Ponemon INSTITUTE


# The 2017 State of Endpoint Security Risk

## Sponsored by Barkly

Independently conducted by Ponemon Institute LLC

Publication Date: November 2017

# The 2017 State of Endpoint Security Risk

Ponemon Institute, November 2017

## Part 1. Introduction

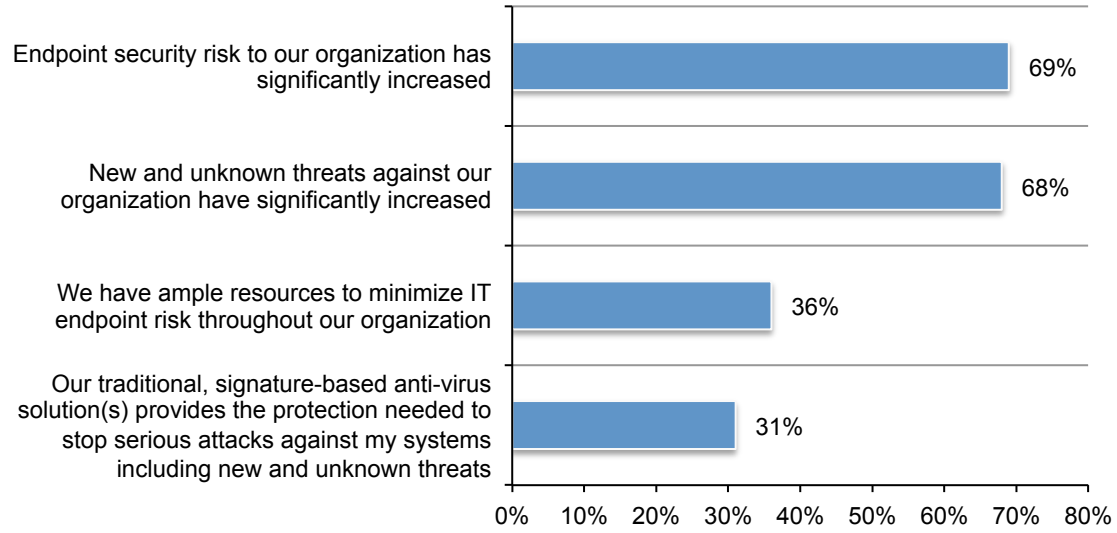
Attacks are evolving. As a result, today's organizations are struggling to secure their endpoints, and paying a steep cost for each successful attack. To discover how exactly endpoint security is breaking down, and what organizations are doing to fix it, Ponemon Institute surveyed 665 IT security professionals responsible for managing and reducing their organization's security risk.

The findings indicate we are in the midst of a significant shift in endpoint security.
The majority of organizations are replacing or augmenting these solutions with new security tools designed to stop fileless attacks, though many remain skeptical such attacks can be stopped at all.

As shown in Figure 1, only 36 percent of respondents say their organizations have ample resources to minimize the risk, despite 69 percent of respondents reporting endpoint security risk has significantly increased. Moreover, 68 percent of respondents say new and unknown threats against their organizations have significantly increased. As a consequence, only 31 percent of respondents say traditional solutions, such as antivirus programs that rely on file scanning and signature matching, provides the protection needed to stop serious attacks against their systems, including new and unknown threats.

**Figure 1. Perceptions about endpoint security risk**

Strongly agree and Agree responses combined




In addition to reporting a significant rise in the new types of attacks they're seeing, respondents also indicate their organizations are struggling to keep the cost and complexity of managing endpoint security down. According to 45 percent of respondents, the biggest problem with their current endpoint protection solutions is that they yield a high number of false positives and security alerts. Adding to that management challenge is the fact that organizations now have an average of seven different agents installed on endpoints, with each requiring its own monitoring.

## Part 2. Key findings

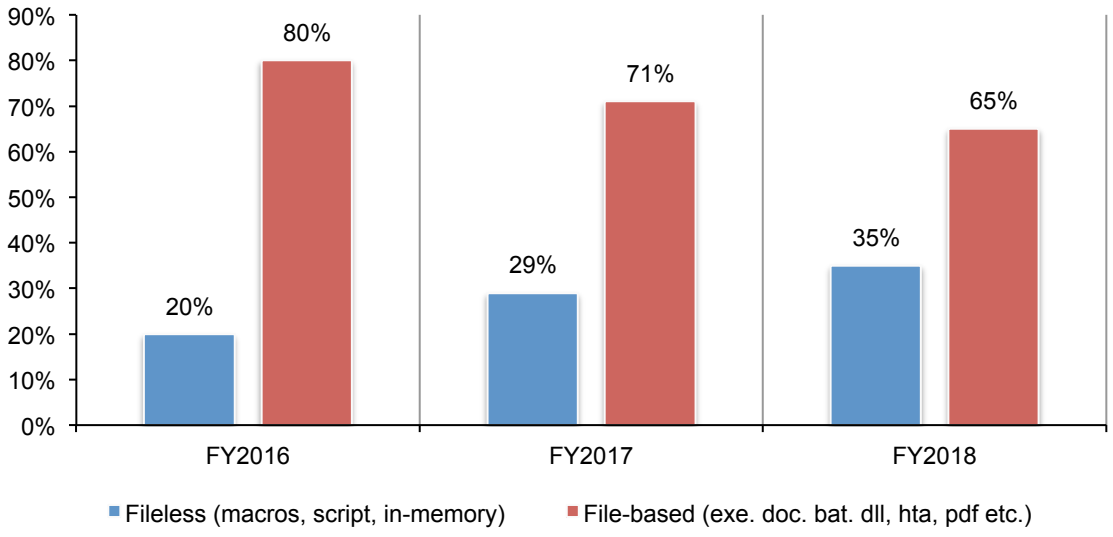
In this section of the report, we provide more details about the state of endpoint security by highlighting the challenges impacting endpoint security today. Also revealed are the specific types of attacks that are most often getting past traditional endpoint solutions and the costs of those attacks.

**Fileless attack techniques that exploit a fundamental gap in traditional endpoint security are on the rise. Current solutions aren't stopping them.** A fileless attack is an attack that avoids downloading malicious executable files at one stage or another by using exploits, macros, scripts, or legitimate system tools, instead.

Rather than install malicious executable files that antivirus solutions can scan and block, these attacks instead leverage exploits designed to run malicious code or launch scripts directly from memory, infecting endpoints without leaving easily-discoverable artifacts behind. Once an endpoint has been compromised, these attacks can also abuse legitimate system administration tools and processes to gain persistence, elevate privileges, and spread laterally across the network.

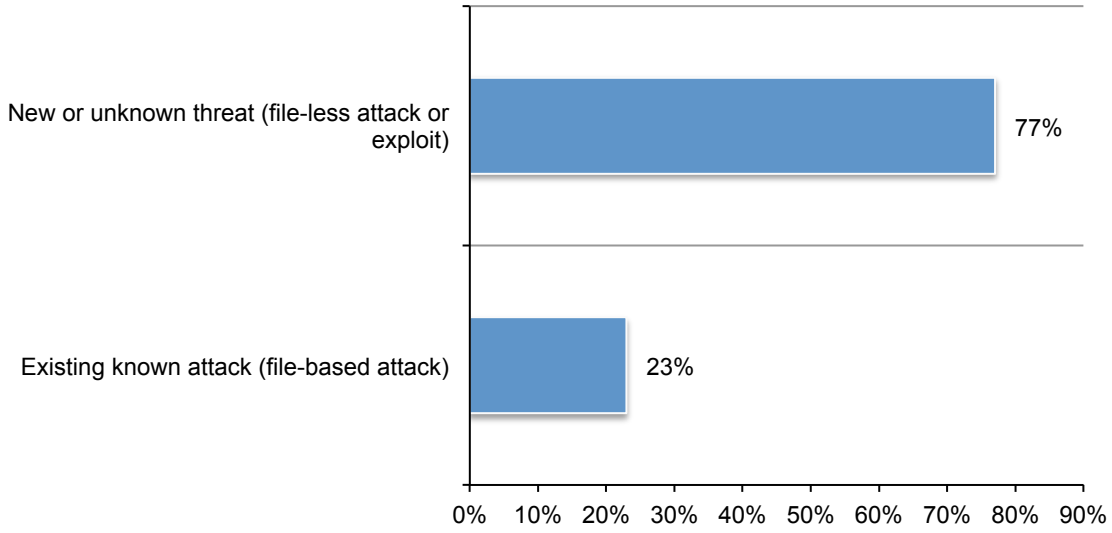
According to Figure 2, respondents in this year's study estimate that 29 percent of the attacks their organizations faced were fileless attacks, up from 20 percent the year before. They project that proportion to continue to rise next year, with fileless attacks estimated to make up 35 percent of all attacks in 2018. In contrast, while still significant, file-based are expected to continue to decline.

**Figure 2. The growth of fileless and file-based attacks**



**Fileless attacks are on the uptick because they are working.** According to 54 percent of respondents, their organizations experienced one or more endpoint attacks that have successfully compromised data assets and/or IT infrastructure over the past 12 months. Of these respondents, as shown in Figure 3, 77 percent report the attack was a fileless attack or exploit.

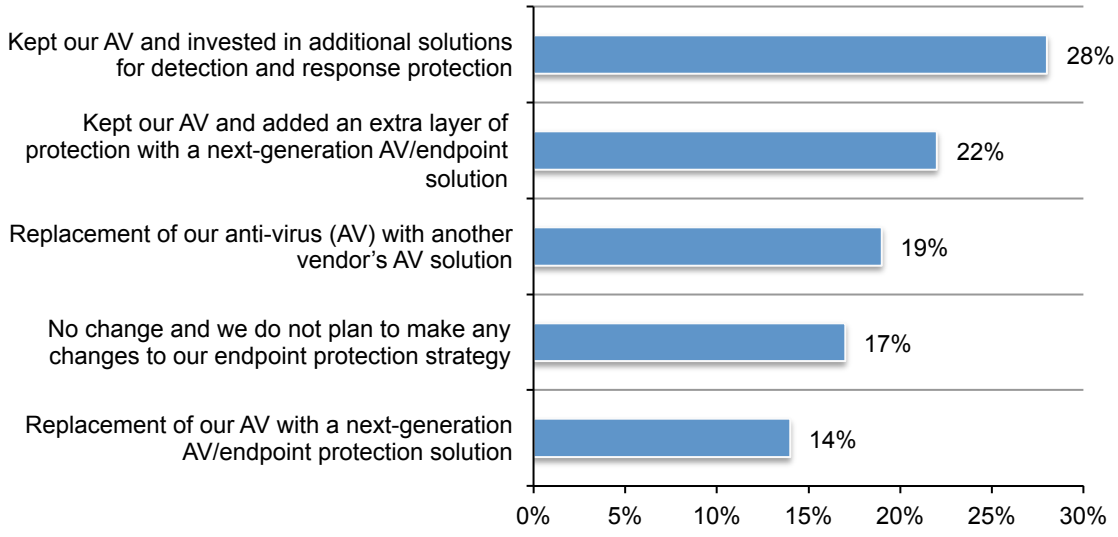
**Figure 3. What type of attack do you believe compromised your organization?**
(According to 54 percent of respondents)



**Antivirus solutions are being replaced or supplemented.** The success of fileless attacks has further eroded organizations' trust in their existing security solutions. As discussed previously, only 31 percent of respondents believe their antivirus (AV) can stop the threats they are seeing. As a result, the majority of respondents say their companies are investing in new technology**.** Despite the addition of new technologies, not all attacks can be stopped. On average, respondents report they are effective in stopping 54 percent of attacks to their endpoints.

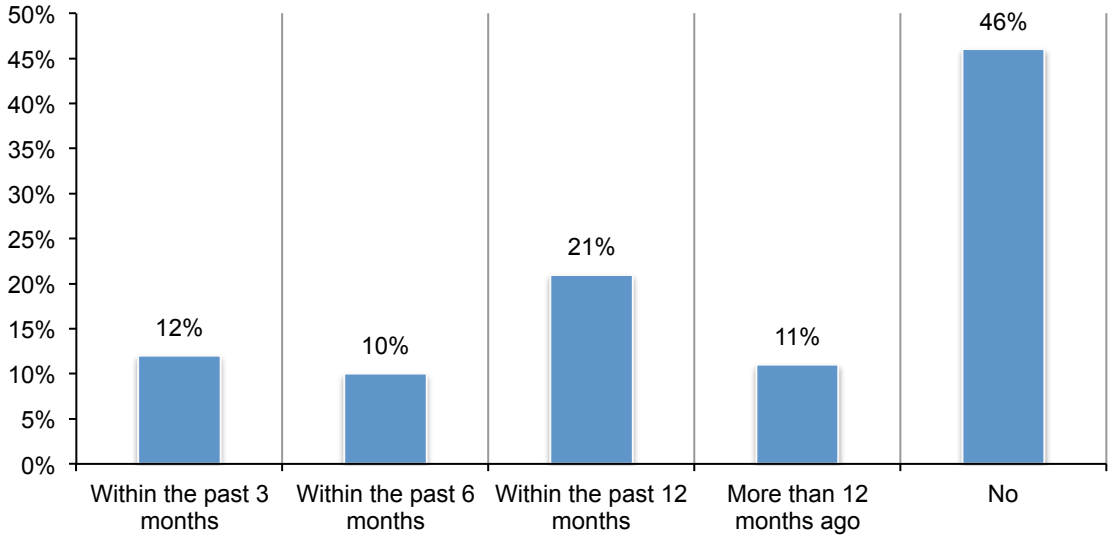
As shown in Figure 4, one-third of respondents report their organization replaced their AV with another vendor's AV (19 percent) or a next-generation endpoint solution (14 percent). Fifty percent of respondents say they either kept their existing AV and added solutions with either additional protection or detection and response capabilities (28 percent) or added an extra layer of protection with a next-generation AV/endpoint solution (22 percent).

**Figure 4. How has your organization's endpoint protection strategy changed in the past year?**



**Ransomware is still a major issue.** Ransomware attacks continue to be a major cause for concern. According to Figure 5, 43 percent of respondents (12 percent + 10 percent + 21 percent) say their organizations experienced one or more ransomware incidents in the 12 months. Sixty-five percent of respondents of these respondents say their organizations paid an average ransom of $3,675.

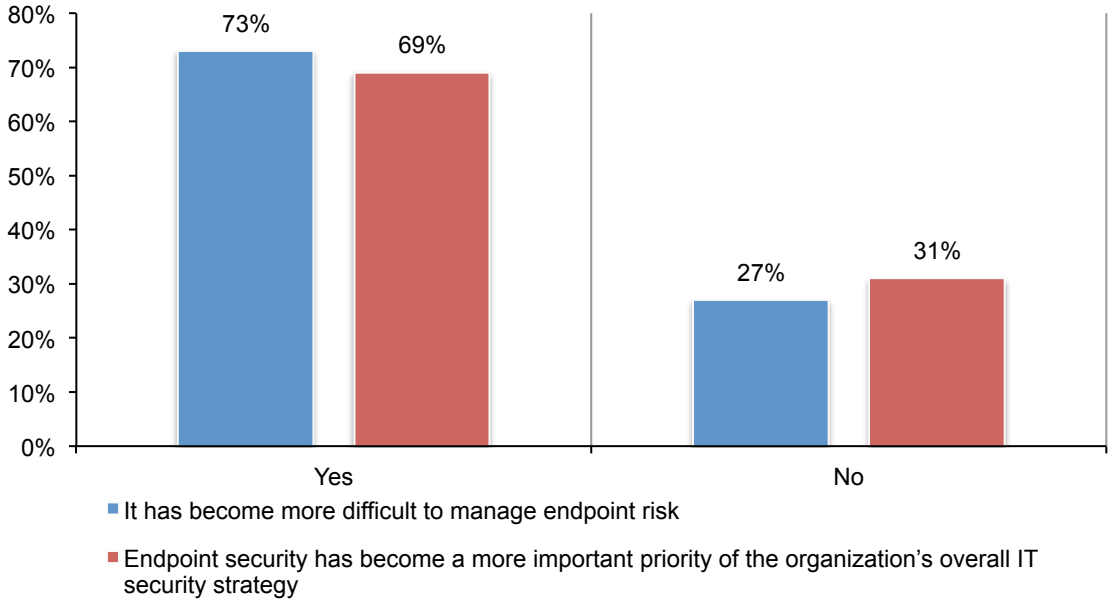
**Figure 5. Has your company experienced ransomware?**



**Endpoint security risk is becoming more difficult and costly to manage.** In addition to failing to stop new attacks, many existing endpoint solutions are also putting an untenable strain on staff, resources, and overall productivity, the respondents report. According to respondents, their organizations have an average of seven different software agents installed on their endpoints to enable IT management and security, making endpoint management noisy and time-consuming.

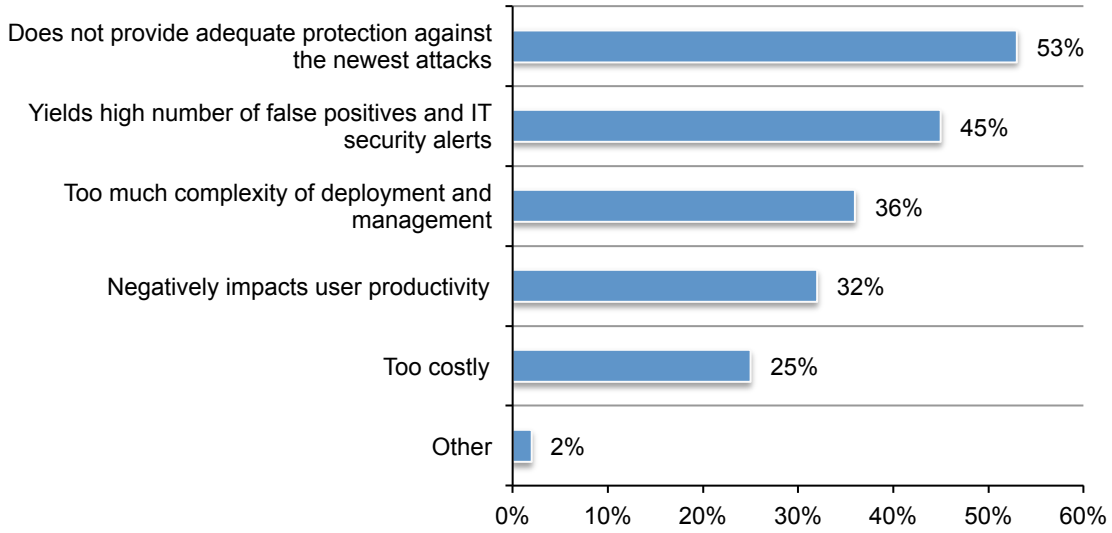
In fact, as shown in Figure 6, nearly three out of four respondents (73 percent) say it has become more difficult for their organization to effectively manage endpoint risk and 69 percent of respondents say endpoint security has become a more important priority for organization's overall IT security strategy. However, as discussed previously, only 36 percent of respondents say they have adequate resources to address the risk.

**Figure 6. Endpoint risk is more difficult to manage and has become a priority**



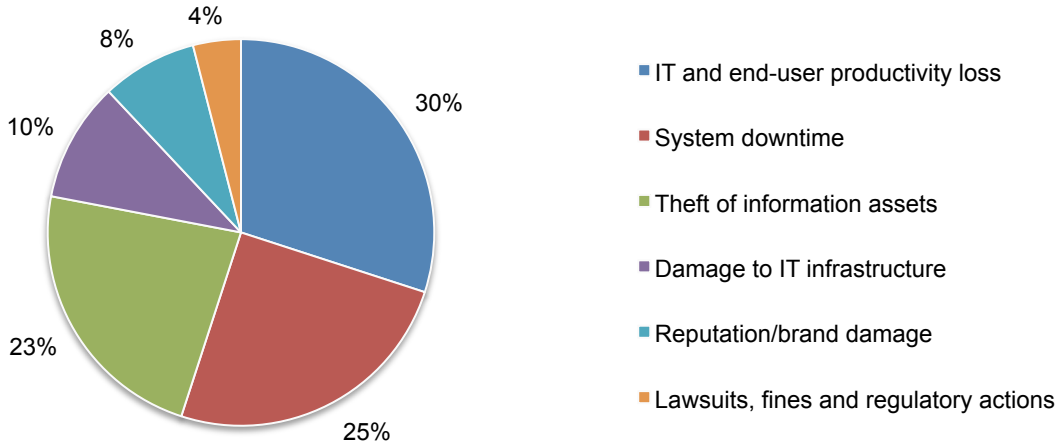
As shown in Figure 7, when asked to identify the biggest problems with their current endpoint solutions, 45 percent of respondents say it was the high number of false positives and IT security alerts they had to respond to. More than half (53 percent of respondents) say their solutions are not providing adequate protection against the newest attacks.

**Figure 7. What are the biggest problems with your current endpoint protection solutions?**
Two responses permitted




**The average total cost of a successful attack is over $5 million.** For the attacks that did get through existing endpoint security, the cost to victim organizations was significant. On average, companies lost a total of $5,010,600**.** As shown in Pie Chart 1, loss of IT and end user productivity was listed as the most costly consequence of successful endpoint attacks (30 percent), with system downtime and theft of informational assets following closely behind (25 percent).

**Pie chart 1. Cost of endpoint attacks**
The average organization lost $5,010,600 due to endpoint attacks in 2017



## Part 3. Conclusion

The current endpoint security solutions organizations are deploying are ineffective at stopping today's new and evolving attacks. In addition, implementation and management of these solutions is placing unjustified strain on organizations' employees and resources.

As a result, many organizations are moving beyond their current antivirus solutions, but the majority are choosing to replace or supplement them with solutions that do not truly address their gaps in protection (e.g. other AVs or endpoint detection and response solutions that mitigate attacks after damage is done).

With the average cost of a successful endpoint attack totaling over $5 million in downtime, damages, and loss of productivity, waiting to address attacks until after they have taken place is untenable.

Based on this research, organizations can clearly benefit from endpoint security solutions designed to block new threats like fileless attacks, which are becoming more pervasive. To restore their faith in endpoint security's effectiveness, new solutions need to address this crucial gap in protection without adding unnecessary complexity to endpoint management.

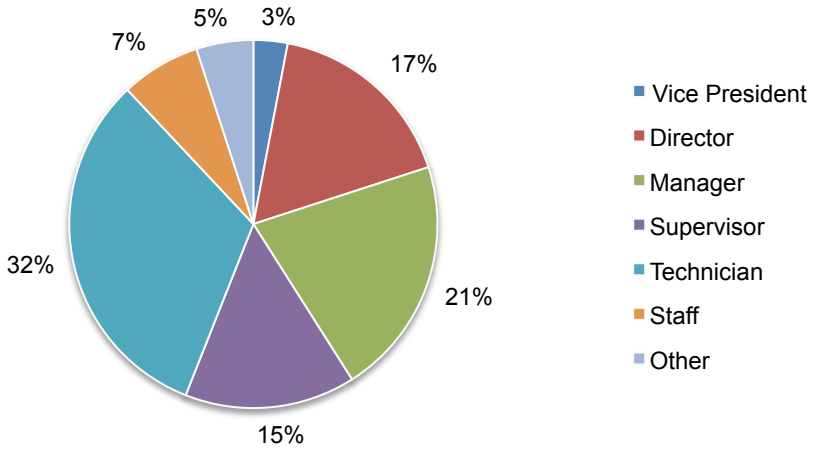
## Part 4. Methods

A sampling frame of 18,289 experienced IT and IT security practitioners located in the United States were selected as participants to this survey. To ensure knowledgeable responses, all participants in this research are familiar and involved in their company's endpoint security. Table 1 shows 830 total returns. Screening and reliability checks required the removal of 165 surveys. Our final sample consisted of 665 surveys (3.6 percent response rate).

| **Table 1. Sample response** | FY2017 |
|---|---|
| Total sampling frame | 18,289 |
| Total returns | 830 |
| Rejected or screened surveys | 165 |
| Final sample | 665 |
| Response rate | 3.6% |

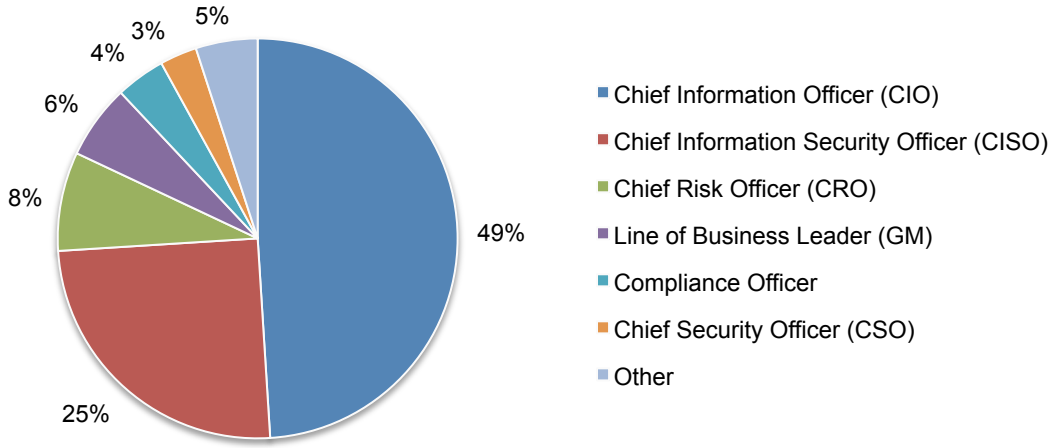
Pie Chart 2 reports the respondents' position in participating organizations. By design, more than half of respondents (56 percent) are at or above the supervisory levels.

**Pie Chart 2. Current position within the organization**



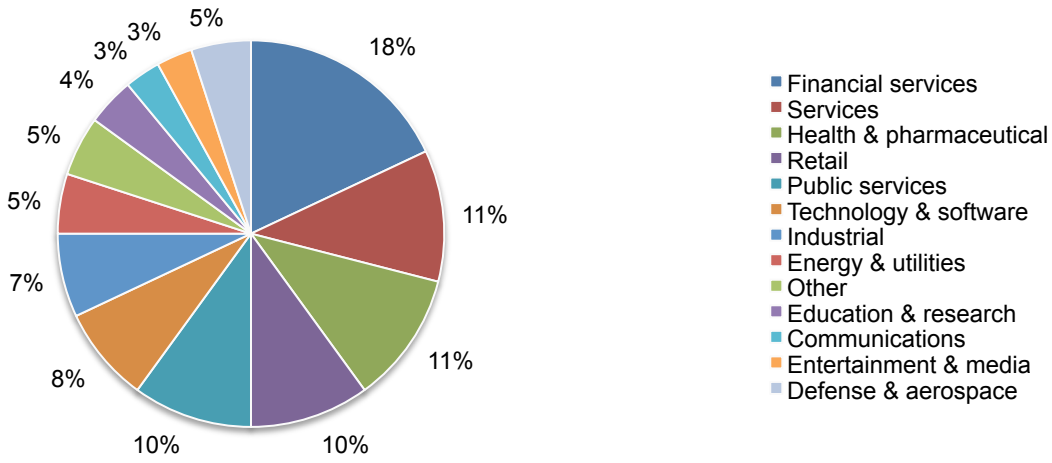

As shown in Pie Chart 3, 49 percent of respondents report to the chief information officer and 25 percent report to the chief information security officer.

**Pie Chart 3. Primary person respondent or IT security leader reports to**



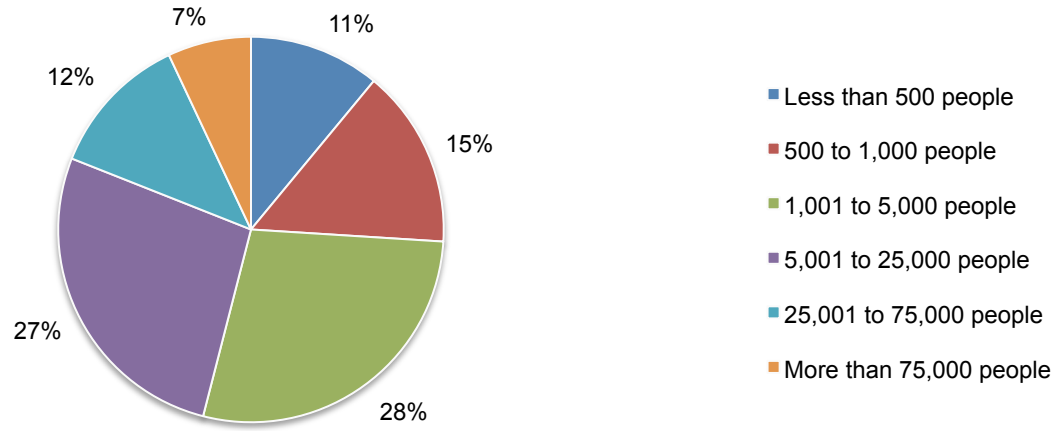
According to Pie Chart 4, financial services (18 percent), services (11 percent) and health and pharmaceutical (11 percent) are the industries most represented in this study.

**Pie Chart 4. Industry focus of respondents' organizations**




According to Pie Chart 5, 74 percent of respondents are from organizations with a global headcount of more than 1,000 employees.

**Pie Chart 5. Worldwide headcount of the organization**



**Part 4. Caveats to this study**

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. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.

- 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.

## 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 October 2017.

| Survey response | FY 2017* |
|---|---|
| Total sampling frame | 18,289 |
| Rejected and screened surveys | 165 |
| Final sample | 665 |
| Response rate | 3.6% |

*Date (year) of research publication

**Part 1. Screening**

| S1. What best describes your level of involvement in endpoint security within your organization? | FY 2017 |
|---|---|
| None (stop) | 0% |
| Responsible for overall solution/purchase | 45% |
| Responsible for administration | 40% |
| Responsible for management | 47% |
| Involved in evaluating solutions | 56% |
| Total | 188% |

| S2. How many network-connected endpoints (servers, laptops, workstations) does your organization support? | FY 2017 |
|---|---|
| Less than 50 (stop) | 0% |
| 50 to 250 | 10% |
| 251 to 1,000 | 34% |
| 1,000+ | 56% |
| Total | 100% |

| S3. What best describes your role within your organization's IT department? | FY 2017 |
|---|---|
| IT leadership (CIO) | 11% |
| Security leadership (CSO/CISO) | 20% |
| IT management | 13% |
| IT operations | 20% |
| Security management | 9% |
| Security monitoring and response | 7% |
| Data administration | 8% |
| Compliance administration | 9% |
| Applications development | 3% |
| I'm not involved in my organization's Security or IT function (stop) | 0% |
| Total | 100% |

**Part 2: Attributions**

| Q1. We have ample resources to minimize IT endpoint risk throughout our organization. | FY 2017 |
|---|---|
| Strongly agree | 15% |
| Agree | 21% |
| Unsure | 22% |
| Disagree | 34% |
| Strongly disagree | 8% |
| Total | 100% |

| Q2. Endpoint security risk to our organization has significantly increased. | FY 2017 |
|---|---|
| Strongly agree | 31% |
| Agree | 38% |
| Unsure | 12% |
| Disagree | 13% |
| Strongly disagree | 6% |
| Total | 100% |

| Q3. New and unknown threats against our organization have significantly increased. | FY 2017 |
|---|---|
| Strongly agree | 29% |
| Agree | 39% |
| Unsure | 13% |
| Disagree | 14% |
| Strongly disagree | 5% |
| Total | 100% |

| Q4. Our traditional, signature-based anti-virus solution(s) provides the protection needed to stop serious attacks against my systems including new and unknown threats. | FY 2017 |
|---|---|
| Strongly agree | 15% |
| Agree | 16% |
| Unsure | 24% |
| Disagree | 33% |
| Strongly disagree | 12% |
| Total | 100% |

| Q5. Our endpoint security solutions provide protection at a high cost of ownership. | FY 2017 |
|---|---|
| Strongly agree | 25% |
| Agree | 24% |
| Unsure | 11% |
| Disagree | 24% |
| Strongly disagree | 16% |
| Total | 100% |

**Part 3: General questions**

| Q6. Please allocate the distribution of attacks that have targeted your organization based on attack type and include an estimated target for 2018. Please use all 100 points. | FY 2017 |
|---|---|
| Fileless (macros, script, in-memory) | 20 |
| File-based (exe. doc. bat. dll, hta, pdf etc.) | 80 |
| Total points | 100 |

| Q7. What types of attacks do you believe your organization is most likely to be targeted by? | FY 2017 |
|---|---|
| Known and existing attacks | 69% |
| Unknown, new or zero-day attacks | 31% |
| Total | 100% |

| Q8.How does your organization allocate most of its current security investment? | FY 2017 |
|---|---|
| Protecting against known and traditional attacks | 55% |
| Protecting against unknown, new or zero-day attacks | 45% |
| Total | 100% |

| Q9a. Has your company experienced one or more endpoint attacks that have successfully compromised data assets and/or IT infrastructure over the past 12 months? | FY 2017 |
|---|---|
| Yes | 54% |
| No | 41% |
| Unsure | 5% |
| Total | 100% |

| Q9b. If yes, what type of attack do you believe compromised your organization? | FY 2017 |
|---|---|
| Existing known attack (file-based attack) | 23% |
| New or unknown threat (fileless attack or exploit) | 77% |
| Total | 100% |

| Q10. In the past 24 months, has it become more difficult to manage endpoint risk? | FY 2017 |
|---|---|
| Yes | 73% |
| No | 27% |
| Total | 100% |

| Q11. In the past 24 months, has endpoint security become a more important priority of your organization's overall IT security strategy? | FY 2017 |
|---|---|
| Yes | 69% |
| No | 31% |
| Total | 100% |

| Q12. How has your organization's endpoint protection strategy changed in the past year? | FY 2017 |
|---|---|
| Replacement of our anti-virus (AV) with another vendor's AV solution | 19% |
| Replacement of our AV with a next-generation AV/endpoint protection solution | 14% |
| Kept our AV and added an extra layer of protection with a next-generation AV/endpoint solution | 22% |
| Kept our AV and invested in additional solutions for detection and response protection | 28% |
| No change and we do not plan to make any changes to our endpoint protection strategy | 17% |
| Total | 100% |

| Q13. What are the biggest problems with your current endpoint protection solutions? Please select the top two problems. | FY 2017 |
|---|---|
| Does not provide adequate protection against the newest attacks | 53% |
| Yields high number of false positives and IT security alerts | 45% |
| Negatively impacts user productivity | 32% |
| Too much complexity of deployment and management | 36% |
| Too costly | 25% |
| Other | 2% |
| Total | 193% |

| Q14. How difficult was the deployment of your current endpoint protection solution? | FY 2017 |
|---|---|
| Very difficult | 17% |
| Difficult | 35% |
| Somewhat difficult | 29% |
| Not difficult | 19% |
| Total | 100% |

| Q15. What percentage of all security alerts from your endpoint security solution are false positives or reliable software (e.g. software that is good but the protection agent thinks it is bad and blocks user)? | FY 2017 |
|---|---|
| Less than 10% | 7% |
| 10 to 24% | 12% |
| 25 to 49% | 31% |
| 50 to 75% | 35% |
| More than 75% | 15% |
| Total | 100% |
| Extrapolated value | 48% |

| Q16. How has the frequency of malware incidents changed over the past year within your organization? Trend | FY 2017 |
|---|---|
| Significantly increased | 23% |
| Increased | 35% |
| Stayed the same | 21% |
| Decreased | 15% |
| Significantly decreased | 6% |
| Total | 100% |

| Q17a. Has your company experienced ransomware? | FY 2017 |
|---|---|
| Yes, within the past 3 months | 12% |
| Yes, within the past 6 months | 10% |
| Yes, within the past 12 months | 21% |
| Yes, more than 12 months ago | 11% |
| No, we have not experienced a ransomware attack | 46% |
| Total | 100% |

| Q17b. If yes, how many ransomware incidents have you or your company experienced over the past 12 months? | FY 2017 |
|---|---|
| 1 | 60% |
| 2 to 5 | 21% |
| 6 to 10 | 13% |
| Greater than 10 | 6% |
| Total | 100% |

| Q17c. If yes, did your company pay the ransom? | FY 2017 |
|---|---|
| Yes | 65% |
| No | 35% |
| Total | 100% |

| Q17d. If yes, how much was the ransom? | FY 2017 |
|---|---|
| Less than $100 | 9% |
| $100 to $500 | 8% |
| $501 to $1,000 | 25% |
| $1,001 to $5,000 | 31% |
| $5,001 to $10,000 | 23% |
| More than $10,000 | 4% |
| Total | 100% |
| Extrapolated value | $3,675 |

| Q18. A growing trend in cyber attacks has been the unleashing of so-called “destructive malware” (such as Cryptolocker, Shamoon, etc.). Is your organization’s endpoint protection solution able to mitigate these attacks? | FY 2017 |
|---|---|
| Yes | 32% |
| No | 60% |
| Unsure | 8% |
| Total | 100% |

| Q19. With your current enabling technologies, processes and in-house expertise, what percentage of attacks to your organization's endpoints can be realistically stopped? | FY 2017 |
|---|---|
| None | 5% |
| 5% or less | 7% |
| 6% to 25% | 6% |
| 26% to 50% | 20% |
| 51% to 75% | 24% |
| 76% to 100% | 28% |
| Cannot determine | 10% |
| Total | 100% |
| Extrapolated value | 54% |

| Q20. What percentage of endpoint devices connected to your organization's network is not secured? | FY 2017 |
|---|---|
| None | 16% |
| Less than 25% | 45% |
| 26% to 50% | 16% |
| 51% to 75% | 15% |
| 76% to 100% | 7% |
| All | 1% |
| Total | 100% |
| Extrapolated value | 28% |

| Q21. What are the fastest growing sources of IT security risk within your IT environment? Please choose only your **top five** choices. ** | FY 2017 |
|---|---|
| Our server environment | 15% |
| Use of unapproved applications or services | 37% |
| Our data centers | 5% |
| Within operating systems (vulnerabilities) | 8% |
| Across third party applications (vulnerabilities) | 86% |
| Our PC desktop/laptop | 36% |
| Removable media (USB sticks) and/or media (CDs, DVDs) | 26% |
| Network infrastructure environment (gateway to endpoint) | 13% |
| Malicious insider risk | 48% |
| Negligent insider risk | 45% |
| Negligent third party risk (partner, vendors, customers, etc.) | 29% |
| Cloud computing infrastructure and providers | 31% |
| Virtual computing environments (servers, endpoints) | 13% |
| Mobile/remote employees | 42% |
| Lack of system connectivity/visibility | 48% |
| Lack of organizational alignment | 20% |
| Total | 500% |

| Q22. Approximately how many **software agents** does your organization typically have installed on each endpoint to enable IT management, security and/or other operations? Please provide your best estimate. * | FY 2017 |
|---|---|
| 1 to 2 | 13% |
| 3 to 5 | 23% |
| 6 to 10 | 32% |
| More than 10 | 27% |
| Cannot determine | 5% |
| Total | 100% |
| Extrapolated value | 7.28 |

* Wording slightly different

| Q23. On a typical day, how many different or distinct software management user interfaces or consoles does your organization use to manage endpoint operations and security functions? Please provide your best estimate. | FY 2017 |
|---|---|
| 1 to 2 | 9% |
| 3 to 5 | 21% |
| 6 to 10 | 43% |
| More than 10 | 22% |
| Cannot determine | 5% |
| Total | 100% |
| Extrapolated value | 7.43 |

| Q24a. Traditional endpoint defense has focused on prevention, but there is a growing movement towards a so-called “detect and respond” orientation. Is your organization moving towards this paradigm? | FY 2017 |
|---|---|
| Yes, doing it now | 61% |
| Yes, planning to do so in the next 24 months | 19% |
| Yes, planning to do so more than 24 months from now | 13% |
| No | 7% |
| Never heard of it | 0% |
| Total | 100% |

| Q24b. If yes, what are the most critical capabilities for endpoint detection and response? Please select the top 3 choices. | FY 2017 |
|---|---|
| Kill the process | 43% |
| Quarantine the executable | 60% |
| Isolate the device | 54% |
| Rollback malicious changes | 23% |
| Revoke credentials | 49% |
| Remove the file/process | 17% |
| Re-image the machine | 54% |
| Total | 300% |

**Part 4. Economic impact**

| Q25. How much does your organization spend on endpoint protection per endpoint (i.e. laptop/desktop)? | FY 2017 |
|---|---|
| Less than $30 per year | 49% |
| $30 to $60 per year | 28% |
| More than $60 per year | 23% |
| Total | 100% |
| Extrapolated value | $39.80 |

| Q26. How much does your organization spend per server on protection? | FY 2017 |
|---|---|
| Less than $30 per year | 19% |
| $30 to $60 per year | 42% |
| More than $60 per year | 39% |
| Total | 100% |
| Extrapolated value | $49.00 |

| Q27. Following are 4 types of ongoing costs related to endpoint protection. Please rank these costs from 1 = most costly to 4 = least costly. | FY 2017 |
|---|---|
| The cost of hiring and retaining security experts | 3.5 |
| The cost of inefficient security practices (e.g. false positives) | 1.7 |
| The cost of engaging outside vendors and consultants | 3.1 |
| The cost caused by software compatibility issues | 2.3 |

| Q28. Please estimate the total economic loss incurred by your company as a result of endpoint attacks experienced over the past 12 months. | FY 2017 |
|---|---|
| Less than $50,000 | 3% |
| $50,000 to $100,000 | 5% |
| $100,001 to $500,000 | 11% |
| $500,001 to $1,000,000 | 37% |
| $1,000,000 to $5,000,000 | 29% |
| $5,000,001 to $10,000,000 | 11% |
| $10,000,001 to $50,000,001 | 1% |
| $50,000,001 to $100,000,000 | 2% |
| More than $100,000,000 | 1% |
| Total | 100% |
| Extrapolated value | $5,010,600 |

| Q29. Following are 6 cost consequences that may be experienced by your company as a result of one or more endpoint attacks over the past 12 months. Please allocate 100 points based on the total cost for each consequence listed in the table below. Use all 100 points in the table to allocate your response. | FY 2017 |
|---|---|
| Cost consequences | Points |
| IT and end-user productivity loss | 30 |
| System downtime | 25 |
| Theft of information assets | 23 |
| Damage to IT infrastructure | 10 |
| Lawsuits, fines and regulatory actions | 4 |
| Reputation/brand damage | 8 |
| Total points | 100 |

**Part 5. Questions about IoT**

| Q30. Does your organization's endpoint security strategy and/or tactics include the Internet of Things (IoT)? | FY 2017 |
|---|---|
| Yes | 40% |
| No | 51% |
| Unsure | 9% |
| Total | 100% |

| Q31. What percentage of your organization's endpoint security budget (or discretionary spending) is dedicated to IoT devices? | FY 2017 |
|---|---|
| None | 26% |
| Less than 10% | 19% |
| 10% to 25% | 33% |
| 26% to 50% | 10% |
| 51% to 75% | 9% |
| 76% to 100% | 3% |
| Total | 100% |
| Extrapolated value | 19% |

| Q32. Relative to other (traditional) endpoints such as laptop computers, printers, routers and servers, how difficult is it to secure IoT devices within your organization? | FY 2017 |
|---|---|
| Much more difficult | 19% |
| More difficult | 28% |
| About the same | 25% |
| Less difficult | 12% |
| Much less difficult | 6% |
| Cannot determine | 10% |
| Total | 100% |

**Part 6. Organizational Characteristics & Demographics**

| D1. What organizational level best describes your current position? | FY 2017 |
|---|---|
| Senior Executive | 2% |
| Vice President | 3% |
| Director | 17% |
| Manager | 21% |
| Supervisor | 15% |
| Technician | 32% |
| Staff | 7% |
| Contractor | 2% |
| Other | 1% |
| Total | 100% |

| D2. Check the **Primary Person** you or your IT security leader reports to within the organization. | **FY 2017** |
|---|---|
| CEO/Executive Committee | 2% |
| Chief Financial Officer (CFO) | 0% |
| General Counsel | 2% |
| Chief Information Officer (CIO) | 49% |
| Chief Information Security Officer (CISO) | 25% |
| Compliance Officer | 4% |
| Line of Business Leader (GM) | 6% |
| Chief Security Officer (CSO) | 3% |
| Chief Risk Officer (CRO) | 8% |
| Other | 1% |
| Total | 100% |

| D3. What industry best describes your organization's **primary** industry focus? | **FY 2017** |
|---|---|
| Communications | 3% |
| Defense & aerospace | 1% |
| Education & research | 4% |
| Energy & utilities | 5% |
| Entertainment & media | 3% |
| Hospitality | 2% |
| Retail | 10% |
| Services | 11% |
| Technology & software | 8% |
| Transportation | 2% |
| Financial services | 18% |
| Health & pharmaceutical | 11% |
| Industrial | 7% |
| Public services | 10% |
| Other | 5% |
| Total | 100% |

| D4. Where are your employees located? Check all that apply. | **FY 2017** |
|---|---|
| United States | 100% |
| Canada | 66% |
| Europe | 73% |
| Middle East & Africa | 37% |
| Asia-Pacific | 60% |
| Latin America (including Mexico) | 39% |

| D5. What is the worldwide headcount of your organization? | **FY 2017** |
|---|---|
| Less than 500 people | 11% |
| 500 to 1,000 people | 15% |
| 1,001 to 5,000 people | 28% |
| 5,001 to 25,000 people | 27% |
| 25,001 to 75,000 people | 12% |
| More than 75,000 people | 7% |
| Total | 100% |
| Extrapolated value | 16,647 |

**Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.**

## 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.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.