


PONEMON INSTITUTE 2022 **REPORT**

MANAGING RISKS & COSTS AT THE EDGE

 adaptiva™ + **Ponemon**
INSTITUTE



Executive Summary

DEEPAK KUMAR, FOUNDER & CEO, ADAPTIVA

As we release this inaugural report – we recognize the world is in a state of tumultuous change and in many cases uncertainty. Managing devices at the edge, pre-2020, was already a challenge for most enterprise IT organizations, but one could argue they got by. Now, halfway through 2022, it seems they aren't getting by anymore.

With a distributed workforce, IT has lost a significant amount of visibility into the devices that are connecting to their networks—48% of them in fact. It's mostly because employees are far less predictable than they've ever been—IT has no idea where they might log-in to work, at what time, on what device, and so on.

The predominant technologies of the day force IT to choose the lesser of two evils: Empower employees to be productive anywhere and expose the company to risk, or force employees to work in an office and go back to getting by. The latter isn't likely to go over so well in 2022 and beyond. Despite the 49% of respondents saying a remote workforce has made it more difficult to manage security updates and patches, we predict more and more companies will lean into distributed workforces. If companies hope to get (and maintain) a handle on their decentralized endpoints things will need to change.

Remote Workplaces Require a New Paradigm

IT is managing unprecedented distribution point sprawl. Roughly 23,000 distribution points are now needed to manage an average of 135,000 devices. That's one distribution point for every six endpoints – and is the biggest threat to endpoint security for 34% of survey respondents.

The sprawl has increased for more than half of respondents in the last two years, and only 33% are effective at reducing it. As a result, we expect more IT organizations to prioritize a reduction of distribution point sprawl in the next 2-5 years and will begin to rely on edge computing technologies to do it.

Automation Should Do More

Automation has yet to make a significant impact on IT's job of managing and securing endpoints. Respondents said that implementation of automation to investigate and remediate vulnerabilities and attacks could reduce the average cost of a breach by 25%, or about \$450,000 annually.

We suspect this is largely due to the fact that most of the work has yet to be truly automated. The automation capabilities in this space are significantly limited to very mundane tasks only achieved through complex scripts and other specialty approaches. This approach rarely leads to significant time and effort savings, thus the underwhelming expectations in cost savings.

While intelligence-driven automation has begun appearing in defensive-focused security technologies, it has yet to make headway in the more

preventative aspects of endpoint management. Driven by demand from security teams, we expect IT operations teams will not only demand this of their tools – but it will be the predominant automation approach for endpoint management tools in the next 5 years.

We Must Work Together

Organizations within IT continue to be siloed, as IT operations and IT security reported some significant perception differences. For instance, 40% of IT security reported challenges with a remote workforce, while it was a much higher 57% for IT operations.

Typically, IT operations teams handle preventative measures such as endpoint management and patching while IT security teams are more defensive in nature managing antivirus and attack detection and response tools. Yet in some cases it seems the two teams are operating in dual realities.

For an IT management and security strategy to work there must be a symbiotic relationship between defense and offense. We expect these two teams to work closer together both organizationally, and in perceptions, over the next two years. As enterprise organizations continue to rely on endpoint devices at the edge to conduct business – they will be faced with many challenges to prevent cyber threats such as opportunistic attacks, phishing exploits, targeted attacks, and advanced persistent threats.

Table of Contents

PART I
Introduction

Pages 6 – 14

PART II
Key Findings

Pages 15 – 31

- 16 THE RISKS TO ENDPOINTS
- 19 CHALLENGES TO IMPROVING
ENDPOINT SECURITY
- 23 THE COST AND INVESTMENT
IN ENDPOINT SECURITY
MANAGEMENT
- 27 ENDPOINT SECURITY
PERCEPTION GAP

PART III
Methodology

Pages 32 – 33

PART IV
**Caveats to
this Study**

Pages 34 – 35

PART V
Appendix

Pages 36 – 49



A Note from a Hacker

BRYAN SEELY, WORLD FAMOUS HACKER

The hacker's life seems to get easier every year – there are more doors to gain access to and it's getting easier to be nefarious. We need to make it harder. In order to make it harder for attackers, we as cybersecurity practitioners have to be willing to do the hard work. There are as many solutions as there are problems, leading companies to keep doing what they've always done because change is hard.

What we've always done is no longer working, yet we seem comfortable. We either think "it won't happen to me" or we simply don't want to be inconvenienced – even if it's in our best interest. Let me be very clear here – it will happen to you. And there isn't a single person in any company that deserves to put everyone else at risk for their own convenience.

There isn't a target on earth, that I'm aware of, that can't be taken by force of some kind. The more effort it requires to successfully breach a target, the less attention it will get from a hacker. I can promise you they are paying attention and are ready to act when they see the easy or convenient way and by then it will be too late to stop them.

The list of reasons to avoid change can be endless. And while many of those reasons have sound logic behind them, each of those reasons gives hackers motivation to act. The results of this data show hackers have a lot of motivation to act, right now. It's this urgency that should encourage all of us to come together, to transform how we approach these challenges, and ultimately make life harder for the hackers.

PART I

Introduction

As organizations' endpoints such as desktops, mobile devices, laptops, and tablets continue to proliferate, it is a challenge to prevent such cyber threats as opportunistic attacks, phishing exploits, targeted attacks, and advanced persistent threats.

Organizations represented in this research have an average of 135,000 endpoints. An average of 48 percent of these endpoints (64,800) are at risk because they are not being detected by IT or the operating system is outdated. Annually, an average of \$4,252,500 (\$31.50 per endpoint x 135,000) is spent on endpoint protection. Most costs

are the result of software compatibility issues followed by the engagement of outside vendors and consultants to supplement existing in-house security teams.

The purpose of this study is to learn the effectiveness of organizations' endpoint management strategy in securing the network and complying with certain standards before network access is granted. As is shown in this report, the cost of endpoint management can be significant based on the hours spent managing endpoints and the supporting infrastructure.

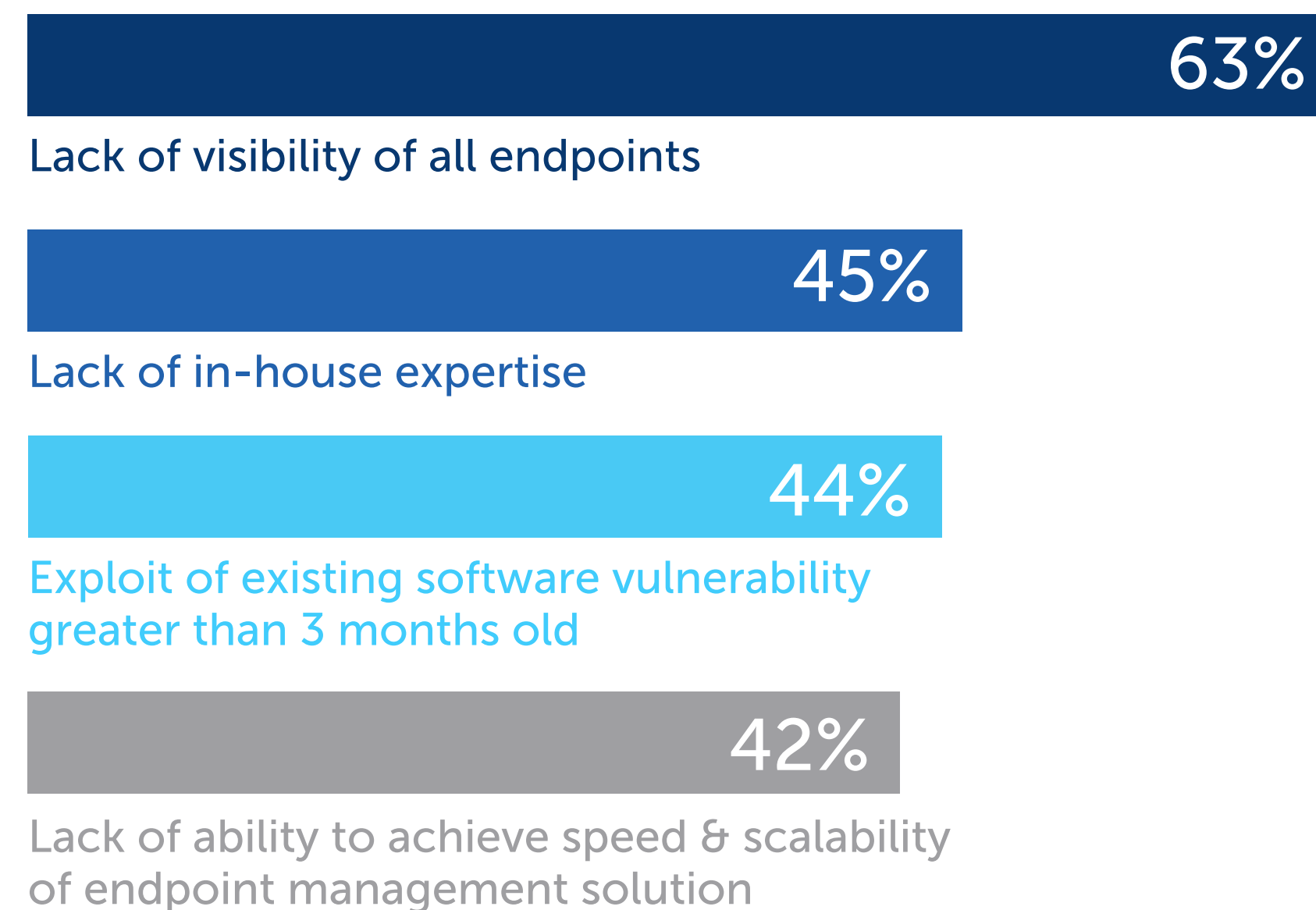
Sponsored by Adaptiva and conducted by Ponemon Institute, 629 IT and IT security practitioners in the United States were surveyed. All respondents are involved and influential in their organization's endpoint management strategy. The average headcount of organizations represented in the study is 13,213.

Endpoint security is affected most by the lack of visibility.

Figure 1 represents the most significant barriers to achieving a strong endpoint security posture. Sixty-three percent of respondents say it is the lack of visibility followed by 45 percent of respondents who say it is a lack of in-house expertise.

Figure 1. What are the most significant barriers to achieving a strong endpoint security posture?

More than one response permitted



The following research findings reveal the challenges of managing risks and costs at the edge.

- 1 **Distribution point sprawl** impacts the security of endpoints because of difficulty managing the increase.
- 2 While the protection of endpoints has become more of a priority, few organizations are allocating enough **resources to minimize endpoint risk**.
- 3 **Ransomware** is considered the biggest threat to endpoint security.
- 4 **Email systems** are the most vulnerable to attacks.
- 5 **New OS and application versions of endpoint configuration management** make it difficult to maintain security across all endpoints.
- 6 Most organizations are ineffective in **managing risks and costs at the edge**, especially with respect to distribution point sprawl.
- 7 **System downtime** is the most significant cost consequence of an endpoint attack. Resources allocated to endpoint management.
- 8 **Resources allocated** to endpoint management.
- 9 Endpoint protection is **costly**.

1

Distribution point sprawl impacts the security of endpoints because of difficulty managing the increase.

While the protection of endpoints has become more of a priority, few organizations are allocating enough resources to minimize endpoint risk. Sixty-three percent of respondents say in the past two years, the prevention and detection of attacks against endpoints has become more of a priority in their organization's overall IT security strategy. However, only 34 percent of respondents say their organizations have ample resources to minimize endpoint risk.

ON AVERAGE, EVERY SIX
ENDPOINTS REQUIRE:



+



a distribution
point server to
manage them

seven agents installed on
each endpoint to provide
management and security

BIGGEST
THREATS TO
ENDPOINT
SECURITY:

48%
Ransomware

45%
Zero-day
Attacks

43%
DDoS

39%
Credential
Theft

34%
Distribution
Point Sprawl



2

Ransomware is the biggest threat to endpoint security.

Ransomware is considered the biggest threat to endpoint security. Respondents are most concerned about ransomware (48 percent), zero-day attacks (45 percent), DDoS (43 percent), credential theft (39 percent), and distribution point sprawl (34 percent).

10

3

Email systems are the most vulnerable to attacks.

Respondents were asked how attacks against endpoints got into their organizations. Forty-one percent say it was through email, 36 percent say APIs, and 35 percent say through software updates/patches. As discussed previously, organizations are having difficulty in getting software updates/patches to endpoints because of the increase in remote working.

4

New OS and application versions of endpoint configuration management make it difficult to maintain security across all endpoints.

Sixty-two percent of respondents say new OS and application versions and 59 percent of respondents say it is patches and security updates that are most difficult to maintain.

5

Distribution point sprawl impacts the security of endpoints because of difficulty managing the increase.

Distribution points play a vital role in delivering content to the clients whenever a client needs to download a new operating system, the bits of an application, or a package it needs to contact. On average, organizations have an average of 22,925 distribution points. In the past two years 61 percent of respondents say distribution points have increased significantly (26 percent) or increased (35 percent).

OS application versions, patches, and security updates are the **most difficult to maintain security** across all endpoints.

6

Most organizations are ineffective in managing risks and costs at the edge, especially with respect to distribution point sprawl.

As discussed, the inability to control distribution point sprawl impacts endpoint risks. Only 33 percent of respondents say their organizations are effective or highly effective at reducing distribution point sprawl. Thirty-nine percent of respondents rate their effectiveness in preventing and detecting attacks as high or highly effective. Only 35 percent of respondents rate their effectiveness in ensuring all software is up-to-date and the configuration complies with their security policy as high or highly effective.

The average cost of an endpoint attack is \$1.8 million annually.



54% OF RESPONDENTS HAD AN AVERAGE OF 5 ATTACKS ON THEIR ORG'S ENDPOINTS.



7

System downtime is the most significant cost consequence of an endpoint attack.

In the past year, 54 percent of respondents had an average of 5 attacks on their organizations' endpoints. Following is the average cost of these endpoint attacks and how much the costs could be reduced with the use of automation. The average cost of these annual attacks is \$1.8 million or an average of \$360,000 per attack. Implementation of automation to investigate and remediate could reduce the \$1.8 million cost by an average of 25 percent or \$450,000 annually according to the research.

8

Resources allocated to endpoint management.

The average annual IT budget for organizations represented in this research is \$184.4 million. Twenty-five percent of the IT budget is allocated to IT security (\$46.1 million) and an average of 20 percent is allocated to endpoint management (\$9.2 million). Only 24 percent of respondents say the budget is more than adequate.

9

Endpoint protection is costly.

Annually, an average of \$4,252,500 (135,000 x \$31.50 per endpoint) is spent on endpoint management. An average of \$507,250 is spent annually on the IT and IT security help desk. An average of 30 percent (\$152,175) of help desk costs is spent annually on endpoint issues.

76% of respondents don't have enough budget for endpoint management.

“

The more effort it requires to successfully breach a target, the less attention it will get from a hacker.

—BRYAN SEELY, WORLD FAMOUS HACKER

PART II

Key Findings

In this section, we provide an analysis of the research. The complete audited findings are presented in the Appendix of this report. We have organized the report according to the following findings.

-
- 1 THE RISKS TO ENDPOINTS
 - 2 CHALLENGES TO IMPROVING
ENDPOINT SECURITY
 - 3 THE COST AND INVESTMENT
IN ENDPOINT SECURITY
MANAGEMENT
 - 4 ENDPOINT SECURITY
PERCEPTION GAP
-

To get further insights from this report you can [visit us here](#).

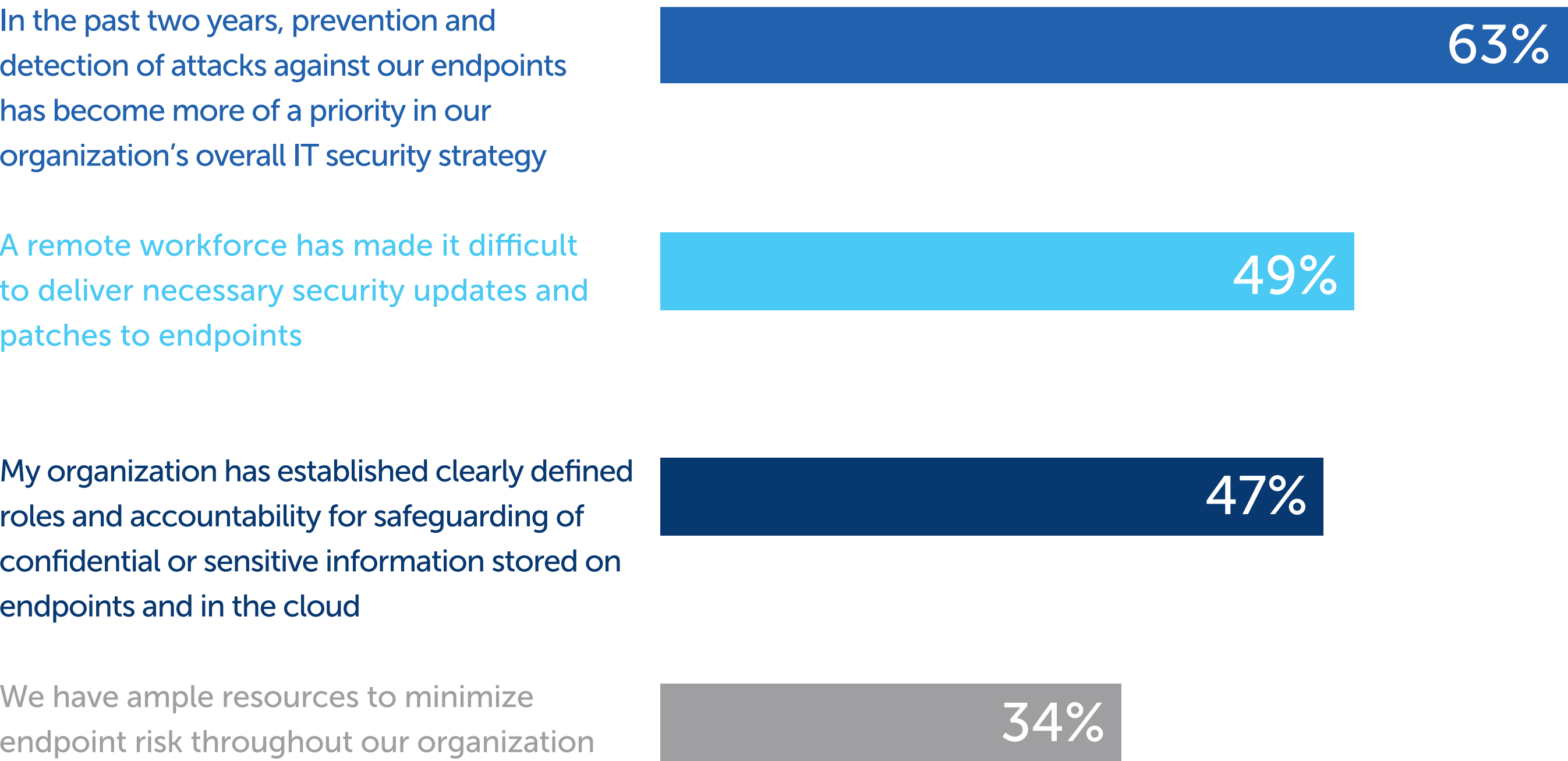
KEY FINDING 1

The Risks to Endpoints

While the protection of endpoints has become more of a priority, few organizations are allocating enough resources to minimize endpoint risk. According to Figure 2, 63 percent of respondents say in the past two years, the prevention and detection of attacks against endpoints has become more of a priority in their organization’s overall IT security strategy. However, only 34 percent of respondents say their organizations have ample resources to minimize endpoint risk.

Having the necessary resources is important because a remote workforce is making it difficult to deliver necessary security updates and patches to endpoints (49 percent of respondents). Also critical is having clearly defined roles and accountability for safeguarding sensitive information stored on endpoints and in the cloud but only 47 percent of respondents say they have such a policy.

Figure 2. Perceptions about endpoint risks
Strongly Agree and Agree responses combined



KEY FINDING 1

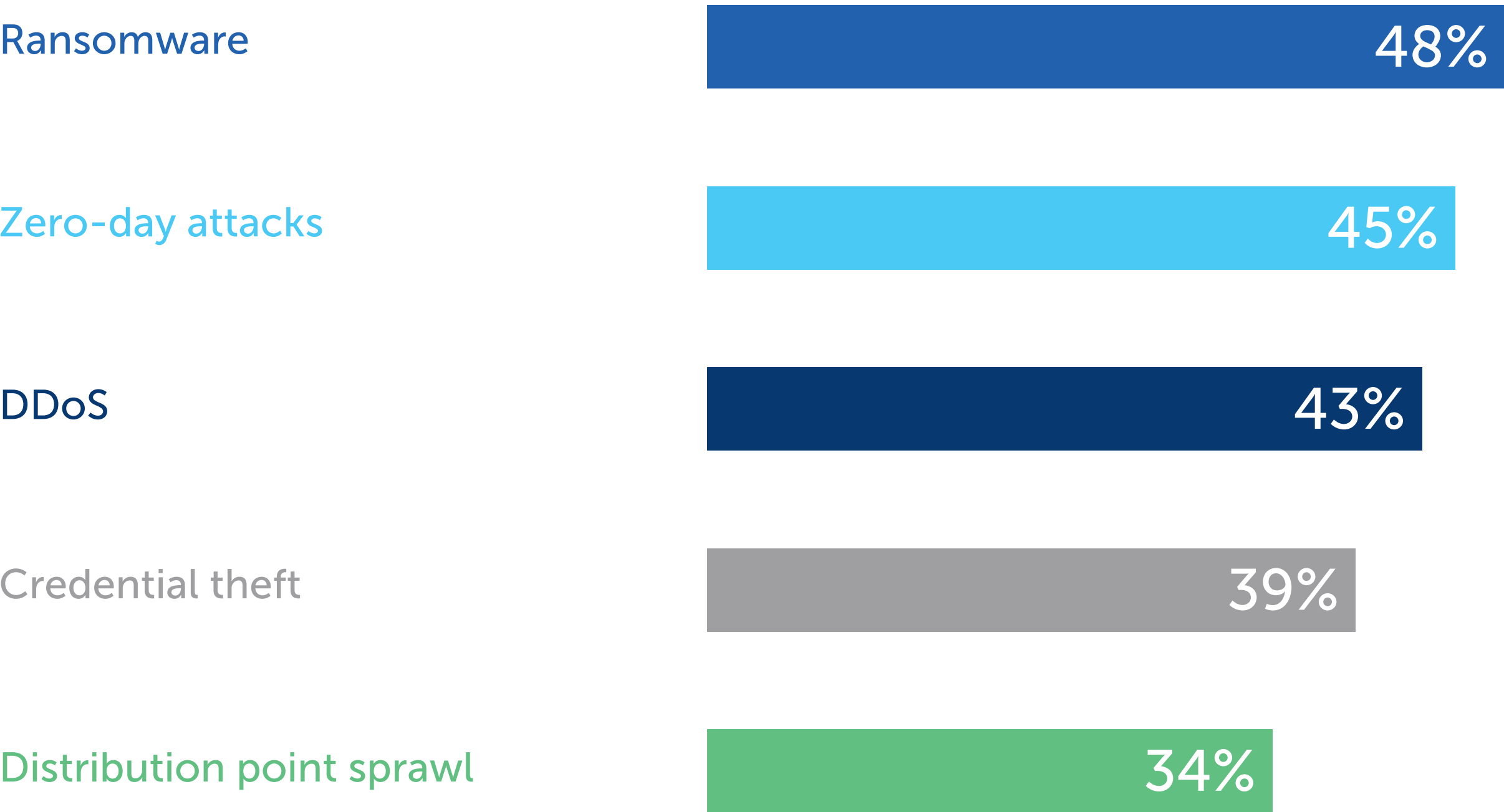
The Risks to Endpoints

Ransomware

Ransomware is considered the biggest threat to endpoint security. As shown in Figure 3, respondents are most concerned about ransomware (48 percent), zero-day attacks (45 percent), DDoS (43 percent), credential theft (39 percent), and distribution point sprawl (34 percent).

Figure 3. What are the biggest threats to endpoint security?

More than one response permitted



KEY FINDING 1

The Risks to Endpoints

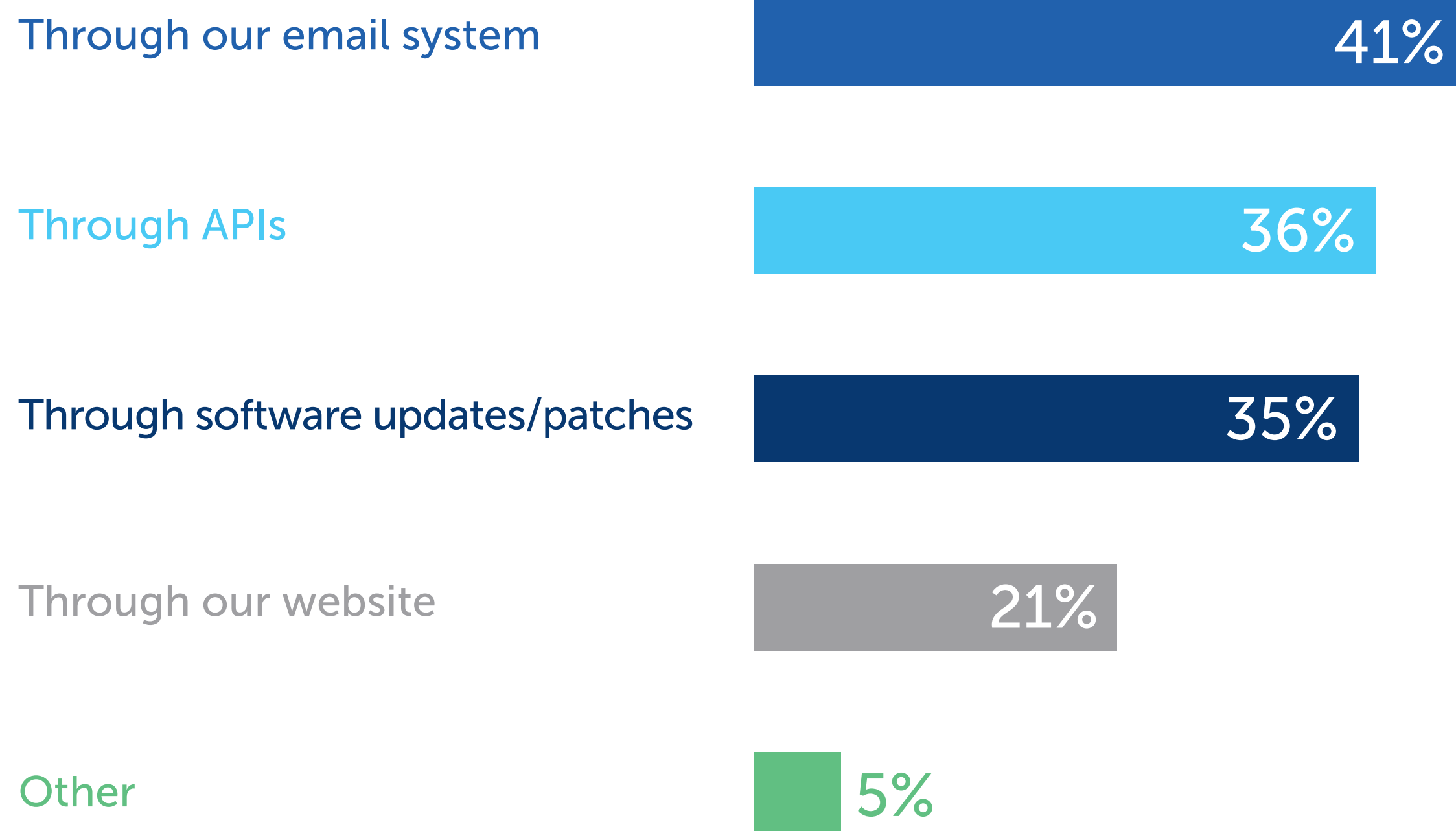
Email Systems

Email systems are the most vulnerable to attacks.

Respondents were asked how attacks against the endpoints got into their organizations. Forty-one percent say it was through email, 36 percent say APIs, and 35 percent say through software updates/patches (Figure 4). As discussed previously, organizations are having difficulty in getting software updates/patches to endpoints because of increases in remote working and lack of automation.

Figure 4. How did endpoint attacks get into your organization?

More than one response permitted

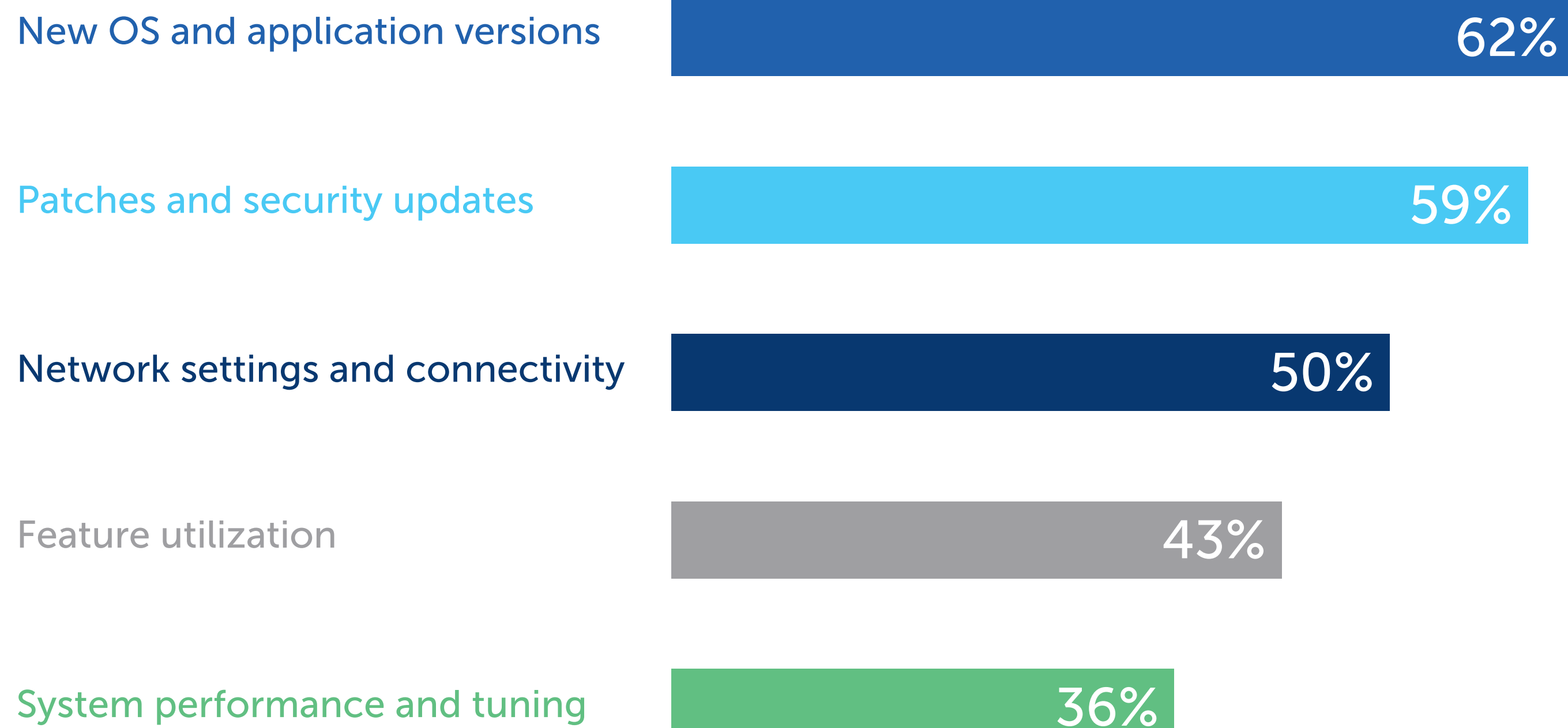


KEY FINDING 2

Challenges to Improving Endpoint Security

New OS and application versions of endpoint configuration management make it difficult to maintain security across all endpoints. Figure 5 presents the aspects of endpoint configuration management that are difficult to maintain across all endpoints. Sixty-two percent of respondents say new OS and application versions and 59 percent of respondents say it is patches and security updates that are most difficult to maintain.

Figure 5. Which aspects of endpoint configuration management are the most difficult to maintain? More than one response permitted



KEY FINDING 2

Challenges to Improving Endpoint Security

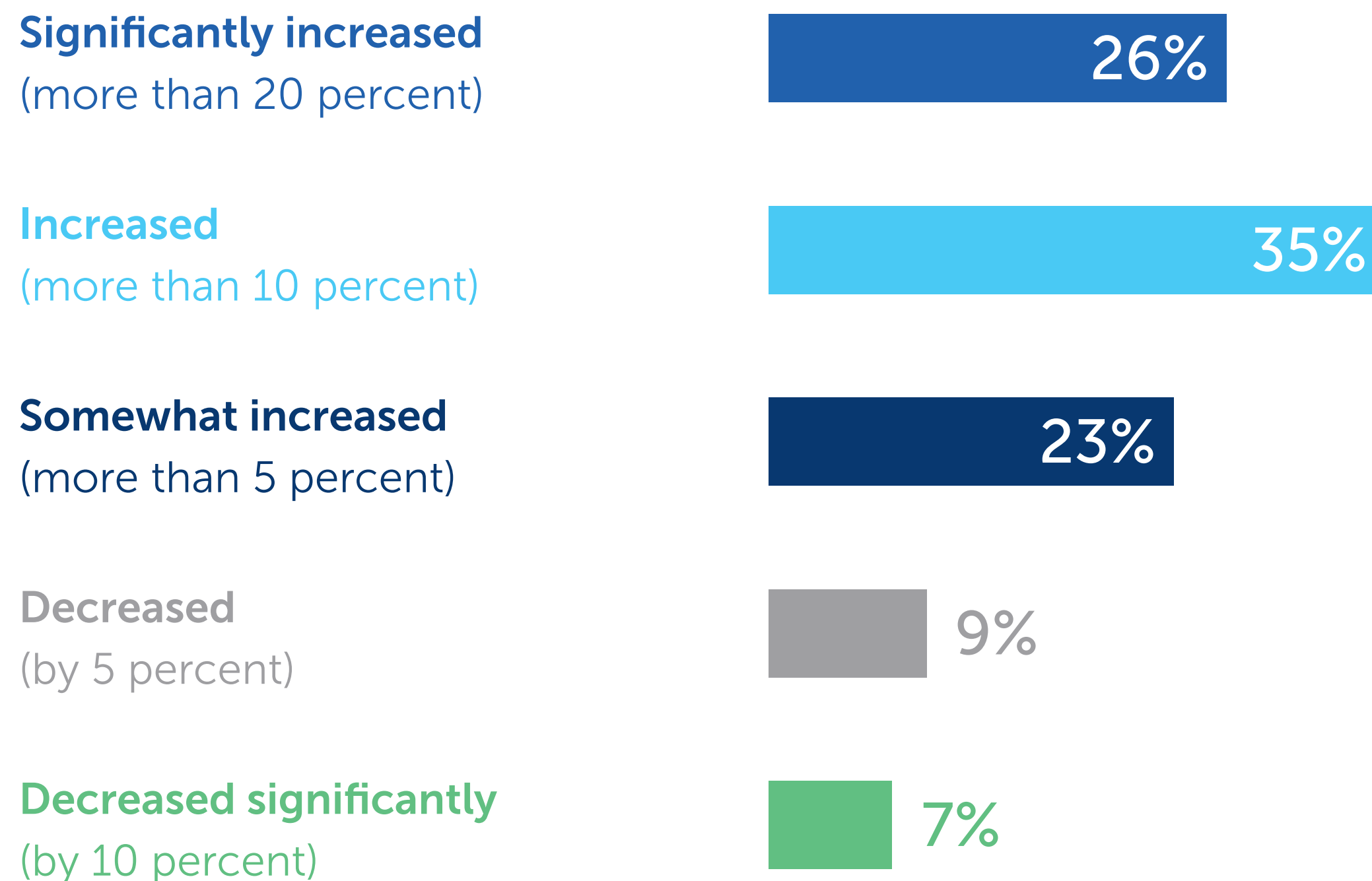
Distribution Point Sprawl

Distribution point sprawl impacts security of endpoints because of the difficulty managing the increase.

Distribution points play a vital role in delivering content to clients whenever a client needs to download a new operating system, the bits of an application or a package it needs to contact.

Organizations have on average 22,925 distribution points. As shown in Figure 6, in the past two years 61 percent of respondents say distribution points have increased significantly (26 percent) or increased (35 percent). Only 33 percent of respondents say their organizations are very or highly effective at reducing distribution point sprawl.

Figure 6. How has the number of distribution points changed in the past two years?



KEY FINDING 2

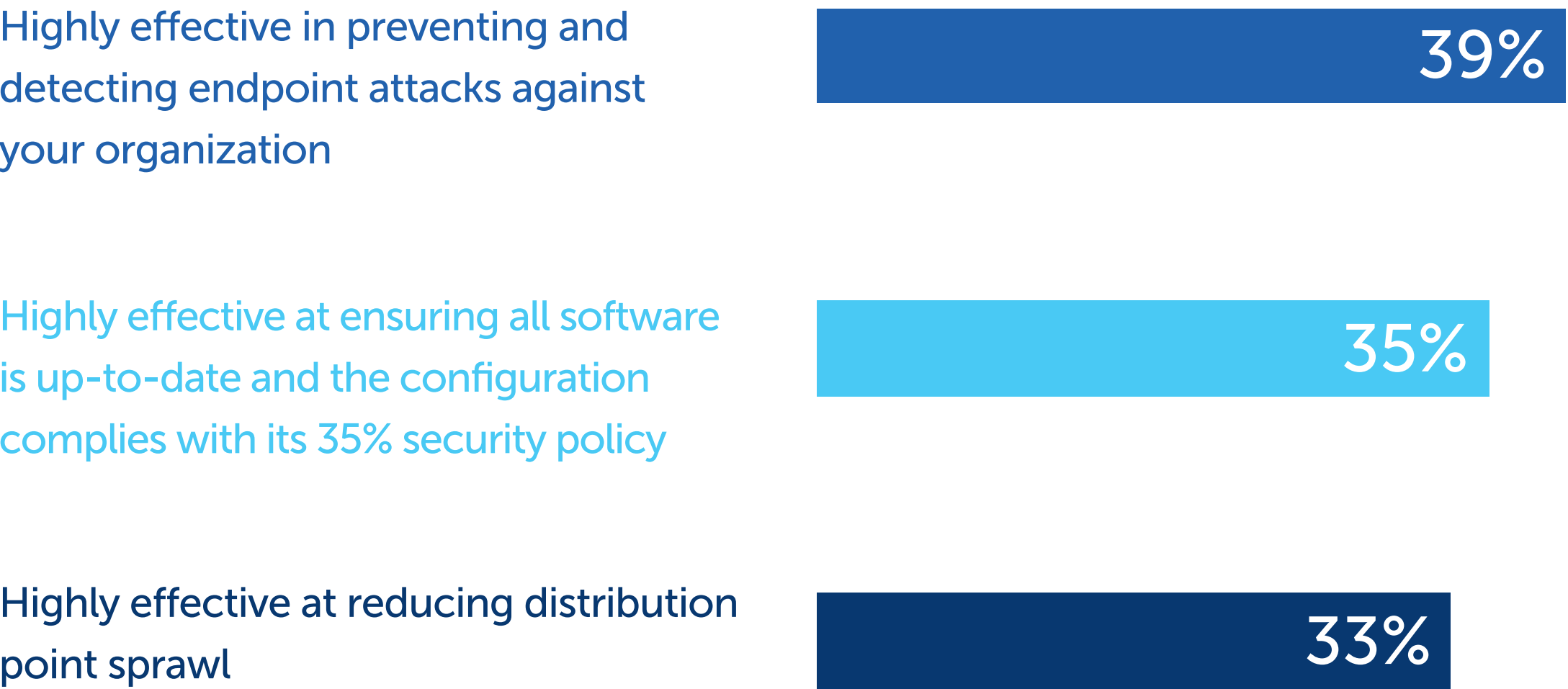
Challenges to Improving Endpoint Security

Managing Risks at the Edge

Most organizations are ineffective in managing risks and costs at the edge, especially with respect to distribution point sprawl. Respondents were asked to rate the effectiveness of their organizations in three different aspects of ensuring security at the edge on a scale from 1 = not effective to 10 = highly effective. Figure 7 presents the highly effective responses (7+ responses on the 10-point scale).

As discussed, the inability to control distribution point sprawl impacts endpoint risks. According to Figure 7, only 33 percent say their organizations are effective or highly effective at reducing distribution point sprawl. Thirty-nine percent of respondents rate their effectiveness in preventing and detecting attacks as high or highly effective. Only 35 percent of respondents rate their effectiveness in ensuring all software is up-to-date and the configuration complies with their security policy as high or highly effective.

Figure 7. Highly effective in achieving endpoint security
On a scale from 1 = not effective to 10 = highly effective, 7+ responses presented



“

Shifting from centralized infrastructure, whether on-premises or in the cloud, to one powered by your edge will help keep endpoints visible, allowing them to remain up to date to protect them against threats.

—DEEPAK KUMAR, CEO, ADAPTIVA

KEY FINDING 3

The Cost and Investment in Endpoint Management

Organizations struggle to achieve compliance with regulations and minimize downtime during maintenance. Respondents were asked to rate effectiveness in doing maintenance anytime without significant downtime and loss of end-user productivity as well as achieving endpoint compliance.

Figure 8 represents the high and highly effective responses. As shown, only 36 percent of respondents say their organizations are very effective at avoiding significant downtime during maintenance. On average, 60 hours of employee time is lost monthly or 720 hours annually due to downtime or attacks against the endpoint. Only 35 percent of respondents say their organizations are very effective at ensuring all software is up-to-date and the configuration complies with their security policies.

Figure 8. Effectiveness in achieving compliance and minimizing downtime

On a scale from 1 = not effective to 10 = highly effective, 7+ responses presented

Highly effective at doing maintenance anytime without significant downtime and loss of end-user productivity

36%

Highly effective at achieving endpoint compliance with regulations

35%

KEY FINDING 3

The Cost and Investment in Endpoint Management

System Downtime

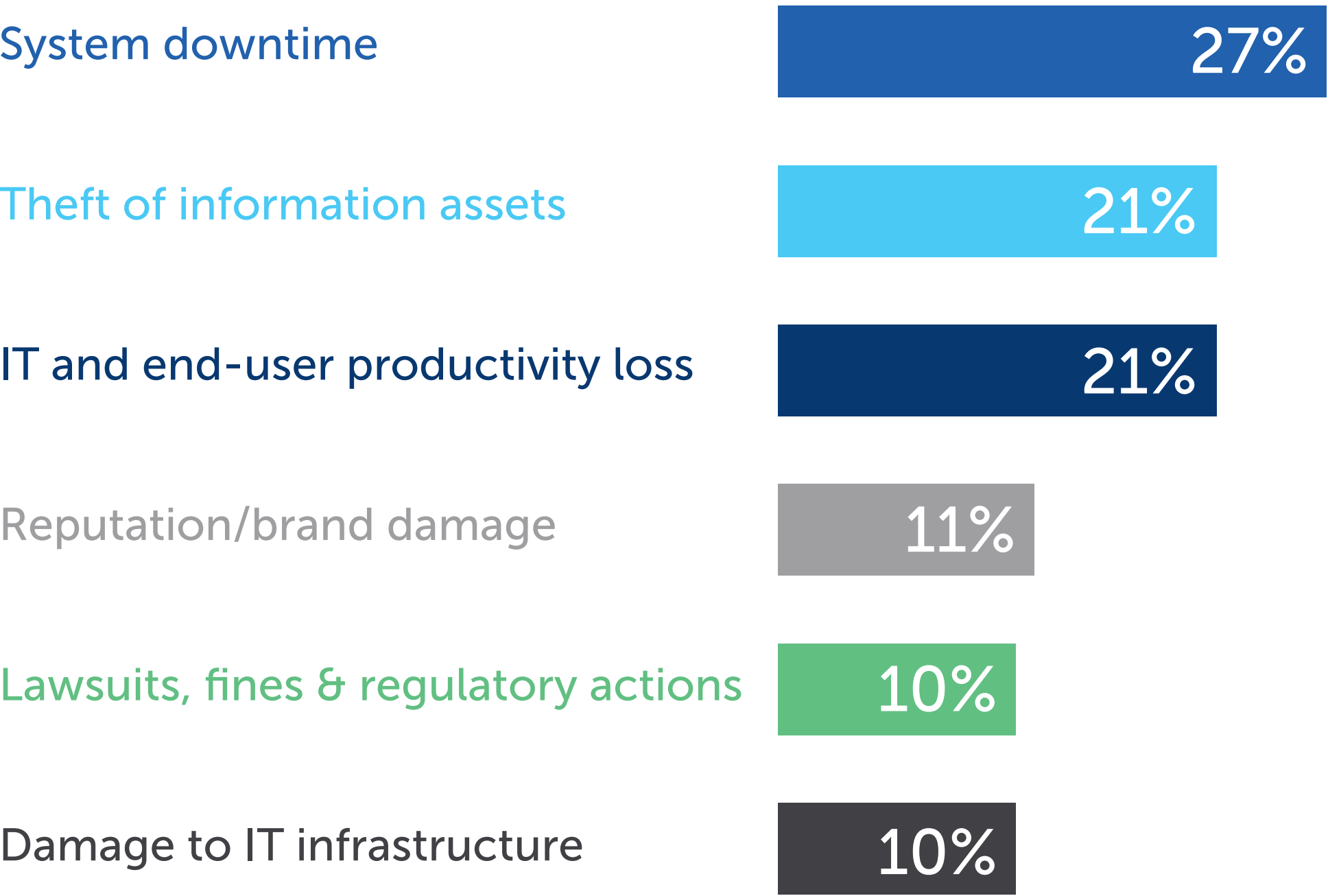
System downtime is the most significant cost consequence of an endpoint attack. In the past year, 54 percent of respondents had an average of 5 attacks on their organizations’ endpoints. Following is the average cost of these endpoint attacks and how much the costs could be reduced with the use of automation.

The average cost of these annual attacks is \$1.8 million or an average of \$360,000 per attack.

Implementation of automation to investigate and remediate could reduce the \$1.8 million cost by an average of 25 percent or \$450,000 annually according to the research.

Respondents were asked to allocate 100 points to six consequences of one or more successful endpoint attacks as presented in Figure 9. As shown, 27 percent of the cost of endpoint attacks is due to system downtime followed by IT and end-user productivity loss (21 percent) and theft of information assets (21 percent).

Figure 9. The cost consequences of one or more successful endpoint attacks



KEY FINDING 3

The Cost and Investment in Endpoint Management

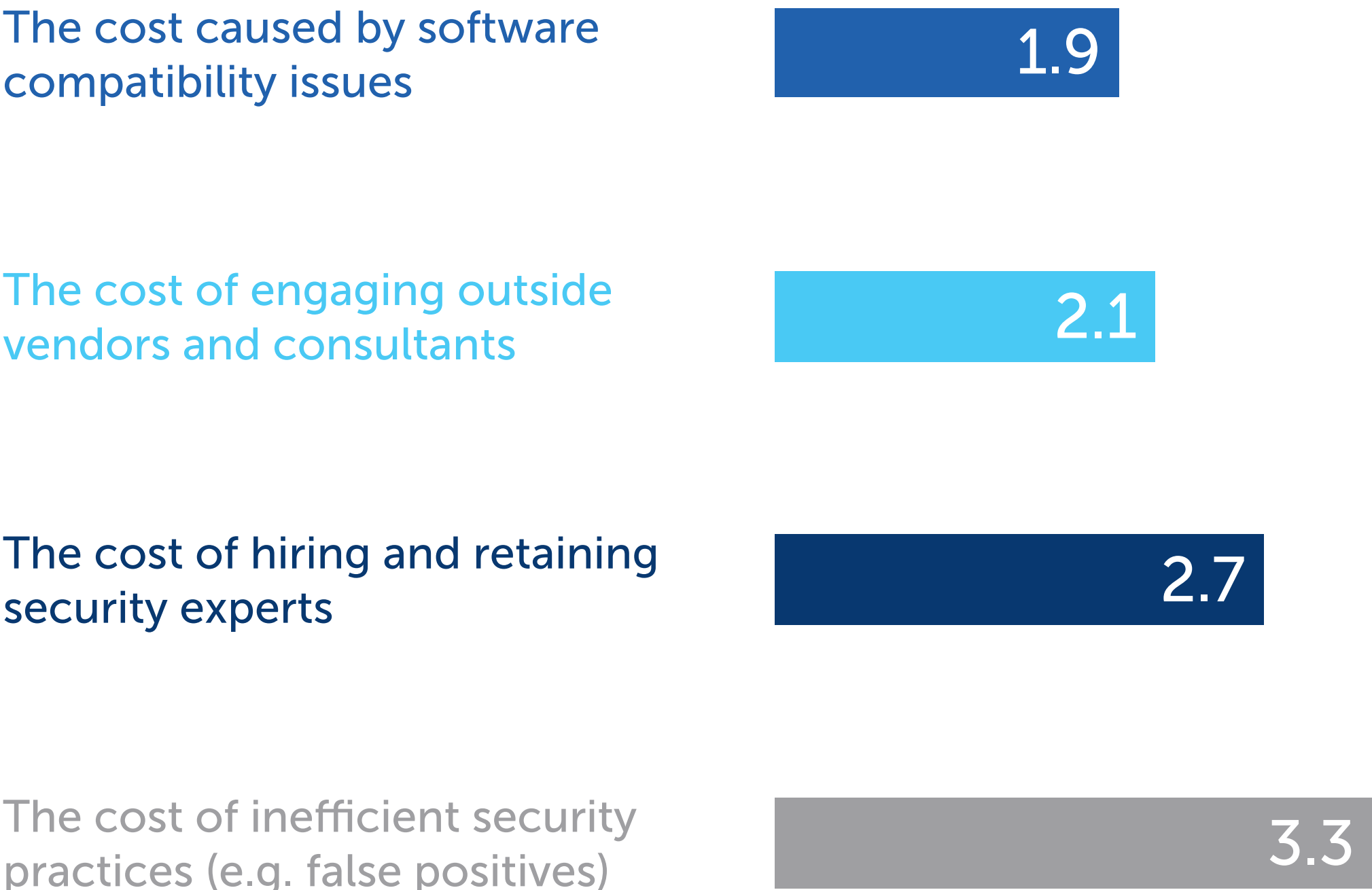
The Price of Protecting Endpoints

The average annual IT budget for organizations represented in this research is \$184.4 million. Twenty-five percent of the IT budget is allocated to IT security (\$46.1 million) and an average of 20 percent is allocated to endpoint management (\$9.2 million). Only 24 percent of respondents say the budget is more than adequate.

Endpoint protection is costly. Annually, an average of \$4,252,500 (135,000 x \$31.50 per endpoint) is spent on endpoint management. An average of \$507,250 is spent annually on the IT and IT security help desk. An average of 30 percent (\$152,175) of help desk costs is spent annually on endpoint issues.

Figure 10 presents the ongoing costs related to endpoint protection. As shown, the top two costs are those caused by software compatibility issues and engaging outside vendors and consultants.

Figure 10. The ongoing costs related to endpoint protection
Ranking from 1 = most costly to 4 = least costly



KEY FINDING 3

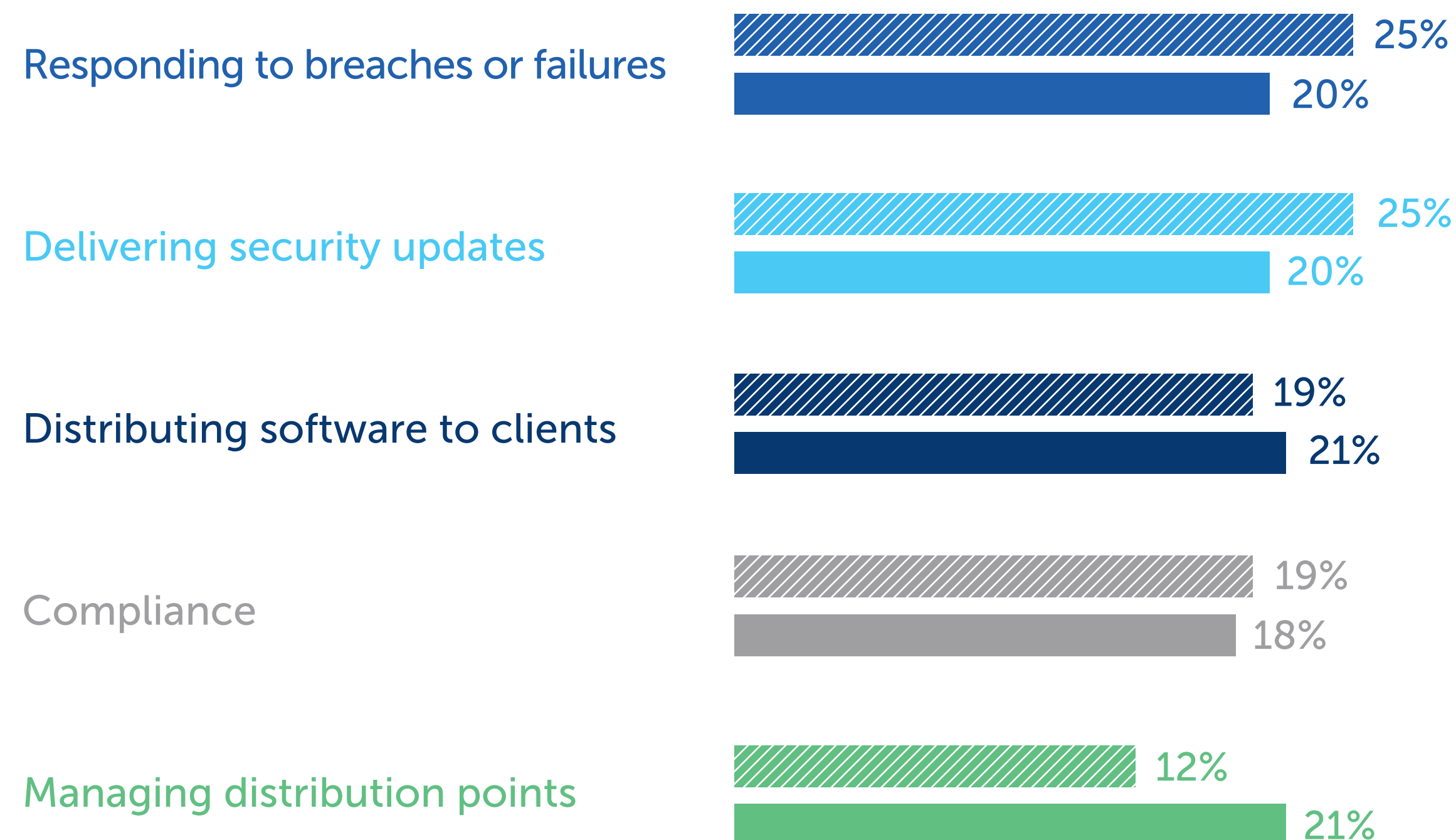
The Cost and Investment in Endpoint Management

Budget Priorities

Managing distribution point sprawl is a budget priority. According to Figure 11, of the \$9.2 million allocated to endpoint security there will be a shift in budget allocation from delivering security updates and responding to breaches or failures to distributing software to clients and managing distribution points.

Figure 11. IT endpoint management budget allocation today and in the next 12 months

 TODAY
 IN THE NEXT 12 MONTHS

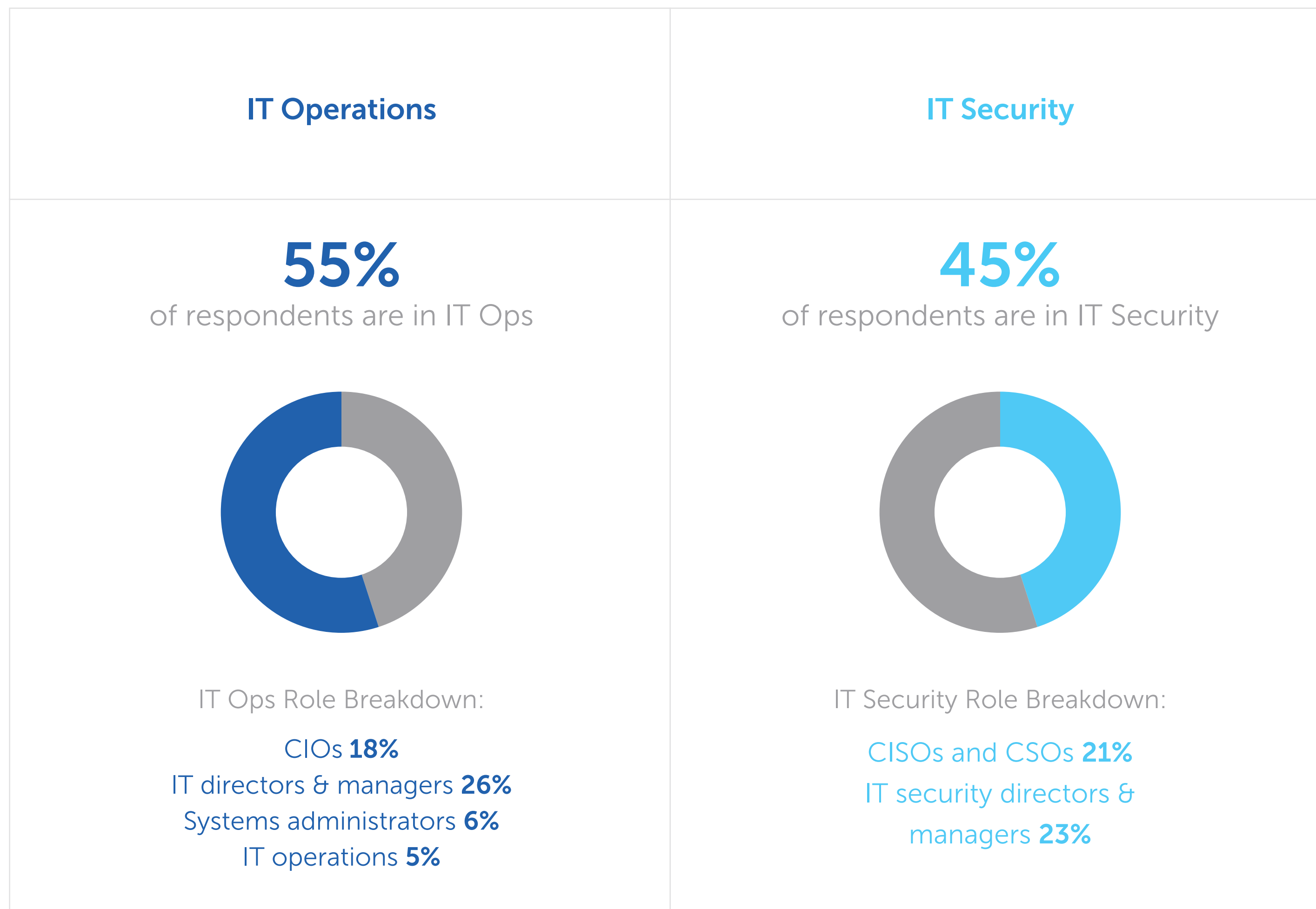


KEY FINDING 4

Endpoint Security Perception Gap

In organizations' efforts to manage the costs and risks of endpoint security, how closely aligned are IT operations and IT security? In this section, we present the different perceptions between IT operations and IT security in their current state of managing security at the edge. These may be keeping organizations from creating a stronger security posture.

Fifty-five percent of respondents are in IT operations and a breakdown of the roles are as follows: CIOs (18 percent), IT directors and managers (26 percent), systems administrators (6 percent), and IT operations (5 percent). Forty-five percent of respondents are in IT security. The following is a breakdown of their roles: CISOs and CSOs (21 percent) and IT security directors and managers (23 percent). The following are the most salient differences.



KEY FINDING 4

Endpoint Security Perception Gap

Managing Endpoints for a Remote Workforce

IT security is less concerned about managing endpoints for a remote workforce. According to Figure 12, 57 percent of IT operations respondents vs. 40 percent of IT security respondents say a remote workforce has made it difficult to deliver necessary security updates and patches to endpoints. However, 50 percent of IT operations vs. 43 percent of IT security respondents say their organizations have established clearly defined roles and accountability for safeguarding confidential or sensitive information stored on endpoints and in the cloud.

Figure 12. Perceptions about endpoint security management

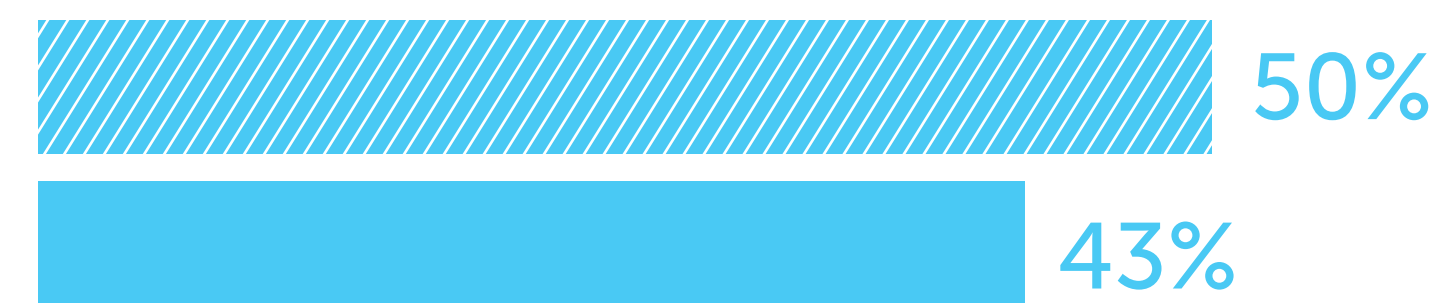
Strongly Agree and Agree responses combined



A remote workforce has made it difficult to deliver necessary security updates and patches to endpoints



My organization has established clearly defined roles and accountability for safeguarding of confidential or sensitive information stored on endpoints and in the cloud



KEY FINDING 4

Endpoint Security Perception Gap

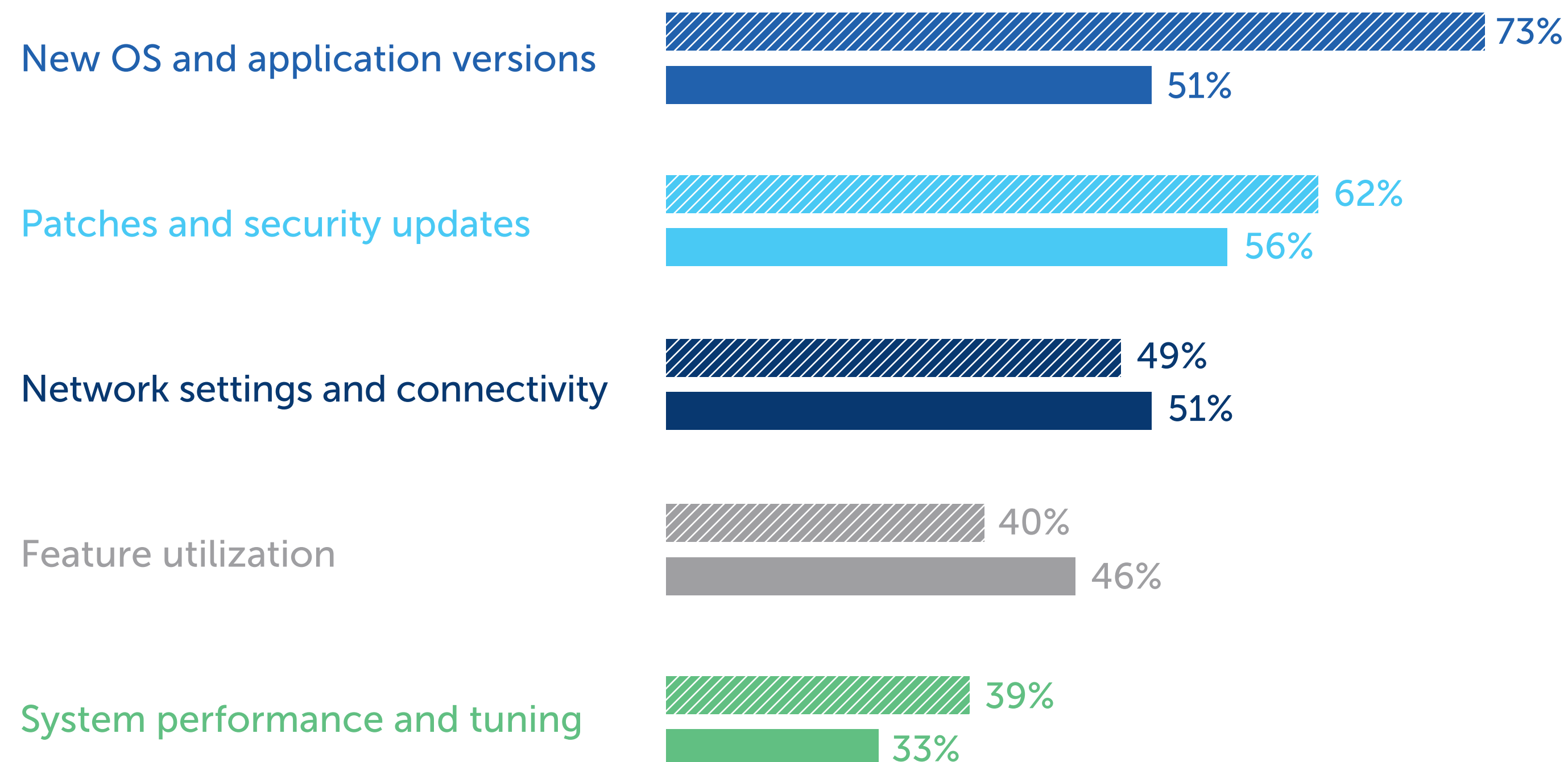
Endpoint Configuration Management

Far more IT operations respondents believe the most difficult endpoint configuration management to maintain across all endpoints is new OS and application versions (73 percent vs. 51 percent of IT security respondents). As shown in Figure 13, IT security is most likely to say feature utilization is most difficult (46 percent of IT security vs. 40 percent of IT).

Both groups believe distribution points have increased or increased significantly over the past two years. Sixty percent of IT agrees, and 61% of ITS agrees.

Figure 13. Which aspects of endpoint configuration management are the most difficult to maintain across all endpoints?

More than one response permitted



KEY FINDING 4

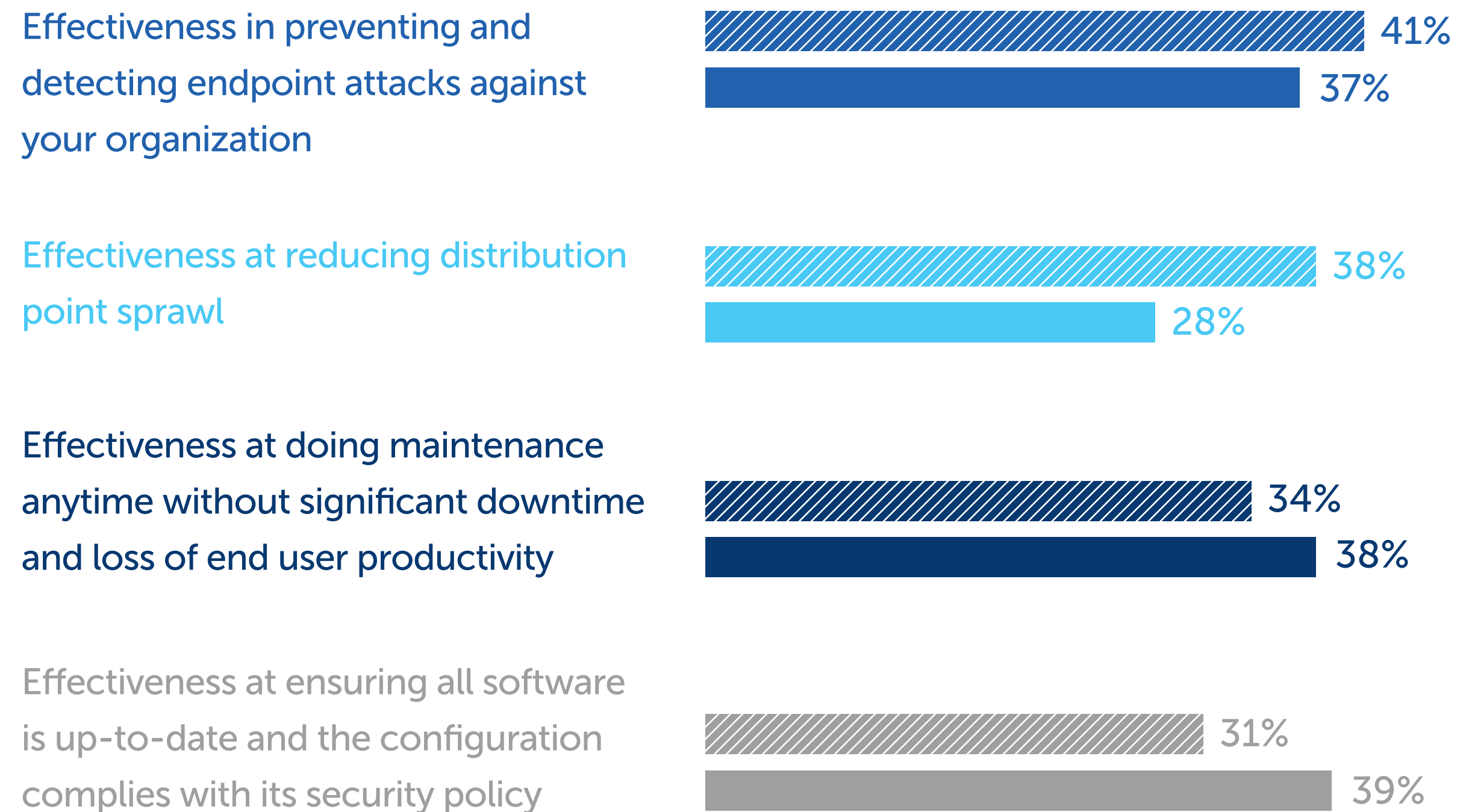
Endpoint Security Perception Gap

Effectiveness of Reducing Risk at the Edge

IT operations is more confident than IT security in their organizations' ability to reduce distribution point sprawl. Respondents were asked to rate the effectiveness of reducing risks at the edge. Figure 15 shows the very effective and highly effective responses (7+ on the 10-point scale). According to the comparison between IT operations and IT security, 38 percent of IT operations vs. 28 percent of IT security rate the effectiveness at reducing distribution point sprawl as very or highly effective. IT security is more confident in its effectiveness in ensuring all software is up-to-date and the configuration complies with its security policy.

Figure 15. Effectiveness in reducing risk at the edge.

On a scale from 1 = not effective to 10 = highly effective, 7+ responses presented



CONCLUSION

An Overdue New Approach to a Generations-old Problem

If the results of this survey teach us anything, it's that something has to change. Companies have acknowledged they have problems managing devices, especially in a distributed context. But no one is sure of the solution; they just plan to spend more on improving the distribution points that underpin their endpoint management infrastructure. On average, they will increase their expenditure from 12% to 21% in the next year. If their investments yield the same results, the problem remains the same. Where they spend that money is critically important. Contrary to popular opinion, investing

more in centralized distribution infrastructures won't solve the problem; simply moving to the cloud won't solve the problem. The plan to invest money in endpoint security content distribution is promising, but it's only one part of the solution. Throwing more money at more distribution servers will just increase the investment without solving the underlying problem. It will increase management costs without improving device visibility. Employing more people to find and fix systems won't work either, because they can't fix what they can't see. And what they can't see is at the core of the problem. Every new security solution that bolts onto your existing stack will just make it more complex and less agile.

Here's how to make your dollars work smarter. Rather than relying on tools that run on centralized infrastructure to monitor and maintain widely distributed endpoint devices, consider utilizing your edge as the infrastructure instead. Shifting from centralized infrastructure, whether on-prem or in the cloud, to one powered by your edge will help keep endpoints visible, allowing them to remain up to date to protect them against threats. You'll have complete visibility from your position of central control and be able to see with more clarity how your endpoint devices are behaving, while containing costs.

This will allow you to eliminate distribution points from your architecture, as the apps that monitor and maintain your endpoints will reside and execute on your edge rather than on unscalable centralized servers. This will create a self-sustaining, fault-tolerant, and adaptive network of peer-to-peer endpoints that heighten performance, security, and resilience. Half of our 629 survey respondents tell us that a remote workforce has made it difficult for them to distribute the security updates and patches that people need. In a new, decentralized reality, these client devices can instead use their spare computing and storage resources to distribute security patches, configuration changes, and software updates to their peers securely and reliably. With many employees unlikely to return to the office full-time, managing endpoint security in an edge-centric world is a priority. It's time to revolutionize endpoint management and push it to the edge.



DEEPAK KUMAR
FOUNDER & CEO, ADAPTIVA

PART III

Methodology

A sampling frame of 17,663 IT operations and IT security professionals in the United States that are involved and influential in their organization’s endpoint management strategy were selected as participants to this survey. Table 1 shows 698 total returns. Screening and reliability checks required the removal of 69 surveys. Our final sample consisted of 629 surveys or a 3.6 percent response.

Survey Response	Frequency	Percent
Sampling frame	17,663	100%
Total returns	698	4.0%
Rejected or screened surveys	69	0.4%
Final sample	629	3.6%

Figure 16. Current position within the organization

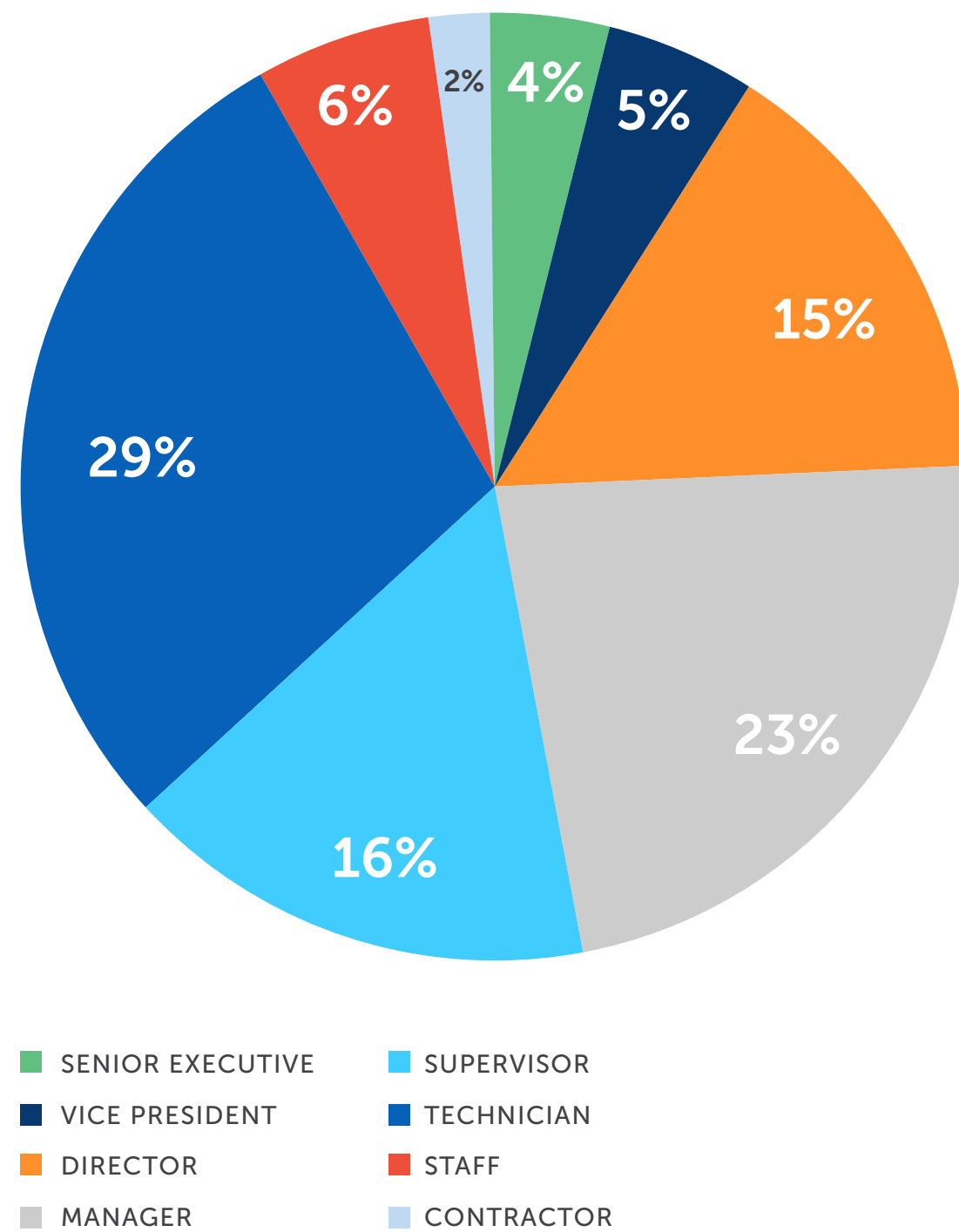
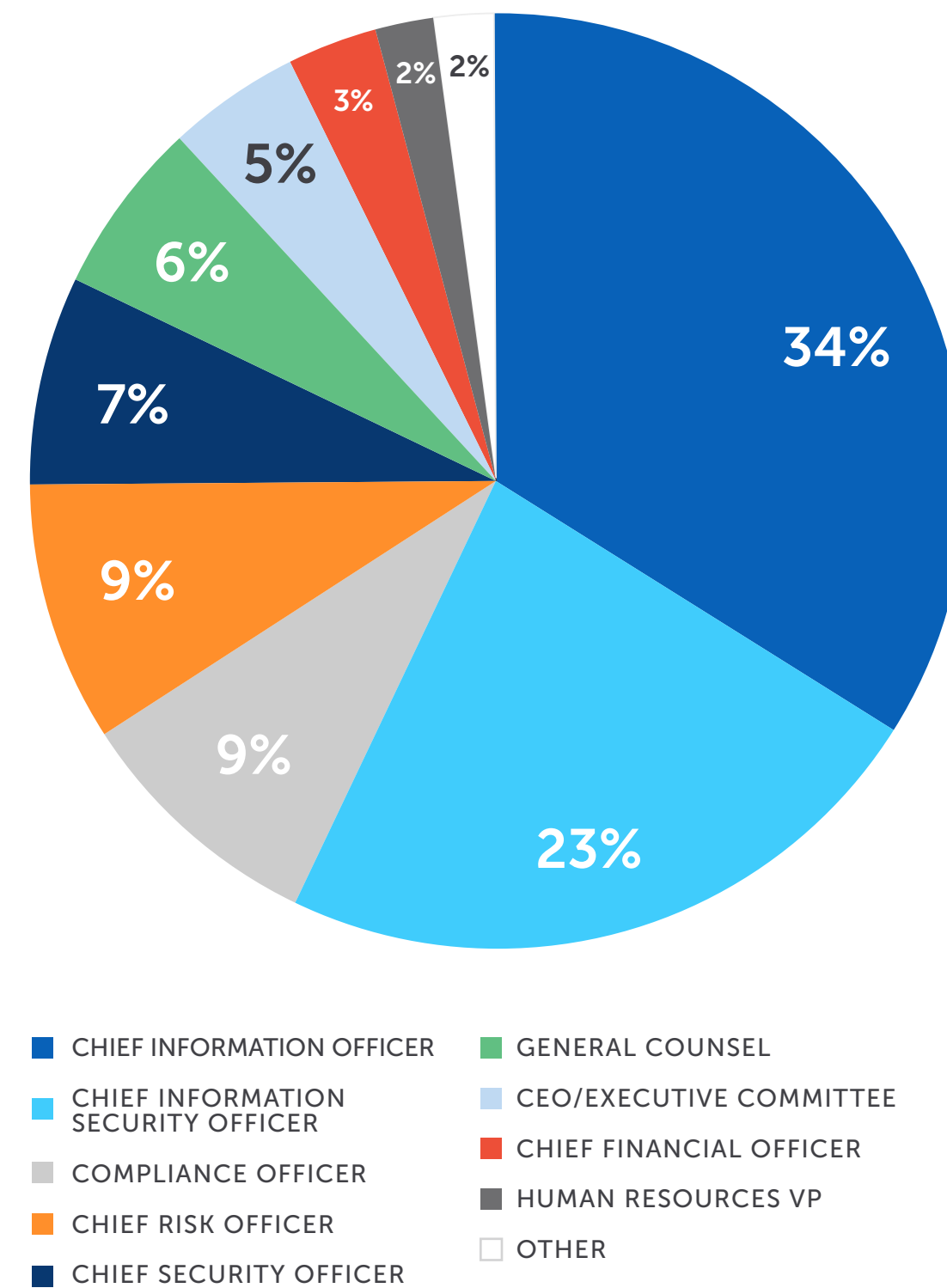


Figure 16 reports the respondent's organizational level within participating organizations. By design, more than half (63 percent) of respondents are at or above the supervisory levels. The largest category at 29 percent of respondents is technician.

Figure 17. Direct reporting channel



As shown in Figure 17, 34 percent of respondents report to the Chief Information Officer, 23 percent of respondents report to the Chief Information Security Officer, 9 percent of respondents report to the Compliance Officer, 9 percent of respondents report to the Chief Risk Officer and 7 percent of respondents report to the Chief Security Officer.

Figure 18. Primary industry classification

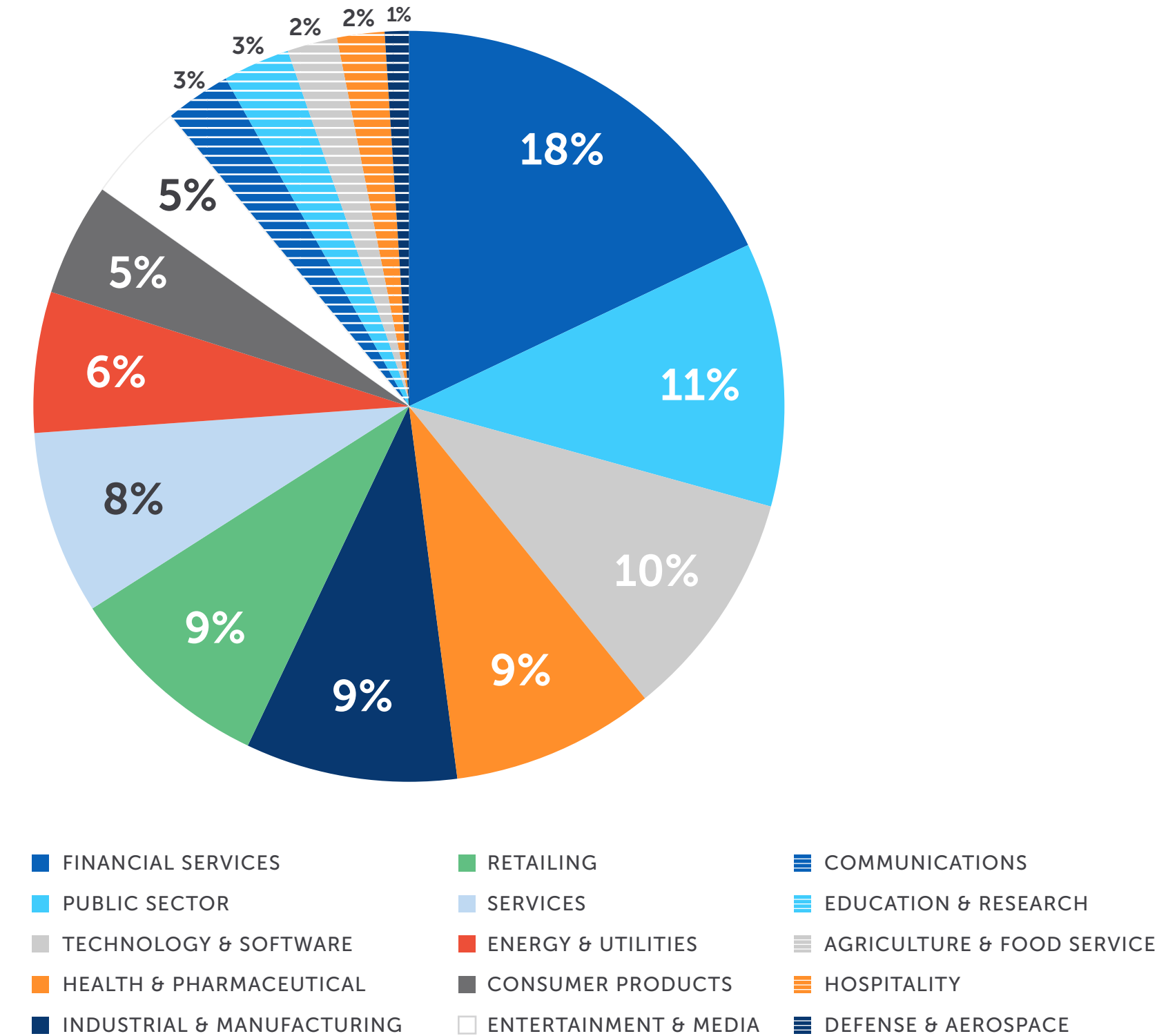


Figure 18 reports the industry classification of respondents' organizations. This chart identifies financial services (18 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by public sector (11 percent of respondents), technology and software (10 percent of respondents), healthcare and pharmaceuticals (9 percent of respondents), industrial and manufacturing (9 percent of respondents), retailing (9 percent of respondents) and services (8 percent of respondents).

PART IV

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 involved and influential in their organization's endpoint management strategy. 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.

PART V

Appendix

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 January 2022.

Survey Response	Frequency
Total sampling frame	17,663
Survey returns	698
Rejected surveys	69
Final sample	629
Response rate	3.6%

Part 1. Screening

S1. How involved and influential are you in your organization’s endpoint management strategy?

No involvement and influence (stop)	0%
Significant involvement and influence in our organization’s endpoint management strategy	39%
Involvement and influence in our organization’s endpoint management strategy	42%
Some involvement and influence in our organization’s end-point management strategy	19%
Total	100%

S2. What is your organization’s headcount?

Less than 1,000 (stop)	0%
1,000 to 2,500	30%
2,501 to 5,000	27%
5,001 to 10,000	11%
10,001 to 25,000	17%
25,001 to 50,000	8%
50,000 to 75,000	5%
75,001 to 100,000	2%
More than 100,000	0%
Total	100%
Extrapolated value	13,213

Part 2. Background

Q1. What best describes your role in the organization?

CIO	18%
IT director	11%
IT manager	15%
IT systems administrator	6%
IT operations	5%
CISO	19%
CSO	2%
IT security director	13%
IT security manager	10%
Other (please specify)	1%
Total	100%

Q2. – Q5. Please rate the following statements using the agreement scale provided below each item. Strongly Agree and Agree response.

We have ample resources to minimize endpoint risk throughout our organization.	34%
A remote workforce has made it difficult to deliver necessary security updates and patches to endpoints.	49%
My organization has established clearly defined roles and accountability for safeguarding of confidential or sensitive information stored on endpoints and in the cloud.	47%
In the past two years, prevention and detection of attacks against our endpoints has become more of a priority in our organization’s overall IT security strategy.	63%

Part 2. Background

Q6. How many endpoints does your organization have?

Less than 5,000	4%
5,001 to 10,000	6%
10,001 to 25,000	14%
25,001 to 50,000	26%
50,001 to 100,000	23%
100,001 to 500,000	19%
More than 500,000	8%
Total	100%
Extrapolated value	135,000

Q7. What percentage of these endpoint devices are at risk because they are not detected by IT or the organization has an outdated operating system?

Less than 10%	8%
10% to 25%	18%
26% to 50%	26%
51% to 75%	31%
76% to 100%	17%
Total	100%
Extrapolated value	48%

Q8. Which aspects of endpoint configuration management are the most difficult to maintain across all endpoints? Please check all that apply.

New OS & application versions	62%
Patches and security updates	59%
Feature utilization	43%
Network settings and connectivity	50%
System performance and tuning	36%

Q9. How many distribution points does your organization have?

Less than 1,000	7%
1,000 to 5,000	18%
5,001 to 10,000	23%
10,001 to 25,000	18%
25,001 to 50,000	25%
50,001 to 100,000	6%
More than 100,000	3%
Total	100%
Extrapolated value	22,925

Part 2. Background

Q10. How has this amount changed in the past two years (i.e. distribution sprawl)?

Significantly increased (more than 20 percent)	26%
Increased (more than 10 percent)	35%
Somewhat increased (more than 5 percent)	23%
Decreased (by 5 percent)	9%
Decreased significantly (by 10 percent)	7%
Total	100%

Q11. 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.

1 to 2	14%
3 to 5	20%
6 to 10	31%
More than 10	35%
Total	100%
Extrapolated value	7.7

Q12. What are the biggest threats to endpoint security in your organization?
Please select all that apply.

Advanced persistent threats (APT)/targeted attacks	26%
Botnet attacks	21%
Clickjacking	11%
Credential theft	39%
DDoS`	43%
Distribution point sprawl	34%
Exploit of existing software vulnerability > 3 months old	21%
Exploit of existing software vulnerability < 3 months old	17%
Ransomware	48%
Rootkits	9%
Spear phishing	25%
SQL injection	10%
Web-borne malware attacks	32%
Zero-day attacks	45%
Spyware	6%

Part 2. Background

Q13. How effective is your organization in preventing and detecting endpoint attacks against your organization? Please use the following scale from 1 = not effective to 10 = highly effective.

1 or 2	16%
3 or 4	22%
5 or 6	23%
7 or 8	19%
9 or 10	20%
Total	100%
Extrapolated value	5.60

Q14. How effective is your organization at doing maintenance any-time without significant downtime and loss of end user productivity? Please use the following scale from 1 = not effective to 10 = highly effective.

1 or 2	12%
3 or 4	19%
5 or 6	33%
7 or 8	21%
9 or 10	15%
Total	100%
Extrapolated value	5.66

Q15. How effective is your organization at achieving endpoint compliance with regulations? Please use the following scale from 1 = not effective to 10 = highly effective.

1 or 2	12%
3 or 4	25%
5 or 6	28%
7 or 8	19%
9 or 10	16%
Total	100%
Extrapolated value	5.54

Q16. How effective is your organization at ensuring all software is up-to-date and the configuration complies with its security policy? Please use the following scale from 1 = not effective to 10 = highly effective.

1 or 2	15%
3 or 4	19%
5 or 6	31%
7 or 8	20%
9 or 10	15%
Total	100%
Extrapolated value	5.52

Part 2. Background

Q17. How effective is your organization at reducing distribution point sprawl? Please use the following scale from 1 = not effective to 10 = highly effective.

1 or 2	15%
3 or 4	25%
5 or 6	27%
7 or 8	20%
9 or 10	13%
Total	100%
Extrapolated value	5.32

Q18. What are the most significant barriers to achieving a strong endpoint security posture? Please select all that apply.

Inability to have enough control over remote user’s personal devices	21%
Inability to keep endpoints up to date, meet standard configurations and detect vulnerabilities	37%
Lack of budget	34%
Lack of in-house expertise	45%
Lack of ability to achieve speed and scalability of endpoint management solution	42%
Lack of bandwidth to send updates without compromising network performance	39%
Amount of time required to ensure new or upgraded content makes it to all endpoints	29%
Exploit of existing software vulnerability less than 3 months old	35%
Exploit of existing software vulnerability greater than 3 months old	44%
Lack of visibility of all endpoints	63%
Clickjacking	15%
Rootkits	13%
Other (please specify)	3%
Total	420%

Part 3. Economic Impact and Budget

Q19. How much does your organization spend on endpoint protection per endpoint (i.e. laptop/desktop)?

Less than \$30 per year	62%
\$30 to \$60 per year	21%
More than \$60 per year	17%
Total	100%
Extrapolated value	31.50

Q20. How much does your organization spend per server on protection?

Less than \$30 per year	32%
\$30 to \$60 per year	33%
More than \$60 per year	35%
Total	100%
Extrapolated value	45.90

Q21a. Has your company experienced one or more endpoint attacks that have successfully compromised data assets and/or IT infrastructure over the past 12 months?

Yes	54%
No (Please skip to Q24)	46%

Q21b. If yes, how many attacks did your organization experience?

1	23%
2 to 4	17%
5 to 6	19%
7 to 8	21%
8 to 10	13%
More than 10	7%
Total	100%
Extrapolated value	5.37

Q22. How did these attacks get into your organization? Please select all that apply.

Through our website	21%
Through our email system	41%
Through APIs	36%
Through software updates/patches	35%
Other (please specify)	5%
Total	138%

Part 3. Economic Impact and Budget

Q23. In the past two years, please estimate the total economic loss as a result of these breaches and failures on your organization’s endpoints. This should include IT staff costs, downtime, lost business, damaged reputation, fines and legal fees and stolen proprietary and sensitive information.

Less than \$50,000	4%
\$50,001 to \$100,000	7%
\$100,001 to \$ 250,000	12%
\$250,001 to \$500,000	15%
\$500,001 to \$750,000	21%
\$750,001 to \$1,00,000	16%
\$1,00,001 to \$5,000,000	11%
\$5,000,001 to \$10,000,000	7%
\$10,000,001 to \$50,000,000	6%
More than \$50,000,000	1%
Extrapolated value	3,602,250

Q24. Following are 6 cost consequences that may be experienced by your company as a result of one or more successful endpoint attacks. 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 to all cost consequences listed below.

IT & end-user productivity loss	21
System downtime	27
Theft of information assets	21
Damage to IT infrastructure	10
Lawsuits, fines, regulatory action	10
Reputation/brand damage	11
Total	100

Q25. With your current enabling technologies, processes and in-house expertise, what percentage of these attacks to your organization’s endpoints could have been stopped?

Less than 10%	7%
10% to 25%	21%
26% to 50%	23%
51% to 75%	18%
76% to 95%	17%
More than 95%	14%
Total	100%
Extrapolated value	52%

Part 3. Economic Impact and Budget

Q26a. How much is spent annually on your organization’s IT and IT security help desk?

Less than \$50,000	4%
\$50,001 to \$100,000	15%
\$100,001 to \$250,000	21%
\$250,001 to \$500,000	23%
\$500,001 to \$1,000,000	16%
More than \$1,000,000	21%
Total	100%
Extrapolated value	\$507,250

Q26b. Currently, what percentage of all help desk costs are attributed to such endpoint issues as break/fix software, password/login security, security problem occurred or is suspected, break/fix hardware, application request or other issue?

Less than 1%	4%
1% to 2%	7%
3% to 5%	4%
6% to 10%	5%
11% to 15%	8%
16% to 20%	9%
21% to 30%	11%
31% to 40%	17%
41% to 50%	13%
>50%	22%
Extrapolated value	30%

Q27. What percentage of costs could be reduced through automation of investigation and remediation?

Less than 1%	0%
1% to 2%	5%
3% to 5%	9%
6% to 10%	15%
11% to 15%	10%
16% to 20%	12%
21% to 30%	15%
31% to 40%	9%
41% to 50%	10%
>50%	15%
Extrapolated value	25%

Q28. How much employee time is lost monthly due to downtime or attacks against the endpoint?

Less than 10 hours	5%
10 hours to 25 hours	11%
26 hours to 50 hours	21%
51 hours to 75 hours	33%
76 hours to 100 hours	21%
More than 100 hours	9%
Total	100%
Extrapolated value (Hours)	59.85

Part 3. Economic Impact and Budget

Q29. Following are 4 types of ongoing costs related to endpoint protection. Please rank these costs from 1 = most costly to 4 = least costly.

The cost of hiring & retaining security experts	2.7
The cost of inefficient security practices (e.g. false positives)	3.3
The cost of engaging outside vendors and consultants	2.1
The cost caused by software compatibility issues	1.9
Average rank	2.5

Q30. What is your organization’s total IT budget?

Less than \$100,000	0%
\$100,000 to \$500,000	3%
\$500,001 to \$1,000,000	5%
\$1,00,001 to \$5,000,000	9%
\$5,000,001 to \$10,000,000	14%
\$10,000,001 to \$50,000,000	21%
\$50,000,001 to \$100,000,000	23%
\$100,000,001 to \$500,000,000	12%
\$500,000,001 to \$1,000,000,000	7%
More than \$1,000,000,000	6%
Total	100%
Extrapolated value (US\$)	\$ 184,366,500

Q31. What percentage of your organization’s IT budget is allocated to IT security?

Less than 10%	5%
10% to 15%	8%
16% to 20%	18%
21% to 25%	16%
26% to 30%	20%
More than 30%	33%
Total	100%
Extrapolated value	25%

Part 3. Economic Impact and Budget

Q32a. What percentage of your organization’s IT security budget is allocated to endpoint management?

Less than 10%	12%
10% to 15%	20%
16% to 20%	23%
21% to 25%	11%
26% to 30%	20%
More than 30%	14%
Total	100%
Extrapolated value	20%

Q32b. Is this budget adequate?

More than adequate	24%
Less than adequate	36%
Not adequate	40%

Q33a. How many IT staff are dedicated to endpoint security management?

Less than 5	11%
5 to 10	28%
11 to 20	38%
21 to 50	15%
More than 50	8%
Total	100%
Extrapolated value	18.7

Q33b. Is this staffing sufficient?

Yes	47%
No	53%

Q34. Please allocate 100 percentage points to show how your endpoint management budget is allocated today and will be allocated in the next 12 months. Average Rank of IT endpoint management budget allocation, today compared to in the next 12 months.

	AVG. RANK TODAY	AVG. RANK IN THE NEXT 12 MONTHS
Delivering security updates	25	20
Compliance	19	18
Responding to breaches or failures	25	20
Distributing software to clients	19	21
Managing distribution points	12	21
Total	100	100

Part 4. Organizational Characteristics & Demographics

D1. What organizational level best describes your current position?

Senior Executive	4%
Vice President	5%
Director	15%
Manager	23%
Supervisor	16%
Technician	29%
Staff	6%
Contractor	2%
Other	0%
Total	100%

D2. Check the Primary Person you or your IT security leader reports to within the organization.

CEO/Executive Committee	5%
Chief Financial Officer (CFO)	3%
General Counsel	6%
Chief Information Officer (CIO)	34%
Chief Information Security Officer (CISO)	23%
Compliance Officer	9%
Human Resources VP	2%
Chief Security Officer (CSO)	7%
Chief Risk Officer (CRO)	9%
Other	2%
Total	100%

D3. What industry best describes your organization’s primary industry focus?

Agriculture & food service	2%
Communications	3%
Consumer products	5%
Defense & aerospace	1%
Education & research	3%
Energy & utilities	6%
Entertainment & media	4%
Financial services	18%
Health & pharmaceutical	9%
Hospitality	2%
Industrial & manufacturing	9%
Public sector	11%
Retailing	9%
Services	8%
Technology & software	10%

THANK YOU

