The Third Annual Study on the State of Endpoint Security Risk

Sponsored by Morphisec

Independently conducted by Ponemon Institute LLC

Publication Date: January 2020

The Third Annual Study on the State of Endpoint Security Risk

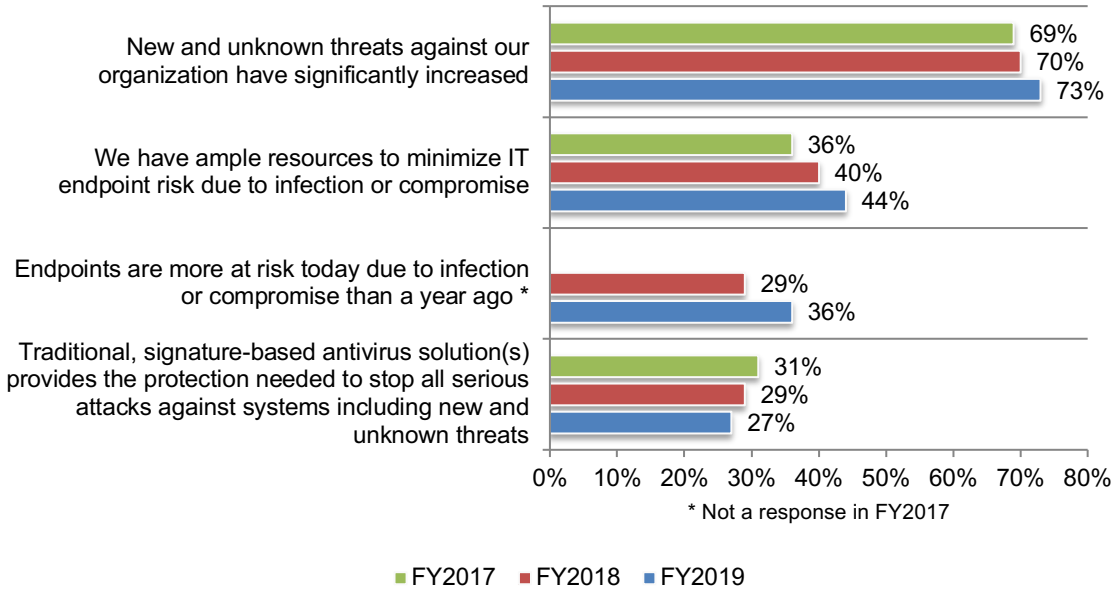
Ponemon Institute, January 2020

Part 1. Introduction

The Third Annual Study on the State of Endpoint Security Risk, sponsored by Morphisec, reveals that organizations are not making progress in reducing their endpoint security risk, especially against new and unknown threats. In fact, in this year's research, 68 percent of respondents report that their company experienced one or more endpoint attacks that successfully compromised data assets and/or IT infrastructure over the past 12 months, an increase from 54 percent of respondents in 2017.

Ponemon Institute surveyed 671 IT security professionals responsible for managing and reducing their organization's endpoint security risk. As shown in Figure 1, companies represented in this research are very concerned about the significant increase in new and unknown threats against their organization (an increase from 69 percent of respondents in 2017 to 73 percent in 2019). On a positive note, since 2017 more respondents say their organizations have ample resources to minimize IT endpoint risk due to infection or compromise (an increase from 36 percent to 44 percent).

Figure 1. Perceptions About endpoint security risk
Strongly Agree and Agree responses combined



Following are 10 key findings from this research.

1. **The frequency of attacks against endpoints is increasing and detection is difficult**. Sixty-eight (68) percent of respondents say the frequency of attacks has increased over the past 12 months. More than half of respondents (51 percent) say their organizations are ineffective at surfacing threats because their endpoint security solutions are not effective at detecting advanced attacks.

2. **The cost of successful attacks has increased from an average of $7.1 million to $8.94 million.** Costs due to the loss of IT and end-user productivity and theft of information assets have increased. The cost of system downtime has decreased significantly since 2017.

3. **New or unknown zero-day attacks are expected to more than double in the coming year.** The frequency of existing or known attacks is expected to decrease significantly from 77 percent to an anticipated 58 percent in the coming year. In contrast, the frequency of new or unknown zero-day attacks is expected to increase to 42 percent next year.

4. **An average of 80 percent of successful breaches are new or unknown "zero-day attacks."** These attacks either involved the exploitation of undisclosed vulnerabilities or the use of new/polymorphic malware variants that signature-based detection solutions do not recognize.

5. **Zero-day attacks continue to increase in frequency.** In addition to being more successful, zero-day attacks have also become more prevalent. As a result, organizations are investing more budget to protect against these threats.

6. **Most organizations either use or plan to use Microsoft Windows Defender antivirus solution.** Eighty percent (80) of respondents say they currently have (34 percent) or plan to have in the near future (46 percent) the Microsoft Windows Defender antivirus solution. The top two reasons are to reduce the number of separate endpoint security tools and the solution is on par with other antivirus tools.

7. **The challenge in the use of traditional antivirus solutions are a high number of false positives and security alerts, inadequate protection and too much complexity.** Fifty-six (56) percent of respondents say their organizations replaced their endpoint security solution in the past two years. Of these respondents, 51 percent say they kept their traditional antivirus solution but added an extra layer of protection. According to these respondents, the challenges with traditional antivirus solutions are a high number of false positives and security alerts, inadequate protection and too much complexity in the deployment and management of these solutions.

8. **Antivirus products missed an average of 60 percent of attacks.** Confidence in traditional antivirus (AV) solutions continues to drop. On average, respondents estimate their current AV is effective at blocking only 40 percent of attacks. In addition to the lack of adequate protection, respondents cite high numbers of false positives and alerts as challenges associated with managing their current AV solutions.

9. **The average time to apply, test and fully deploy patches is 97 days.** The findings reveal the difficulties in keeping endpoints effectively patched. Forty percent (40) of respondents say their organizations are taking longer to test and roll out patches in order to avoid issues and assess the impact on performance.

10. **Ineffectiveness and lack of in-house expertise are reasons not to use an EDR.** Sixty-four (64) percent of respondents who say their organizations do not have an EDR cite its ineffectiveness against new or unknown threats (65 percent of respondents) followed by 61 percent who say they don't have the staff to support.

Part 2. Key Findings

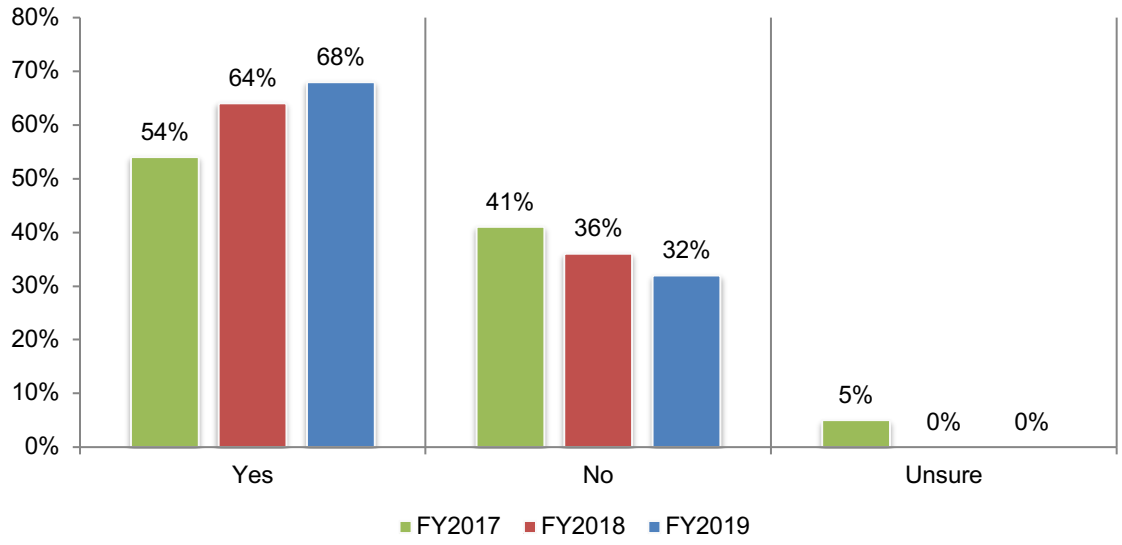
In this section of the report, we provide more details about the state of endpoint security by highlighting the financial consequences and barriers to achieving a more effective endpoint protection strategy. The complete audited findings are presented in the Appendix of this report. We have organized the report according to the following topics:

- The financial consequences of endpoint attacks
- Vulnerabilities in endpoint risk management
- How organizations are responding to endpoint attacks

The financial consequences of endpoint attacks

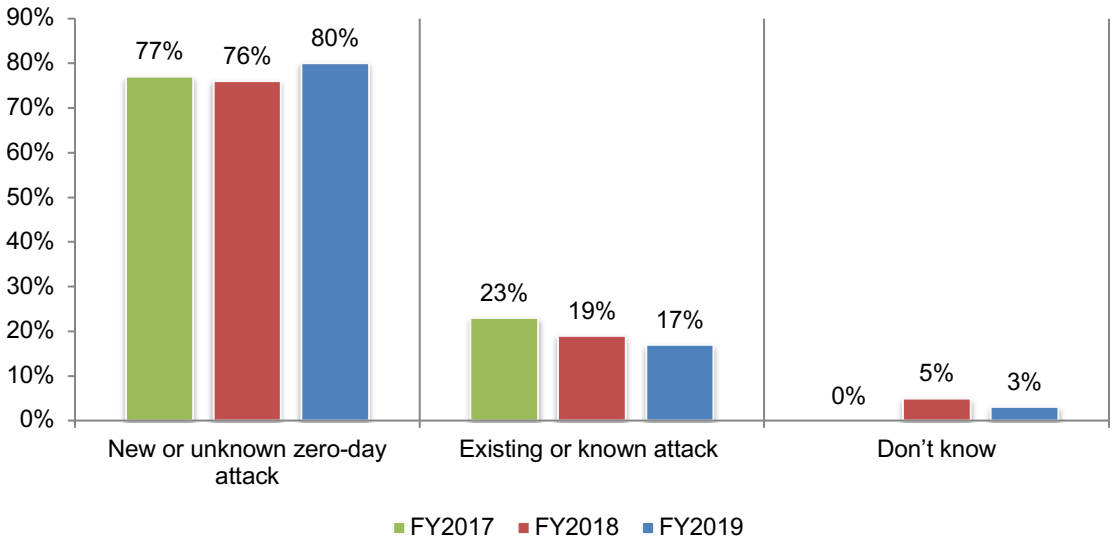
Since 2017, successful endpoint attacks have increased significantly. According to Figure 2, the percentage of respondents reporting that their organizations experienced an endpoint attack that compromised data assets and/or IT infrastructure increased from 54 percent in 2017 to 68 percent in this year's research.

Figure 2. Has your organization experienced one or more endpoint attacks that have successfully compromised data assets and/or IT infrastructure over the past two years?



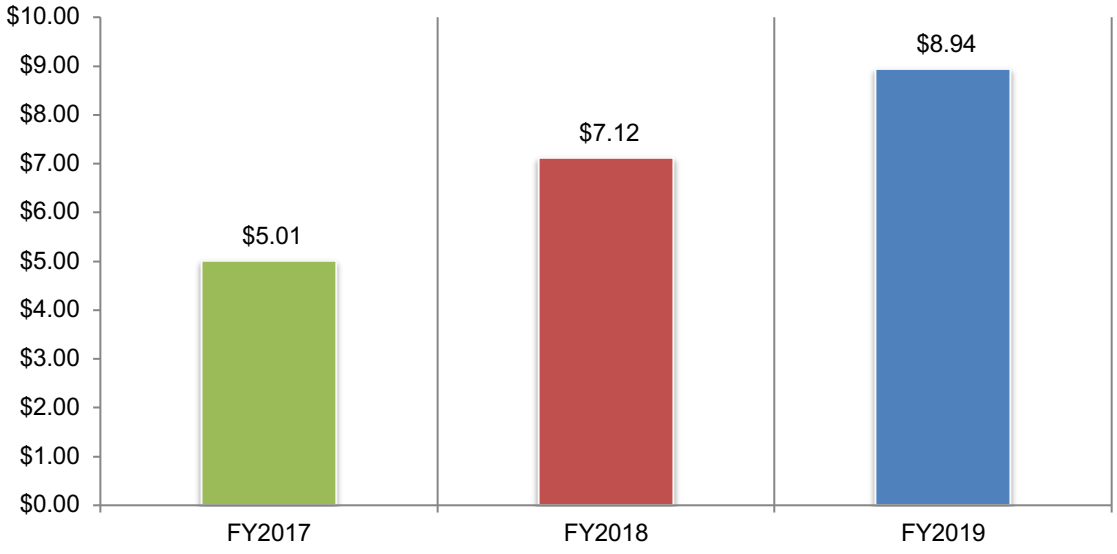
Most organizations have had to deal with new or unknown zero-day attacks. As shown in Figure 3, 80 percent of respondents say the type of endpoint attack they experienced was a new or unknown zero-day attack.

Figure 3. What type of attack do you believe compromised your organization?



The average economic loss from endpoint attacks increases. The average cost companies represented in this research incurred increased from $7.12 million in 2018 to $8.94 million in 2019.

Figure 4. Growth in the total economic loss incurred as a result of endpoint attacks
Extrapolated values presented

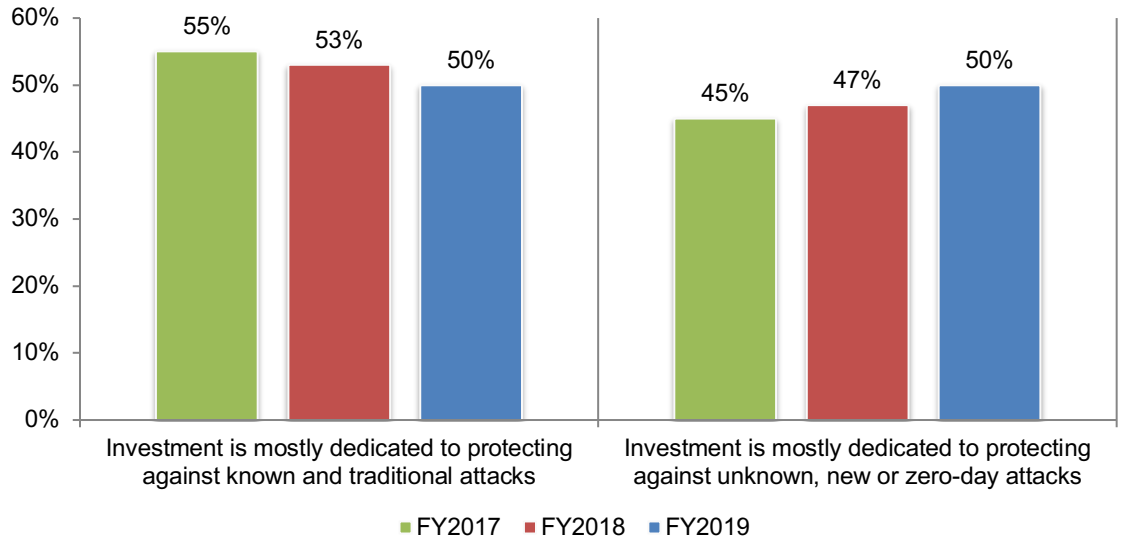


The costliest consequence of a successful endpoint attack is IT and end-user productivity loss. Table 1 lists six cost consequences that result from one or more successful endpoint attacks over the past 12 months. Respondents were asked to allocate 100 points based on the total cost for each consequence listed. As shown, the cost of IT and end-user productivity loss and theft of information assets has increased significantly since 2017. The cost of system downtime has decreased.

Table 1. Trends in the cost consequences of one or more successful endpoint attacks over the past 12 months	FY2017	FY2018	FY2019
IT and end-user productivity loss	30%	35%	37%
Theft of information assets	23%	27%	30%
System downtime	25%	20%	15%
Damage to IT infrastructure	10%	8%	9%
Reputation/brand damage	8%	7%	5%
Lawsuits, fines and regulatory actions	4%	3%	4%
Total	100%	100%	100%

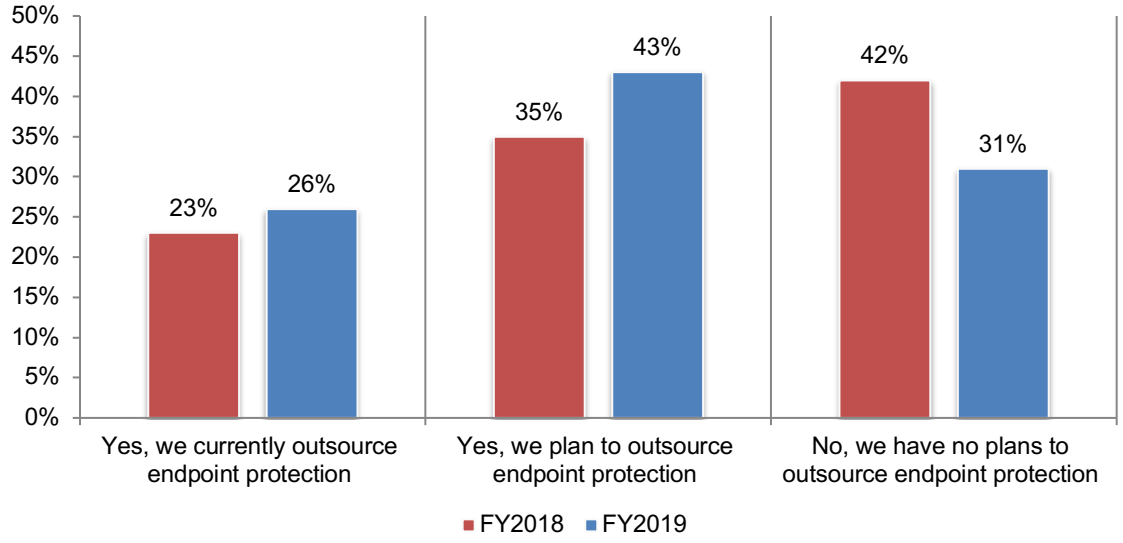
More investment is being allocated to protecting against unknown, new or zero-day attacks. The average total IT budget has increased from $165 million in 2018 to $186.5 million in this year's study. The percentage of the budget allocated to endpoint protection averages 5 percent. Figure 5 shows how organizations allocate their budget to endpoint protection.

Figure 5. How does your organization allocate most of its current endpoint security investment?



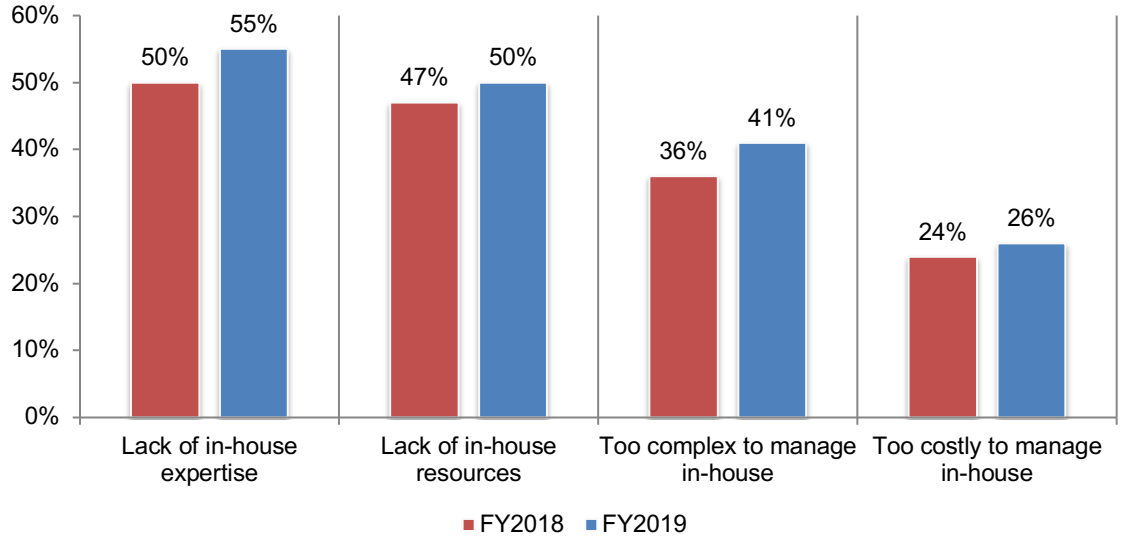
To manage risk, organizations plan to allocate resources to the outsourcing of endpoint protection. As shown in Figure 6, 69 percent of respondents say their organizations either currently or plan to outsource endpoint protection to a managed service provider or other third party.

Figure 6. Does your organization outsource or plan to outsource endpoint protection to a managed service provider or other third party?



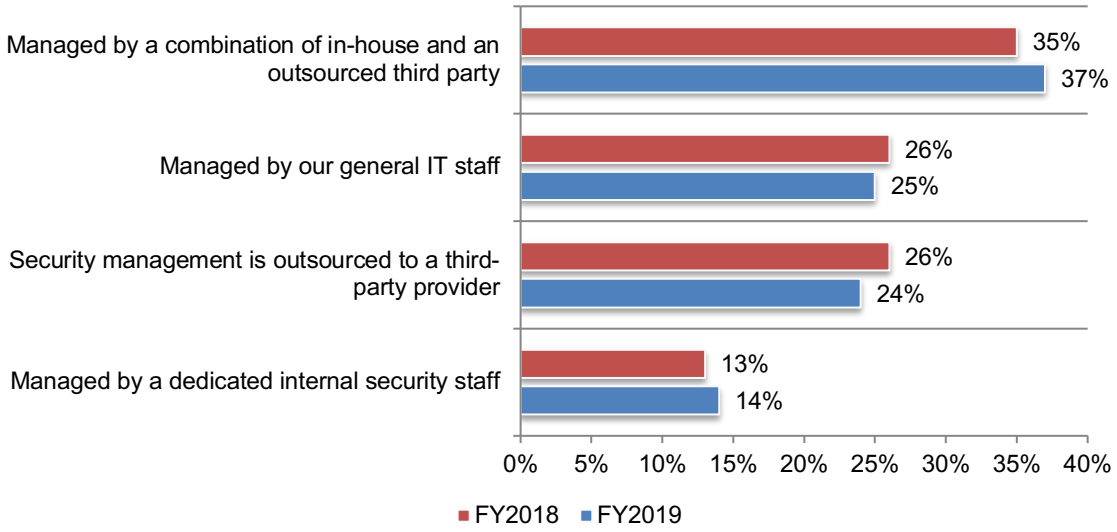
Reasons to outsource are a lack of in-house expertise and resources. According to Figure 7, only 26 percent of respondents say the reason to outsource is due to the cost of managing endpoint protection in-house.

Figure 7. Why does your organization outsource or plan to outsource?
More than one response permitted



Outsourcing supplements the lack of in-house expertise. As shown in Figure 8, only 14 percent of respondents say they have a dedicated internal security staff. Most organizations staff the IT security function with a combination of outsourcing and in-house personnel, or completely outsource it to a third-party provider.

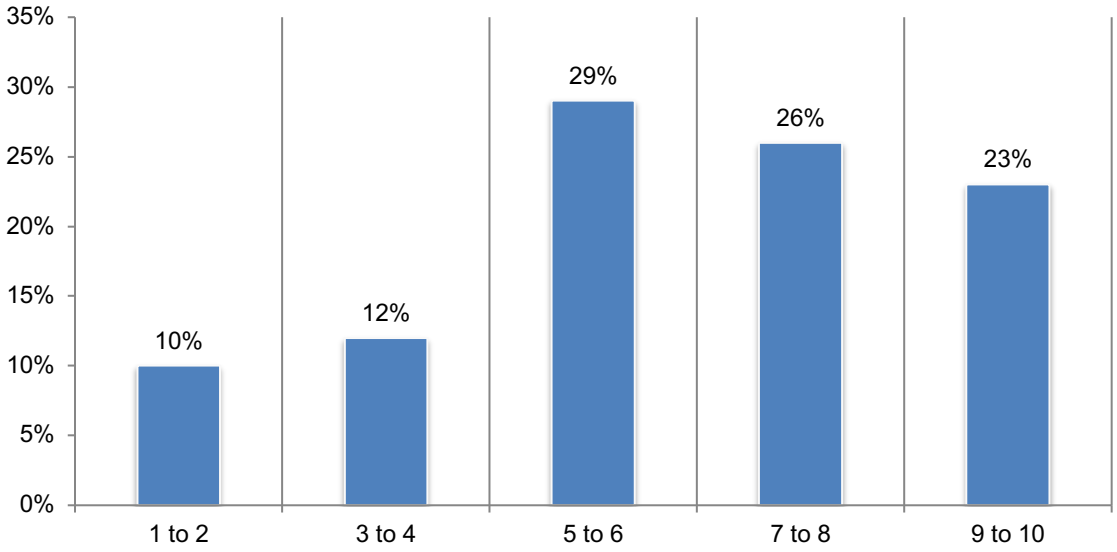
Figure 8. What best describes your organization's IT security staffing?



Vulnerabilities in endpoint risk management

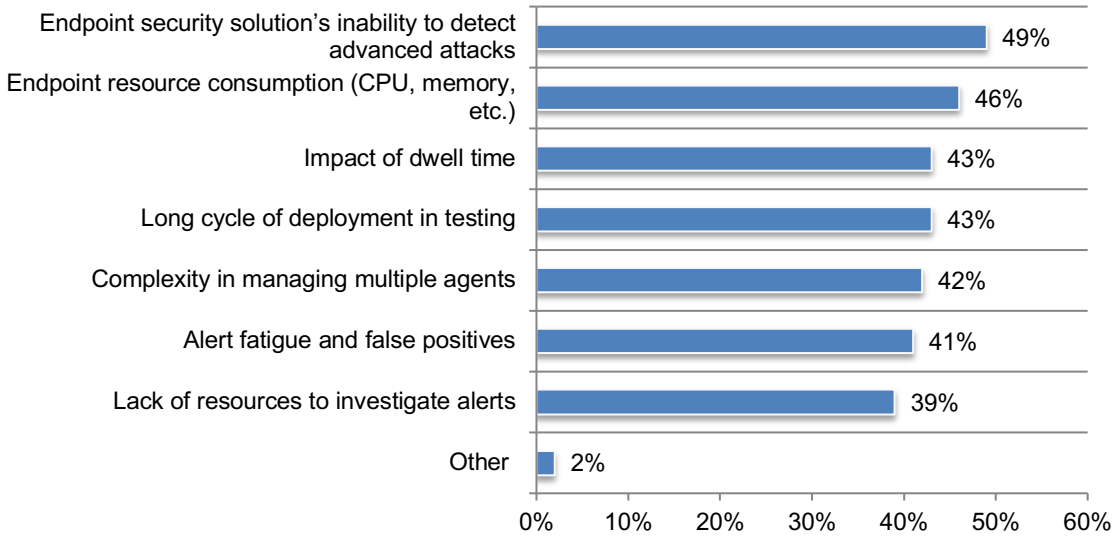
More than half of respondents rate the security team's ability to detect endpoint attacks as ineffective. Respondents were asked to rate their security team's effectiveness in detecting endpoint attacks on a scale from 1 = not effective to 10 = highly effective. As shown in Figure 9, 51 respondents rate effectiveness at less than 5 to 6 on the 10-point scale.

Figure 9. How effective is your security team's ability to detect endpoint attacks?
On a scale from 1 = not effective to 10 = highly effective



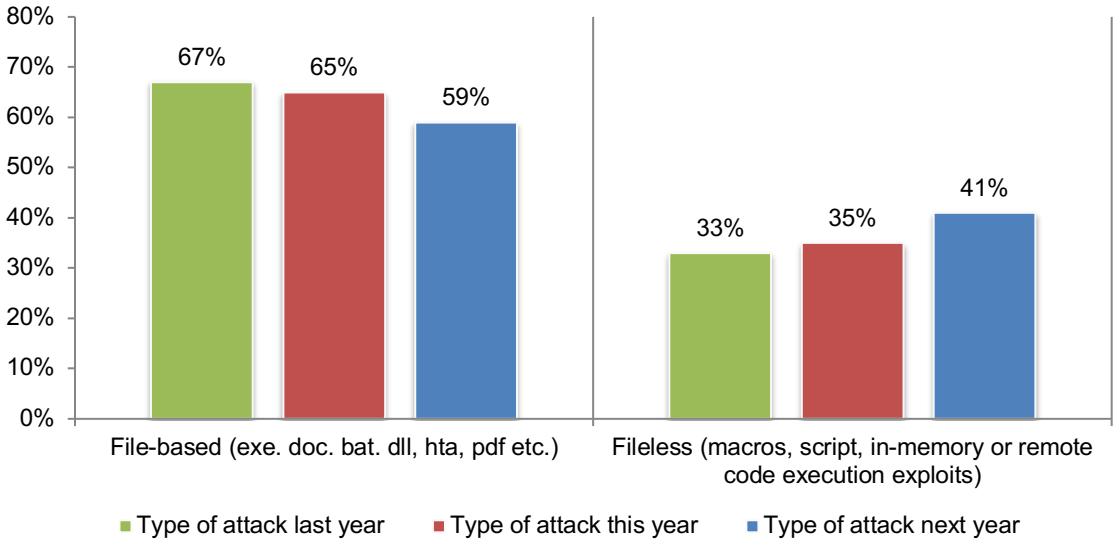
The inability to detect advanced attacks and endpoint resource consumption are the top reasons security teams are considered ineffective, as shown in Figure 10.

Figure 10. Why is your security team not effective in detecting endpoint attacks?
More than one response permitted



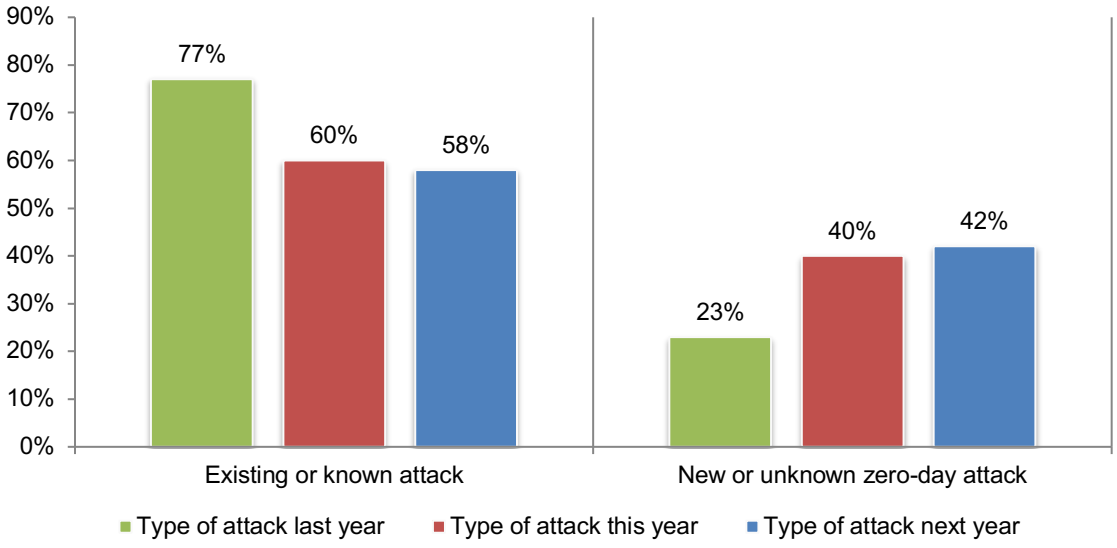
Fileless attacks are expected to increase. Since 2018, the frequency of file-based attacks has steadily decreased while the frequency of fileless attacks are increasing. As shown in Figure 11, survey respondents expect 41 percent of attacks to be fileless in the coming year and 59 percent to be file-based.

Figure 11. Frequency of fileless and file-based attacks



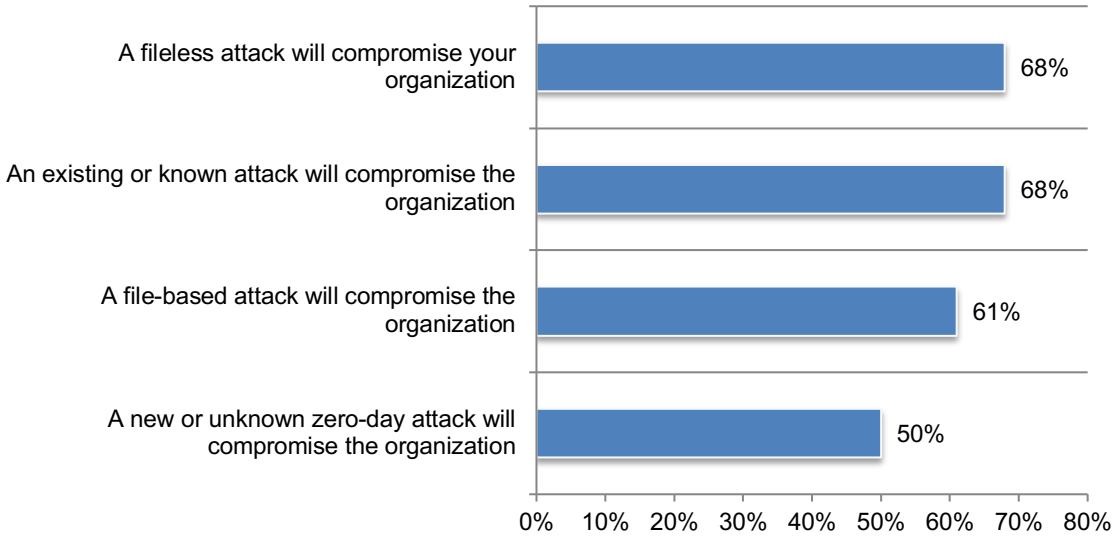
New or unknown zero-day attacks are expected to more than double in the coming year. As shown in Figure 12, the frequency of existing or known attacks is expected to decrease significantly from 77 percent to an anticipated 58 percent in the coming year. In contrast, the frequency of new or unknown zero-day attacks is expected to increase to 42 percent next year.

Figure 12. Frequency of existing or known attacks and new or unknown zero-day attacks



Fileless and existing or known attacks are equally likely to compromise organizations. As shown in Figure 13, respondents expect that fileless and known attacks are equally likely to compromise their organizations (68 percent). Fifty percent (50) of respondents say it is likely their organization will experience a new or unknown zero-day attack.

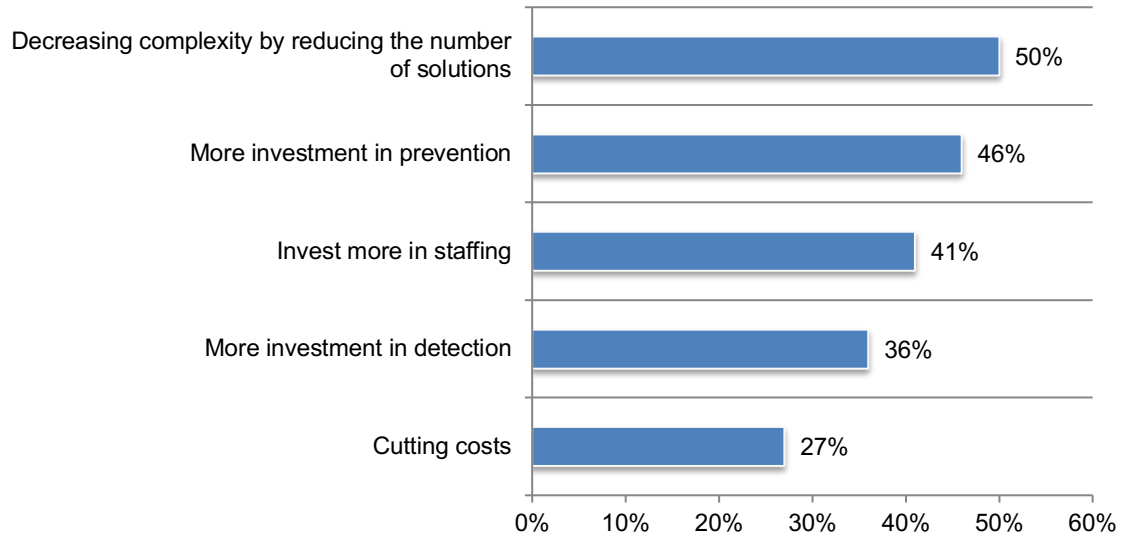
Figure 13. Likelihood of attacks compromising your organization
Very likely and Likely responses combined



How organizations are responding to endpoint attacks

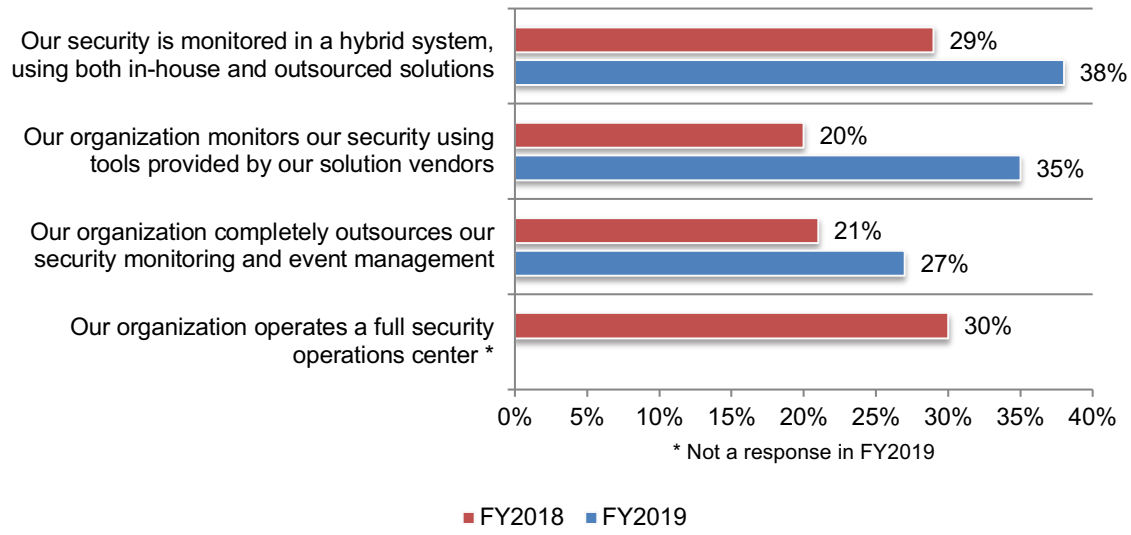
Complexity is considered a barrier to improving endpoint security. As shown in Figure 14, 50 percent of respondents say their organizations are reducing the number of solutions to decrease complexity as part of their endpoint security strategy. Investments in prevention and staffing are also considered priorities.

Figure 14. What are your two major priorities in your endpoint security strategy?
Two responses permitted



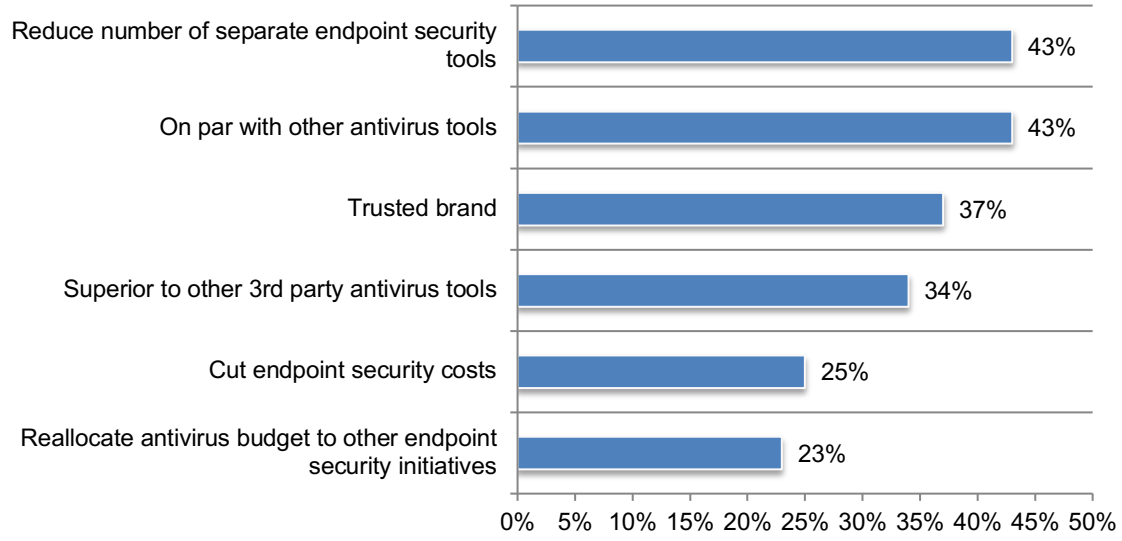
Third parties are involved in monitoring and responding to security events. According to Figure 15, most organizations are monitoring security in a hybrid system or using tools provided by solution vendors. Twenty-seven (27) percent of respondents say security monitoring and event management is completely outsourced. As discussed previously, most organizations staff the IT security function with a combination of third parties and in-house personnel.

Figure 15. How do you monitor and respond to security events in your organization?



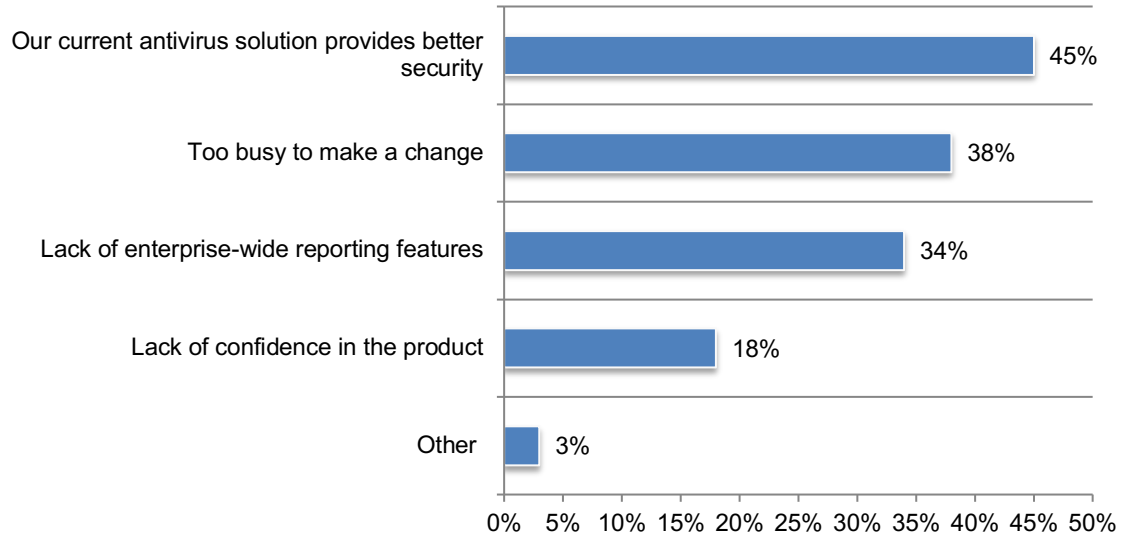
Most organizations either use or plan to use Microsoft Windows Defender antivirus solution. Eighty percent (80) of respondents say they currently have (34 percent) or plan to have in the near future (46 percent) the Microsoft Windows Defender antivirus solution. The top two reasons, as presented in Figure 16, are to reduce the number of separate endpoint security tools and the solution is on par with other antivirus tools.

Figure 16. If you use or plan to use Windows Defender, why?
More than one response permitted



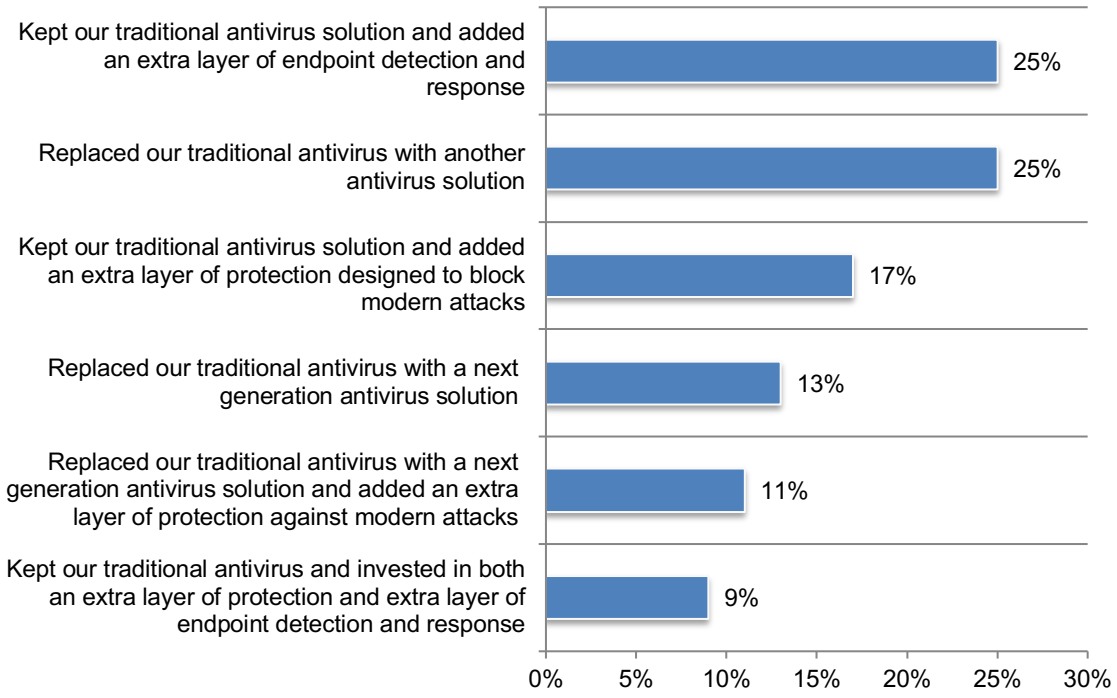
The 20 percent of respondents who say their organizations will not adopt the Microsoft Windows Defender antivirus solution say their current antivirus solution provides better security or they are too busy to change.

Figure 17. If you do not use or plan to use Windows Defender, why?
More than one response permitted



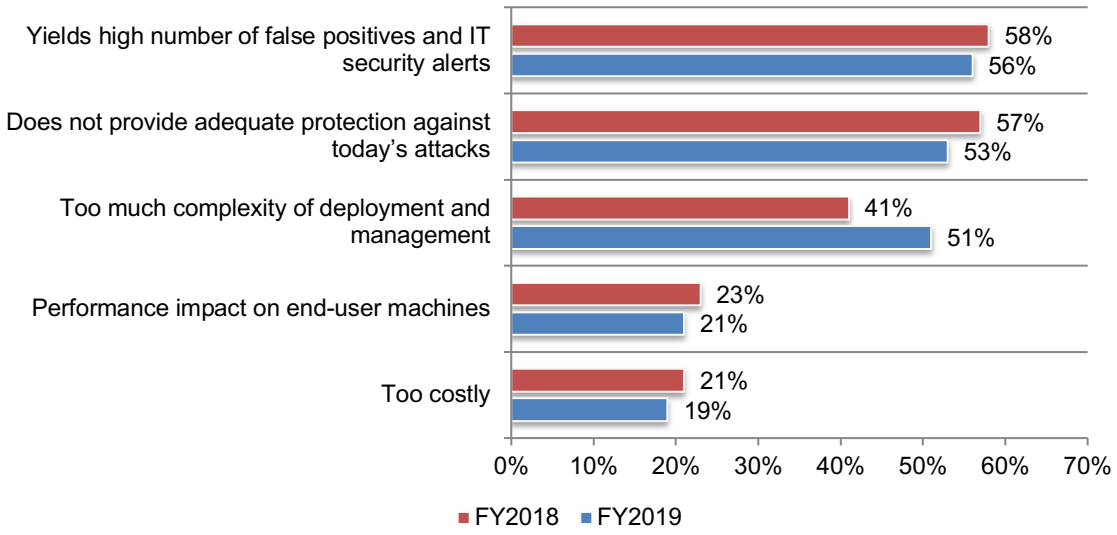
As part of their endpoint security strategy, 56 percent of respondents say their organizations replaced their endpoint security solution within the last two years. According to Figure 18, of the 56 percent of respondents who say their organizations replaced their endpoint security solution, 51 percent added an extra layer of protection to their traditional antivirus solution (25 percent + 17 percent + 9 percent). Forty-nine (49) percent of respondents say their organizations replaced their traditional antivirus solution (25 percent + 13 percent + 11 percent)

Figure 18. What replaced your organization's endpoint security solution?
Only one choice permitted



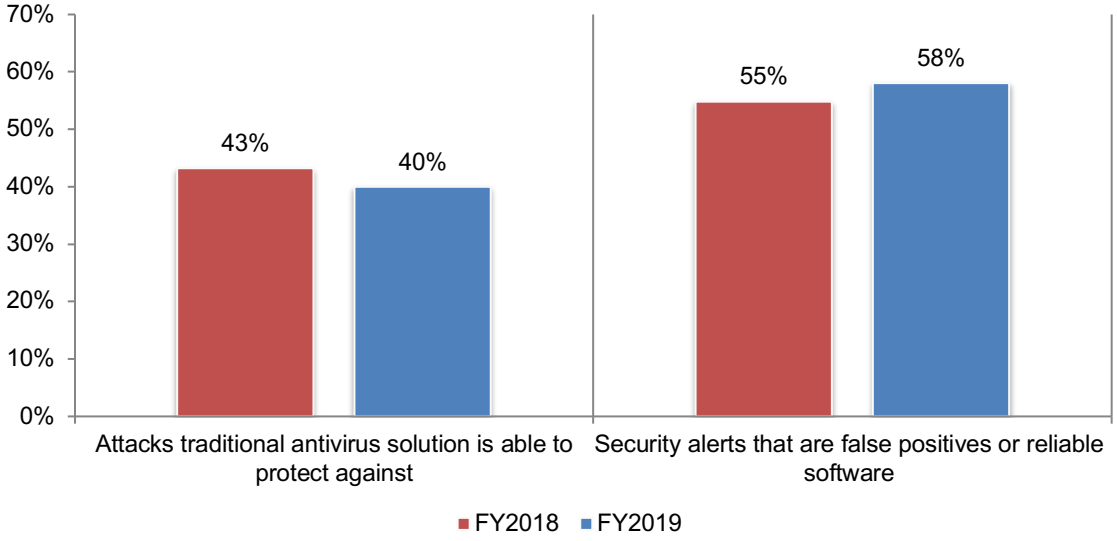
The challenges with traditional antivirus solutions include a high number of false positives and IT security alerts, inadequate protection and too much complexity. In this year's research, 51 percent of respondents say there is too much complexity of deployment and management of their traditional antivirus solutions, an increase from 41 percent in 2018 as shown in Figure 19. The top two challenges are the high number of false positives and IT security alerts (56 percent of respondents) and inadequate protection against attacks.

Figure 19. What are the biggest challenges with your traditional antivirus solutions?
Two responses permitted



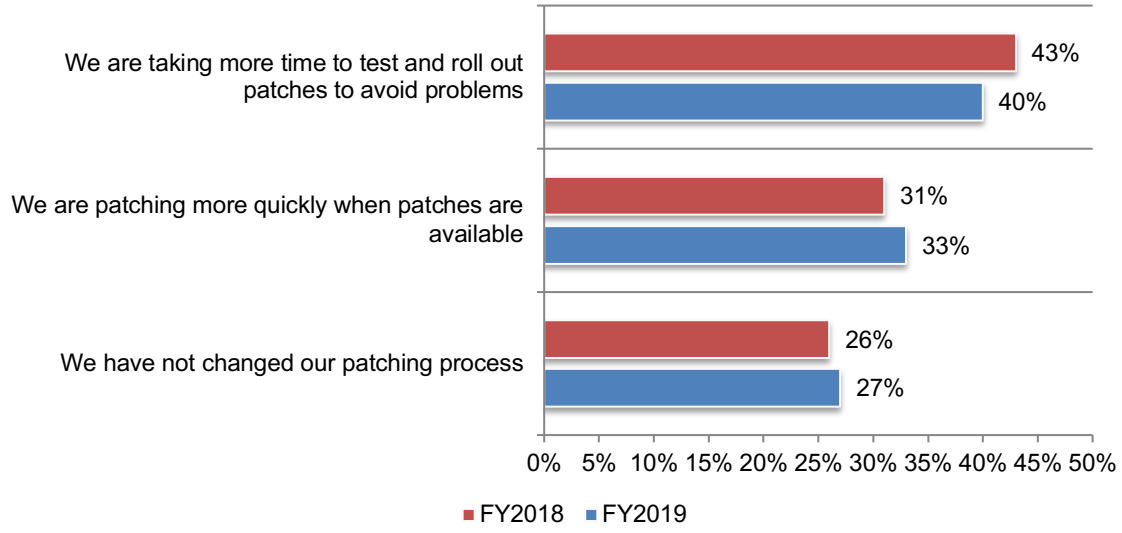
Antivirus products missed an average of 60 percent of attacks. Confidence in traditional antivirus solutions continues to drop. On average, respondents estimate their current antivirus is effective at blocking only 40 percent of attacks. In addition to the lack of adequate protection, respondents cite high numbers of false positives and alerts as challenges associated with managing their current antivirus solutions.

Figure 20. What percentage of attacks can your traditional antivirus protect against and what percentage of security alerts are false positives or reliable software?
Extrapolated values presented



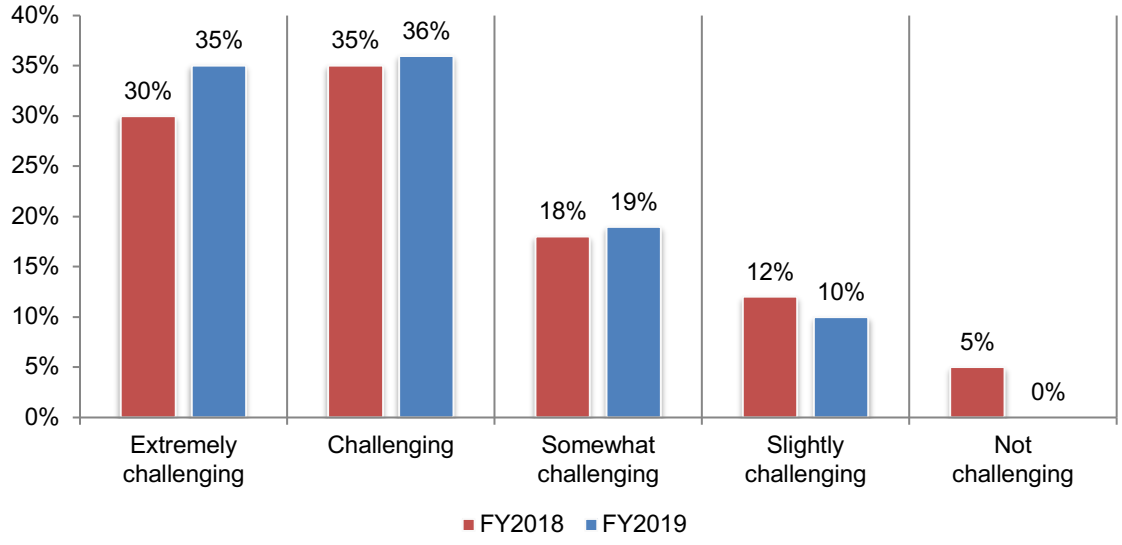
Only one-third of organizations are patching vulnerabilities more quickly. As shown in Figure 21, 33 percent of respondents say their organizations are patching more quickly when patches are available. Forty percent (40) of respondents are taking more time to test and roll out patches to avoid problems.

Figure 21. Has there been a change in your organization's process for patching vulnerabilities in the past 12 months?
Only one choice permitted



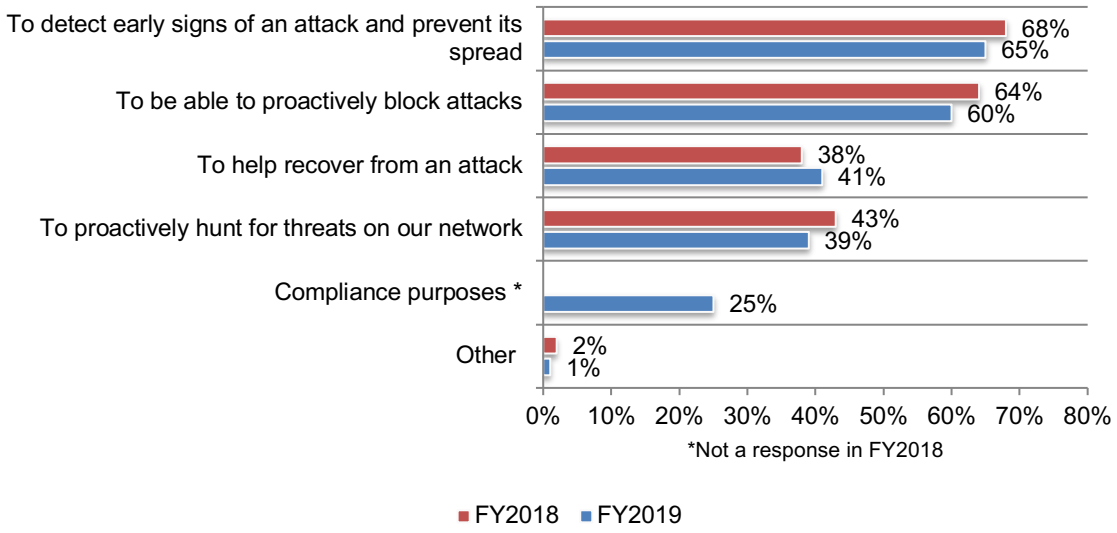
Keeping up with patch updates is more challenging. Seventy-one (71) percent of respondents say it is either extremely challenging or challenging to keep up with the frequency of patch updates, as shown in Figure 22. This is an increase from 65 percent of respondents in the 2018 research.

Figure 22. How challenging is it to keep up with the frequency of patch updates?



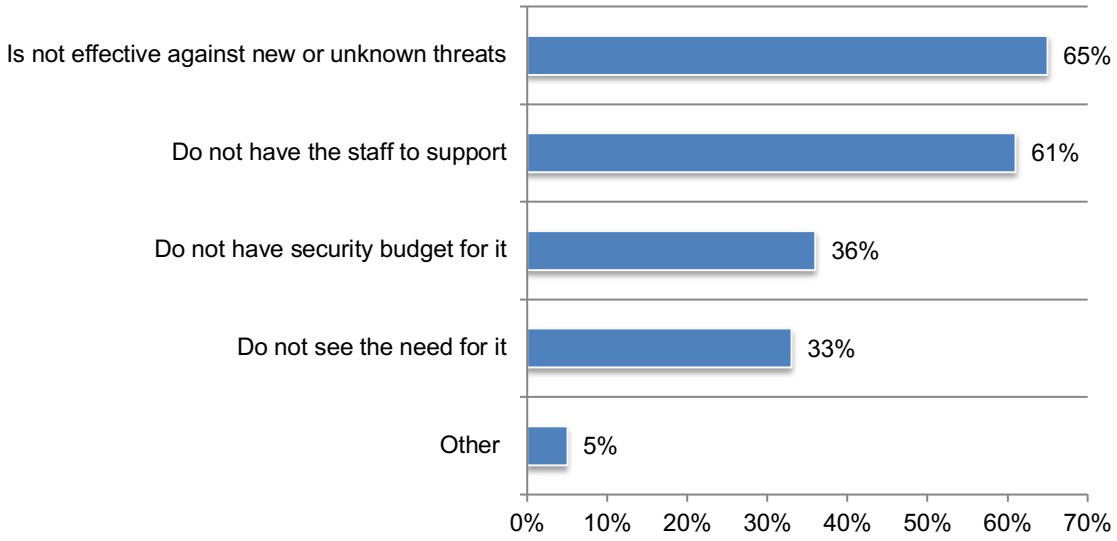
Thirty-six (36) percent of respondents say their organizations have endpoint detection and response (EDR) tools. As shown in Figure 23, 65 percent of respondents in organizations with EDR tools say its use is to detect early signs of an attack and prevent its spread followed by the ability, and 60 percent say it is to proactively block attacks.

Figure 23. Why do you have an EDR?
More than one response permitted



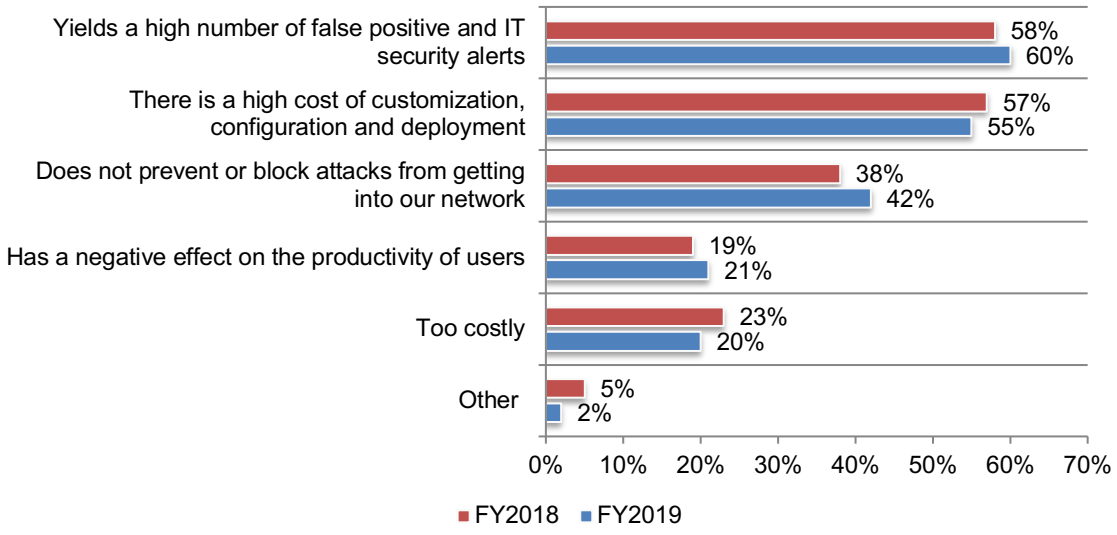
Ineffectiveness and lack of in-house expertise are reasons not to use an EDR. Sixty-four (64) percent of respondents who say their organizations do not have an EDR cite its ineffectiveness against new or unknown threats (65 percent of respondents) followed by 61 percent who say they don't have the staff to support, as shown in Figure 24.

Figure 24. Why don't you have an EDR?
Two responses permitted



Too many false positives and the cost are the top challenges with EDRs. Of the 36 percent of respondents who say their organizations have an EDR solution, 60 percent say it yields a high number of false positives and IT security alerts and 55 percent say there is a high cost of customization, configuration and deployment.

Figure 25. What are the top challenges with your organization's EDR?
Two responses permitted



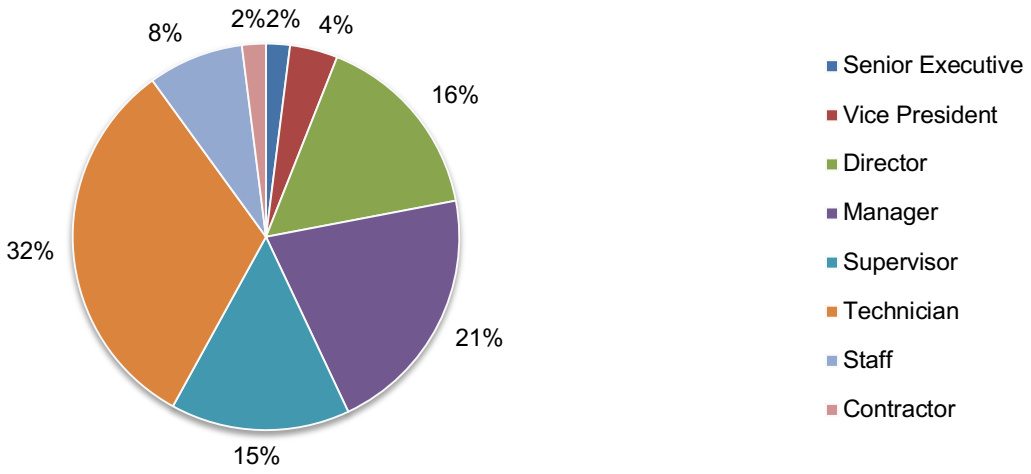
Part 3. Methods

A sampling frame of 17,655 IT and IT security practitioners located in the United States were selected as participants in this survey. Table 2 shows 814 total returns. Screening and reliability checks required the removal of 143 surveys. Our final sample consisted of 671 surveys or a 3.8 percent response.

Table 2. Survey response	FY2017	FY2018	FY2019
Total sampling frame	18,289	17,889	17,655
Total survey returns	830	817	814
Rejected surveys	165	157	143
Final sample	665	660	671
Response rate	3.6%	3.7%	3.8%

The following pie chart summarizes the position level of qualified respondents. At 32 percent, the largest segment contains those who are rank-and-file level employees (e.g., technicians or analysts). The smallest segment (2 percent) includes senior-level executives (C-suite). More than half (58 percent) of respondents are at or above the supervisory level.

Figure 26. Position level of respondents



As shown in Figure 27, 46 percent of respondents report to the chief information officer, 27 percent of respondents report to the chief information security officer, and 10 percent of respondents indicated they report to the compliance officer.

Figure 27. Reporting channel or chain of command

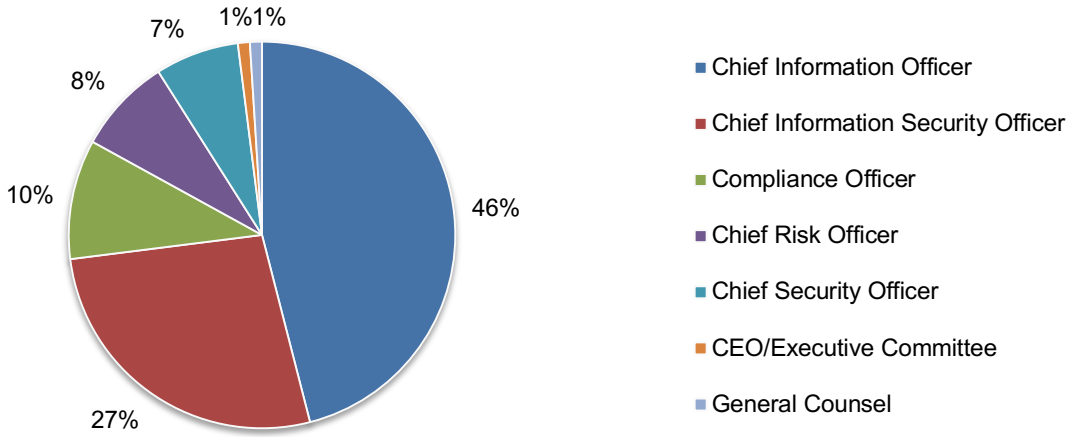


Figure 28 shows the percentage distribution of respondents' companies across 14 industries. Financial services represents the largest industry sector (at 19 percent of respondents), which includes banking, insurance, brokerage, investment management and payment processing. Other large verticals include public services, health and pharma, retailing and services.

Figure 28. Primary industry sector of respondents' companies

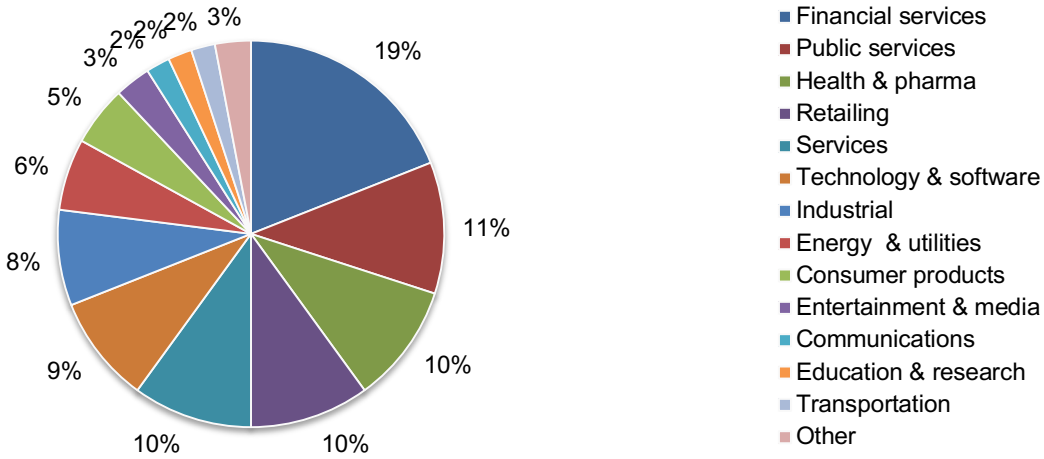
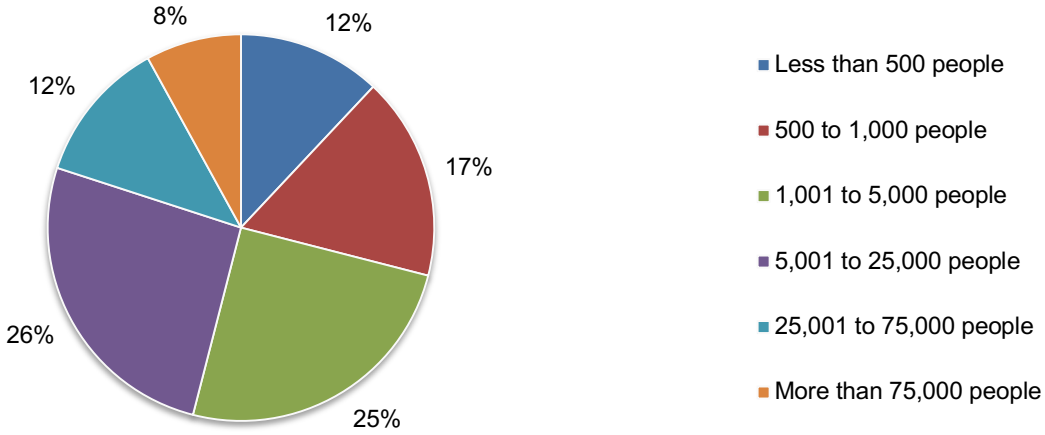


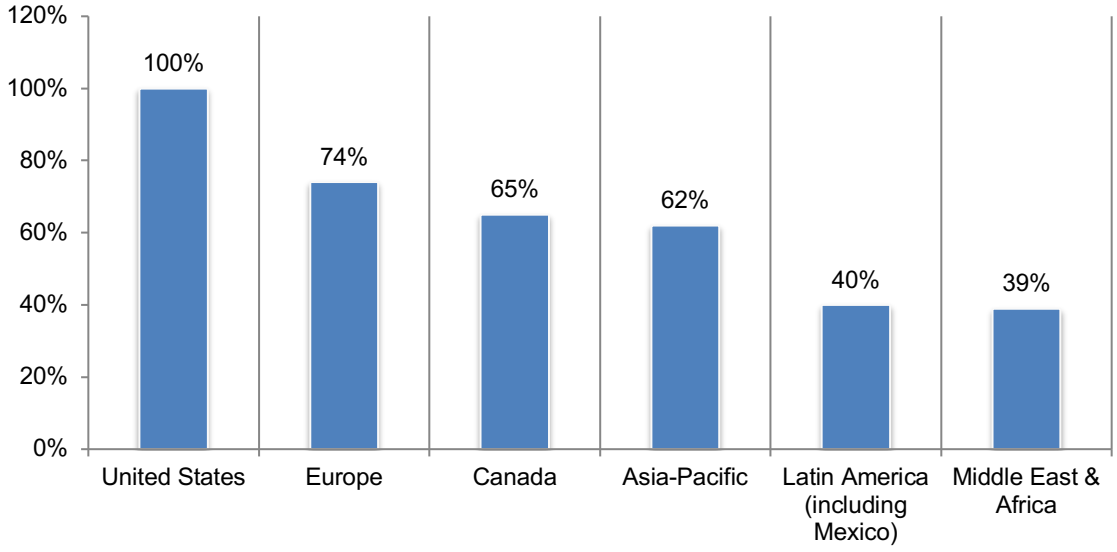
Figure 29 summarizes the total worldwide headcount of respondents' companies. In the context of this study, headcount serves as an indicator of size. At 26 percent, the largest segment contains larger-sized organizations with 5,000 to 25,000 full-time equivalent employees. The smallest segment (8 percent) includes larger-sized organizations with 75,000 or more employees.

Figure 29. Global headcount of respondents' companies



In addition to the United States, 74 percent of respondents have employees located in Europe, 65 percent of respondents have employees located in Canada followed by 62 percent in Asia-Pacific.

Figure 30. Geographic location of employees



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 in various organizations within the United States. 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 October 14, 2019, to October 28, 2019.

Survey response	FY2019	FY2018	FY2017
Total sampling frame	17,655	17,889	18,289
Total survey returns	814	817	830
Rejected surveys	143	157	165
Final sample	671	660	665
Response rate	3.8%	3.7%	3.6%

Part 1. Screening

S1. What is your role in your organization's endpoint security strategy?	FY2019	FY2018	FY2017
None (stop)	0%	0%	0%
Responsible for purchase of endpoint security solutions	46%	41%	45%
Responsible for the evaluation of endpoint security solutions	47%	44%	40%
Responsible for influencing the purchase of endpoint security solutions	51%	50%	47%
Responsible for managing and administering endpoint security solutions	49%	56%	56%
Total	193%	191%	188%

S2. How many network-connected endpoints (servers, laptops, workstations) does your organization support?	FY2019	FY2018
Less than 25 (stop)	0%	0%
25 to 100	6%	7%
101 to 500	12%	13%
501 to 1,000	37%	34%
1,001 to 5,000	21%	26%
5,001 to 10,000	16%	11%
More than 10,000	8%	9%
Total	100%	100%
Extrapolated value	3,107	2,983

S3. What best describes your role within your organization's IT department?	FY2019	FY2018	FY2017
IT leadership (CIO/director)	10%	10%	11%
Security leadership (CSO/CISO)	22%	21%	20%
IT management	8%	11%	13%
Security analyst	7%	8%	
IT operations	13%	16%	20%
IT administration	6%		
Security management	8%	8%	9%
Security monitoring and response	7%	8%	7%
Data administration	6%	5%	8%
Compliance administration	7%	8%	9%
Applications development	6%	5%	3%
I'm not involved in my organization's Security or IT function (stop)	0%	0%	0%
Total	100%	100%	100%

Part 2: Attributions

Please rate the following four (4) statements using the scale provided below each item. **Strongly Agree and Agree.**	FY2019	FY2018	FY2017
Q1. We have ample resources to minimize IT endpoint risk due to infection or compromise.	44%	40%	36%
Q2. Our organization's endpoints are more at risk today due to infection or compromise than a year ago.	36%	29%	
Q3. New and unknown threats against our organization have significantly increased.	73%	70%	69%
Q4. Our traditional, signature-based antivirus solution(s) provides the protection needed to stop **all** serious attacks against my systems including new and unknown threats.	27%	29%	31%
Q5. Our endpoint security strategy will increasingly rely upon detection and response tools over early prevention tools.	51%		

Part 3. Evolution of endpoint attacks

Q6. Please allocate the distribution of attacks that have targeted your organization based on attack type and include an estimated target for 2020. Please use all 100 points.	FY2019	FY2018	FY2017
Q6a. Type of attack (last year)	Points	Points	Points
Fileless (macros, script, in-memory or remote code execution exploits)	33	30	20
File-based (exe. doc. bat. dll, hta, pdf etc.)	67	70	80
Total points	100	100	100

Q6b. Type of attack (this year)	Points	Points	Points
Fileless (macros, script, in-memory or remote code execution exploits)	35	35	29
File-based (exe. doc. bat. dll, hta, pdf etc.)	65	65	71
Total points	100	100	100

Q6c. Type of attack (next year)	Points	Points	Points
Fileless (macros, script, in-memory or remote code execution exploits)	41	38	35
File-based (exe. doc. bat. dll, hta, pdf etc.)	59	62	65
Total points	100	100	100

Q7. Please allocate the distribution of attacks that have targeted your organization based on attack type and include an estimated target for 2020. Please use all 100 points.	FY2019	FY2018	FY2017
Q7a. Type of attack (last year)	Points	Points	
Existing or known attack	77	75	
New or unknown zero-day attack	23	25	
Total points	100	100	

Q7b. Type of attack (this year)	Points	Points	Points
Existing or known attack	60	63	69
New or unknown zero-day attack	40	37	31
Total points	100	100	100

Q7c. Type of attack (next year)	Points	Points	Points
Existing or known attack	58	63	
New or unknown zero-day attack	42	37	
Total points	100	100	

Q8. How likely is it an existing or known attack will compromise your organization?	FY2019
Very likely	33%
Likely	35%
Somewhat likely	24%
Not likely	8%
Total	100%

Q9. How likely is a new or unknown zero-day attack will compromise your organization?	FY2019
Very likely	25%
Likely	25%
Somewhat likely	41%
Not likely	9%
Total	100%

Q10. How likely is a fileless attack (e.g. macros, scripts, in-memory or remote code execution exploits) will compromise your organization?	FY2019
Very likely	30%
Likely	38%
Somewhat likely	24%
Not likely	8%
Total	100%

Q11. How likely is a file-based attack (e.g. exe.doc, bat.dill, hta.pdf etc.) will compromise your organization?	FY2019
Very likely	27%
Likely	34%
Somewhat likely	28%
Not likely	11%
Total	100%

Q12. How does your organization allocate most of its current endpoint security investment? Please select only one choice.	FY2019	FY2018	FY2017
Investment is mostly dedicated to protecting against known and traditional attacks	50%	53%	55%
Investment is mostly dedicated to protecting against unknown, new or zero-day attacks	50%	47%	45%
Total	100%	100%	100%

Q13a. Has your company experienced one or more endpoint attacks that have successfully compromised data assets and/or IT infrastructure over the past 12 months?	FY2019	FY2018	FY2017
Yes	68%	64%	54%
No	32%	36%	41%
Unsure		0%	5%
Total	100%	100%	100%

Q13b. If yes, what type of attack do you believe compromised your organization?	FY2019	FY2018	FY2017
Existing or known attack	17%	19%	23%
New or unknown zero-day attack	80%	76%	77%
Don't know	3%	5%	0%
Total	100%	100%	100%

Q14. With your current enabling technologies, processes and in-house expertise, what percentage of attacks to your organization's endpoints can be realistically stopped?	FY2019	FY2018	FY2017*
Less than 10%	14%	13%	
10% to 25%	18%	18%	
26% to 50%	26%	21%	
51% to 75%	22%	25%	
76% to 100%	20%	23%	
Total	100%	100%	
Extrapolated value	45%	48%	54%

**FY2017 used a different scale*

Part 4. Current and future endpoint security tools

Q15. What are your two major priorities in your endpoint security strategy? Please select your top two choices.	FY2019
More investment in prevention	46%
More investment in detection	36%
Cutting costs	27%
Decreasing complexity by reducing the number of solutions	50%
Invest more in staffing	41%
Other	0%
Total	200%

Q16a. Please rate the effectiveness of your security team's ability to detect endpoint attacks on a scale from 1 = not effective to 10 = effective.	FY2019
1 to 2	10%
3 to 4	12%
5 to 6	29%
7 to 8	26%
9 to 10	23%
Total	100%
Extrapolated value	6.30

Q16b. If not effective (responses 5 and below) why?	FY2019
Lack of resources to investigate alerts	39%
Complexity in managing multiple agents	42%
Long cycle of deployment in testing	43%
Endpoint resource consumption (CPU, memory, etc.)	46%
Endpoint security solution's inability to detect advanced attacks	49%
Alert fatigue and false positives	41%
Impact of dwell time	43%
Other	2%
Total	305%

Q17. Does your organization currently use memory protection to protect its endpoints?	FY2019
Yes	27%
No	73%
Total	100%

Q18a. Does your organization use or plan to use Microsoft Windows Defender antivirus solution?	FY2019
Yes, currently have	34%
Will have in the near future	46%
We have no plans	20%
Total	100%

Q18b. If yes, why? Please select all that apply.	FY2019
Cut endpoint security costs	25%
Reallocate antivirus budget to other endpoint security initiatives	23%
Superior to other 3rd party antivirus tools	34%
On par with other antivirus tools	43%
Trusted brand	37%
Reduce number of separate endpoint security tools	43%
Total	205%

Q18c. If no, why? Please select all that apply.	FY2019
Too busy to make a change	38%
Lack of confidence in the product	18%
Our current antivirus solution provides better security	45%
Lack of enterprise-wide reporting features	34%
Other	3%
Total	138%

Q19a. In the past 24 months, has your organization replaced its endpoint security solution?	FY2019
Yes	56%
No	44%
Total	100%

Q19b. If yes, what replaced your organization's endpoint security solution? Please select one choice	FY2019
Replaced our traditional antivirus with another antivirus solution (please skip to Q22)	25%
Replaced our traditional antivirus with a next generation antivirus solution (please skip to Q22)	13%
Replaced our traditional antivirus with a next generation antivirus solution and added an extra layer of protection against modern attacks (please skip to Q22)	11%
Kept our traditional antivirus solution and added an extra layer of protection designed to block modern attacks	17%
Kept our traditional antivirus solution and added an extra layer of endpoint detection and response	25%
Kept our traditional antivirus and invested in both an extra layer of protection and extra layer of endpoint detection and response	9%
Other (please specify)	0%
Total	100%

Q20. What are the biggest challenges with your **traditional antivirus** solutions? Please select the top two challenges.	FY2019	FY2018
Does not provide adequate protection against today's attacks	53%	57%
Yields high number of false positives and IT security alerts	56%	58%
Performance impact on end-user machines	21%	23%
Too much complexity of deployment and management	51%	41%
Too costly	19%	21%
Other (please specify)	0%	0%
Total	200%	200%

Q21. What percentage of attacks can your **traditional antivirus** solution protect against?	FY2019	FY2018
Less than 10%	14%	12%
10% to 25%	26%	23%
26% to 50%	27%	27%
51% to 75%	18%	20%
76% to 100%	15%	18%
Total	100%	100%
Extrapolated value	40%	43%

Q22. What percentage of all security alerts from your **antivirus** are false positives or reliable software (e.g. software that is good but the protection agent thinks it is bad and blocks user)?	FY2019	FY2018	FY2017
Less than 10%	10%	12%	
10% to 25%	15%	11%	
26% to 50%	9%	19%	
51% to 75%	27%	23%	
76% to 100%	39%	35%	
Total	100%	100%	
Extrapolated value	58%	55%	48%

**FY2017 used a different scale*

Q23. Does your organization have a patch management process to fix discovered software problems, bugs or vulnerabilities?	FY2019	FY2018
Yes	56%	53%
No	44%	47%
Total	100%	100%

Q24. Has there been a change in your organization's process for patching vulnerabilities in the past 12 months?	FY2019	FY2018
We are patching more quickly when patches are available	33%	31%
We are taking more time to test and roll out patches to avoid problems	40%	43%
We have not changed our patching process	27%	26%
Total	100%	100%

Q25. How long does it take to apply, test and fully deploy patches?	FY2019	FY2018
1 day	1%	3%
3 days	3%	5%
1 week	0%	3%
2 weeks	2%	4%
3 weeks	10%	8%
4 weeks	5%	7%
5 weeks	9%	10%
6 weeks	11%	9%
7 weeks	7%	6%
8 weeks	10%	9%
9 weeks to 6 months	18%	15%
7 months to 1 year	15%	13%
More than 1 year	9%	9%
Unsure	0%	
Total	100%	100%
Extrapolated value (days)	97	89

Q26. How challenging is it to keep up with the frequency of patch updates?	FY2019	FY2018
Extremely challenging	35%	30%
Challenging	36%	35%
Somewhat challenging	19%	18%
Slightly challenging	10%	12%
Not challenging	0%	5%
Total	100%	100%

Q27. Does your organization have an endpoint detection and response (EDR) tool?	FY2019	FY2018
Yes, we have an EDR	36%	31%
No, but we plan to have an EDR (skip to Q32)	38%	33%
No and we do not plan to have an EDR (skip to Q32)	26%	36%
Total	100%	100%

Q28. Why do you have an EDR? Please select all that apply.	FY2019	FY2018
To be able to proactively block attacks	60%	64%
To detect early signs of an attack and prevent its spread	65%	68%
To help recover from an attack	41%	38%
To proactively hunt for threats on our network	39%	43%
Compliance purposes	25%	
Other (please specify)	1%	2%
Total	231%	215%

Q29. How long did it take your organization to achieve full adoption of its EDR?	FY2019	FY2018
Less than 1 week	3%	2%
1 week to 1 month	4%	5%
1 to 3 months	19%	16%
3 to 6 months	25%	24%
More than 6 months	23%	23%
We have not achieved full adoption	26%	30%
Total	100%	100%
Extrapolated value (weeks)	13.0	12.6

Q30. What percentage of the features or functionality in your EDR are actively used?	FY2019	FY2018
Less than 10%	7%	8%
10% to 25%	16%	20%
26% to 50%	30%	33%
51% to 75%	21%	19%
76% to 100%	26%	20%
Total	100%	100%
Extrapolated value	51%	46%

Q31. What are the top challenges with your organization's EDR? Please select your top two choices.	FY2019	FY2018
Does not prevent or block attacks from getting into our network	42%	38%
There is a high cost of customization, configuration and deployment	55%	57%
Yields a high number of false positive and IT security alerts	60%	58%
Has a negative effect on the productivity of users	21%	19%
Too costly	20%	23%
Other (please specify)	2%	5%
Total	200%	200%

Q32. Why don't you have an EDR? Please select your top two choices.	FY2019
Is not effective against new or unknown threats	65%
Do not have the staff to support	61%
Do not have security budget for it	36%
Do not see the need for it	33%
Other (please specify)	5%
Total	200%

Q33. What best describes your organization's IT security staffing?	FY2019	FY2018
Security is managed by a dedicated internal security staff	14%	13%
Security is managed by our general IT staff	25%	26%
Security management is outsourced to a third-party provider	24%	26%
Security is managed by a combination of in-house and an outsourced third party	37%	35%
Total	100%	100%

Q34. How do you monitor and respond to security events in your organization?	FY2019	FY2018
Our organization monitors our security using tools provided by our solution vendors	35%	20%
Our security is monitored in a hybrid system, using both in-house and outsourced solutions	38%	29%
Our organization completely outsources our security monitoring and event management	27%	21%
Our organization operates a full security operations center (SOC)		30%
Total	100%	100%

Q35. Does your organization operate a security operations center (SOC)?	FY2019
Yes	55%
No (please skip to Q37a)	45%
Total	100%

Q36. How many dedicated SOC analysts does your organization have?	FY2019
1 to 2	5%
3 to 5	16%
6 to 10	26%
More than 10	53%
Total	100%
Extrapolated value	9.2

Q37a. Does your organization outsource or plan to outsource endpoint protection to a managed service provider (MSP) or other third party?	FY2019	FY2018
Yes, we currently outsource endpoint protection	26%	23%
Yes, we plan to outsource endpoint protection	43%	35%
No, we have no plans to outsource endpoint protection	31%	42%
Total	100%	100%

Q37b. If yes, why does your organization outsource or plan to outsource?	FY2019	FY2018
Lack of in-house resources	50%	47%
Too complex to manage in-house	41%	36%
Lack of in-house expertise	55%	50%
Too costly to manage in-house	26%	24%
Total	172%	157%

Part 5. Economic impact and budget

Q38. What is your organization's total IT budget?	FY2019	FY2018
Less than $50,000	0%	0%
$50,000 to $100,000	0%	1%
$100,001 to $500,000	2%	4%
$500,001 to $1,000,000	8%	9%
$1,000,000 to $5,000,000	9%	17%
$5,000,001 to $10,000,000	12%	11%
$10,000,001 to $50,000,000	10%	8%
$50,000,001 to $100,000,000	19%	15%
$100,000,001 to $500,000,000	24%	20%
More than $500,000,000	16%	15%
Total	100%	100%
Extrapolated value (US$ millions)	$186.49	$165.07

Q39. What percentage of your organization's IT budget is allocated to endpoint protection?	FY2019	FY2018
Less than 2%	43%	47%
2 to 5%	31%	27%
6 to 10%	11%	13%
11 to 15%	9%	6%
16 to 20%	6%	7%
More than 20%	0%	0%
Total	100%	100%
Extrapolated value (percentage)	4.6%	4.5%

Q40. Please estimate the total economic loss incurred by your company as a result of endpoint attacks that infiltrated your organization's IT infrastructure over the past 12 months.	FY2019	FY2018	FY2017
Less than $50,000	0%	1%	3%
$50,000 to $100,000			
$100,001 to $500,000	10%	10%	11%
$500,001 to $1,000,000	29%	33%	37%
$1,000,000 to $5,000,000	27%	28%	29%
$5,000,001 to $10,000,000	21%	18%	11%
$10,000,001 to $50,000,000	6%	3%	1%
$50,000,001 to $100,000,000	2%	3%	2%
$100,000,001 to $500,000,000	1%	1%	1%
More than $500,000,000	0%	0%	0%
Total	100%	100%	100%
Extrapolated value (US$ millions)	$ 8.94	$ 7.12	$ 5.01

Q41. Following are 6 cost consequences that your organization may have experienced as a result of one or more successful 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.	FY2019 Points	FY2018 Points	FY2017 Points
IT and end-user productivity loss	37	35	30
System downtime	15	20	25
Theft of information assets	30	27	23
Damage to IT infrastructure	9	8	10
Lawsuits, fines and regulatory actions	4	3	4
Reputation/brand damage	5	7	8
Total points	100	100	100

Part 6. Organizational Characteristics & Demographics			
D1. What organizational level best describes your current position?	FY2019	FY2018	FY2017
Senior Executive	2%	3%	2%
Vice President	4%	4%	3%
Director	16%	15%	17%
Manager	21%	23%	21%
Supervisor	15%	14%	15%
Technician	32%	31%	32%
Staff	8%	6%	7%
Contractor	2%	3%	2%
Other	0%	1%	1%
Total	100%	100%	100%

D2. Check the **Primary Person** you or your IT security leader reports to within the organization.	FY2019	FY2018	FY2017
CEO/Executive Committee	1%	1%	2%
Chief Financial Officer (CFO)	0%	0%	0%
General Counsel	1%	2%	2%
Chief Information Officer (CIO)	46%	45%	49%
Chief Information Security Officer (CISO)	27%	26%	25%
Compliance Officer	10%	5%	4%
Human Resource VP	0%		
Chief Security Officer (CSO)	7%	3%	3%
Chief Risk Officer (CRO)	8%	7%	8%
Other	0%	0%	1%
Line of Business Leader (GM)		11%	6%
Total	100%	100%	100%

D3. What industry best describes your organization's primary industry focus?	FY2019	FY2018	FY2017
Communications	2%	2%	3%
Consumer products	5%	4%	0%
Defense & aerospace	1%	2%	1%
Education & research	**2%**	8%	4%
Energy & utilities	6%	5%	5%
Entertainment & media	3%	2%	3%
Financial services	19%	17%	18%
Health & pharma	**10%**	10%	11%
Hospitality	1%	2%	2%
Industrial	8%	7%	7%
Public services	11%	12%	10%
Retailing	10%	9%	10%
Services	**10%**	10%	11%
Technology & software	9%	7%	8%
Transportation	2%	1%	2%
Other	1%	2%	5%
Total	100%	100%	100%

D4. Where are your employees located? Check all that apply.	FY2019	FY2018	FY2017
United States	100%	100%	100%
Canada	65%	63%	66%
Europe	74%	70%	73%
Middle East & Africa	39%	40%	37%
Asia-Pacific	62%	59%	60%
Latin America (including Mexico)	40%	41%	39%

D5. What is the worldwide headcount of your organization?	FY2019	FY2018	FY2017
Less than 500 people	12%	12%	11%
500 to 1,000 people	17%	16%	15%
1,001 to 5,000 people	25%	27%	28%
5,001 to 25,000 people	26%	26%	27%
25,001 to 75,000 people	12%	13%	12%
More than 75,000 people	8%	6%	7%
Total	100%	100%	100%

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.