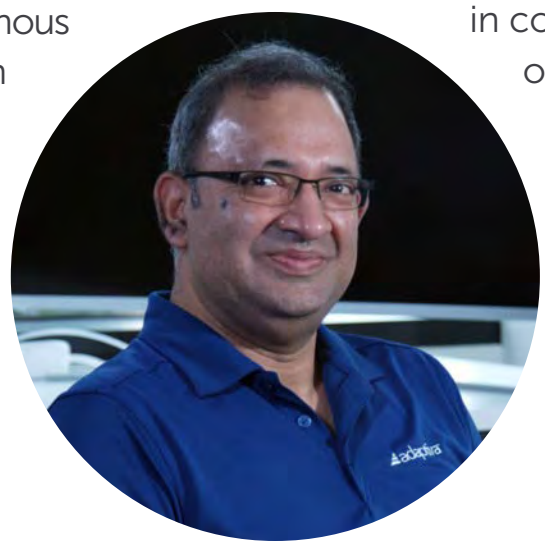
2023 PONEMON INSTITUTE REPORT

2023 REPORT
THE STATE OF PATCH MANAGEMENT
IN THE DIGITAL WORKPLACE

adaptiva + Ponemon INSTITUTE

Executive Summary

DEEPAK KUMAR, FOUNDER & CEO, ADAPTIVA



After the recent launch of our new Autonomous Patch solution, we partnered with Ponemon Institute to develop a report on the state of Patch Management. This research found that three core aspects of patch management are broken—**Visibility, Deployment, and Process Management.** IT doesn't have reliable visibility over the applications that run on their organizations' devices. Detecting vulnerabilities and assessing risk and exposure of applications are two of the hardest and most complex parts of the process, according to 54% and 50% of respondents respectively. There is little confidence that a deployed patch has been installed correctly and, on the machines requiring it. Further, bandwidth issues continue to plague IT as remote and hybrid workplaces are now the norm. Finally, patching takes up an inordinate amount of time across multiple people's schedules every single week. **This report paints a clear picture—patching is hard.**

VISIBILITY

Sixty-Nine percent of respondents reported that they don't know how many applications are installed on endpoint devices. The average organization has nearly 3,000 applications (2,908) installed on their endpoint devices, and that number is increasing for 54% of respondents. Considering 31% of respondents reported more than 5,000 applications on their endpoints—that number could be tens of thousands, a much scarier number considering IT is mostly flying blind with little visibility over all those apps.

DEPLOYMENT

Fifty-nine percent of respondents take at least 2 weeks to begin a patch deployment after it has been released, but only 34% can reliably confirm that a deployed patch has been installed on the appropriate devices. This is probably why nearly 80% of applications are out of compliance with organization SLAs (only 20.8% in compliance). It also explains why 62% of respondents have low confidence in complying with SLAs. And with so many employees in the digital workplace working in unpredictable locations with unreliable networks – bandwidth continues to be an issue as 56% of respondents agree that low bandwidth makes patching more difficult.

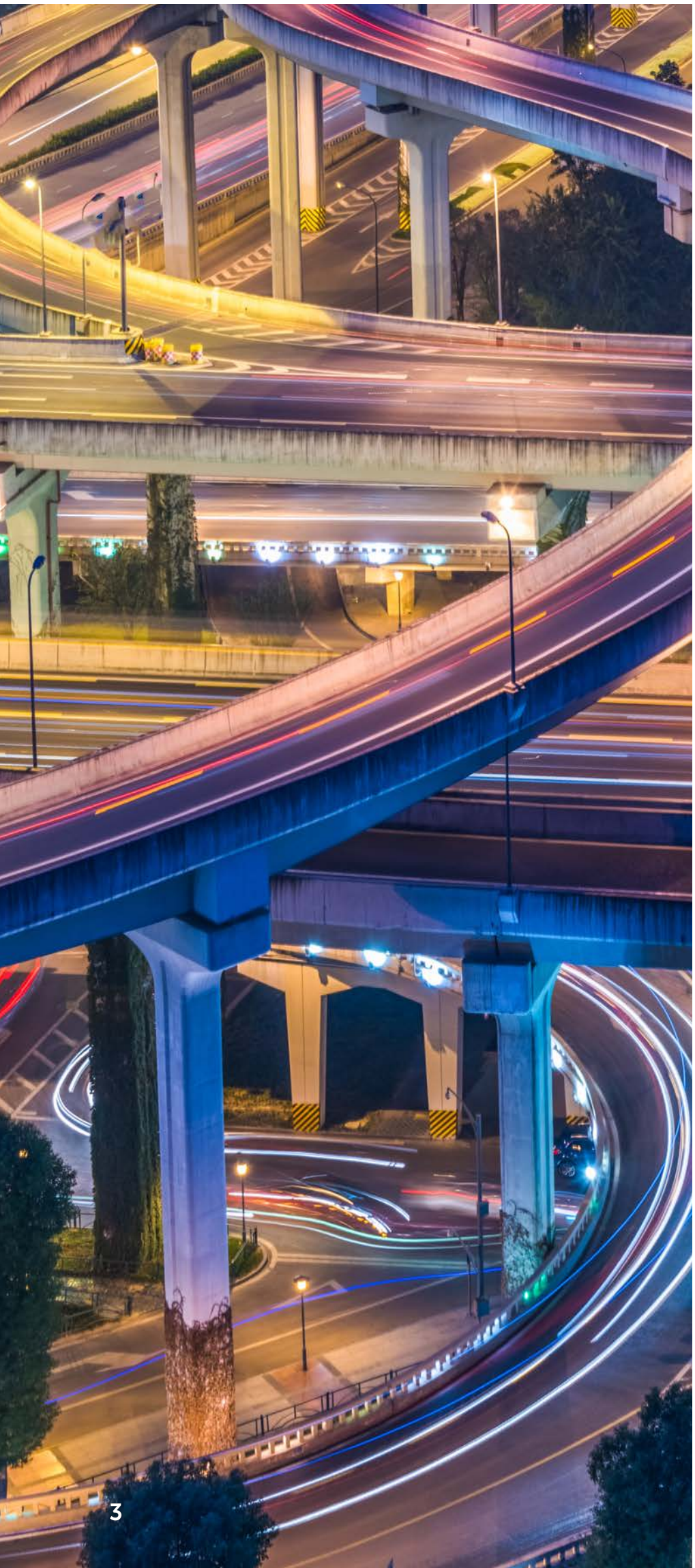
PROCESS MANAGEMENT

Patching devices is a complex process that gets more complicated as the volume of applications, patches, and people increases. Most patches are handled with an ad-hoc approach (44%) and only 31% of patches are distributed using automation, leaving humans to painstakingly manage the entire process and repeat mundane tasks over and over again. On average, 20 IT people are involved in the patching process, which represents about half the headcount in the average IT organization.

Sixty-five percent of respondents are spending over 10 hours a week on patching, 26% are over 25 hours a week. That could range from 520 to 1,300 hours in a year spent on patching alone. With 20 people involved in the process the time spent on patching can get out of hand quickly across an organization and reduce the time available to solve for unique problems, leaving even more vulnerabilities.

But before you think about adding more humans to the process, take note that **69% of respondents don't believe an IT team of any size can keep up with 100% patching.** Ponemon Institute also found that implementing automation to investigate and remediate vulnerabilities and attacks can reduce the average cost of a breach by 25% or $450,000 per breach. **Enjoy the report—and make sure to stick around to the end for a path through this madness.**

Table of Contents



adaptiva + Ponemon INSTITUTE

PART I
Introduction

Patching paralysis is diminishing organizations' security posture. A key takeaway from this research is that IT teams are overburdened and struggle to keep up with an ever-increasing volume of patches. The average full-time IT staff is 51 and an average of 21 IT staff are directly involved in the patching process. That means over 40 percent of IT staff's valuable time is consumed by patching.

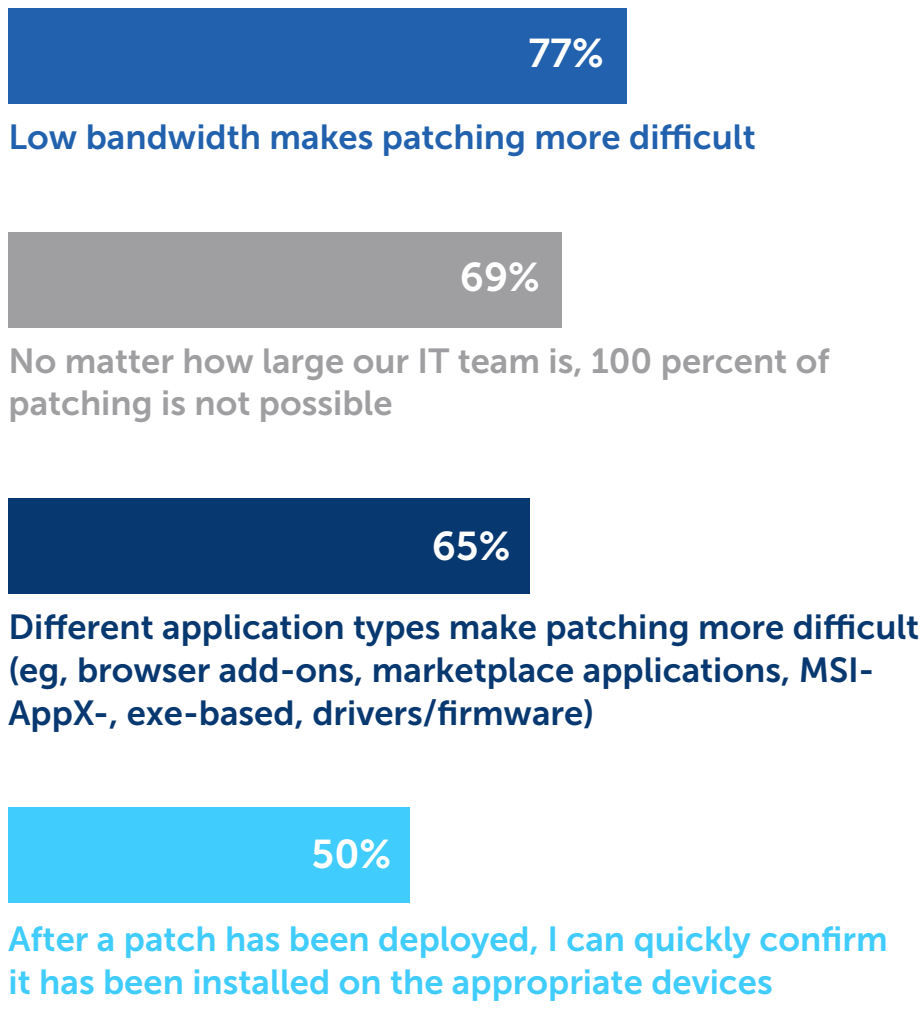
Ponemon Institute surveyed 663 IT and IT security practitioners in the United States who are involved and influential in their organizations' patch management strategy. The average headcount of organizations represented in this research is 30,405.

Bandwidth and Visibility Issues

According to the research, patching problems are not going away because of the reasons cited in Figure 1. The number one complaint, according to 77 percent of respondents, is the impact of low bandwidth on the ability to patch, which needs to be addressed if the process of patching vulnerabilities is to be improved. With an expanding digital workforce, the implications of the struggle with low bandwidth becomes an even greater challenge to overcome.

Because of the inordinate amount of time required to patch, 69 percent of respondents say that no matter how large the IT team is, the ability to patch 100 percent of applications is not possible. Only half of respondents (50 percent) say that after a patch has been deployed, they can quickly confirm it has been installed on the appropriate devices. This lack of real-time visibility into the process means that half of enterprises are playing a game of guesswork. Patching is also more difficult because of the wide range of application types they have to oversee (65 percent of respondents).

Figure 1. Why patching continues to be a herculean task Strongly agree, Agree and Unsure responses combined



The following findings reveal the state of patch management.

1 **Detection of vulnerabilities** is the hardest part of the patching process.

2 **The lack of application visibility** diminishes the effectiveness of patch management programs.

3 An increase in the number of applications means that **the volume of patches will continue to grow.**

4 Organizations lack confidence in their ability to **comply with current patch SLAs.**

5 An average of **60 percent of tracked applications are out of compliance** because they are not at approved versions that meet SLAs.

6 Patch deployment after release by the manufacturer **can take as long as two weeks.**

7 Patch deployment delays are **opportunities for hackers.**

8 It takes at least 5 hours and as much as more than 10 hours to **remediate a broken or failed patch.**

9 **Patch deployment is ad hoc.**

10 When patches are broken or fail, **how are organizations rolling them back?**

11 Decisions about patch distribution are **dispersed throughout the organization.**

12 **Decisions about patch deployment** should not be a one-size-fits-all.

13 Advances in technology such as **artificial intelligence and machine learning** make patch automation faster, smoother, and easier.

1

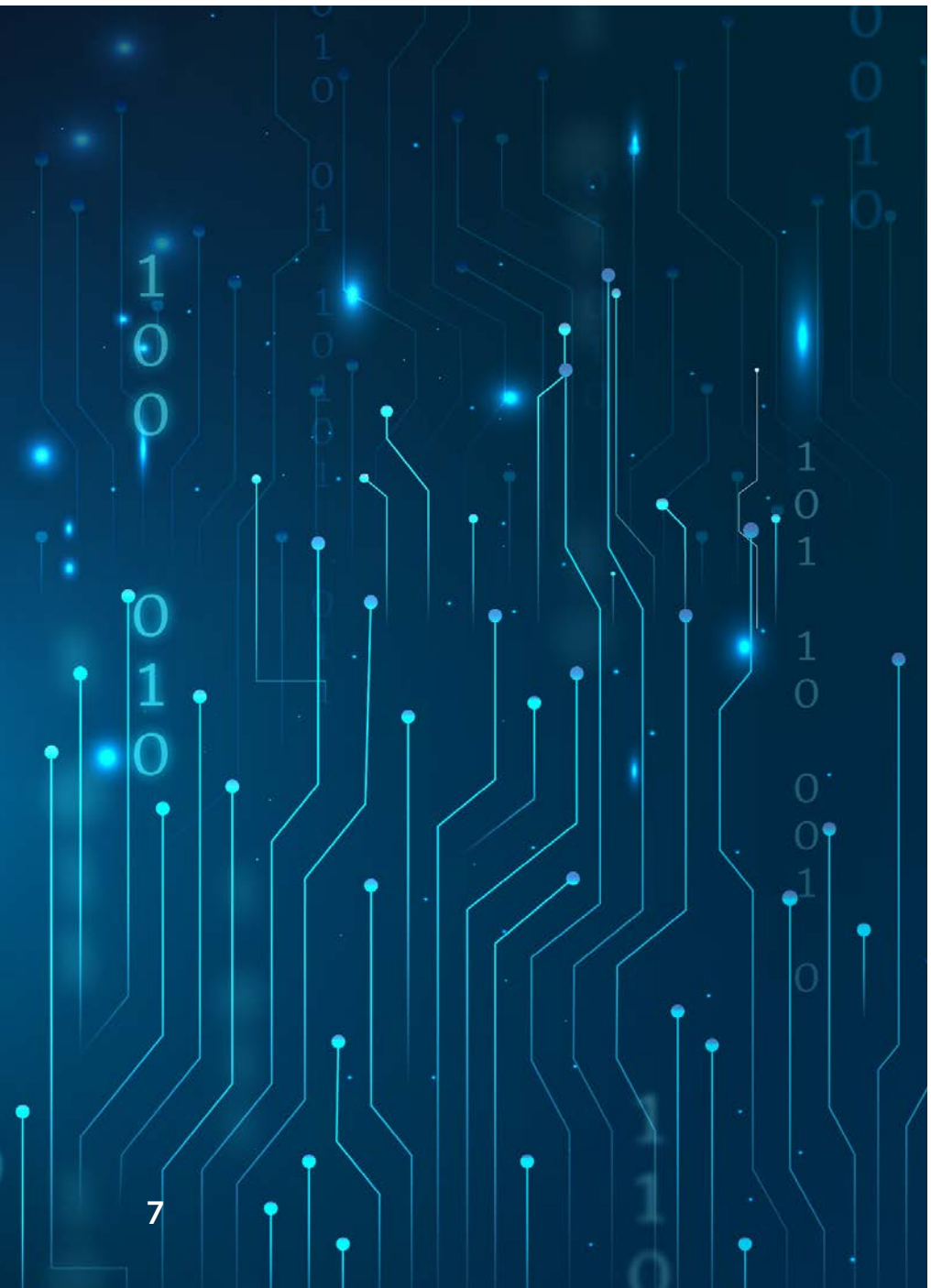
Detection of vulnerabilities is the hardest part of the patching process.

Most organizations are in the dark about how many distinct applications are installed on endpoint devices, making it difficult to determine the number of vulnerabilities that need to be patched and those that pose the greatest risk. Most challenging is the detection of vulnerabilities (54 percent of respondents) and risk and exposure (50 percent of respondents).

2

The lack of application visibility diminishes the effectiveness of patch management programs.

Only 31 percent of respondents say their organizations know approximately how many distinct applications are installed on endpoint devices. These respondents estimate that their organizations have an average of 2,908 applications installed on endpoint devices today. Most respondents (71 percent) say they use antivirus/malware scanning tools and 67 percent of respondents say they use vulnerability scanning tools to gain visibility.



3

An increase in the number of applications means that the volume of patches will continue to grow.

Fifty-four percent of respondents say the number of applications increased significantly or increased in the past two years.

4

Organizations lack confidence in their ability to comply with current patch SLAs.

Only 40 percent of respondents measure compliance with application patching SLAs. Of these respondents, only 22 percent rate their organizations' confidence in their ability to comply with current patch SLAs as high or very high. Commercial applications and in-house line of business applications are most often tracked.

5

An average of 60 percent of tracked applications are out of compliance because they are not at approved versions that meet SLAs.

Compliance with SLAs is at risk because of application version problems. On average, less than half of tracked applications are on the latest version and only 41 percent are on an approved version that meets SLAs.

6

Patch deployment after release by the manufacturer can take as long as two weeks.

It also takes an average of 12 hours to determine when an update has been deployed. Almost half of respondents (48 percent) say it can take at least two weeks for a patch to be deployed across the entire organization.

7

Patch deployment delays are opportunities for hackers.

An average of 10 hours to more than 25 hours is spent deploying patches weekly, according to 65 percent of respondents.

8

It takes at least 5 hours and as much as more than 10 hours to remediate a broken or failed patch.

Only 39 percent of respondents say they can remediate a broken or failed patch in less than 4 hours. Sixty percent of respondents (23 percent + 21 percent + 16 percent) say it takes a minimum of two weeks to achieve the secure installation percentage for a zero-day patch.

9

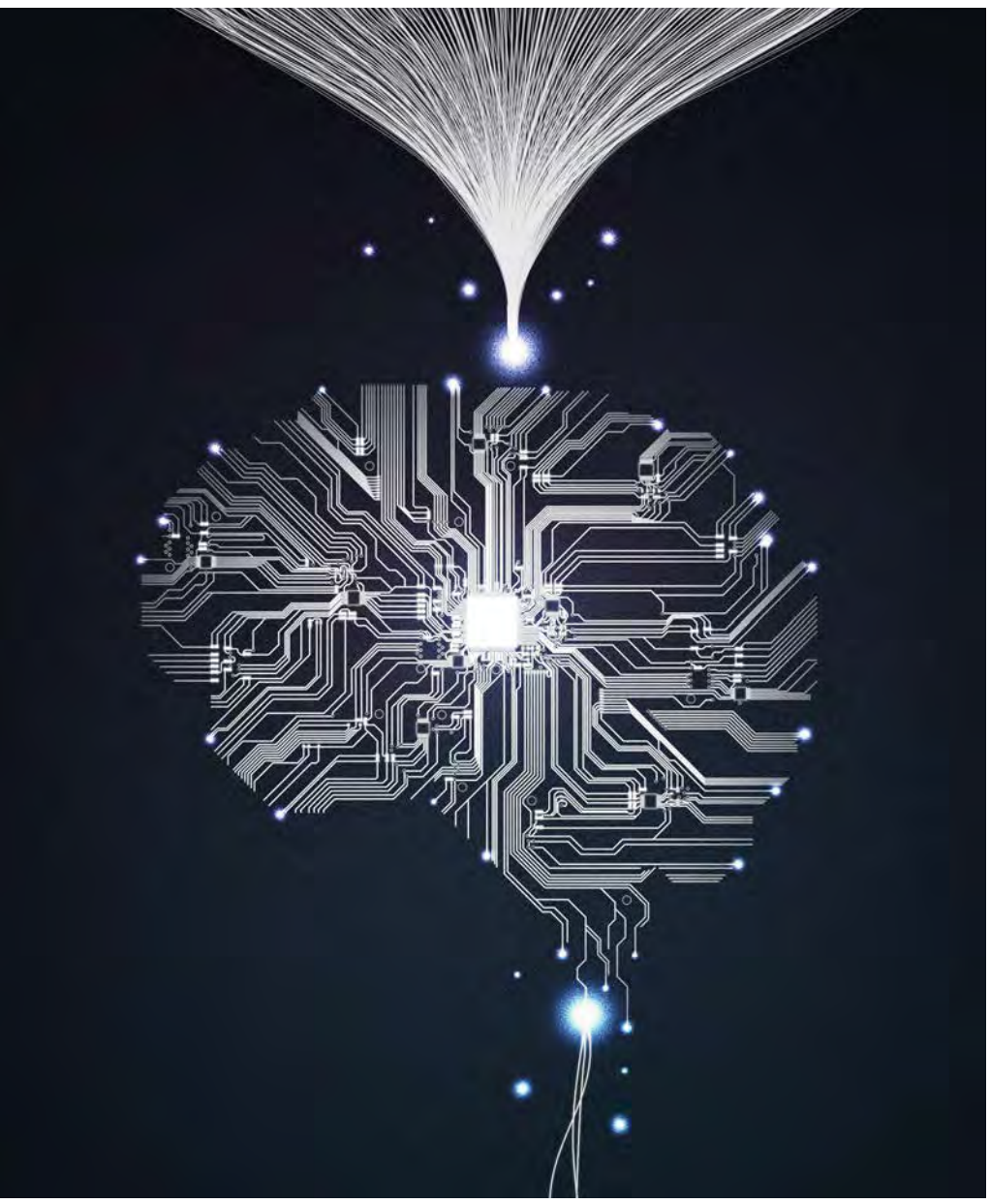
Patch deployment is ad hoc.

Forty-four percent of respondents say scheduling patch deployment is mostly ad hoc. Only 21 percent say it is on a regular schedule applying templatized deployment. Templatizing patch deployments is its own hurdle when using legacy third party patching tools.

10

When patches are broken or fail, how are organizations rolling them back?

Thirty-eight percent of respondents say they start the entire process over from scratch. According to the research, a significant amount of time is spent deploying patches. When organizations have a patch that needs to be reapplied, this can add significant amount of time to the patching process.



11

Decisions about patch distribution are dispersed throughout the organization.

Application owners and IT security are the functions most responsible for deciding when a patch should be distributed. More than half of respondents say their organizations use generic software distribution tools and 47 percent say they use ConfigMgr/SCCM/MEM/Intune to distribute patches.

12

Decisions about patch deployment should not be a one-size-fits-all.

Fifty-six percent of respondents say their organizations deploy patches based on different characteristics such as business unit, function, geographic location, device type, type of users, and risk and exposure. These decisions are mostly based on function, risk, and business unit. These characteristics multiplied by thousands of applications makes patching a herculean task.

13

Advances in technology such as artificial intelligence and machine learning make patch automation faster, smoother, and easier.

However, only an average of 31.4 percent of application patches are distributed using automation. According to Ponemon Institute research, using automation to investigate and remediate vulnerabilities and attacks could reduce the average cost of a breach by 25 percent, or $450,000 per breach.

> If the average organization has almost 3,000 applications installed on their devices and thousands if not hundreds of thousands of devices on its network then it's no wonder IT teams can't keep up. It's no wonder hackers are finding a way in.

—**DAN RICHINGS,**
SVP GLOBAL PRESALES AND SOLUTIONS ENGINEERING AT ADAPTIVA

PART II
Key Findings

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

KEY FINDING 1

Current Patching Practices

KEY FINDING 2

Patching Problems Are Not Going Away

KEY FINDING 3

Time is the Enemy to Achieving a Successful Patching Strategy in a Digital Workplace

CONCLUSION

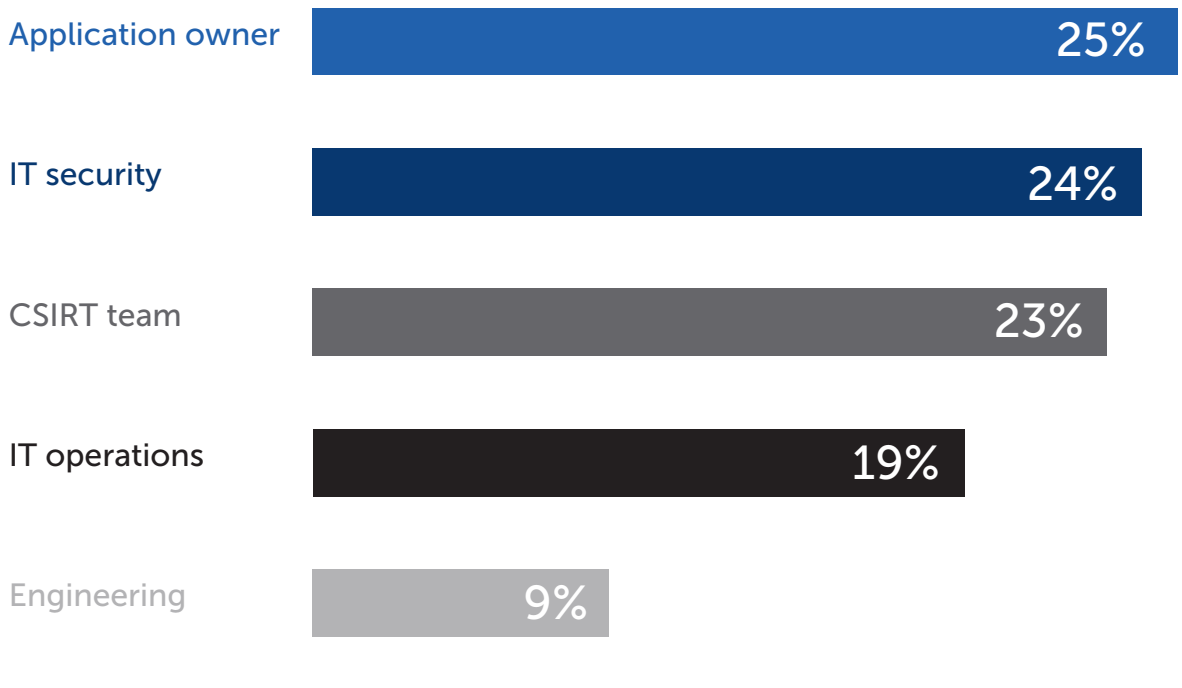
The State of Patch Management in the Digital Workplace

KEY FINDING 1

Current Patching Practices

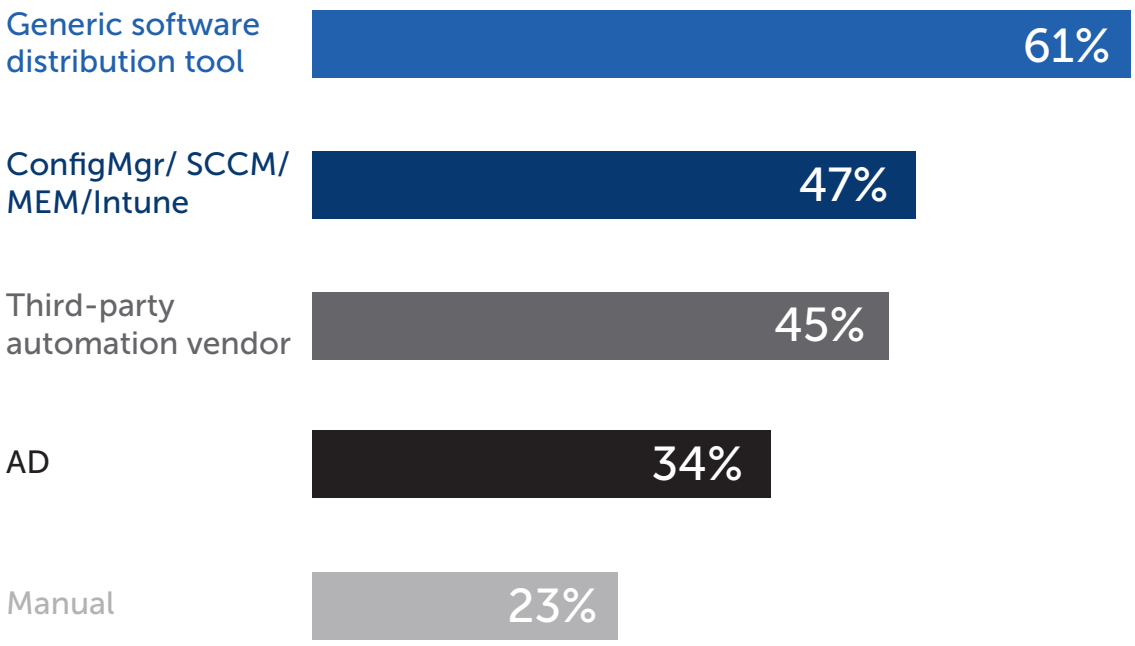
Decisions about patch distribution are dispersed throughout the organization. Application owners and IT security are the functions most responsible for deciding when a patch should be distributed, as shown in Figure 14.

Figure 14. Who decides when a patch should be distributed?



According to Figure 15, more than half of respondents say their organizations use generic software distribution tools and 47 percent say they use ConfigMgr/SCCM/MEM/Intune to distribute patches.

Figure 15. How does your organization distribute patches?
More than one response permitted

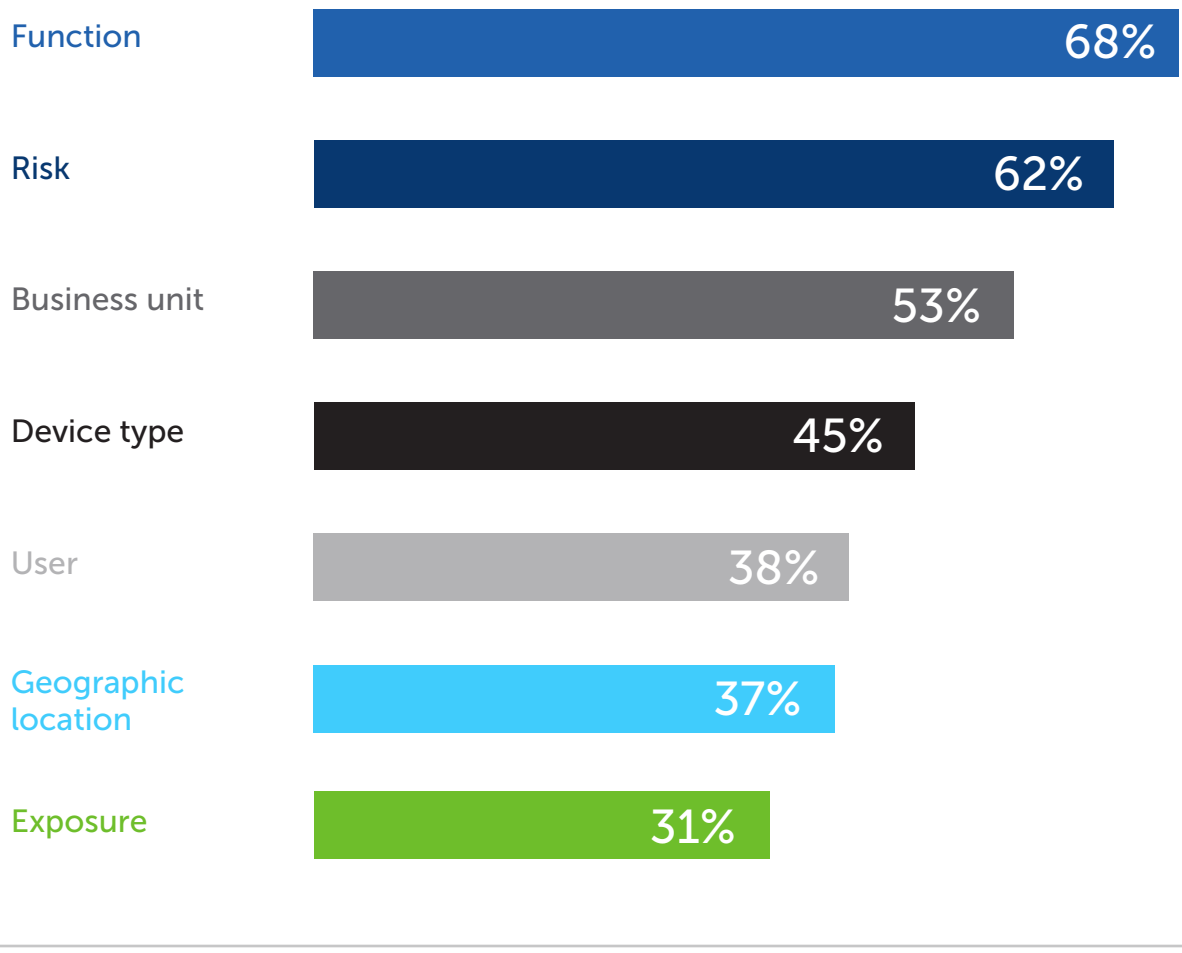


KEY FINDING 1

Current Patching Practices

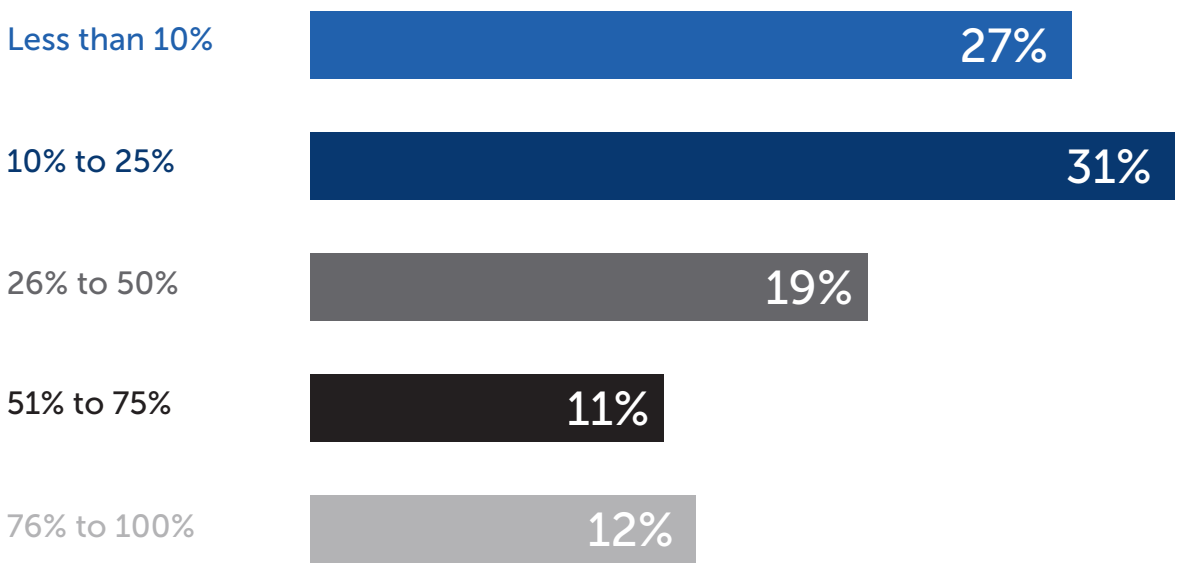
Decisions about patch deployment should not be a one-size-fits-all. Fifty-six percent of respondents say their organizations deploy patches based on different characteristics such as business unit, function, geographic location, device type, type of users, and risk and exposure. According to Figure 16, these decisions are mostly based on function, risk, and business unit.

Figure 16. Which characteristics are used to create unique patching strategies and processes? More than one response permitted



Advances in technology such as artificial intelligence and machine learning make patch automation faster, smoother, and easier than ever. However, as shown in Figure 17, only an average of 31.4 percent of application patches are distributed using automation. According to Ponemon Institute research, using automation to investigate and remediate vulnerabilities and attacks could reduce the average cost of a breach by 25 percent or $450,000 per breach.

Figure 17. What percentage of application patches are distributed using automation? Extrapolated value 31.4 percent



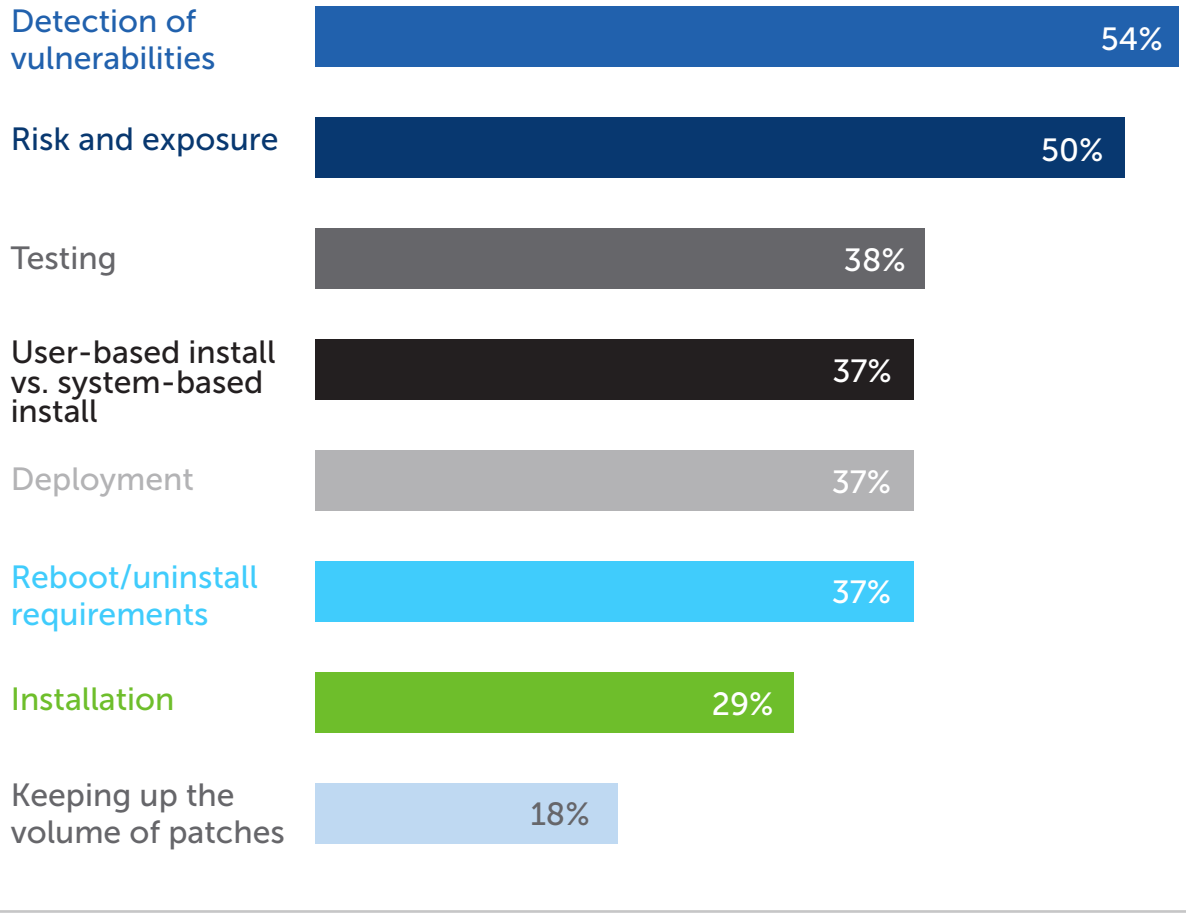
KEY FINDING 2

Patching Problems Are Not Going Away

Detection of vulnerabilities is the hardest part of the patching process. Most organizations are in the dark about how many distinct applications are installed on endpoint devices today making it difficult to determine the number of vulnerabilities that need to be patched and those that pose the greatest risk.

Figure 2 lists the factors that can make patching difficult. Most challenging is the detection of vulnerabilities (54 percent of respondents) and risk and exposure (50 percent of respondents).

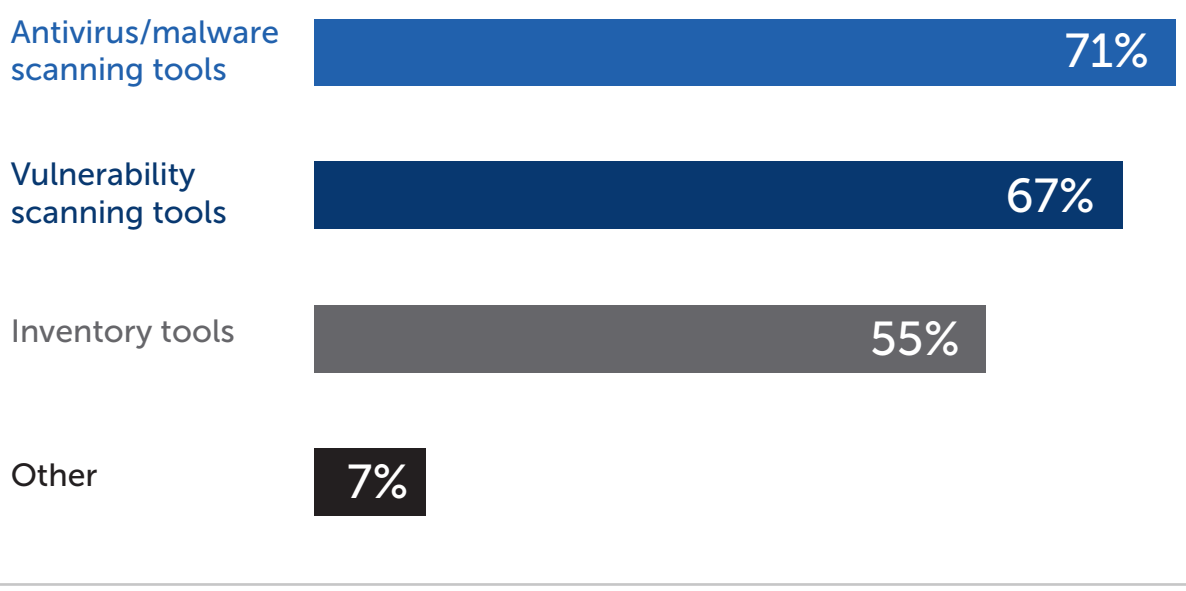
Figure 2. What is the hardest part of the patching process?
Three responses permitted



The lack of application visibility diminishes the effectiveness of patch management programs. Only 31 percent of respondents say their organizations knows approximately how many distinct applications are installed on endpoint devices. These respondents estimate that their organizations have an average of 2,908 applications installed on endpoint devices today.

Figure 3 lists the steps organizations are taking to gain visibility over all applications in use. Most respondents (71 percent) say they use antivirus/ malware scanning tools and 67 percent of respondents say they use vulnerability scanning tools to gain visibility.

Figure 3. What steps are taken to gain visibility over all applications in use across your organization? More than one response permitted

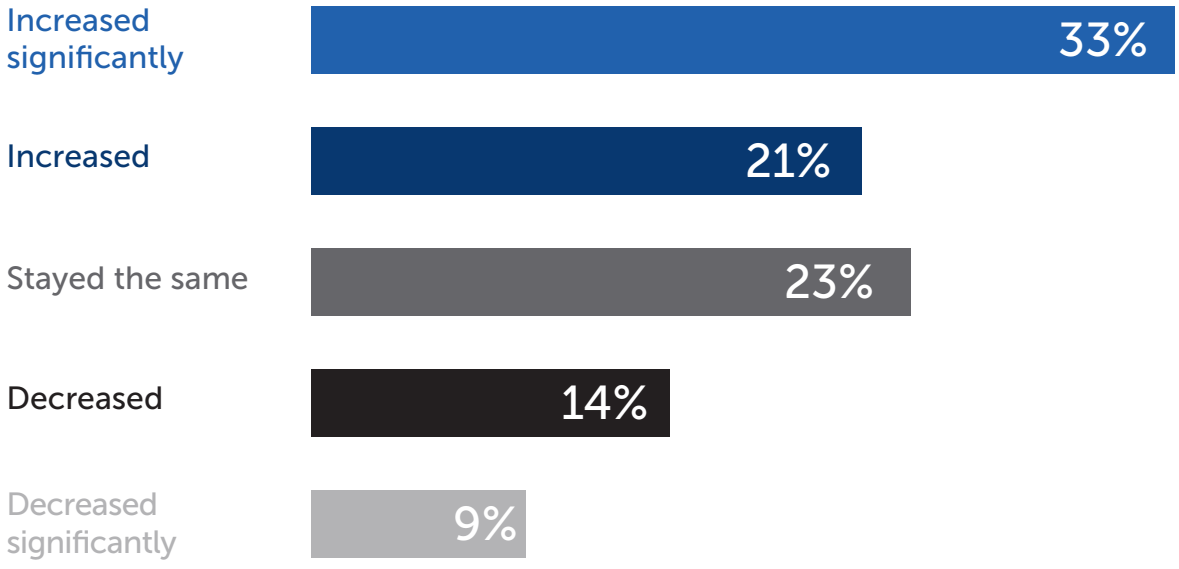


KEY FINDING 2

Patching Problems Are Not Going Away

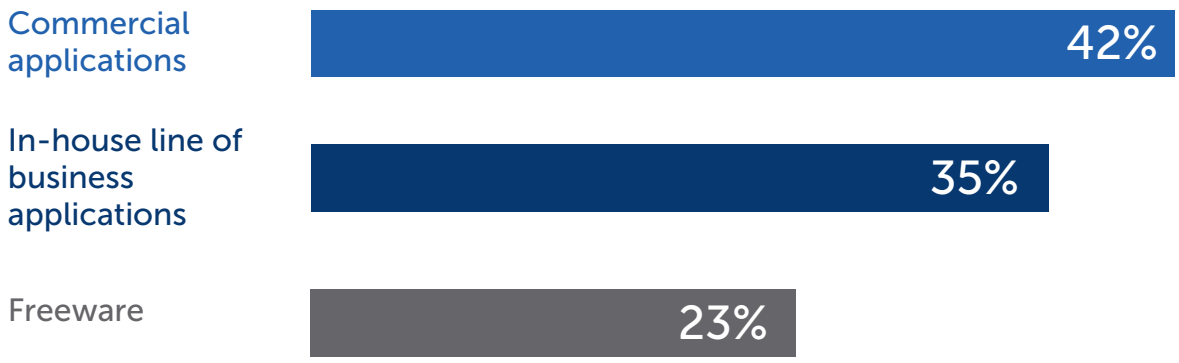
An increase in the number of applications means that the volume of patches will continue to grow. As shown in Figure 4, 54 percent of respondents say the number of applications increased significantly or increased in the past two years.

Figure 4. How has the number of applications changed in the past two years?



Organizations lack confidence in the ability to comply with current patch SLAs. Only 40 percent of respondents measure compliance with application patching SLAs. Of these respondents, only 22 percent rate their organizations' confidence in their ability to comply with current patch SLAs as high or very high. As shown in Figure 5, commercial applications and in-house line of business applications are most often tracked.

Figure 5. What types of applications must your organization track to comply with its SLAs?



An average of 60 percent of tracked applications are out of compliance because they are not at an approved version that meets SLAs. As shown in Figure 6, compliance with SLAs is at risk because of application version problems. An average of less than half of tracked applications are on the latest version and only 41 percent are on an approved version that meets SLAs.

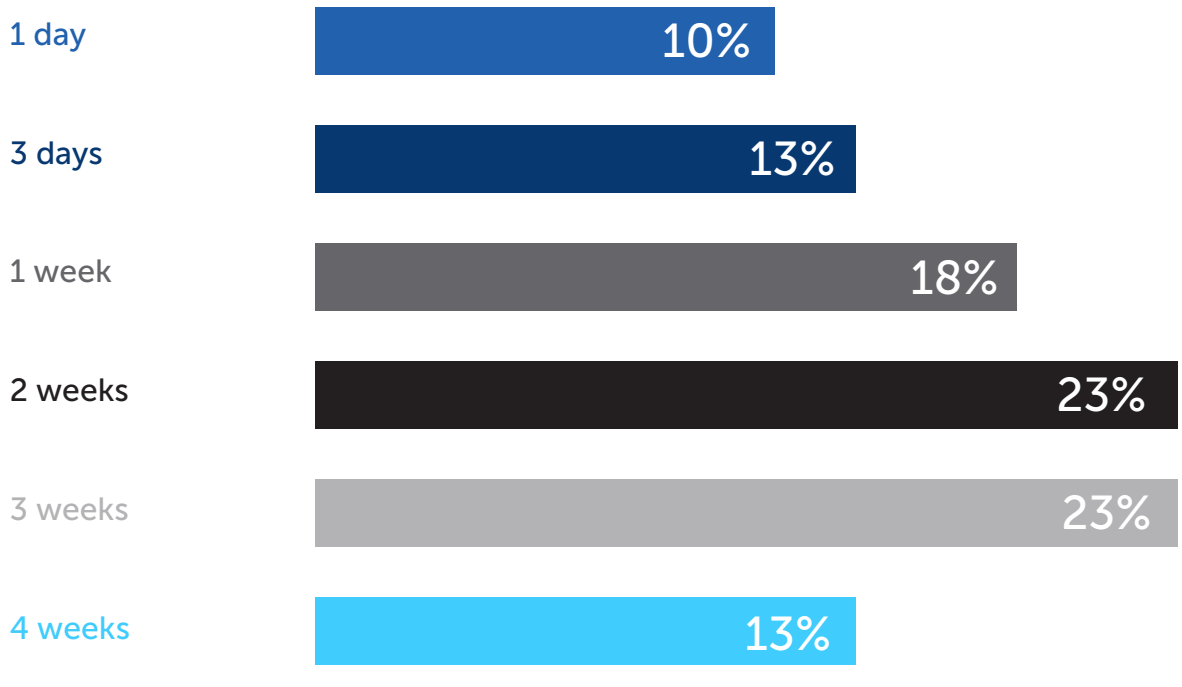
Figure 6. Percentage of applications that are on the latest version and at the approved version to meet your organization's SLAs. Extrapolated values presented

KEY FINDING 3

Time is the Enemy of a Successful Patching Strategy in a Digital Workplace

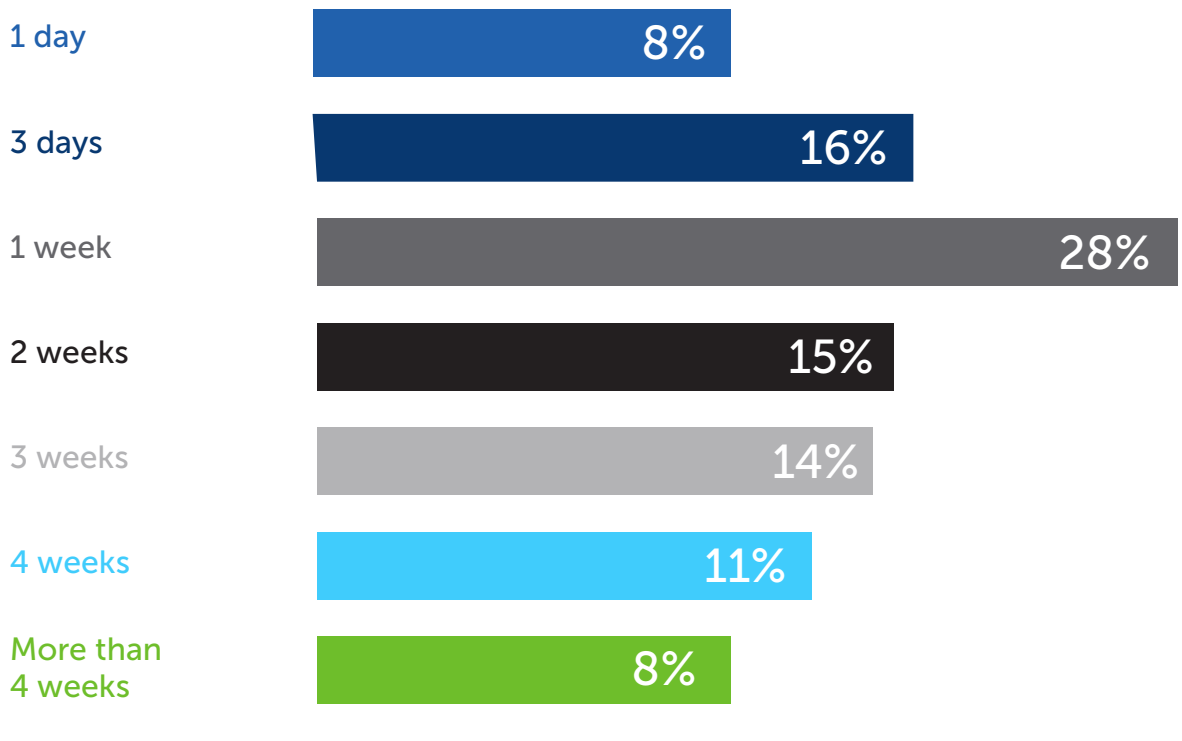
Patch deployment after release by the manufacturer can take as long as two weeks. According to Figure 7, 59 percent of respondents say it takes an average of two weeks or more to deploy a patch once it is released by the manufacturer. It can take an average of 12 hours to determine when an update is deployed.

Figure 7. How long does it take to begin a patch deployment after one is released by the manufacturer?



Almost half of respondents (48 percent) say it can take at least two weeks for a patch to be deployed across the entire organization, as shown in Figure 8.

Figure 8. How much time does it take for a patch to be deployed across the entire organization?



KEY FINDING 3

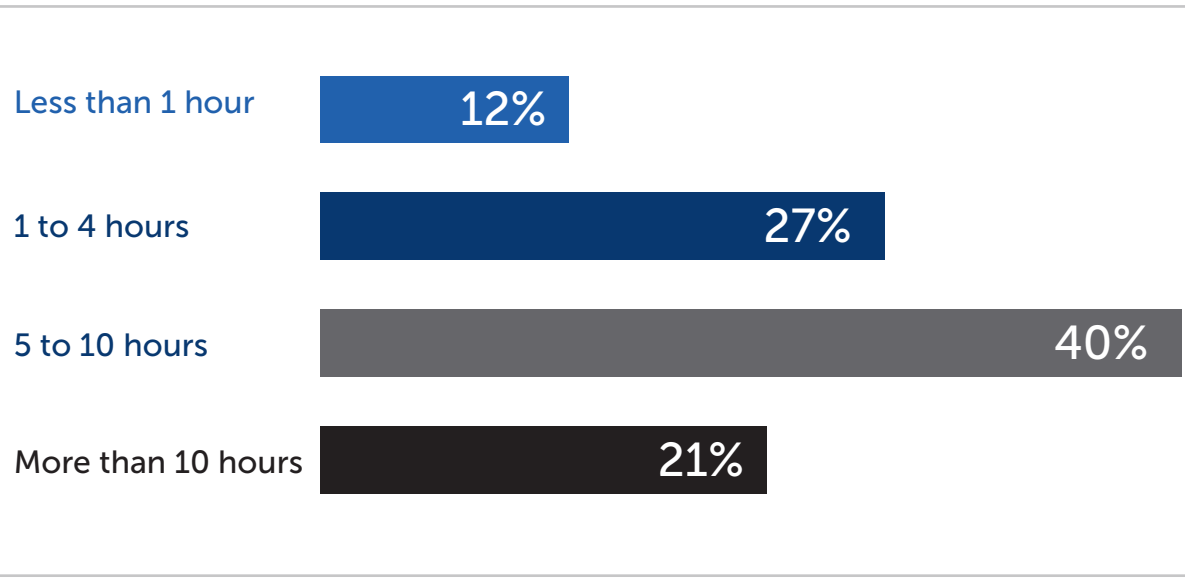
Time is the Enemy of a Successful Patching Strategy in a Digital Workplace

Patch deployment delays are opportunities for hackers. As shown in Figure 9, an average of 10 hours to more than 25 hours is spent deploying patches weekly, according to 65 percent of respondents.

Figure 9. How much total time is spent deploying patches weekly?

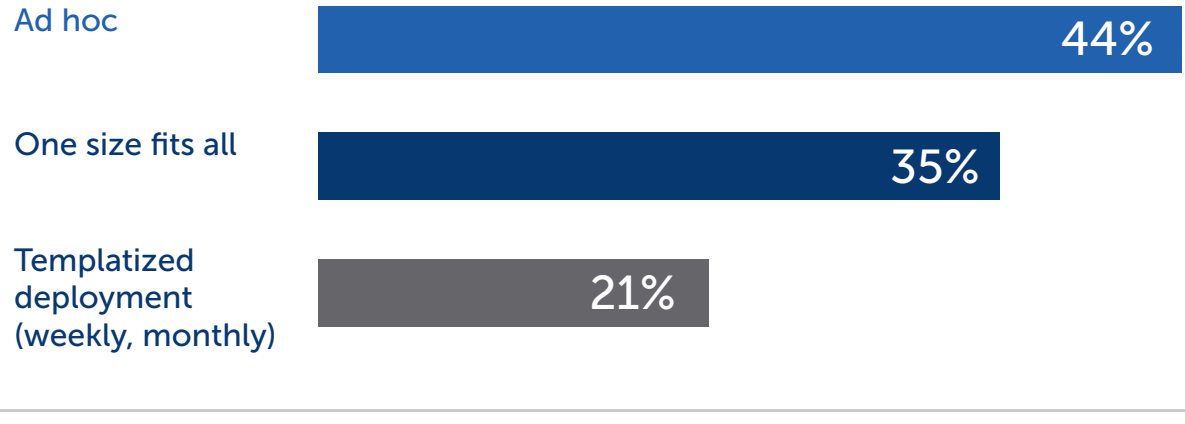
It takes at least 5 hours and can take more than 10 hours to remediate a broken or failed patch. As shown in Figure 10, only 39 percent of respondents say they can remediate a broken or failed patch in less than 4 hours.

Figure 10. How quickly can your organization remediate a broken or failed patch?



Patch deployment is ad hoc. According to Figure 11, 44 percent of respondents say scheduling patch deployment is mostly ad hoc. Only 21 percent say it is on a regular schedule applying templatized deployment.

Figure 11. How do you schedule patch deployment?

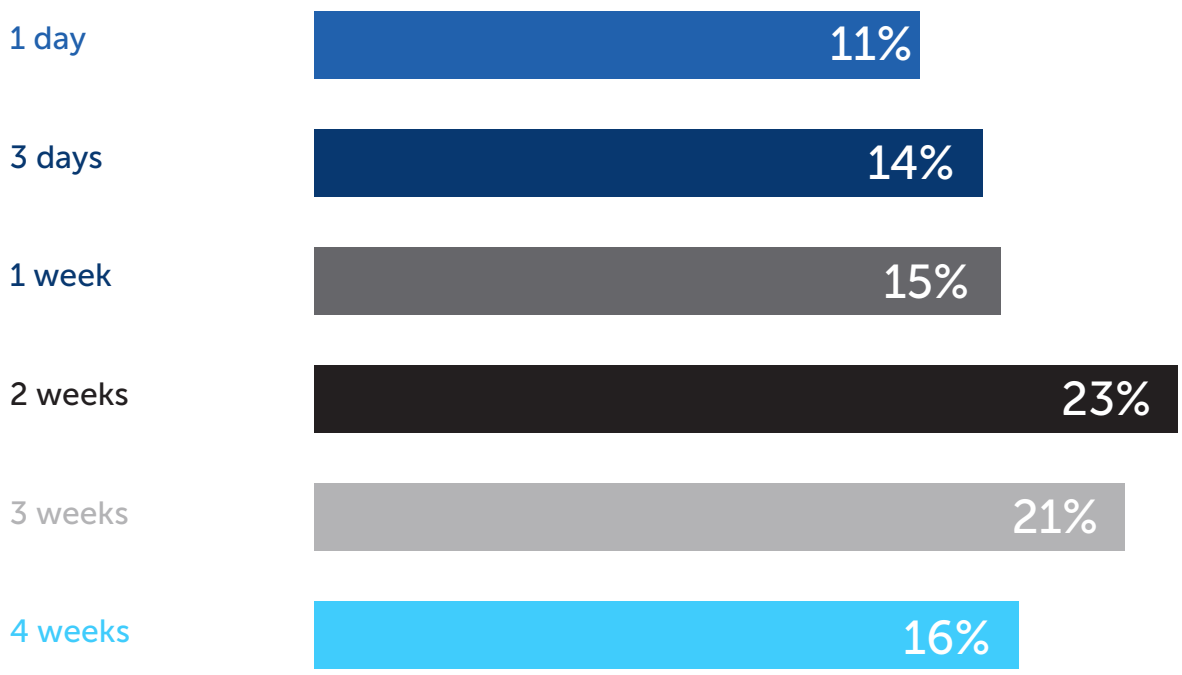


KEY FINDING 3

Time is the Enemy of a Successful Patching Strategy in a Digital Workplace

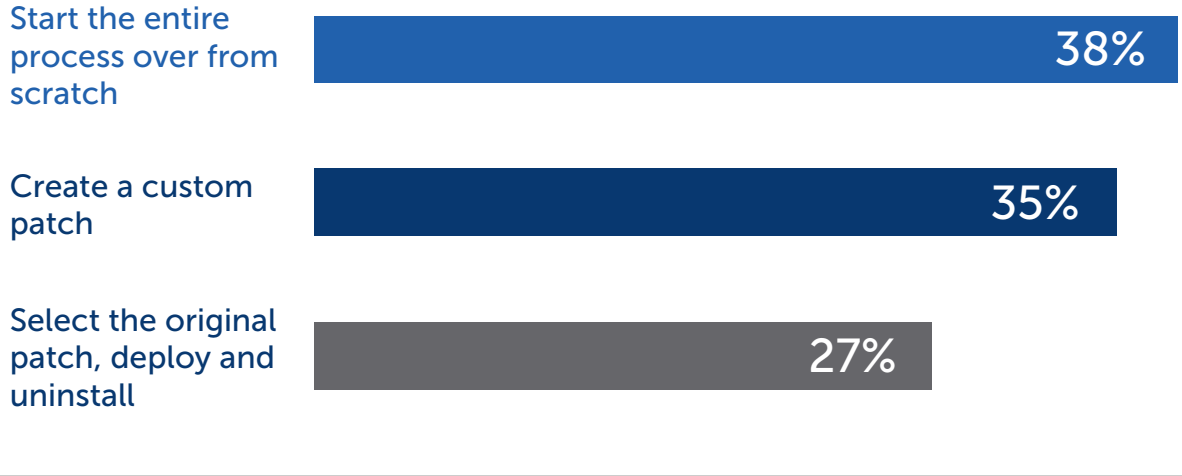
Sixty percent of respondents say it takes a minimum of two weeks to achieve the secure installation percentage for a zero-day patch, according to Figure 12.

Figure 12. How much time is spent achieving the secure installation percentage for a zero-day patch?



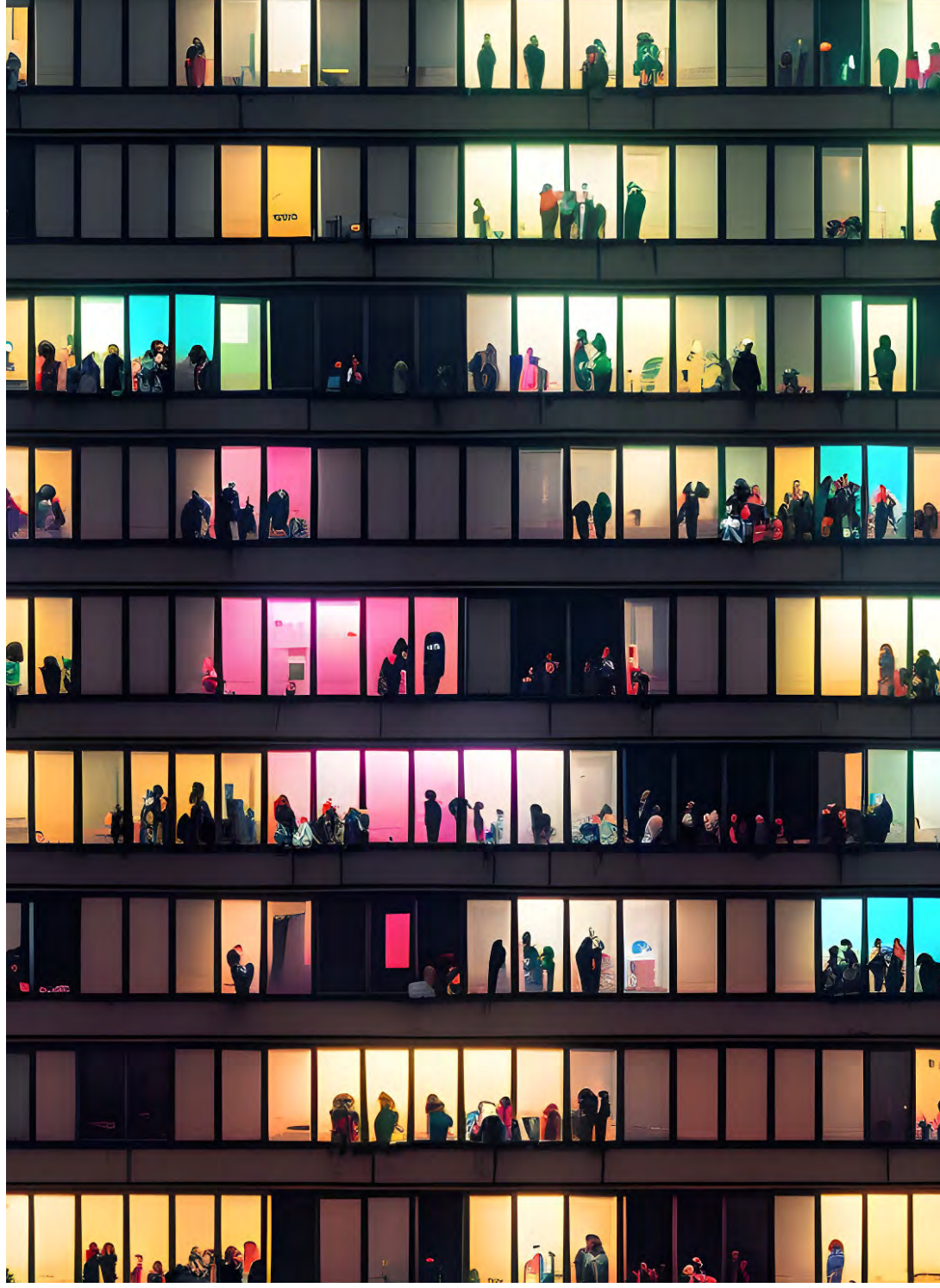
When patches are broken or fail, organizations lack a sophisticated approach for rolling them back. According to Figure 13, 38 percent of respondents say they start the entire process over from scratch. According to the research, a significant amount of time is spent deploying patches. When organizations have a patch that needs to be reapplied, this can add significant additional time to the patching process.

Figure 13. How do you handle rolling back a patch that has been applied?



CONCLUSION

The State of Patch Management in the Digital Workplace



Application proliferation has become unruly over the years making device patching a frustrating game of Tetris with real-world consequences. There are no winners and losing is just a matter of time. Patching devices remains one of the most important and effective measures for IT and security to protect a digital workplace and its assets – but as the respondents to this study reported, it remains one of the most laborious and difficult parts of their job.

Patching devices remains one of the most important and effective measures for IT and security to protect a digital workplace and its assets.

Most respondents rely on traditional endpoint management for patching, whether that be SCCM (47%) or some other conventional software distribution solution (51%). This software represents the backbone of how many large organizations keep track of and manage their devices. However, these legacy tools are plagued with fundamental problems in visibility, software deployment, and process management. We know because we've been helping the world's largest organizations solve those problems leveraging our platform and applications for nearly two decades. The only way to solve the patching problem is with a truly modern approach.

Shifting to a modern methodology in patching devices and managing endpoints will quickly alleviate the problems of visibility and deployment in Patch Management. Modern management allows for seamless delivery of patches and quick updates to any device, anywhere in the world. This is important in the digital workplace era, where the delivery of patches can be a challenge due to their size and potential impact on network and system resources. Utilizing edge computing technologies that include peer-to-peer, predictive bandwidth harvesting, and memory pipeline architectures will allow content and software to move around freely without worrying about network limitations, disk storage, or device impact.

While many organizations may be looking to automate their way out of the patching problem, the reality is most software vendors offer only simple automation tricks that don't meet the complex needs of delivering the amount of software, to the number of devices, that an enterprise organization uses to run their business. Set your sets one step further – Autonomous. A modern endpoint management approach comes with the promise of autonomy. The goal of patch management, and endpoint management in the broader context, should not just be less human intervention. It should be non-human.

Extreme automation must completely eliminate the manual effort typically required for patching software to be autonomous. Traditional patching processes involve multiple steps including download, approvals, roll out, and troubleshooting issues. An autonomous solution allows for comprehensive modeling of both business environment and processes and can be tailored to fit a wide range of requirements. It operates using a "fire and forget" model, meaning that once it is configured the autonomous system will handle patch deployment consistently and without further intervention.

Adaptiva Autonomous Patch is the pioneering product that makes this possible and is now generally available.

The goal of patch management, and endpoint management in the broader context, should not just be less human intervention. It should be non-human.

PART III
Methodology

A sampling frame of 16,865 IT and IT security practitioners in the United States who are involved and influential in their organizations' patch management strategy were selected as participants to this survey. Table 1 shows 731 total returns. Screening and reliability checks required the removal of 68 surveys. Our final sample consisted of 663 surveys or a 3.9 percent response.

Survey Response	Frequency	Percent
Sampling frame	16,865	100%
Total returns	731	4.3%
Rejected or screened surveys	68	0.4%
Final sample	663	3.9%

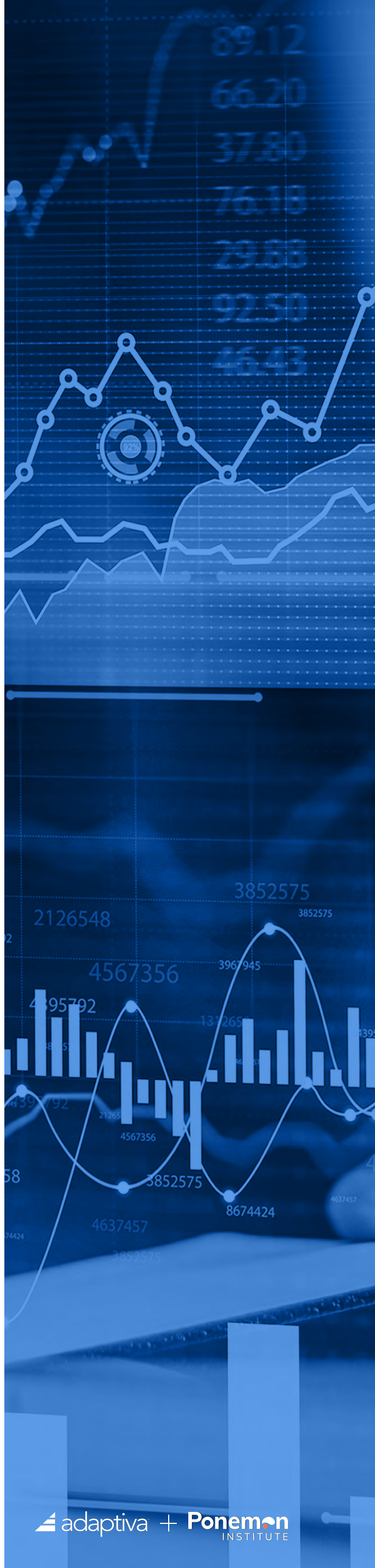


Figure 18. Current Position Within the Organization

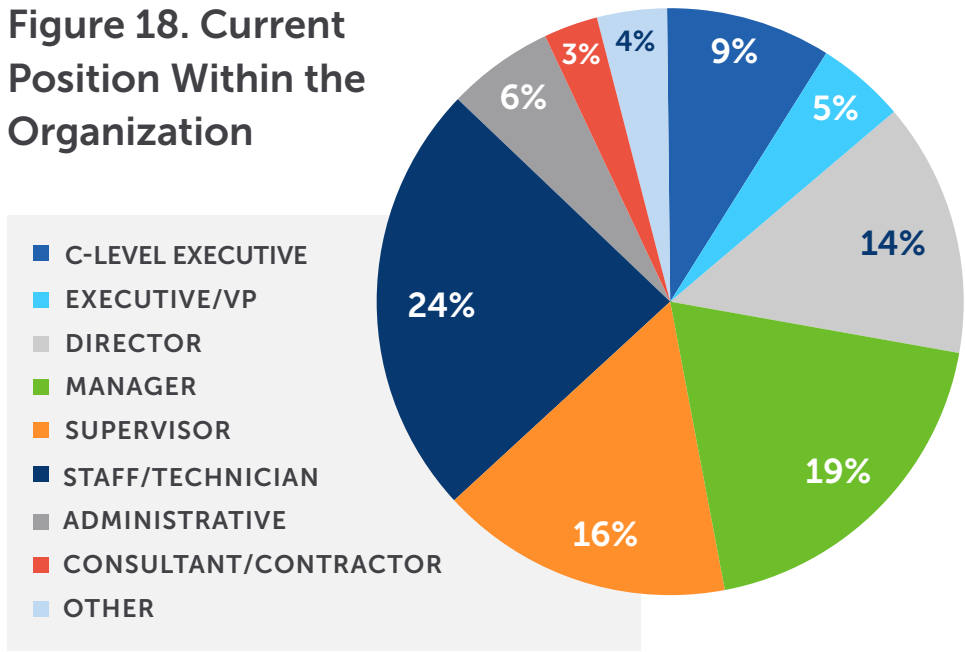
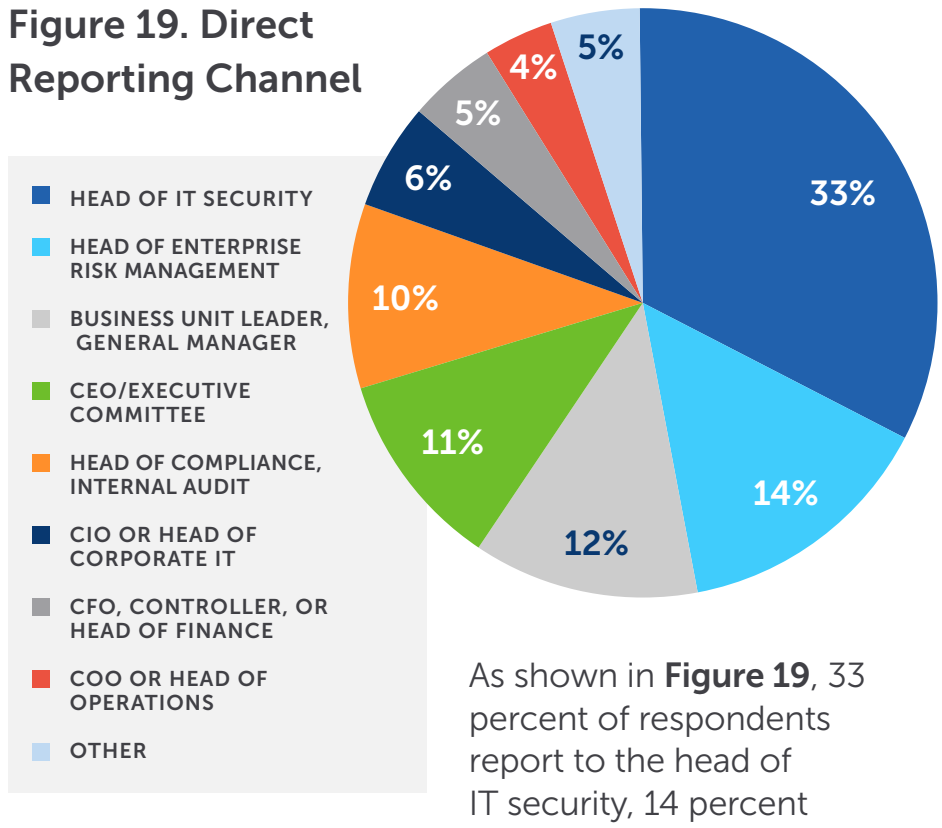


Figure 18 reports the respondent's organizational level within participating organizations. By design, more than half (63 percent) of respondents are at or above the supervisory levels. The largest category at 24 percent of respondents is staff/technician.

Figure 19. Direct Reporting Channel



As shown in **Figure 19**, 33 percent of respondents report to the head of IT security, 14 percent of respondents report to the head of enterprise risk management, 12 percent of respondents report to the business unit leader or general manager, 11 percent of respondents report to the CEO/executive committee and 10 percent of respondents report to the head of compliance or internal audit.

Figure 20. Current Position Within the Organization

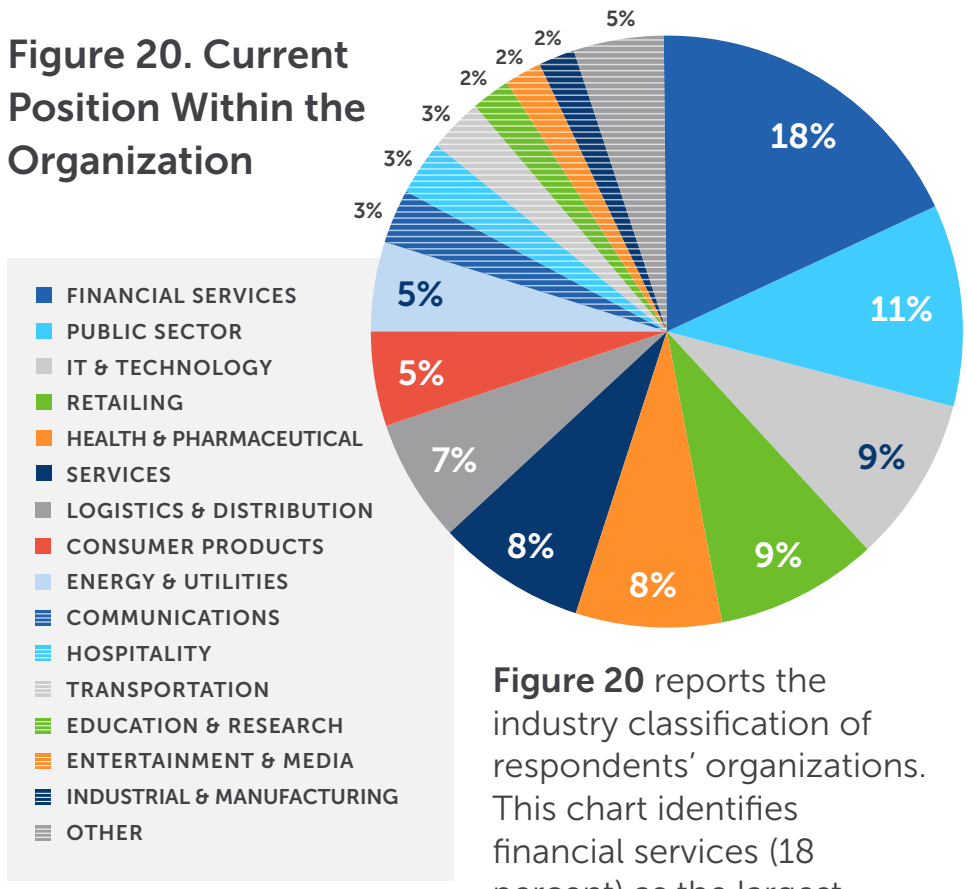
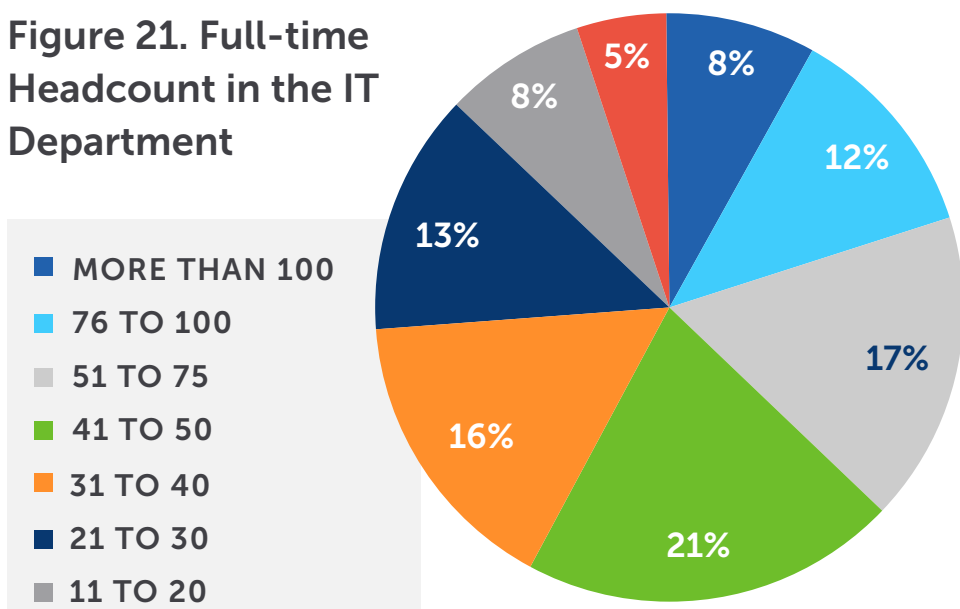


Figure 20 reports the industry classification of respondents' organizations. This chart identifies financial services (18 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by public sector (11 percent of respondents), IT and technology (9 percent of respondents), health and pharmaceuticals (8 percent of respondents), and services (8 percent of respondents).

Figure 21. Full-time Headcount in the IT Department



As shown in **Figure 21**, 59 percent of respondents are from organizations with a global headcount of more than 5,000 employees.

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.

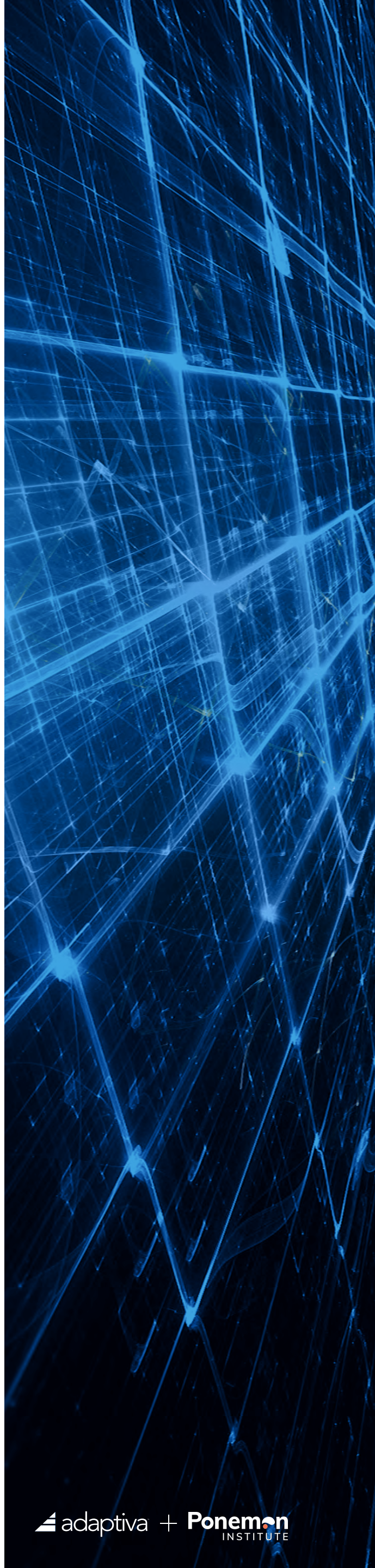
Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are involved and influential in their organization's endpoint management strategy. We also acknowledge that the results may be biased by external events such as media 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	16,865
Survey returns	731
Rejected surveys	68
Final sample	663
Response rate	3.9%



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	29%
Involvement and influence in our organization's endpoint management strategy	36%
Some involvement and influence in our organization's endpoint management strategy	35%
Total	100%

S2. What is your organization's headcount?

Less than 1,000 (stop)	0%
1,000 to 2,500	7%
2,501 to 5,000	13%
5,001 to 10,000	18%
10,001 to 25,000	20%
25,001 to 50,000	19%
50,000 to 75,000	11%
75,001 to 100,000	8%
More than 100,000	4%
Total	100%
Extrapolated value	30,405

Part 2. Application Visibility

Q1. Does your organization know approximately how many distinct applications are installed on endpoint devices?

Yes	31%
No (please skip to Q3)	69%
Total	100%

Q2. Approximately, how many applications does your organization have installed on endpoint devices today?

Less than 50	2%
50 to 100	5%
101 to 500	9%
501 to 1,000	10%
1,001 to 2,500	16%
2,501 to 5,000	27%
More than 5,000	31%
Total	100%
Extrapolated value	2,908

Part 2. Application Visibility

Q3. How has the number of applications changed in the past two years?

Increased significantly	33%
Increased	21%
Stayed the same	23%
Decreased	14%
Decreased significantly	9%
Total	100%

Q4. What steps are taken to gain visibility over all applications in use across your organization? Please select all that apply.

Vulnerability scanning tools	67%
Inventory tools	55%
Antivurs/Malware scanning tools	71%
Other (please specify)	7%
Total	200%

Q5. Do you measure compliance with application patching SLAs?

Yes	40%
No (Please skip to Q10)	60%
Total	100%

Q6. Using the following 10-point scale, please rate your organization's confidence in it is ability to comply with current patch SLAs from 1 = low confidence to 10 = high confidence.

1 or 2	32%
3 or 4	30%
5 or 6	16%
7 or 8	13%
9 or 10	9%
Total	100%

Q7. What types of applications must your organization track to comply with its SLAs? Please select all that apply.

Freeware	23%
Commercial applications	42%
In-house line of business applications	35%
Total	100%

Part 2. Application Visibility

Q8. Of the applications tracked, what percentage are on the latest version?

Less than 25 percent	23%
25 percent to 50 percent	27%
51 percent to 75 percent	31%
76 percent to 100 percent	19%
Total	100%
Extrapolated value	49.4%

Q9. What percentage of tracked applications are at the approved version and meet your organization's SLAs?

Less than 10 percent	6%
10 percent to 15 percent	11%
16 percent to 25 percent	23%
26 percent to 50 percent	21%
50 percent to 75 percent	30%
76 percent to 100 percent	9%
Total	100%
Extrapolated value	41.2%

Part 3. Patch Distribution and Deployment

Q10. What is the hardest part of the patching process? Please select 3 top choices

Keeping up the volume of patches	18%
Detection of vulnerabilities	54%
Installation	29%
Reboot/uninstall requirements	37%
Testing	38%
Deployment	37%
Risk and exposure	50%
User-based install vs. system-based install	37%
Total	300%

Part 3. Patch Distribution and Deployment

Q11a. Low bandwidth makes patching more difficult.

Strongly agree	34%
Agree	22%
Unsure	21%
Disagree	18%
Strongly disagree	5%
Total	100%

11b. Different application types make patching more difficult (e.g., browser add-ons, marketplace applications, MSI-based, AppX-based, exe-based, drivers/firmware).

Strongly agree	26%
Agree	21%
Unsure	18%
Disagree	21%
Strongly disagree	14%
Total	100%

Q12. Following deployment of a patch, certain applications can wreak havoc.

Strongly agree	23%
Agree	19%
Unsure	27%
Disagree	15%
Strongly disagree	16%
Total	100%

Q13. No matter how large our IT team is, 100 percent patching of applications is not possible.

Strongly agree	20%
Agree	25%
Unsure	24%
Disagree	21%
Strongly disagree	10%
Total	100%

Q14. After a patch has been deployed, I can quickly confirm it has been installed on the appropriate devices.

Strongly agree	14%
Agree	20%
Unsure	16%
Disagree	30%
Strongly disagree	20%
Total	100%

Q15. How quickly do you know when an update is deployed within your organization?

Less than 1 hour	10%
1 to 5 hours	19%
6 to 10 hours	25%
10 to 20 hours	23%
More than 20 hours	23%
Total	100%
Extrapolated value (hours)	12

Part 3. Patch Distribution and Deployment

Q16. What are the two hardest applications to patch? Please select two choices only.

Freeware	78%
Commercial applications	59%
In-house line of business applications	63%
Total	200%

Q17. How long does it take to begin a patch deployment after one is released by the manufacturer?

1 day	10%
3 days	13%
1 week	18%
2 weeks	23%
3 weeks	23%
4 weeks	13%
Total	100%

Q18. How do you schedule patch deployment? Please select one choice only.

Templatized deployment (weekly, monthly)	21%
Ad hoc	44%
One size fits all	35%
Total	100%

Q19. Following deployment, how long does it take to achieve the secure installation percentage for a zero-day patch (i.e. percentage of approved and updated devices that meet your organization's SLAs for a zero-day patch)?

1 day	11%
3 days	14%
1 week	15%
2 weeks	23%
3 weeks	21%
4 weeks	16%
Total	100%

Q20. How long does it take for a patch to be deployed across the entire organization?

1 day	8%
3 days	16%
1 week	28%
2 weeks	15%
3 weeks	14%
4 weeks	11%
More than 4 weeks	8%
Total	100%

Q21. How much total time is spent deploying patches weekly?

Less than 10 hours	35%
10 to 25 hours	39%
More than 25 hours	26%
Total	100%

Part 3. Patch Distribution and Deployment

Q22. How quickly can your organization remediate a broken or failed patch?

Less than 1 hour	12%
1 to 4 hours	27%
5 to 10 hours	40%
More than 10 hours	21%
Total	100%

Q23. How do you handle rolling back a patch that has been applied? Please select one choice only.

Select the original patch, deploy and uninstall	27%
Create a custom patch	35%
Start the entire process over from scratch	38%
Total	100%

Q24a. Does your organization have unique processes for deploying patches based on different characteristics such as business unit, function, geographic location, device type, type of users and risk and exposure?

Yes	56%
No (please skip to Q25)	44%
Total	100%

Q24b. If yes, which characteristics are used to create unique patching strategies and processes? Please select all that apply.

Business unit	53%
Function	68%
Geographic location	37%
Device type	45%
User	38%
Risk	62%
Exposure	31%
Total	334%

Q25. Who decides when a patch should be distributed? Please select one choice only.

Application owner	25%
IT operations	19%
IT security	24%
CSIRT team	23%
Engineering	9%
Total	100%

Q26. How does your organization distribute patches? Please select all that apply.

ConfigMgr/SCCM/MEM/Intune	47%
Generic software distribution tool	51%
AD	34%
Manual	23%
Third-party automation vendor	45%
Total	200%

Part 3. Patch Distribution and Deployment

Q27. What percentage of application patches are distributed using automation?

Less than 10%	27%
10% to 25%	31%
26% to 50%	19%
51% to 75%	11%
76% to 100%	12%
Total	100%
Extrapolated value	31.6%

Q28. How many people in your IT team are directly involved in the patching process?

1 to 3	3%
4 to 6	9%
7 to 10	11%
11 to 15	23%
16 to 20	23%
21 to 50	25%
More than 50	6%
Total	100%
Extrapolated value	20.93

D1. What best describes your position level within the organization?

C-level executive	9%
Executive/VP	5%
Director	14%
Manager	19%
Supervisor	16%
Staff/technician	24%
Administrative	6%
Consultant/contractor	3%
Other (please specify)	4%
Total	100%

D2. What best describes your reporting channel or chain of command?

CEO/executive committee	11%
COO or head of operations	4%
CFO, controller or head of finance	5%
CIO or head of corporate IT	6%
Business unit leader or general manager	12%
Head of compliance or internal audit	10%
Head of enterprise risk management	14%
Head of IT security	33%
Other (please specify)	5%
Total	100%

Part 4. Organizational Demographics

D1. What best describes your position level within the organization?

C-level executive	9%
Executive/VP	5%
Director	14%
Manager	19%
Supervisor	16%
Staff/technician	24%
Administrative	6%
Consultant/contractor	3%
Other (please specify)	4%
Total	100%

D2. What best describes your reporting channel or chain of command?

CEO/executive committee	11%
COO or head of operations	4%
CFO, controller or head of finance	5%
CIO or head of corporate IT	6%
Business unit leader or general manager	12%
Head of compliance or internal audit	10%
Head of enterprise risk management	14%
Head of IT security	33%
Other (please specify)	5%
Total	100%

D3. What best describes your organization's primary industry classification?

Agriculture & food services	0%
Communications	3%
Consumer products	5%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	5%
Entertainment & media	2%
Financial services	18%
Health & pharmaceutical	8%
Hospitality	3%
Industrial & manufacturing	2%
IT & technology	9%
Logistics & distribution	7%
Public sector	11%
Retailing	9%
Services	8%
Transportation	3%
Other (please specify)	4%
Total	100%

THANK YOU

adaptiva + Ponemon INSTITUTE