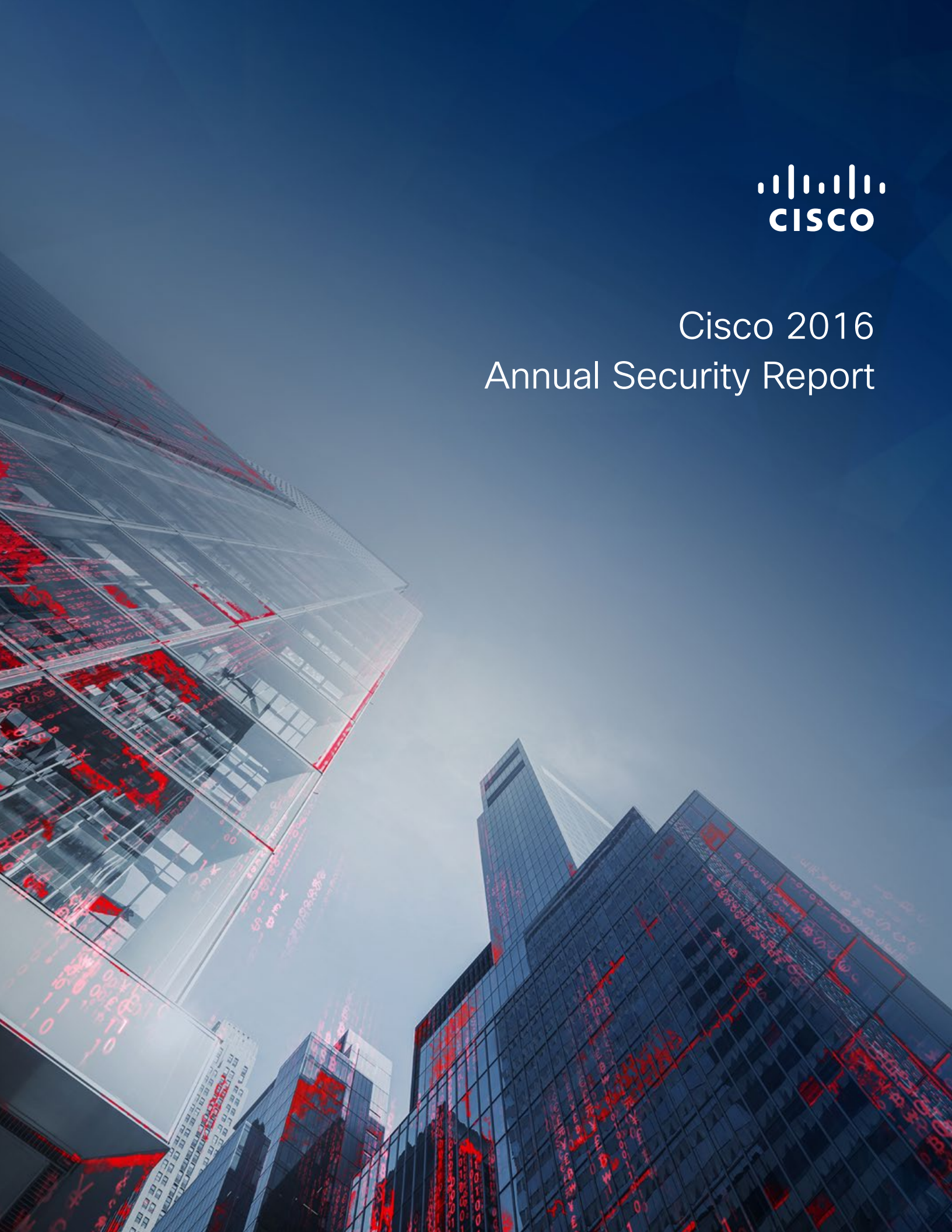




# Cisco 2016 Annual Security Report



# Executive Summary

Security professionals must rethink their defense strategies.

Adversaries and defenders are both developing technologies and tactics that are growing in sophistication. For their part, bad actors are building strong back-end infrastructures with which to launch and support their campaigns. Online criminals are refining their techniques for extracting money from victims and for evading detection even as they continue to steal data and intellectual property.

The Cisco 2016 Annual Security Report—which presents research, insights, and perspectives from Cisco Security Research—highlights the challenges that defenders face in detecting and blocking attackers who employ a rich and ever-changing arsenal of tools. The report also includes research from external experts, such as Level 3 Threat Research Labs, to help shed more light on current threat trends.

We take a close look at data compiled by Cisco researchers to show changes over time, provide insights on what this data means, and explain how security professionals should respond to threats.

## In this report, we present and discuss:

### THREAT INTELLIGENCE

This section examines some of the most compelling trends in cybersecurity as identified by our researchers as well as updates on web attack vectors, web attack methods, and vulnerabilities. It also includes a more extensive look into growing threats such as ransomware. To produce its analysis of observed trends in 2015, Cisco Security Research used a global set of telemetry data.

### INDUSTRY INSIGHTS

This section examines security trends affecting enterprises, including the growing use of encryption and the potential security risks it presents. We look at the weaknesses in how small and midsize businesses (SMBs) are protecting their networks. And we present research on enterprises relying on outdated, unsupported, or end-of-life software to support their IT infrastructure.

### SECURITY CAPABILITIES BENCHMARK STUDY

This section covers the results of Cisco's second Security Capabilities Benchmark study, which focused on security professionals' perceptions of the state of security in their organizations. In comparing 2015 survey results with those of 2014, Cisco found that chief security officers (CSOs) and security operations (SecOps) managers are less confident that their security infrastructure is up to date, or that they are able to thwart attacks. However, the survey also indicates that enterprises are stepping up training and other security processes in a bid to strengthen their networks. The study's findings are exclusive to the Cisco 2016 Annual Security Report.

### A LOOK FORWARD

This section offers a view of the geopolitical landscape affecting security. We discuss findings from two Cisco studies—one examining executives' concerns about cybersecurity, and the other focusing on IT decision-makers' perceptions about security risk and trustworthiness. We also give an update on our progress in reducing time to detection (TTD), and underscore the value of moving to an integrated threat defense architecture as a way to combat threats.

# Table of Contents

|   |           |   |           |
|---|-----------|---|-----------|
| <b>EXECUTIVE SUMMARY .....</b>  | <b>2</b>  | <b>INDUSTRY INSIGHTS.....</b>   | <b>29</b> |
| <b>MAJOR DEVELOPMENTS<br/>AND DISCOVERIES .....</b>   | <b>4</b>  | Encryption: A Growing Trend—and a<br>Challenge for Defenders .....                          | 30        |
| <b>EYE ON THE PRIZE: FOR MODERN<br/>CYBERCRIMINALS, MAKING MONEY<br/>IS PARAMOUNT .....</b>                                 | <b>7</b>  | Online Criminals Increase Server Activity on WordPress .....                                | 33        |
| <b>THREAT INTELLIGENCE .....</b>  | <b>9</b>  | Aging Infrastructure: A Problem 10 Years in the Making.....                                 | 35        |
| <b>Featured Stories.....</b>  | <b>10</b> | Are Small and Midsize Businesses a Weak Link to<br>Enterprise Security? .....               | 37        |
| Industry Collaboration Helps Cisco Sideline Far-<br>Reaching and Highly Profitable Exploit Kit and Ransomware Campaign..... | 10        | <b>CISCO SECURITY CAPABILITIES<br/>BENCHMARK STUDY .....</b>                                | <b>41</b> |
| Coordinated Industry Effort Helps Cripple One of the<br>Internet’s Largest DDoS Botnets .....                               | 14        | Decline in Confidence Amid Signs of Preparedness .....                                      | 42        |
| Browser Infections: Widespread—<br>and a Major Source of Data Leakage .....   | 16        | <b>A LOOK FORWARD .....</b>   | <b>55</b> |
| Botnet Command and Control: A Global Overview .....   | 17        | Geopolitical Perspective: Uncertainty in the<br>Internet Governance Landscape .....         | 56        |
| The DNS Blind Spot: Attacks Using DNS for<br>Command and Control .....  | 19        | Cybersecurity Concerns Weigh on Minds of Executives.....                                    | 57        |
| <b>Threat Intelligence Analysis .....</b>   | <b>20</b> | Trustworthiness Study: Shining a Light on the<br>Risks and Challenges for Enterprises ..... | 58        |
| Web Attack Vectors.....   | 20        | Time to Detection: The Race to Keep<br>Narrowing the Window.....                            | 60        |
| Web Attack Methods.....   | 21        | The Six Tenets of Integrated Threat Defense .....   | 62        |
| Threat Updates .....  | 23        | Power in Numbers: The Value of Industry Collaboration.....                                  | 63        |
| Vertical Risk of Malware Encounters.....  | 25        | <b>ABOUT CISCO .....</b>  | <b>64</b> |
| Web Block Activity: Geographic Overview.....  | 27        | Contributors to the Cisco 2016 Annual Security Report.....                                  | 65        |
|   |           | Cisco Partner Contributor.....  | 67        |
|   |           | <b>APPENDIX.....</b>  | <b>68</b> |



# Major Developments and Discoveries



# Major Developments and Discoveries

Cybercriminals have refined their back-end infrastructures to carry out attacks in ways that increase efficiency and profits.

- Cisco, with help from Level 3 Threat Research Labs and cooperation from the hosting provider Limestone Networks, identified and sidelined the largest Angler exploit kit operation in the United States, which was targeting 90,000 victims per day and generating tens of millions of dollars annually for the threat actors behind the campaign.
- SSHPsychos (Group 93), one of the largest distributed denial of service (DDoS) botnets ever observed by Cisco researchers, was significantly weakened by the combined efforts of Cisco and Level 3 Threat Research Labs. Like the Angler case study mentioned above, this success points to the value of industry collaboration to combat attackers.
- Malicious browser extensions can be a major source of data leakage for businesses and are a widespread problem. We estimate that more than 85 percent of organizations studied are affected by malicious browser extensions.
- Well-known botnets like Bedep, Gamarue, and Miuref represented the majority of botnet command-and-control activity affecting one group of organizations we analyzed in July 2015.
- Cisco's analysis of malware validated as "known bad" found that the majority of that malware—91.3 percent—uses the Domain Name Service (DNS) to carry out campaigns. Through retrospective investigation into DNS queries, Cisco uncovered "rogue" DNS resolvers in use on customer networks. The customers were not aware that the resolvers were being used by their employees as part of their DNS infrastructure.
- Adobe Flash vulnerabilities continue to be popular with cybercriminals. However, software vendors are reducing the risk that users will be exposed to malware through Flash technology.
- Observing the trends in 2015, our researchers suggest that HTTPS encrypted traffic has reached a tipping point: it will soon become the dominant form of Internet traffic. Although encryption can help protect consumers, it also can undermine the effectiveness of security products, making it more difficult for the security community to track threats. Adding to the challenge, some malware may initiate encrypted communications across a diverse set of ports.
- Bad actors are making use of compromised websites created by the popular web development platform WordPress for their criminal activities. There they can marshal server resources and evade detection.

- Aging infrastructure is growing and leaves organizations increasingly vulnerable to compromise. We analyzed 115,000 Cisco® devices on the Internet and discovered that 92 percent of the devices in our sample were running software with known vulnerabilities. In addition, 31 percent of the Cisco devices in the field that were included in our analysis are “end of sale” and 8 percent are “end of life.”
- In 2015, security executives showed lower confidence in their security tools and processes than they did in 2014, according to Cisco’s 2015 Security Capabilities Benchmark Study. For example, in 2015, 59 percent of organizations said their security infrastructure was “very up to date.” In 2014, 64 percent said the same. However, their growing concerns about security are motivating them to improve their defenses.
- The benchmark study shows that small and midsize businesses (SMBs) use fewer defenses than larger enterprises. For example, 48 percent of SMBs said in 2015 that they used web security, compared to 59 percent in 2014. And 29 percent said they used patching and configuration tools in 2015, compared with 39 percent in 2014. Such weaknesses can place SMBs’ enterprise customers at risk, since attackers may more easily breach SMB networks.
- Since May 2015, Cisco has reduced the median time to detection (TTD) of known threats in our networks to about 17 hours—less than one day. This far outpaces the current industry estimate for TTD, which is 100 to 200 days.



Eye on the Prize:  
For Modern Cybercriminals,  
Making Money Is Paramount

# Eye on the Prize: For Modern Cybercriminals, Making Money Is Paramount

In the past, many online criminals lurked in the shadows of the Internet. They tried to avoid detection by making only brief incursions into enterprise networks to launch their exploits. Today, some emboldened cybercriminals are tapping into legitimate online resources. They leach server capacity, steal data, and demand ransoms from online victims whose information they hold hostage.

These campaigns are a sobering escalation in the war between defenders and attackers. If adversaries find more places online from which to operate, then their impact can grow exponentially.

In this report, Cisco security researchers highlight the tactics that threat actors use to build a solid infrastructure to make their campaigns stronger and more effective. Adversaries continue to adopt more efficient methods for boosting their profits—and many are paying special attention to harnessing server resources.

The explosion in ransomware (see [page 10](#)) is a prime example. Ransomware provides criminals with an easy way to extract more money directly from users. When adversaries establish campaigns that compromise tens of thousands of users per day with little or no interruption, the “paycheck” for their efforts can be staggering. In addition to developing better ways to monetize their campaigns, attackers are encroaching on legitimate resources as staging grounds.

Creators of some ransomware variants as well as developers of other exploits are now shifting traffic to hacked WordPress websites as a way to avoid detection and use server space (see [page 33](#)). And the perpetrators of SSHPsychos, one of the largest botnets ever seen by Cisco researchers, operated on standard networks with little interference until a combined takedown effort by Cisco and Level 3 Threat Research Labs persuaded service providers to block the botnet creator’s traffic.



# Threat Intelligence

# Threat Intelligence

Cisco has assembled and analyzed a global set of telemetry data for this report. Our ongoing research and analysis of discovered threats, such as malware traffic, can provide insights on possible future criminal behavior and aid in the detection of threats.

## Featured Stories

### Industry Collaboration Helps Cisco Sideline Far-Reaching and Highly Profitable Exploit Kit and Ransomware Campaign

The Angler exploit kit is one of the largest and most effective exploit kits on the market. It has been linked to several high-profile malvertising (malicious advertising) and ransomware campaigns. And it has been a major factor in the overall explosion of ransomware activity that our threat researchers have been monitoring closely for the past several years. Miscreants use ransomware to encrypt users' files, providing the keys for decryption only after users pay a "ransom"—usually in the \$300 to \$500 range.

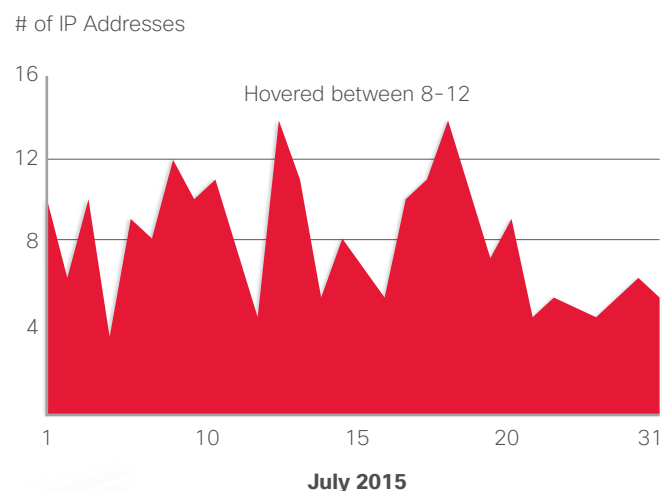
As reported in the Cisco 2015 Midyear Security Report, cryptocurrencies like bitcoin and anonymization networks such as Tor make it easy for adversaries to enter the malware market and quickly begin generating revenue. Ransomware's rise in popularity can be tied to two main advantages: It is a low-maintenance operation for threat actors, and it offers a quick path to monetization because the users pay adversaries directly in cryptocurrencies.

Through research of Angler and related ransomware trends, Cisco determined that some operators of the exploit kit were using an inordinate percentage of worldwide proxy servers for Angler that were on servers operated by Limestone Networks. This server use is a prime example of another trend that our researchers have been observing in the shadow economy of late: threat actors commingling legitimate and malicious resources to carry out their campaigns.

In this case, the IP infrastructure supporting Angler was not large. The daily number of active systems generally hovered between 8 and 12. Most were active for only one day. Figure 1 shows the number of unique IP addresses that Cisco observed throughout July 2015.

Cisco found that Angler operators were essentially rolling through IP addresses in a linear fashion to conceal the threat activity and to prevent any interruption to their moneymaking.

**Figure 1. Number of Angler IP Addresses by Date, July 2015**



Source: Cisco Security Research

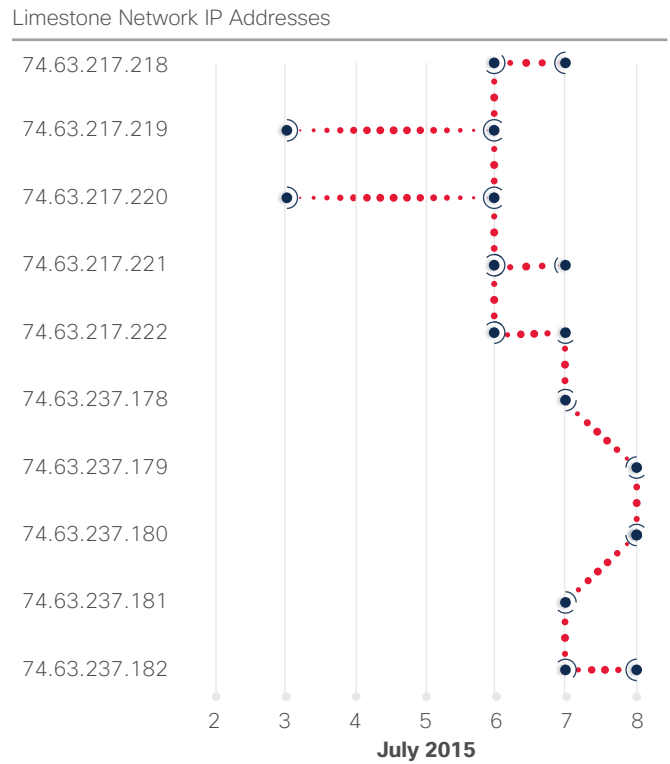
SHARE    

As Figure 2 illustrates, Angler starts with an IP address (here, 74.63.217.218). As the system compromises users and generates “noise” that defenders begin to detect, the adversaries shift to an adjacent IP address (74.63.217.219). This activity continues through near-contiguous blocks of IP space from a single hosting provider.

Cisco examined the IP information to identify the autonomous system numbers (ASNs) and the providers associated with the IP addresses. We determined that most of the Angler-related traffic was coming from servers operated by two legitimate hosting providers: Limestone Networks and Hetzner (Figure 3). They accounted for almost 75 percent of the overall volume of traffic for the month of July.

Cisco reached out first to Limestone Networks, which appeared to be hosting the largest global portion of Angler. Limestone embraced the opportunity to collaborate. The company had been dealing with excessive credit card chargebacks every month because adversaries were using fraudulent names and credit cards to buy random batches of their servers worth thousands of dollars.

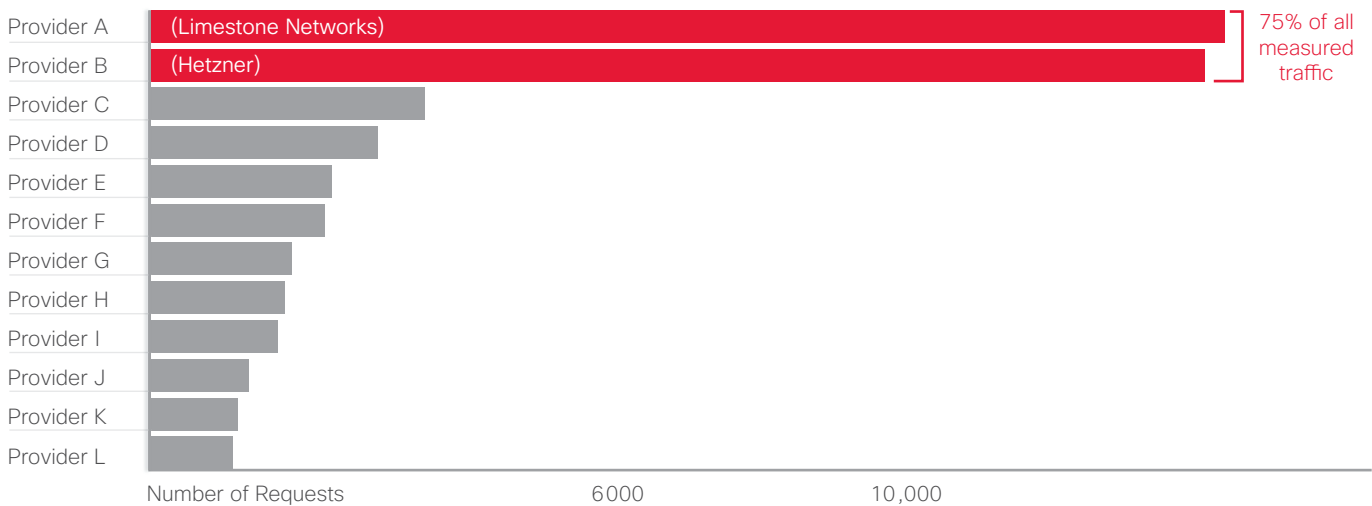
Figure 2. Low IP Infrastructure Supporting Angler



Source: Cisco Security Research

SHARE

Figure 3. Angler HTTP Requests by Provider, July 2015



Source: Cisco Security Research

The adversaries' approach to purchasing the servers made it difficult to associate the fraudulent activity with a single actor. For example, a miscreant might buy three or four servers on one day, and then use a different name and credit card to purchase three or four servers the next day. In this way, they could essentially "roll" from one IP address to the next when compromised servers were identified and taken offline by defenders.

To investigate this activity, Cisco enlisted help from Level 3 Threat Research Labs as well as from OpenDNS, a Cisco company. Level 3 Threat Research Labs was able to provide greater global insight into the threat, giving Cisco the ability to see a little deeper into the scope of the threat and how far-reaching it was at its peak. OpenDNS, meanwhile, provided a unique look at the domain activity associated with the threat, giving Cisco a more complete understanding of how techniques like domain shadowing were being incorporated by the adversaries.

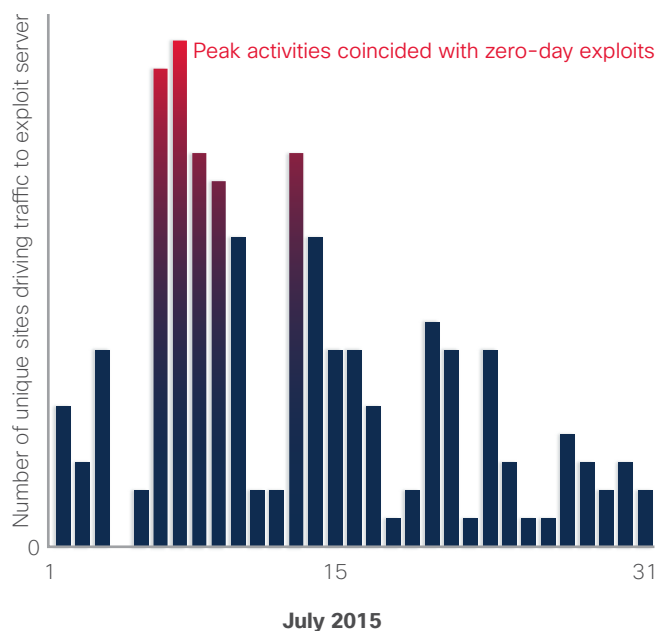
Cisco threat researchers then looked into how, specifically, users were encountering Angler and subsequently being served malicious payloads. The researchers observed popular websites redirecting users to the Angler exploit kit through malvertising. The false ads were placed on hundreds of major news, real estate, and popular culture sites. These types of sites are commonly referred to in the security community as "known good" sites.

Additionally, Cisco threat researchers found countless examples of small, seemingly random websites doing the same type of redirection, including a single person's obituary from a small, rural newspaper in the United States. More than likely, the latter strategy was designed to target elderly people. This population is generally more likely to use default web browsers such as Microsoft Internet Explorer and are less likely to be aware of the need to regularly patch Adobe Flash vulnerabilities.

Another notable aspect of this Angler operation was the volume of unique referers and the low frequency with which they were used (Figure 4). We found more than 15,000 unique sites pushing people to the Angler exploit kit, 99.8 percent of which were used fewer than 10 times. Most of the referers were therefore active only for a short period

and were removed after a handful of users were targeted. In our July 2015 analysis, we noted that the peaks in activity coincided with the various Hacking Team zero-day exploits (CVE-2015-5119, CVE-2015-5122).<sup>1</sup>

**Figure 4.** Unique Referers by Day, July 2015



Source: Cisco Security Research

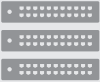
Cisco determined that about 60 percent of the Angler payloads delivered through this particular operation were delivering some type of ransomware variant, the majority being Cryptowall 3.0. Other types of payloads included Bedep, a malware downloader that is commonly used to install click-fraud campaign malware. (See "Browser Infections: Widespread—and a Major Source of Data Leakage," [page 16](#).) Both types of malware are designed to help adversaries make a lot of money from compromised users very quickly, and with little or no effort.

<sup>1</sup> "Adobe Patches Hacking Team's Flash Player Zero-Day," by Eduard Kovacs, *SecurityWeek*, July 8, 2015: <http://www.securityweek.com/adobe-patches-hacking-teams-flash-player-zero-day>.



**!** Angler Revenue

**147**  
redirection  
servers  
per month



**90K**  
targets  
per server  
per day



**10%**  
served exploits



**40%**  
compromised





**62%**  
delivered  
ransomware



**2.9%**  
of ransoms paid



**X**  **\$300** **=**  **\$34M**

average ransom gross yearly income for ransomware per campaign

9515 users are paying ransoms per month

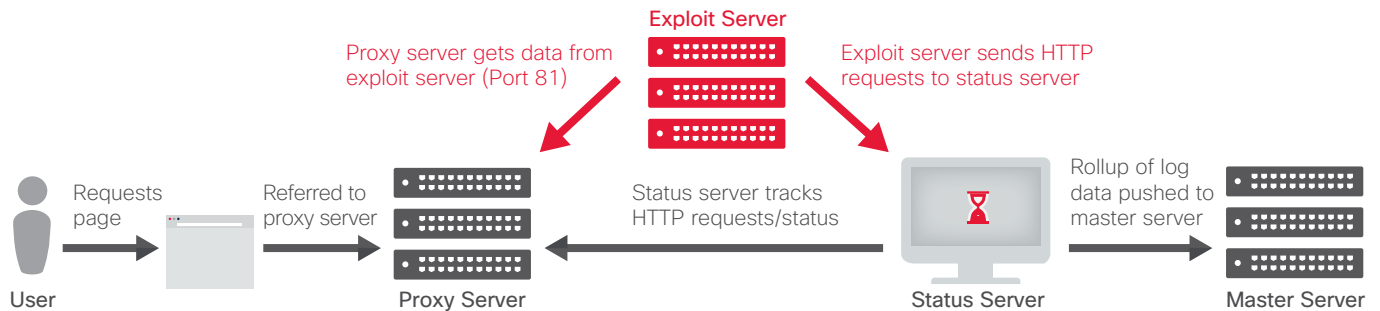
Source: Cisco Security Research

According to Cisco’s research, the primary actor responsible for about half of the Angler exploit kit activity in this particular campaign was targeting up to 90,000 victims per day. By our estimation, the campaign was netting the adversaries more than \$30 million annually.

Presumably, the network out of Hetzner had a similar success rate. That means the threat actor behind the operation involving the Limestone Networks and Hetzner servers was responsible for half of all global Angler activity at the time of Cisco’s analysis. Cisco researchers estimate that this operation was capable of generating gross income of \$60 million per year.

SHARE    

Figure 5. Angler Back-End Infrastructure



Source: Cisco Security Research

Cisco also discovered that the servers that the users were connecting to did not actually host any of the malicious Angler activity. They were serving as a conduit. A user would get into the redirection chain and submit a GET request for a landing page, which would land on the proxy server. The proxy server would route the traffic to an exploit server in a different country, on a different provider. During our research, we found that a single exploit server was associated with multiple proxy servers. (See Figure 5.)

Cisco identified a status server that was handling tasks such as health monitoring. Every single proxy server that the status server was monitoring had a pair of unique URLs. If the path was queried, the status server would return an HTTP status code “204” message. The adversaries could uniquely identify each proxy server and make sure it not only was operating, but also that defenders had not tampered with it. Using the other URL, the attackers could collect the logs from the proxy server and determine how efficiently their network was operating.

Industry collaboration was a critical component in Cisco’s ability to investigate the Angler exploit kit activity. Ultimately, it helped stop redirects to the Angler proxy servers on a U.S. service provider and bring awareness to a highly sophisticated cybercrime operation that was affecting thousands of users every day.

SHARE    

Cisco worked closely with Limestone Networks to identify new servers as they were brought online and monitored them closely to make sure they were taken down. After a while the adversaries moved away from Limestone Networks, and a global decrease in Angler activity followed.



For more information on how Cisco disrupted a significant international revenue stream generated by the Angler exploit kit, read the Cisco Security blog post **“Threat Spotlight: Cisco Talos Thwarts Access to Massive International Exploit Kit Generating \$60M Annually from Ransomware Alone.”**

## Coordinated Industry Effort Helps Cripple One of the Internet’s Largest DDoS Botnets

Integrated threat defense technologies can often halt major attacks before they affect enterprise networks. However, in many cases, bringing down a potentially massive attack requires not only technological defenses, but also coordination among service providers, security vendors, and industry groups.

As criminals become even more serious about monetizing their activities, the technology industry needs to do a better job of partnering to take down criminal campaigns. SSHPsychos (also called Group 93), one of the largest DDoS botnets ever observed by Cisco security researchers, was significantly weakened after Cisco collaborated with Level 3 Threat Research Labs.

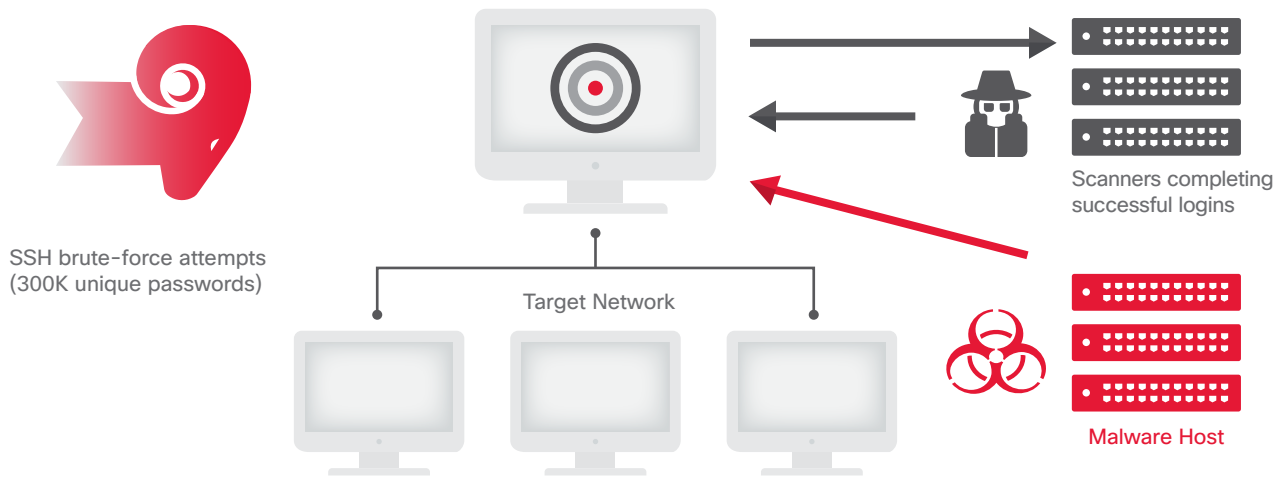
**UNIQUE THREAT**

The SSHPsychos DDoS network is a unique threat for several reasons. Because it enlists tens of thousands of machines distributed across the Internet, it has the power to launch a distributed denial of service (DDoS) attack that cannot be addressed on a device-by-device basis. In this case, the botnet was being created using brute-force attacks involving secure shell (SSH) traffic (Figure 6). The SSH protocol is used to allow secure communications, and it is commonly used for the remote administration of systems. At times, SSHPsychos accounted for more than 35 percent of all global Internet SSH traffic (Figure 7), according to analysis by Cisco and Level 3.

SSHPsychos is operational in two countries: China and the United States. The brute-force login attempts, using 300,000 unique passwords, originated from a hosting provider based in China. When adversaries were able to log in by guessing the correct root password, the brute-force attacks ceased. Twenty-four hours later, adversaries then logged in from a U.S. IP address and installed a DDoS rootkit to the affected machine. This was clearly a tactic to reduce suspicion from network administrators. The botnet’s targets varied, but in many cases appeared to be large Internet service providers (ISPs).

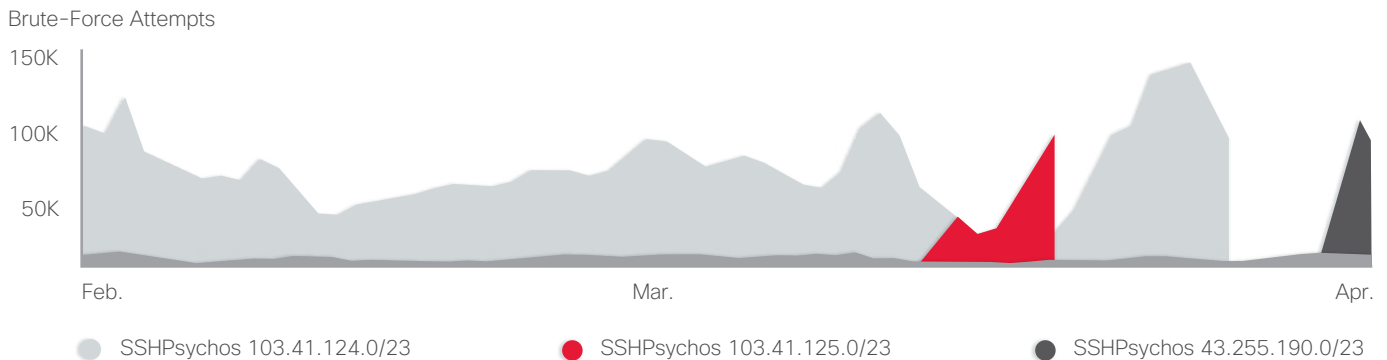
SHARE    

**Figure 6.** SSHPsychos Uses Brute-Force Attacks



Source: Cisco Security Research

**Figure 7.** At Its Peak, SSHPsychos Accounted for 35 Percent of Global Internet Traffic



Source: Cisco Security Research

**COLLABORATING WITH SECURITY EXPERTS**

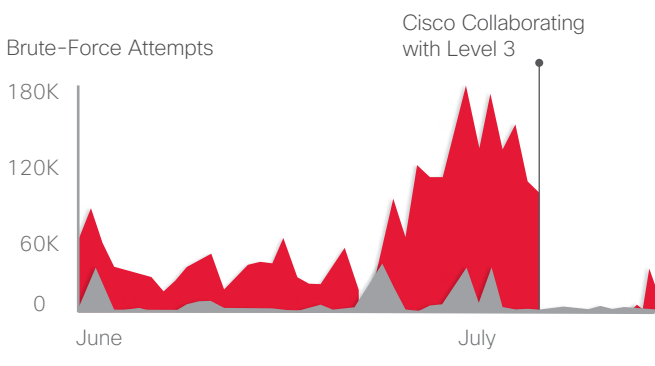
Because of the scale of the DDoS network, our researchers believed that the damage would be difficult to contain. It was essential to work in tandem with an organization that could remove the brute-forcing group from the Internet effectively. However, backbone providers are hesitant to filter their customers’ content.

Cisco reached out to Level 3 Threat Research Labs. Level 3 analyzed the traffic at the netblock, or range of IP addresses, where SSHPsychos was thought to reside (103.41.124.0/23). It confirmed that no legitimate traffic was originating from or destined for that address. It null-routed the network traffic within its own networks. Then it contacted service providers for the relevant domains to ask them to remove the network’s traffic.

The results of this effort were seen immediately (Figure 8). The original network showed almost no new activity. However, a new network at netblock 43.255.190.0/23 showed large amounts of SSH brute-force attack traffic. It had the same behavior that was associated with SSHPsychos. Following this sudden re-emergence of SSHPsychos-like traffic, Cisco and Level 3 decided to take action against 103.41.124.0/23, as well as the new netblock 43.255.190.0/23.

Taking down the netblocks used by SSHPsychos did not permanently disable the DDoS network. However, it certainly slowed down its creators’ ability to run their operations, and it prevented SSHPsychos from spreading to new machines, at least temporarily.

**Figure 8. SSHPsychos Traffic Drops Dramatically After Intervention**



Source: Cisco Security Research

As cybercriminals build large attack networks, the security industry must explore ways to collaborate when faced with a threat such as SSHPsychos. Top-level domain providers, ISPs, hosting providers, DNS resolvers, and security vendors can no longer sit on the sidelines when online criminals launch their exploits on networks that are intended to carry only legitimate traffic. In other words, when criminals deliver malicious traffic in what is more or less plain sight, the industry must remove the malicious pathways to these legitimate networks.



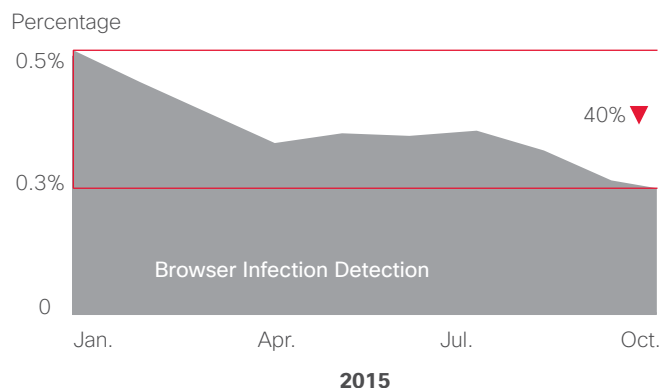
To learn more about Cisco and Level 3 Threat Research Labs’ response to the SSHPsychos threat, read the Cisco Security blog post **“Threat Spotlight: SSHPsychos.”**

**Browser Infections: Widespread—and a Major Source of Data Leakage**

Security teams often view browser add-ons as a low-severity threat. However, they should make monitoring them a higher priority so that they can quickly identify and remediate these types of infections.

The reason for urgency: Our research indicates that browser infections are much more prevalent than many organizations may realize. From January to October 2015, we examined 26 families of malicious browser add-ons (Figure 9). Looking at the pattern of browser infections during these months, the number of infections seemed to be on a general decline.

**Figure 9. Browser Infections, January to October 2015**



Source: Cisco Security Research



This pattern is deceptive, however. The increasing volume of HTTPS traffic over those months made it difficult to identify the indicators of compromise typically associated with the 26 families we tracked because URL information was not visible due to encryption. (For more on encryption, and the challenges it creates for defenders, see “Encryption: A Growing Trend—and a Challenge for Defenders,” [page 30](#).)

Malicious browser extensions can steal information, and they can be a major source of data leakage. Every time a user opens a new webpage with a compromised browser, malicious browser extensions collect data. They are exfiltrating more than the basic details about every internal or external webpage that the user visits. They are also gathering highly sensitive information embedded in the URL. This information can include user credentials, customer data, and details about an organization’s internal APIs and infrastructure.

Multipurpose malicious browser extensions are delivered by software bundles or adware. They are designed to pull in revenue by exploiting users in a number of ways. In an infected browser, they can lead users to click on malvertising such as display ads or pop-ups. They can also distribute malware by enticing users to click a compromised link or to download an infected file encountered in malvertising. And they can hijack users’ browser requests and then inject malicious webpages into search engine results pages.

Across the 45 companies in our sample, we determined that in every month we observed more than 85 percent of organizations were affected by malicious browser extensions—a finding that underscores the massive scale of these operations. Because infected browsers are often considered a relatively minor threat, they can go undetected or unresolved for days or even longer—giving adversaries more time and opportunity to carry out their campaigns (see “Time to Detection: The Race to Keep Narrowing the Window,” [page 60](#)).

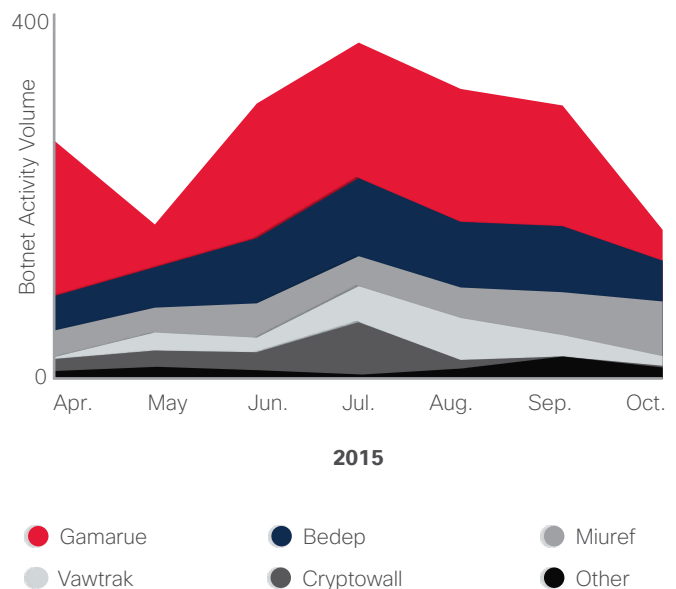
We therefore suggest that it is well worth security teams’ time to devote more resources to monitoring this risk, and to consider increased use of automation to help prioritize threats.

## Botnet Command and Control: A Global Overview

Botnets are networks of malware-infected computers. Adversaries can control them as a group and command them to carry out a specific task, such as sending spam or launching a DDoS attack. They have been growing in both size and number for years. To better understand the current threat landscape on a global scale, we analyzed the networks of 121 companies from April to October 2015 for evidence of one or more of eight commonly seen botnets. The data was normalized to provide a general overview of botnet activity (Figure 10).

We found that during this period, Gamarue—a modular, multipurpose information stealer that has been around for years—was the most common command-and-control threat.

**Figure 10.** Growth of Individual Threats (Ratio of Infected Users)



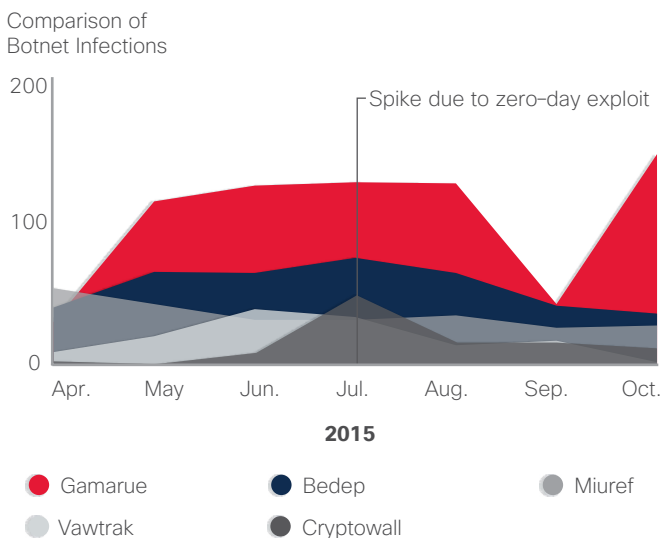
Source: Cisco Security Research

A significant spike in the number of infections involving the ransomware Cryptowall 3.0 was identified in July. This activity is attributed largely to the Angler exploit kit, which is known to drop the Cryptowall payload. As reported in the Cisco 2015 Midyear Security Report, the authors of Angler and other exploit kits have been quick to exploit “patching gaps” with Adobe Flash—the time between Adobe’s release of an update and when users actually upgrade.<sup>2</sup> Cisco threat researchers attribute the July 2015 spike to the Flash zero-day exploit CVE-2015-5119 that was exposed as part of the Hacking Team leaks.<sup>3</sup>

The Angler exploit kit also delivers the Bedep Trojan, which is used to perform click-fraud campaigns. A slight spike in the prevalence of that threat was noted during July as well (Figure 11).

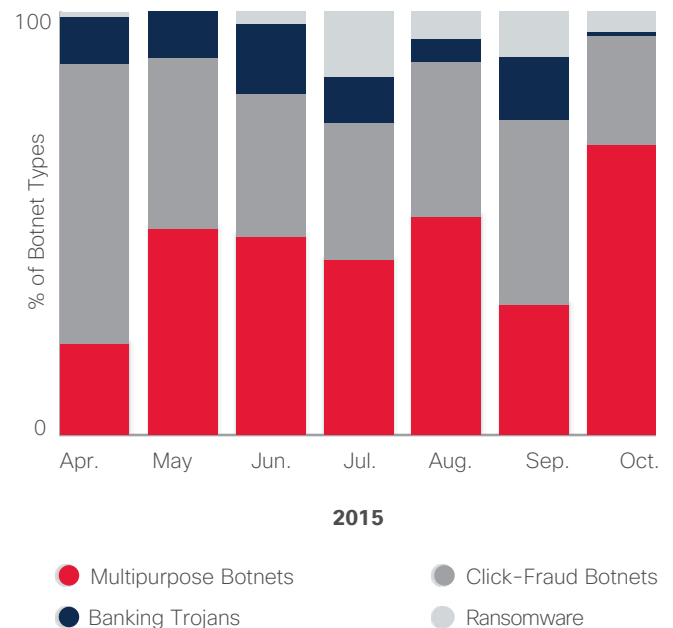
Bedep, Gamarue, and Miuref (another Trojan and browser hijacker that can perform click fraud) together represented more than 65 percent of the botnet command-and-control activity in the user base we analyzed.

**Figure 11. Monthly Threat Coverage, Based on the Number of Infected Users**



Source: Cisco Security Research

**Figure 12. Monthly Threat Coverage, Based on Threat Categories**



Source: Cisco Security Research

The percentage of Bedep infections remained relatively stable during the period we analyzed. However, a perceived decrease in Miuref infections was observed. We attribute this to the increase in HTTPS traffic, which helped to conceal Miuref’s indicators of compromise.

Figure 12 shows the types of botnets that were responsible for the most infections during the time frame we monitored. Multipurpose botnets like Gamarue and Sality led the pack, followed by click-fraud botnets. Banking Trojans were third, showing that this type of threat, while old, is still widespread.

SHARE    

<sup>2</sup> Cisco 2015 Midyear Security Report: <http://www.cisco.com/web/offers/lp/2015-midyear-security-report/index.html>.

<sup>3</sup> “Adobe Patches Hacking Team’s Flash Player Zero-Day,” by Eduard Kovacs, *SecurityWeek*, July 8, 2015: <http://www.securityweek.com/adobe-patches-hacking-teams-flash-player-zero-day>.

## The DNS Blind Spot: Attacks Using DNS for Command and Control

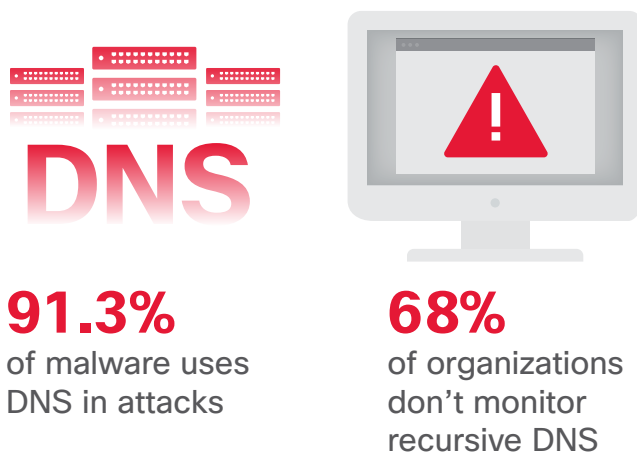
Cisco's analysis of malware validated as "known bad" found that the majority of that malware—91.3 percent—use the Domain Name Service in one of these three ways:

- To gain command and control
- To exfiltrate data
- To redirect traffic

To arrive at this percentage, we mined all sample behaviors from a variety of sandboxes that we own. Malware that was determined not to use DNS in any way, or that simply used DNS to conduct Internet "health checks," was removed from the sample for analysis. The remaining malware was using DNS to connect to sites that were validated as bad or were considered suspicious.

Despite adversaries' reliance on DNS to help further malware campaigns, few companies are monitoring DNS for security purposes (or monitoring DNS at all). This lack of oversight makes DNS an ideal avenue for attackers. According to a recent survey we conducted (see Figure 13), 68 percent of security professionals report that their organizations do not monitor threats from recursive DNS. (Recursive DNS nameservers provide the IP addresses of intended domain names to the requesting hosts.)

**Figure 13.** Monitoring Threats from Recursive DNS



Source: Cisco Security Research

Why is DNS a security blind spot for so many organizations? A primary reason is that security teams and DNS experts typically work in different IT groups within a company and don't interact frequently.

But they should. Monitoring DNS is essential for identifying and containing malware infections that are already using DNS for one of the three activities listed earlier. It is also an important first step in mapping out other components that can be used for further investigating an attack, from determining the type of infrastructure supporting the attack to finding its source.

Monitoring DNS takes more than collaboration between security and DNS teams, however. It requires the alignment of the right technology and expertise for correlation analysis. (For more insight, see "Industry Collaboration Helps Cisco Sideline Far-Reaching and Highly Profitable Exploit Kit and Ransomware Campaign" on [page 10](#) to find out how OpenDNS helped Cisco gain more domain visibility into the IPs that the Angler exploit kit was using.)

### RETROSPECTIVE DNS ANALYSIS

Cisco's retrospective investigation into DNS queries and subsequent TCP and UDP traffic identifies a number of malware sources. These include command-and-control servers, websites, and distribution points. Retrospective investigation also detects high-threat content using intelligence from threat lists, community threat reports, observed trends in cyber compromises, and knowledge of the unique vulnerabilities facing a customer's industry.

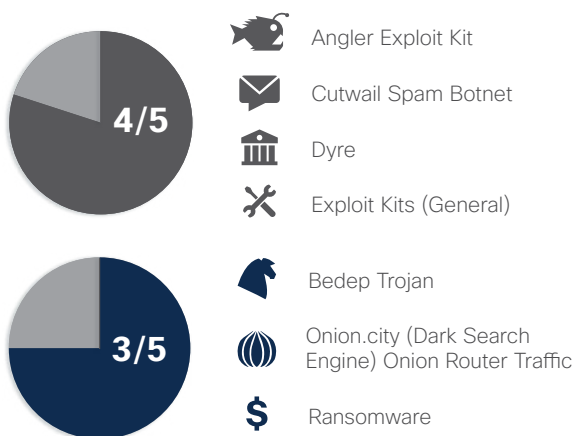
Our retrospective reporting helps to identify "low and slow" data exfiltration attempts commonly associated with advanced persistent threat (APT) behavior and which, in many cases, is not captured by traditional threat detection technologies. The objective of the analysis is to identify anomalies within the vast quantity of outgoing communications traffic. This "inside out" approach can uncover possible data compromises and damaging network activity that might otherwise be overlooked.

This is how we have uncovered “rogue” DNS resolvers in use on customer networks. The customers were not aware that the resolvers were being used by their employees as part of their DNS infrastructure. Failing to actively manage and monitor the use of DNS resolvers can result in malicious behavior such as DNS cache poisoning and DNS redirection.

Besides discovering and identifying rogue DNS resolvers, retrospective investigation has also uncovered the following issues in customer networks:

- Customer address space found on third-party spam and malware blocklists
- Customer address space beaconing for known Zeus and Palevo command-and-control servers
- Active malware campaigns, including CTB-Locker, Angler, and DarkHotel
- Suspicious activity, including the use of Tor, email auto-forwarding, and online document conversion
- Pervasive DNS tunneling to Chinese-registered domains
- DNS “typosquatting”<sup>4</sup>
- Internal clients bypassing the customer’s trusted DNS infrastructure

Looking at a select sample of Cisco Custom Threat Intelligence customers across multiple verticals, we also found the following types of malware in the respective percentage of total customers examined:



<sup>4</sup> Typosquatting is the act of registering a domain name that is similar to an existing domain name; this is a strategy used by adversaries to target users who inadvertently mistype intended domain names.

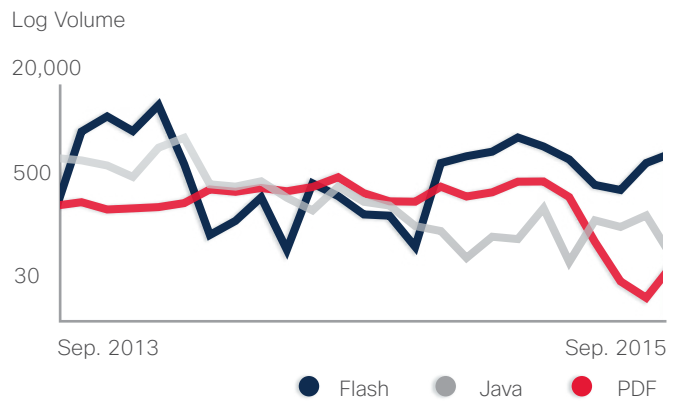
## Threat Intelligence Analysis

### Web Attack Vectors

#### ADOBE FLASH: ON THE WAY OUT—EVENTUALLY

Despite the fact that overall Flash volume has decreased over the past year (see next section, “**Adobe Flash and PDF Content Trends**”), it still remains a favored tool of exploit kit developers. In fact, there was no discernable trend in Flash malware either increasing or decreasing in 2015 (Figure 14). Flash-related malware is likely to remain a primary exploitation vector for some time: Of note, the Angler exploit kit authors heavily target Flash vulnerabilities.

Figure 14. Share of Attack Vectors, 2-Year Comparison



Source: Cisco Security Research

Industry pressure to remove Adobe Flash from the browsing experience is leading to a decrease in the amount of Flash content on the web (see next section, “**Adobe Flash and PDF Content Trends**”). This is similar to what has been seen with Java content in recent years, and which has, in turn, led to a steady downward trend in the volume of Java malware (In fact, Angler’s authors don’t even bother to include Java exploits anymore). Meanwhile, the volume of PDF malware has remained fairly steady.

Microsoft Silverlight also has diminished as an attack vector because many vendors have discontinued supporting the API that Silverlight uses to integrate into browsers. Many companies are moving away from Silverlight as they embrace HTML5-based technologies. Microsoft has indicated that there is no new version of Silverlight on the horizon and is currently only issuing security-related updates.

### ADOBE FLASH AND PDF CONTENT TRENDS

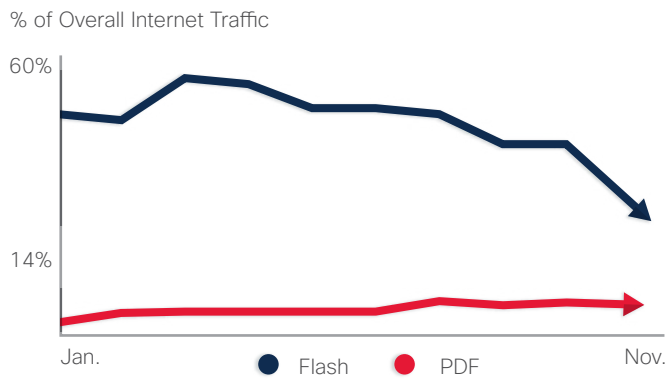
Cisco researchers have been watching a general decline in the amount of Adobe Flash content on the web (Figure 15). Recent actions by Amazon, Google, and other large players in the Internet space are a factor for the decrease in Flash content. These companies either no longer accept web advertising that uses Flash, or they block it.

PDF content, meanwhile, has remained fairly stable over the past year and is likely to remain so. However, it has not been a major web attack vector for some time.

The decline in Flash content is likely to continue—and perhaps, even accelerate—in the near term now that Adobe has announced that it will be phasing out Flash.<sup>5</sup> But it will likely be some time before Flash content fades. Flash is embedded in browsers such as Google Chrome, Microsoft Internet Explorer, and Microsoft Edge and is still widely used in web content, including gaming and video content.

However, in the years ahead, as new technologies are adopted (such as HTML5 and mobile platforms), the longer-term trend for web attack vectors like Java, Flash, and Silverlight is becoming increasingly clear. Over time, they will become less prevalent. Therefore, they are likely to become much less attractive vectors to profit-minded adversaries who focus on vectors that allow them to easily compromise large populations of users and generate revenue quickly.

**Figure 15.** Percentage of Overall Traffic for Flash and PDF

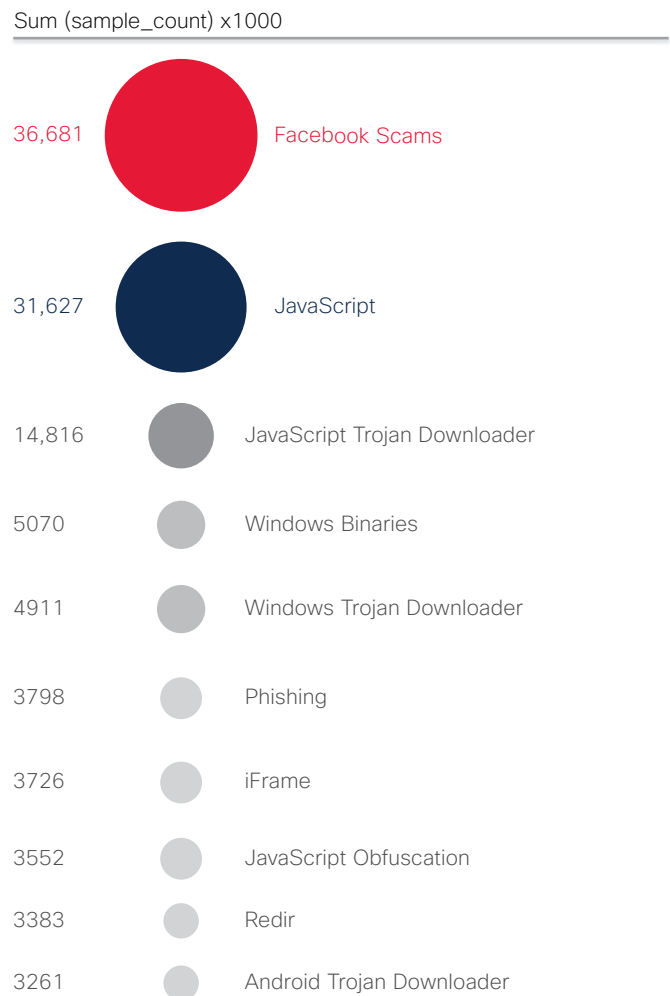


Source: Cisco Security Research

### Web Attack Methods

Figures 16 and 17 show the various types of malware that adversaries are using to gain access to organizational networks. Figure 16 illustrates the most commonly seen malware: adware, spyware, malicious redirectors, iFrame exploits, and phishing.

**Figure 16.** Most Commonly Observed Malware



Source: Cisco Security Research

<sup>5</sup> “Adobe News: Flash, HTML5 and Open Web Standards,” Adobe, November 30, 2015: <http://blogs.adobe.com/conversations/2015/11/flash-html5-and-open-web-standards.html>.



Figure 16 can essentially be viewed as a collection of types of malware that criminals use to gain initial access. These are the tried-and-true and most cost-effective methods of compromising large populations of users with relative ease. JavaScript exploits and Facebook scams (social engineering) were the most frequently used attack methods, according to our research.

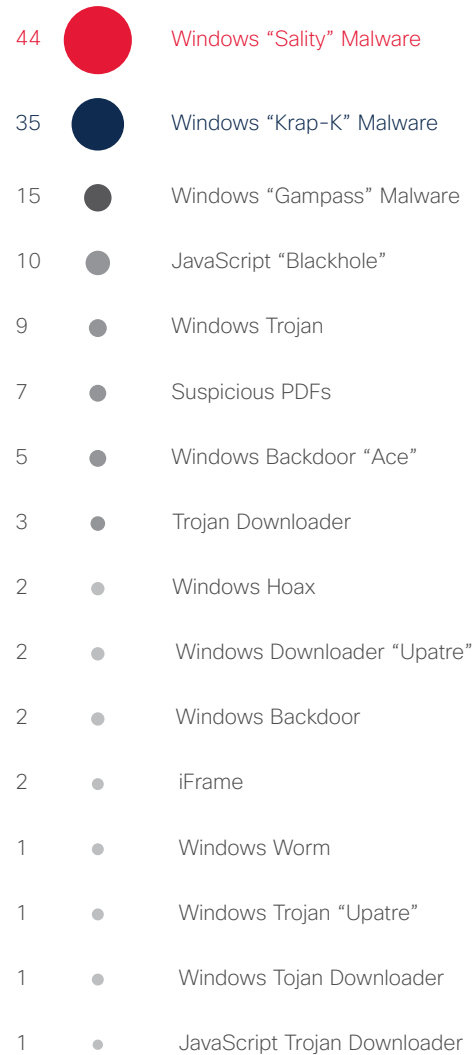
Figure 17 shows lower-volume malware. Note that “lower volume” does not mean “less effective.” According to Cisco Security Research, lower-volume malware can represent emerging threats or highly targeted campaigns.

Many of these more sophisticated techniques are designed to extract as much value as possible from compromised users. They steal high-value data, or hold users’ digital assets for ransom.

Therefore, when monitoring web malware, it is not enough to simply focus on the types of threats most commonly seen. The full spectrum of attacks must be considered.

**Figure 17. Sample of Observed Lower-Volume Malware**

Sum (sample\_count) <40



Source: Cisco Security Research

## Threat Updates


### ADOBE FLASH TOPS VULNERABILITIES LIST

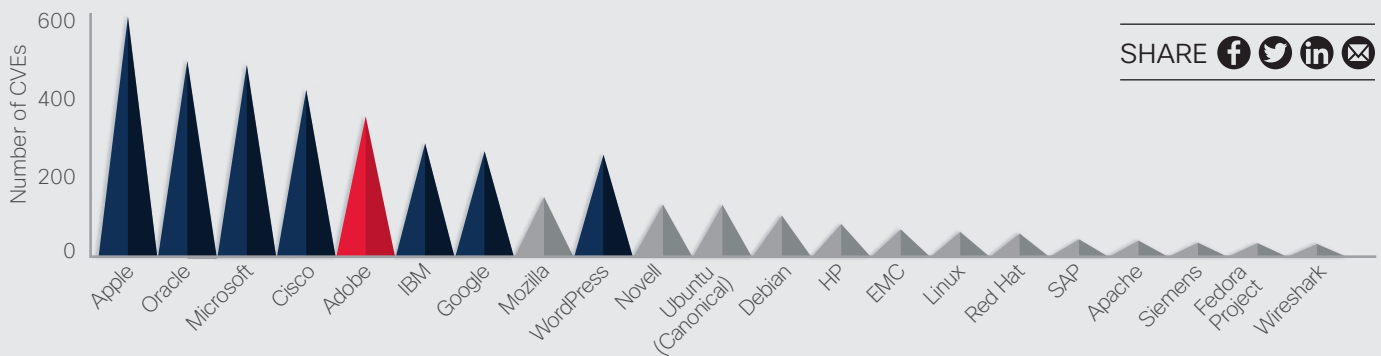
The Adobe Flash platform has been a popular threat vector for criminals for several years. Flash vulnerabilities still turn up frequently on lists of high-urgency alerts. In 2015, the good news was that the vendors of products in which these exploits commonly occur, such as web browsers, recognized this weakness and are now taking steps to reduce opportunities for adversaries.

In 2016, criminals are most likely to focus their exploits and attacks on Adobe Flash users. Some of these Flash vulnerabilities have exploits available online either publicly or for sale as part of exploit kits. (As noted on [page 21](#), the volume of Flash-related content has declined, but Flash remains a primary exploitation vector.)

Following up on tactics used to lessen the impact of Java—another common threat vector—many web browsers block or sandbox Flash as a way to protect users. Although this is a positive development, it’s important to remember that attackers will still succeed in launching exploits for some time to come. Users may fail to update their browsers as needed, and criminals will continue to launch exploits aimed at older versions of browser software.

However, Cisco researchers believe that the protections now built into some commonly used web browsers and operating systems will lessen criminals’ reliance on Flash. Because online attackers focus on achieving the best possible results (such as high profitability) for the most efficiency, they will put little effort into attacks that are less likely to provide a return on investment.

 **Figure 18. Total Number of CVEs by Vendor**



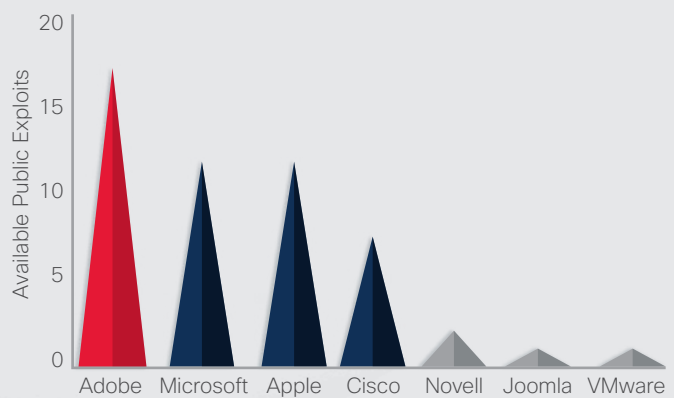
Source: Cisco Security Research, National Vulnerability Database

The chart above shows the total number of CVEs published in 2015 by vendor. Note that Adobe is not as prominent on this chart as it is in the chart on the right, which shows the vulnerabilities for which exploits are available.

In addition, WordPress shows only 12 vulnerabilities for 2015 for its own product. The additional 240 vulnerabilities come from plugins and scripts created by third-party contributors.

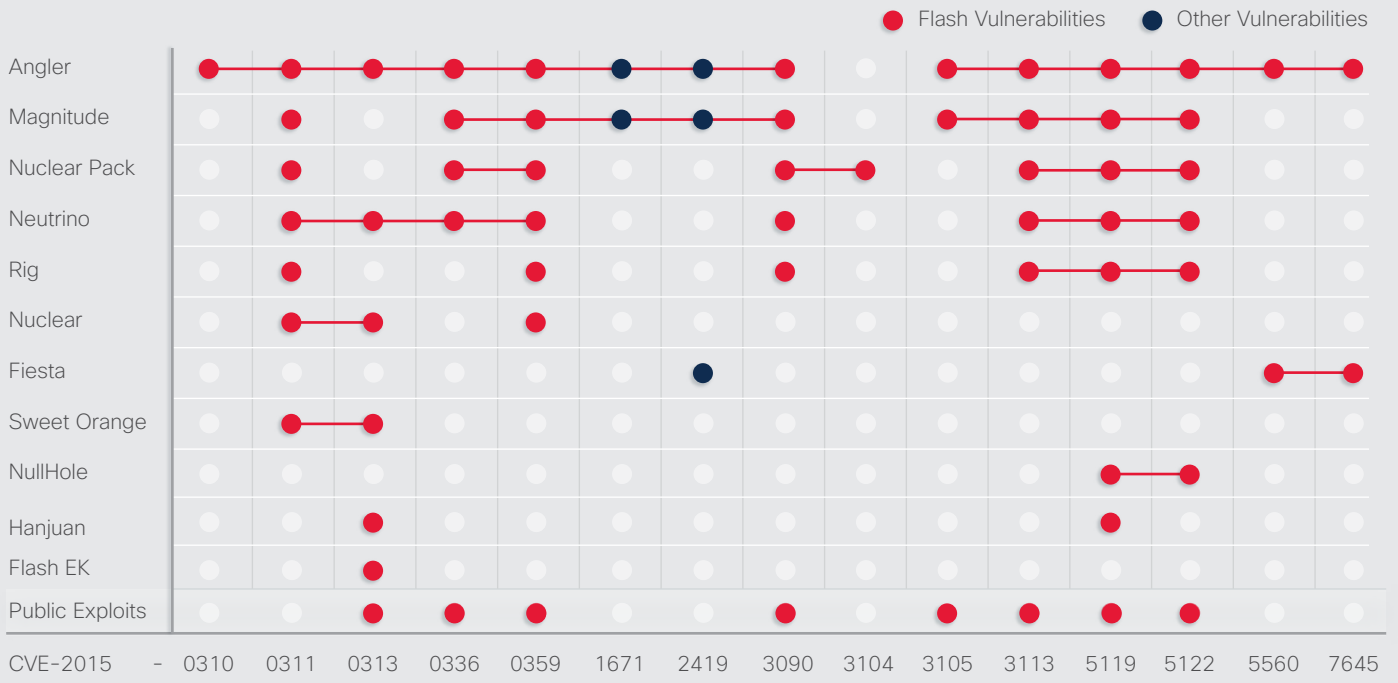
As noted in Figure 20, lists of vulnerabilities and related exploits can provide guidance for security professionals. They can use them to manage and prioritize the vulnerabilities that are high risk and most common, and patch them more quickly than low-risk vulnerabilities. See the CVE Details website (<https://www.cvedetails.com/top-50-products.php>) for more information about CVEs by vendor.

**Figure 19. Number of Public Exploits Available by Vendor Vulnerability**



Source: Cisco Security Research, Metasploit, Exploit DB

Figure 20. Common Vulnerabilities



Source: Cisco Security Research

Figure 20 displays high-risk vulnerabilities, and indicates whether the vulnerability is part of an exploit kit for hire (see “Flash EK” line) or has exploits publicly available (see “Public Exploits” line). Vulnerabilities for which functional exploits are available are a high priority for patching.

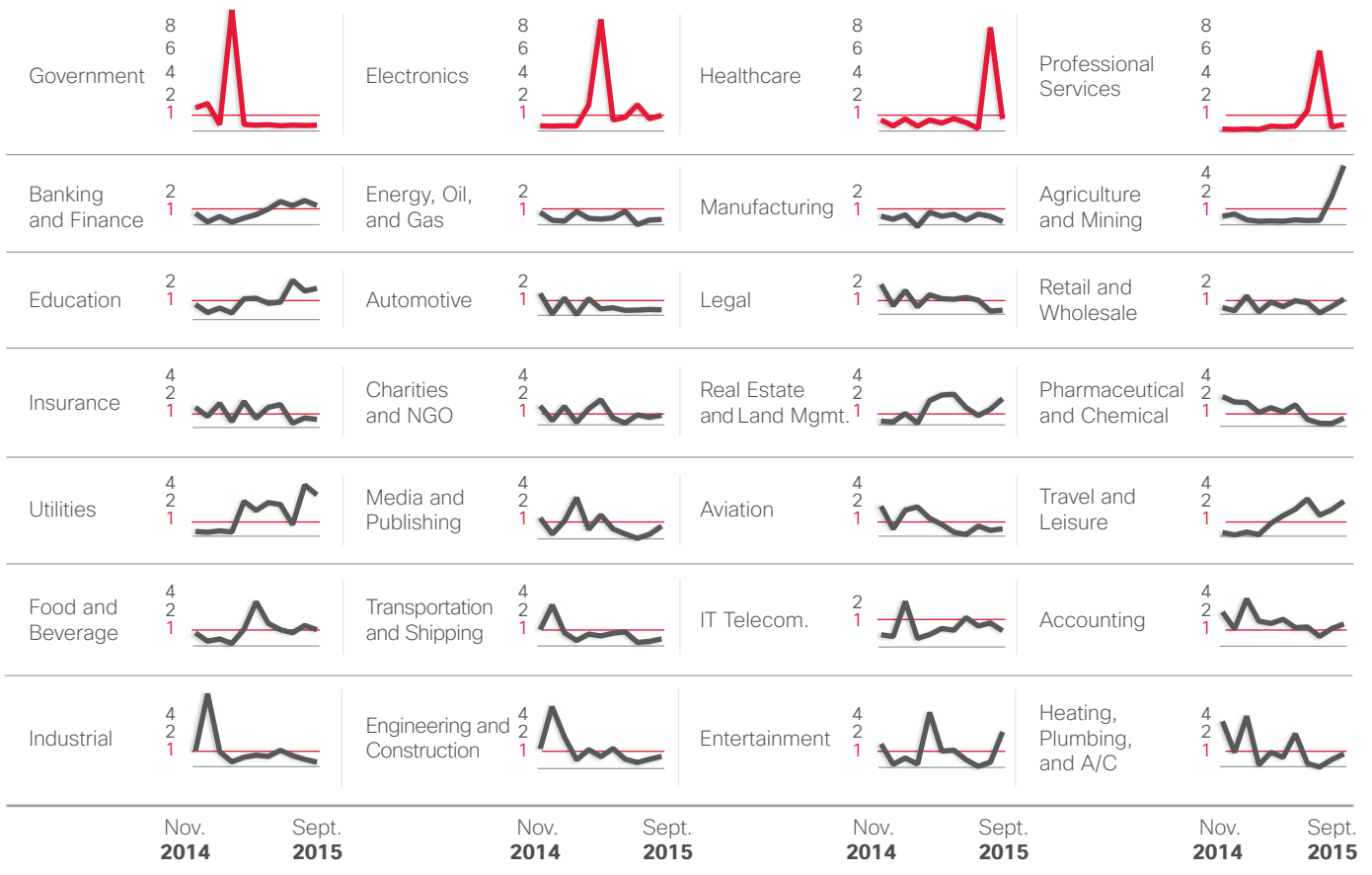
This list can be used to help security professionals prioritize their patching and remediation activities. The existence of an exploit for a given product—publicly or within an exploit kit—does not necessarily indicate that attacks are occurring.

### Vertical Risk of Malware Encounters

To track high-risk verticals for web malware encounters, we examined the relative volumes of attack traffic (“block rates”) and “normal” or expected traffic.

Figure 21 shows the top 28 industries and their relative block activity as a proportion of normal network traffic. A ratio of 1.0 means the number of blocks is proportional to the volume of observed traffic. Anything above 1.0 represents higher-than-expected block rates, and anything below 1.0 represents lower-than-expected block rates.

**Figure 21. Monthly Vertical Block Rates, November 2014–September 2015**



Source: Cisco Security Research

Figure 22 illustrates how adversaries' focus on specific verticals can be fleeting. (Zero represents no net change.) From January to March 2015, government was the vertical with the highest block rate activity. From March to May, it was electronics. In midsummer, professional services saw the most blocks. And in the fall of 2015, healthcare was leading all verticals in the number of block rates.

According to our research, the four verticals with the most block activity in 2015 were all targeted with Trojan-related attacks. The government vertical also faced a high number of PHP injection attacks, while the professional services vertical was hit with a high number of iFrame attacks.

**Figure 22. Relative Block Rates of Verticals, Month to Month Comparison**



Source: Cisco Security Research

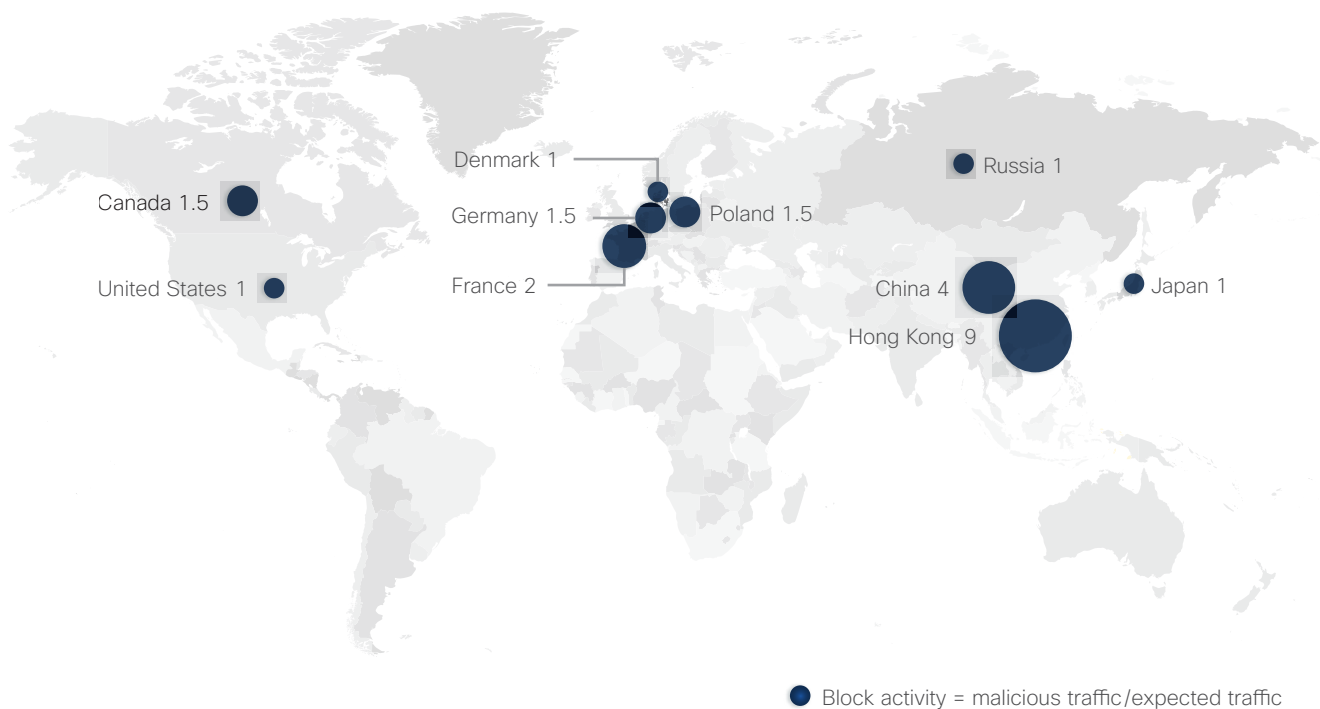
SHARE    

## Web Block Activity: Geographic Overview

We also examined where malware-based block activity originates by country or region, as seen in Figure 23. The countries were selected for the study based on their volume of Internet traffic. A “block ratio” value of 1.0 indicates that the number of blocks we see is proportional to network size.

Countries and regions with block activity that we consider higher than normal probably have many web servers and hosts with unpatched vulnerabilities on their networks. Malicious actors do not respect country boundaries and will host malware where it is most effective.

**Figure 23.** Web Blocks by Country or Region



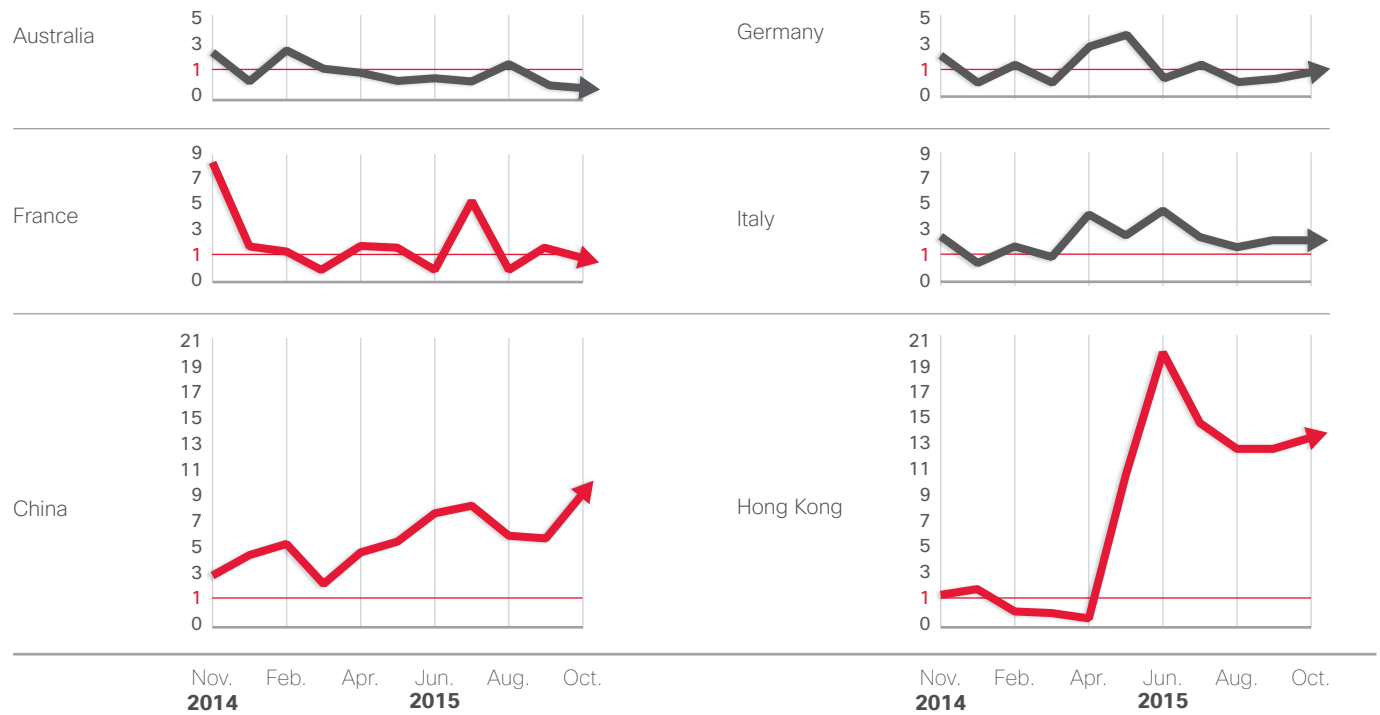
Source: Cisco Security Research

A presence in large, commercially viable networks that handle high Internet volume is another factor for high block activity—which is one reason why Hong Kong tops our list.

Figure 24, which shows a month-to-month comparison of web blocks by country or region from November 2014 to October 2015, provides some additional context for these rankings.

Note that Hong Kong saw higher than normal web block activity beginning in the spring of 2015, as did France. Both have since experienced a significant drop in web block activity, but because the higher rates of activity earlier this year were so far above the baseline, the recent decline in activity still leaves Hong Kong quite higher by the end of the year than at the start. The spike in block activity in France returned to normal levels by midsummer.

**Figure 24. Web Blocks by Country or Region, Month to Month, November 2014–October 2015**



Source: Cisco Security Research



# Industry Insights

# Industry Insights

Cisco provides research and analysis on security trends and practices. Paradoxically, some may make defenders' ability to track threats more challenging and place organizations and individual users at greater risk for compromise or attack.

## Encryption: A Growing Trend—and a Challenge for Defenders

Encryption makes sense. Companies need to protect their intellectual property and other sensitive data, advertisers want to preserve the integrity of their ad content and back-end analytics, and businesses are placing more focus on protecting their customers' privacy.

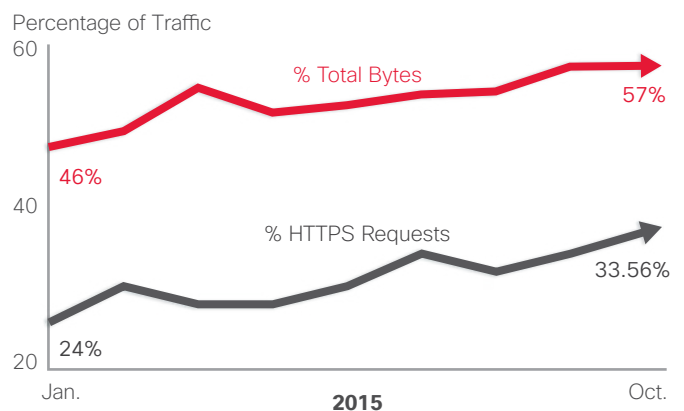
But encryption also creates security issues for organizations—including a false sense of security. Organizations have become better at encrypting data when it is transmitted between entities, but data at rest is often left unsecured. Many of the most notable breaches in the last few years have taken advantage of unencrypted data stored in the data center and other internal systems. For attackers, this is like following a secured supply truck to an unlocked warehouse.

It is also important for organizations to understand that end-to-end encryption can lessen the effectiveness of some security products. Encryption conceals the indicators of compromise used to identify and track malicious activity.

But there is no excuse to leave sensitive data unencrypted. Security tools and their operators need to adapt to this brave new world by gathering headers and other non-encrypted parts of the data stream along with other sources of contextual information to analyze encrypted traffic. Tools that rely on payload visibility, such as full packet capture, are becoming less effective. Running Cisco NetFlow and other metadata-based analyses is now essential.

Observing the trends of 2015, our researchers suggest that encrypted traffic, particularly HTTPS, has reached a tipping point. While not yet the majority of transactions, it will soon become the dominant form of traffic on the Internet. In fact, our research shows that it already consistently represents over 50 percent of bytes transferred (Figure 25) due to the HTTPS overhead and larger content that is sent via HTTPS, such as transfers to file storage sites.

**Figure 25. SSL Percentages**



Source: Cisco Security Research

For any web transaction, a number of bytes is sent out (outbound) and received (inbound). HTTPS transactions have larger outbound requests than HTTP outbound requests—about an extra 2000 bytes. HTTPS inbound requests, meanwhile, also have overhead, but this becomes less significant with larger responses.

SHARE    

By combining the incoming and outgoing bytes per web transaction, we can determine the overall percentage of all bytes involved per web transaction that are encrypted using HTTPS. Due to the increase in HTTPS traffic and the extra overhead, we determined that HTTPS bytes represented 57 percent of all web traffic in October 2015 (Figure 25), up from 46 percent in January.

We also determined through web traffic analysis that HTTPS requests have been increasing gradually, but significantly, since January 2015. As Figure 25 shows, 24 percent of the requests in January used the HTTPS protocol; the rest of them used HTTP.

By October, 33.56 percent of the requests observed were HTTPS. Additionally, we found that the percentage of inbound HTTPS bytes had increased. This was true throughout the year. As the amount of traffic using HTTPS increases, more bandwidth is required. An additional 5 Kbps is required per transaction.

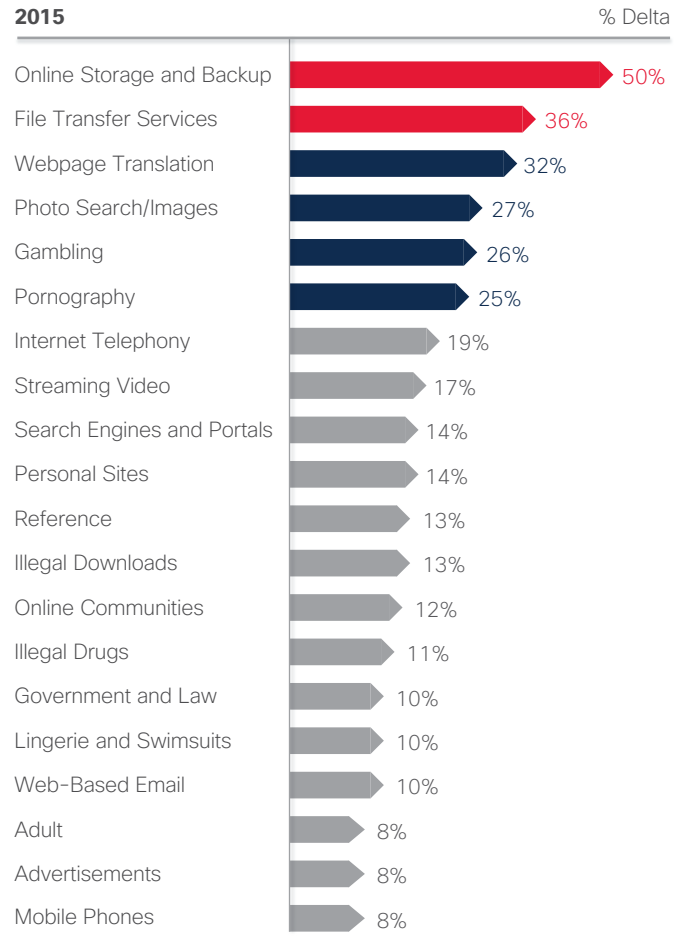
We attribute the overall increase in encrypted web traffic primarily to these factors:

- More mobile traffic from applications, which inherently encrypt
- More requests from users to download encrypted video
- More requests to storage and backup servers that hold sensitive “data at rest,” which adversaries are eager to tap

In fact, Figure 26 shows that HTTPS requests to online storage and backup resources had increased by 50 percent since the start of 2015. File transfer services are also up significantly during the same period—36 percent.

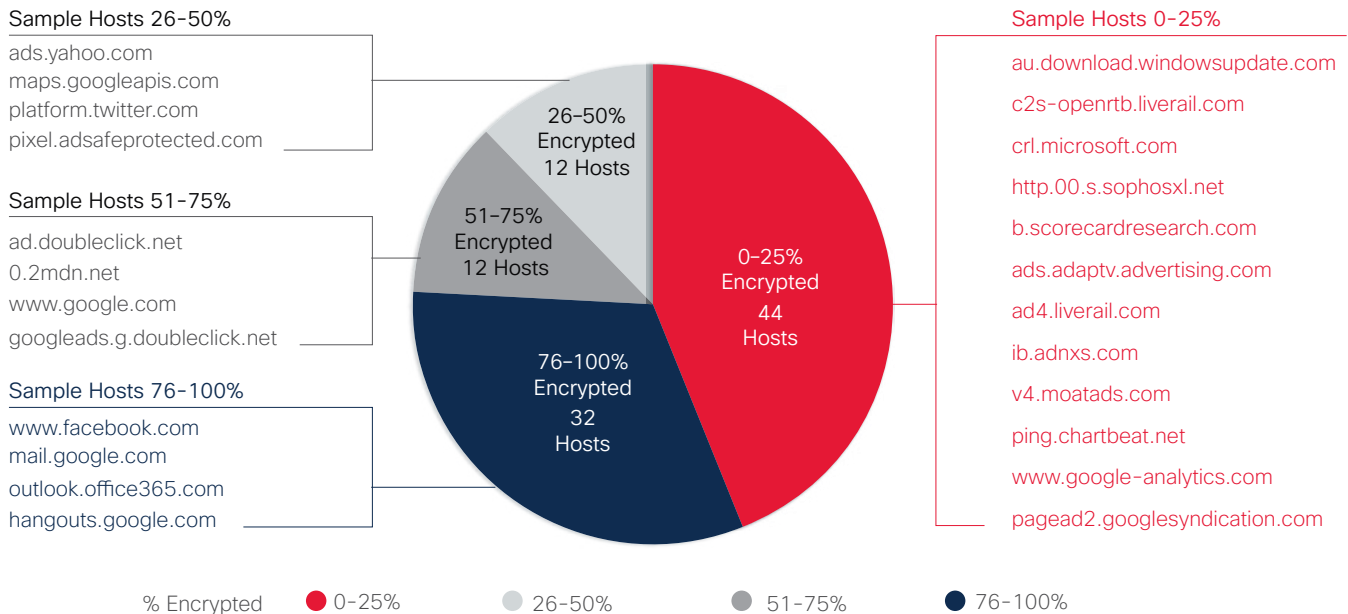
Ultimately, there is increasing encrypted activity occurring in both the number of encrypted transactions and the number of encrypted bytes in each transaction. Each one poses its own benefit and its own potential risk, ushering in the need for an integrated threat defense that helps increase visibility.

**Figure 26. HTTPS Requests: Biggest Changes from January to September 2015**



Source: Cisco Security Research

SHARE    

**Figure 27. Top Hosts Encrypting HTTPS Traffic**

Source: Cisco Security Research

Looking at the top domains by requests (Figure 27), we see that many of the main content pages of Google and Facebook are encrypted. Typically, only 10 percent of their advertising traffic is encrypted.

Regardless of the challenges, data encryption is a requirement in the current threat landscape. Attackers are too adept at circumventing access control for users to leave critical information unprotected at any stage of storage or transfer.

This is why it is essential for security teams to monitor web traffic patterns to make sure that HTTPS requests are not coming from or going to suspicious locations. A word of caution: Don't look for encrypted traffic over a predefined set of ports. As discussed in the next section, our research shows that malware is likely to initiate encrypted communications over a diverse set of ports.

### THE ENTROPY FACTOR

High entropy is a good indication of encrypted or compressed file transfers or communication.<sup>6</sup> The good news for security teams is that entropy is relatively easy to monitor because it does not require knowledge of the underlying cryptographic protocols.

During a 3-month period beginning June 1, 2015, Cisco security researchers observed 7,480,178 flows from 598,138 "threat score: 100" malware samples submitted. There were 958,851 high-entropy flows during this period, or 12.82 percent.

We also identified 917,052 flows over the Transport Layer Security (TLS) protocol (12.26 percent). In addition, 8419 TLS flows were over a port other than 443—the default port for secured HTTP. Some of the ports that the observed malware used for communication were ports 21, 53, 80, and 500.

As the level of encrypted Internet traffic continues to rise, it will become increasingly important for organizations to embrace an integrated threat defense architecture (see "The Six Tenets of Integrated Threat Defense," [page 62](#)). Point solutions are not effective at identifying potential threats in encrypted traffic. Integrated security platforms provide security teams with more visibility into what's happening on devices or networks, so they can more easily identify suspicious patterns of activity.

<sup>6</sup> Entropy: In computing, entropy (lack of order or predictability) is the randomness collected by an operating system or application for use in cryptography or other uses that require random data.

## ! The Move Toward Encryption: Case Data

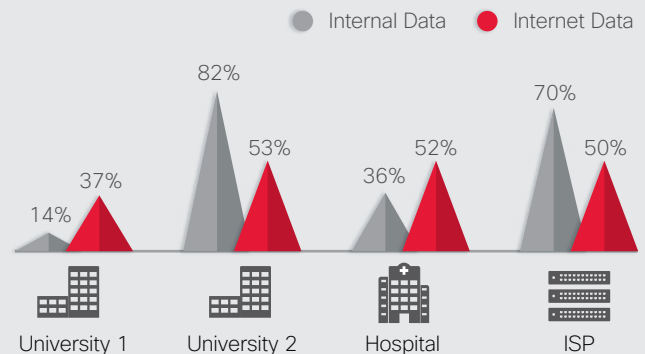
Lancope, a Cisco company, examined encryption rates for both internal and Internet traffic across three business sectors (two universities, a hospital, and an ISP provider, all based in the United States).

At one of the universities, Lancope found that almost all internal traffic was encrypted (82 percent). In addition, 53 percent of the university's Internet traffic was encrypted. These findings are on par with trends that Lancope has observed in other industries.

Only 36 percent of the hospital's internal data was encrypted. However, more than half (52 percent) of the Internet traffic was encrypted.

At the leading ISP provider, 70 percent of the internal traffic was encrypted, and 50 percent of Internet traffic was encrypted.

The study by Lancope tells a story of broad-based adoption of encryption for data in motion across various sectors. Cisco suggests a similar focus should now be applied to the encryption of data at rest to limit the impacts of organizational compromises.



Source: Lancope Threat Research Labs

## Online Criminals Increase Server Activity on WordPress

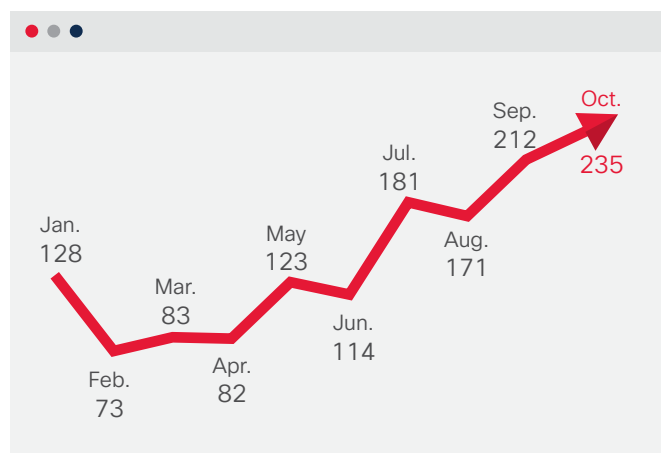
As discussed in the introduction to this report, online criminals are continually on the lookout for methods to add efficiency and cost savings to their operations—along with new ways to evade detection. Increasingly, cybercriminals are finding this efficiency within websites created using WordPress, the popular website and blog development platform. In WordPress sites, attackers can take control of a steady stream of compromised servers to create an infrastructure that supports ransomware, bank fraud, or phishing attacks. The Internet is filled with abandoned sites created with WordPress that are not maintained from a security perspective; as new security issues surface, these sites are often compromised and incorporated into attack campaigns.

Analyzing the systems used to support ransomware and other malware, Cisco security researchers found that many online criminals are shifting online activity to compromised WordPress servers. The number of WordPress domains used by criminals grew 221 percent between February and October 2015 (see Figure 28).

This shift in venue, Cisco researchers believe, has happened for a couple of reasons. When ransomware uses other tools to communicate encryption keys or other

command-and-control information, those communications can be detected or blocked, which prevents the encryption process from completing. However, communications that relay encryption keys through compromised WordPress servers may appear normal, thus increasing the chances that file encryption will be completed. In other words, the WordPress sites act as relay agents.

**Figure 28.** Number of WordPress Domains Used by Malware Creators



Source: Cisco Security Research

To sidestep the drawbacks of other technologies, criminals have turned to WordPress, which they use to host malware payloads and command-and-control servers. WordPress sites offer several advantages. For example, the many abandoned sites give criminals more opportunities for compromising sites with weak security protections.

The risk of using compromised systems to run a malware operation is that one of the hacked servers may be taken down when the compromise is discovered. If this happens in the middle of a campaign, the malware downloader may fail to retrieve its payload or the malware may be unable to communicate with its command-and-control servers. Cisco security researchers noticed that malware overcame this by using more than one WordPress server; Cisco even discovered lists of compromised WordPress servers stored on data-sharing sites such as Pastebin.

The malware used these lists to find working command-and-control servers, allowing the malware to operate even if a compromised server failed. Researchers also identified malware downloaders that contained a list of WordPress sites storing payloads. If one download site was not working, the malware went to the next one and downloaded malicious payloads from the working WordPress server.

The compromised WordPress sites were often not running the latest version of WordPress, had weak admin passwords, and used plugins that were missing security patches.

These vulnerabilities allowed attackers to co-opt WordPress servers and use them as malware infrastructure (see Figure 29).

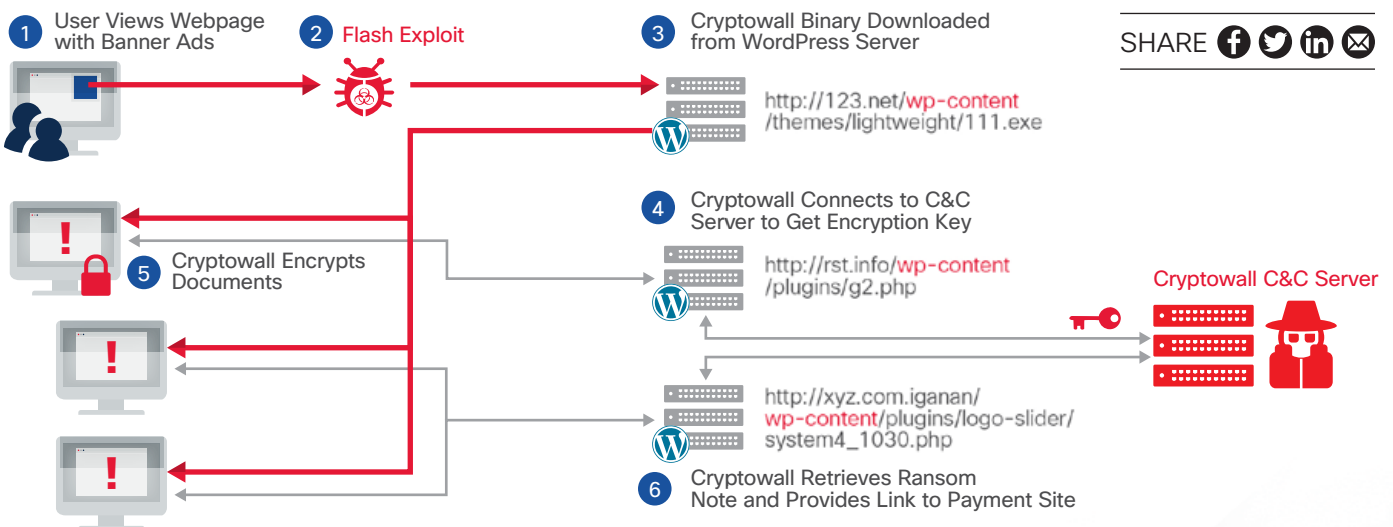
Cisco researchers have identified some of the software and file types commonly hosted on compromised WordPress sites:

- Executable files that are payloads for exploit kit attacks
- Configuration files for malware such as Dridex and Dyre
- Proxy code that relays command-and-control communication to hide command-and-control infrastructure
- Phishing webpages for collecting usernames and passwords
- HTML scripts that redirect traffic to exploit kit servers

In addition, Cisco researchers have identified many malware families that are using compromised WordPress sites for infrastructure:

- Dridex infostealer
- Pony password stealer
- TeslaCrypt ransomware
- Cryptowall 3.0 ransomware
- TorrentLocker ransomware
- Andromeda spam botnet
- Bartallex Trojan dropper
- Necurs infostealer
- Fake login pages

**Figure 29. How WordPress Sites Are Compromised**



Source: Cisco Security Research

SHARE    

Security professionals concerned about the threats posed by WordPress hosting by criminals should seek web security technology that examines content coming from WordPress-created sites. Such traffic could be considered unusual if the network is downloading programs from WordPress sites instead of just webpages and images (although WordPress sites can host legitimate programs as well).

### Aging Infrastructure: A Problem 10 Years in the Making

All companies today are IT companies to some degree, because they are dependent on their IT and OT (operational technology) infrastructure to be connected, digitized, and successful. That means they need to make IT security a priority. Yet many organizations rely on network infrastructures built of components that are old, outdated, and running vulnerable operating systems—and are not cyber-resilient.

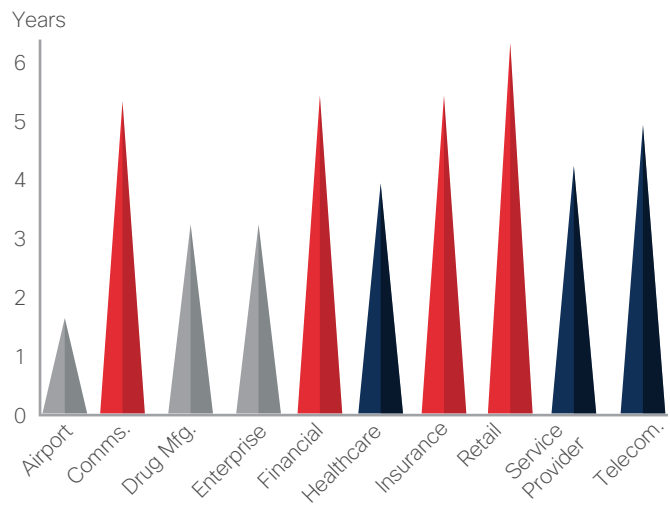
We recently analyzed 115,000 Cisco devices on the Internet and across customer environments as a way to bring attention to the security risks that aging infrastructure—and lack of attention to patching vulnerabilities—present.

We identified the 115,000 devices in our one-day sample by scanning the Internet and then looking at the devices from the “outside in” (from the Internet view and into the enterprise). Through our scanning and analysis, we found that 106,000 of the 115,000 devices had known vulnerabilities in the software they were running. That means 92 percent of the Cisco devices on the Internet in our sample are susceptible to known vulnerabilities.

Cisco also discovered that the version of the software that those devices were running had 26 vulnerabilities, on average. In addition, we learned that many organizations

were running outdated software in their network infrastructure (Figure 30). We found some customers in the financial, healthcare, and retail verticals using versions of our software that are more than 6 years old.

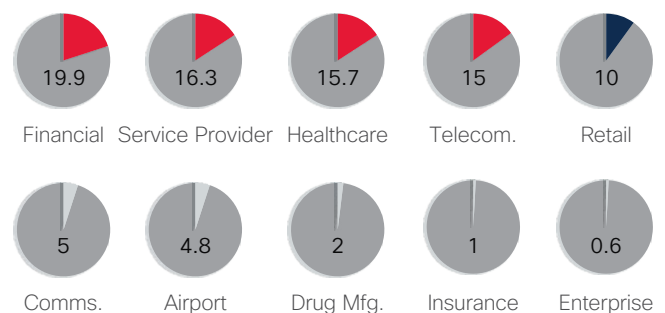
Figure 30. Average Software Age in Years



Source: Cisco Security Research

We also discovered that many of the infrastructure devices we analyzed had reached their last day of support (LDoS)—meaning they cannot be updated and made more secure (Figure 31). These devices are not even receiving patches for known vulnerabilities, so they are not being provided information about new threats. Customers have been made aware of this issue.

Figure 31. Percentage of LDoS for Infrastructure Devices



Source: Cisco Security Research

**!** For more on this topic, read the **Cisco Security blog posts:**  
**“IT Security: When Maturity Is Overrated”**  
**“Evolution of Attacks on Cisco IOS Devices”**  
**“SYNful Knock: Detecting and Mitigating Cisco IOS Software Attacks”**



In addition, 8 percent of the 115,000 devices in our sample that we analyzed have reached their end-of-life stage, and another 31 percent will reach end of support within one to four years.

Aging, outdated IT infrastructure is a vulnerability for organizations. As we move closer to the Internet of Things (IoT)—and the Internet of Everything (IoE)—it becomes more important for businesses to make sure they are relying on a network infrastructure that is secure, thus ensuring the integrity of the data and communications traversing the network. This is critical to the success of the emerging IoE.

Many Cisco customers built their network infrastructure a decade ago. Back then, many businesses simply did not account for the fact that they would be 100 percent reliant on that infrastructure. Nor did they anticipate that their infrastructure would become a prime target for adversaries.

Organizations tend to avoid making infrastructure updates because it's expensive and requires network downtime. In some cases, a simple update won't be enough. Some products are so old they cannot be upgraded to incorporate the latest security solutions needed to protect the business.

These facts alone speak to the criticality of maintaining infrastructure. Organizations need to plan for regular upgrades and recognize the value of taking control of their critical infrastructure proactively—before an adversary does.

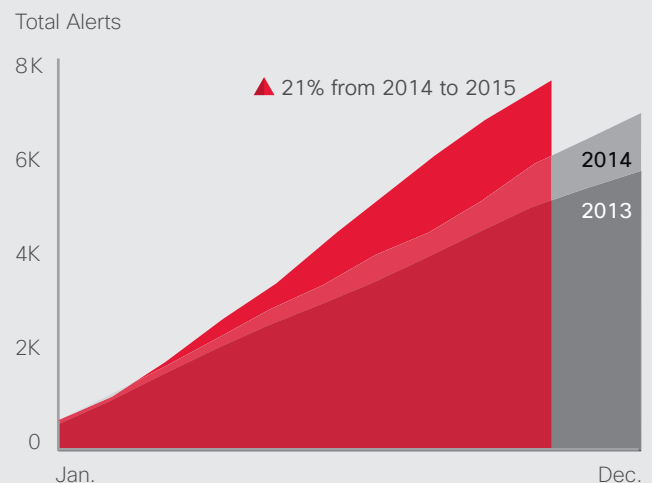
## ! Cumulative Alert Totals Show Growing Commitment to Managing Vulnerabilities

Reliance on aging infrastructure opens the door to attackers. However, the rise in cumulative alerts—which include product vulnerabilities in open-source and proprietary solutions—is a positive sign that the technology industry is paying close attention to eliminating opportunities for attackers.

Cumulative alert totals have increased 21 percent from 2014 to 2015. From July through September 2015, the increase was notably high. This increase can be attributed in large part to major software updates from vendors such as Microsoft and Apple, because product updates lead to more reporting of software vulnerabilities.

Major software vendors now release patches and upgrades in greater volume, and they are more transparent about this activity. The increasing volume is a main driver for organizations automating their vulnerability management through the use of security intelligence and management platforms that help manage the volume of system and software inventory, vulnerability, and threat information. Using these systems and application programming interfaces (APIs) allows for more efficient, timely, and effective security management across large and small organizations.

Figure 32. Cumulative Annual Alert Totals



Source: Cisco Security Research

SHARE    

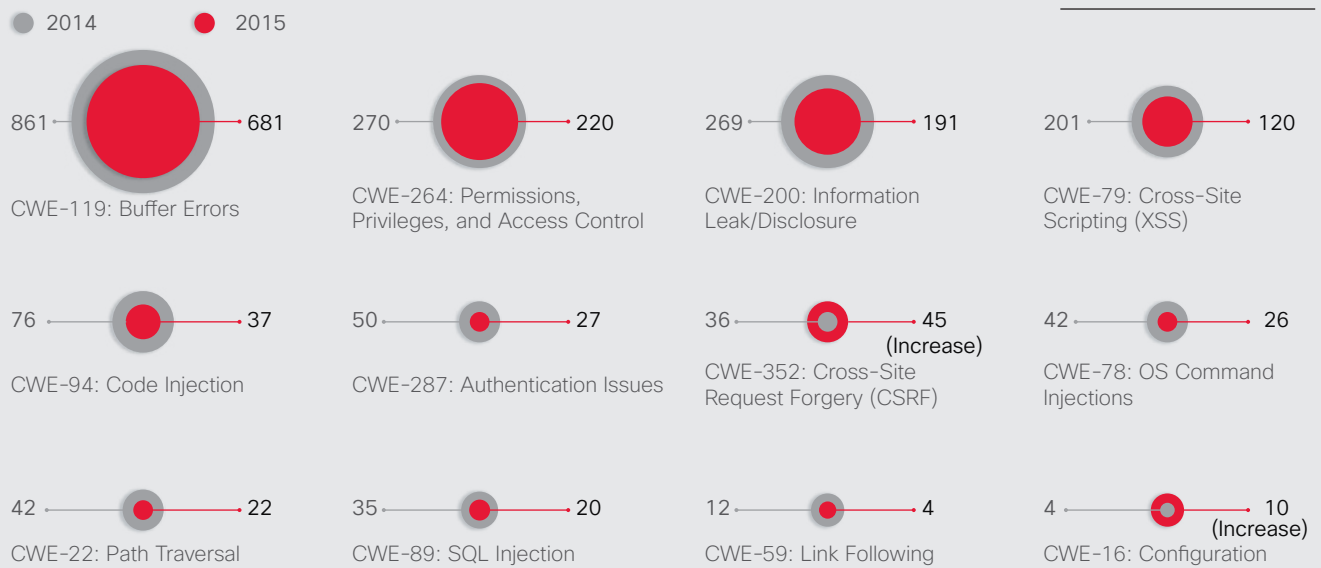
**Threat Categories: Decline in Buffer Errors, Information Leaks, and Disclosures**

In examining common vulnerability categories, cross-site scripting (XSS) vulnerabilities dropped 47 percent from 2014 to 2015 (Figure 33). The decrease may be a result of the greater attention paid to vulnerability testing. Vendors have become more skilled at identifying these particular vulnerabilities and fixing them before their products go to market.

Information leak or information disclosure vulnerabilities dropped 15 percent in 2015. These vulnerabilities involve unintentional disclosures to parties that don't have explicit access. Vendors have become attentive to controls that allow or disallow access to data, making this common vulnerability a less-frequent occurrence.

**Figure 33.** Number of Vulnerabilities in Common Categories

SHARE    



Source: Cisco Security Research

**Are Small and Midsize Businesses a Weak Link to Enterprise Security?**

SMBs play a critical role in national economies. When entrusted with data by their customers, SMBs also carry the responsibility of protecting this information from online attackers. However, as detailed in the Cisco 2015 Security Capabilities Benchmark Study (see [page 41](#)), SMBs show signs that their defenses against attackers are weaker than their challenges demand. In turn, these weaknesses can place SMBs' enterprise customers at risk. Attackers that can breach an SMB network could also find a path into an enterprise network.

Judging from the results of the Cisco 2014 Security Capabilities Benchmark Study, SMBs are using fewer processes to analyze compromises and fewer threat defense tools than they used last year. For example, 48 percent of SMBs said in 2015 that they used web security; 59 percent said they did in 2014. Only 29 percent said they used patching and configuration tools in 2015, compared with 39 percent in 2014.

In addition, of the SMB respondents that do not have an executive responsible for security, nearly one-quarter do not believe their businesses are high-value targets for online criminals. This belief hints at overconfidence in their business's ability to thwart today's sophisticated online attacks—or, more likely, that attacks will never happen to their business.

### SMBS LESS LIKELY TO USE INCIDENT RESPONSE TEAMS

In many cases, SMBs are less likely than large enterprises to have incident response and threat intelligence teams. This may be due to budget constraints: Respondents pointed to budget issues as one of the biggest obstacles to adopting advanced security processes and technology. Seventy-two percent of large enterprises (those with more than 1000 employees) have both teams, compared with 67 percent of businesses with fewer than 500 employees.





SMBs also use fewer processes to analyze compromises, eliminate the causes of an incident, and restore systems to pre-incident levels (Figure 35). For example, 53 percent of enterprises with more than 10,000 employees use network flow analysis to analyze compromised systems,

compared with 43 percent of businesses with fewer than 500 employees. Sixty percent of businesses with more than 10,000 employees patch and update applications deemed vulnerable, compared with 51 percent of businesses with fewer than 500 employees.

SMBs' use of certain threat defenses appears to be on the decline. For example, in 2014, 52 percent of SMBs used mobility security, but only 42 percent did so in 2015. Also, in 2014, 48 percent of SMBs used vulnerability scanning, compared to 40 percent in 2015 (see Figure 36).

### Figure 34. SMB Biggest Obstacles

Which of the Following do You Consider the Biggest Obstacles to Adopting Advanced Security Processes and Technology?

| Company Size                             |  250-499 |  500-999 |  1000-9999 |  10,000+ |
|--|--|--|--|--|
| Budget Constraints                       | 40%  | 39%  | 39%  | 41%  |
| Compatibility Issues with Legacy Systems | 34%  | 30%  | 32%  | 34%  |
| Competing Priorities                     | 25%  | 25%  | 24%  | 24%  |

Source: Cisco 2015 Security Capabilities Benchmark Study

### Figure 36. SMB Defenses Decrease in 2015





Which—If Any—of These Types of Security Threat Defenses Does Your Organization Currently Use?

|  | 2014 | 2015 |
|--|------|------|
| Mobile Security                                  | 52%  | 42%  |
| Secured Wireless                                 | 51%  | 41%  |
| Vulnerability Scanning                           | 48%  | 40%  |
| VPN  | 46%  | 36%  |
| Security Information and Event Management (SIEM) | 42%  | 35%  |
| Penetration Testing                              | 38%  | 32%  |
| Network Forensics                                | 41%  | 29%  |
| Patching and Configuration                       | 39%  | 29%  |
| Endpoint Forensics                               | 31%  | 23%  |

Source: Cisco 2015 Security Capabilities Benchmark Study

### Figure 35. SMBs Use Fewer Security Processes than Large Enterprises

Which of These Processes—If Any—Does Your Organization Use to Analyze Compromised Systems?

| Company Size  |  250-499 |  500-999 |  1000-9999 |  10,000+ |
|---|---|---|---|---|
| Memory Forensics  | 36%   | 36%   | 35%   | 34%   |
| Network Flow Analysis                                   | 43%   | 47%   | 52%   | 53%   |
| Correlated Event/Log Analysis                           | 34%   | 34%   | 40%   | 42%   |
| External (Third-Party) Incident Response/Analysis Teams | 40%   | 32%   | 34%   | 39%   |
| Systems Log Analysis                                    | 47%   | 51%   | 55%   | 59%   |
| Registry Analysis                                       | 43%   | 47%   | 52%   | 53%   |
| IOC Detection   | 31%   | 34%   | 37%   | 36%   |

What Processes Does Your Organization Use to Restore Affected Systems to Pre-Incident Operational Levels?

|   | 250-499 | 500-999 | 1000-9999 | 10,000+ |
|---|---------|---------|-----------|---------|
| Patch and Update Applications Deemed Vulnerable     | 51%     | 53%     | 57%       | 60%     |
| Implement Additional or New Detections and Controls | 49%     | 55%     | 57%       | 61%     |

Source: Cisco 2015 Security Capabilities Benchmark Study

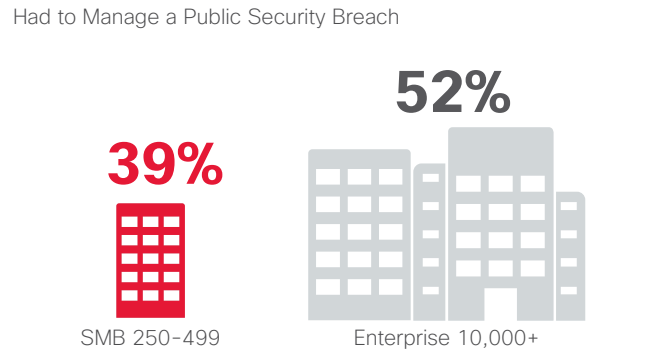
Why is it significant that SMBs tend to use fewer defenses than their larger counterparts? In a security environment where attackers are developing more sophisticated tactics for entering networks and remaining undetected, no business can afford to leave its networks unprotected, or to put off using processes that might offer insights on how a compromise occurred so it can be avoided in the future.

In addition, SMBs may not realize that their own vulnerability translates to risks for larger enterprise customers and their networks. Today's criminals often gain entry into one network as a means to find an entry point into another, more lucrative network—and the SMB may be the starting point for such an attack.

**LESS LIKELY TO HAVE EXPERIENCED PUBLIC DATA BREACHES**

SMBs are less likely than large enterprises to have dealt with a public security breach, probably a result of their smaller footprint from a network standpoint. While 52 percent of enterprises with more than 10,000 employees have managed the aftermath of a public security breach, only 39 percent of businesses with fewer than 500 employees have done so.

**Figure 37. SMBs Report Fewer Public Breaches**



Source: Cisco 2015 Security Capabilities Benchmark Study

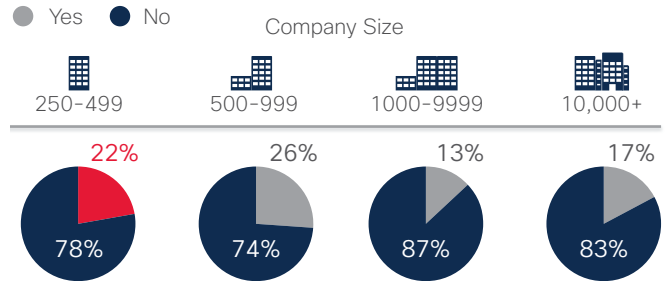
SHARE    

Public security breaches are obviously disruptive and damaging to a business, but they do offer one benefit: They often encourage businesses to take a closer look at their security protections and consider strengthening them. Cisco survey data (see [page 74](#)) shows that when large enterprises suffer a public data breach, they significantly upgrade their security technology and implement stronger processes.

**Figure 38. SMBs Do Not Perceive Themselves as High-Value Targets**



Organization is Not a High-Value Target for Attackers. (Explanation for Why an Organization Does Not Have an Executive with Direct Responsibility and Accountability for Security).



Source: Cisco 2015 Security Capabilities Benchmark Study

SMBs' view of their businesses as targets of cybercriminals may demonstrate a gap in their perception of the threat landscape. As illustrated above in Figure 38, 22 percent of businesses with fewer than 500 employees said they do not have an executive with direct responsibility and accountability for security because they do not view themselves as high-value targets.

**SMBs MORE LIKELY TO OUTSOURCE SECURITY FUNCTIONS IN 2015**





Although the survey shows that more SMBs overall are outsourcing some of their security functions, SMBs are generally less likely than large enterprises to outsource certain services, such as advice and consulting. For example, 55 percent of large enterprises outsource advice and consulting services, compared with 46 percent of businesses with fewer than 500 employees. Fifty-six percent of large enterprises outsource security auditing tasks, compared with 42 percent of businesses with fewer than 500 employees (see Figure 39).

However, in 2015, more SMBs are outsourcing at least some security services. In 2014, 24 percent of SMBs with less than 499 employees said they did not outsource any services. In 2015, only 18 percent of SMBs said the same.

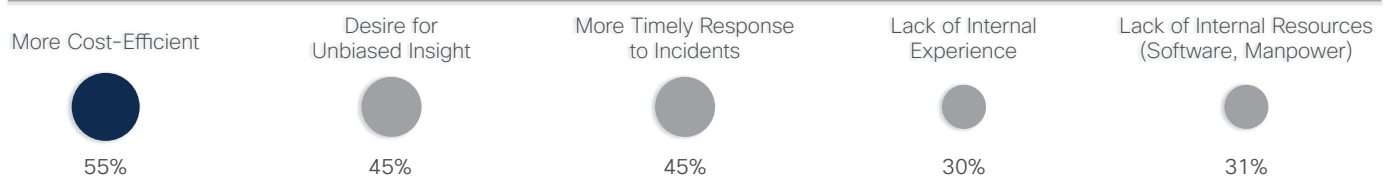
The fact that more SMBs are adopting outsourcing as a way to manage security is good news. It says that SMBs are seeking flexible tools for securing networks that do not place a burden on their smaller staffs or more conservative budgets. However, SMBs may mistakenly believe that outsourcing security processes will greatly reduce the likelihood of a network breach. Or they may place the onus for security on a third party. Such a viewpoint would be wishful thinking, since only a truly integrated threat defense system—one that examines and mitigates attacks as well as prevents them—can provide enterprise-level security protection.

**Figure 39. More SMBs Outsource Security Services in 2015**

When it Comes to Security, Which of the Following Types of Services, if Any, Are Outsourced Fully or in Part to Third Parties?

| Company Size          |  250-499 |  500-999 |  1000-9999 |  10,000+ |
|-----------------------|---|---|--|---|
| Advice and Consulting | 46%   | 51%   | 54%  | 55%   |
| Monitoring            | 45%   | 46%   | 42%  | 44%   |
| Auditing              | 42%   | 46%   | 46%  | 56%   |
| Incident Response     | 39%   | 44%   | 44%  | 40%   |
| Threat Intelligence   | 35%   | 37%   | 42%  | 41%   |
| Remediation           | 33%   | 38%   | 36%  | 36%   |
| None                  | 18%   | 12%   | 11%  | 10%   |

Why Does Your Organization (SMB 250-499) Choose to Outsource This/These Service(s)?



Source: Cisco 2015 Security Capabilities Benchmark Study

SHARE    



# Cisco Security Capabilities Benchmark Study

# Cisco 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 security resources and procedures. The Cisco 2015 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 inaugural 2014 study.

## Decline in Confidence Amid Signs of Preparedness

In the face of more sophisticated threats, the Cisco study suggests that the confidence of security professionals appears to be flagging. On the other hand, deepening concerns about security are changing how these professionals protect networks. For example, we are seeing more security training, an increase in formal written policies, and more outsourcing of tasks such as security audits, consulting, and incident response. In short, security professionals show signs that they are taking action to combat the threats that loom over their networks.

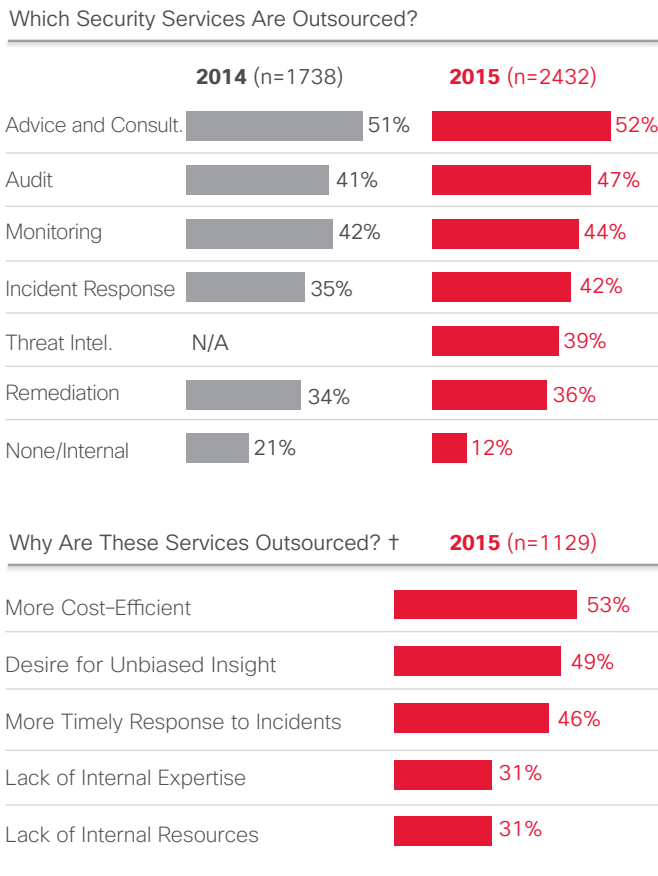
The moves toward training and outsourcing are positive developments, but the security industry can't stop there. It must continue to increase its use of tools and processes to improve the detection, containment, and remediation of threats. Given the barriers of budget limitations and solution compatibility, the industry must also explore effective solutions that provide an integrated threat defense. The industry must also do a better job of collaborating with other organizations when public breaches occur (such as with the SSHPsychos botnet; see [page 14](#)), since knowledge-sharing can help prevent future attacks.



**RESOURCES: ORGANIZATIONS MORE LIKELY TO OUTSOURCE**

As security professionals become aware of threats, they may be seeking ways to improve their defenses—for example, by outsourcing security tasks that can be managed more efficiently by consultants or vendors. In 2015, 47 percent of our surveyed companies outsourced security audits, an increase from 41 percent in 2014. Also in 2015, 42 percent outsourced incident response processes, compared with 35 percent in 2014 (Figure 40).

**Figure 40. Outsourced Services Overview**



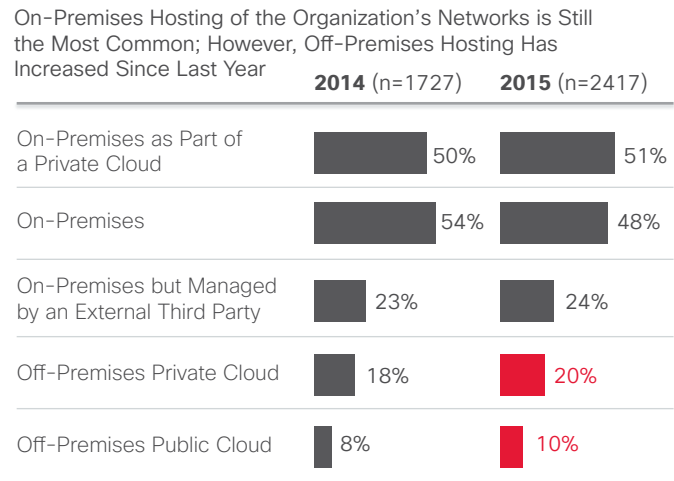
† Security respondents that outsource security services (2015; n=2129)

Source: Cisco 2015 Security Capabilities Benchmark Study

In addition, more security professionals are outsourcing at least some security functions. In 2014, 21 percent of the survey respondents said they did not outsource any security services. In 2015, that number dropped significantly, to 12 percent. Fifty-three percent said they outsource services because doing so was more cost-efficient, while 49 percent said they outsource services to obtain unbiased insights.












To add protection to their networks and data, security professionals indicated that they are receptive to the concept of hosting networks off-premises. While on-premises hosting is still the favored option, the number of professionals using off-premises solutions has increased. In 2015, 20 percent used off-premises private cloud solutions compared with 18 percent in 2014 (Figure 41).

**Figure 41. Off-Premises Hosting on the Rise**



Source: Cisco 2015 Security Capabilities Benchmark Study

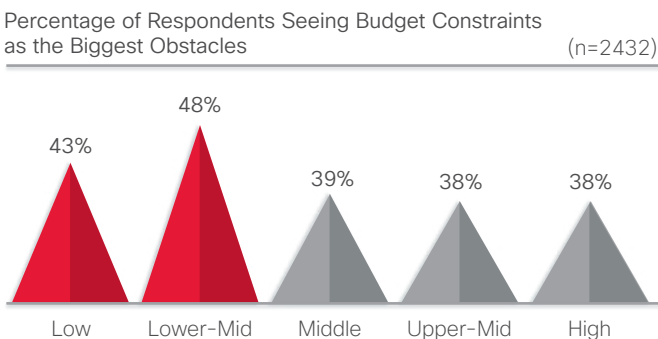
**Figure 42. Budget Constraints Are the Major Barrier to Security Upgrades**

| Biggest Barriers to Adopting Advanced Security Processes and Technology                              |   | 2015 (n=2432) |
|--|---|---------------|
| Budget Constraints  |    | 39%           |
| Compatibility Issues   |    | 32%           |
| Certification Requirements   |    | 25%           |
| Competing Priorities   |    | 24%           |
| Current Workload Too Heavy   |    | 24%           |
| Lack of Knowledge  |  | 23%           |
| Organizational Culture/Attitude  |  | 23%           |
| Lack of Trained Personnel  |  | 22%           |
| Reluctance to Purchase Until Proven  |  | 22%           |
| Upper Management Buy-In  |  | 20%           |

Source: Cisco 2015 Security Capabilities Benchmark Study

The security teams surveyed by Cisco are more intent on protecting their networks more effectively, but they may be limited in their ability to carry out their plans. Security professionals said that budget constraints (39 percent) top the list of likely reasons to choose or reject security services and tools, followed by technology compatibility issues (32 percent; see Figure 42). Budget constraints become more of a problem for enterprises that rank in the low and lower-mid maturity levels (see Figure 43). In the responses from all security professionals, 39 percent cite budget constraints as an obstacle to adopting advanced security processes. That figure is 43 percent of enterprises in the low-maturity range, and 48 percent in the lower-mid maturity range.

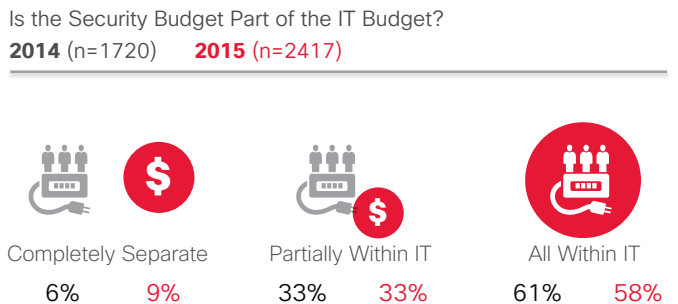
**Figure 43. Budget Constraints Are Greater Obstacle for Low-Maturity Companies**



Source: Cisco 2015 Security Capabilities Benchmark Study

One sign that some organizations are giving more thought to their security resources is how they structure their security budget. The survey shows a slight increase in the number of organizations that separate the security budget from overall IT budget. In 2014, 6 percent of professionals said they had completely separated security and IT budgets; in 2015, that number rose to 9 percent (see Figure 44).

**Figure 44. Slight Increase in Organizations with Separate Security Budgets**



Source: Cisco 2015 Security Capabilities Benchmark Study

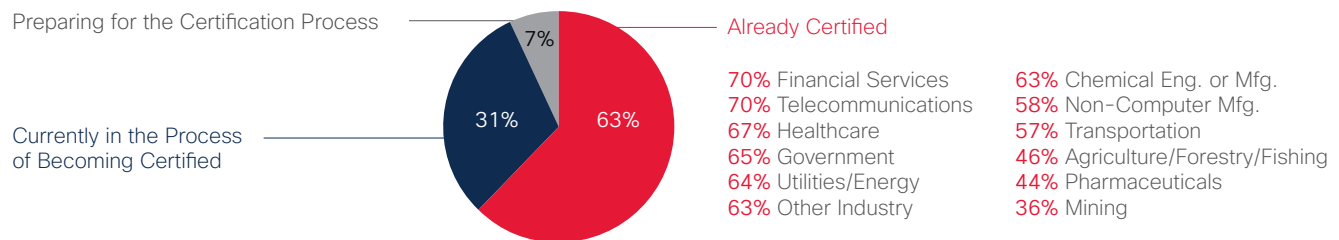
SHARE    

When organizations standardize on security policies or seek certification, they show a commitment to improving security. Nearly two-thirds of security professionals said their organizations are certified on standardized security

policies or practices, or are in the process of becoming certified (Figure 45). This is another positive sign that enterprises see value in improving their security knowledge and responding to threats.

**Figure 45. Most Organizations Are Certified or Seeking Certification**

Organization Follows Standardized Information Security Policy Practice (2015 n=1265)



Source: Cisco 2015 Security Capabilities Benchmark Study

In examining the use of security defenses, we found that firewalls are the most commonly used security tools by enterprises (65 percent), followed by data loss prevention (56 percent) and authentication tools (53 percent; see Figure 46). In 2015, enterprises were somewhat less likely to

rely on cloud-based tools. Although security professionals have shown a willingness to outsource security services (see page 43), they may be trending toward an in-house deployment of tools. (See page 71 for full list.)

**Figure 46. Firewalls and Data Loss Prevention Are Most Commonly Used Security Tools**

| Security Threat Defenses Used by Organization           | 2014 (n=1738) |            | 2015 (n=2432) |            | Defenses Administered Through Cloud-Based Services (Security Respondents Who Use Security Threat Defenses) |               |
|---|---------------|------------|---------------|------------|--|---------------|
|   | Percentage    | Percentage | Percentage    | Percentage | 2014 (n=1646)  | 2015 (n=2268) |
| Firewall*   | N/A           |            | 65%           |            |  | 31%           |
| Data Loss Prevention                                    | 55%           |            | 56%           |            |  |               |
| Authentication  | 52%           |            | 53%           |            |  |               |
| Encryption/Privacy/Data Protection                      | 53%           |            | 53%           |            |  |               |
| Email/Messaging Security                                | 56%           |            | 52%           |            | 37%  | 34%           |
| Web Security  | 59%           |            | 51%           |            | 37%  | 31%           |
| Network, Security, Firewalls, and Intrusion Prevention* | 60%           |            | N/A           |            | 35%  |               |

\*Firewall and intrusion prevention were one code in 2014: "Network security, firewalls, and intrusion prevention."

Source: Cisco 2015 Security Capabilities Benchmark Study

**CAPABILITIES: CONFIDENCE IS DOWN**

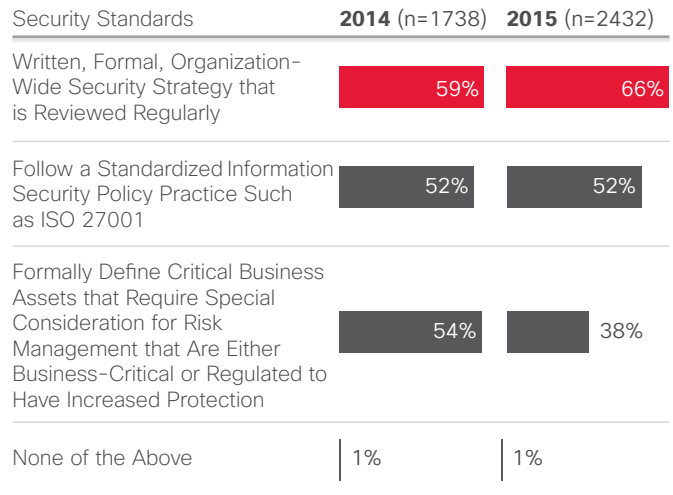
In 2015, security professionals were less confident that their security infrastructure is up to date than they were in 2014. This decline in confidence is due, no doubt, to the steady drumbeat of high-profile attacks on major enterprises, the corresponding theft of private data, and the public apologies from companies whose networks have been breached.

However, this decline in confidence is accompanied by a growing interest in developing stronger policies. As seen in Figure 47, more companies (66 percent) have a written, formal security strategy in 2015 than was the case in 2014 (59 percent).



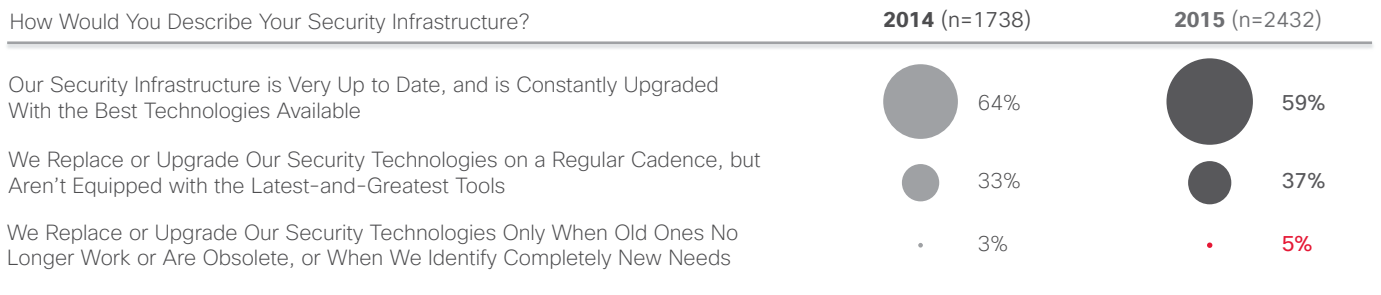
**Figure 47. More Organizations Create Formal Security Policies**

Nearly Two-Thirds are Already Certified on a Standardized Security Policy or Practice.



Source: Cisco 2015 Security Capabilities Benchmark Study

**Figure 48. Confidence Is Lower in 2015**



Source: Cisco 2015 Security Capabilities Benchmark Study

As a sign that confidence is on the decline, security professionals show slightly less confidence in their technologies. In 2014, 64 percent said their security infrastructure was up to date and constantly upgraded. In 2015, that number dropped to 59 percent (Figure 48). Also, in 2014, 33 percent said their organizations were not equipped with the latest security tools; that number rose to 37 percent in 2015.

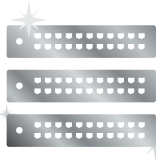
Confidence is somewhat higher among CSOs, who are more optimistic than security operations managers: 65 percent of CSOs believe their security infrastructure is up to date, compared with 54 percent of SecOps managers. The confidence of SecOps managers is likely to suffer because they respond to day-to-day security incidents, giving them a less positive view of their security readiness.

**Figure 49. Mixed Confidence in Ability to Detect Compromises**

How Would You Describe Your Security Infrastructure?

(2015 n=2432)

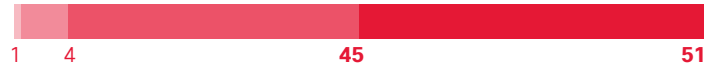
Strongly Disagree | Disagree | **Agree** | **Strongly Agree**



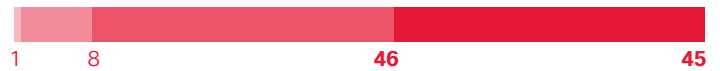
**59%**

Our Security Infrastructure is Very Up to Date, and is Constantly Upgraded with the Best Technologies Available.

Percentage of Organizations Able to Detect Security Weaknesses Before They Become Full-Blown Incidents



Percentage of Organizations Confident in Determining the Scope of a Compromise and Remediating It



Source: Cisco 2015 Security Capabilities Benchmark Study

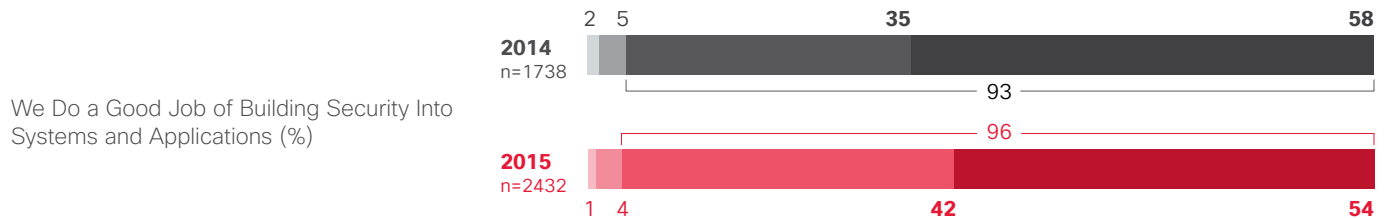
Security professionals also show mixed levels of confidence in terms of their ability to thwart attackers. Fifty-one percent strongly believe they can detect security weaknesses before they become full-blown incidents; only 45 percent are confident in their ability to determine the scope of a network compromise, and to remediate the damage (see Figure 49).

Security professionals also show weaker confidence levels in their capability to defend their networks against attacks. For example, in 2015, fewer professionals strongly believe that they do a good job of building security into procedures for acquiring, developing, and maintaining systems (54 percent in 2015, compared with 58 percent in 2014; see Figure 50). (See [page 76](#) for full list.)

**Figure 50. Lower Confidence in Ability to Build Security into Systems**

Security Policies

Strongly Disagree | Disagree | **Agree** | **Strongly Agree**



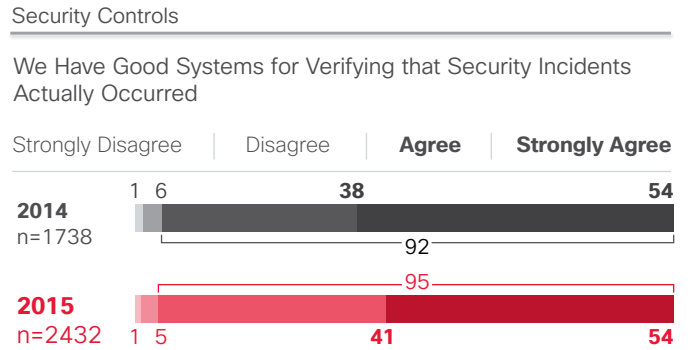
Source: Cisco 2015 Security Capabilities Benchmark Study

SHARE

In some areas, confidence levels in security capabilities are not very high. For example, in 2015, only 54 percent of respondents said they believe they have a good system for verifying that security incidents have actually occurred (see Figure 51). (See [page 77](#) for full list.)

Respondents are also not entirely confident that their systems can scope and contain such compromises. Fifty-six percent said they review and improve security practices regularly, formally, and strategically; 52 percent believe their security technologies are well integrated and work effectively together (see Figure 52). (See [page 79](#) for full list.)

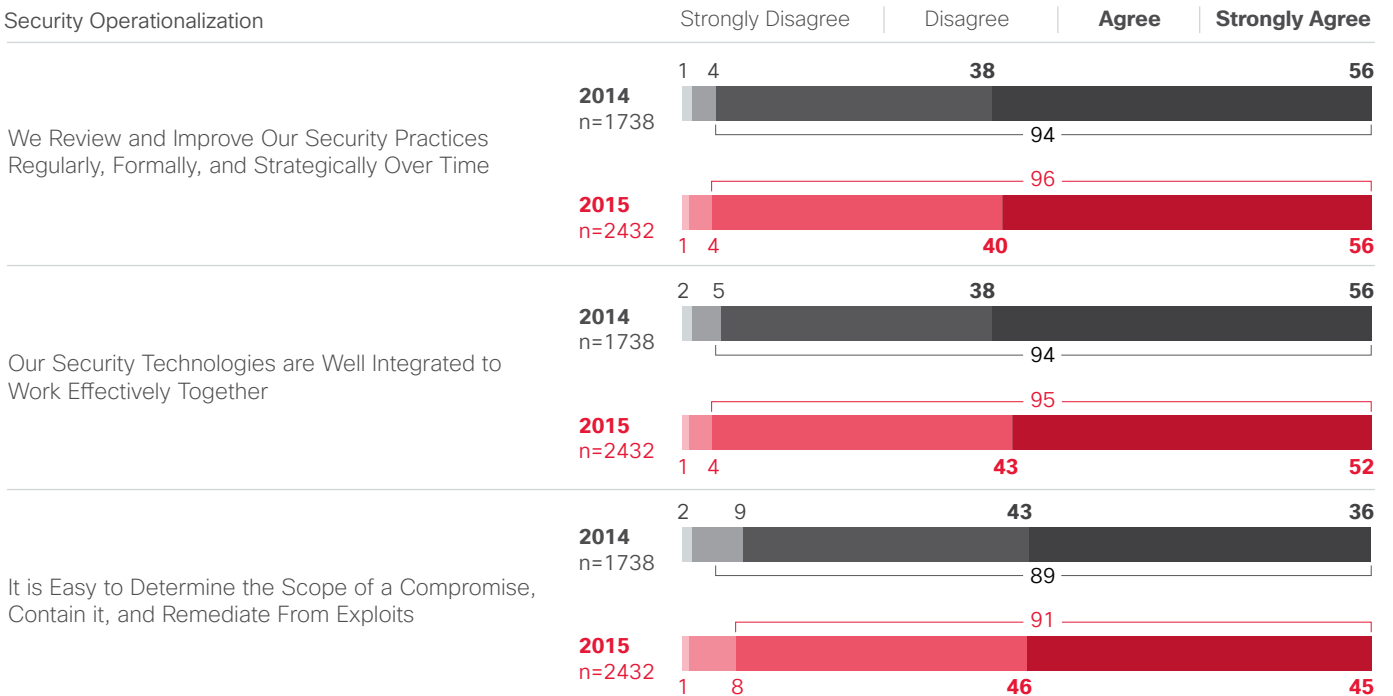
**Figure 51. Enterprises Believe They Have Good Security Controls**



Source: Cisco 2015 Security Capabilities Benchmark Study

SHARE    

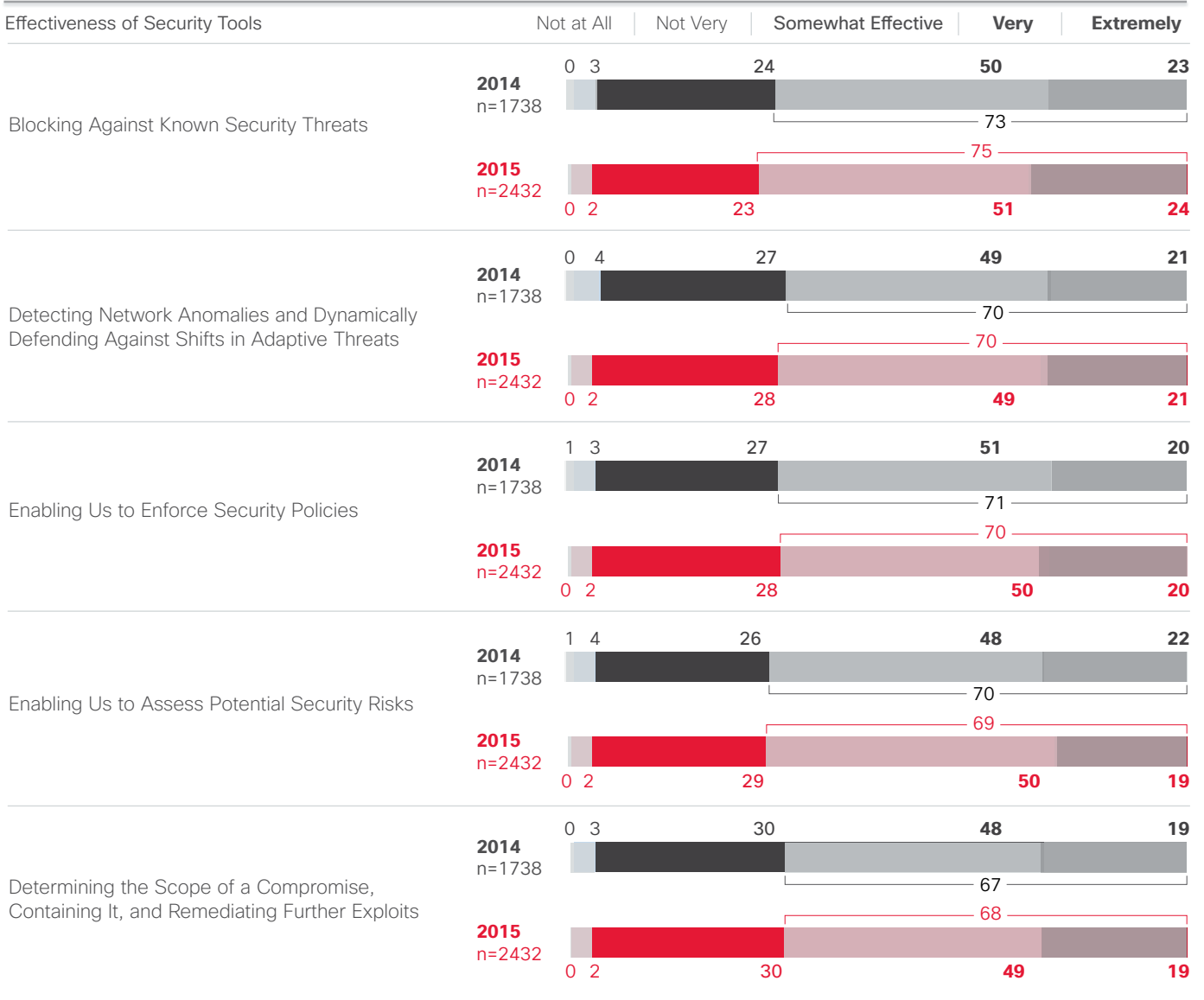
**Figure 52. Enterprises Express Mixed Confidence in Ability to Contain Compromise**



Source: Cisco 2015 Security Capabilities Benchmark Study

**Figure 53. One-Fourth of Enterprises Believe Security Tools Are Only Somewhat Effective**

Similar to Last Year, Over a Quarter Perceive Their Security Tools to be Only “Somewhat” Rather Than “Very” or “Extremely” Effective



Source: Cisco 2015 Security Capabilities Benchmark Study

Similar to the respondents in 2014, more than one-fourth of the security professionals in 2015 said they perceive their security tools to be only somewhat effective (Figure 53).



Public security breaches tend to be a defining moment for organizations. Once they occur, organizations seem to become more aware of the need to prevent future breaches. However, in 2015, fewer security professionals said their organizations had to deal with public security breaches: they made up 53 percent of the professionals in 2014, and 48 percent in 2015 (Figure 54).

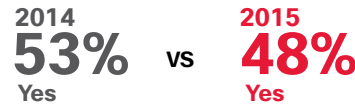
Professionals acknowledge the value that breaches have in terms of delivering a wake-up call about the importance of strengthening security processes: 47 percent of the security professionals affected by public breaches said the breaches resulted in better policies and procedures. For example, 43 percent of the respondents said they increased security training after a public breach, and 42 percent said they increased investments in security defense technologies.

The good news is that organizations that have suffered a public breach are increasingly likely to strengthen their security processes. In 2015, 97 percent of security professionals said they conduct security training at least once a year, a solid increase from 82 percent in 2014 (see Figure 90 on [page 82](#)).

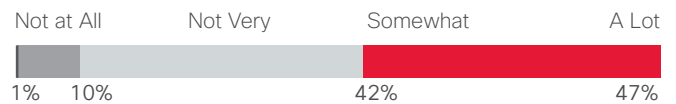
SHARE    

**Figure 54. Public Breaches Can Improve Security**

Has Your Organization Ever Had to Manage Public Scrutiny of a Security Breach? (n=1701) (n=1347)



How Much Did the Breach Drive Improvements in Your Security Threat Defense Policies, Procedures, or Technologies? (n=1134)



Source: Cisco 2015 Security Capabilities Benchmark Study

**Figure 55. More Organizations Conduct Security Training**

In 2015, 43 percent of respondents said they increased security training after a public breach.



Source: Cisco 2015 Security Capabilities Benchmark Study

**MATURITY: BUDGET CONSTRAINTS RANK HIGH AT EVERY LEVEL**

As organizations deploy more sophisticated security practices and policies, their perceptions of their security readiness may shift. The Cisco 2015 Security Capabilities Benchmark Study places survey respondents and their organizations into five maturity categories, based on responses about their security processes (Figure 56). The study examines how different characteristics such as capabilities, industries, and countries may affect maturity levels.

Interestingly, organizations at different maturity levels seem to share some of the obstacles to implementing more sophisticated security processes and tools. Although the exact percentages may vary, the challenge of budget constraints ranks at the top of the list at every level of maturity (Figure 57).

**Figure 56. Maturity Model Ranks Organizations Based on Security Processes**

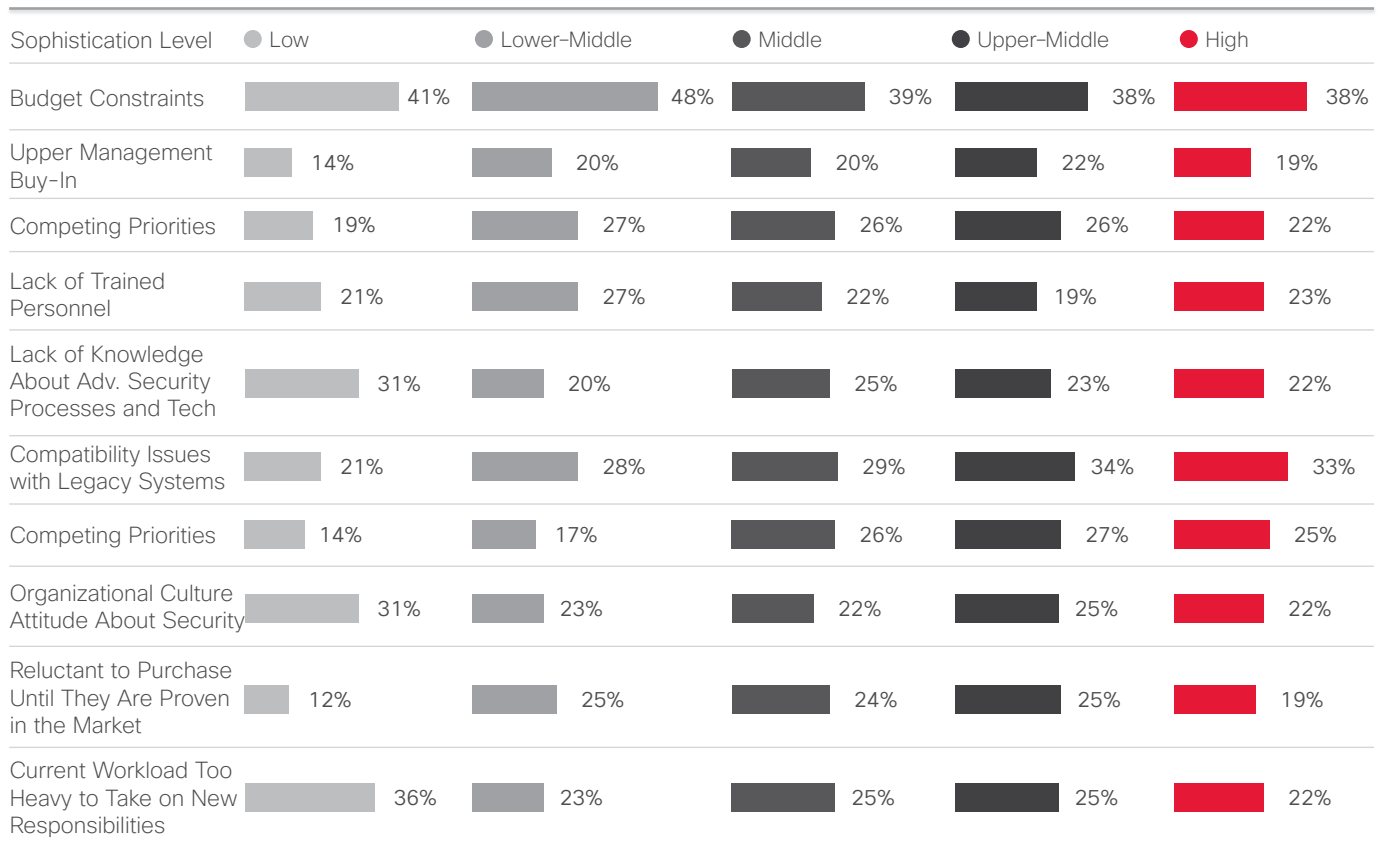
Cisco explored several options for sample segmentation before selecting a five-segment solution based on a series of questions targeting security processes. The five-segment solution maps fairly closely to the Capability Maturity Model Integration (CMMI).

|                        | Level   | 5-Segment-Based Solution |
|------------------------|---|--------------------------|
| Optimizing             | 1 Focus Is on Process Improvement                               | High                     |
| Quantitatively Managed | 2 Processes Quantitatively Measured and Controlled              | Upper-Middle             |
| Defined                | 3 Processes Characterized for the Organization; Often Proactive | Middle                   |
| Repeatable             | 4 Processes Characterized for Projects; Often Reactive          | Lower-Middle             |
| Initial                | 5 Processes Are Ad Hoc, Unpredictable                           | Low                      |

Source: Cisco 2015 Security Capabilities Benchmark Study

**Figure 57. Obstacles to Adopting Better Security Not Affected by Maturity Level**

Which of the Following Do You Consider the Biggest Obstacles to Adopting Advanced Security Processes and Technology?

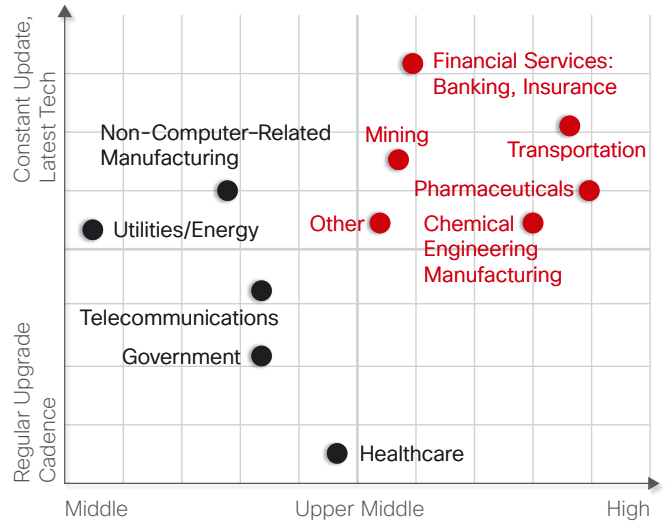


Source: Cisco 2015 Security Capabilities Benchmark Study

The chart to the right maps the quality of the security infrastructure and maturity levels of various industries. It is based on survey respondents' perceptions of their security processes. The industries that appear in the upper-right quadrant show the highest levels of maturity as well as infrastructure quality.

The chart below shows placement in Cisco's maturity levels by industry. In 2015, nearly half of transportation and pharmaceutical organizations surveyed are in the high-maturity segment. Telecommunications and utilities are less likely to be in the high-maturity segment in 2015, compared to 2014. The results are based on survey respondents' perceptions of their security processes.

**Figure 58. Gauging Security Maturity by Infrastructure and Industry**



Source: Cisco 2015 Security Capabilities Benchmark Study

SHARE

**Figure 59. Maturity Levels by Industry**

Segment Distribution by Industry

| Sophistication Level               | Low | Lower-Middle | Middle | Upper-Middle | High |
|------------------------------------|-----|--------------|--------|--------------|------|
| Utilities/Energy                   | 1%  | 15%          | 28%    | 32%          | 23%  |
| Transportation                     | 1%  | 5%           | 28%    | 20%          | 46%  |
| Telecommunications                 | 2%  | 11%          | 26%    | 28%          | 33%  |
| Pharmaceutical                     | 2%  | 3%           | 30%    | 21%          | 44%  |
| Non-Computer-Related Manufacturing | 1%  | 10%          | 34%    | 22%          | 32%  |
| Healthcare                         | 1%  | 10%          | 30%    | 22%          | 37%  |
| Government                         | 3%  | 10%          | 28%    | 25%          | 34%  |
| Financial Services                 | 1%  | 10%          | 26%    | 26%          | 38%  |
| Chemical Engineering               | 1%  | 6%           | 21%    | 33%          | 39%  |

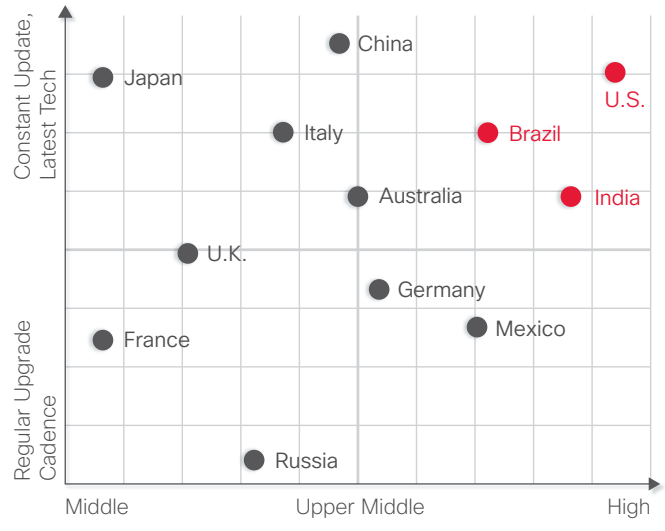
Source: Cisco 2015 Security Capabilities Benchmark Study

The chart to the right maps the quality of the security infrastructure, and maturity levels, of various countries. The countries that appear in the upper-right quadrant show the highest levels of maturity as well as infrastructure quality. It's important to note that these findings are based on security professionals' perceptions of their security readiness.

The chart below shows placement in Cisco's maturity levels by country. The results are based on survey respondents' perceptions of their security processes.

SHARE    

**Figure 60. Gauging Security Maturity by Infrastructure and Country**



Source: Cisco 2015 Security Capabilities Benchmark Study

**Figure 61. Maturity Levels by Country**

| Segment Distribution by Country | 2014 (n=1637) |              |        |              |      | 2015 (n=2401) |              |        |              |      |
|---------------------------------|---------------|--------------|--------|--------------|------|---------------|--------------|--------|--------------|------|
|                                 | Low           | Lower-Middle | Middle | Upper-Middle | High | Low           | Lower-Middle | Middle | Upper-Middle | High |
| United States                   | 3%            | 2%           | 10%    | 4%           | 27%  | 22%           | 16%          | 27%    | 44%          | 45%  |
| Brazil                          | 2%            | 1%           | 5%     | 9%           | 24%  | 24%           | 35%          | 26%    | 34%          | 40%  |
| Germany                         | 1%            | 1%           | 4%     | 12%          | 27%  | 24%           | 25%          | 24%    | 43%          | 39%  |
| Italy                           | 1%            | 4%           | 23%    | 3%           | 13%  | 36%           | 25%          | 23%    | 38%          | 34%  |
| United Kingdom                  | 8%            | 0%           | 8%     | 14%          | 25%  | 32%           | 18%          | 22%    | 41%          | 32%  |
| Australia                       | 9%            | 1%           | 7%     | 5%           | 19%  | 29%           | 35%          | 36%    | 30%          | 29%  |
| China                           | 0%            | 0%           | 3%     | 6%           | 32%  | 37%           | 29%          | 25%    | 36%          | 32%  |
| India                           | 7%            | 1%           | 3%     | 4%           | 20%  | 21%           | 16%          | 34%    | 54%          | 40%  |
| Japan                           | 7%            | 2%           | 15%    | 16%          | 14%  | 34%           | 40%          | 16%    | 32%          | 32%  |
| Mexico                          | 6%            |              | 8%     |              | 20%  |               | 16%          |        | 50%          |      |
| Russia                          | 1%            |              | 14%    |              | 27%  |               | 26%          |        | 32%          |      |
| France                          | 1%            |              | 15%    |              | 35%  |               | 20%          |        | 29%          |      |

Source: Cisco 2015 Security Capabilities Benchmark Study

**RECOMMENDATIONS: RESPONDING TO THE REALITY CHECK**

As our Security Benchmark Capabilities Study shows, reality has set in for security professionals. Security professionals' confidence in their readiness to block attackers is wavering. However, the reality checks provided by high-profile exploits have had a positive effect on the industry, judging from the uptick in security training and formal policy development. In addition, the more frequent outsourcing of audits and incident response services indicates that defenders are searching for expert help.

Enterprises should continue to raise their awareness of their security preparedness, and security professionals must champion the growth of budgetary outlays to support technology and personnel. In addition, confidence will rise when security practitioners deploy tools that can not only detect threats, but also contain their impact and boost understanding of ways to prevent future attacks.

# A Look Forward

# A Look Forward

Cisco geopolitical experts offer insight on the changing landscape for Internet governance, including changes in data transfer legislation and the debate over the use of encryption. Also featured in this section are select findings from two Cisco studies. One examines executives' concerns about cybersecurity. The other focuses on IT decision-makers' perceptions about security risk and trustworthiness. We also give an overview of the value of an integrated threat defense architecture and provide an update on Cisco's progress in reducing time to detection (TTD).

## Geopolitical Perspective: Uncertainty in the Internet Governance Landscape

In the post-Edward Snowden era, the geopolitical landscape for Internet governance has changed dramatically. There is now pervasive uncertainty surrounding the free flow of information across borders. The landmark case brought by the Austrian privacy activist Max Schrems against the social networking giant Facebook had perhaps the biggest impact, leading the Court of Justice of the European Union (CJEU) to overturn the U.S. Safe Harbor agreement on October 6, 2015.<sup>7</sup>

Consequently, companies are now forced to rely on mechanisms and legal safeguards other than Safe Harbor when transferring data out of the EU to the United States—which are, in turn, subject to investigation. Data companies are still trying to assess the fallout from this move. And while EU and U.S. authorities have been working on a replacement for Safe Harbor for the last two years, there are concerns about the anticipated new mechanism. It could either fail to materialize by the January 2016 deadline

or, perhaps more likely, fail to restore market confidence if it does not fully address the concerns of the CJEU and proves once more to be at risk of invalidation.<sup>8</sup>

Data protection experts expect Safe Harbor 2.0 to be no less controversial than its predecessor. It may even follow the same path by being challenged in court and also declared invalid.<sup>9</sup>

End-to-end encryption—how it benefits consumers and organizations, and the challenges it creates for law enforcement in their investigations of criminal and terrorist activity—will also be a topic of much debate between governments and industry in the year ahead. The terrorist attacks in Paris in November 2015 have some policymakers pushing even harder to give investigators the ability to access the content of encrypted communications.<sup>10</sup> This could give additional momentum to the development of Safe Harbor 2.0, as civil liberties concerns take a back seat to security concerns.

<sup>7</sup> "The Court of Justice declares that the Commission's U.S. Safe Harbour Decision is invalid," CJEU, October 6, 2015: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf>.

<sup>8</sup> "Safe Harbor 2.0 framework begins to capsize as January deadline nears," by Glyn Moody, *Ars Technica*, November 16, 2015: <http://arstechnica.com/tech-policy/2015/11/safe-harbour-2-0-framework-begins-to-capsize-as-january-deadline-nears/>.

<sup>9</sup> "Safe Harbor 2.0 framework begins to capsize as January deadline nears," by Glyn Moody, *Ars Technica*, November 16, 2015: <http://arstechnica.com/tech-policy/2015/11/safe-harbour-2-0-framework-begins-to-capsize-as-january-deadline-nears/>.

<sup>10</sup> "Paris Attacks Fan Encryption Debate," by Danny Yadron, Alistair Barr, and Daisuke Wakabayashi, *The Wall Street Journal*, November 19, 2015: <http://www.wsj.com/articles/paris-attacks-fan-encryption-debate-1447987407>.



Amid such uncertainty, what should organizations ask data providers in order to make sure that their business is in compliance with data transfer regulations? In the short term, they should certainly seek assurances from vendors that they are using EU Model Contract Clauses or Binding Corporate Rules—and not just Safe Harbor—when transferring data out of the EU.

Another major geopolitical issue that organizations should monitor relates to vulnerabilities and exploits. Some governments are expressing great concern about the rise of a market for unpatched vulnerabilities—so-called weaponized software. Such tools are vital to the security research community as it looks for ways to protect networks around the globe. But in the wrong hands, particularly those of repressive regimes, this technology, intended for good, could be used for financial crime, to steal national and commercial secrets, suppress political dissent, or disrupt critical infrastructure.

How to restrict access to unpatched vulnerabilities without tying the hands of those conducting vital research is an issue that governments will clearly wrestle with in the coming months and years. As governments attempt to tackle this thorny problem, they need to carefully assess how their policymaking decisions affect security. For example, the uncertainty about laws that govern the transmission of information about unpublished vulnerabilities could chill the advancement of security threat research, or encourage the publication of vulnerabilities before vendors have an opportunity to patch them. Any approach to resolving this uncertainty should be compatible across the globe.

## Cybersecurity Concerns Weigh on Minds of Executives

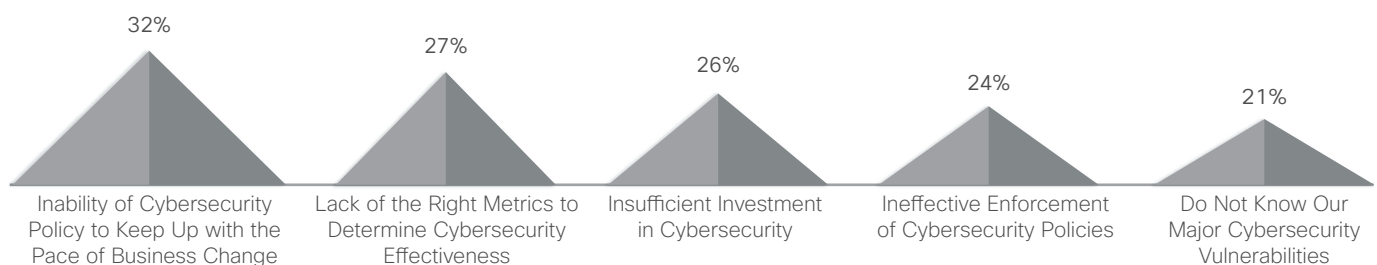
Obviously, in-depth security can help enterprises avoid calamitous breaches and attacks. But can it help improve the chances of a company's success? According to an October 2015 Cisco study of finance and line-of-business executives regarding cybersecurity's role in business and digital strategy, enterprise executives understand that protecting their businesses from threats may dictate whether they succeed or fail. As organizations become more digitized, growth will depend on their ability to protect the digital platform.

As the survey shows, cybersecurity is a growing concern for executives: 48 percent said they were very concerned, and 39 percent said they were moderately concerned, about cybersecurity breaches. This concern is on the rise; 41 percent said they were much more concerned about security breaches than they were three years ago, and 42 percent said they were a little more concerned than before.

Business leaders are also anticipating that investors and regulators will ask tougher questions about security processes, just as they ask questions about other business functions. Ninety-two percent of the respondents agreed that regulators and investors will expect companies to provide more information on cybersecurity risk exposure in the future.

Enterprises also appear to have a keen sense of the cybersecurity challenges they face. The inability of cybersecurity policies to keep pace with business change was the most common challenge cited, followed by the lack of metrics to determine security effectiveness (Figure 62).

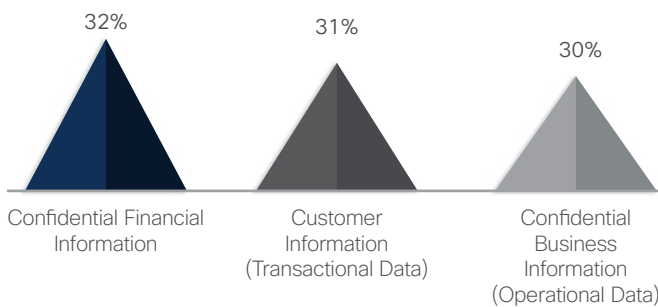
**Figure 62.** Enterprises Face Tough Cybersecurity Challenges



Source: Cisco Security Research

About a third of executives are also worried about their ability to safeguard critical data. When asked to name the types of information that are most difficult to protect, 32 percent selected “confidential financial information.” Respondents named “customer information” and “confidential business information” as the next two most difficult types of data to protect (see Figure 63).

**Figure 63.** Executives Concerned About Securing Critical Data



Source: Cisco Security Research

### Trustworthiness Study: Shining a Light on the Risks and Challenges for Enterprises

The relentless rise in information security breaches underscores the deep need for enterprises to trust that their systems, data, business partners, customers, and citizens are safe. We are seeing trust become a major factor for businesses selecting IT and networking infrastructure. In fact, many are now requiring that security and trustworthiness be integrated throughout the product lifecycle of the solutions that comprise their infrastructure.

In October 2015, Cisco conducted a study to assess IT decision-makers’ perceptions of their security risks and challenges and to determine the role that IT vendor trustworthiness plays in their IT investments. We surveyed both information security and non-information-security decision-makers at organizations in several countries. (See the **Appendix** for more details on the Security Risk and Trustworthiness Study, including our methodology.)

### FOLLOWING ARE SELECT FINDINGS FROM OUR RESEARCH:

We found that 65 percent of the respondents think that their organization faces a significant level of security risk—namely, from the use of mobility, IT security, and cloud-based solutions in the enterprise (Figure 64).

**Figure 64.** Perceptions of Security Risk



Enterprises believe the following areas of their organization’s infrastructure are at a high risk for a security breach:



Source: Security Risk and Trustworthiness Study, Cisco

SHARE

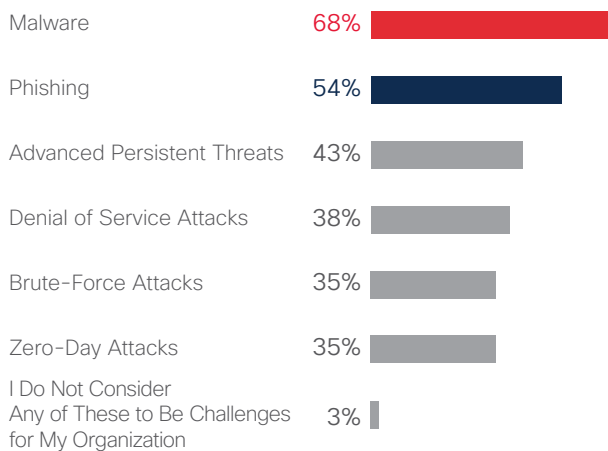
Sixty-eight percent of the respondents to our study identified malware as the top external security challenge that their organization faces. Phishing and advanced persistent threats rounded out the top three responses—at 54 percent and 43 percent, respectively (see Figure 65).

As for internal security challenges (see Figure 66), more than half (54 percent) of our respondents cited malicious software downloads as the top threat, followed by internal security breaches by employees (47 percent), and hardware and software vulnerabilities (46 percent).

We also found that most enterprises (92 percent) employ a dedicated security team within their organization. Eighty-eight percent of respondents reported that they have a formal, organization-wide security strategy that is renewed regularly. However, only 59 percent have standardized policies and procedures in place to validate IT vendor trustworthiness (see Figure 67).

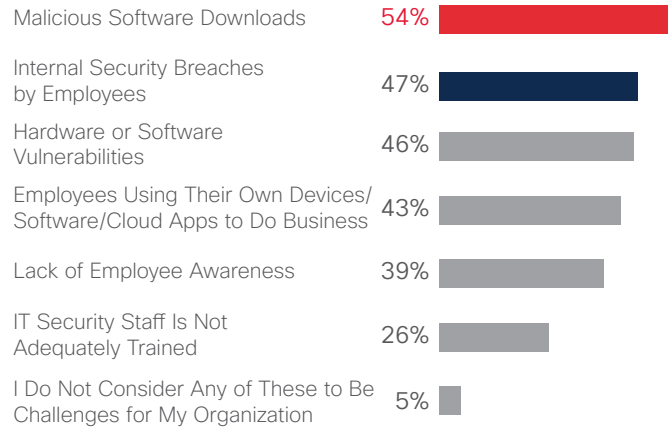
In addition, about half (49 percent) of large enterprise organizations keep their security infrastructure up to date with the most current technologies, and most others upgrade their infrastructure regularly. Very few wait to upgrade until the technology they use is obsolete, according to our study.

**Figure 65. External Challenges Faced (Total Respondents)**



Source: Security Risk and Trustworthiness Study, Cisco

**Figure 66. Internal Security Challenges Faced (Total Respondents)**



Source: Security Risk and Trustworthiness Study, Cisco

**Figure 67. Most Large Enterprises Have a Dedicated Security Team In-House**



Source: Security Risk and Trustworthiness Study, Cisco

SHARE    

**! How Vendors Can Demonstrate Trustworthiness**

In today’s threat-centric landscape, confidence in a vendor’s processes, policies, technologies, and people—and the ability to verify them—are foundational to building a lasting, trusted relationship between vendors and enterprises.

Technology vendors demonstrate trustworthiness by:

- Building security into their solutions and the value chain from inception
- Having and following policies and processes in place that reduce risk
- Creating a security-aware culture
- Responding to breaches quickly and transparently
- Providing rapid remediation and constant vigilance after an incident

Upgrading infrastructure is good practice, of course. Organizations of all sizes need to deploy a secure, trustworthy infrastructure in which security is designed into all facets of the network. However, they can also help to shrink the attack surface by fostering an open, security-aware culture.

Building this culture requires that organizations implement consistent, enterprise-wide policies and processes that ensure security is embedded into every aspect of the business. They must then work to extend this security-centric mindset to their ecosystem of partners and suppliers, and continually work to demonstrate transparency and accountability with customers, partners, and other stakeholders.

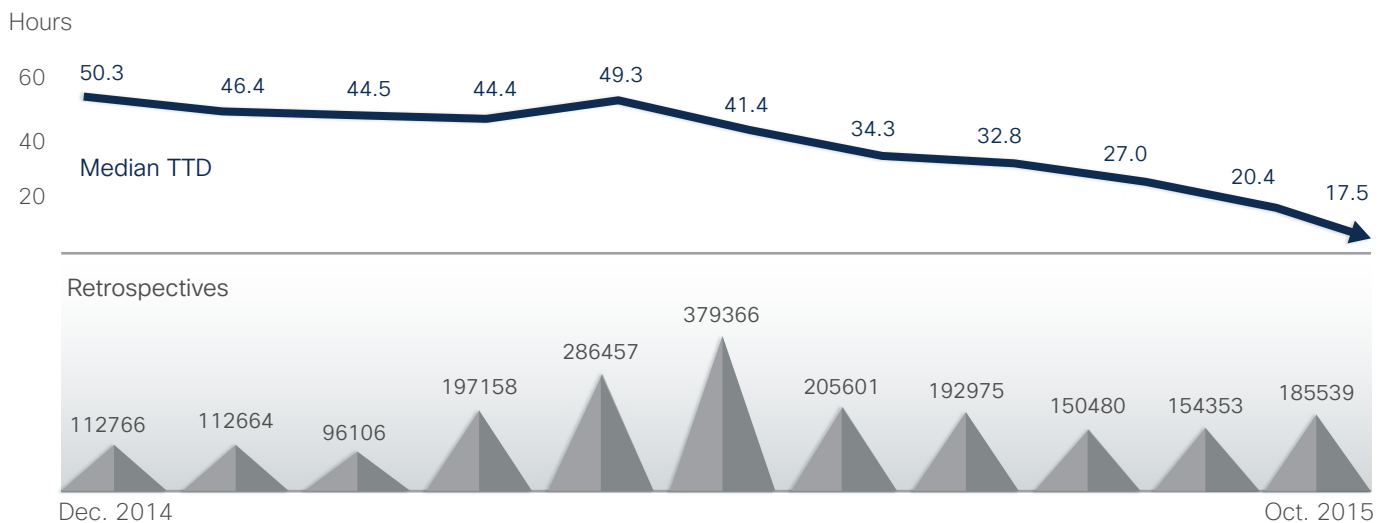
**Time to Detection: The Race to Keep Narrowing the Window**

We define “time to detection,” or TTD, as the window of time between the first observation of an unknown file 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.

The “retrospectives” category in Figure 68 shows the number of files that Cisco initially categorized as “unknown” and later converted to “known bad.”

As reported in the Cisco 2015 Midyear Security Report, the median TTD was about two days (50 hours).

**Figure 68.** Time to Detection, December 2014–October 2015



Source: Cisco Security Research

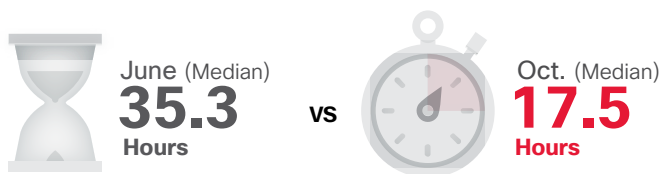
From January to March, the median TTD was roughly the same—between 44 and 46 hours, but with a slight trend downward. In April, it had edged up slightly to 49 hours. However, by the end of May, TTD for Cisco had decreased to about 41 hours.

**!** Since that time, the median TTD has been on a rapid decline. By October, Cisco had reduced the median TTD to about 17 hours—less than one day. This far outpaces the current industry estimate for TTD (100 to 200 days). The speed is due to the inclusion of more detail about how short-lived infections are mitigated.

The industrialization of hacking and the greater use of commodity malware have played an important role in our ability to narrow the window on TTD. As soon as a threat becomes industrialized, it becomes more widespread and thus easier to detect.

However, we also suggest that the combination of sophisticated threat defenses and close collaboration among skilled security researchers has been perhaps even more critical to our ability to consistently and significantly reduce the median TTD over the course of 2015.

**Figure 69.** Time to Detection Comparison, December 2014 to October 2015



Source: Cisco Security Research

SHARE    

The TTD comparison in Figure 69 shows that many threats in June were being caught within around 35.3 hours. By September, more threats were being stopped within around 17.5 hours. Again, we attribute the reduction in median TTD partly to a faster identification of commodity malware, such as Cryptowall 3.0, Upatre, and Dyre. The integration of new technologies, such as those from ThreatGRID, a Cisco company, is another factor.

However, even with the narrowed time window for TTD, some threats remain harder to detect than others. Downloaders that target Microsoft Word users are typically the easiest to detect (<20 hours). Adware and browser injections are among the most difficult threats to detect (<200 hours).

One reason the latter threats are so challenging to detect is that they are typically designated as a lower priority by security teams, and are therefore often overlooked in the race to deflect adversaries' onslaught of zero-day attacks (see "Browser Infections: Widespread—and a Major Source of Data Leakage" on [page 16](#)).

Figure 70 provides an overview of the types of threats that usually come to light within 100 days.

**Figure 70.** Tag Cloud for 100 Days



Source: Cisco Security Research

## The Six Tenets of Integrated Threat Defense

In the Cisco 2015 Midyear Security Report, Cisco security experts asserted that the need for adaptive, integrated solutions will lead to major changes in the security industry within the next five years. The outcomes will be industry consolidation and a unified movement toward a scalable, integrated threat defense architecture. Such an architecture will provide visibility, control, intelligence, and context across many solutions.

This “detection and response” framework will make possible a faster response to both known and emerging threats. At the core of this new architecture will be a visibility platform that delivers full contextual awareness and is continuously updated to assess threats, correlate local and global intelligence, and optimize defenses. The intent of this platform is to build a foundation that all vendors can operate on and contribute to. With visibility, there is more control, which leads to better protection across more threat vectors and the ability to thwart more attacks.

Below, we present six tenets of integrated threat defense to help organizations, and their security vendors, better understand the intent and potential benefits of this architecture:

### 1. **A richer network and security architecture is needed to address the growing volume and sophistication of threat actors.**

For the past 25 years, the traditional model for security has been “See a problem, buy a box.” But these solutions, often a collection of technologies from many different security vendors, don’t talk to each other in any meaningful way. They produce information and intelligence about security events, which are integrated into an event platform and then analyzed by security personnel.

An integrated threat defense architecture is a detection and response framework that offers more capabilities and supports faster threat responses by collecting more information from deployed infrastructure in an automated, efficient manner. The framework observes the security environment more intelligently. Instead of just alerting security teams to suspicious events and policy violations, it can paint a clear picture of the network and what’s happening on it to help inform better decision-making around security.

### 2. **Best-in-class technology alone cannot deal with the current—or future—threat landscape; it just adds to the complexity of the networked environment.**

Organizations invest in “best in class” security technologies, but how do they know if those solutions are really working? The headlines about major security breaches over the past year are evidence that many security technologies aren’t working well. And when they fail, they fail badly.

A proliferation of security vendors offering best-in-class solutions doesn’t help to improve the security environment unless those vendors offer radically different—not just slightly different—solutions from those of their competitors. But today, there are no stark differences in many offerings from leading vendors in most core areas of security.

### 3. **More encrypted traffic will require an integrated threat defense that can converge on encrypted malicious activity that renders particular point products ineffective.**

As discussed in this report, encrypted web traffic is on the rise. There are good reasons for using encryption, of course, but encryption also makes it challenging for security teams to track threats.

The answer to the encryption “problem” is to have more visibility into what’s happening on devices or networks. Integrated security platforms can help to provide this.

### 4. **Open APIs are crucial to an integrated threat defense architecture.**

Multivendor environments need a common platform that provides greater visibility, context, and control. Building a front-end integration platform can support better automation and bring better awareness into the security products themselves.

### 5. **An integrated threat defense architecture requires less gear and software to install and manage.**

Security vendors should strive to offer platforms that are as feature-rich as possible and that offer extensive functionality on one platform. This will help to reduce the complexity and fragmentation in the security environment that create too many opportunities for easy access and concealment for adversaries.

**6. The automation and coordination aspects of an integrated threat defense help to reduce time to detection, containment, and remediation.**

Reducing false positives helps security teams focus on what matters most. Contextualization supports a front-line analysis of events underway, helps teams assess whether those events require immediate attention, and can ultimately produce automated responses and deeper analytics.

## Power in Numbers: The Value of Industry Collaboration

Industry collaboration is essential not only to developing a future architecture for integrated threat defense that will enable faster threat response, but also for keeping pace today with a global community of increasingly bold, innovative, and persistent threat actors. Adversaries are becoming only more adept at deploying hard-to-detect and highly profitable campaigns. Many now employ legitimate assets in the infrastructure to support their campaigns—and with great success.

Given this landscape, it is not surprising that the defenders surveyed for our Cisco 2015 Security Capabilities Benchmark Study are less confident in their ability to help secure their organization. We suggest that defenders consider the powerful impact that proactive and continuous industry collaboration can have in bringing cybercriminal activity to light, undermining adversaries' ability to generate revenue, and reducing the opportunity to launch future attacks.

As discussed in depth earlier in this report (see “Featured Stories,” starting on [page 10](#)), collaboration between a Cisco Partner Contributor and within our Cisco Collective Security Intelligence (CSI) ecosystem, and cooperation with service providers, were significant factors in Cisco's ability to uncover, verify, and sideline global operations involving the Angler exploit kit, and to weaken one of the largest DDoS botnets our researchers have ever observed, SSHPsychos.



# About Cisco

# 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 at Cisco. 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 products and services 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](http://www.cisco.com/go/security).

## Contributors to the Cisco 2016 Annual Security Report

### 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 comprised 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.

### ADVANCED SERVICES CLOUD AND IT TRANSFORMATION, OPTIMIZATION TEAM

The team provides recommendations and optimizes networks, data center, and cloud solutions for the largest service providers and enterprises around the world. This consulting offer focuses on maximizing the availability, performance, and security of clients' critical solutions. The optimization service is delivered to more than 75 percent of Fortune 500 companies.

### ACTIVE THREAT ANALYTICS TEAM

The Cisco Active Threat Analytics (ATA) team helps organizations defend against known intrusions, zero-day attacks, and advanced persistent threats by taking advantage of advanced big data technologies. This fully managed service is delivered by our security experts and our global network of security operations centers. It provides constant vigilance and on-demand analysis 24 hours a day, seven days a week.

### CISCO THOUGHT LEADERSHIP ORGANIZATION

The Cisco Thought Leadership Organization illuminates the global opportunities, market transitions, and key solutions that transform organizations, industries, and experiences. The organization provides an incisive and predictive lens into what firms can expect in a rapidly changing world—and how they can best compete. Much of the team's thought leadership focuses on helping organizations become digital by bridging physical and virtual environments—seamlessly and securely—to innovate faster and achieve their desired business outcomes.

### 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.

### 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 comprised 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.

### INTELLISHIELD TEAM

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

### LANCOPE

Lancope, a Cisco company, is a leading provider of network visibility and security intelligence to protect enterprises against today's top threats. By analyzing NetFlow, IPFIX, and other types of network telemetry, Lancope's StealthWatch® System delivers Context-Aware Security Analytics to quickly detect a wide range of attacks from APTs and DDoS to zero-day malware and insider threats. Combining continuous lateral monitoring across enterprise networks with user, device, and application awareness, Lancope accelerates incident response, improves forensic investigations, and reduces enterprise risk.

### OPENDNS

OpenDNS, a Cisco company, is the world's largest cloud-delivered security platform, serving more than 65 million daily users spread across more than 160 countries. OpenDNS Labs is the security research team at OpenDNS that supports the security platform. For more information visit [www.opendns.com](http://www.opendns.com) or <https://labs.opendns.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 cyber 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>.

## SECURITY RESEARCH AND OPERATIONS (SR&O)

Security Research & 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 innovates to deliver 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 Partner Contributor

### LEVEL 3 THREAT RESEARCH LABS

Level 3 Communications is a premier global communications provider headquartered in Broomfield, Colorado, that provides communications services to enterprise, government, and carrier customers. Anchored by extensive fiber networks on three continents and connected by undersea facilities, our global services platform features deep metro assets reaching more than 500 markets in more than 60 countries. Level 3's network provides an expansive view of the global threat landscape.

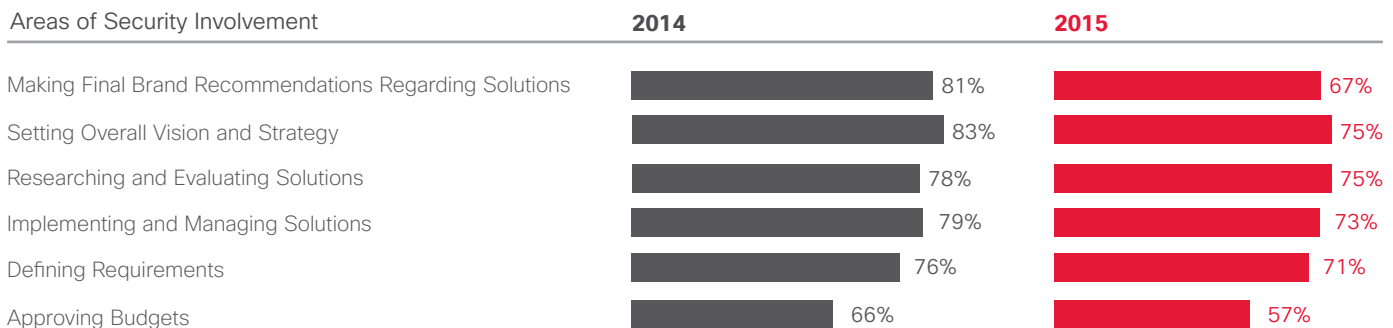
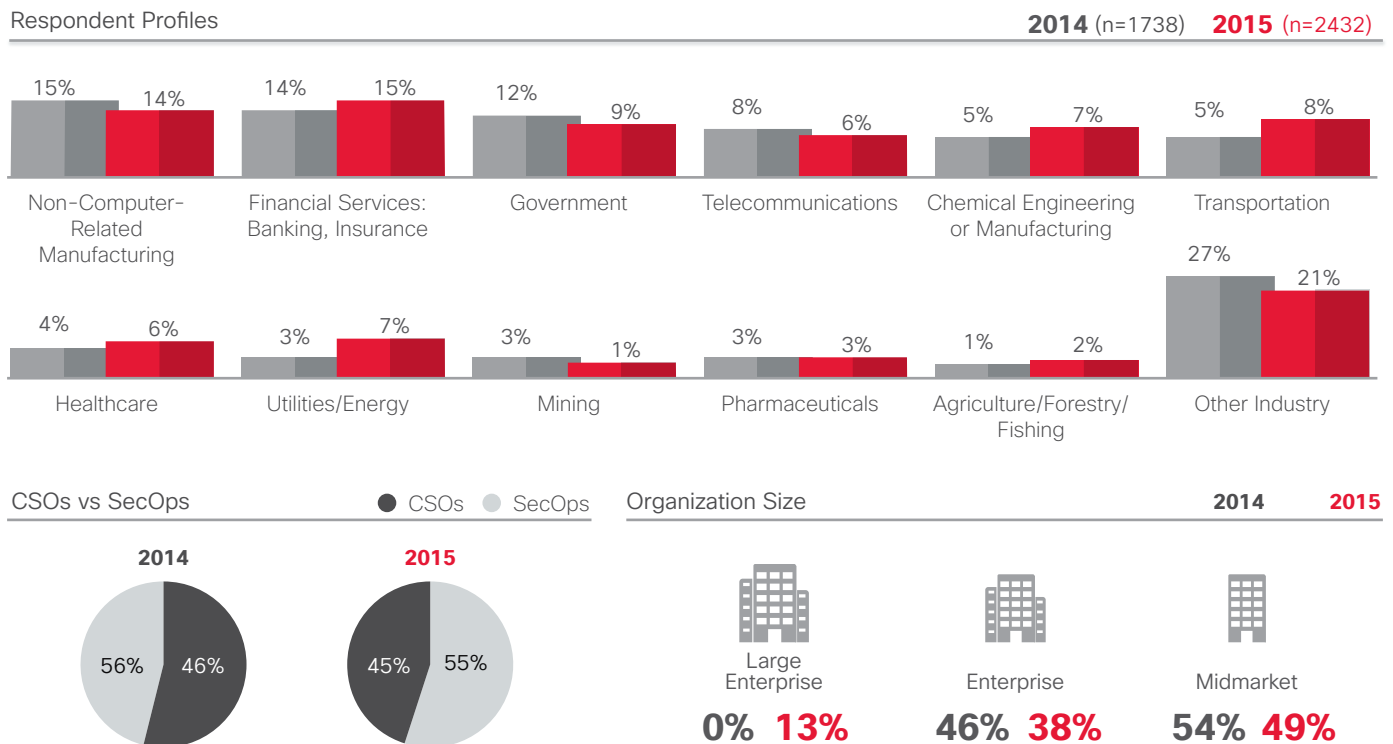
Level 3 Threat Research Labs is the security group that proactively analyzes the global threat landscape and correlates information across internal and external sources to help protect Level 3 customers, its network, and the public Internet. The group regularly partners with industry leaders, such as Cisco Talos, to help research and mitigate threats.

# Appendix

# Appendix

## Cisco's 2015 Security Capabilities Benchmark Study: Respondent Profile and Resources

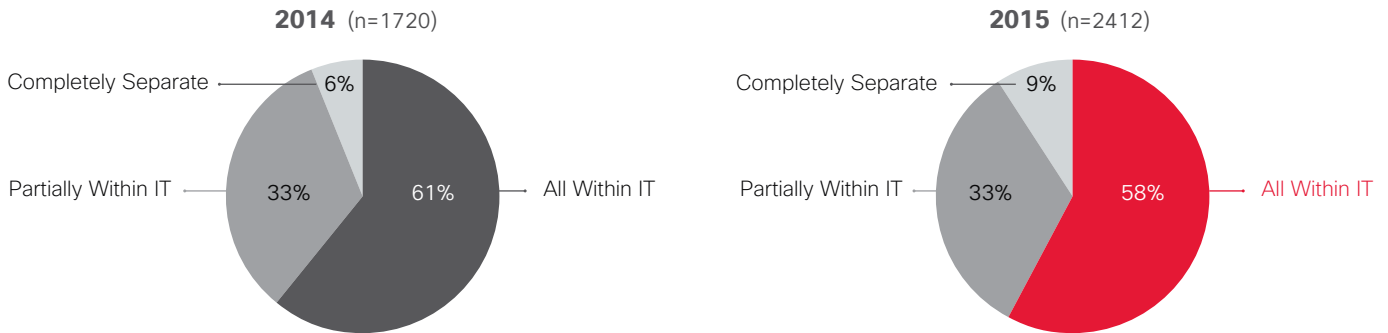
Figure 71. Respondent Profiles



Source: Cisco 2015 Security Capabilities Benchmark Study

**Figure 72.** Although Only 9% Have a Security Budget That’s Separate From the IT Budget, This Has Increased Significantly Since 2014

Is the Security Budget Part of the IT Budget? (IT Department Members)



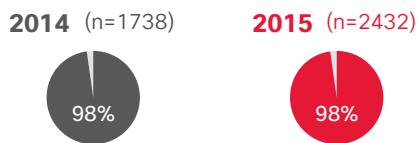
Source: Cisco 2015 Security Capabilities Benchmark Study

**Figure 73.** Job Titles: Respondents and Their Managers

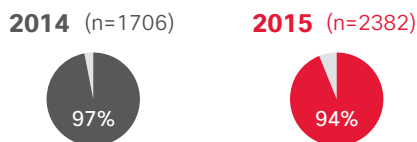
Members of the IT Department



Department or Team Dedicated to Security



Members of a Security Team



Job Title























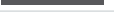


















Manager’s Job Title

|                                 |     |                           |     |
|---------------------------------|-----|---------------------------|-----|
| Chief Security Officer          | 22% | Chief Executive Officer   | 34% |
| Chief Technology Officer        | 18% | President/Owner           | 18% |
| Director or Manager of IT       | 16% | Chief Security Officer    | 6%  |
| Chief Information Officer       | 13% | Chief Information Officer | 6%  |
| Director of Security Operations | 7%  | Chief Technology Officer  | 6%  |
| VP of IT Security               | 5%  | Director or Manager of IT | 4%  |
| Risk and Compliance Officer     | 4%  | VP of IT Security         | 4%  |
| Security Operations Manager     | 4%  | VP of IT                  | 2%  |
| Security Architect              | 4%  | Executive Board           | 2%  |
| VP of IT                        | 3%  | Chief Operations Officer  | 1%  |
| Chief Operations Officer        | 3%  | Chief Financial Officer   | 1%  |
| Another Title                   | 2%  | Another Title             | 0%  |

Source: Cisco 2015 Security Capabilities Benchmark Study



**Figure 74. Firewall Is the Most Common Security Threat Defense Tool Used; Fewer Security Threat Defenses Are Being Administered Through Cloud-Based Services in 2015 Compared to 2014**

| Security Threat Defenses Used by Organization           | 2014 (n=1738)   |     | 2015 (n=2432)  |     | Defenses Administered Through Cloud-Based Services (Security Respondents Who Use Security Threat Defenses) |               |
|---|---|-----|--|-----|--|---------------|
|   |   |     |  |     | 2014 (n=1646)  | 2015 (n=2268) |
| Firewall*   | N/A   |     |    | 65% |  | 31%           |
| Data Loss Prevention                                    |    | 55% |    | 56% |  |               |
| Authentication  |    | 52% |    | 53% |  |               |
| Encryption/Privacy/Data Protection                      |    | 53% |    | 53% |  |               |
| Email/Messaging Security                                |    | 56% |    | 52% | 37%  | 34%           |
| Web Security  |    | 59% |    | 51% | 37%  | 31%           |
| Endpoint Protection/Anti-Malware                        |    | 49% |    | 49% | 25%  | 25%           |
| Access Control/Authorization                            |    | 53% |    | 48% |  |               |
| Identity Administration/User Provisioning               |    | 45% |    | 45% |  |               |
| Intrusion Prevention*                                   | N/A   |     |    | 44% |  | 20%           |
| Mobility Security                                       |    | 51% |    | 44% | 28%  | 24%           |
| Secured Wireless  |  | 50% |  | 41% | 26%  | 19%           |
| Vulnerability Scanning                                  |  | 48% |  | 41% | 25%  | 21%           |
| VPN   |  | 48% |  | 40% | 26%  | 21%           |
| Security Information and Event Management               |  | 43% |  | 38% |  |               |
| DDoS Defense  |  | 36% |  | 37% |  |               |
| Penetration Testing                                     |  | 38% |  | 34% | 20%  | 17%           |
| Patching and Configuration                              |  | 39% |  | 32% |  |               |
| Network Forensics                                       |  | 42% |  | 31% |  |               |
| Endpoint Forensics                                      |  | 31% |  | 26% |  |               |
| Network, Security, Firewalls, and Intrusion Prevention* |  | 60% | N/A  |     | 35%  |               |
| None of the Above                                       |  | 1%  |  | 1%  | 13%  | 11%           |

\*Firewall and intrusion prevention were one code in 2014: "Network security, firewalls, and intrusion prevention."

Source: Cisco 2015 Security Capabilities Benchmark Study

## Outsourcing

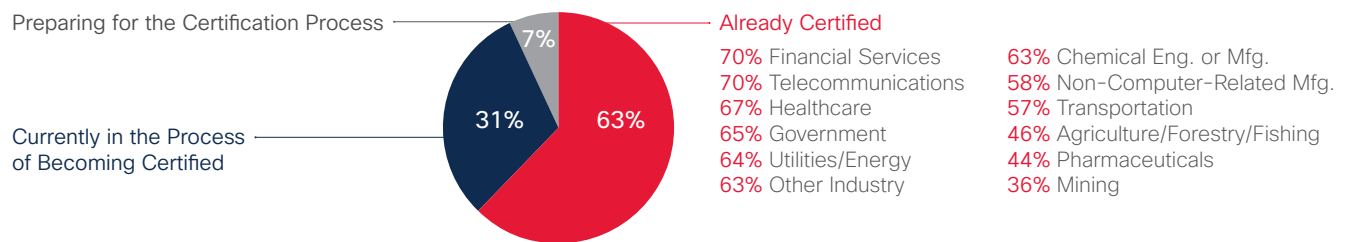
**Figure 75. Advice and Consulting Still Topmost Security Services Outsourced**

Significant Increases Seen in Audit and Incident Response Outsourcing. Outsourcing Is Seen as Being More Cost-Efficient.

Half (52%) follow a standardized security policy practice such as ISO 27001—the same as last year. Of these, the vast majority are either already certified or in the process of becoming certified.

### Standardized Security Policy Practice

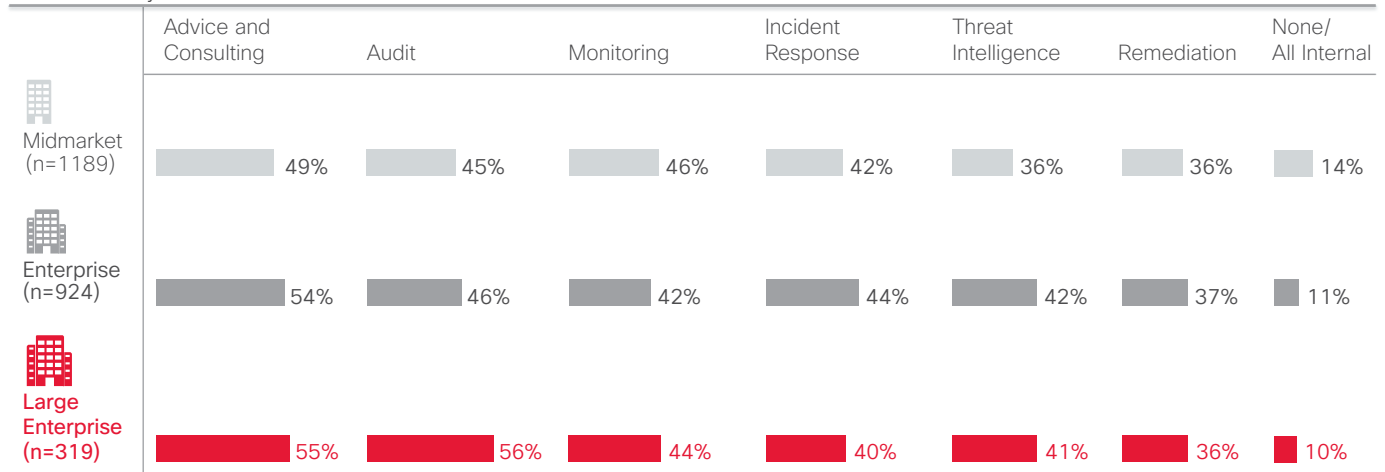
Organization follows standardized information security policy practice (2015: n=1265)



Source: Cisco 2015 Security Capabilities Benchmark Study

**Figure 76. Company View of Outsourcing: Large Enterprises Are Significantly More Likely to Outsource Audits, Advice and Consulting**

Which Security Services Are Outsourced?



Source: Cisco 2015 Security Capabilities Benchmark Study

**Figure 77. Country View of Outsourcing: Japan Is Significantly More Likely to Outsource Advice and Consulting**

Which Security Services Are Outsourced?

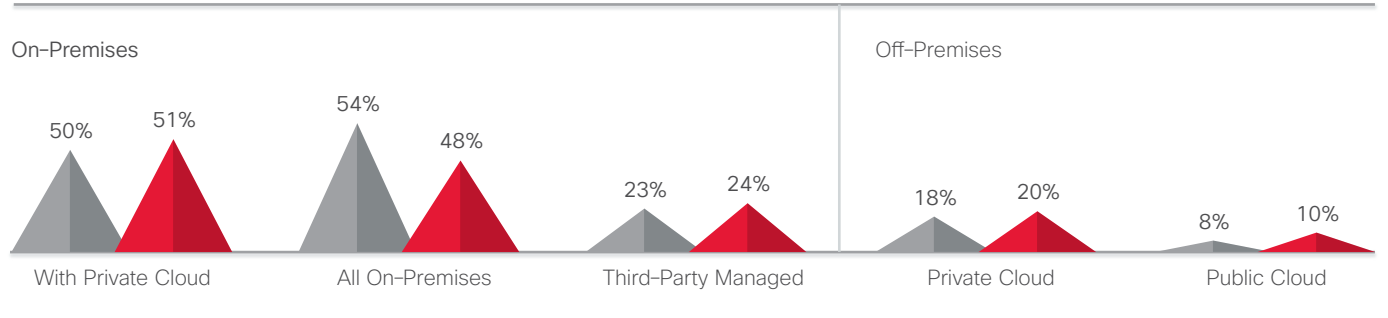
| TOTAL                                   | U.S. | Brazil | Germany | Italy | U.K. | Australia | China | India | Japan | Mexico | Russia | France |
|---|------|--------|---------|-------|------|-----------|-------|-------|-------|--------|--------|--------|
| Advice and Consulting<br>██████████ 52% | 52%  | 51%    | 19%     | 51%   | 44%  | 54%       | 52%   | 54%   | 64%   | 58%    | 41%    | 55%    |
| Audit<br>██████████ 47%                 | 50%  | 55%    | 38%     | 48%   | 50%  | 36%       | 33%   | 51%   | 41%   | 63%    | 40%    | 59%    |
| Monitoring<br>██████████ 44%            | 48%  | 49%    | 32%     | 39%   | 41%  | 52%       | 31%   | 51%   | 51%   | 49%    | 37%    | 50%    |
| Incident Response<br>██████████ 42%     | 46%  | 39%    | 32%     | 38%   | 43%  | 53%       | 34%   | 49%   | 53%   | 45%    | 27%    | 54%    |
| Threat Intelligence<br>██████████ 39%   | 42%  | 40%    | 37%     | 46%   | 36%  | 16%       | 36%   | 48%   | 47%   | 44%    | 42%    | 39%    |
| Remediation<br>██████████ 36%           | 34%  | 32%    | 38%     | 34%   | 31%  | 47%       | 37%   | 41%   | 40%   | 21%    | 41%    | 41%    |
| None/All Internal<br>███ 12%            | 18%  | 9%     | 18%     | 13%   | 19%  | 4%        | 19%   | 12%   | 10%   | 3%     | 16%    | 4%     |

Source: Cisco 2015 Security Capabilities Benchmark Study

**Figure 78. On-Premises Hosting of Networks Is Still the Most Common; However, Off-Premises Hosting has Increased Since Last Year**

Where Networks Are Hosted

2014 (n=1727) 2015 (n=2417)



Source: Cisco 2015 Security Capabilities Benchmark Study

## Public Security Breach

**Figure 79.** Fewer Organizations in 2015 Report Having Had to Manage Public Scrutiny of Security Breaches

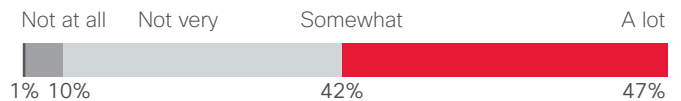
Security Breaches Are Strong Drivers of Security Improvements:

Fewer Organizations in **2015** Report Having Had to Manage Public Scrutiny of Security Breaches Compared to **2014**.



**2014**  
**53%** vs **2015**  
**48%**

How Much Did the Breach Drive Improvements in Your Security Threat Defense Policies, Procedures, or Technologies? (n=1134)



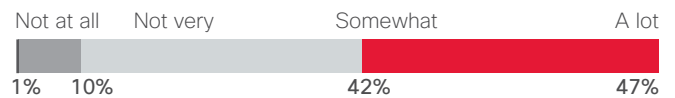
Source: Cisco 2015 Security Capabilities Benchmark Study

**Figure 80.** Public Breaches Can Improve Security

Security Breaches are Strong Drivers of Security Improvements: Respondents Dedicated to Security. **2014** (n=1701) **2015** (n=1347)

**2014**  
**53%** Yes vs **2015**  
**48%** Yes

How Much Did the Breach Drive Improvements in Your Security Threat Defense Policies, Procedures, or Technologies? (n=1134)



CSOs Mention More Improvements After Security Breach Than SecOps Managers Do.

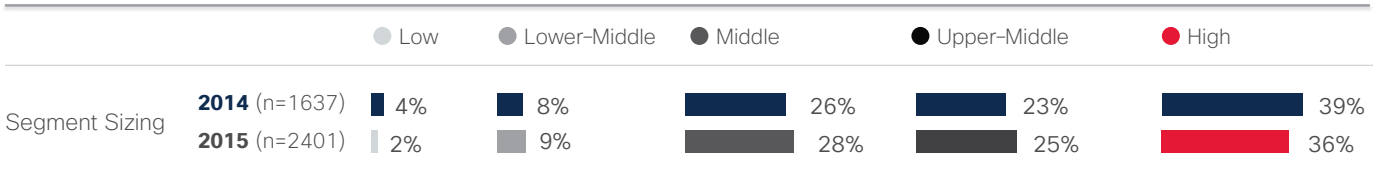
Source: Cisco 2015 Security Capabilities Benchmark Study

## Leadership and Maturity

**Figure 81. 5-Segment Model Tracks Closely to Security Capability Maturity Model (CMM)**

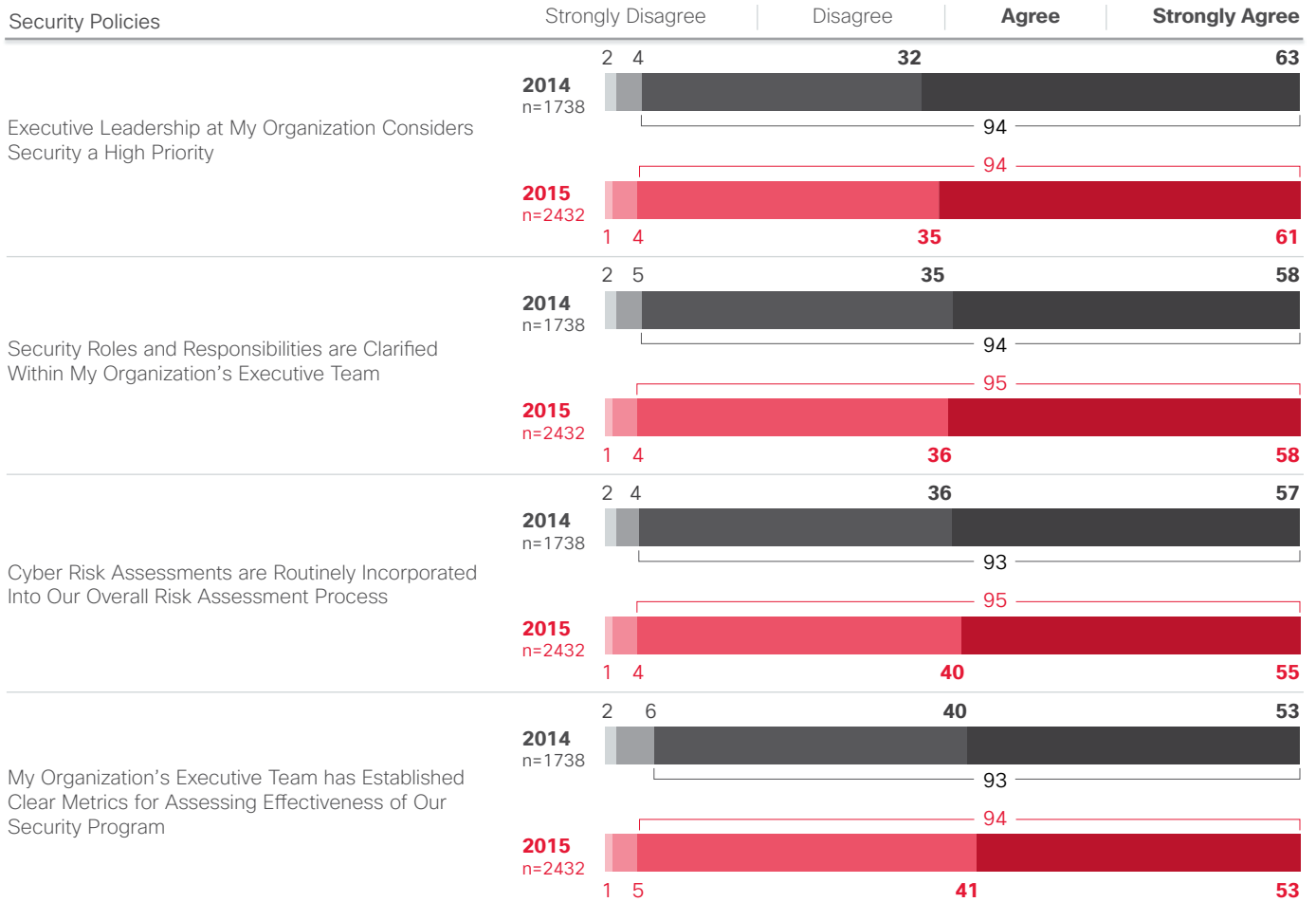
Segments Reflect a Similar Pattern to Last Year's Study in Terms of Maturity Around the Priority of Security and How that Translates Into Processes and Procedures.

**60%** or More Fit More Security-Mature Profiles. This is True for the Most Part Across Countries and Industry.



Source: Cisco 2015 Security Capabilities Benchmark Study

**Figure 82. As in 2014, Nearly All Agree or Strongly Agree that Executive Leadership Considers Security a High Priority**



Significantly more pharmaceutical respondents strongly agree with the statement "my organization's executive team has established clear metrics for assessing the effectiveness of our security program" than do professionals from most other industries.



Significantly more CSOs agree with all statements around executive engagement compared with SecOps.

Source: Cisco 2015 Security Capabilities Benchmark Study

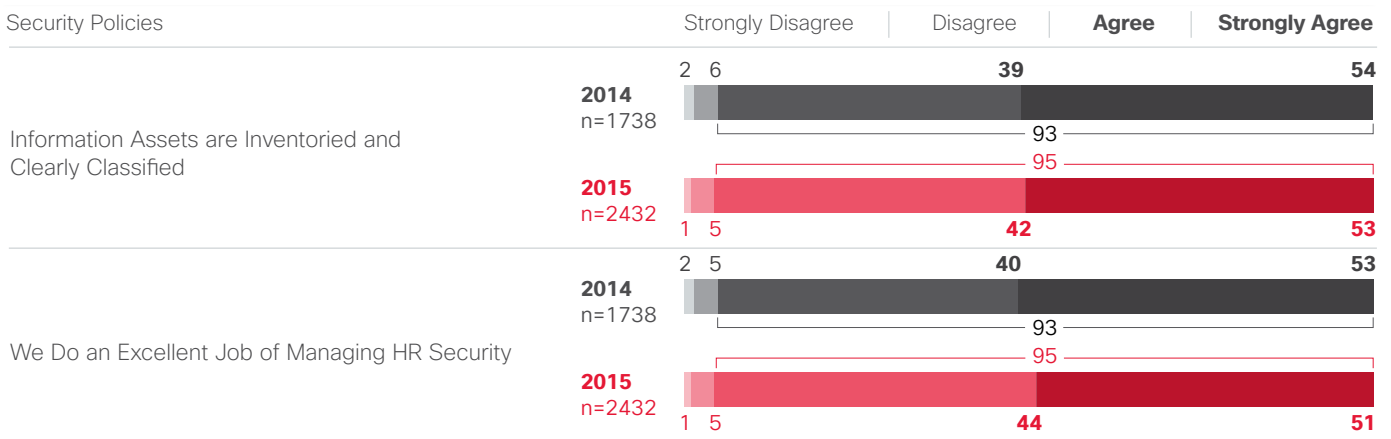
## Processes

**Figure 83. Mixed Confidence in Ability to Build Security into Systems**



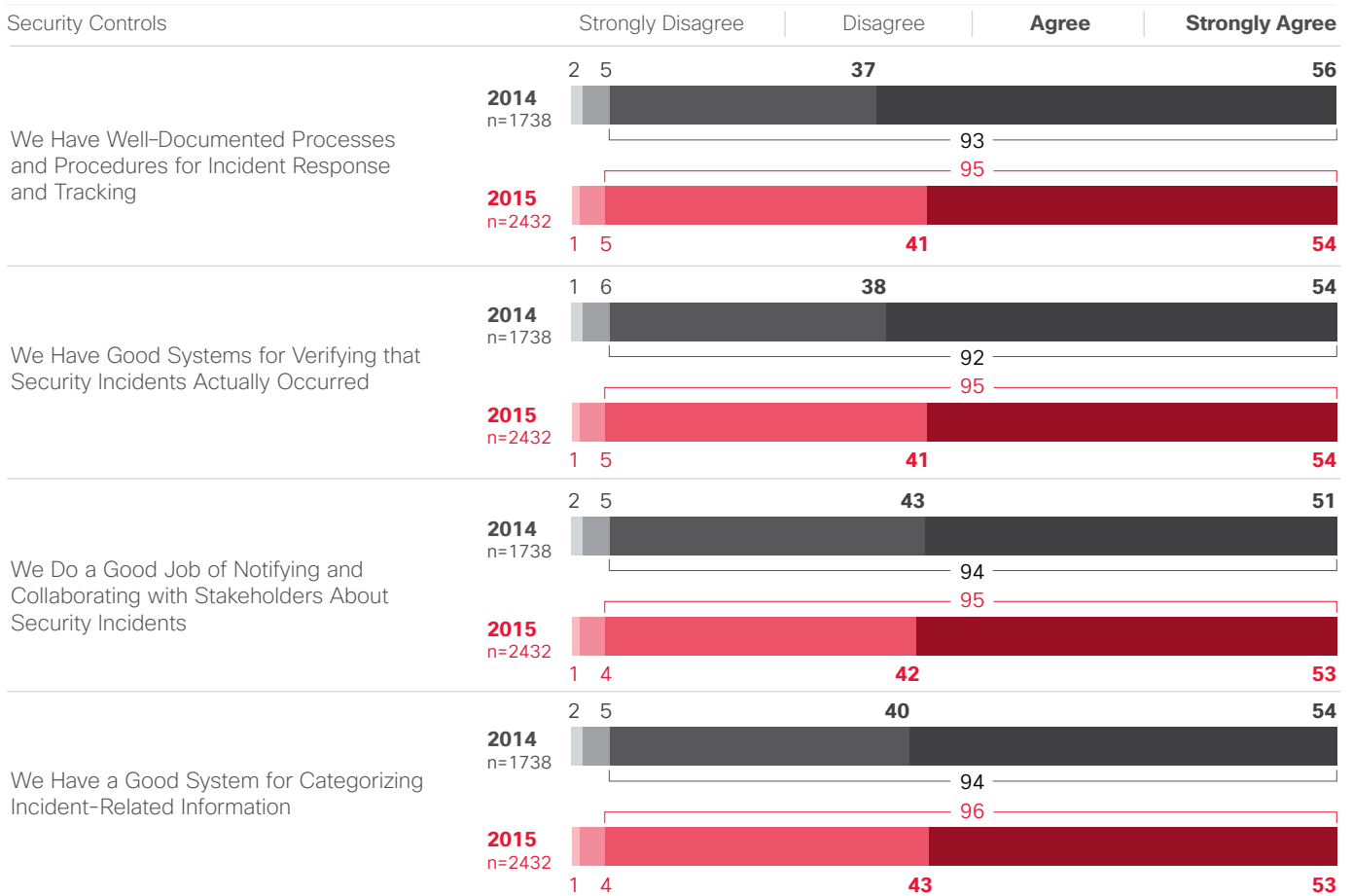
Source: Cisco 2015 Security Capabilities Benchmark Study

**Figure 83. Mixed Confidence in Ability to Build Security into Systems (continued)**



Source: Cisco 2015 Security Capabilities Benchmark Study

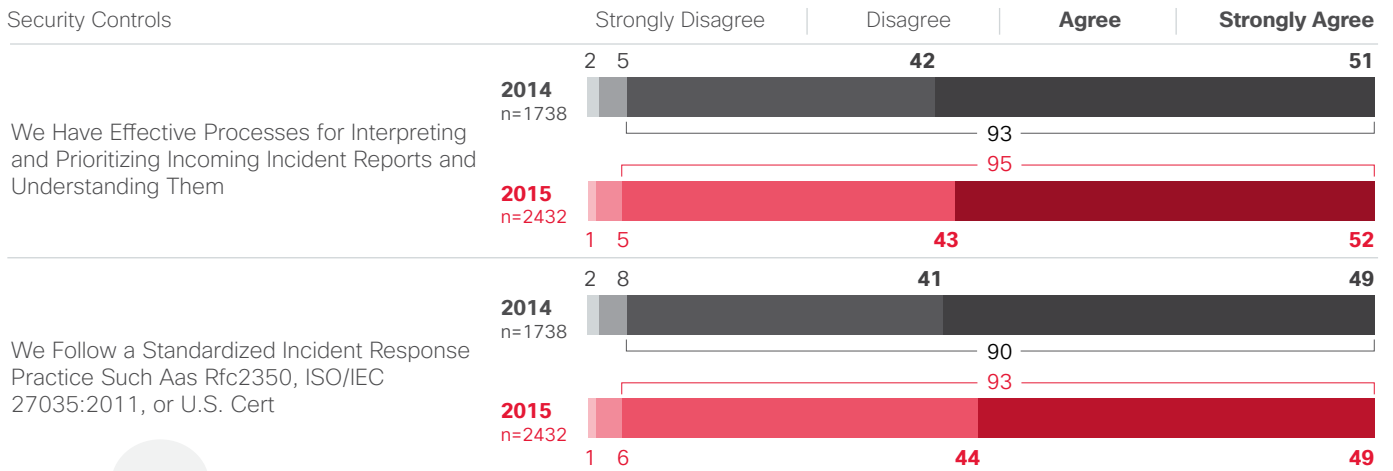
**Figure 84. Enterprises Believe They Have Good Security Controls**



Source: Cisco 2015 Security Capabilities Benchmark Study



**Figure 84. Enterprises Believe They Have Good Security Controls (continued)**

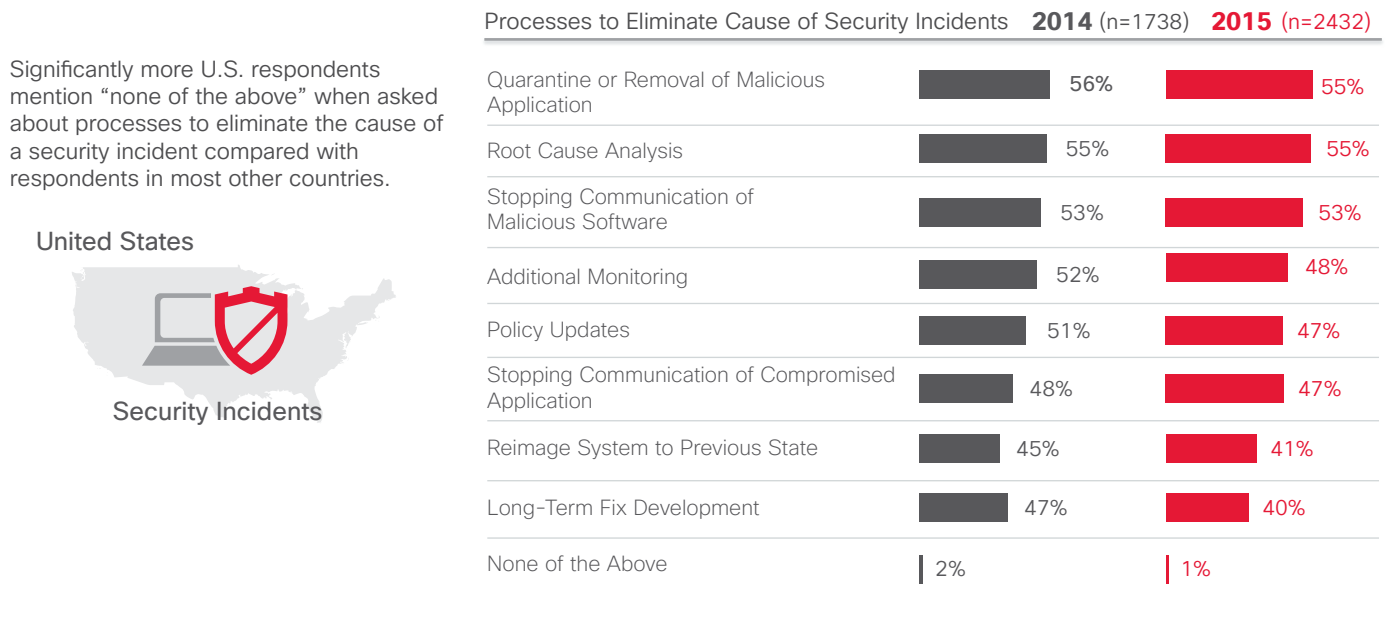


Financial services respondents are more likely to strongly agree with the statement “We have a good system for categorizing incident-related information” than professionals from most other industries.

Except for the statement “We do a good job of notifying and collaborating with stakeholders about security incidents,” CSOs are more positive about attributes surrounding security controls than SecOps managers.

Source: Cisco 2015 Security Capabilities Benchmark Study

**Figure 85. Quarantine/Removal of Malicious Applications and Root Cause Analysis Continue to Be the Top Processes Used**

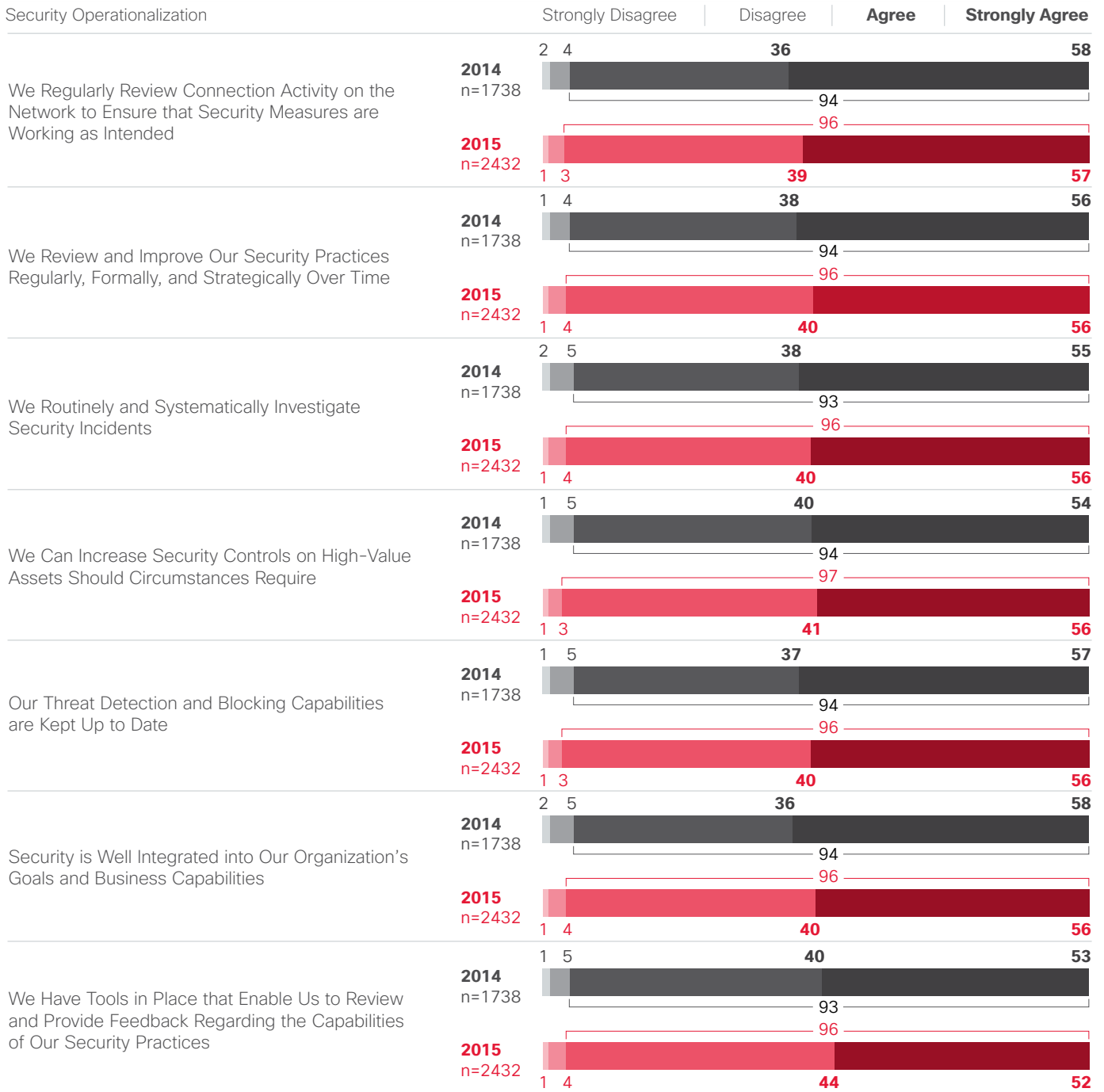


Significantly more U.S. respondents mention “none of the above” when asked about processes to eliminate the cause of a security incident compared with respondents in most other countries.



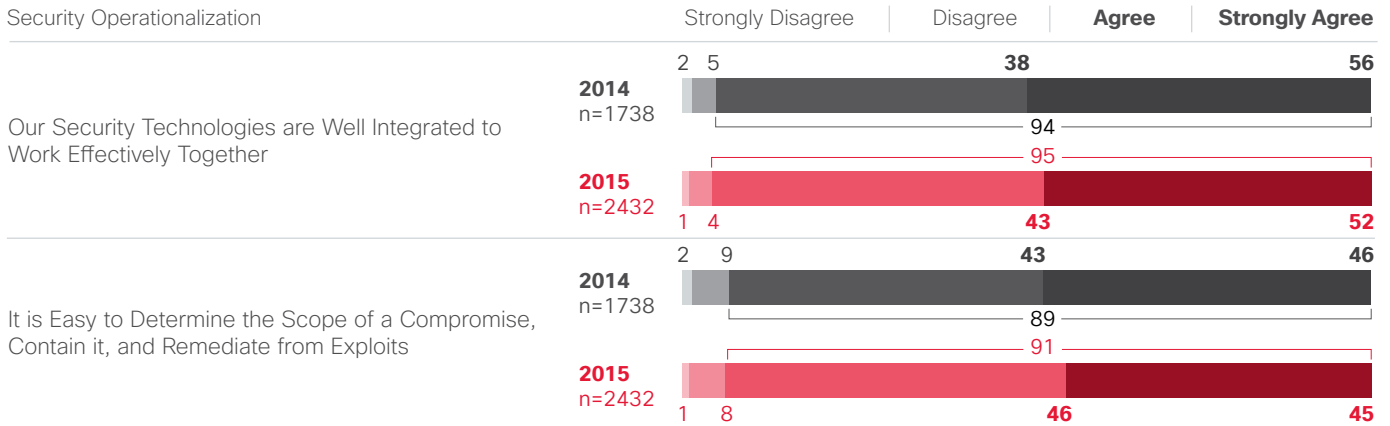
Source: Cisco 2015 Security Capabilities Benchmark Study

**Figure 86. Enterprises Exhibit Mixed Confidence in Ability to Contain Compromises**



Source: Cisco 2015 Security Capabilities Benchmark Study

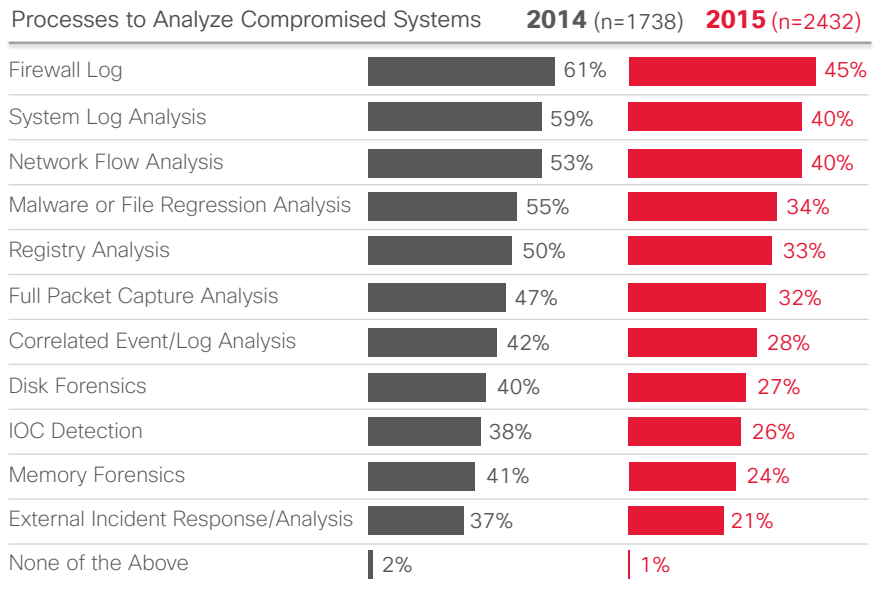
**Figure 86. Enterprises Exhibit Mixed Confidence in Ability to Contain Compromises (continued)**



Source: Cisco 2015 Security Capabilities Benchmark Study

**Figure 87. Firewall Logs and System Log Analysis Continue to Be the Most Commonly Used Processes to Analyze Compromised Systems**

Enterprise and Large Enterprise companies report using more processes for analyzing compromised systems than do Midmarket companies.



Source: Cisco 2015 Security Capabilities Benchmark Study

**Figure 88.** Restoring From a Pre-Incident Backup Is the Most Common Process to Restore Affected Systems in 2015

Respondents in China say they patch and update applications deemed vulnerable more frequently than do respondents in other countries surveyed.



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

Source: Cisco 2015 Security Capabilities Benchmark Study

**Figure 89.** The CEO or President Is Most Likely to Be Notified of Security Incidents, Followed by Operations and the Finance Department

Significantly more large enterprise respondents mention notifying external authorities in the event of an incident than those from Midmarket and Enterprise companies.

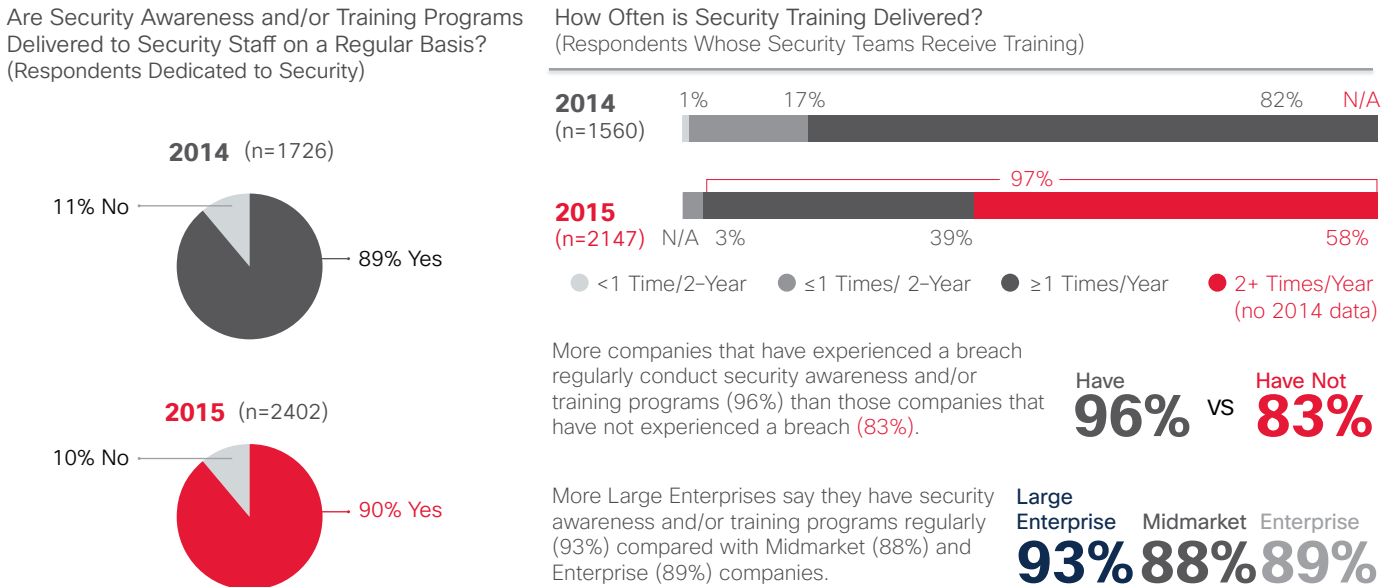


| Groups Notified in the Event of an Incident | 2014 (n=1738) | 2015 (n=2432) |
|---|---------------|---------------|
| Chief Executive Officer                     | N/A           | 45%           |
| Operations                                  | 46%           | 40%           |
| Finance Department                          | N/A           | 40%           |
| Technology Partners                         | 45%           | 34%           |
| Engineering                                 | 38%           | 33%           |
| Human Resources                             | 36%           | 32%           |
| Legal                                       | 36%           | 28%           |
| Manufacturing                               | 33%           | 27%           |
| All Employees                               | 35%           | 26%           |
| Public Relations                            | 28%           | 24%           |
| Business Partners                           | 32%           | 21%           |
| External Authorities                        | 22%           | 18%           |
| Insurance Companies                         | N/A           | 15%           |

Source: Cisco 2015 Security Capabilities Benchmark Study

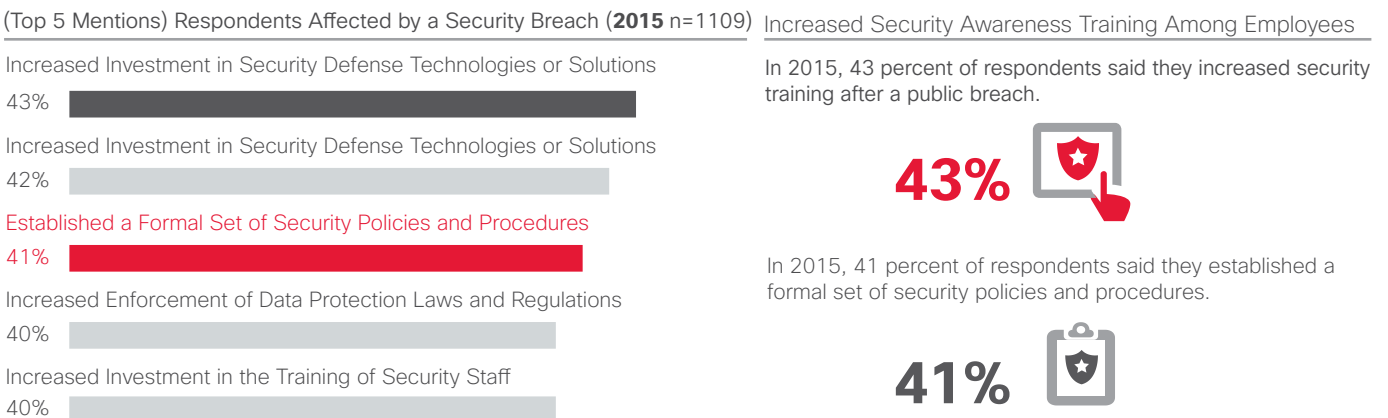
## Training

**Figure 90. Nearly All Companies (97%) Deliver Security Training at Least Once a Year**



Source: Cisco 2015 Security Capabilities Benchmark Study

**Figure 91. Frequency of Security Awareness Training and Incidence of Formal Security Policies Are Both Up Since 2014—Evidence of Action**



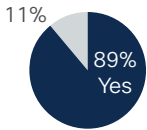
Source: Cisco 2015 Security Capabilities Benchmark Study

**Figure 92.** As in 2014, Nearly 9 in 10 Say Their Security Staff Attend Security-Focused Conferences or Training

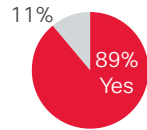
Do Security Staff Members Attend Conferences and/or External Training to Improve and Maintain Their Skills?  
(Respondents Dedicated to Security)

Do Employees Serve on Security Industry Boards or Committees?  
(Respondents Dedicated to Security)

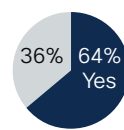
**2014** (n=1738)



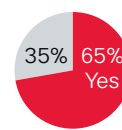
**2015** (n=2432)



**2014** (n=1738)



**2015** (n=2432)



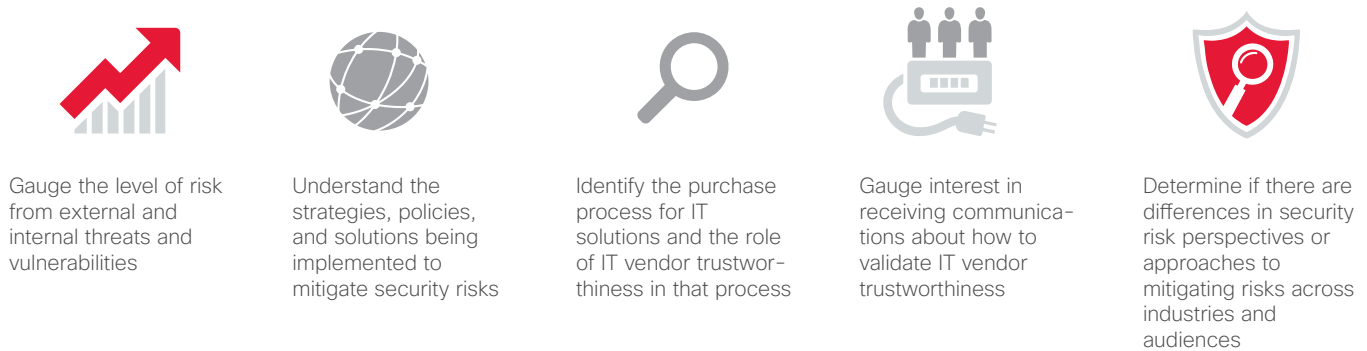
Source: Cisco 2015 Security Capabilities Benchmark Study

## Security Risk and Trustworthiness Study

**Figure 93. Background and Methodology**

Cisco is interested in obtaining a deeper understanding of Enterprise and Service Provider IT decision makers' perceptions of their organization's security risks and challenges and the role that IT vendor trustworthiness plays in IT solution purchases.

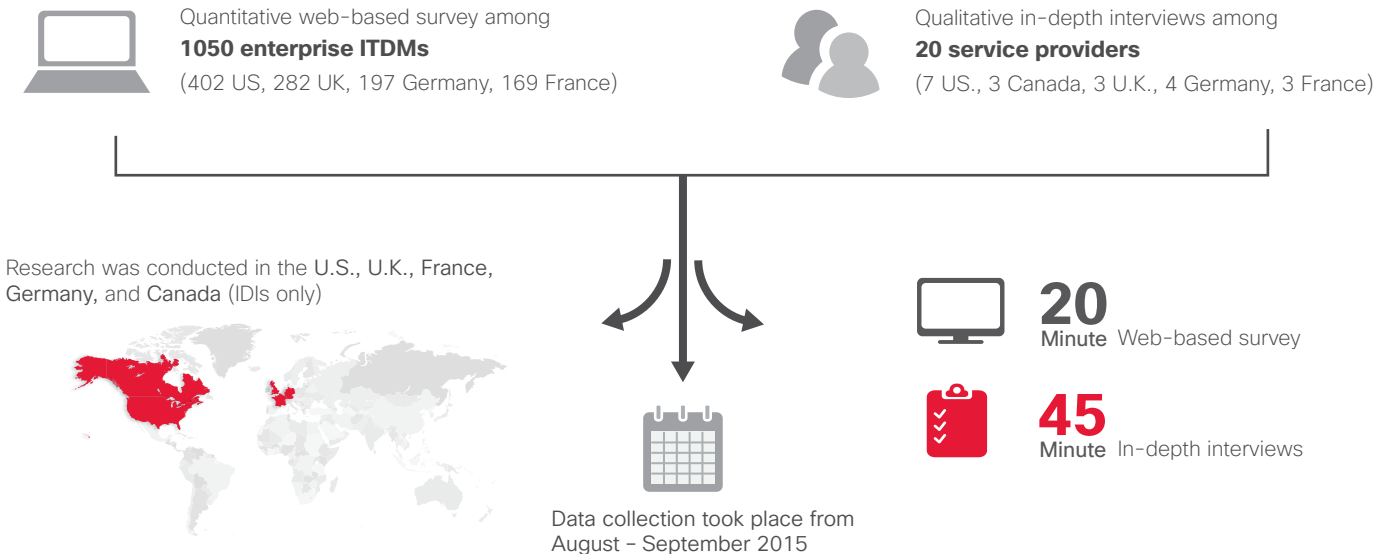
Specific objectives include:



### Methodology: Quantitative and Qualitative Approach

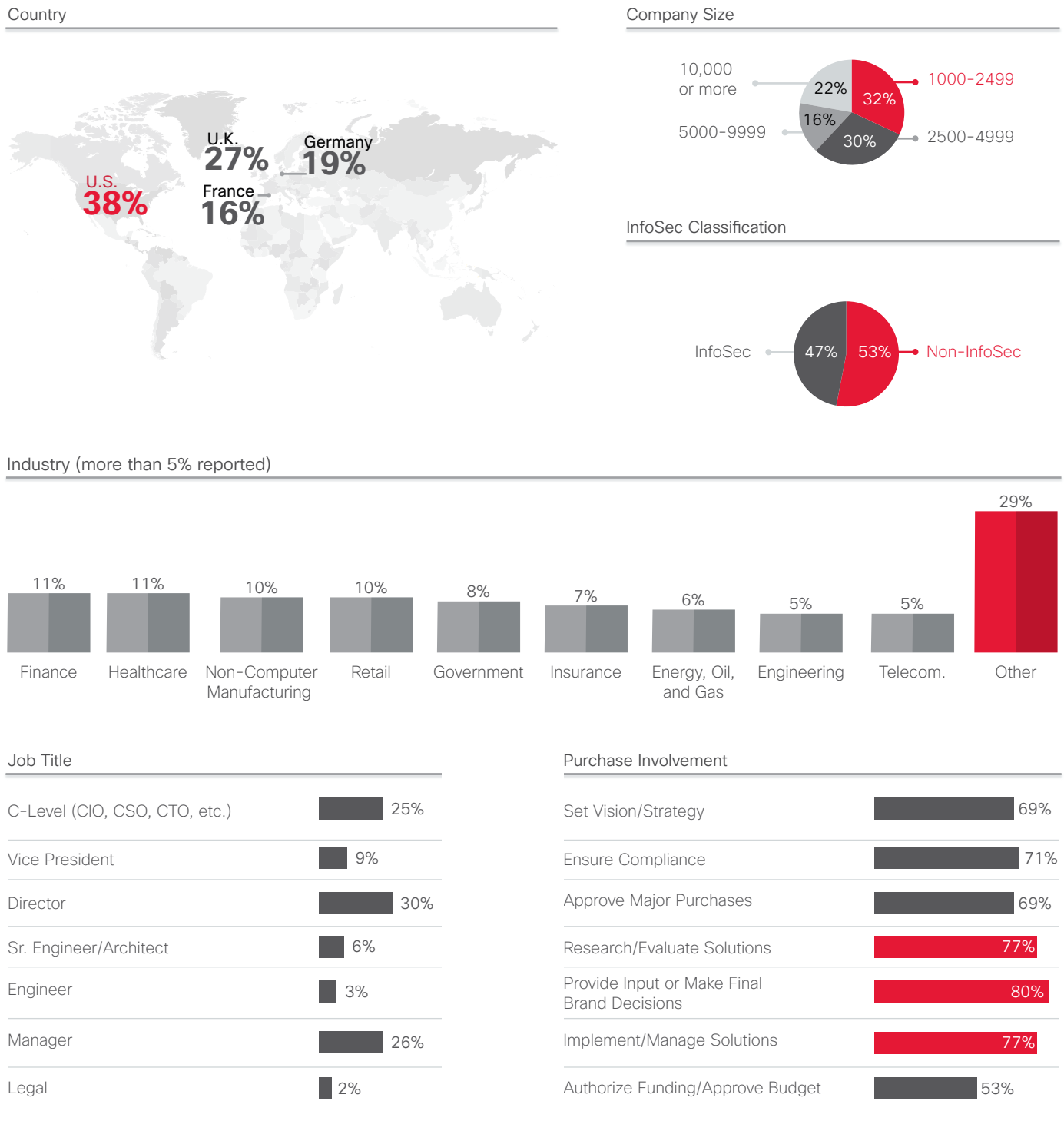
Two methodologies were utilized to provide insight into each of these research objectives:

(All respondents involved in IT purchase decision-making)



Source: Security Risk and Trustworthiness Study, Cisco

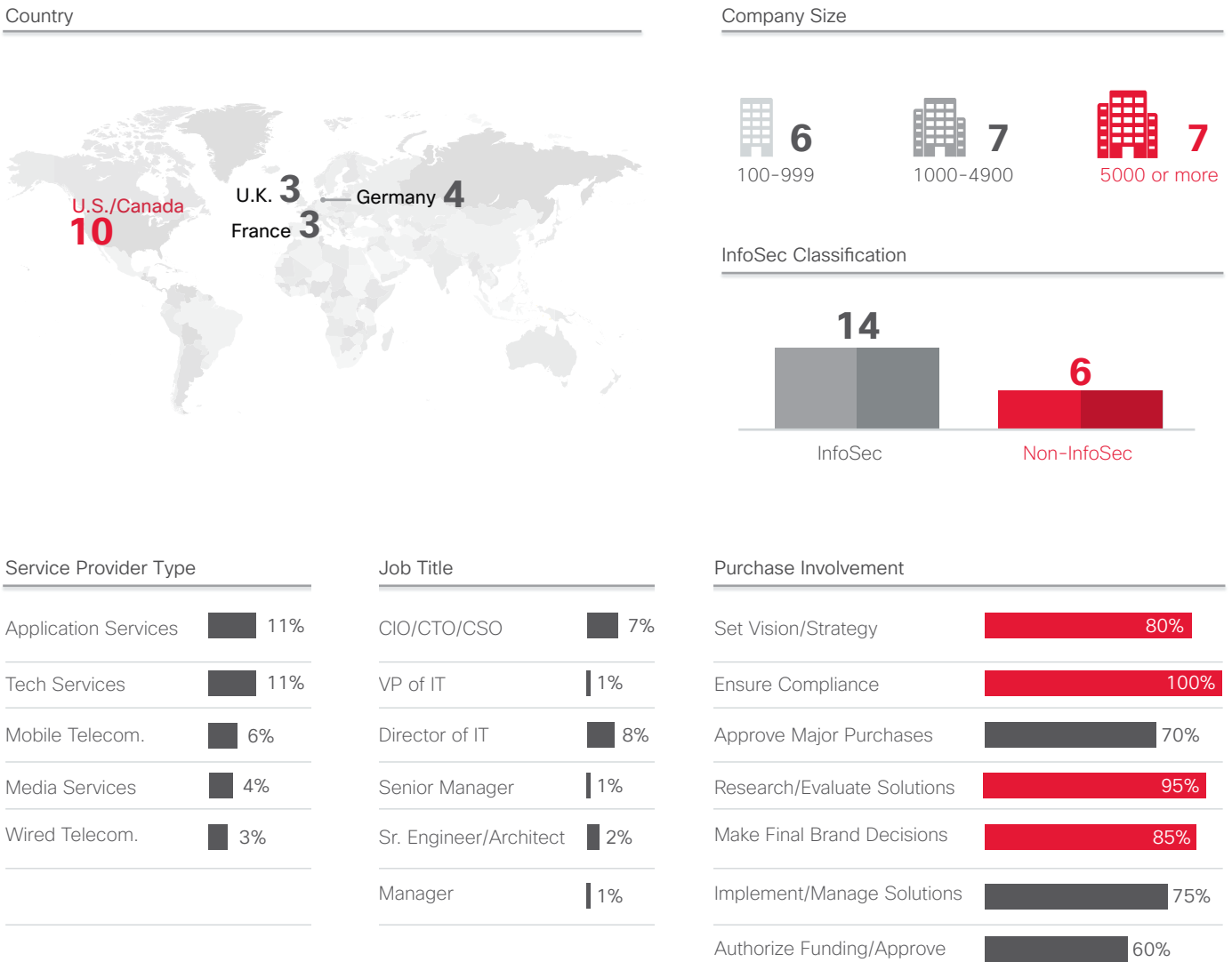
**Figure 94. Enterprise Respondent Profile Quantitative**



Source: Security Risk and Trustworthiness Study, Cisco



**Figure 95. Service Provider Respondent Profile: Qualitative**



Source: Security Risk and Trustworthiness Study, Cisco



---

**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](http://www.cisco.com/go/offices).

Published January 2016

---

© 2016 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](http://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.