
2016
GLOBAL
THREAT
REPORT
Forward Without Fear
FORCEPOINT™ Security Labs™

FORCEPOINT
POWERED BY Raytheon

# TABLE OF CONTENTS




# EXECUTIVE SUMMARY

In the past year, major shifts have changed the complexion of cyberattacks. While under-the-radar, data-stealing malware is still common, the autonomous modern employee could be the biggest threat to your organization's data. A bold new crop of ransomware actors eschew such covert action by simply exclaiming they have encrypted, and are ransoming, your data – in a much quicker path to profits. Facing new anti-malware tools, attackers are recycling attack methods of yesteryear – going back to macro-laden Microsoft® Office files that land on desktops. The growing migration to cloud computing with inconsistent controls is posing serious challenges to security. Meanwhile, in the background, new botnets are testing the security community's ability to detect and intercept adversaries' short-term tactical and big picture aims.

Thus, the priority is on informing decision-makers about the crucial context around these attacks in the wild, around the globe and within their networks, so that the most time and resources can be applied to the most severe threats. True to its "Forward Without Fear" motto, Forcepoint's Security Labs, Special Investigations (SI) and Office of the CSO (OoCSO) teams continually sort and cut through the dense, complex noise of worldwide attack activity and identify the threats and breakthroughs that matter the most, offering guidance at every step.

The Forcepoint **2016 Global Threat Report** is a definitive breakdown of many of today's most impactful cybersecurity threats with far-reaching technical, operational and cost impacts on affected organizations. Each section of this report closes with guidance from the Forcepoint Security Labs team on how to best address the outlined threat(s). Chapters include:

## 1. INSIDER THREAT: THE MALICIOUS AND THE ACCIDENTAL

Forcepoint and third-party research (page 5) shows that policing insider activity and accounting for privileged credentials are security issues organizations feel least-prepared to confront. A full 30% of security remains focused on perimeter defenses[1], with less than 40% of organizations surveyed having dedicated budget to insider threat programs[2]. Yet, many employees are empowered to connect remotely and are on and off networks constantly accessing servers (where your most sensitive data lives).

## 2. ADVANCED THREATS AND SPECIAL INVESTIGATIONS CASE STUDIES: REVEALING "JAKU" AND BREAKING RANSOMWARE

One of the best windows on advanced threats comes via Forcepoint's Special Investigations team, an elite group of threat researchers and incident response experts specializing in threats exhibiting unique tools, tactics and processes (TTPs). In the past year, highlights of the SI team's work include discovering a new botnet campaign dubbed JAKU and cracking a persistent strain of ransomware known as Locky.

## 3. WEB AND EMAIL: A TWO-PRONGED THREAT

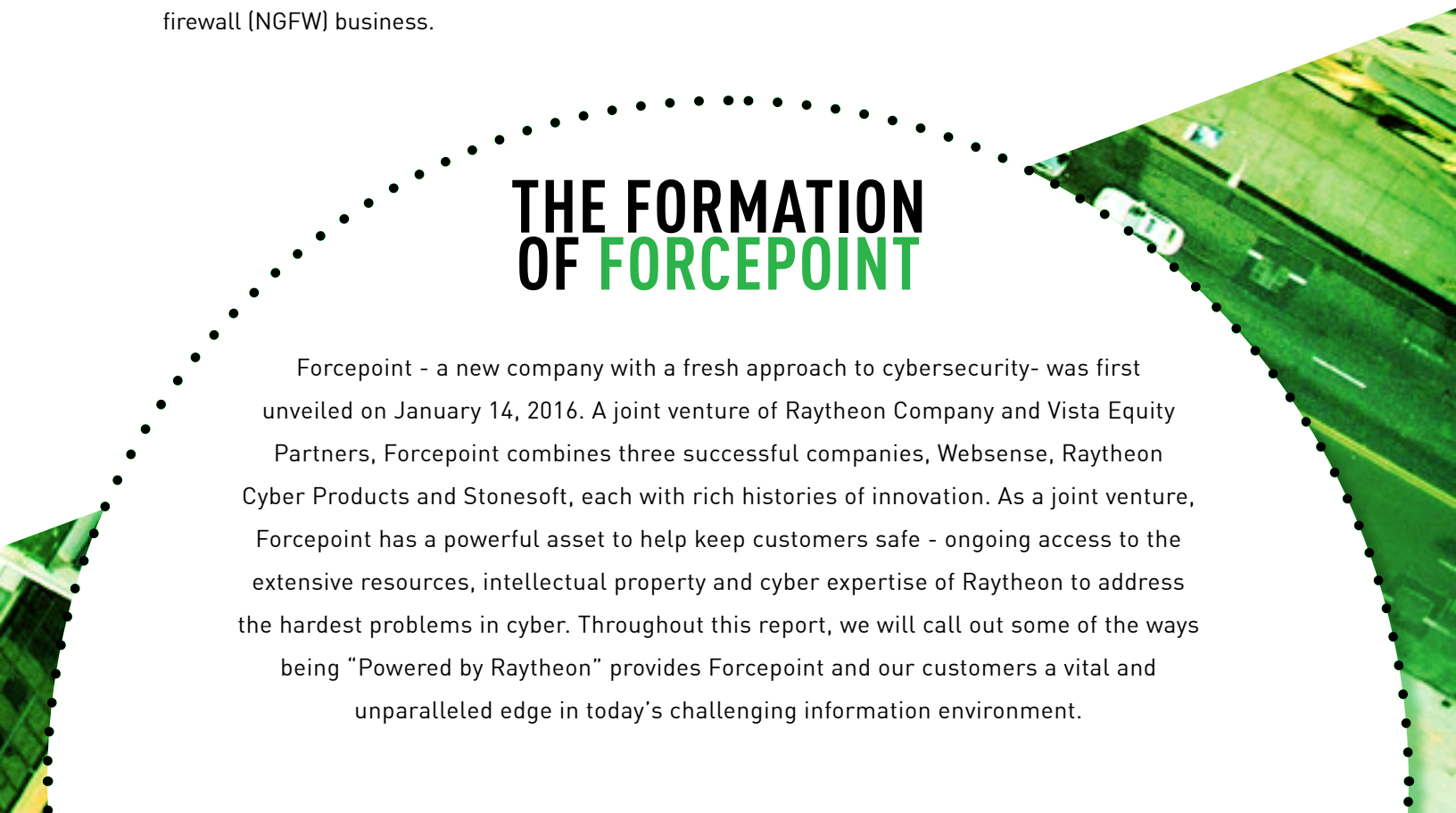
Employees in even the most restricted and secure workplaces typically cannot be productive without the Web and email, making these mediums ideal for serving up malicious payloads in the form of links to malware-laden Web sites and malicious email attachments. Almost 92% of unwanted (e.g., spam, malicious) email now contains a URL and the presence of malicious macros in e-mail is up 44.7 % (page 20).

## 4. SECURITY CONCERNS STILL HAUNT MOVES TO THE CLOUD

Cloud computing's cost, scalability and accessibility have offset security concerns for many enterprises, yet these issues present headaches for many cloud prospects wary of how inconsistent security controls between cloud providers and their own environments could upend data protection. Somewhat ironically, CIOs and CISOs holding off on cloud adoption nonetheless find themselves wrestling with the consequences of employees' independent decisions to use the cloud apps they prefer for personal productivity and convenience. More than 80% of surveyed decision-makers feel "shadow" IT poses severe consequences[3].

## 5. THOUGHTS FROM FORCEPOINT'S OFFICE OF THE CSO

In 2015, the Forcepoint Office of the CSO team saw M&A activity as one of the greatest cybersecurity risk catalysts across industry sectors. In a real-world example, the OoCSO taps the expertise of its own cybersecurity and data protection leaders to recap how comprehensive security controls were managed during the M&A activities that created Forcepoint itself – the integration of the former companies Websense® and Raytheon Cyber Products (RCP), and the Stonesoft® next generation firewall (NGFW) business.



# THE FORMATION OF FORCEPOINT

Forcepoint - a new company with a fresh approach to cybersecurity- was first unveiled on January 14, 2016. A joint venture of Raytheon Company and Vista Equity Partners, Forcepoint combines three successful companies, Websense, Raytheon Cyber Products and Stonesoft, each with rich histories of innovation. As a joint venture, Forcepoint has a powerful asset to help keep customers safe - ongoing access to the extensive resources, intellectual property and cyber expertise of Raytheon to address the hardest problems in cyber. Throughout this report, we will call out some of the ways being "Powered by Raytheon" provides Forcepoint and our customers a vital and unparalleled edge in today's challenging information environment.

# INSIDER THREAT

Insider threats refer to attacks that either originate or receive cooperation (willingly or unwillingly) from sources within an organization. Attackers are targeting insiders within organizations – or via business partners and third-party suppliers – and gaining access to networks by manipulating staff into revealing their credentials. With these stolen credentials, criminals then move among networks, accessing and removing sensitive data, often going unnoticed until it's too late. Breaches caused by insider threats continue to climb, with accidental insiders the leading source of problems. Of firms surveyed by Forrester that had experienced a breach in 2015, internal incidents were the leading cause, and more than 50% of those were due to inadvertent misuse or user error[4], known as the "accidental insider."

## EXAMPLES OF THE ACCIDENTAL INSIDER:

- Employee clicks on suspicious link in email, unknowingly enabling malicious code to download onto their machine.
- Employee uses a 'found' USB drive (an Idaho National Laboratory study revealed 20% of employees plugged found USB drives into work computers[5]).
- Employee loses laptop, tablet, or storage device with proprietary information.
- Employee ignores security policy to take work home for afterhours use.

## UNPARALLELED TESTING METHODS

**Raytheon's team of security researchers leverages the latest technologies to assess vulnerabilities, reduce threat surfaces and maximize security effectiveness. These include: hundreds of millions of tests per week, static and dynamic software analysis, cooperative and uncooperative engagements, network emulation of more than 100,000 endpoints and processes for turning threat indicators into defensive actions.**

According to Ponemon Institute research[6] sponsored by Forcepoint, employees represent the biggest threat to company security largely because insider abuse can be difficult to detect. For example, stolen credentials from valid user accounts are often used to attain sensitive data to which the legitimate user would normally have access, specifically to avoid raising any red flags. This was echoed by a March 2016 survey[7], which found that detecting malicious insider activity or the hijacking of privileged users' credentials by a hacker were the top areas for which banks felt least prepared. The increasing popularity of conducting business from personal devices (known as Bring Your Own Device or BYOD) adds to the complexity of the insider threat, creating more avenues for hackers to gain a foothold without popping up on the security team's radar. As a result, organizations are constantly balancing access to data against the risk of its loss or misuse.

Often, the weak link that leads to inadvertent loss of critical data is the user who improperly handles data because they are unaware of, or careless in the use of effective security practices

## Employee error/negligence was responsible for nearly 15% of data breach incidents in 2015[8]

... and it's easy to see why, when little more than half of staff are aware of company security policies[9].

Despite increasing damage (with authentication credentials, intellectual property, corporate financial data, and personally identifiable information (PII) most commonly lost as a result), organizations continue to use ineffective means to educate staff, and employees remain unaware of how to exercise good security practices at work[10]. With the insider threat a clear and present danger, why do perimeter defenses remain more of a priority than insider threat programs?

A recent Ponemon study[11] provides some insight. Though a recognized problem, less than 40% of organizations surveyed had dedicated budget for an insider threat program. Citing a lack of contextual information along with volumes of false positives and insufficient visibility, most were relying on existing tools not suited to solve the issue. More sophisticated technology, combining data loss prevention (DLP) and user behavior analytics that correlate with other IT and business systems activity (like RFID access logs and IP log records), is now evolving to determine whether a threat is from a true insider or a masquerader using stolen credentials.

The insider threat; however, is not just an 'IT' issue; it's one that must also involve personnel. An effective insider threat program incorporates technology controls with risk management plans and employee training on best practices. Key components of a successful insider threat program include:

- **Policies:** Communicating policies on how technology should be used within the organization from appropriate devices to the handling of data and Internet use.
- **Processes:** Applying appropriate segregation of duties and other checkpoints into processes.
- **Technology controls:** Limiting access to according to least privilege principles, based on each individual's assigned role.
- **Risk management:** Identifying and developing a risk management plan to give the highest areas of risk top priority.
- **Auditing and monitoring:** Verifying that each of the key components are effective and meet the organizational needs.

## INSIDER THREAT CASE STUDY: DATA MEETS THE DOWNSIZE

According to a Forrester security survey[13], 39% of breaches the last 12 months resulted from an internal incident. Of these, 26% were the result of deliberate abuses or malicious intent, while 56% were the result of inadvertent misuse of data (18% were a combination of both).

The following Forcepoint case study, which is being shared for the first time here, illustrates a typical insider threat scenario. Following M&A activity, a customer began the process of downsizing its software engineering staff. Employees were informed of impending layoffs – some immediate, others after current projects were completed. A generous severance package, including a full-year of pay, was conditional on company intellectual property and assets remaining in-house. Regardless, a surprisingly large number of engineers returned to their desks and began trying to steal confidential data. Having prepared for this scenario, the organization employed Forcepoint's SureView® Insider Threat technology to observe high-risk employee behaviors (measured against a 30-day history of typical daily behaviors). As a result, uncommon operations – attempts to copy and save files to USB storage devices or email files and send source code out through web channels to cloud storage – were made immediately apparent by Forcepoint technology. SureView Insider Threat was able to stop the breaches and, most importantly, the company was able to protect their most valuable intellectual property by identifying employees who broke the severance agreement by attempting to steal data. Though this particular case illustrates the malicious insider, an accidental insider (one whose credentials are stolen or whose computer is hijacked) could just as easily trigger the same alerts through unusual network movement, access after-hours or transfers of data.

## FORCEPOINT GUIDANCE

1. Understand where your organization's particular risks lie and why. Don't wait to establish a baseline for normal user behavior. Understanding historical user behavior is necessary to detecting anomalies that may indicate an insider threat.
2. Empower users by proactively addressing risks through training and awareness programs.
3. Establish an insider incident response plan with formal processes for the identification, communication, and escalation of insider events.
4. Consider investing in solutions that offer sophisticated behavioral analysis and tracking over time to quickly identify user behavior that may lead to or suggest a compromise. By identifying risky users early, breaches can be stopped before or soon after they start.

# ADVANCED THREATS

## SPECIAL INVESTIGATIONS CASE STUDIES

A dramatic increase in the size and complexity of IT is quickly making the conventional view of an "advanced threat" outdated. Organizations now face "aggregate threats" that have expanded in capability as traditional perimeters dissolve and data spreads across endpoints, networks, mobile and the cloud. These new complexities require novel approaches and bring the importance of integrated solutions that can share threat intelligence and reduce dwell time[14].

***Dwell time begins when an attacker enters a network and continues until they leave or are forced out. Minimizing dwell time reduces the opportunity for an attacker to achieve lateral movement and remove critical data.***

These new, advanced attacks are the focus of Forcepoint's Special Investigations team, who are engaged when an exploit exhibits Tools, Tactics, and Processes (TTP) outside of what is considered normal. The SI team's skillset and knowledge covers reverse engineering, advanced attack analysis and neutralization of evasive malware on which they collaborate with law enforcement.

The SI team also takes reference points from known attack data and dives several levels deeper to build understanding and mitigation techniques of new TTP. This approach was used to analyze JAKU – a newly identified global botnet campaign described here for the first time.

## INTRODUCING JAKU

JAKU is an on-going global botnet campaign. It demonstrates the re-use of infrastructure and TTP and exhibits a split personality. JAKU herds victims en masse and conducts highly targeted attacks on specific victims through the execution of concurrent operational campaigns. The outcome is data leakage of machine information, end-user profiling and incorporation into larger attack data sets.

By conducting a six month investigation, Forcepoint Security Labs has been able to accurately plot the locations of command and control servers and victims, globally. Through static and behavioral analysis, the Labs team has been able to understand the components of the attack and the tracking mechanism used by this botnet. Throughout their research, they coordinated with various law enforcement agencies throughout the investigation and are now at a point where they are able to share their insights publicly. Forcepoint customers have been protected from the threats presented by JAKU since before the inception of this investigation in October 2015.

> "What is somewhat of a step-change is the execution of a number of concurrent operations within a campaign, using almost identical TTP to herd thousands of victims while at the same time executing a targeted operation."
>
> – Dr. Richard Ford, Forcepoint Chief Scientist, on JAKU

## TOP FIVE JAKU VICTIMS BY COUNTRY


## MEAN DWELL TIME

**93 DAYS**

**MAXIMUM DWELL TIME: 348 DAYS**

# JAKU
## FACTS & FIGURES

LENGTH OF INVESTIGATION TO DATE:
**6 MONTHS**

LOCATION OF VICTIMS:
**GLOBAL**
*(SIGNIFICANT CLUSTERING IN JAPAN, SOUTH KOREA & CHINA)*

PAYLOADS ARE DELIVERED VIA:
**EXPOSURE TO COMPROMISED BITTORRENT SITES, USE OF UNLICENSED SOFTWARE & DOWNLOADING OF WAREZ SOFTWARE**

EVASION TECHNIQUES USED:
**CRYPTOGRAPHY, STEGANO-GRAPHY, FAKE FILE TYPES, STEALTH INJECTION, ANTI-VIRUS ENGINE DETECTION (AND OTHERS)**

LOCATION OF COMMAND AND CONTROL SERVERS:
**MALAYSIA, THAILAND & SINGAPORE**

NUMBER OF UNIQUE VICTIMS

**19k**

**MALWARE TYPE:**

**MULTI-STAGE TRACKING AND DATA EXFILTRATION MALWARE**

NUMBER OF COUNTRIES WITH JAKU VICTIMS

**134**

## FAQ ON JAKU

***When will a full technical analysis of JAKU be made available to the public?***

A full technical write-up sharing all known IOCs (Indicators of Compromise) will be made available on the Security Labs blog May 4, 2016.

***What other members of the security community were involved in the research?***

Forcepoint would like to recognize the extensive work done by Kaspersky in their analysis of the Dark Hotel campaign as well as the UK National Crime Agency (NCA), CERT-UK, Europol and Interpol for their cooperation and assistance in this investigation. Only with a collaborative approach to information collection, collation and analysis can the Internet become a safer place for people to do business and conduct their modern lives.

## FORCEPOINT GUIDANCE

1. Build processes within your organization to reduce potential dwell time[15].
2. Limit or avoid contact with torrent sites and illegal software.
3. Monitor for unusual activity, such as traffic sent to command and control servers, known to threat intelligence systems.

## A **FORCE** TO BE RECKONED WITH

**"DeepRed," a team of Raytheon engineers and Forcepoint computer experts, is creating a computer program to find security flaws in software and fix them almost instantly as part of the Defense Advanced Research Projects Agency's Cyber Grand Challenge. DeepRed will compete at the hacker convention, DEF CON in August 2016 in Las Vegas for a $2 million prize.**

## FIGHTING BACK AGAINST RANSOMWARE:
## A LOOK AT LOCKY

Ransomware is the name given to malware that encrypts your files and then offers to sell you the encryption key to retrieve your files. Ransomware translates to data destruction if the data owner is unable to retrieve their files.

Ransomware became an all-too-familiar sight over the past year. Forcepoint Security Labs has been tracking the development of ransomware techniques, often delivered through malicious email attachments or malvertising, for several years.

Following news of a hospital[16] paying ransom to a service-disabling attack, the SI team investigated how to prevent the encryption of files and to share that knowledge with the wider community.

## FORCEPOINT UNLOCKS LOCKY:
## REVERSE ENGINEERING THE DOMAIN GENERATION ALGORITHM

Forcepoint offered customers protection from the lure used to disseminate the Locky payload (a malicious email containing a Microsoft Office document file that included a malicious macro) and Forcepoint Security Labs also discovered they could disable the file encryption process.

Locky uses 128-bit AES encryption and is capable of encrypting SQL databases, source code, BitCoin wallets and others. Analysis of the payload in our Threat Protection Cloud (behavioral file sandbox) module identified an obvious call to known command and control servers.

Unfortunately, Locky employs a Domain Generation Algorithm that generates a different set of URLs based on a time stamp and a seed value. As such, there exists the possibility that not all URLs could be known without further investigation. Labs' first analysis showed Locky contacted up to six URLs per day.

Forcepoint Security Labs reverse-engineered the Domain Generation Algorithm (DGA) of Locky ransomware and revealed it to the public, giving defenders an opportunity to fight back and block access to the domains the ransomware was contacting[17]. By stopping the ransomware from accessing the known URLs and obtaining the required encryption keys used on a given day, files remain untouched.

Five days later, the malware authors changed their DGA and updated the seed values. The ransomware was then able to reach out to 14 domains on a given day. Once again, Forcepoint unveiled the algorithm and provided the list of domains to be contacted during the following 30 calendar days[18]. With continued monitoring, Forcepoint found the malware authors changed their tactics once again 23 calendar days later[19].

Though paying ransom may not ensure file retrieval, some businesses have resorted to shelling out the fee, often up to several thousand dollars[20].


Some ransomware variants, such as CTB-Locker, do not need to reach out to a command and control server to access the key required to encrypt files, giving defenders one less opportunity to disrupt the data destruction incident. This is why Forcepoint focuses its efforts on intercepting the malware in the early stages of the threat lifecycle, particularly at the "Lure" stage (when cybercriminals create an innocuous looking email or other lure to fool users into clicking links to compromised sites[22]).

Ransomware is now also adjusting itself to the local language of its targets[23] or, conversely, purposely avoiding infecting users in particular territories[24]. Malware authors may do so to avoid attracting attention from law enforcement where they operate, or to target countries and economies where a high ransom is more likely to be paid.

## FAQ ON RANSOMWARE

***How quickly does ransomware encrypt your files after infection?***

*Immediately*; as soon as it can connect to its command and control.

A ransomware will start encrypting as soon as it has enumerated all the drives and searched for its target file types (by extension).

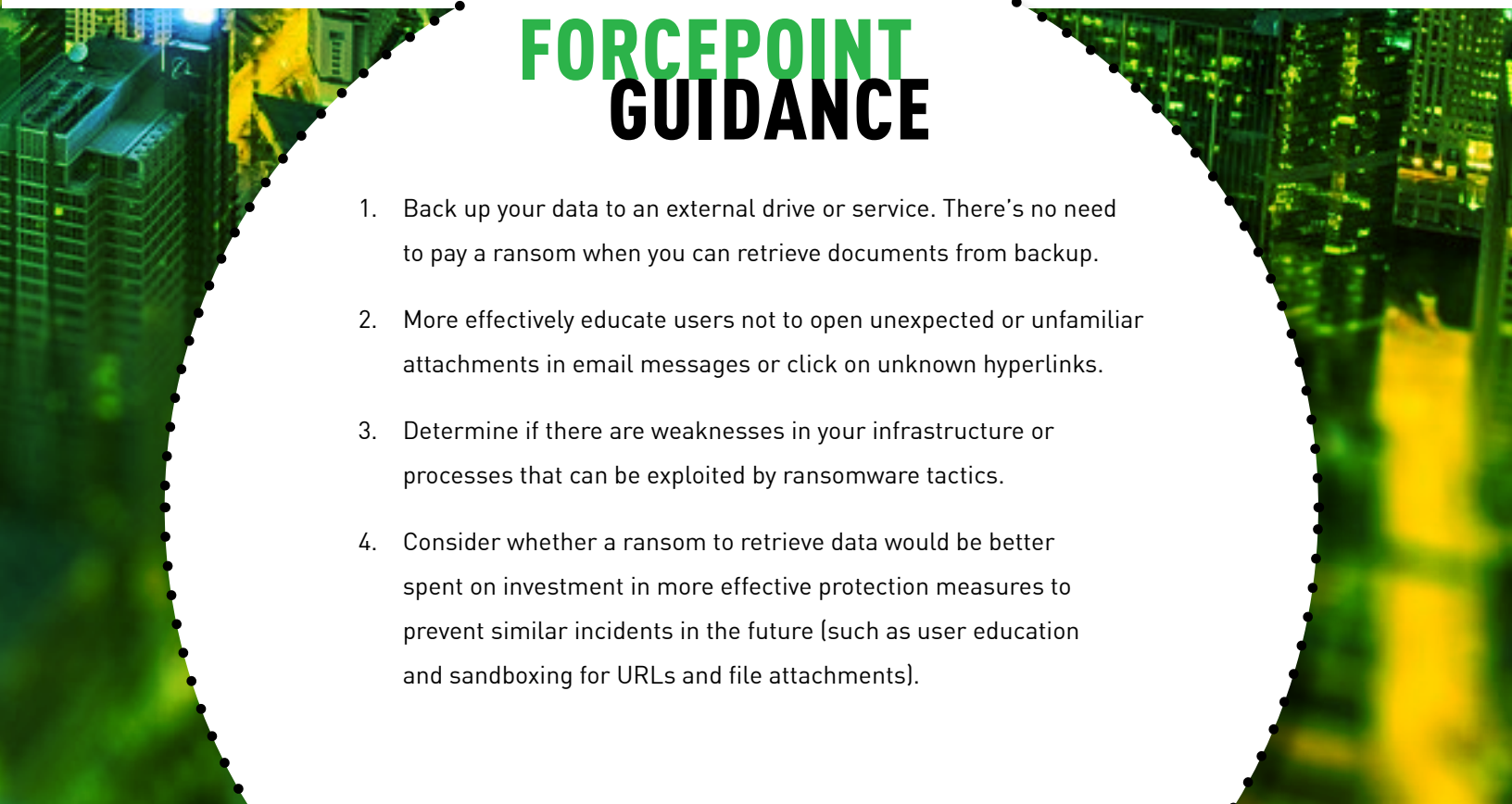
It is worth noting that some ransomware do not need command and control connection to begin encryption, as they can generate the keys themselves and, only once the encryption process is completed, is the key information sent back to command and control. An example of not needing to connect to command and control is CTB-Locker.

***How likely are you to get your files back after paying a ransomware?***

Malware authors are motivated to release files to encourage future victims to pay. However, if the command and control server that stores the key information has been taken down, there will be no way to unencrypt the files, even after paying the ransom.

***What encryption algorithms are used by ransomware?***

Some ransomware variants use symmetric algorithms such as AES-256 (Teslacrypt); others use public-key RSA-2048 (CryptoLocker, CryptoWall). Occasionally, ransomware will use a custom crypto algorithm.



## FORCEPOINT GUIDANCE

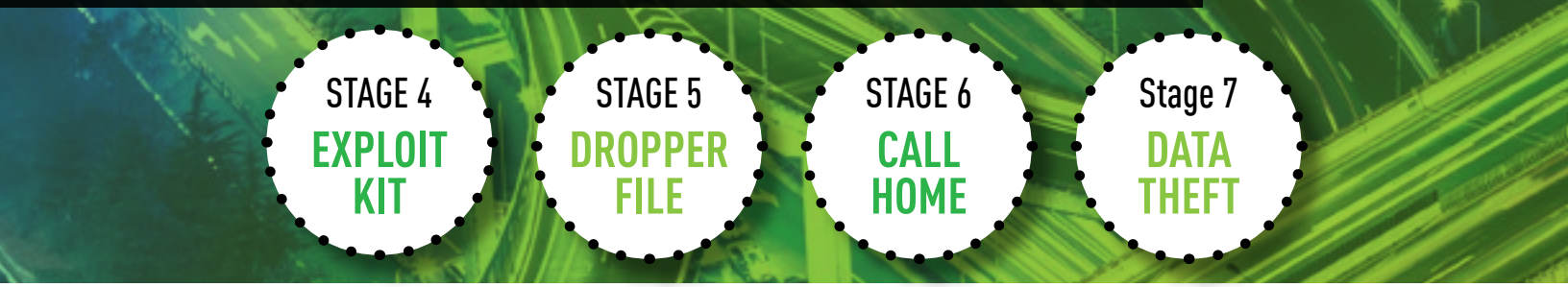
1. Back up your data to an external drive or service. There's no need to pay a ransom when you can retrieve documents from backup.
2. More effectively educate users not to open unexpected or unfamiliar attachments in email messages or click on unknown hyperlinks.
3. Determine if there are weaknesses in your infrastructure or processes that can be exploited by ransomware tactics.
4. Consider whether a ransom to retrieve data would be better spent on investment in more effective protection measures to prevent similar incidents in the future (such as user education and sandboxing for URLs and file attachments).

## EXPOSING EVASION

Next Generation Firewalls (NGFWs) are used to control users and applications while providing very effective identification and mitigation of attacks. They differ from traditional firewalls in that they are application-aware and able to track the state of network traffic flow granularly, among other features. NGFWs are also great tools to provide visibility to the network.

Evasion techniques are used to bypass solution security controls (attackers may combine techniques to create intrusion approach even harder to detect). These tactics are a direct response from malware authors to the visibility afforded to the security administrator by today's best of breed security solutions (including the NGFW).

**FORCEPOINT SECURITY LABS HAS OBSERVED EVASION TECHNIQUES EMPLOYED AT THE FOLLOWING STAGES OF THE THREAT LIFECYCLE:**




Forcepoint Security Labs groups the scenarios in which evasion is employed into three categories: the inbound channel (an attack using evasion to get through network defenses); the outbound channel (an attack payload using evasion to call home); or evasion to access denied resources (for example, by using TOR). These advanced evasion techniques pose a major threat to any organizations data security.

## EVASION IN THE WILD

Advanced evasion techniques combine multiple existing evasion methods to create new, unknown evasion methods; evasion methods that are more successful. Malware and exploit authors have been observed to use a repertoire of evasive methods to manipulate the protocol-level stream and bypass detection.

- **IP Fragmentation**

  IP fragmentation is the process of breaking up a single Internet Protocol (IP) datagram into multiple packets of smaller size, and is specified in RFC 791[25].

  IP fragmentation exploits use the fragmentation protocol within IP as an attack vector by spreading the payload across multiple frames.

- **TCP Segmentation & Out-of-order**

  The Transmission Control Protocol (TCP) is defined in RFC 793[26]. Sequence numbers are used to correctly order segments that may be received out of order.

  TCP segmentation & out-of-order attacks seek to disguise attacks by using this feature of TCP.

- **TCP URG Pointer**

  Also specified in RFC 793 is the TCP Urgent Pointer field (URG). This pointer specifies the presence of urgent, or out-of-band, data which, if included during payload analysis can cause malicious or exploit code to evade detection.

# TOP FIVE PREDICTED USES FOR EVASION IN 2016

## 1. BYPASS ACCESS CONTROL

to gain access into an otherwise unauthorized network

## 2. ATTACK WATERING HOLES

communicating to a water hole in an untraceable manner would not raise the usual alarms and response expected of a network security team

## 3. BOTNET C&C

disguising traffic to/from the command and control enhances resilience and maintains uptime of the botnet

## 4. EXPLOITS (DELIVERY & EXECUTION)

code execution can be obtained by pushing exploits that would otherwise be easily detected

## 5. EXFILTRATE DATA

traffic that is undetectable by the firewall can be used to hide transfer of stolen data

## FORCEPOINT GUIDANCE

1. Ensure that you have suitable technologies deployed that identify and mitigate the use of evasion.
2. Confirm evasion techniques are understood throughout the kill chain. The weakest link principle applies if visibility at any stage in the lifecycle is reduced or is insufficient.

# WEB & EMAIL
## A TWO-PRONGED THREAT

Web and email are the primary communication channels today and remain the primary attack vectors for cybercriminals. Widely acknowledged as the initial entry point into an organization for targeted attacks, the email-attack vector delivered malicious payloads to organizations in 2015, with a focus on Office documents and zip files. Forcepoint Security Labs found malicious content in email increased 250% compared to 2014. Dridex[27] (a strain of banking malware) and various ransomware[28] campaigns were largely responsible for the rise. Malware or malicious web links inside an email can leverage vulnerabilities to compromise machines – and eventually whole networks – via the Internet. Email and web attack vectors had a significant convergence in 2015, with nine out of 10 unwanted emails containing a URL. According to the Identity Theft Resource Center's 2015 Data Breach report[29], accidental email/Internet exposure was 2015's third most common cause of compromised data, underscoring the importance of threat analysis across both attack vectors.

- **91.7%** of unwanted email contains a URL.
- **2.34%** of unwanted email contains an attachment.
- Malicious macros in emails attachments up **44.7%** – macros are used to deliver a further payload hosted on the Web.
- **68.4%** of email is spam (down from 88.5% in 2014).

Forcepoint data found that malicious macros embedded into Microsoft Office file types were a prominent attack-delivery mechanism in 2015. Last year's Threat Report[30] revealed three million malicious macros observed over a thirty-day period at the end of 2014. In performing a similar sampling period at the end of 2015, Forcepoint found more than four million macros, up 44.7% from 2014.

# TOP 5 MALICIOUS FILE TYPES AS EMAIL ATTACHMENTS

1. ZIP ARCHIVE
2. SDOS/WINDOWS PROGRAM
3. TEXT-FILE BASED
4. MICROSOFT WORD 97
5. MHT FORMAT

# TOP 10 COUNTRIES HOSTING MALICIOUS CONTENT

1. UNITED STATES
2. ITALY
3. GERMANY
4. RUSSIA
5. TURKEY
6. IRELAND
7. UNITED KINGDOM
8. FRANCE
9. NETHERLANDS
10. INDONESIA

# TOP 8 COUNTRIES HOSTING PHISHING WEBSITES

1. UNITED STATES*
2. BELIZE
3. HONG KONG
4. BELGIUM
5. UNITED KINGDOM
6. CHILE
7. GERMANY
8. SWEDEN

*The United States hosted more phishing websites than all other top 8 countries combined

# FORCEPOINT GUIDANCE

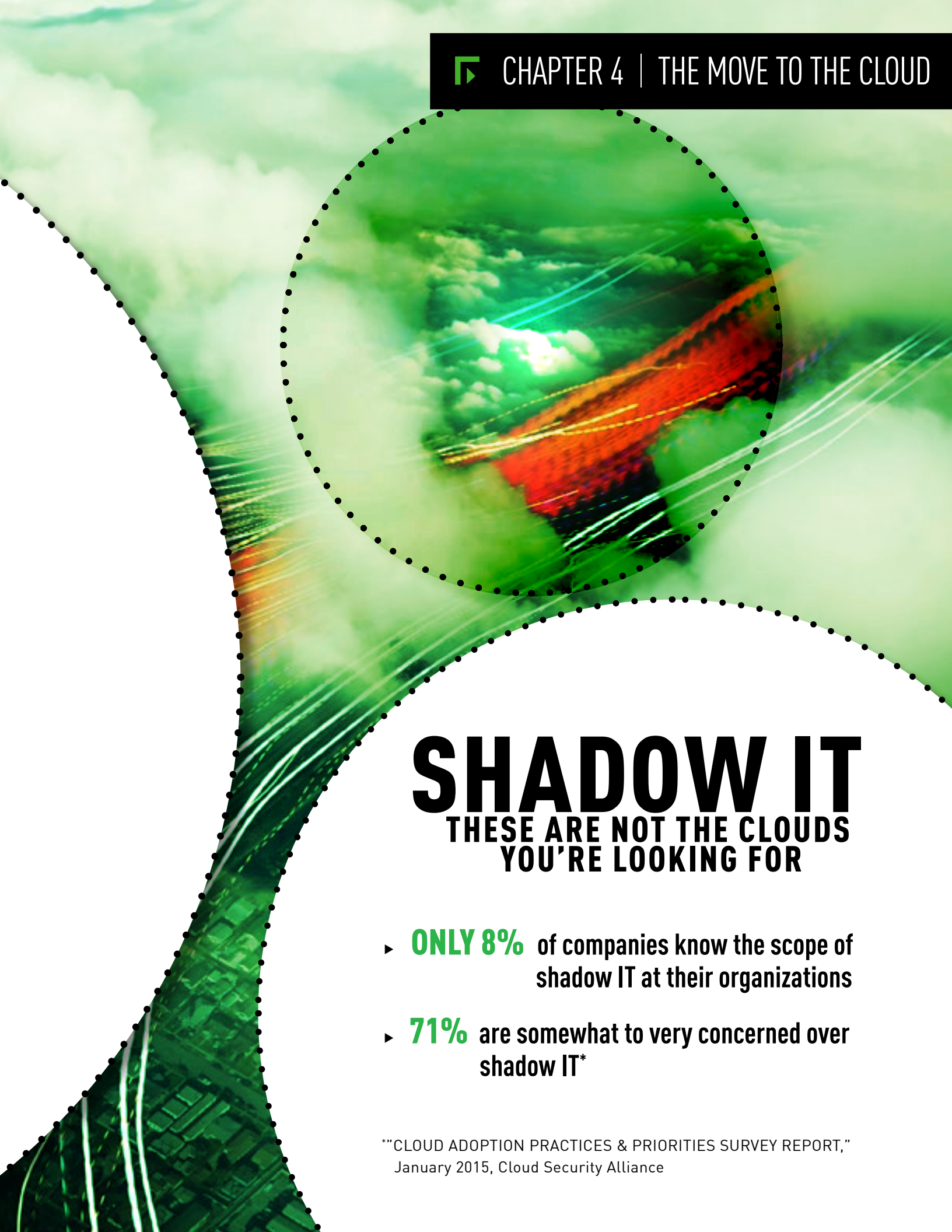
1. Explore security solutions fed by attack analysis from both Web and email attack vectors, which will achieve greater efficacy for each product.
2. Implement a user education/training program that periodically reminds users of the typical ways to identify a malicious email with attachments or URLs likely to trigger a connection to the Web for additional payloads.
3. Consider activating URL sandboxing and file attachment sandboxing technology to prevent users from making bad decisions, or not recognizing a malicious email.

# THE MOVE TO THE CLOUD

More companies are embracing cloud-based technologies for both cost savings and collaboration. Though still a growing market, the benefits of cloud computing in reducing hardware and support needs and offering employees flexibility and speed to complete critical business tasks, has resulted in a gradual but steady shift. In a global survey by Harvard Business Review Analytic Services[31], 85% of respondents said their organizations will be using cloud tools moderately-to-extensively over the next three years.

Though advantageous to enterprise missions in many ways, some organizations have been slower to adopt cloud IT, hindered by concerns that cloud-based applications may be ineffectively secured or may conflict with compliance requirements. More than 60% of organizations indicate "concerns about security" as being the most important reason for deferring cloud adoption[32]. According to Ponemon research[33], difficulty enforcing effective security methods in cloud apps and products, along with uncertainty over whether end-users or cloud providers are responsible for data security in the cloud, fuel concern.

However, resisting cloud adoption may not delay its use. Employees, groups or even whole divisions often migrate to the cloud even if their business has not; bypassing approval or formal integration efforts when outside solutions better address productivity requirements. This creates the possibility for unsanctioned technology to disrupt an organization's security and compliance posture, exposing it to unwanted and unplanned-for risks.



# SHADOW IT

## THESE ARE NOT THE CLOUDS YOU'RE LOOKING FOR

- **ONLY 8%** of companies know the scope of shadow IT at their organizations
- **71%** are somewhat to very concerned over shadow IT*

*"CLOUD ADOPTION PRACTICES & PRIORITIES SURVEY REPORT," January 2015, Cloud Security Alliance

More than 80% of IT decision-makers feel shadow IT poses a risk to IT security, with a third considering it an extremely significant risk and 16% considering it the most significant risk[34]. However, only 34% of those using shadow IT believe it poses a risk to security, with more than half citing that its use allows business departments to be more productive[35]. Unfortunately, when IT can't see data, it also can't adequately protect it, creating the perfect environment for data to be lost or stolen.

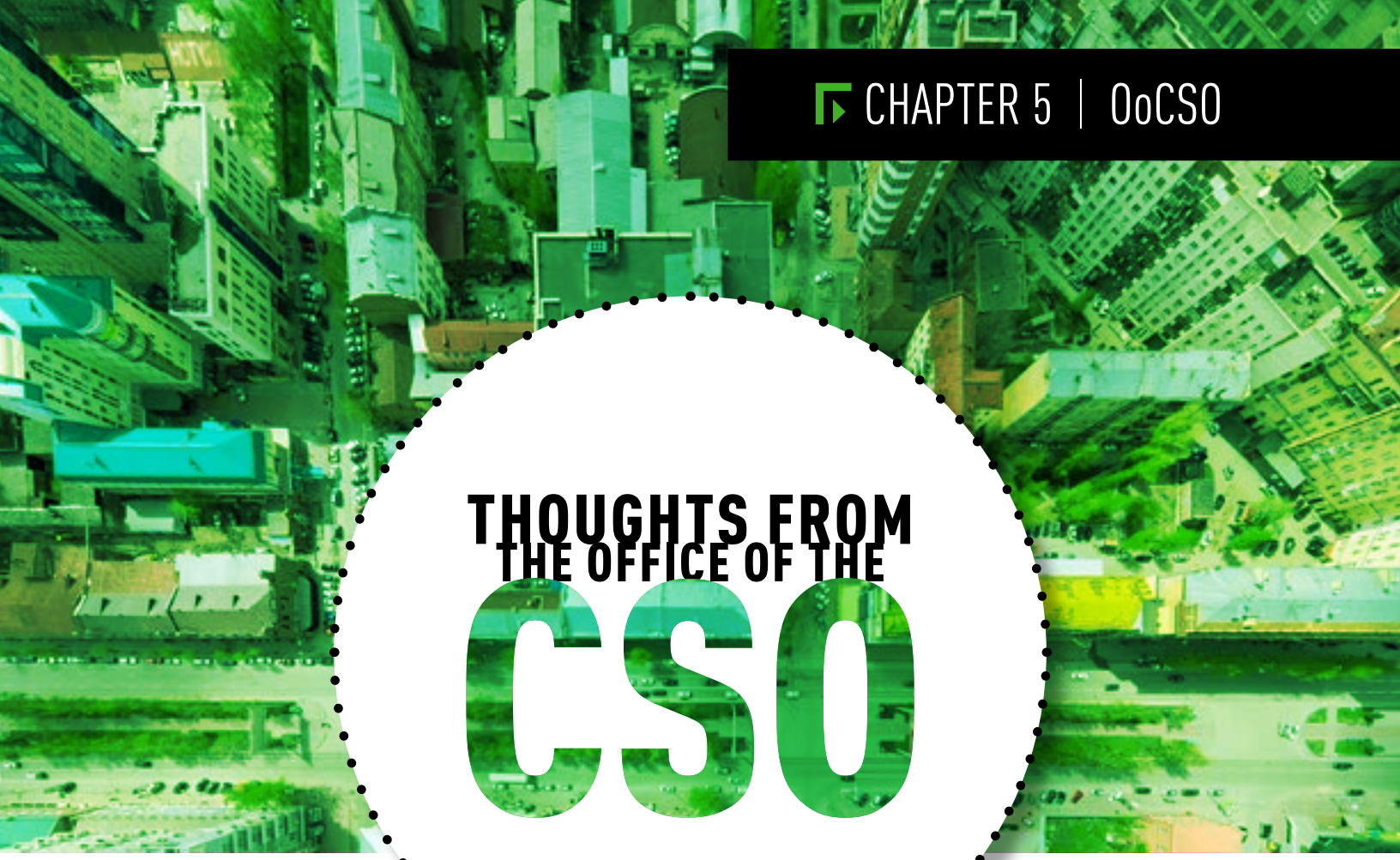
An IDG Enterprise survey[36] found that CIOs believe 2016 will be the first year when more IT services live in the cloud than on premise. Data-centric security and privacy solutions that cover all computing platforms and systems are key to compliance with security and privacy regulations. In addition to data-aware defenses, third party independent assessments, like the CSA STAR Certification[37], can help determine the security of cloud service providers.

## FORCEPOINT GUIDANCE

1. Data Loss Prevention (DLP) solutions and Next Generation Firewalls (NGFW) can help organizations realize the scope of their shadow IT.
2. Once the services and IT entities users are connecting to are known, organizations can either enforce data and usage guidelines, train users, or disable the IT based on their policies.
3. Employees often use shadow IT to think and work outside of the box. Too much control may lead to frustrated users and attempts to bypass restrictions. Consider working with staff to help them be more productive rather than blocking their attempts to innovate outright.

# A NEED FOR CYBER TALENT

**As data continues to move father from perimeter defenses, fostering a cybersecurity workforce capable of protecting information from cyber threats is paramount. Raytheon's annual study Securing Our Future: Closing the Cyber Talent Gap[38], in cooperation with the National Cyber Security Alliance, works to identify the root causes of the cyber talent gap as part of a shared long-term commitment to building a robust talent pipeline.**



# THOUGHTS FROM THE OFFICE OF THE CSO

New business acquisition and merger activity is on the rise, but blending companies increases the complexity in protecting an organization's sensitive data. Given that 84% of the total value of the S&P 500 now consists of intellectual property (IP) and other intangibles[39], making data accessible to the appropriate parties while simultaneously protecting it from loss, theft and misuse is essential. The technology and business processes needed to protect sensitive data and maintain a competitive advantage are an inherent part of mergers, acquisitions and other business propositions. A loss of IP or other data has an immediate effect on reputation, can result in legal and regulatory action and can adversely affect competitive positioning, stock price, and shareholder value. The creation of a blueprint for secure consolidation and management of critical data is indispensable to the successful integration of formerly independent organizations.

## FORMING FORCEPOINT: HOW A CYBERSECURITY ORGANIZATION SAFELY INTEGRATES

On January 14, 2016, a new joint venture built on the integration of Websense, Raytheon Cyber Products and the Stonesoft NGFW business was announced. Known as Forcepoint, this new company was a culmination of nearly a year's worth of business systems integration.

## EVALUATION

Before any data, systems or process integration of Websense, RCP and Stonesoft could begin, an evaluation of each company's internal and external security posture was necessary. A third-party performed penetration testing and dug into the dark web for any chatter around vulnerabilities or ongoing hacks of which the companies may not have been aware. Security staff members were asked to detail their security programs – including user education, vulnerability management, data classification and flow, and administration of access controls. This security due diligence confirmed the policies in place were actually in practice and highlighted potential disparities, for instance where one organization had more strict security requirements that required the other organization(s) be brought into alignment.

## ASSESSMENT

Following the completion of our own security evaluation, an evaluation of the soon-to-be-combined entities' networks for threats began. In this instance, a custom tool was deployed to detect and report on suspicious activity and to assess network health on which guidance could then be developed. Often this guidance was as simple as patching a server or updating certificates.

**"UNDERSTANDING WHAT DATA SETS WERE IMPORTANT TO THE COMBINED COMPANY, AND IDENTIFYING WHERE THEY WERE AND WHAT CONTROLS WERE IN PLACE TO PROTECT THEM GAVE US A BETTER VIEW OF WHAT RISKS WE NEEDED TO ADDRESS."**

**-DAVE BARTON**
**FORCEPOINT CISO**

At the same time, RCP and Websense's "crown jewels" (IP, financial data, etc.) were identified and appropriate communications were developed to combat targeted threats and malicious activity (e.g. spam and phishing attacks) common when companies consolidate. Forcepoint received what appeared to be (but were not) legitimate emails from Raytheon requesting sensitive data and financial information, but thanks to the proactive measures already put in place, they did not fall victim to these attempted malicious intrusions.

## ACTION

Prior to announcement day, a static and dynamic testing of code was performed on all source code of the newly combined entities. This was done to determine code vulnerabilities that may not have been known or disclosed.

## ANNOUNCEMENT DAY

While networks may not have been connected to or communicating directly with one another, there were still steps to take to ensure that the months of integration to follow proceeded smoothly. First, communication to all employees regarding data access policies was performed, especially around the handling of critical or sensitive data throughout the transition. Employees also needed to understand that proprietary pricing models and other competitive information could not be shared until the acquisition was formally completed. This proactive end-user communication was key to protecting assets and information through the M&A process.

## A NEW LEVEL OF STRESS TESTING

Raytheon's Cyber Operations, Development and Evaluation (CODE) Center is a state-of-the-art cyber range used to test existing and future mission-critical systems against cyber-attacks. The CODE Center is part of Raytheon's network of cyber innovation and demonstration centers around the world that help customers rapidly pinpoint solutions to their most difficult and complex cyber challenges.

Second, an increase in the monitoring of company networks was instituted, using data theft protection tools with a focus on administrator account use and the attempted transfer of sensitive data over email or the Internet. As alerts came, the IT, Security and Development teams began remediation of identified threats and vulnerabilities. This way, any remaining issues, or gaps and differences in security policies, could be fixed before networks were connected.

Never an entirely simple process, the Forcepoint integration was more complex than most. At the same time the Websense and RCP joint venture was being completed, we acquired Stonesoft, and many of the same steps taken to ensure a smooth and secure integration had to be revisited. In addition, the shift to a new brand identity required IT to move employees, their workstations and data to a new domain – Forcepoint.com. All of this took place while working to prevent our new brand and name leaking prior to the formal announcement. This was achieved by deploying our own tools that restricted the ability to share data containing the new name and other brand information outside of the internal network. Even with these potential stumbling blocks, the planning and work preceding them meant that integration continued apace and minor challenges remediated and mitigated prior to the merger closing.

***Security involvement is a must in any M&A activity. There are too many potential risks during mergers that will not be discovered without significant involvement of security experts.***


# CONCLUSION

The Forcepoint 2016 Global Threat Report confirms a notable shift in the nature of attacks this past year. Often the domain of technical debates, alerts and "IT" issues, cybersecurity today is ultimately a top, mainstream risk and consequence issue for corporate officers, elected officials, government authorities and leaders everywhere.

The actions of an opportunistic ransomware gang, a careless employee or well-conceived advanced attack mechanism can bring swift and dire impact – in some cases threatening the very stability of organizations' finances, mission capacity and priceless brands. Still, not every attack is an existential threat – in an era when any Internet-connected office or object can be bombarded with attacks at any given time.

We believe a new, holistic approach is needed, giving enterprises a 360-degree view with real-time analysis and meaningful alerts that anticipate and communicate the threat landscape and its implications so that customers can act quickly to defeat even the most determined adversary. Forcepoint's Security Labs, Special Investigations and Office of the CSO teams continue to apply their expertise on identifying worldwide threats and attack activity.  With guidance along the way, together, we can move ***Forward Without Fear***.

# CITATIONS


1. Ponemon Institute LLC. " 2015 Cost of Cyber Crime Study: Global." October 2015. https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf

2. Ponemon Institute LLC. "Privileged User Abuse & The Insider Threat." May 2014. http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_257010.pdf

3. Anderson, Ed; Nag, Sid, and Gartner, Inc. "Forecast Overview: Public Cloud Services, Worldwide, 2016 Update." February 17, 2016. https://www.gartner.com/doc/3214717?ref=SiteSearch&sthkw=security%20concerns%20cloud%20adoption&fnl=search&srcId=1-3478922254

4. Shey, Heidi. "Understand The State Of Data Security And Privacy: 2015 To 2016."Forrester Research, Inc., 8 Jan. 2016. https://www.forrester.com/report/Understand+The+State+Of+Data+Security+And+Privacy+2015+To+2016/-/E-RES117447

5. Mearian, Lucas. "Government Tests Show Security's People Problem." Computerworld. July 6, 2011. http://www.computerworld.com/article/2510014/security0/government-tests-show-security-s-people-problem.html

6. Ponemon Institute LLC. "Ponemon Study: The Unintentional Insider Risk in United States and German Organizations." July 30, 2015. http://www.raytheoncyber.com/spotlight/ponemon/index.html

7. Bank Director. "Bank Director's 2016 Risk Practices Survey." March 21, 2016. http://www.bankdirector.com/download_file/view_inline/4996

8. Identity Theft Resource Center. "2015 Data Breaches | ITRC Surveys & Studies | ID Theft Blog." January 25, 2016. http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html

9. Forrester Research, Inc. "Global Business Technographics® Security Survey, 2015." July 2015. https://www.forrester.com/Global Business Technographics Security Survey 2015/-/E-sus2957

10. Forrester Research, Inc. " Global Business Technographics® Devices And Security Workforce Survey, 2015." August 2015. https://www.forrester.com/Global+Business+Technographics+Devices+And+Security+Workforce+Survey+2015/-/E-sus2971

11. Ponemon Institute LLC. "Privileged User Abuse & The Insider Threat." May 2014. http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_257010.pdf

12. Litan, Avivah, and Gartner, Inc. "Best Practices and Success Stories for User Behavior Analytics." March 4, 2015. https://www.gartner.com/doc/2998124/best-practices-success-stories-user

13. Forrester Research, Inc. "Global Business Technographics® Security Survey, 2015." July 2015. https://www.forrester.com/Global Business Technographics Security Survey 2015/-/E-sus2957

14. Forcepoint LLC. "Cyber Dwell Time and Lateral Movement THE NEW CYBERSECURITY BLUEPRINT." https://www.forcepoint.com/resources/white-papers/cyber-dwell-time-and-lateral-movement

15. Forcepoint LLC. "Cyber Dwell Time and Lateral Movement THE NEW CYBERSECURITY BLUEPRINT." https://www.forcepoint.com/resources/white-papers/cyber-dwell-time-and-lateral-movement

16. Vanian, Jonathan. "Hollywood Hospital Pays Off Hackers To Restore Computer System." February 18, 2016. http://fortune.com/2016/02/18/hollywood-hospital-hackers-computer-system/

17. Forcepoint Security Labs and Forcepoint LLC. "Locky Ransomware - Encrypts Documents, Databases, Code, BitCoin Wallets and More..." February 19, 2016. https://blogs.forcepoint.com/security-labs/locky-ransomware-encrypts-documents-databases-code-bitcoin-wallets-and-more

18. Forcepoint Security Labs and Forcepoint LLC. "Locky's New DGA - Seeding the New Domains [RUSSIA UPDATE: 26/FEB/16]." February 25, 2016. https://blogs.forcepoint.com/security-labs/lockys-new-dga-seeding-new-domains

19. @Forcepointsec Twitter handle. March 22, 2016. Tweet, https://twitter.com/Forcepointsec/status/712316915687948289

20. Winton, Richard. "Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating." Los Angeles Times. February 18, 2016. http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

# CITATIONS


21. Vijayan, Jai. "With $325 Million In Extorted Payments CryptoWall 3 Highlights Ransomware Threat." Dark Reading. October 29, 2015. http://www.darkreading.com/endpoint/with-$325-million-in-extorted-payments-cryptowall-3-highlights-ransomware-threat/d/d-id/1322899

22. Forcepoint LLC (formerly Websense). "The Seven Stages of Advanced Threats." https://www.websense.com/assets/pdf/understanding-the-cyber-attack-infographic.pdf

23. Forcepoint Security Labs and Forcepoint LLC. "TorrentLocker is Back and Targets Sweden & Italy." March 15, 2016. https://blogs.forcepoint.com/security-labs/torrentlocker-back-and-targets-sweden-italy

24. Forcepoint Security Labs and Forcepoint LLC. "Locky's New DGA - Seeding the New Domains [RUSSIA UPDATE: 26/FEB/16]." February 25, 2016. https://blogs.forcepoint.com/security-labs/lockys-new-dga-seeding-new-domains

25. Information Sciences Institute; University of Southern California. "DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION." INTERNET PROTOCOL, September 1981. https://tools.ietf.org/html/rfc791

26. Information Sciences Institute; University of Southern California. "DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION." TRANSMISSION CONTROL PROTOCOL, September 1981. https://tools.ietf.org/html/rfc793

27. Forcepoint Security Labs and Forcepoint LLC. "Dridex Down Under." November 5, 2015. https://blogs.forcepoint.com/security-labs/dridex-down-under

28. Forcepoint Security Labs and Forcepoint LLC. "Accounts Payable in the Czech Republic Targeted by Dridex." August 4, 2015. https://blogs.forcepoint.com/security-labs/accounts-payable-czech-republic-targeted-dridex

29. Identity Theft Resource Center. "2015 Data Breaches | ITRC Surveys & Studies | ID Theft Blog." January 25, 2016. http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html

30. Forcepoint LLC. "Websense 2015 Threat Report." April 8, 2015. https://www.websense.com/content/websense-2015-threat-report.aspx

31. Harvard Business Review. "How the Cloud Looks from the Top: Achieving Competitive Advantage In the Age of Cloud Computing." 2011. https://hbr.org/resources/pdfs/tools/16700_HBR_Microsoft%20Report_LONG_webview.pdf

32. Anderson, Ed; Nag, Sid, and Gartner, Inc. "Forecast Overview: Public Cloud Services, Worldwide, 2016 Update." February 17, 2016. https://www.gartner.com/doc/3214717?ref=SiteSearch&sthkw=security%20concerns%20cloud%20adoption&fnl=search&srcId=1-3478922254

33. Ponemon Institute LLC. "The Challenges of Cloud Information Governance: A Global Data Security Study." October 2014. http://www2.gemalto.com/cloud-security-research/SafeNet-Cloud-Governance.pdf

34. VansonBourne. "Shadow IT ITDMs Data Summary." p. 34. July 11, 2014. http://www.vansonbourne.com/files/1914/1225/3447/VB-Shadow_IT-ITDMs-Data-Summary.pdf

35. VansonBourne. "Shadow IT BDM Data Summary." p. 24. July 22, 2014. http://www.vansonbourne.com/files/7614/1225/3401/VB-Shadow_IT-BDM-Data-Summary.pdf

36. IDG Enterprise. "2015 IDG enterprise cloud computing survey." November 17, 2015. http://www.idgenterprise.com/resource/research/2015-cloud-computing-study/

37. CAS Cloud Security Alliance. https://cloudsecurityalliance.org/star/certification/

38. Raytheon Company, "Securing Our Future: Closing the Cyber Talent Gap." October 19, 2015. http://raytheon.mediaroom.com/2015-10-26-Many-more-men-than-women-are-drawn-to-cybersecurity-careers-and-the-gap-is-widening-dramatically-new-survey-says

39. Ocean Tomo LLC. "Intangible Asset Market Value Study." March 4, 2015. http://www.oceantomo.com/2015/03/04/2015-intangible-asset-market-value-study/

# WHO IS FORCEPOINT?

Forcepoint exists to help organizations move their business forward. Our goal is to enable our customers' need to adopt transformative business technologies safely in a world where cloud services, hybrid architectures, and mobile workforces are the norm. With the perimeter-based security model of past obsolete, organizations need solutions that put security close to data wherever it goes – across multiple environments and devices, from network to endpoint and from mobile to cloud. Regardless of region, business vertical or size, the threats our customers face are becoming ever more challenging, and resource-strapped security teams are struggling to keep up. The Forcepoint platform enables organizations to automate the routine parts of security, eliminate the patchwork of point products, and uncover true insights like those included in this, our annual Threat Report.

## THREATSEEKER® INTELLIGENCE CLOUD

Threatseeker Intelligence Cloud was developed to provide Forcepoint visibility into the very latest threats. Processing up to five billion data points per day collected from multiple inputs in a 155 countries, Threatseeker helps us protect our customers, working behind-the-scenes 24x7x365 to allow them to do business safely. Forcepoint experts interact with Threatseeker daily, gathering the accurate, real-time threat intelligence and insights featured in our annual threat, industry drill-down and predictions reports.

FORCEPOINT
POWERED BY Raytheon