gaps—the weaknesses that provided the operational space adversaries needed to succeed—that were identified during the compromise.

About Cisco

Cisco delivers intelligent cybersecurity for the real world, providing one of the industry's most comprehensive advanced-threat protection portfolios of solutions across the broadest set of attack vectors. Cisco's threat-centric and operationalized approach to security reduces complexity and fragmentation while providing superior visibility, consistent control, and advanced threat protection before, during, and after an attack.

Threat researchers from the Cisco Collective Security Intelligence (CSI) ecosystem bring together, under a single umbrella, the industry's leading threat intelligence, using telemetry obtained from the vast footprint of devices and sensors, public and private feeds, and the open-source community. This amounts to a daily ingest of billions of web requests and millions of emails, malware samples, and network intrusions.

Our sophisticated infrastructure and systems consume this telemetry, helping machine-learning systems and researchers to track threats across networks, data centers, endpoints, mobile devices, virtual systems, web, email, and from the cloud to identify root causes and scope outbreaks. The resulting intelligence is translated into real-time protections for our product and service offerings that are immediately delivered globally to Cisco customers.

To learn more about Cisco's threat-centric approach to security, visit www.cisco.com/go/security.

Contributors to the Cisco 2017 Annual Cybersecurity Report

CloudLock

CloudLock, a Cisco company, is a leading provider of cloud access security broker (CASB) solutions that help organizations securely use the cloud. CloudLock delivers visibility and control for software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS) environments across users, data, and applications. CloudLock delivers actionable cybersecurity intelligence through its data scientist-led CyberLab and crowd-sourced security analytics. For more information, visit <https://www.cloudlock.com>.

Security and Trust Organization

Cisco's Security and Trust Organization underscores Cisco's commitment to address two of the most critical issues that are top of mind for boardrooms and world leaders alike. The organization's core missions include protecting Cisco's public and private customers, enabling and ensuring Cisco Secure Development Lifecycle and Trustworthy Systems efforts across Cisco's product and service portfolio, and protecting the Cisco enterprise from ever-evolving threats. Cisco takes a holistic approach to pervasive security and trust, which includes people, policies, processes, and technology. The Security and Trust Organization drives operational excellence, focusing across InfoSec, Trustworthy Engineering, Data Protection and Privacy, Cloud Security, Transparency and Validation, and Advanced Security Research and Government. For more information, visit <http://trust.cisco.com>.

Global Government Affairs

Cisco engages with governments at many different levels to help shape public policy and regulations that support the technology sector and help governments meet their goals. The Global Government Affairs team develops and influences pro-technology public policies and regulations. Working collaboratively with industry stakeholders and association partners, the team builds relationships with government leaders to influence policies that affect Cisco's business and overall ICT adoption, looking to help shape policy decisions at a global, national, and local level. The Government Affairs team is composed of former elected officials, parliamentarians, regulators, senior U.S. government officials, and government affairs professionals who help Cisco promote and protect the use of technology around the world.

Cognitive Threat Analytics

Cisco's Cognitive Threat Analytics is a cloud-based service that discovers breaches, malware operating inside protected networks, and other security threats by means of statistical analysis of network traffic data. It addresses gaps in perimeter-based defenses by identifying the symptoms of a malware infection or data breach using behavioral analysis and anomaly detection. Cognitive Threat Analytics relies on advanced statistical modeling and machine learning to independently identify new threats, learn from what it sees, and adapt over time.

IntelliShield Team

The IntelliShield team performs vulnerability and threat research, analysis, integration, and correlation of data and information from across Cisco Security Research and Operations and external sources to produce the IntelliShield Security Intelligence Service, which supports multiple Cisco products and services.

Talos Security Intelligence and Research Group

Talos is Cisco's threat intelligence organization, an elite group of security experts devoted to providing superior protection for Cisco customers, products, and services. Talos is composed of leading threat researchers supported by sophisticated systems to create threat intelligence for Cisco products that detect, analyze, and protect against known and emerging threats. Talos maintains the official rule sets of Snort.org, ClamAV, SenderBase.org, and SpamCop, and is the primary team that contributes threat information to the Cisco CSI ecosystem.

Security Research and Operations (SR&O)

Security Research and Operations (SR&O) is responsible for threat and vulnerability management of all Cisco products and services, including the industry-leading Product Security Incident Response Team (PSIRT). SR&O helps customers understand the evolving threat landscape at events such as Cisco Live and Black Hat, as well as through collaboration with its peers across Cisco and the industry. Additionally, SR&O delivers new services such as Cisco's Custom Threat Intelligence (CTI), which can identify indicators of compromise that have not been detected or mitigated by existing security infrastructures.

Cisco Visual Networking Index (VNI)

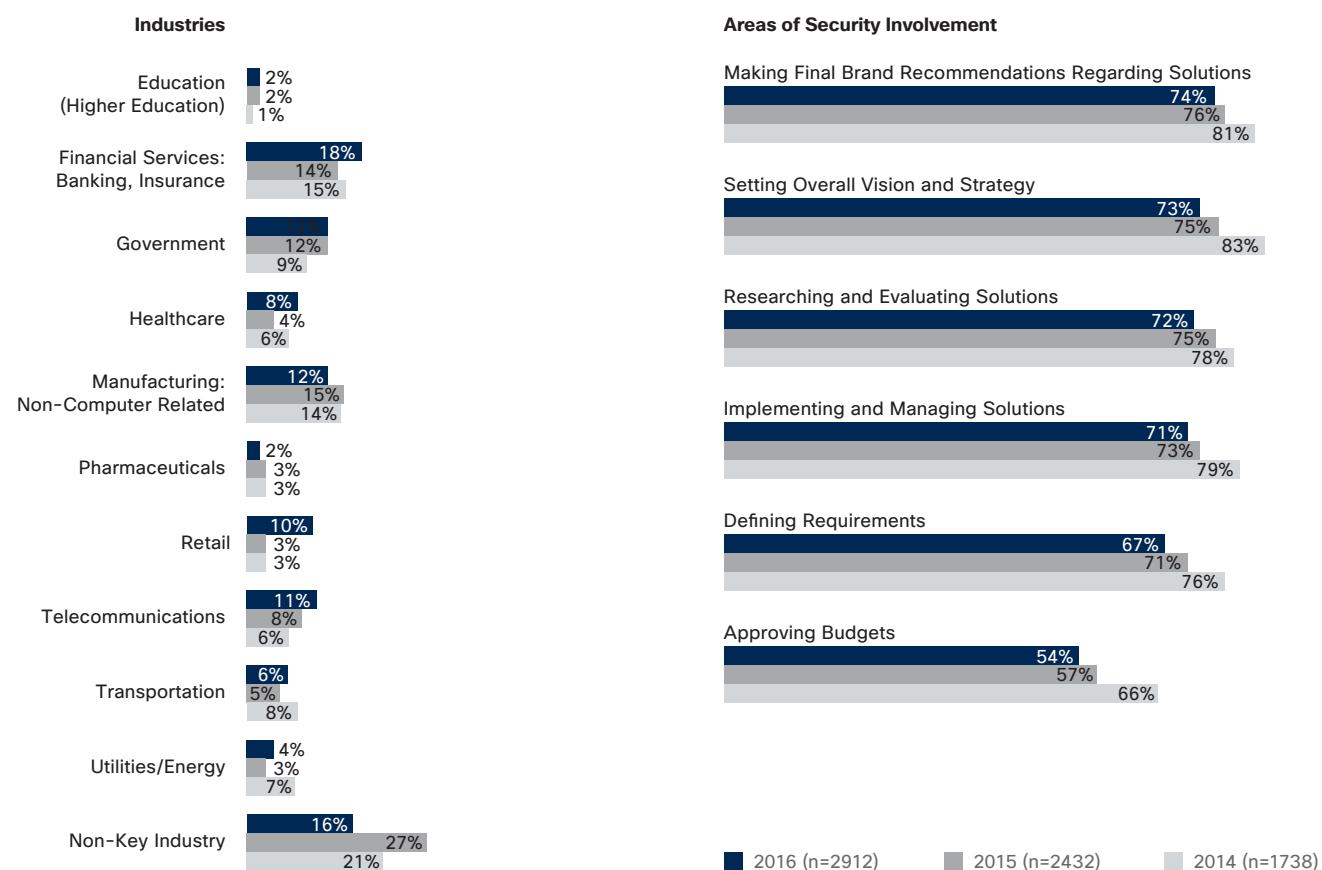
The Cisco VNI Global IP Traffic Forecast for 2015 to 2020 relies on independent analyst forecasts and real-world network usage data. Upon this foundation are layered Cisco's own estimates for global IP traffic and service adoption. A detailed methodology description is included in the complete report. Over its 11-year history, Cisco VNI research has become a highly regarded measure of the Internet's growth. National governments, network regulators, academic researchers, telecommunications companies, technology experts, and industry and business press and analysts rely on the annual study to help plan for the digital future.

Appendix

Appendix

Cisco 2017 Security Capabilities Benchmark Study

Figure 69 Survey Capabilities Benchmark Study



Organization Size

	Midmarket	Enterprise	Large Enterprise	
2016		50%	38%	12%
2015		49%	38%	13%
2014		54%	46%	

CSO vs. Sec Op

	CSO	Sec Op
2016	49%	51%
2015	45%	55%
2014	54%	46%

Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 70 Number of Dedicated Security Professionals

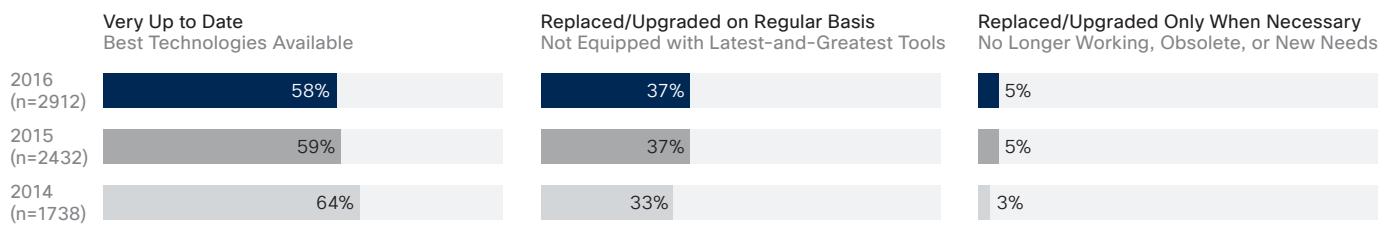
	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)
1-9	18%	17%	15%
10-19	16%	18%	17%
20-29	12%	17%	13%
30-39	8%	9%	8%
40-49	4%	4%	6%
50-99	19%	16%	19%
100-199	9%	9%	9%
200 or more	15%	10%	12%
Median Number of Professionals Dedicated to Security	30	25	33

Source: Cisco 2017 Security Capabilities Benchmark Study

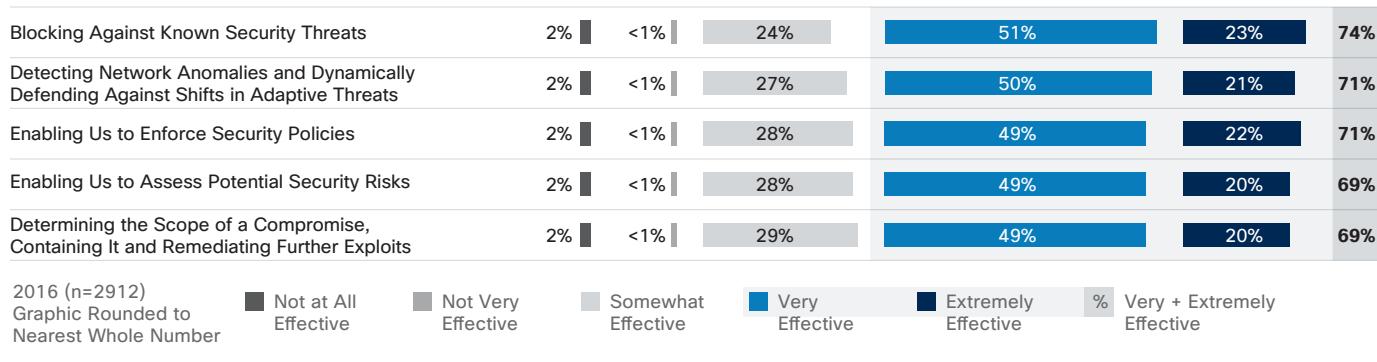
Perceptions

Figure 71 Majority of Security Professionals Feel Security Infrastructure Is Up to Date

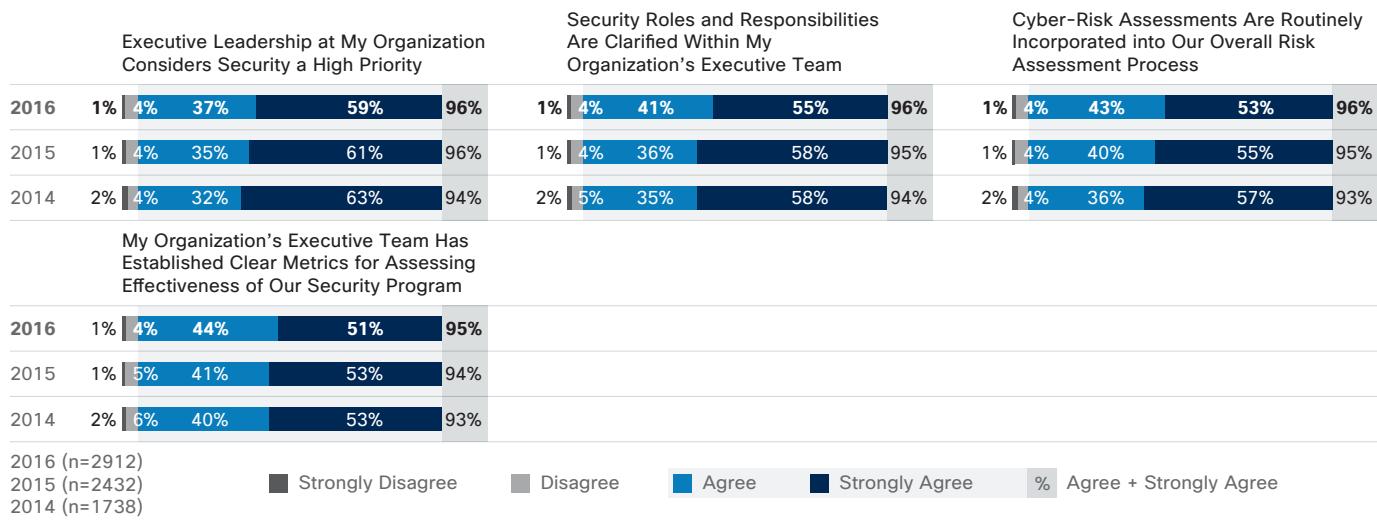
How Would You Describe Your Security Infrastructure?



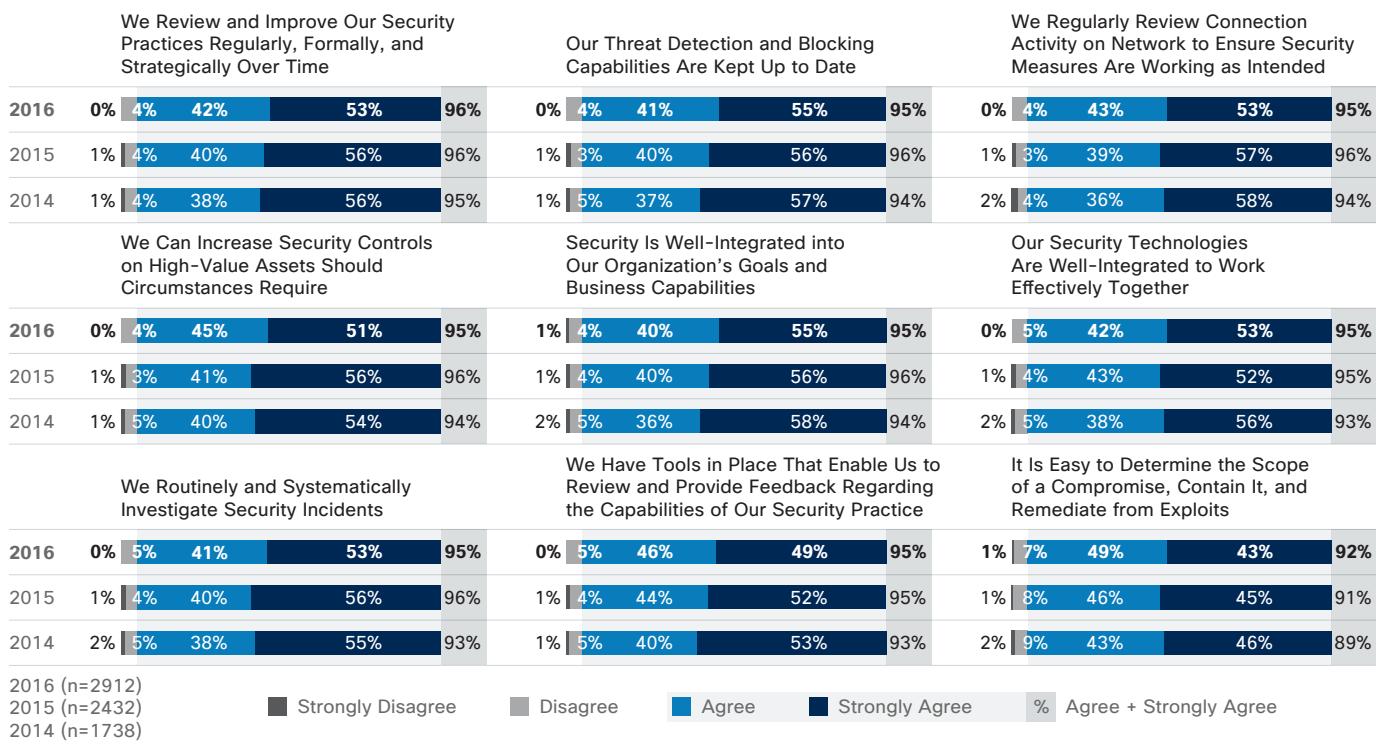
Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 72 Percentages of Security Professionals Who Perceive Various Security Tools to Be Highly Effective


Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 73 Percentages of Security Professionals Who Believe Security Is a High Priority at the Executive Level


Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 74 Percentages of Respondents Who Strongly Agree with Security Operationalization Statements


Source: Cisco 2017 Security Capabilities Benchmark Study

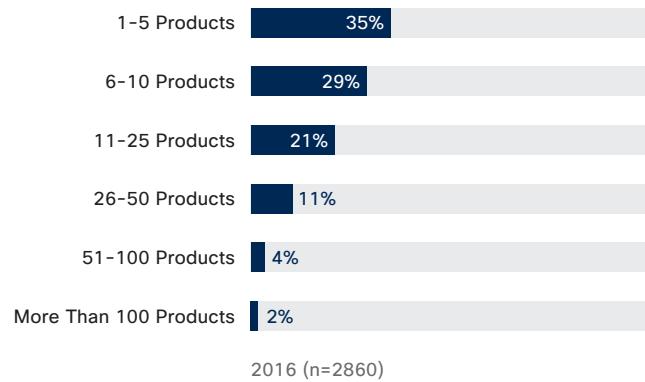
Constraints

Figure 75 Biggest Obstacles to Security

	2015 (n=2432)	2016 (n=2912)
Budget Constraints	39%	35%
Compatibility Issues	32%	28%
Certification Requirements	25%	25%
Lack of Trained Personnel	22%	25%
Competing Priorities	24%	24%
Current Workload Too Heavy	24%	23%
Lack of Knowledge	23%	22%
Reluctance to Purchase Until They're Proven	22%	22%
Organizational Culture/Attitude	23%	22%
Organization Is Not a High-Value Target for Attacks	N/A	18%
Security Is Not an Executive Level Priority	N/A	17%

Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 76 Number of Security Vendors and Products Used by Organizations



Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 77 Number of Security Vendors Used by Size of Organization

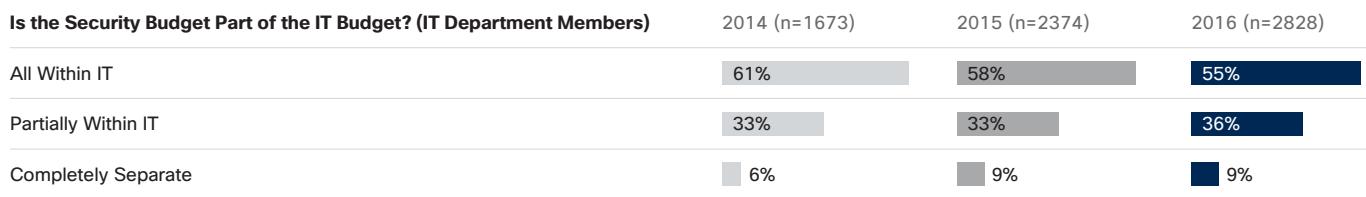
How Many Different Security Vendors (i.e., Brands, Manufacturers) Are in Your Security Environment?	Midmarket 250-1K Employees	Enterprise 1K-10K Employees	Large Enterprise 10K+ Employees
1-5	46.9%	43.4%	39.9%
6-10	28.4%	30.9%	21.3%
11-20	17.6%	15.8%	23.1%
21-50	5.6%	7.1%	8.7%
More Than 50	1.4%	2.8%	6.9%
Total Organizations	1435	1082	333

Source: Cisco 2017 Security Capabilities Benchmark Study

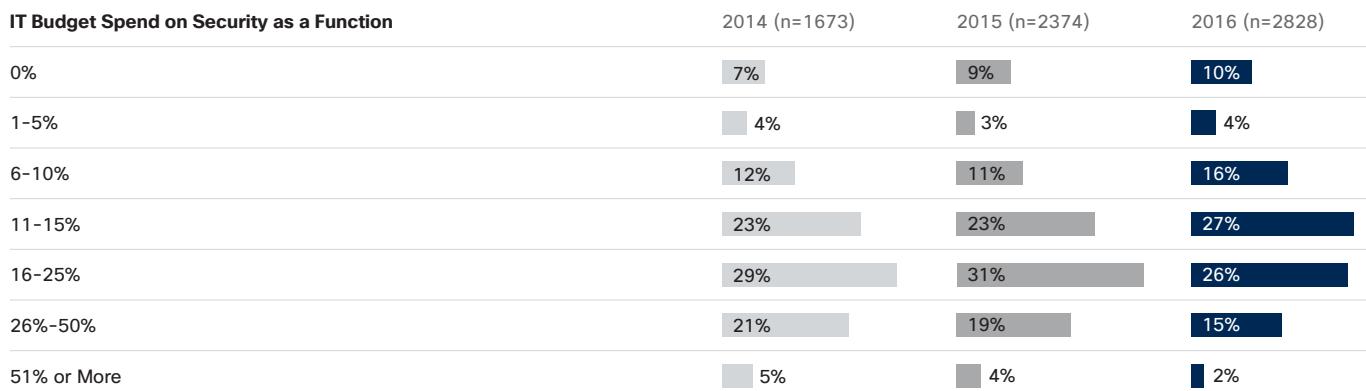
Figure 78 Number of Security Products Used by Size of Organization

How Many Different Security Products Are in Your Security Environment?	Midmarket 250-1K Employees	Enterprise 1K-10K Employees	Large Enterprise 10K+ Employees
1-5	37.9%	32.7%	25.1%
6-10	29.0%	30.1%	22.5%
11-25	19.8%	20.4%	23.7%
26-50	9.6%	10.5%	15.6%
51-100	3.0%	4.3%	7.8%
More Than 100	0.8%	1.9%	5.4%
Total Organizations	1442	1084	334

Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 79 Year-over-Year Decrease of Security Budget Coming Within IT Budget

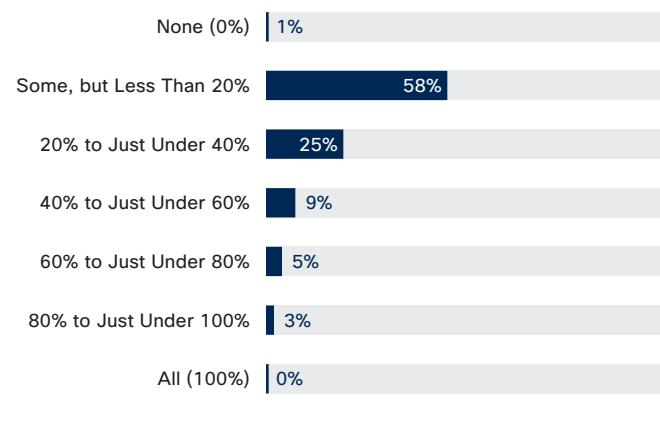
Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 80 Year-over-Year Decrease of Security Spend as a Proportion of the IT Budget

Source: Cisco 2017 Security Capabilities Benchmark Study

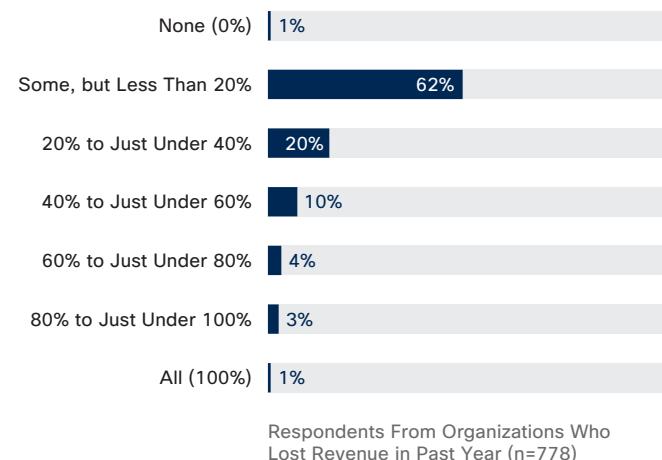
Impacts

Figure 81 Percentages of Organization's Opportunities Lost as a Result of Attacks



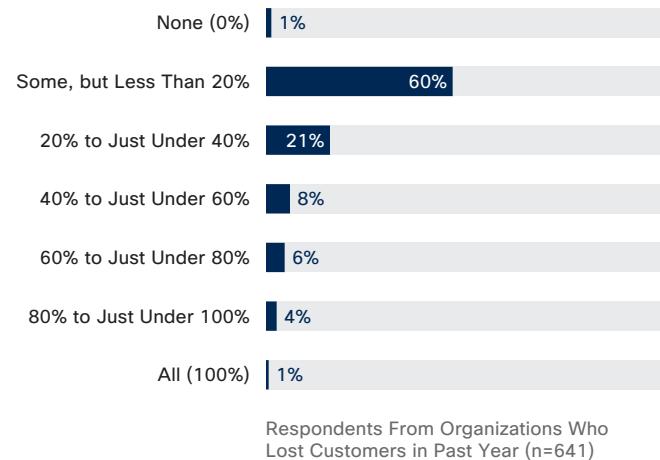
Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 82 Percentages of Organization's Revenue Lost as a Result of Attacks



Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 83 Percentages of Organization's Customers Lost as a Result of Attacks



Source: Cisco 2017 Security Capabilities Benchmark Study

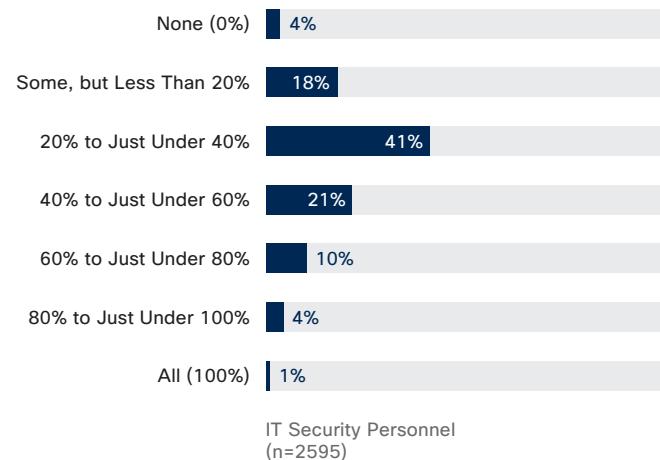
Outcomes

Figure 84 Percentages of Organizations Relying on Outsourcing

Which Security Services Are Outsourced?	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)	Why Are These Services Outsourced?	2015 (n=2129)	2016 (n=2631)
Advice and Consulting	51%	52%	51%	More Cost-Efficient	53%	52%
Audit	41%	47%	46%	Desire for Unbiased Insight	49%	48%
Incident Response	35%	42%	45%	More Timely Response to Incidents	46%	46%
Monitoring	42%	44%	45%	Lack of Internal Expertise	31%	33%
Threat Intelligence	N/A	39%	41%	Lack of Internal Resources	31%	33%
Remediation	34%	36%	35%			
None/All Internal	21%	12%	10%			

Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 85 Percentages of Organization's Security Reliant Upon Third-Party Vendors

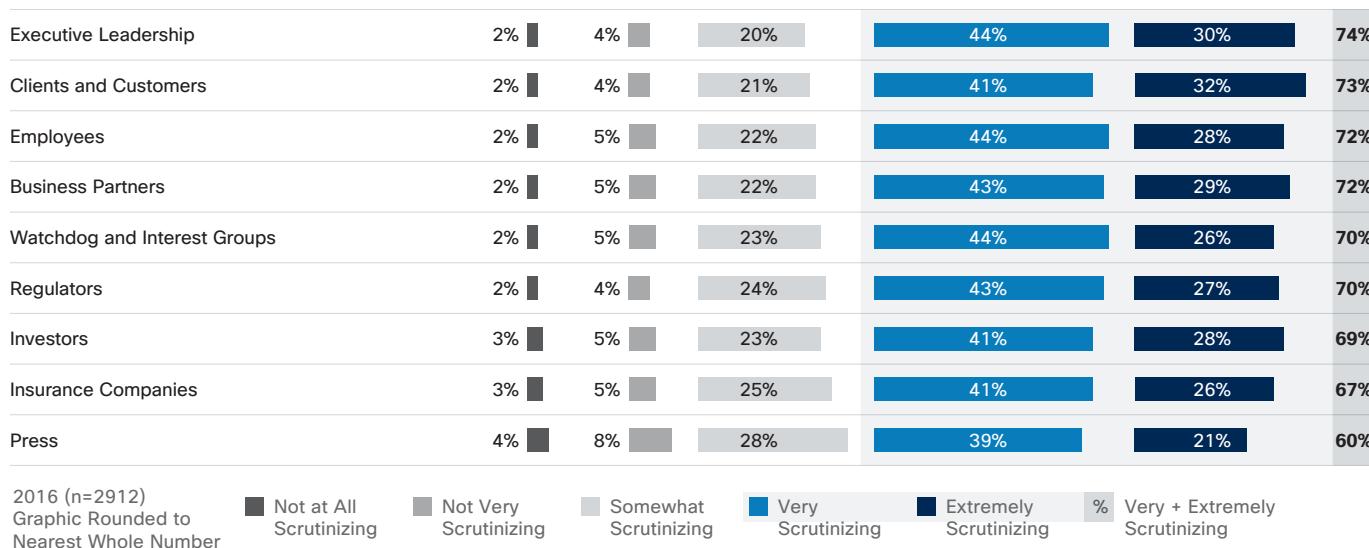


Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 86 Percentages of Security Services Outsourced by Size of Organization

Which Security Services Are Outsourced?	Midmarket (n=1459)	Enterprise (n=1102)	Large Enterprise (n=351)
Advice and Consulting	50%	52%	51%
Audit	44%	47%	50%
Monitoring	46%	43%	44%
Threat Intelligence	41%	41%	40%
Incident Response	48%	44%	39%
Remediation	35%	34%	37%
None/All Internal	8%	11%	11%

Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 87 Sources of Increased Scrutiny


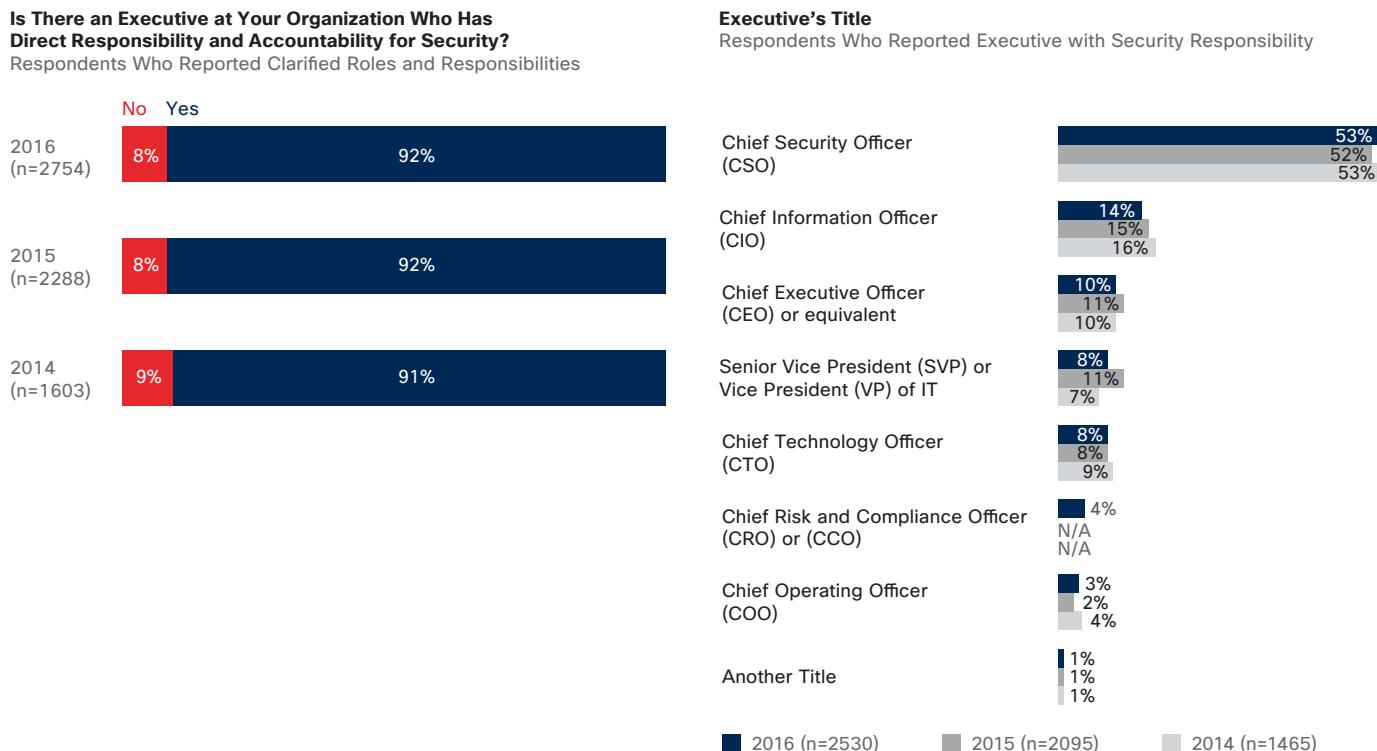
Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 88 Increase of Off-Premises Private Cloud and Third-Party Managed On-Premises Hosting

Where Networks Are Hosted	2014 (n=1727)	2015 (n=2417)	2016 (n=2887)
On-Premises as Part of a Private Cloud	50%	51%	50%
On-Premises	54%	48%	46%
On-Premises but Managed by an External Third-Party	23%	24%	27%
Off-Premises Private Cloud	18%	20%	25%
Off-Premises Public Cloud	8%	10%	9%

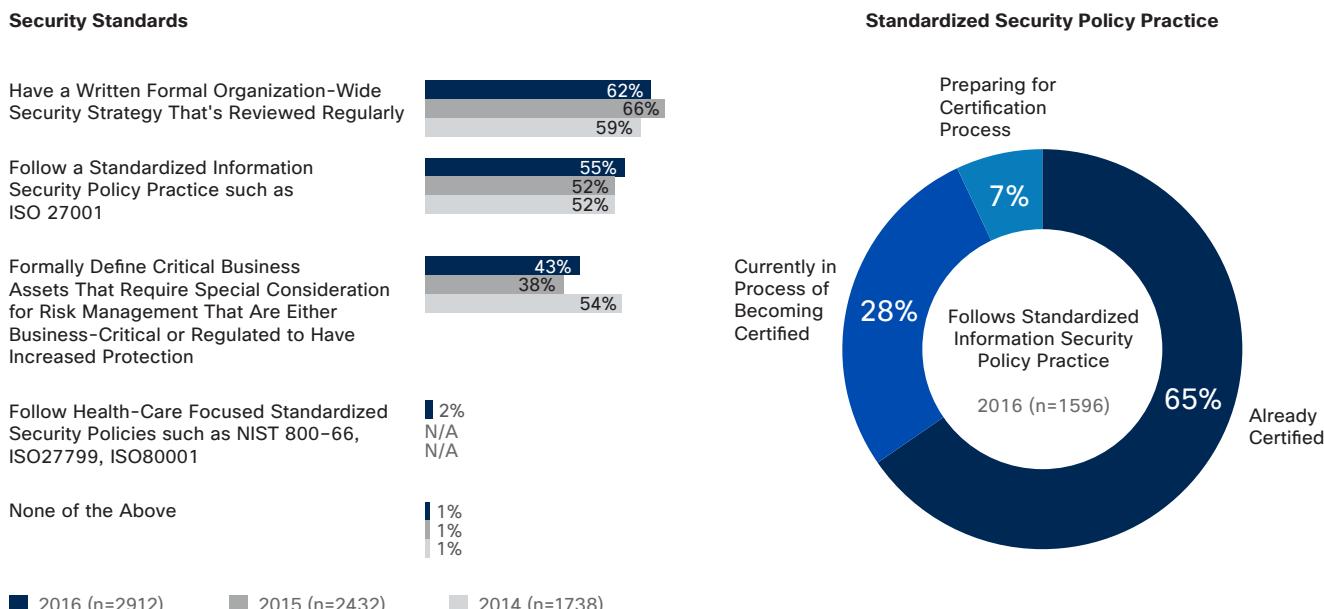
Source: Cisco 2017 Security Capabilities Benchmark Study

Operations, Policies, Procedures, and Capabilities

Figure 89 Proportion of Companies with a Security Executive

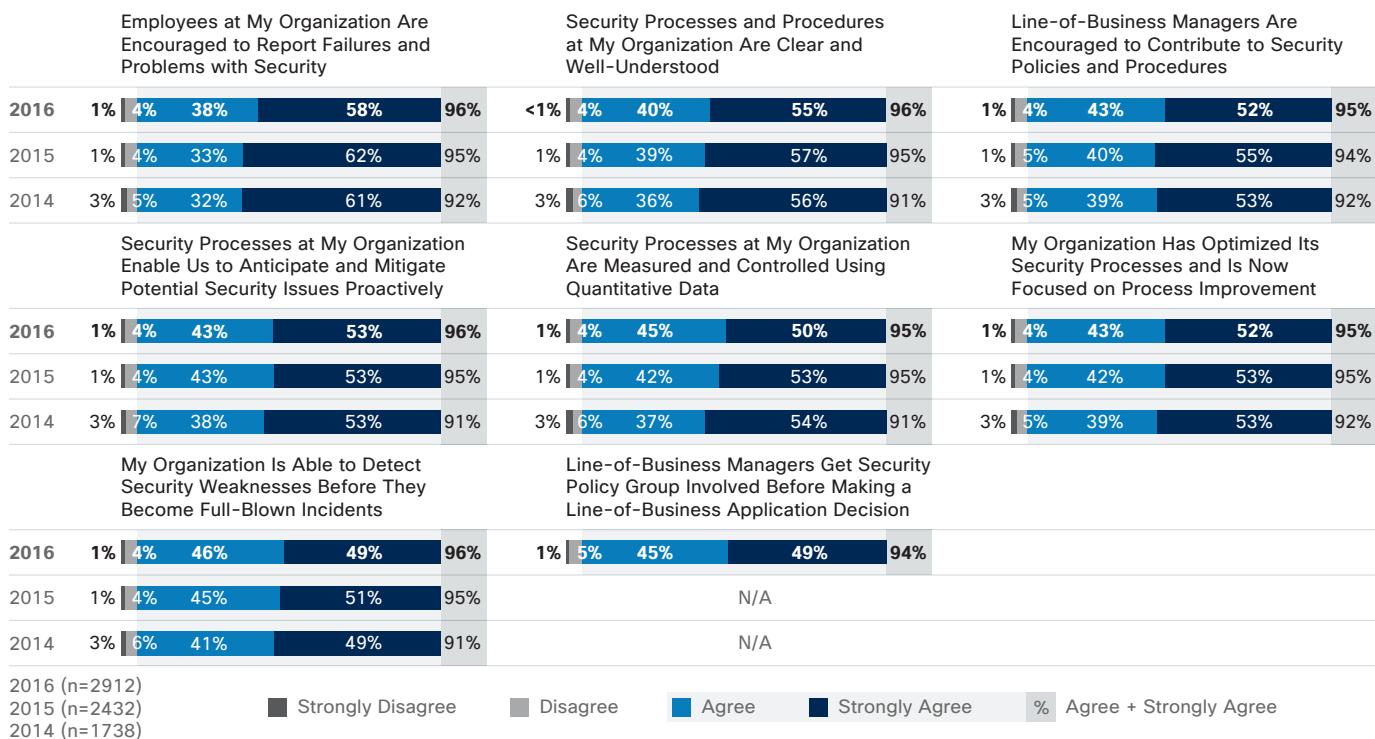
Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 90 Percentages of Companies That Have a Formal Organization-Wide Security Strategy and Follow Standardized Security Policy Practices

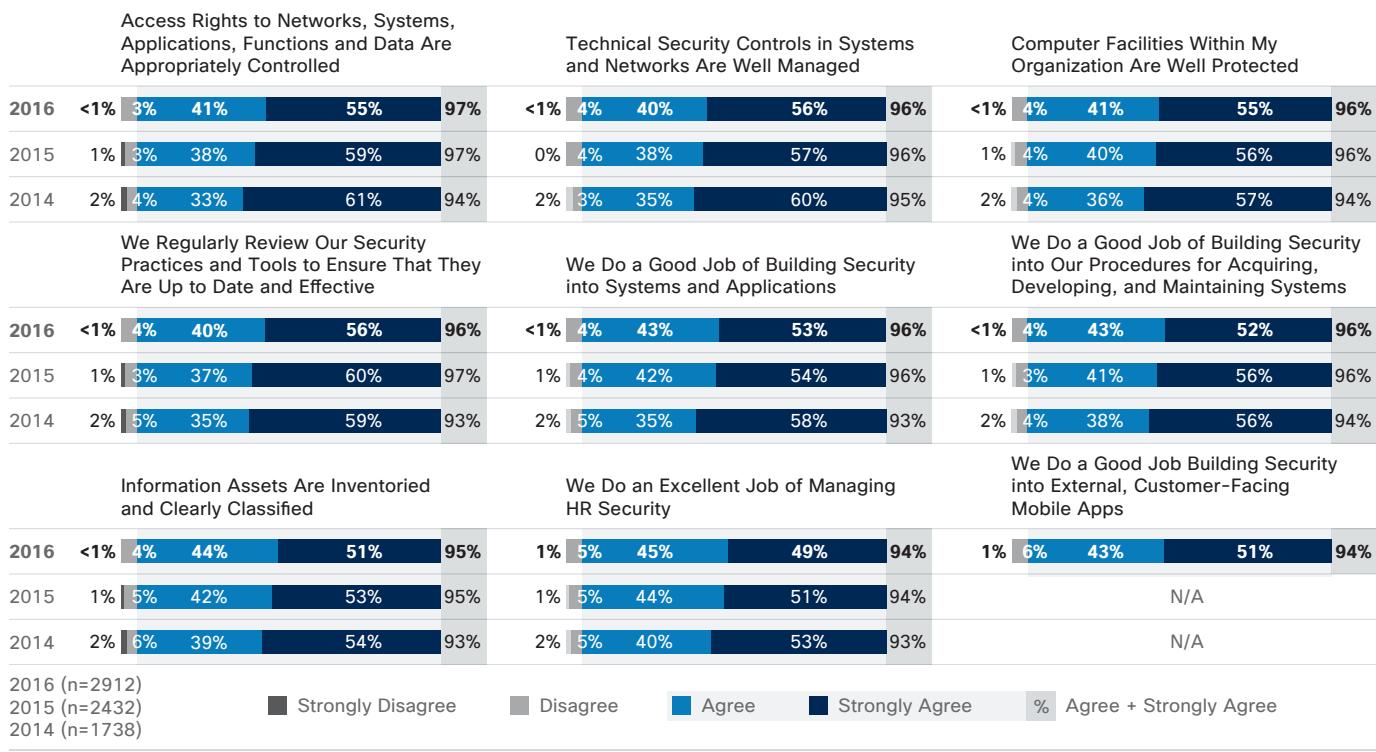


Source: Cisco 2017 Security Capabilities Benchmark Study

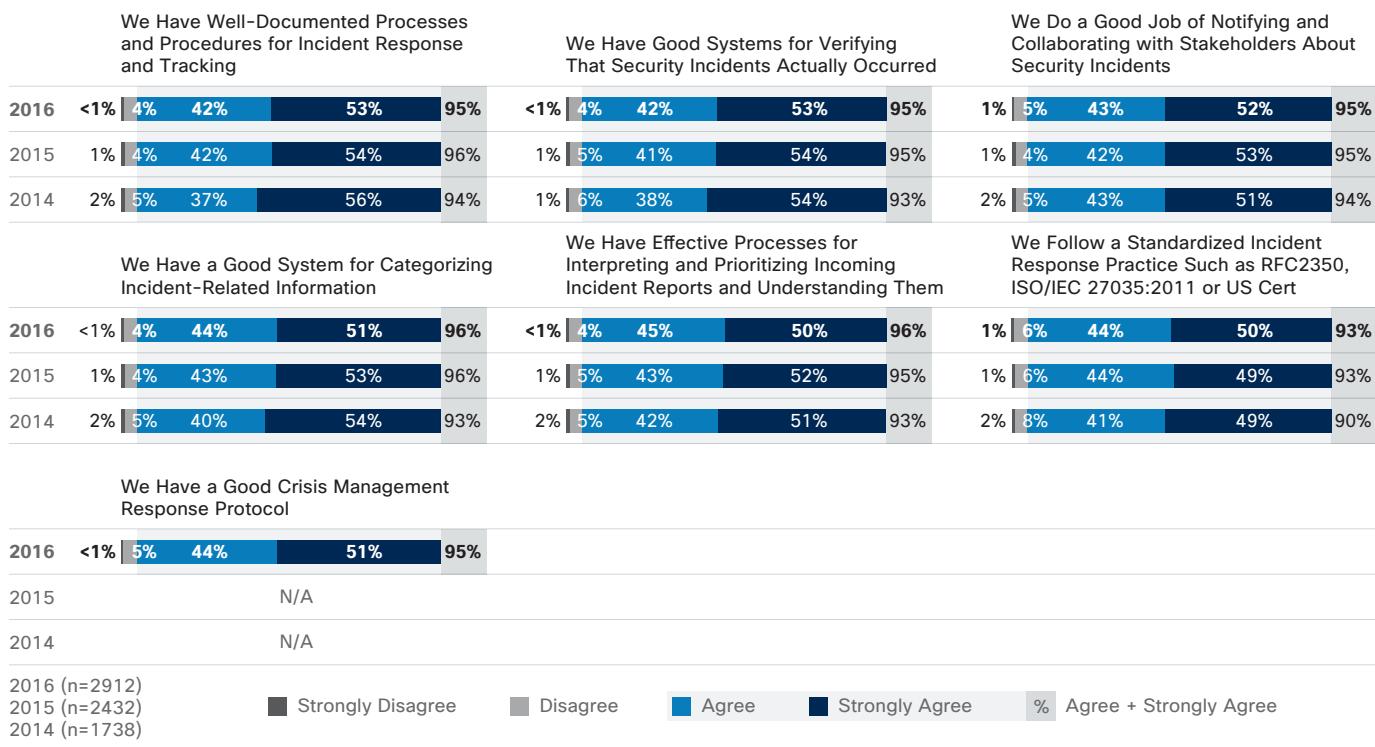
Figure 91 Percentages of Respondents Who Strongly Agree with Security Process Statements



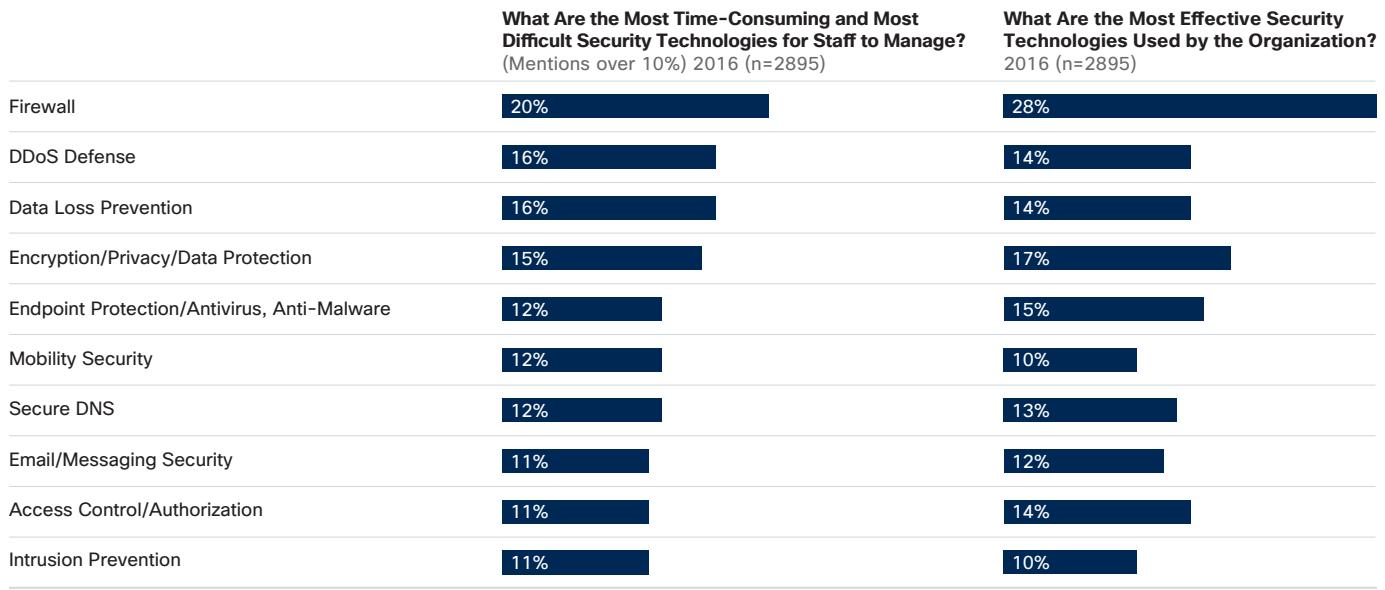
Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 92 Percentages of Respondents Who Strongly Agree with Security Process Statements


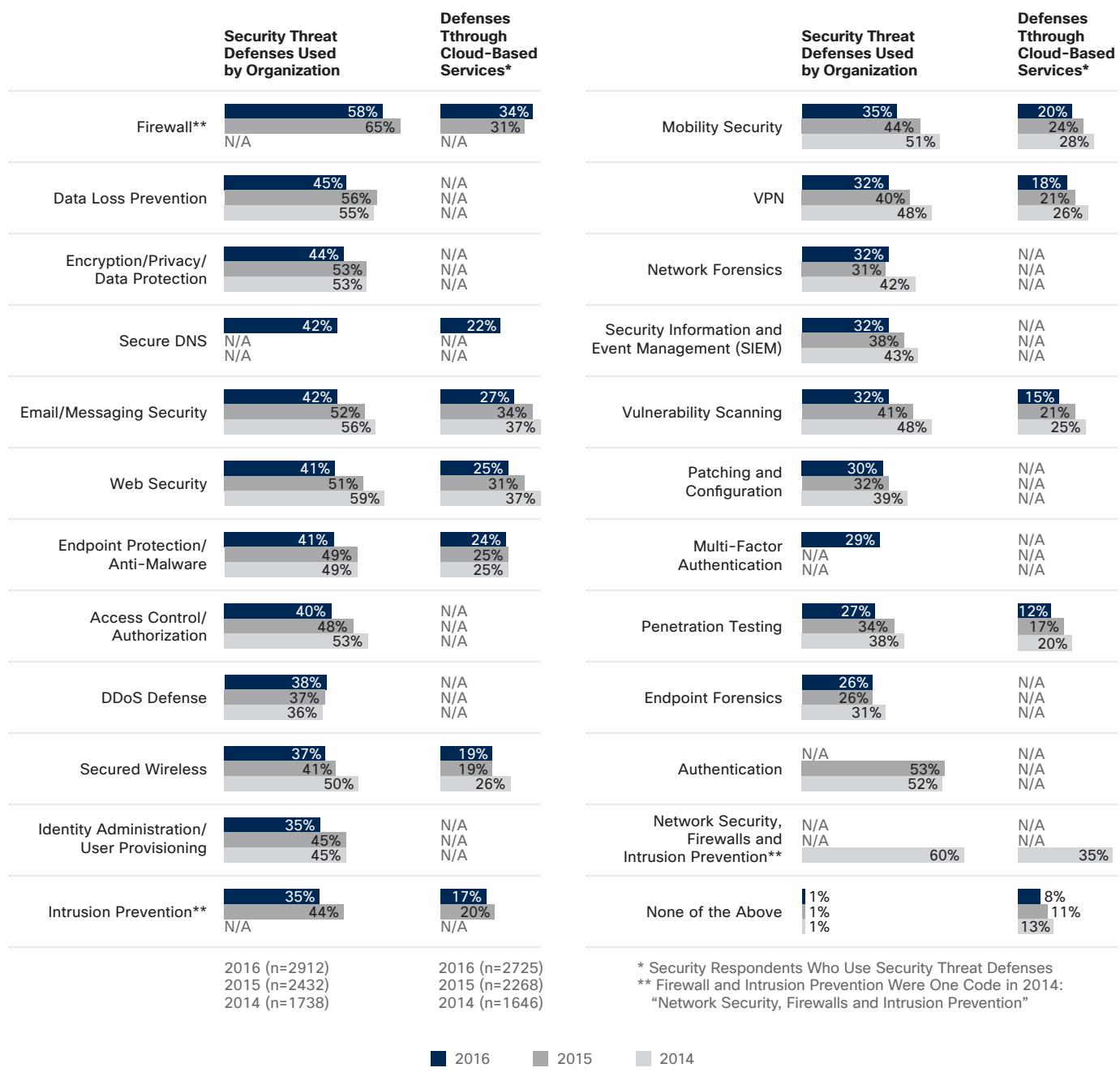
Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 93 Percentages of Respondents Who Strongly Agree with Security Controls Statements


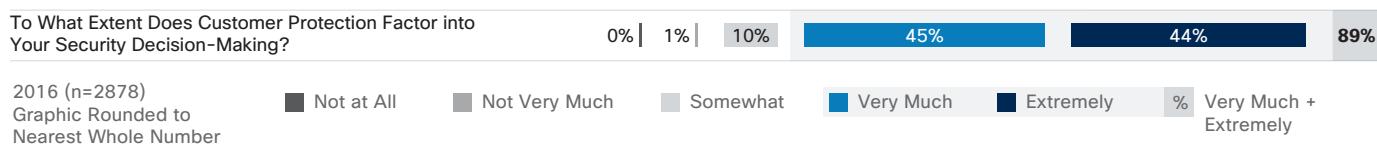
Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 94 Management and Efficacy of Security Technologies


Source: Cisco 2017 Security Capabilities Benchmark Study

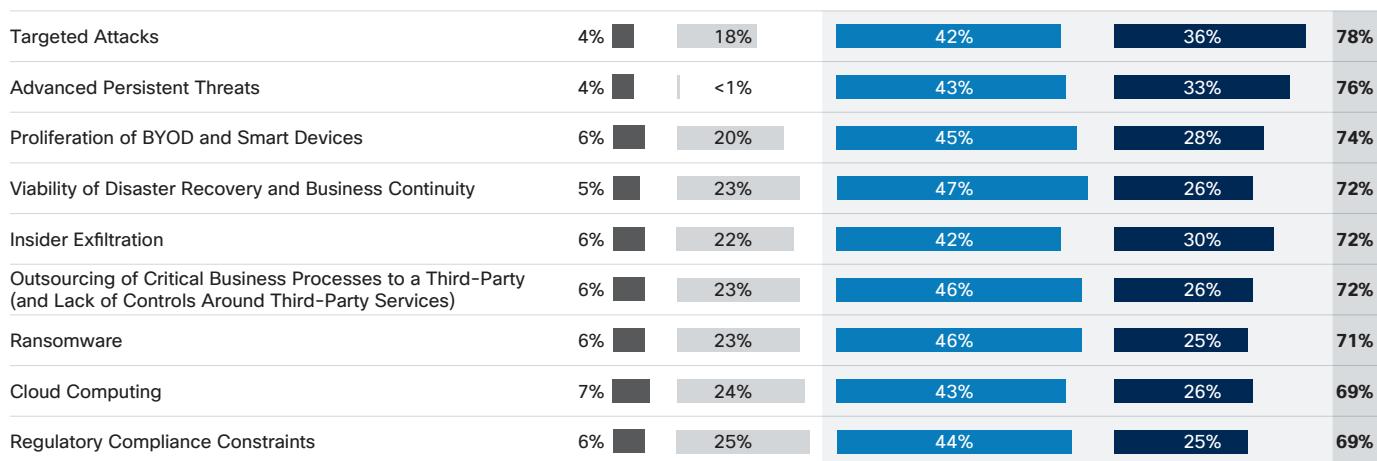
Figure 95 Year-over-Year Use of Security Threat Defense


Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 96 Extent That Customer Protection Factors into Security Decision-Making

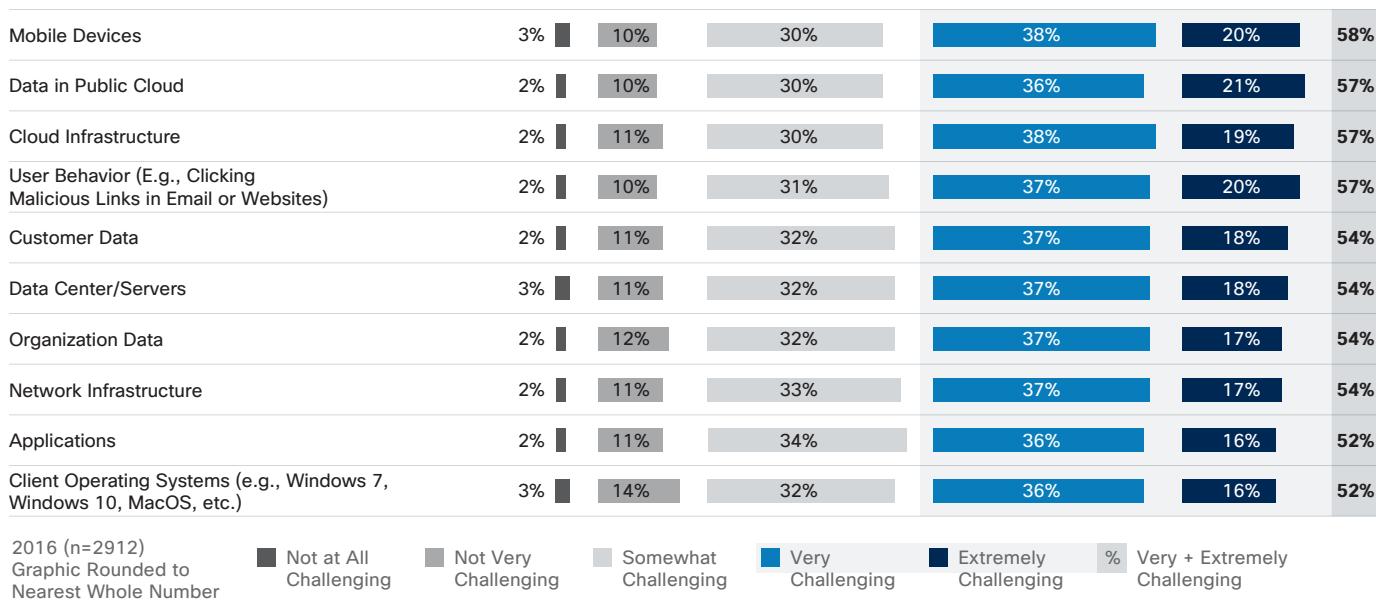
Source: Cisco 2017 Security Capabilities Benchmark Study

Risks and Vulnerabilities

Figure 97 IT Security Personnel's Biggest Sources of Concern Related to Cyber Attacks

2016 (n=2912)
Graphic Rounded to Nearest Whole Number

Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 98 Security Professionals' Biggest Sources of Concern Related to Cyber Attacks


Source: Cisco 2017 Security Capabilities Benchmark Study

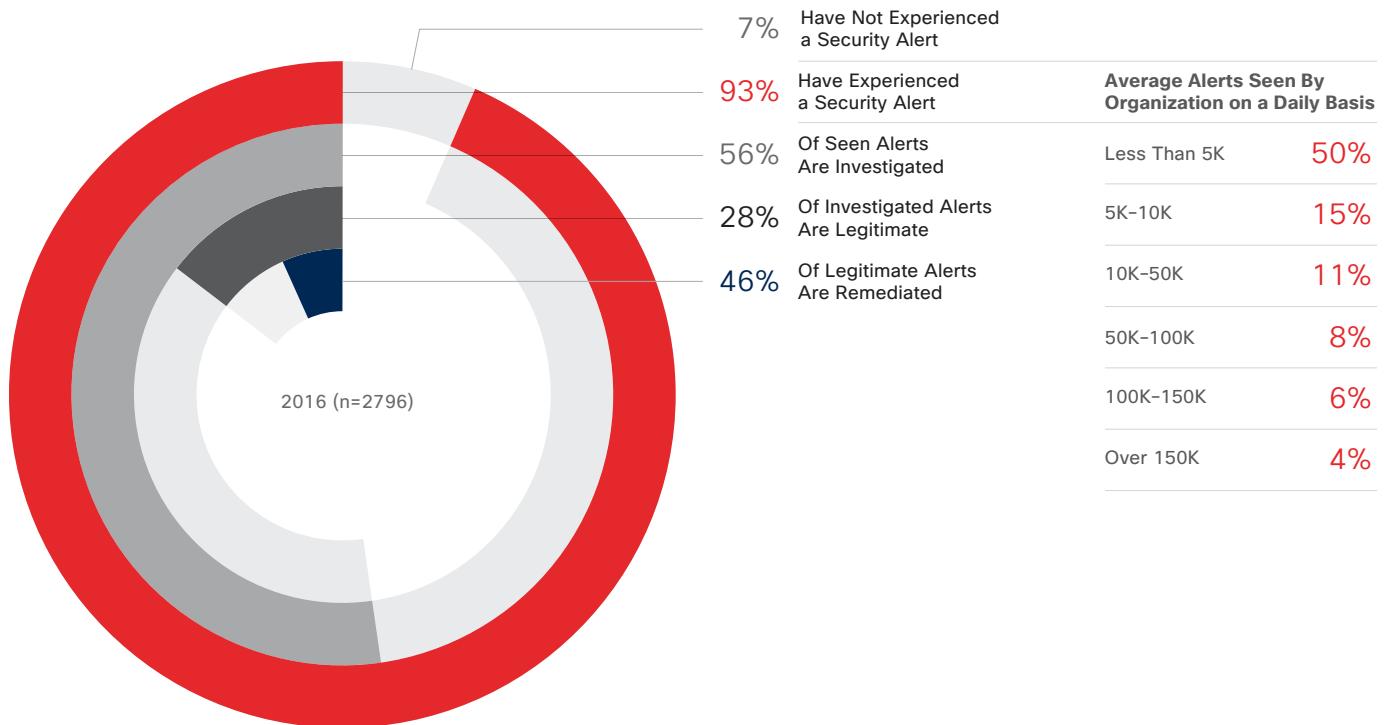
Figure 99 Distribution of Security Teams' Efforts

IT Security Personnel (n=2854)	Endpoints	Customer Data	Servers
Where Does the Security Team Spend the Majority of Its Efforts?	23%	29%	47%

Source: Cisco 2017 Security Capabilities Benchmark Study

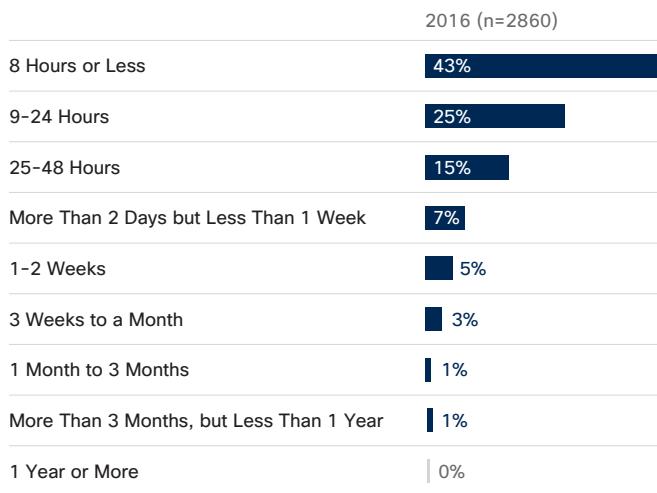
Incident Response

Figure 100 Percentages of Security Alerts That Are Investigated or Remediated

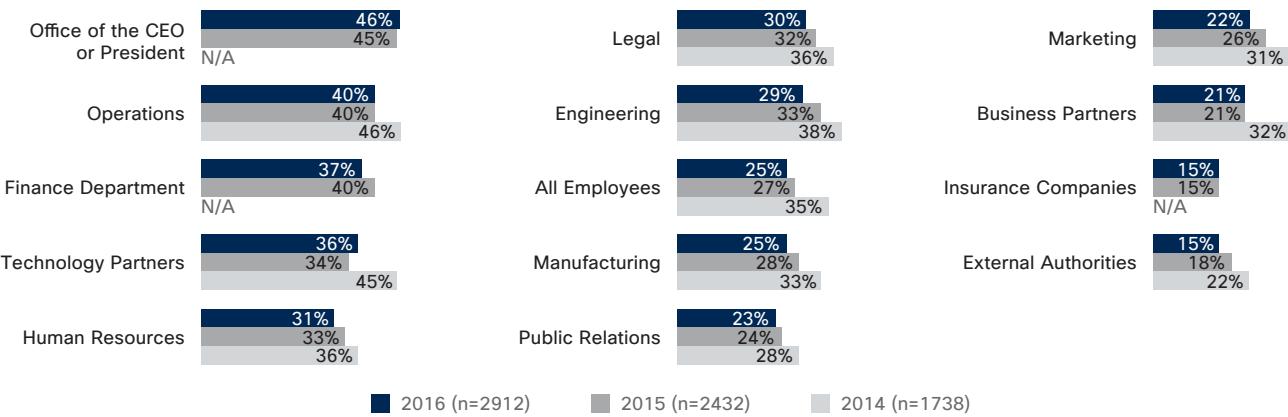


Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 101 Average Time to Detect Security Breaches



Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 102 Groups Notified in the Event of an Incident

Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 103 KPIs Used by Organizations to Assess Security Performance

Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 104 Year-over-Year Use of Process to Analyze Compromised Systems

Processes to Analyze Compromised Systems	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)
Firewall Log	61%	57%	56%
System Log Analysis	59%	53%	50%
Network Flow Analysis	53%	49%	49%
Malware or File Regression Analysis	55%	48%	47%
Registry Analysis	50%	47%	43%
Full Packet Capture Analysis	47%	38%	40%
IOC Detection	38%	35%	38%
Disk Forensics	40%	36%	36%
Correlated Event/Log Analysis	42%	37%	35%
Memory Forensics	41%	34%	34%
External Incident Response/Analysis Teams	37%	33%	34%
None of the Above	2%	1%	1%

Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 105 Year-over-Year Use of Process to Eliminate the Cause of Security Incidents

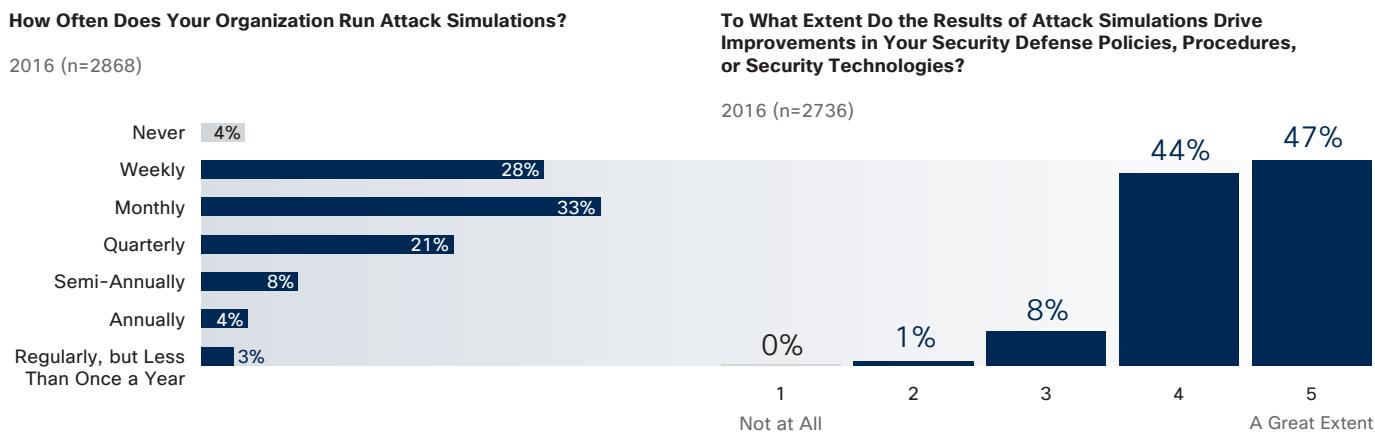
Processes to Eliminate Cause of Security Incidents	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)
Quarantine or Remove Malicious Application	58%	55%	52%
Root Cause Analysis	55%	55%	51%
Stop Communication of Malicious Software	53%	53%	48%
Additional Monitoring	52%	48%	48%
Policy Updates	51%	47%	45%
Stop Communication of Compromised Application	48%	47%	43%
Long-Term Fix Development	47%	40%	41%
Re-image System to Previous State	45%	41%	39%
None of the Above	2%	1%	1%

Source: Cisco 2017 Security Capabilities Benchmark Study

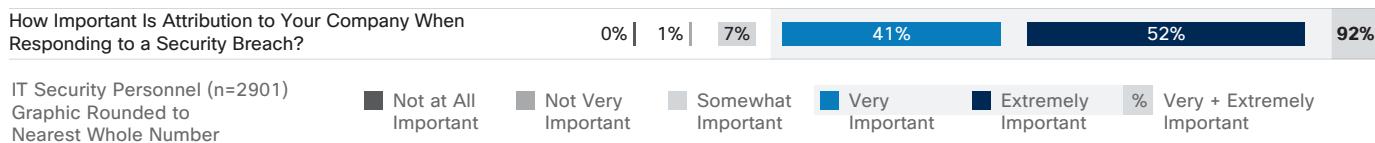
Figure 106 Year-over-Year Use of Process to Restore Affected Systems

Processes to Restore Affected Systems	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)
Implementing Additional or New Detections and Controls Based on Identified Weaknesses Post Incident	60%	56%	56%
Restoring from a Pre-Incident Backup	57%	59%	55%
Patching and Updating Applications Deemed Vulnerable	60%	55%	53%
Differential Restoration (Removing Changes Caused by an Incident)	56%	51%	50%
Gold Image Restoration	35%	35%	34%
None of the Above	2%	1%	1%

Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 107 Attack Simulations: Frequency and Extent of Driving Security Defense Improvements

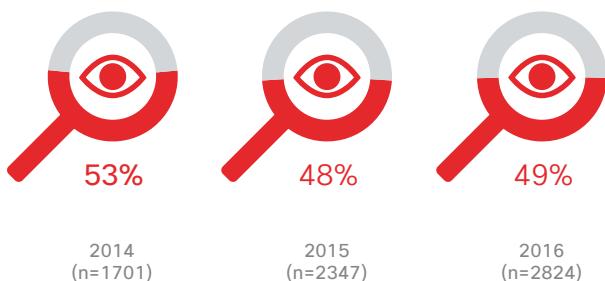
Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 108 Importance of Attributing Origin of a Security Breach

Source: Cisco 2017 Security Capabilities Benchmark Study

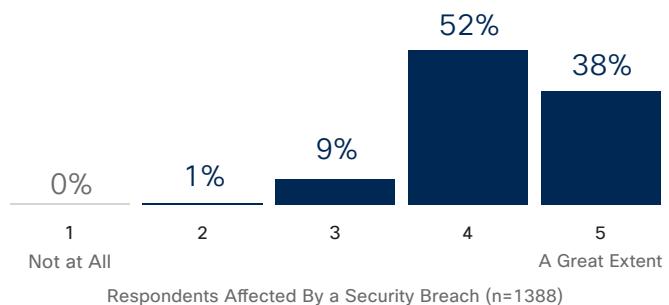
Breaches and Their Impacts

Figure 109 Percentage of Organizations Experience a Public Breach



Source: Cisco 2017 Security Capabilities Benchmark Study

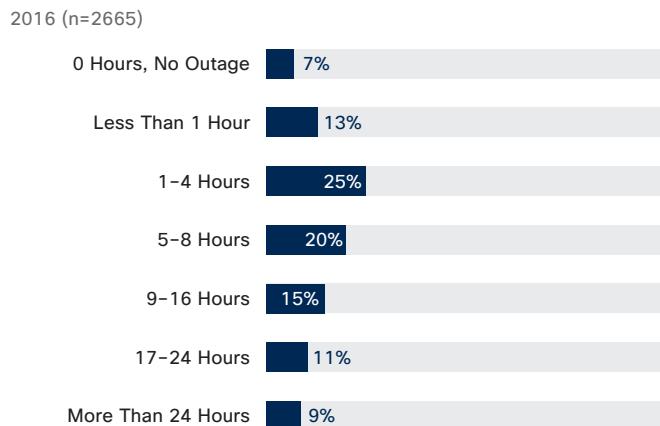
Figure 110 How Much Did the Breach Drive Improvements in Your Security Threat Defense Policies, Procedures, or Technologies?



Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 111 Length and Extent of Outages Caused by Security Breaches

Length of System Outages Due to Breach



Source: Cisco 2017 Security Capabilities Benchmark Study

Percentage of Systems Impacted Due to Breach

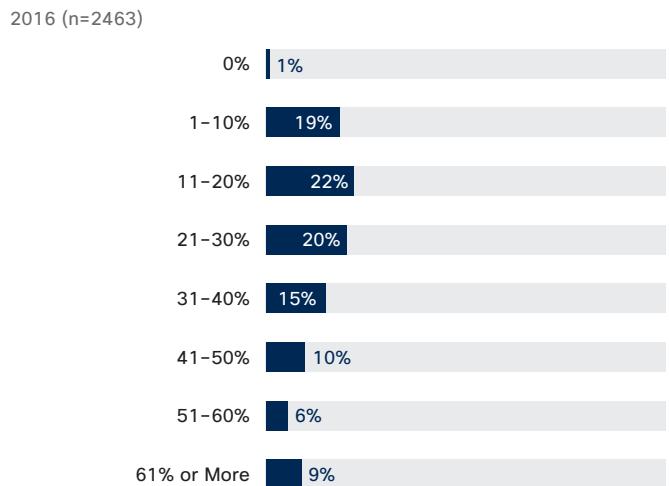


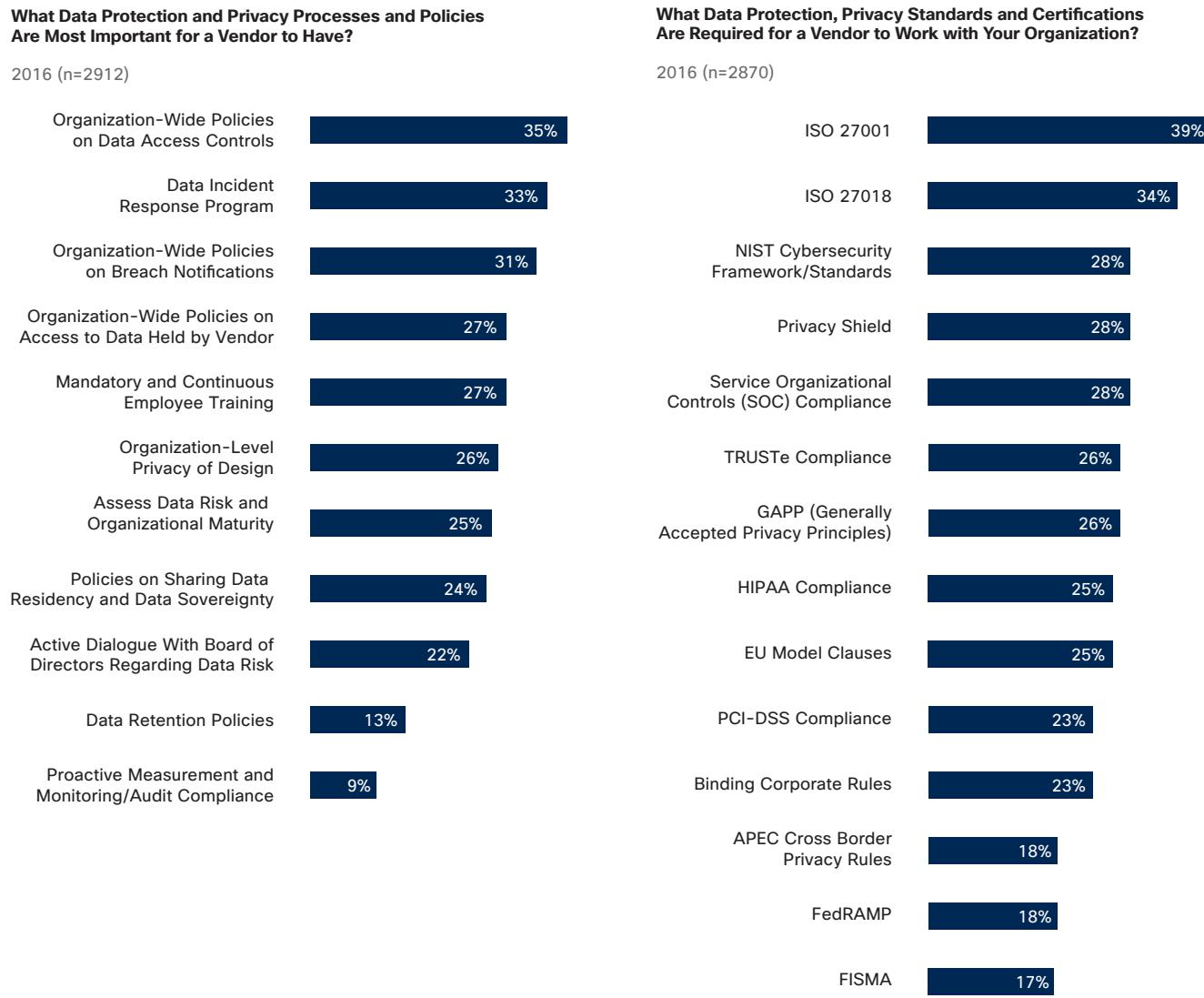
Figure 112 Improvements Made to Protect Your Company from Security Breaches



Source: Cisco 2017 Security Capabilities Benchmark Study

Vendor Choice and Expectations

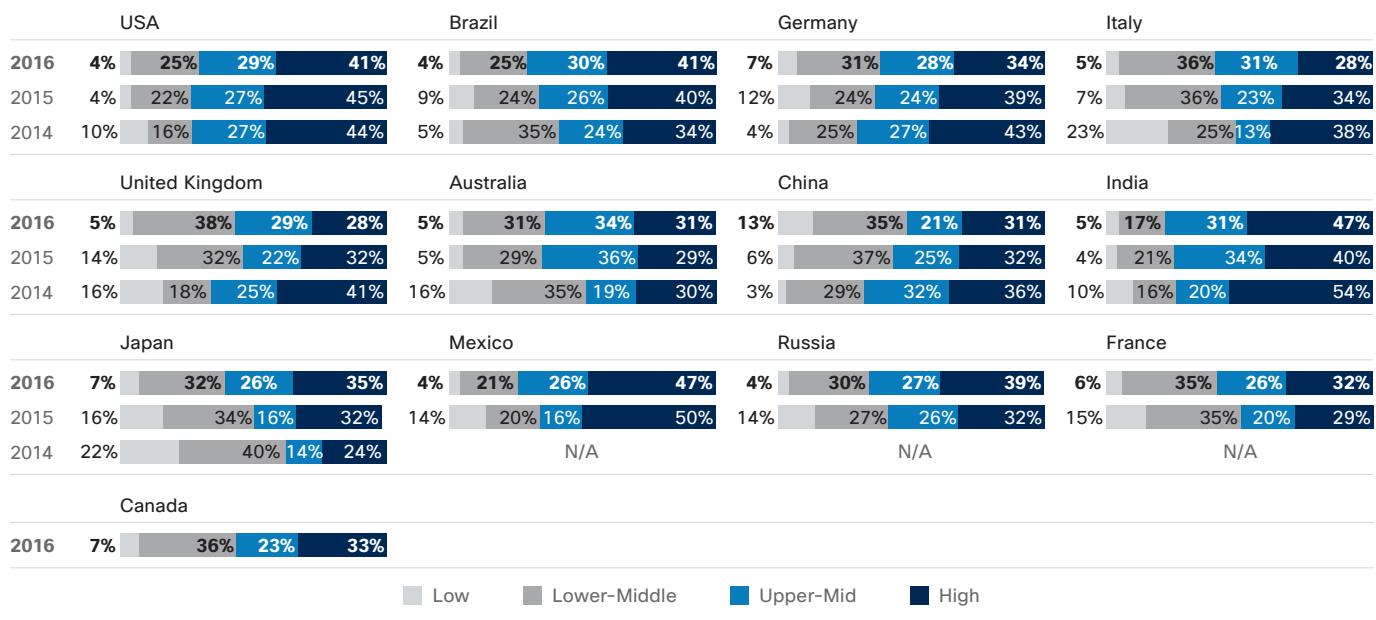
Figure 113 Importance of Data Protection and Privacy for Vendors



Source: Cisco 2017 Security Capabilities Benchmark Study

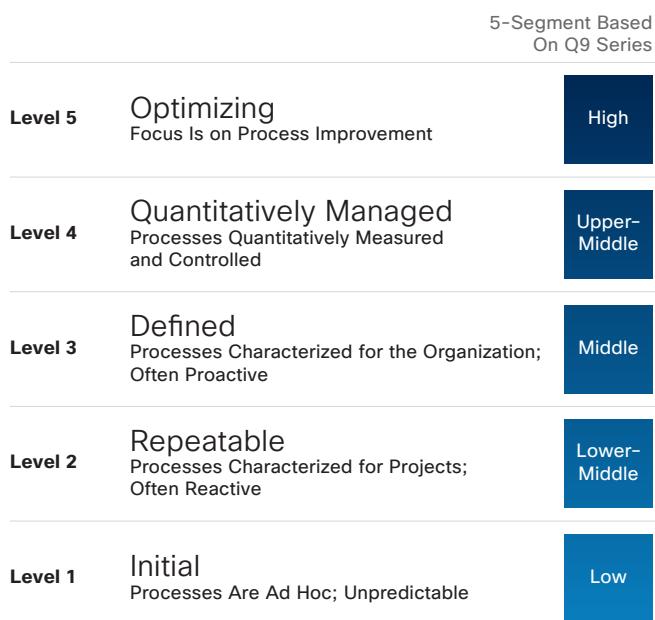
Security Capability Maturity Model

Figure 114 Security Maturity by Country



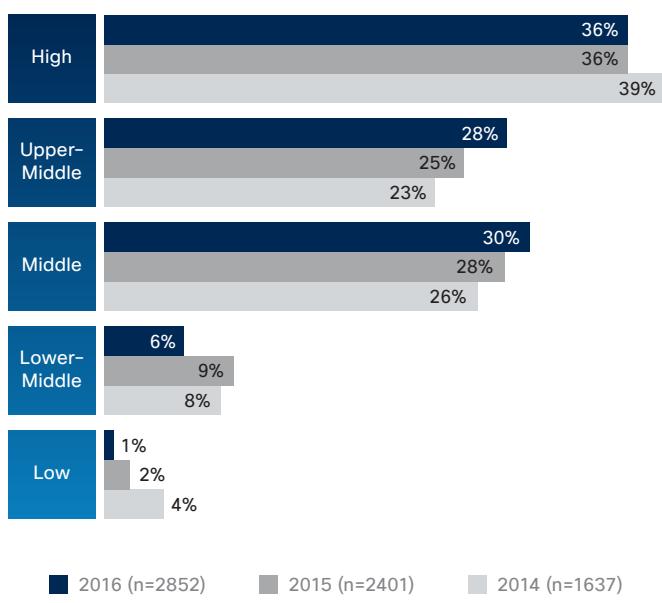
Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 115 Maturity Model Ranks Organizations Based on Security Process



Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 116 Segment Sizing for Maturity Model



Source: Cisco 2017 Security Capabilities Benchmark Study

Industry-Specific

Figure 117 Percentage of Healthcare Businesses That Have Implemented Standardized Security Policies

Implemented Standardized Security Policies

Healthcare Business Follows Healthcare-Specific Information Security Policy Practice, 2016 (n=65)

ISO80001 (Medical Device)	74%
ISO27799	60%
NIST 800-66	45%

Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 118 Resources Healthcare Companies Use to Measure Themselves Against HIPAA Privacy Rules

Which Resources Are Used to Measure Companies Against HIPAA Privacy Rules and Security?

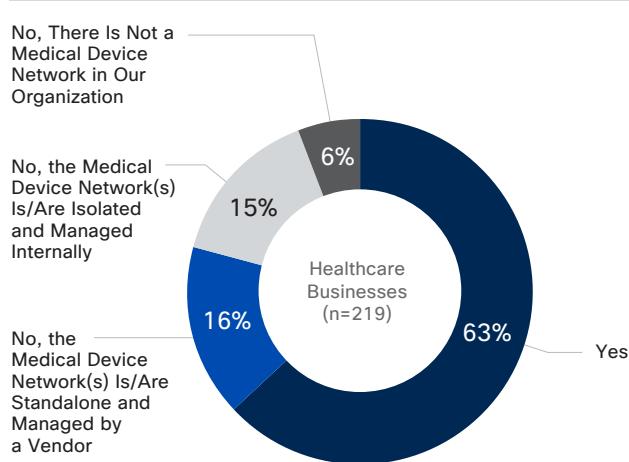
Healthcare Businesses 2016 (n=219)

HIT Security Guidance	52%
Current HIPAA Document (Currently Omnibus)	52%
HHS.OCR Audit Frameworks	40%
HITRUST or Other Private Framework	37%
Third-Party Assessments	24%
None of the Above	6%

Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 119 Most Common Security Measures Among the Healthcare Businesses with Medical Device Networks

Does Your Organization Have a Medical Device Network That Is Converged with a Main Hospital Network?

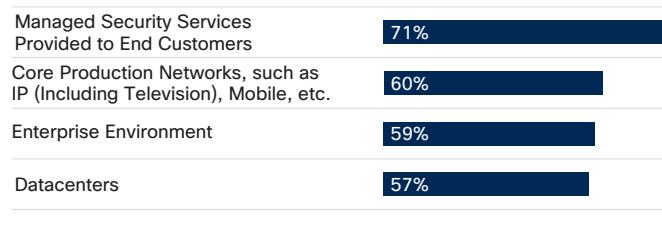


Source: Cisco 2017 Security Capabilities Benchmark Study

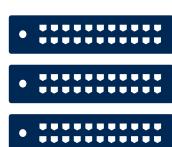
Which of These Security Measures, if Any, Has Your Company Implemented to Protect and Secure Your Medical Device Network?

Companies with a Medical Device Network in Their Organization (n=207)

Network Access Control	59%
Advanced Malware Protection/Detection	56%
Multi-Factor Device Authentication	49%
IPS/IDS, Deep Packet Inspection	48%
Automated Threat Defense/Response	48%
Traffic Analysis/Anomaly Detection	45%
Posture Assessments and/or Device Profiling	40%
Segmentation/Micro Segmentation	32%
None of the Above	1%

Figure 120 Sample Profile for Telecommunications**Which Telecommunications Subsector Is Your Organization Primarily Involved In?**
Telecommunications Businesses (n=307)**Which of These Services Does Your Company Offer to Your Customers?**
Telecommunications Businesses (n=308)

Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 121 Security Strategies Factors for Telecommunications**Relative Priority to Security Strategies and Protocols**
Telecommunications Businesses (n=308)

Average Percentage of Availability

34%

Availability: Assuring Reliable Access to Data

Average Percentage of Confidentiality

36%

Confidentiality: Assuring That Data Is Only Accessed by Appropriate Parties

Average Percentage of Integrity

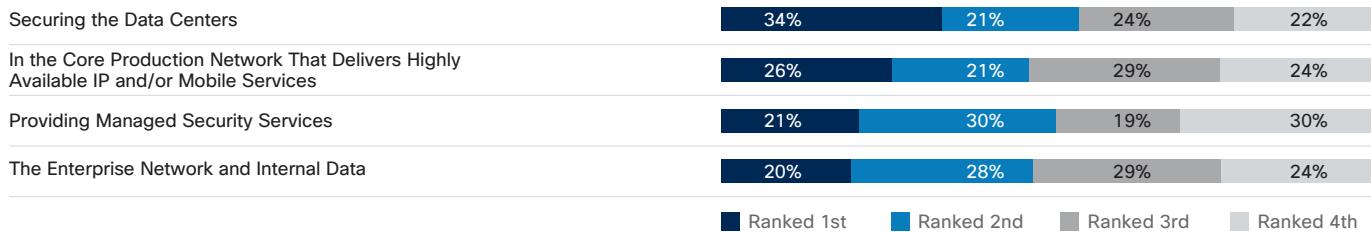
31%

Integrity: Assuring That Data Is Precise and Accurate

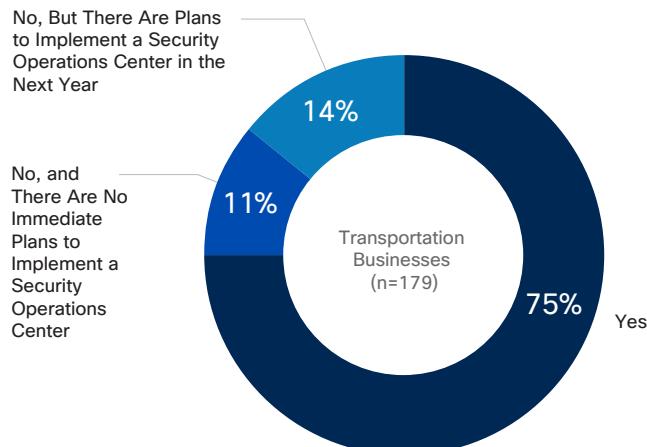
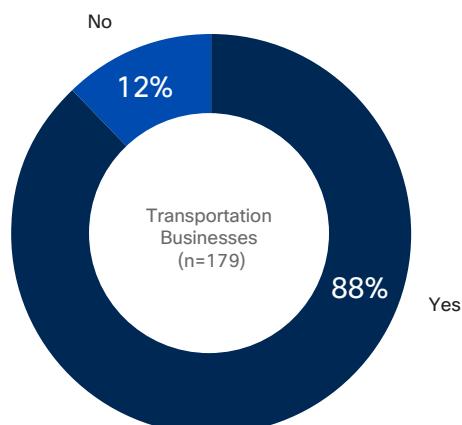
Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 122 Security Priorities for Telecommunications**Rank in Terms of Priority to Security in Organization**

Telecommunications Businesses (n=308)



Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 123 Sample Profile for Transportation**Does Your Company Utilize a Security Operations Center (SOC)?****Does Your Company Participate In Security Standards Bodies or Industry Organizations?****Which Transportation Subsector Is Your Organization Primarily Involved In?**

Transportation Businesses (n=180)

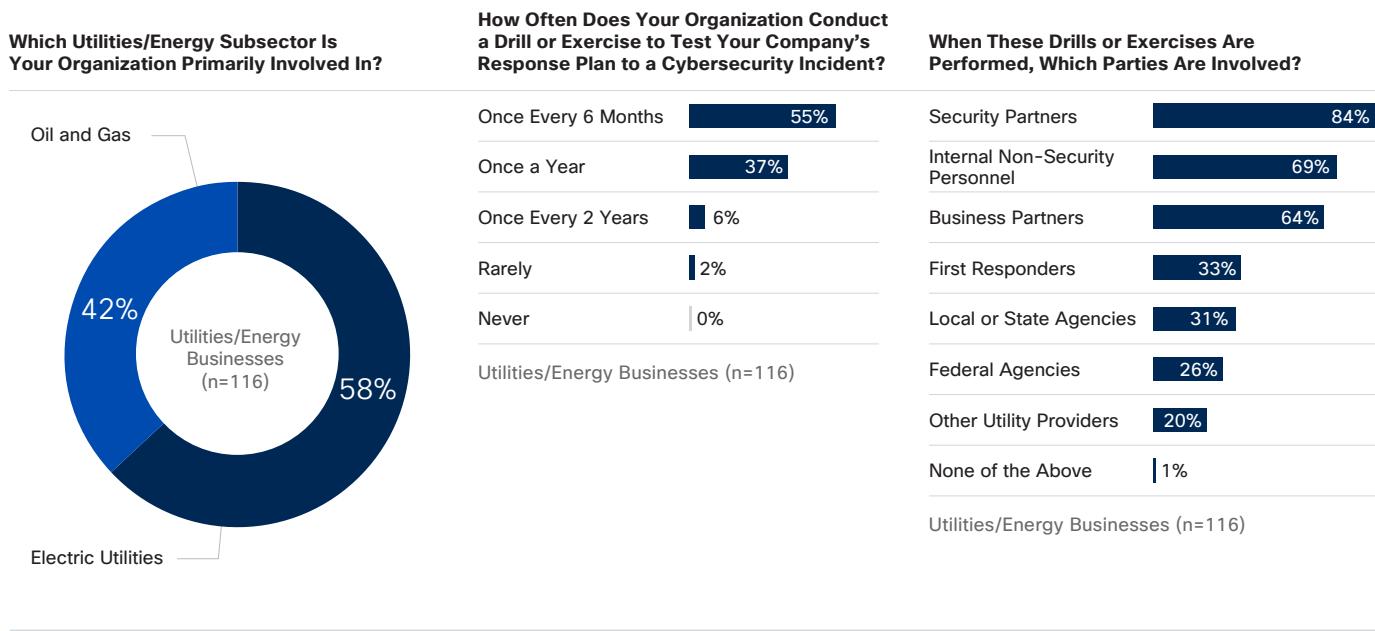
Freight and Logistics	54%
Mass Transit	11%
Rail	9%
Roadways	9%
Aviation	7%
Maritime	5%
Vehicles	5%

Source: Cisco 2017 Security Capabilities Benchmark Study

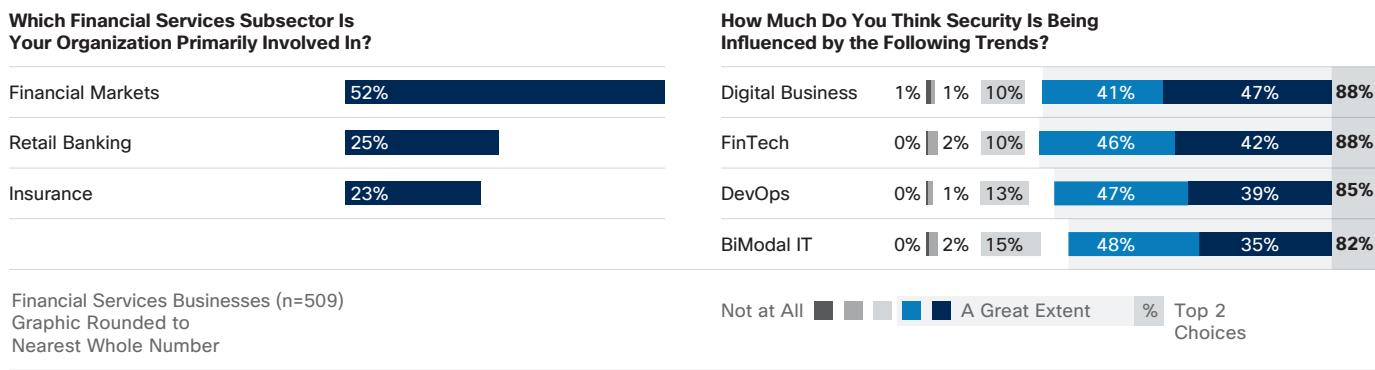
Which of the Following Security Areas Do You Have Responsibility In?

Transportation Businesses (n=180)

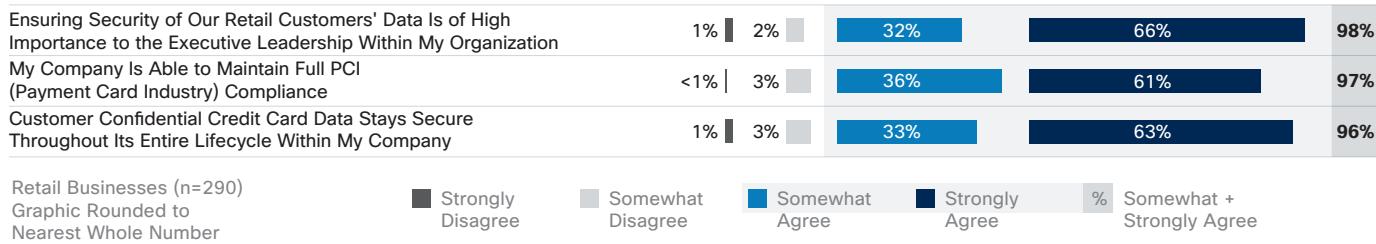
Operational Technology Security	84%
Critical Infrastructure Security	71%
Vehicle Security	43%

Figure 124 Sample Profile for Utilities/Energy

Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 125 Sample Profile for Financial Services

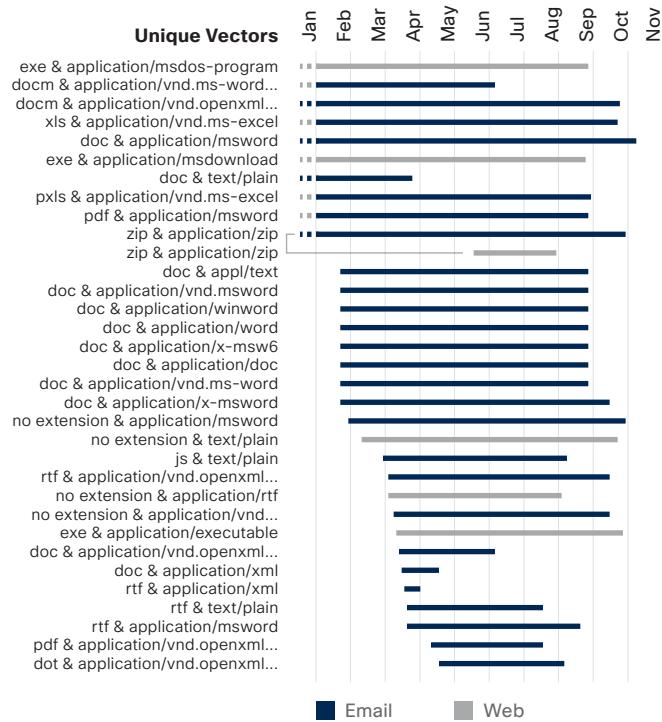
Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 126 Data Security for Retail**To What Extent Do You Agree or Disagree
With Each of These Statements?**

Source: Cisco 2017 Security Capabilities Benchmark Study

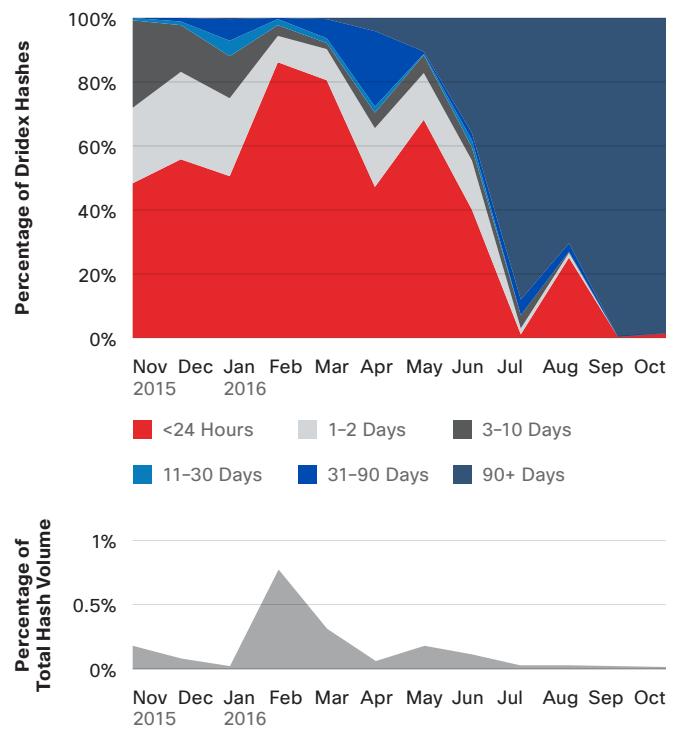
Malware Families

Figure 127 File Extension and MIME Combinations for Dridex (Web and Email Vectors)



Source: Cisco Security Research

Figure 128 Hash Ages for the Dridex Malware Family and Percent of Total Hash Volume Observed Per Month



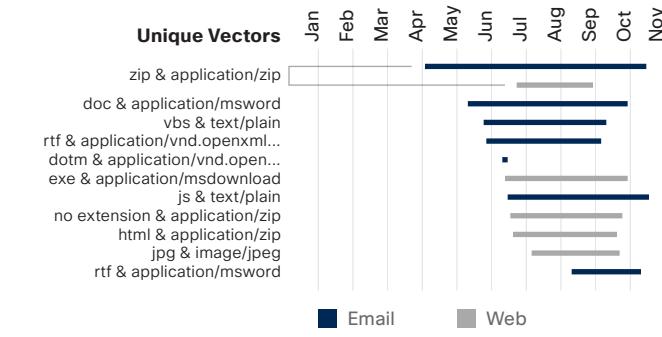
Source: Cisco Security Research

Figure 129 TTD for the Dridex Malware Family



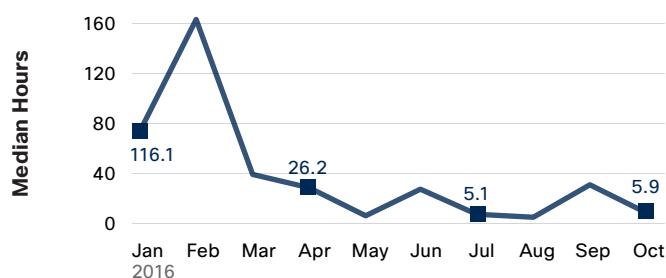
Source: Cisco Security Research

Figure 130 File Extension and MIME Combinations for the Family of Threats and Indicators That Lead to and Include the Cerber Payload (Web and Email Vectors)



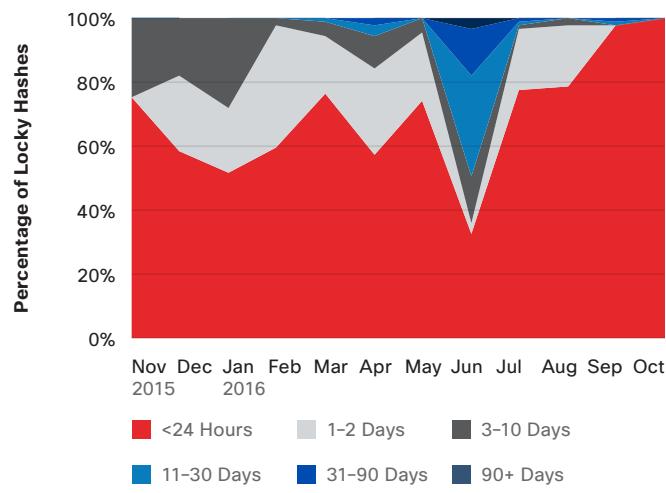
Source: Cisco Security Research

Figure 131 TTD for the Cerber Malware Family



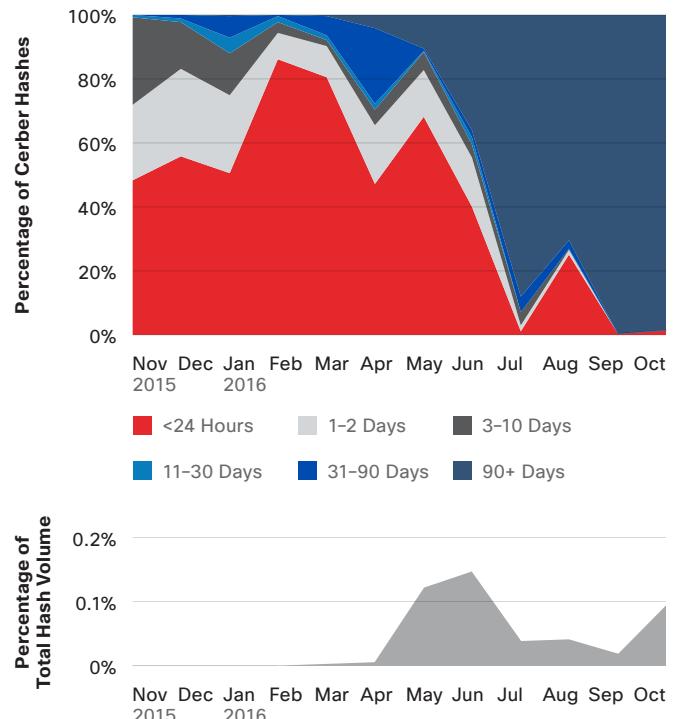
Source: Cisco Security Research

Figure 133 Hash Ages for the Locky Malware Family Per Month



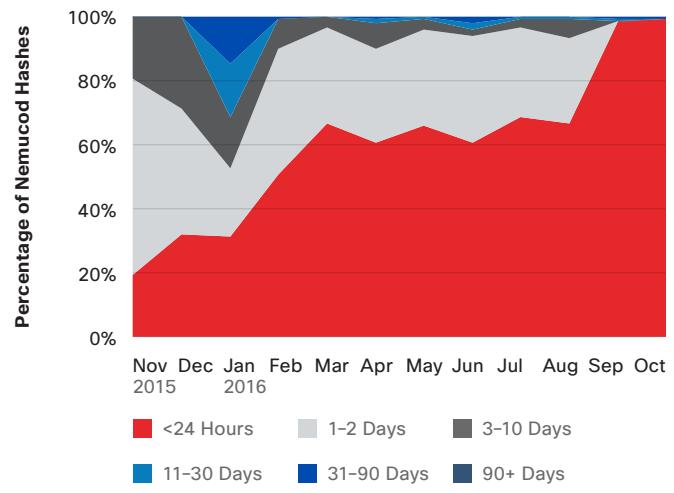
Source: Cisco Security Research

Figure 132 Hash Ages for the Cerber Malware Family and Percent of Total Hash Volume Observed Per Month



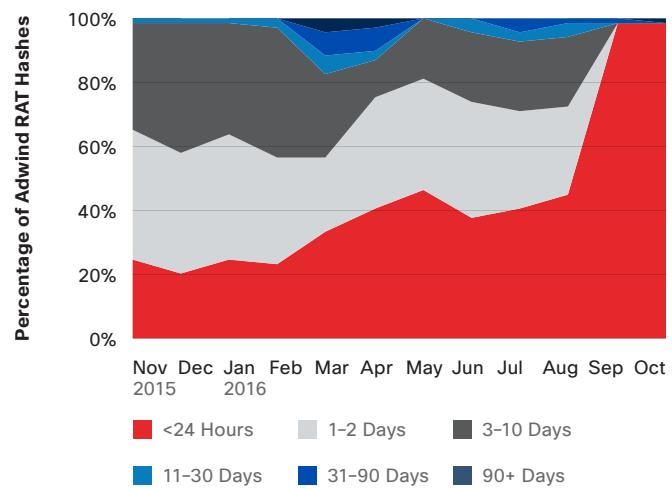
Source: Cisco Security Research

Figure 134 Hash Ages for the Nemucod Malware Family Per Month



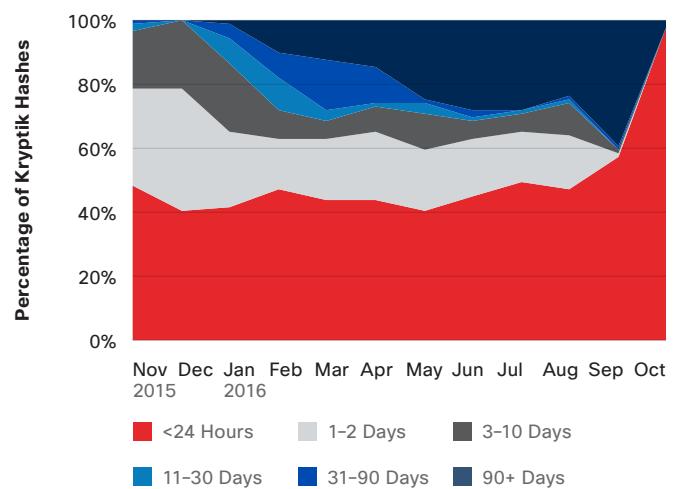
Source: Cisco Security Research

Figure 135 Hash Ages for the Adwind RAT Malware Family Per Month



Source: Cisco Security Research

Figure 136 Hash Ages for the Kryptik Malware Family Per Month



Source: Cisco Security Research

Download the Graphics

All the graphics in this report are downloadable at:
www.cisco.com/go/acr2017graphics

Updates and Corrections

To see updates and corrections to the information in this report, visit: www.cisco.com/go/acr2017errata

**Americas Headquarters**

Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters

Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters

Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Published January 2017

© 2017 Cisco and/or its affiliates. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Adobe, Acrobat, and Flash are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.