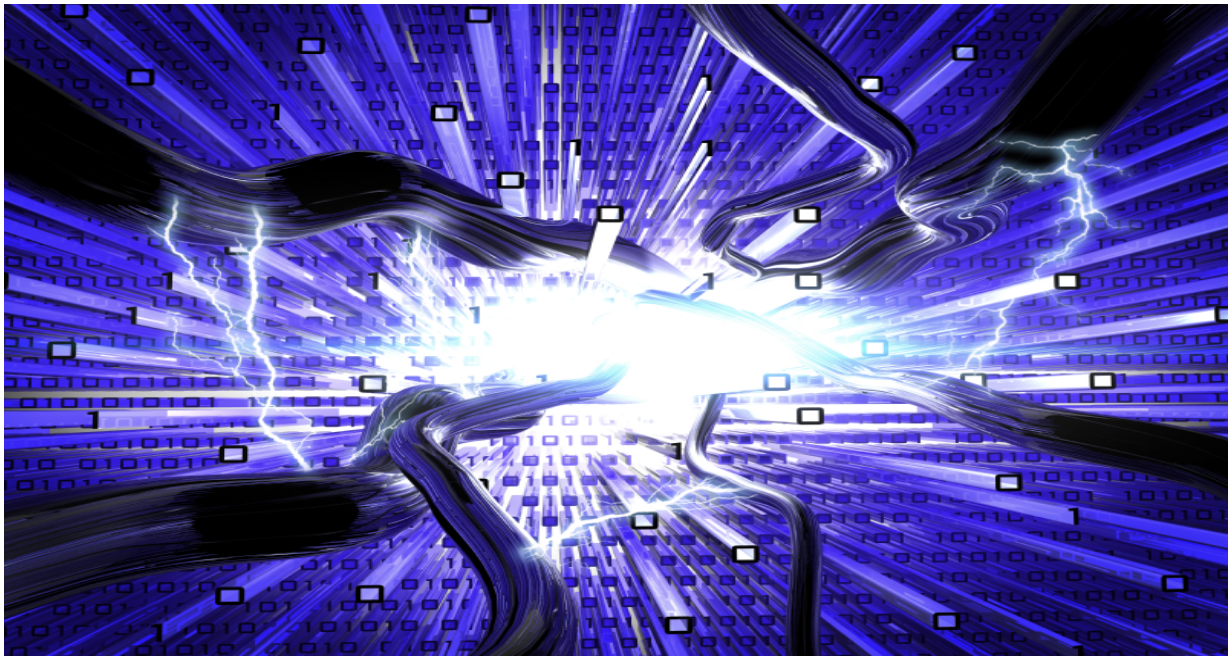


Hidden Threats in Encrypted Traffic: A Study of North America & EMEA

Sponsored by A10

Independently conducted by Ponemon Institute LLC

Publication Date: May 2016

Hidden Threats in Encrypted Traffic
A Study of North America & EMEA[1]
Ponemon Institute, May 2016

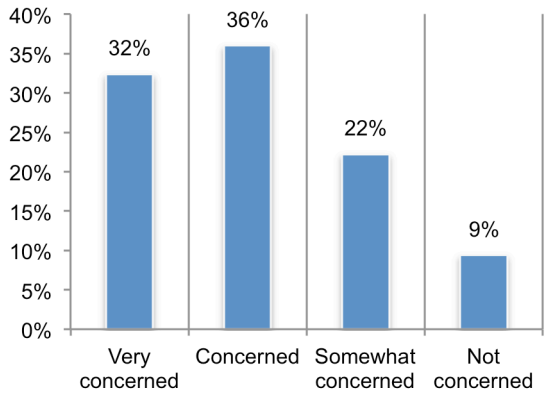
Part 1. Introduction

Ponemon Institute is pleased to present the results of *Hidden Threats in Encrypted Traffic: A Study of North America & EMEA,* sponsored by A10. The purpose of this study is to highlight the challenges organizations face in preventing and detecting web-based attacks.

The hidden threat in encrypted traffic exists because SSL encryption hides everything as intended, but security tools cannot inspect encrypted traffic. While SSL encryption is crucial to protecting data in transit during web transactions, email communications and the use of mobile apps, data encrypted with this common method can sometimes pass uninspected through almost all the components of an organization's security framework—both inbound and outbound.

We surveyed 1,023 IT and IT security practitioners in North America and EMEA who are involved in preventing and/or detecting web-based attacks and familiar with the organization's network traffic inspection. Participants in this research have acknowledged the hidden threat. In the past 12 months, 80 percent of respondents say their organizations have been the victim of a cyber attack or malicious insider. Further, 41 percent say these attacks have used encryption to evade detection.

Figure 1. How concerned are you that encrypted communications will leave your network vulnerable to hidden threats?



The threat is expected to worsen. The majority of respondents (54 percent of respondents) believe in the next 12 months network attackers will increase their use of encryption to evade detection and bypass controls. As shown in Figure 1, 68 percent of respondents (32 percent + 36 percent) are concerned that encrypted communications will leave their network vulnerable to hidden threats that are able to bypass existing security solutions by hiding in SSL traffic.

The following are key takeaways from the research.

Organizations are not prepared to address the problem of malware hiding inside encrypted SSL traffic. Seventy-five percent of respondents say compromised insider credentials due to malware hiding inside encrypted SSL traffic could cause a data breach. However, most companies believe they are not able to do this. Only 36 percent of respondents believe their company could prevent costly data breaches and the loss of intellectual property by detecting SSL traffic that is malicious. Companies also risk non-compliance as well. Sixty-two percent of respondents agree the inability of their company's current security infrastructure to inspect encrypted traffic compromises the ability to meet existing and future compliance requirements.

What are the problems with existing approaches to minimizing web-based attacks? Only 36 percent of respondents say they are able to eliminate the blind spot in corporate defenses by

[1] North America includes Canada and the United States. EMEA countries include Denmark, France, Germany, Italy, Saudi Arabia, South Africa, Spain, Sweden, Turkey, United Arab Emirates and United Kingdom.

decrypting SSL traffic at high speeds. Fifty-three percent of respondents say their security solutions are collapsing under growing SSL bandwidth demands and SSL key lengths.

Encryption of inbound and outbound web traffic is expected to increase over the next 12 months. Today, an average of 39 percent of inbound web traffic is encrypted and this is expected to increase to 45 percent of inbound web traffic. An average of 33 percent of outbound web traffic is encrypted today and is expected to increase to an average of 41 percent.

Decryption of web traffic to detect attacks, intrusions and malware will increase over the next 12 months. Thirty-eight percent of respondents currently decrypt web traffic. However, 51 percent of respondents who report their organizations are not decrypting say they will implement traffic decryption over the next 12 months.

Why companies do not decrypt web traffic. The primary reasons for not decrypting web traffic are due to a lack of enabling security tools, insufficient resources and performance degradation (47 percent, 45 percent and 45 percent of respondents, respectively). Companies that inspect decrypted traffic primarily use a commercial platform that utilizes deep packet inspection (53 percent of respondents), a commercial platform that utilizes meta data (44 percent of respondents) or homegrown traffic monitoring systems (35 percent of respondents).

Inspection of SSL traffic is considered essential or very important by 57 percent of respondents. Respondents were asked to identify the features essential or very important to SSL inspection tools. The two features considered essential or very important are the secure management of SSL certificates and keys (79 percent of respondents) and scale to meet current and future SSL performance demands (68 percent of respondents).

Despite the importance of a SSL decryption solution, 61 percent of respondents say lack of performance is the biggest barrier to implementing such a solution. Other barriers are not having the right tools and lack of in-house expertise. Eighty-three percent of respondents say decrypting SSL traffic during the inspection process results in performance degradation.

Part 2. Key findings

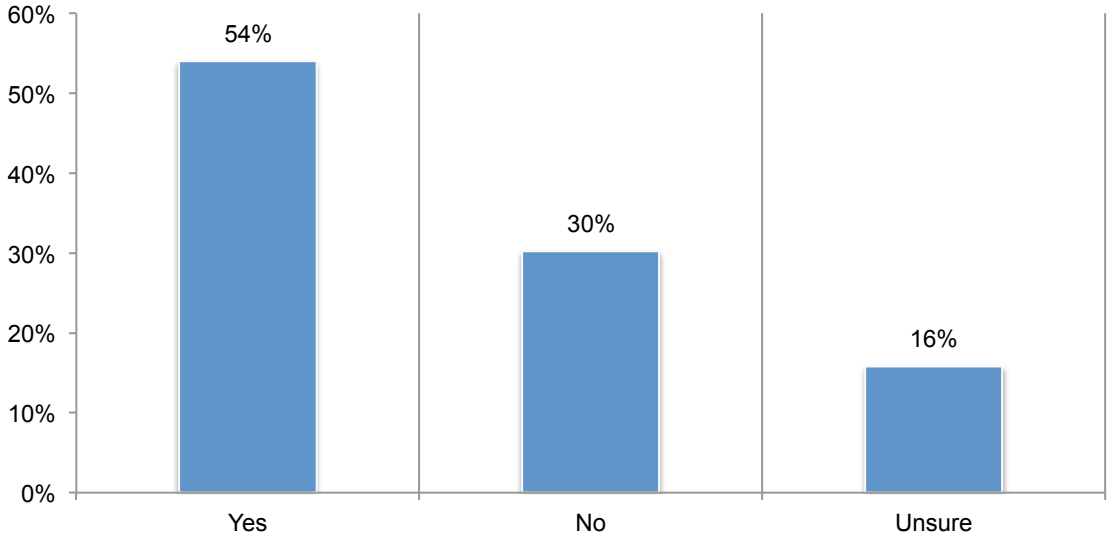
In this section, we provide a deeper analysis of the research findings. The complete audited findings are presented in the appendix of this report. We have organized the report according to the following main topics:

- The hidden threats in encrypted traffic
- The inability to stop hidden threats
- The importance of SSL inspection tools

The hidden threats in encrypted traffic

Attackers have used encryption to evade detection. In the past 12 months, 80 percent of respondents say their organizations have been the victim of a cyber attack or malicious insider and 41 percent of these attacks have used encryption to invade detection. As shown in Figure 1, the threat is expected to become more pervasive. Fifty-four percent of respondents say they think network attackers will increase their use of encryption to evade detection and bypass controls.

Figure 2. In the next 12 months, will network attackers increase their use of encryption?

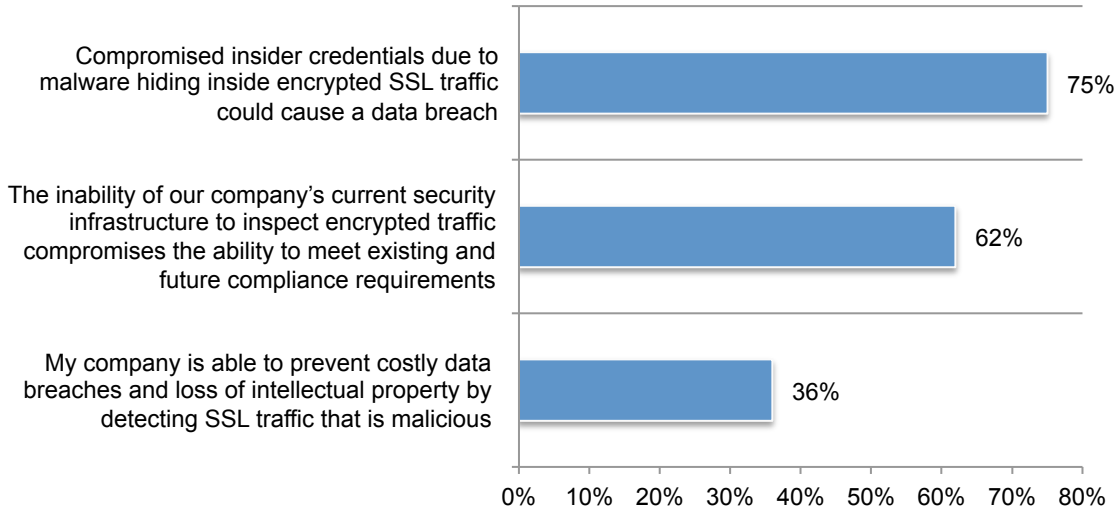


Organizations are not prepared to address the problem of malware hiding inside encrypted SSL traffic. Even with all the usual enterprise security practices in place, monitoring tools can only see the destinations and, in some cases, the host name within the unencrypted portion of the SSL handshake. The organizations cannot see the full path, content type or content itself. That can be a problem when the command and control channels or the exfiltration of sensitive data are hidden by encryption.

As shown in Figure 3, 75 percent of respondents say compromised insider credentials due to malware hiding inside encrypted SSL traffic could cause a data breach. However, most companies do not believe they are able to do this. Only 36 percent of respondents believe their company could prevent costly data breaches and the loss of intellectual property by detecting SSL traffic that is malicious.

Companies also risk non-compliance as well. Sixty-two percent of respondents agree the inability of their company's current security infrastructure to inspect encrypted traffic compromises the ability to meet existing and future compliance requirements.

Figure 3. Perceptions about the risk of data breaches and non-compliance
Unsure, disagree and strongly disagree responses combined



Despite the recognition of these threats, respondents admit their organizations are not prepared to resolve these attacks. We asked respondents to rank the likelihood of specific attacks occurring and the ability to resolve those attacks.

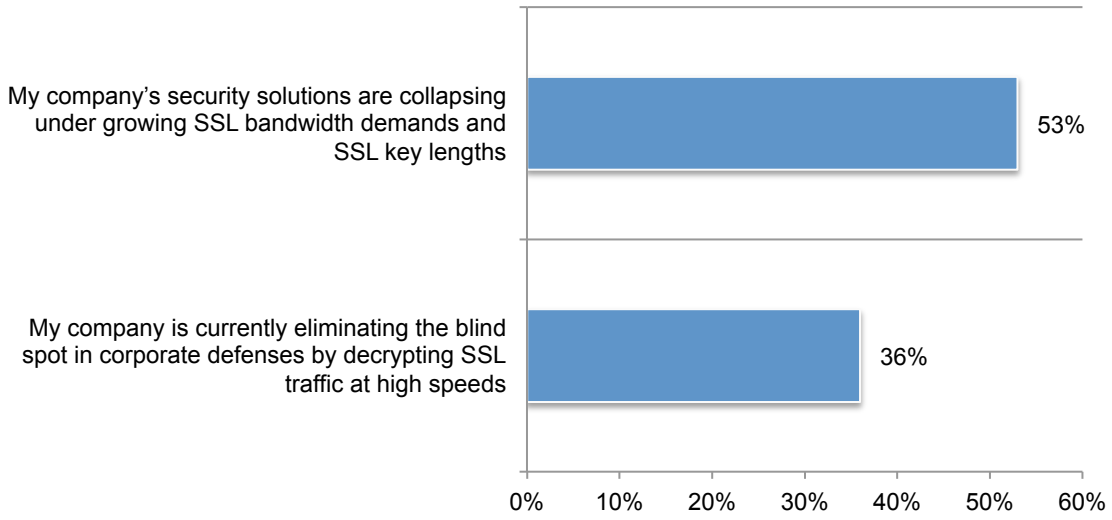
Table 1 describes the attacks and the huge gaps between the likelihood of the attack and the ability to remediate the attack. For example, in the first scenario 79 percent of respondents say it is very likely their organization will experience such an attack. However, only 17 percent say they would be able to resolve the attack.

Table 1. Summary of five attacks	Highly likely we will have this attack	We would be able to resolve the attack
S1. The attacker makes phishing threats look even more legitimate and even informed recipients think the SSL usage makes it secure. Clicking the link, however, takes them to an SSL server loaded with malware that infects the client because the malware traffic is encrypted and not recognized by an IPS.	79%	17%
S2. An attacker sends an encrypted stream of protected, sensitive and other critical data outbound through the firewall over "normal" ports, such as 443 or 80, which the firewall is tuned to accept because they are approved ports.	78%	30%
S3. A number of malware families use encryption to hide network information, including passwords or sensitive data they are sending out to SSL servers. The encryption blinded the monitoring/inspection systems to these internal network activities.	74%	16%
S4. An attacker would obfuscate malware communications when a worm, virus or botnet "phones home" to send stolen data to a master computer or download instructions or more malicious code.	66%	26%
S5. Through cross-site scripting, attackers steal cookies that can be used for a number of things, including account or session hijacking, changing user settings, cookie poisoning and/or false advertising. All of this can be accomplished while hiding within SSL-encrypted traffic.	62%	19%

The inability to stop hidden threats

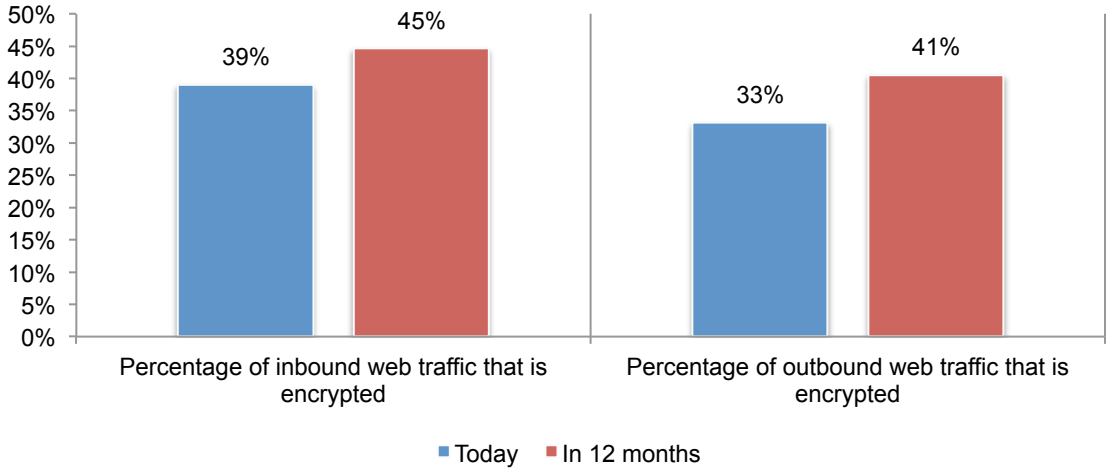
What are the problems with existing approaches to minimizing web-based attacks? According to Figure 4, 53 percent of respondents say their security solutions are collapsing under growing SSL bandwidth demands and SSL key lengths. Only 36 percent of respondents say they are able to eliminate the blind spot in corporate defenses by decrypting SSL traffic at high speeds.

Figure 4. Perceptions about minimizing web-based attacks
Strongly agree and agree response combined



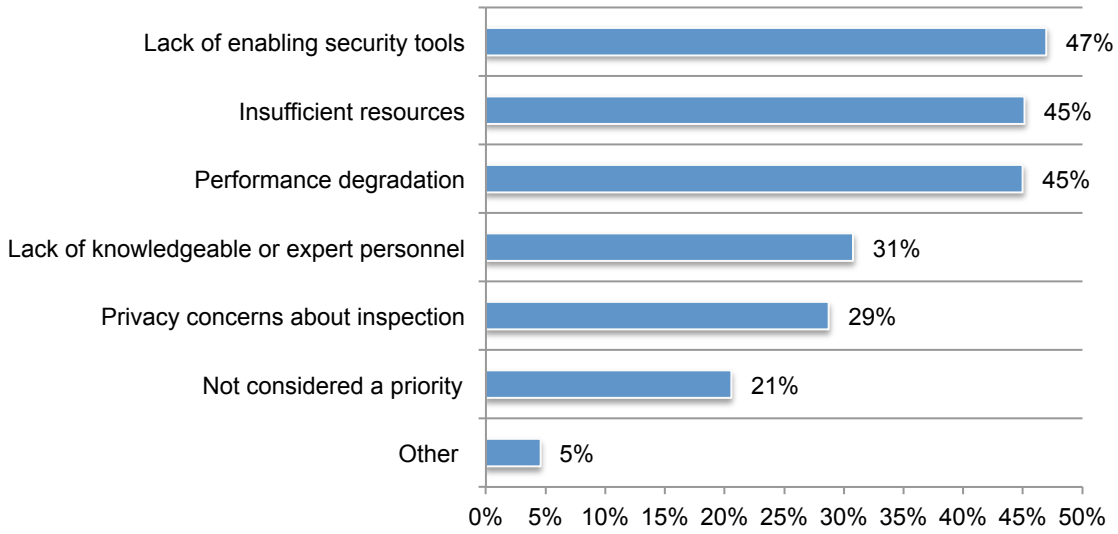
Encryption of inbound and outbound web traffic is expected to increase over the next 12 months. As shown in Figure 5, today, an average of 39 percent of inbound web traffic is encrypted and this is expected to increase to 45 percent of inbound web traffic. An average of 33 percent of outbound web traffic is encrypted today and is expected to increase to an average of 41 percent.

Figure 5. What percentage of inbound and outbound web traffic is encrypted today and in the next 12 months?
Extrapolated values



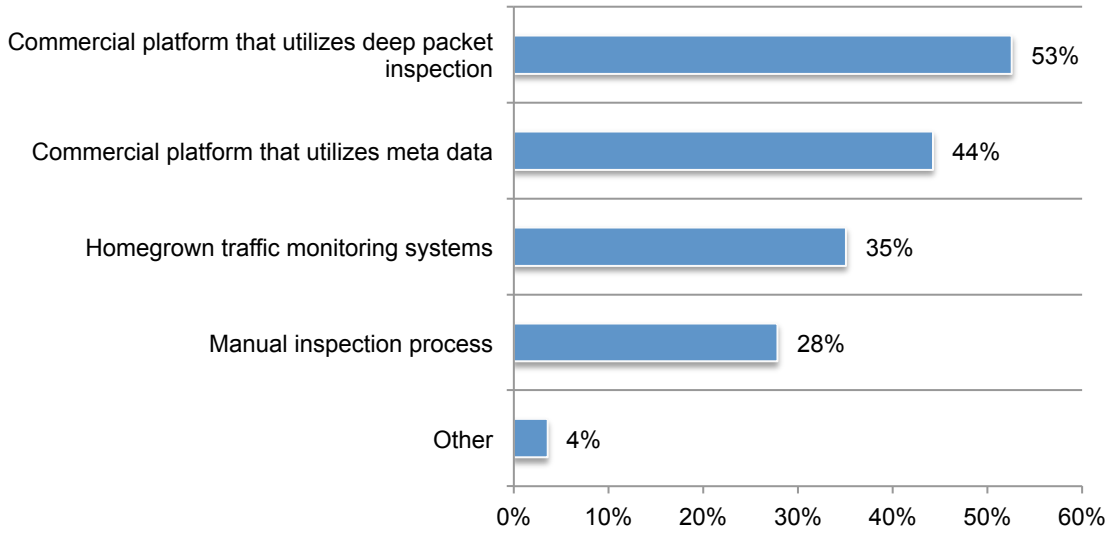
Decryption of web traffic to detect attacks, intrusions and malware will increase over the next 12 months. Thirty-eight percent of respondents currently decrypt web traffic. However, 51 percent of respondents who report their organizations are not decrypting say they will implement traffic decryption over the next 12 months. According to Figure 6, the primary reasons for not decrypting web traffic are due to a lack of enabling security tools, insufficient resources and performance degradation (47 percent, 45 percent and 45 percent of respondents, respectively).

Figure 6. Reasons for not inspecting decrypted web traffic
More than one response permitted



How companies inspect decrypted traffic. Companies that inspect decrypted traffic primarily use a commercial platform that utilizes deep packet inspection (53 percent of respondents), a commercial platform that utilizes meta data (44 percent of respondents) or homegrown traffic monitoring systems (35 percent of respondents), as shown in Figure 7.

Figure 7. How does your company inspect decrypted traffic?
More than one response permitted



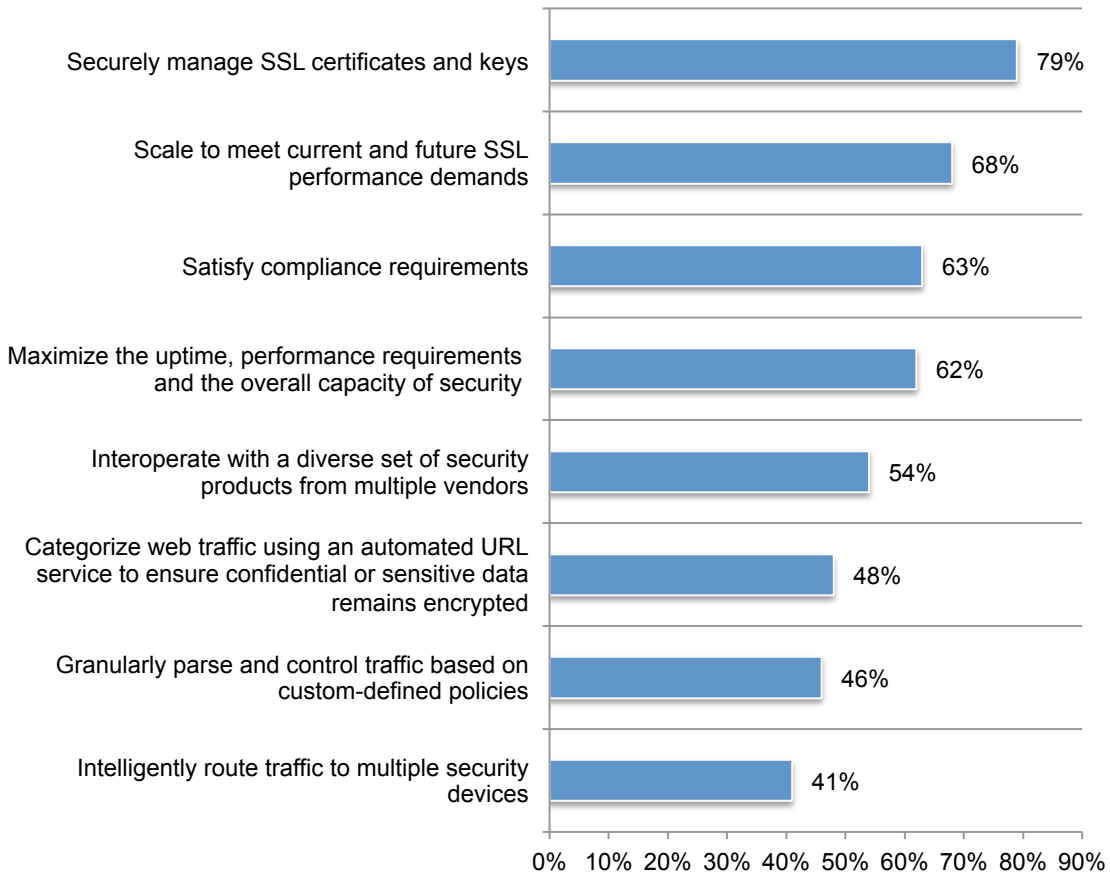
The importance of SSL encryption tools

Inspection of SSL traffic is considered essential or very important by 57 percent of respondents. Respondents were asked to identify the features essential or very important to SSL inspection tools.

As shown in Figure 8, The features considered essential or very important are: the secure management of SSL certificates and keys (79 percent of respondents), scale to meet current and future SSL performance demands (68 percent of respondents), satisfy compliance requirements (63 percent of respondents), maximize the uptime, performance requirements and the overall capacity of security infrastructure (62 percent of respondents) and interoperate with a diverse set of security products from multiple vendors (54 percent of respondents).

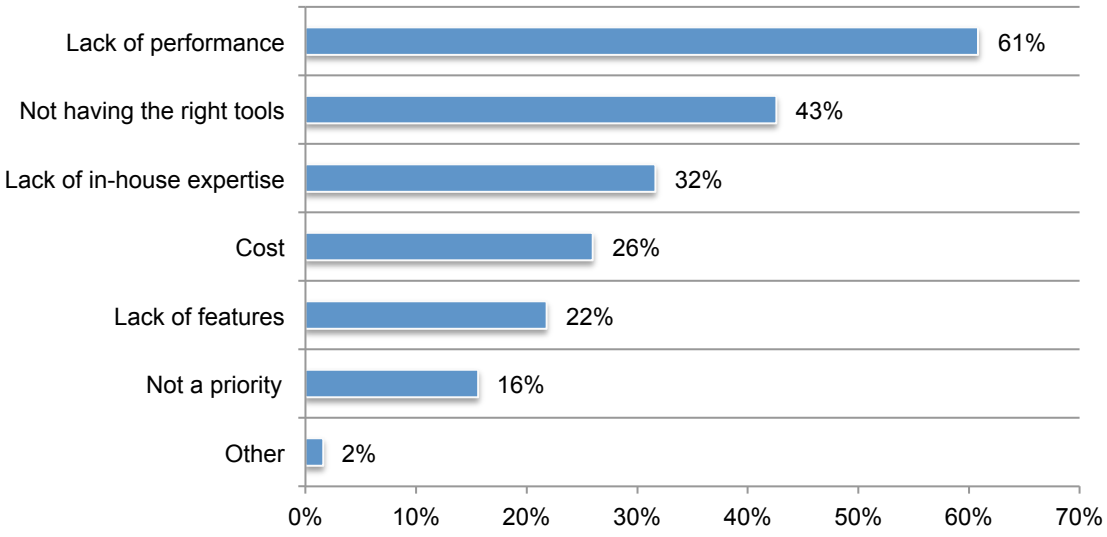
Features considered less important are: categorizing web traffic using an automated URL service to ensure confidential or sensitive data remains encrypted (e.g. bypass sensitive traffic to satisfy regulatory requirements) (48 percent of respondents), granularly parse and control traffic-based on custom-defined policies (46 percent of respondents) and intelligently route traffic to multiple security devices (41 percent of respondents).

Figure 8. Features most important in a SSL inspection tool
Essential and very important responses combined



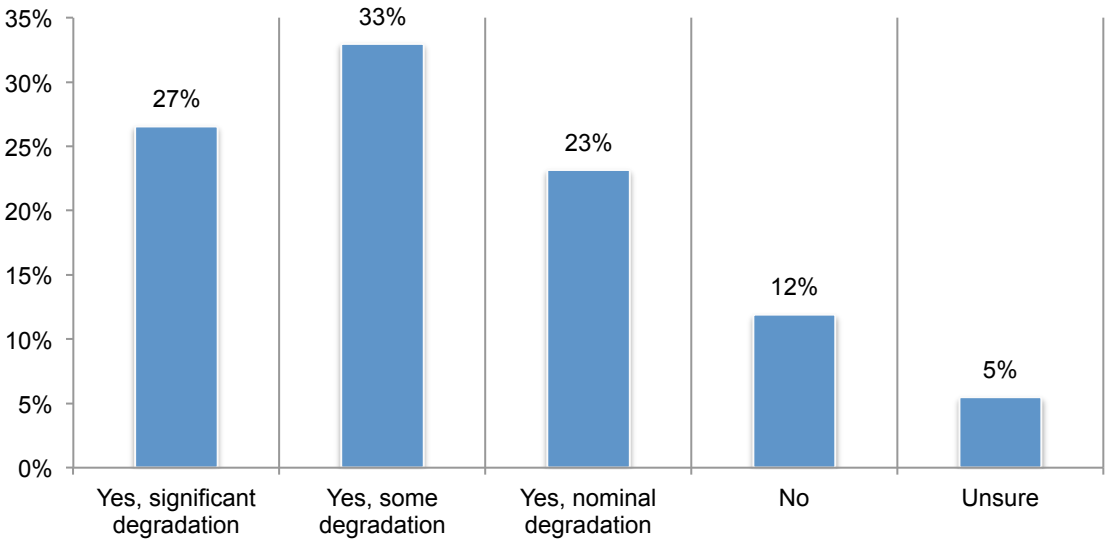
Despite the importance of a SSL decryption solution, 61 percent of respondents say lack of performance is the biggest barrier to implementing such a solution. As shown in Figure 9, other barriers are not having the right tools and lack of in-house expertise.

Figure 9. What are the biggest barriers to implementing a SSL decryption solution?



Another problem is performance degradation. Figure 10 reveals that 83 percent of respondents say decrypting SSL traffic during the inspection process results in performance degradation (27 percent + 33 percent + 23 percent).

Figure 10. Does decrypting SSL traffic during the inspection process result in performance degradation?



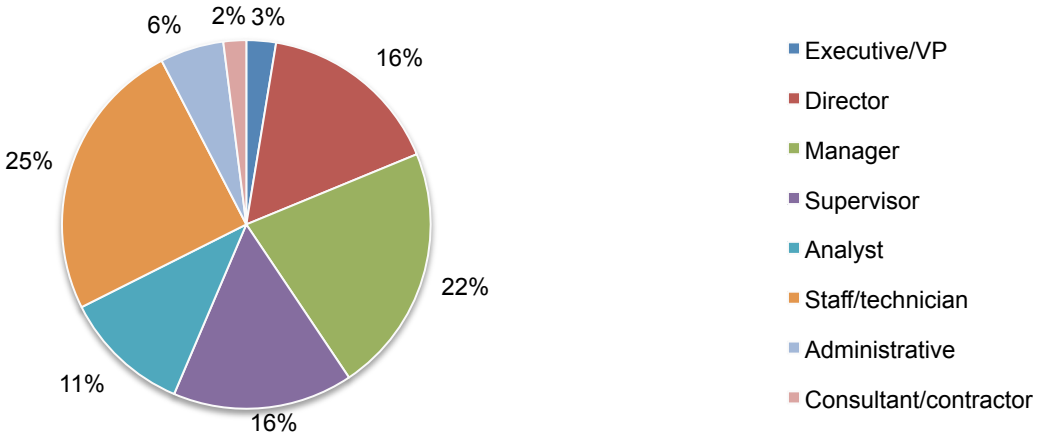
Part 3. Methods

The sampling frame is composed of 27,572 IT and IT security practitioners located in North America and EMEA who are involved in preventing and/or detecting web-based attacks and are familiar with the organization's network traffic inspection in the United States. As shown in Table 1, 1,120 respondents completed the survey. The screening process removed 97 surveys. The final sample was 1,023 surveys (or a 3.7 percent response rate).

Table 2. Sample response	Freq
Total sampling frame	27,572
Total returns	1,120
Rejected or screened surveys	97
Final sample	1,023
Response rate	3.7%

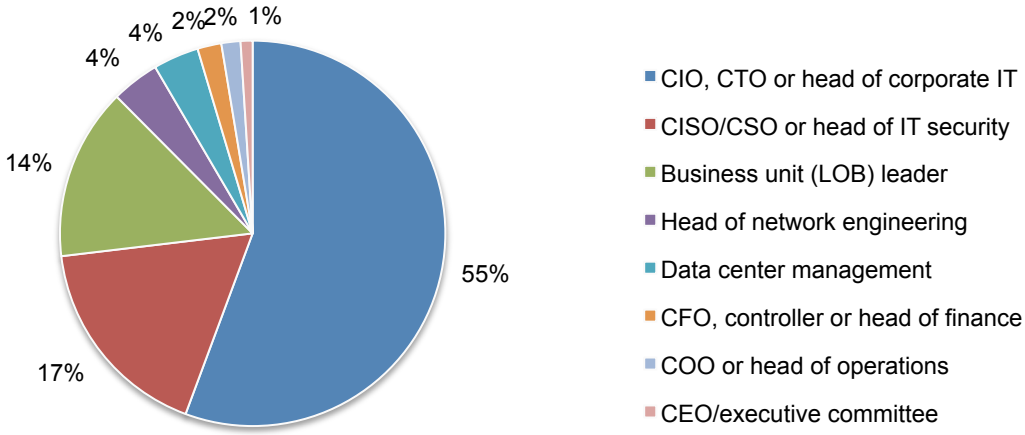
Pie Chart 1 summarizes the approximate position levels of respondents in our study. As can be seen, the majority of respondents (56 percent) are at or above the supervisory level.

Pie Chart 1. Distribution of respondents according to position level



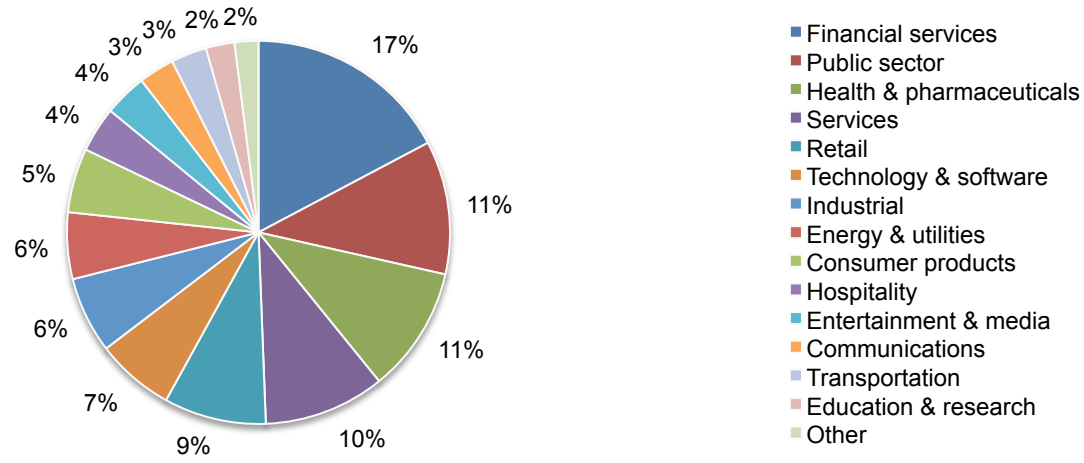
Fifty-five percent of respondents report to the Chief Information Officer, CTO or head of corporate IT and 17 percent report to the Chief Information Security Officer or head of IT security as shown in Pie Chart 2.

Pie Chart 2. Primary person respondent reports to within the organization



Pie Chart 3 reports the primary industry sector of respondents' organizations. This chart identifies financial services (17 percent) as the largest segment, followed by public sector (11 percent) and Health and Pharmaceutical (11 percent).

Pie Chart 3. Primary industry classification



According to Pie Chart 4, the majority of respondents (73 percent) are from organizations with a global headcount of 5,000 or more employees.

Pie Chart 4. Worldwide headcount of the organization

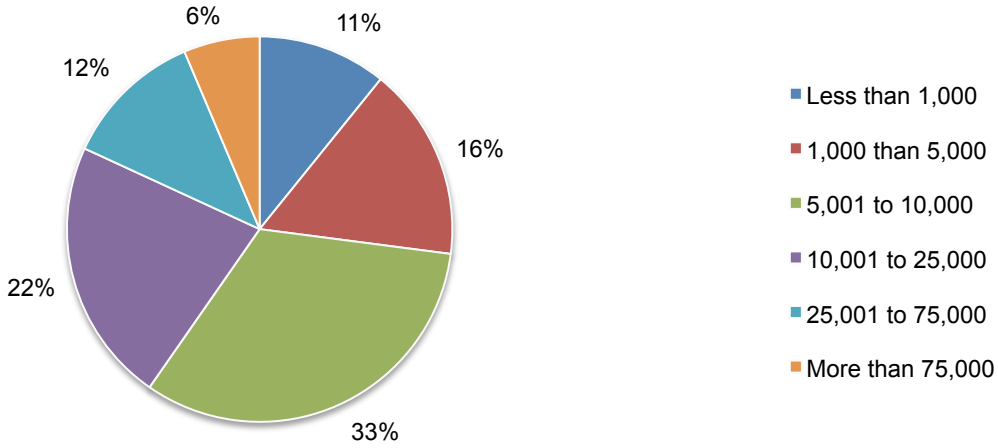


Table 3 reports the country distribution of the survey sample. The United States is the largest segment with 510 respondents. Canada has 98 respondents followed by the United Kingdom with 83 respondents.

Table 3. Country totals	Combined
United States	510
Canada	98
United Kingdom	83
Germany	81
France	67
Italy	43
Spain	39
Saudi Arabia	27
Denmark	20
UAE	16
Turkey	13
Israel	11
South Africa	8
Sweden	7
Total	1023

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in March 2016.

Survey response	Combined
Total sampling frames	27,572
Total returns	1,120
Rejected or screened surveys	97
Final samples	1,023
Response rates	3.7%
Sample weights	100.0%

*EMEA cluster = 12 countries; North America = Canada + US.

1. Screening Questions

S1. Do you have any role or involvement in preventing and/or detecting web-based attacks?	Combined
Yes, full involvement	36%
Yes, partial involvement	53%
Yes, minimal involvement	11%
No involvement (Stop)	0%
Total	100%

S2. How familiar are you with your organization's network traffic inspection process?	Combined
Very familiar	35%
Familiar	34%
Somewhat familiar	31%
No knowledge (Stop)	0%
Total	100%

2. Background

Q1. What percentage of your company's total web traffic is inspected for attacks, intrusions and malware?	Combined
None	18%
Less than 10%	12%
10% to 25%	12%
26% to 50%	15%
51% to 75%	9%
76% to 100%	8%
All	13%
Cannot determine	13%
Total	100%
Extrapolated value	39%

Q2. Today, what percentage of your company's inbound web traffic is encrypted? Your best estimate is welcome.	Combined
None	4%
Less than 10%	10%
10% to 25%	19%
26% to 50%	25%
51% to 75%	17%
76% to 100%	7%
All	4%
Cannot determine	15%
Total	100%
Extrapolated value	39%

Q3. Looking ahead 12 months, what percentage of your company's inbound web traffic will be encrypted? Your best estimate is welcome.	Combined
None	2%
Less than 10%	6%
10% to 25%	21%
26% to 50%	24%
51% to 75%	16%
76% to 100%	9%
All	7%
Cannot determine	15%
Total	100%
Extrapolated value	45%

Q4. Today, what percentage of your company's outbound web traffic is encrypted? Your best estimate is welcome.	Combined
None	9%
Less than 10%	18%
10% to 25%	17%
26% to 50%	18%
51% to 75%	11%
76% to 100%	6%
All	5%
Cannot determine	16%
Total	100%
Extrapolated value	33%

Q5. Looking ahead 12 months, what percentage of your company's outbound web traffic will be encrypted? Your best estimate is welcome.	Combined
None	7%
Less than 10%	13%
10% to 25%	14%
26% to 50%	18%
51% to 75%	18%
76% to 100%	9%
All	6%
Cannot determine	16%
Total	100%
Extrapolated value	41%

Q6a. Has your organization been the victim of a cyber attack or malicious insider activity in the past 12 months?	Combined
Yes, known with certainty	27%
Yes, most likely	33%
Yes, likely	20%
No, unlikely	14%
No chance	7%
Total	100%

Q6b. If yes, have any of the attacks used encryption to evade detection?	Combined
Yes	41%
No	44%
Unsure	15%
Total	100%

Q7. Looking ahead 12 months, do you think network attackers will increase their use of encryption (to evade detection and bypass controls)?	Combined
Yes	54%
No	30%
Unsure	16%
Total	100%

Q8. How concerned are you that encrypted communications will leave your network vulnerable to hidden threats that are able to bypass existing security solutions by hiding in SSL traffic?	Combined
Very concerned	32%
Concerned	36%
Somewhat concerned	22%
Not concerned	9%
Total	100%

Q9a. Does your company decrypt web traffic to detect attacks, intrusions and malware?	Combined
Yes	38%
No	53%
Unsure	9%
Total	100%

Q9b. If no, does your company intend to implement traffic decryption over the next 12 months?	Combined
Yes	51%
No	49%
Total	100%

Q9c. If your company does not inspect decrypted web traffic, why not?	Combined
Insufficient resources	45%
Performance degradation	45%
Not considered a priority	21%
Lack of knowledgeable or expert personnel	31%
Lack of enabling security tools	47%
Privacy concerns about inspection	29%
Other (please specify)	5%
Total	222%

Q9d. If yes, how does you company inspect decrypted traffic?	Combined
Commercial platform that utilizes deep packet inspection	53%
Commercial platform that utilizes meta data	44%
Homegrown traffic monitoring systems	35%
Manual inspection process	28%
Other (please specify)	4%
Total	163%

Q10a. Does your company currently use SSL decryption with the following security solutions? Please select all that apply	Combined
Firewall/NGFW/UTM	17%
UTM	10%
IPS	51%
DLP	31%
ATP	19%
SIEM	41%
Total	169%

Q10b. Does your company intend to integrate SSL decryption with any of the following security solutions in the next 12 months? Please select all that apply	Combined
Firewall/NGFW/UTM	24%
UTM	12%
IPS	60%
DLP	33%
ATP	20%
SIEM	46%
Total	195%

Q11. If your company currently decrypts SSL traffic during the inspection process, does it result in performance degradation?	Combined
Yes, significant degradation	12%
Yes, some degradation	15%
Yes, nominal degradation	11%
No	6%
Unsure	3%
Not currently decrypting SSL traffic today	53%
Total	100%

Q11 [adjusted]. If your company currently decrypts SSL traffic during the inspection process, does it result in performance degradation?	Combined
Yes, significant degradation	27%
Yes, some degradation	33%
Yes, nominal degradation	23%
No	12%
Unsure	5%
Total	100%

Q12. What are the biggest barriers to implementing a SSL decryption solution? Please select the top two reasons.	Combined
Cost	26%
Lack of features	22%
Lack of performance	61%
Lack of in-house expertise	32%
Not having the right tools	43%
Not a priority	16%
Other	2%
Total	200%

Q13. How important is the inspection of SSL traffic to your company's overall security infrastructure?	Combined
Essential	26%
Very important	31%
Important	32%
Not important	10%
Irrelevant	1%
Total	100%

3. Attributions: Please rate each statement using the agreement scale.

Q14. My company is currently eliminating the blind spot in corporate defenses by decrypting SSL traffic at high speeds.	Combined
Strongly agree	16%
Agree	20%
Unsure	18%
Disagree	32%
Strongly disagree	14%
Total	100%

Q15. My company is able to prevent costly data breaches and loss of intellectual property by detecting SSL traffic that is malicious.	Combined
Strongly agree	16%
Agree	20%
Unsure	20%
Disagree	27%
Strongly disagree	17%
Total	100%

Q16. Compromised insider credentials due to malware hiding inside encrypted SSL traffic could cause a data breach.	Combined
Strongly agree	44%
Agree	31%
Unsure	16%
Disagree	5%
Strongly disagree	3%
Total	100%

Q17. My company recognizes that malicious users leverage SSL encryption to conceal their exploits.	Combined
Strongly agree	22%
Agree	23%
Unsure	20%
Disagree	26%
Strongly disagree	9%
Total	100%

Q18. My company's security solutions are collapsing under growing SSL bandwidth demands and SSL key lengths.	Combined
Strongly agree	23%
Agree	30%
Unsure	23%
Disagree	16%
Strongly disagree	9%
Total	100%

Q19. The inability of our company's current security infrastructure to inspect encrypted traffic compromises the ability to meet existing and future compliance requirements.	Combined
Strongly agree	32%
Agree	30%
Unsure	19%
Disagree	13%
Strongly disagree	6%
Total	100%

Q20. Our enterprise perimeter security investment is ineffective because of our out/inbound encrypted traffic.	Combined
Strongly agree	19%
Agree	20%
Unsure	31%
Disagree	20%
Strongly disagree	10%
Total	100%

4. Product Features: Following are features of a SSL inspection tool. Please rate each feature using the importance scale below the item.

Q21. Scale to meet current and future SSL performance demands	Combined
Essential	34%
Very important	34%
Important	19%
Not important	8%
Irrelevant	5%
Total	100%

Q22. Satisfy compliance requirements	Combined
Essential	29%
Very important	34%
Important	18%
Not important	13%
Irrelevant	7%
Total	100%

Q23. Interoperate with a diverse set of security products from multiple vendors	Combined
Essential	26%
Very important	28%
Important	22%
Not important	17%
Irrelevant	6%
Total	100%

Q24. Maximize the uptime, performance requirements and the overall capacity of security infrastructure	Combined
Essential	26%
Very important	36%
Important	20%
Not important	11%
Irrelevant	7%
Total	100%

Q25. Securely manage SSL certificates and keys	Combined
Essential	41%
Very important	38%
Important	9%
Not important	9%
Irrelevant	3%
Total	100%

Q26. Categorize web traffic using an automated URL service to ensure confidential or sensitive data remains encrypted (i.e., bypass sensitive traffic to satisfy regulatory requirements)	Combined
Essential	22%
Very important	26%
Important	28%
Not important	19%
Irrelevant	5%
Total	100%

Q27. Intelligently route traffic to multiple security devices	Combined
Essential	20%
Very important	21%
Important	31%
Not important	20%
Irrelevant	7%
Total	100%

Q28. Granularly parse and control traffic based on custom-defined policies	Combined
Essential	21%
Very important	25%
Important	29%
Not important	18%
Irrelevant	7%
Total	100%

5. Scenarios

Attacker sends an encrypted stream of protected, sensitive and other critical data outbound through your firewall over “normal” ports, such as 443 or 80, which the firewall is tuned to accept because they are approved ports.	
Q29a. Likelihood of occurrence:	Combined
1 or 2	5%
3 or 4	7%
5 or 6	10%
7 or 8	13%
9 or 10	65%
Total	100%
Extrapolated value	7.98

Q29b. Ability to resolve:	Combined
1 or 2	23%
3 or 4	26%
5 or 6	20%
7 or 8	16%
9 or 10	14%
Total	100%
Extrapolated value	4.93

Attacker obfuscates malware communications when a worm, virus or botnet “phones home” to send stolen data to a master computer or download instructions or more malicious code.	
Q30a. Likelihood of occurrence:	Combined
1 or 2	11%
3 or 4	11%
5 or 6	12%
7 or 8	21%
9 or 10	45%
Total	100%
Extrapolated value	7.04

Q30b. Ability to resolve:	Combined
1 or 2	23%
3 or 4	30%
5 or 6	22%
7 or 8	17%
9 or 10	9%
Total	100%
Extrapolated value	4.70

Attacker makes phishing threats look even more legitimate, as even informed recipients would think the SSL usage makes it secure. Clicking the link, however, takes them to an SSL server loaded with malware that infects the client because the malware traffic is encrypted and not recognized by an IPS.	
Q31a. Likelihood of occurrence:	Combined
1 or 2	1%
3 or 4	7%
5 or 6	13%
7 or 8	22%
9 or 10	57%
Total	100%
Extrapolated value	8.03

Q31b. Ability to resolve:	Combined
1 or 2	27%
3 or 4	29%
5 or 6	27%
7 or 8	10%
9 or 10	7%
Total	100%
Extrapolated value	4.35

Through cross-site scripting, attackers steal cookies that can be used for a number of things, including account or session hijacking, changing user settings, cookie poisoning and/or false advertising. All of this can be accomplished while hiding within SSL-encrypted traffic.	
Q32a. Likelihood of occurrence:	Combined
1 or 2	5%
3 or 4	13%
5 or 6	20%
7 or 8	29%
9 or 10	33%
Total	100%
Extrapolated value	6.94

Q32b. Ability to resolve:	Combined
1 or 2	29%
3 or 4	29%
5 or 6	24%
7 or 8	14%
9 or 10	5%
Total	100%
Extrapolated value	4.26

A number of malware families use encryption to hide network information, including passwords or sensitive data they are sending out to SSL servers. The encryption blinded the monitoring/inspection systems to these internal network activities.	
Q33a. Likelihood of occurrence:	Combined
1 or 2	2%
3 or 4	8%
5 or 6	16%
7 or 8	36%
9 or 10	38%
Total	100%
Extrapolated value	7.52

Q33b. Ability to resolve:	Combined
1 or 2	34%
3 or 4	36%
5 or 6	15%
7 or 8	11%
9 or 10	5%
Total	100%
Extrapolated value	3.84

6. Organization and Respondents' Demographics

D1. What best describes your position level within the organization?	Combined
Executive/VP	3%
Director	16%
Manager	22%
Supervisor	16%
Analyst	11%
Staff/technician	25%
Administrative	6%
Consultant/contractor	2%
Other	0%
Total	100%

D2. What best describes your direct reporting channel?	Combined
Business unit (LOB) leader	14%
CEO/executive committee	1%
CFO, controller or head of finance	2%
CIO, CTO or head of corporate IT	55%
CISO/CSO or head of IT security	17%
COO or head of operations	2%
Data center management	4%
Head of compliance or internal audit	0%
Head of network engineering	4%
Other	0%
Total	100%

D3. What range best describes the full-time headcount of your global organization?	Combined
Less than 1,000	11%
1,000 than 5,000	16%
5,001 to 10,000	33%
10,001 to 25,000	22%
25,001 to 75,000	12%
More than 75,000	6%
Total	100%

D4. What best describes your organization's primary industry classification?	Combined
Agriculture & food services	1%
Communications	3%
Consumer products	5%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	6%
Entertainment & media	4%
Financial services	17%
Health & pharmaceuticals	11%
Hospitality	4%
Industrial	6%
Public sector	11%
Retail	9%
Services	10%
Technology & software	7%
Transportation	3%
Other	0%
Total	100%

Country totals withiin clusters	Combined
Canada	98
Denmark	20
France	67
Germany	81
Israel	11
Italy	43
Saudi Arabia	27
South Africa	8
Spain	39
Sweden	7
Turkey	13
UAE	16
United Kingdom	83
United States	510
Total	1023

Part 4. Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners located in the United States. We also acknowledge that the results may be biased by external events, such as media coverage.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.