adaptiva | DEMAND METRIC

# The State of Patch Management

## 2025 REPORT

# Table of Contents

# Introduction

Enterprise businesses face significant challenges managing and securing company devices. The traditional manual approach to endpoint management is proving inadequate, leading to inefficiencies, security vulnerabilities, and compliance risks.

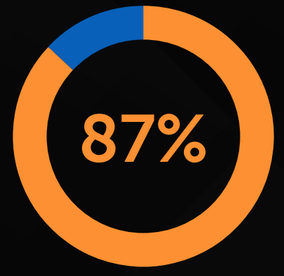
To stay competitive, enterprises must adopt automation-driven solutions that accelerate endpoint management and security, and the need for an adaptive platform for endpoint management has become critical. Autonomous solutions are revolutionizing endpoint management, allowing companies to maintain secure, compliant, and efficiently managed devices without burdening their security or IT teams. Many organizations have already embraced this technology, reaping the benefits of autonomous endpoint management.

Achieving a level of sophistication where technology responds proactively to changing risk and network conditions doesn't have to be complicated but requires organizations to transition from manual processes to automated, adaptive, and autonomous solutions.

Adaptiva and Demand Metric recently partnered to understand the value of automation in patch management within the enterprise and the impact of advanced adoption. The following report shares crucial insights from more than 250 security and IT professionals into the state of patch management at enterprise organizations. **This model can help IT and Security professionals enhance speed, control, and reliability in their patching strategies.**

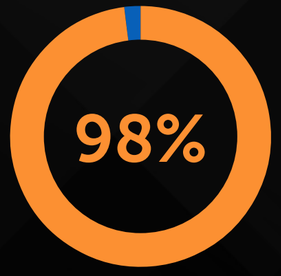
# Key Findings

### Third Party Risk



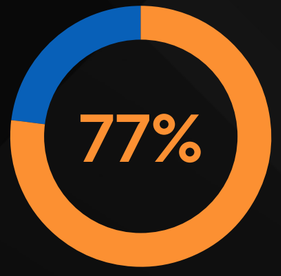

of organizations have had third-party applications with vulnerabilities that made patching a necessity.

### Manual Patching



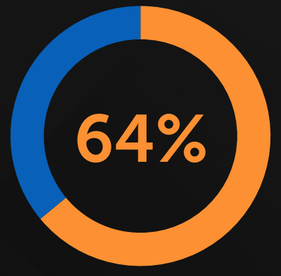

of IT and Security pros say patching disrupts their work, forcing them to reallocate resources.

### Slow Remediation



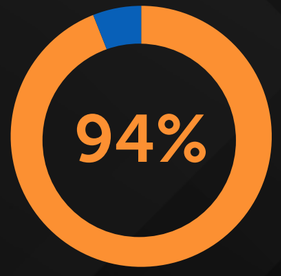

of organizations need more than a week to deploy patches.

### Collaboration Issues




say coordination between detection and remediation is their biggest challenge.

### Automation Adoption




of organizations are automating, or plan to automate, patch distribution within the next year.

***Fifty-one percent say patching is now a bigger issue than vulnerability detection.***

# The Current State of Patch Management

As vulnerabilities in third-party applications and operating systems continue to pose significant risks, patch management has become critical to maintaining enterprise security and operational integrity.

However, as the number of patches increases, managing and deploying patches has become more complex and resource-intensive, impacting productivity and exposing companies to unnecessary risks.

**This section reviews the latest patch management findings and the challenges organizations face today.**

# Patching Vulnerabilities in Third-Party Applications

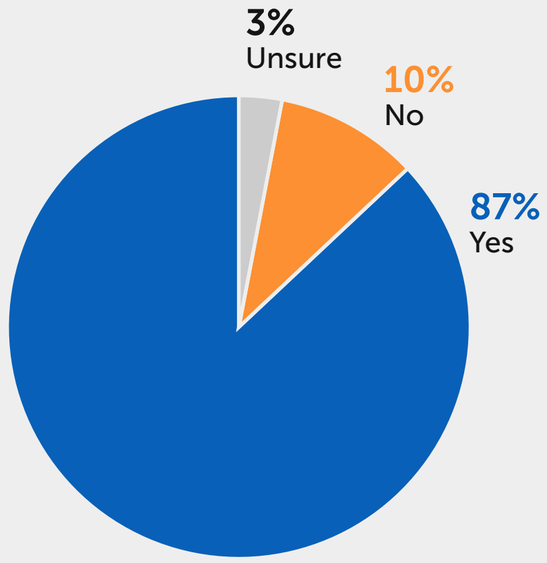
The reliance on third-party applications has significantly contributed to the patching burden in enterprise environments.

**In the past year, 87% of organizations reported encountering vulnerabilities in third-party applications, necessitating the patching process.**

The frequency of these vulnerabilities underscores the importance of having a robust patch management strategy, as delays in patching can expose organizations to severe security risks.

Figure 1

Have you encountered situations where third-party applications used in your organization had vulnerabilities that require patching in the past year?



# Impact on Resources, Productivity, and Liability

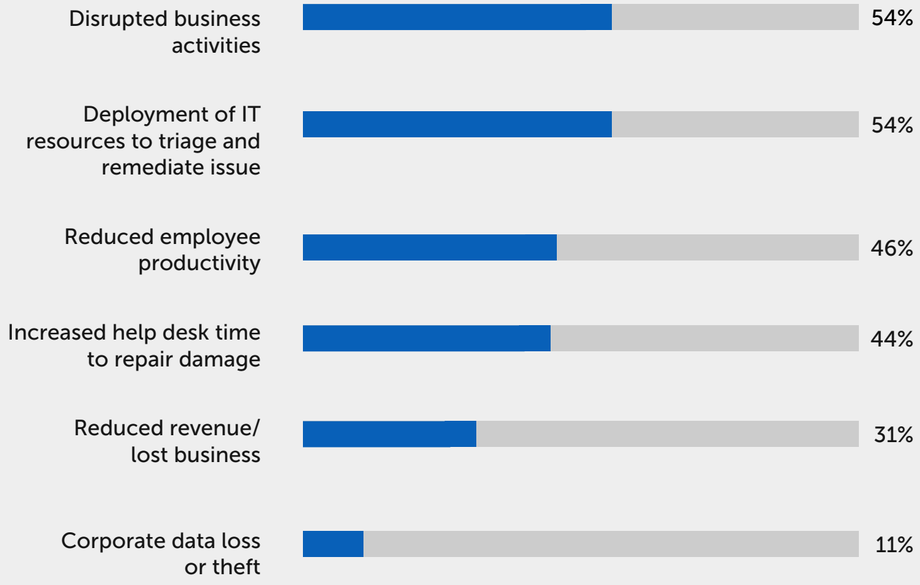
The consequences of unpatched vulnerabilities extend beyond security risks. According to this study's participants, IT security incidents caused by delayed or incomplete patching efforts impact resources, productivity, and revenue while creating unnecessary legal liabilities.

**In the past year, more than half of security and IT professionals report that these incidents have disrupted business activities, forcing organizations to reallocate resources to triage and remediate issues.**

This leads to significant operational inefficiencies as IT teams are pulled away from their primary responsibilities to manage emergencies and to provide support, as shown in **Figure 2**.

Figure 2

What negative impact have IT security incidents had on your company in the past 12 months? Check all that apply.



# The Complexity of Patch Customization

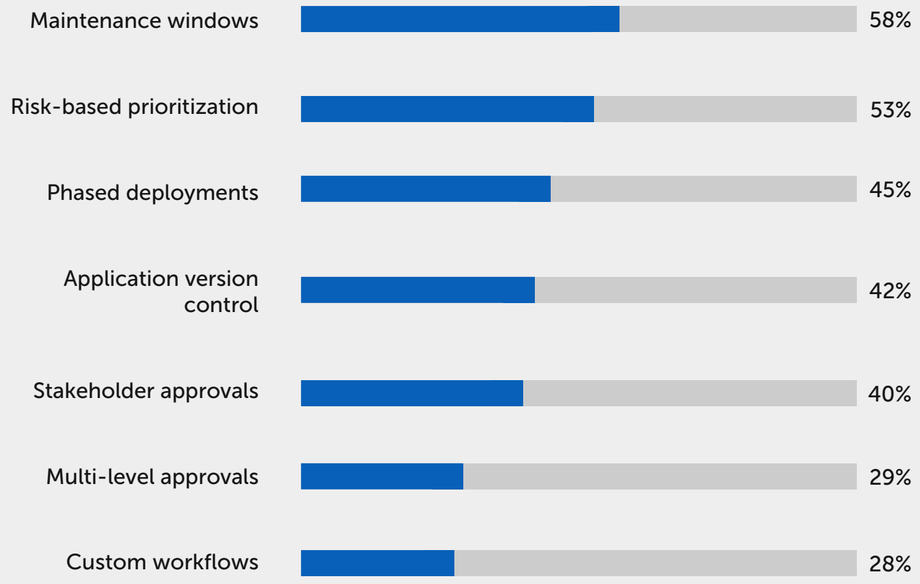
**The growing complexity of organizational IT infrastructures has made it increasingly difficult to implement a one-size-fits-all patching approach.**

Enterprises require customized patching options to meet specific operational needs, including considerations for maintenance windows and risk-based prioritization, as **Figure 3** shows.

Tailoring patches to the business's needs often involves determining the optimal time for deployment to avoid disrupting critical systems and assessing the relative risk posed by different vulnerabilities to prioritize appropriately.

Figure 3

What patching customization options does your organization require to meet organizational needs?



# Collaboration Between IT and Security Teams

Patch management is no longer the sole responsibility of IT teams. A collaborative effort between IT and security teams is required to track compliance, prioritize and deploy patches effectively, and report on remediation.

**64% agree their biggest impediment is coordinating vulnerability detection with remediation.**

More than half (51%) of respondents say that patching has become a bigger issue than detection and more than 75% indicate that both IT and security must approve patches before deployment. This increased collaboration is necessary to ensure that patches are applied to minimize security risks without compromising operational needs.

Table 1

Please rate the following statements based on how strongly you agree/disagree:

| | Agree | Neutral | Disagree |
|---|---|---|---|
| Patching has become a bigger issue than detection. | **51%** | **28%** | **21%** |
| Our biggest impediment is coordinating vulnerability prioritization/detection with the IT processes that remediate them. | **64%** | **27%** | **9%** |
| Our patch deployment is on par with our peers. | **72%** | **21%** | **7%** |
| We have a standard process in place to manage patch deployment. | **82%** | **15%** | **3%** |
| Our ability to patch new patches quickly has improved since last year. | **70%** | **23%** | **7%** |
| We share responsibility for prioritizing patches between security and IT teams. | **81%** | **15%** | **4%** |
| We share accountability for vulnerability remediation between security and IT teams. | **80%** | **15%** | **5%** |

# Patching Process Challenges

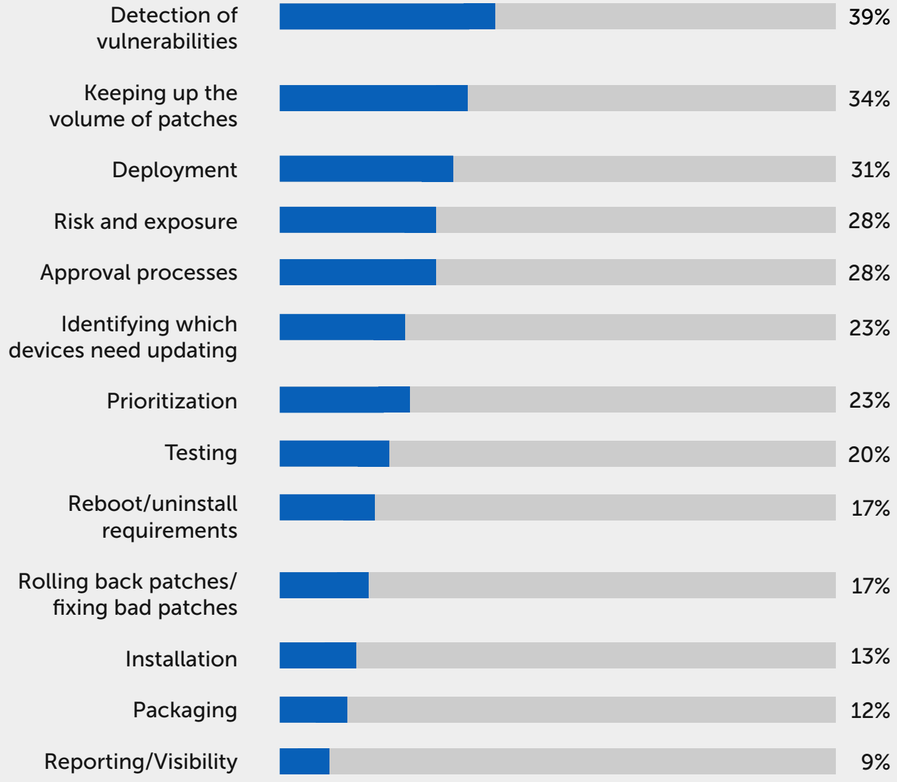
**IT and security professionals face several significant challenges in the patch management process, with the detection of vulnerabilities and keeping up with the volume of patches emerging as the most challenging aspects, as Figure 4 shows.**

Managing the deployment of patches, particularly in balancing risk and exposure, is a close contender, as teams must prioritize patches based on the severity of vulnerabilities while ensuring minimal disruption to business operations. Additionally, the approval processes—which involve coordination between IT, security, change control teams, and sometimes other stakeholders—add another layer of complexity, contributing to delays in deployment and leaving systems exposed for extended periods.

These challenges emphasize the need for streamlined processes, better prioritization, and enhanced team collaboration to manage security risks effectively.

Figure 4

What is the hardest part of the patching process? Please select the top three.



# Stakeholder Influence on the Patching Process

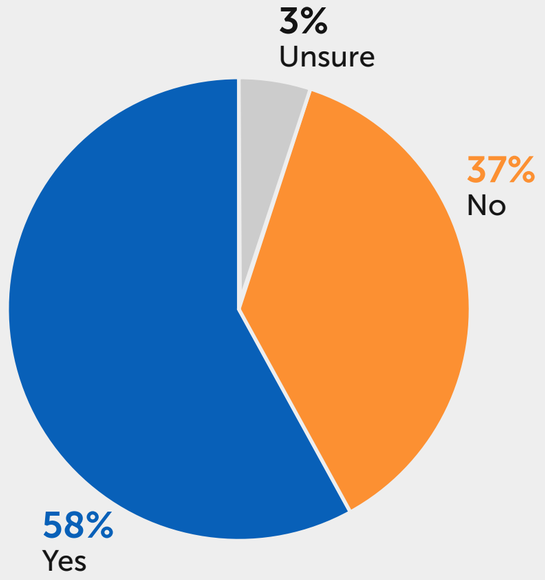
As mentioned, a significant challenge in the patch management process is the involvement of external stakeholders outside the IT and security teams. These stakeholders, who may represent various business units, often have differing priorities and operational concerns that can slow down the timely deployment of patches. This can be particularly problematic when urgent vulnerabilities, which demand immediate attention, need to be addressed quickly.

**According to this study's participants, 58% of security and IT professionals report experiencing delays due to the need for approvals or decisions made by stakeholders, as shown in Figure 5.**

The added layers of approval or input create bottlenecks, increasing the exposure window for potential security breaches and prolonging the patching timeline. Addressing these inefficiencies requires better coordination and streamlined processes to minimize delays and ensure timely patch deployment.

Figure 5

Have you experienced delays in patching process due to involvement or decisions made by stakeholders outside of IT and security teams?



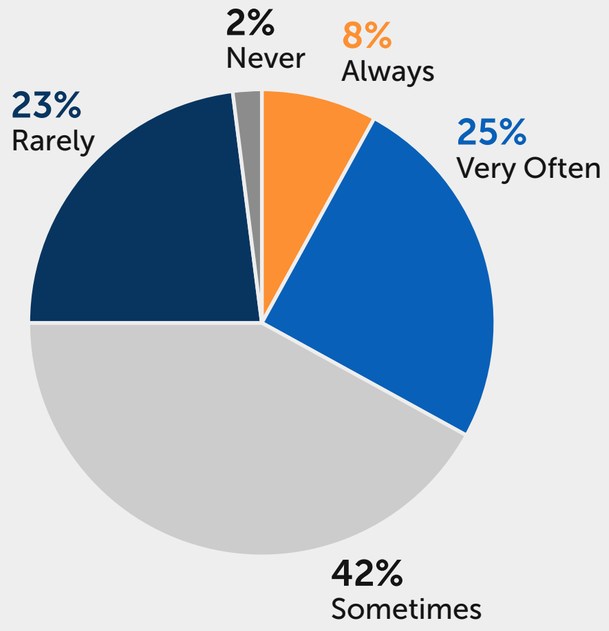
# Hidden Costs of Patch Management Disruptions

**The patch management process can be time-consuming, and 98% of IT and security professionals report that patch deployments disrupt their other job responsibilities – with 33% noting constant interruptions, as Figure 6 shows.**

This disruption often forces teams to delay strategic initiatives or other pressing security tasks, leaving organizations vulnerable to emerging threats. As IT environments become more complex, streamlining patch management becomes essential to reduce teams' workloads, improve efficiency, and maintain a strong security posture without compromising other key responsibilities.

Figure 6

How often do patch deployments and management activities disrupt your other job responsibilities?



# Patch Deployment Approvals

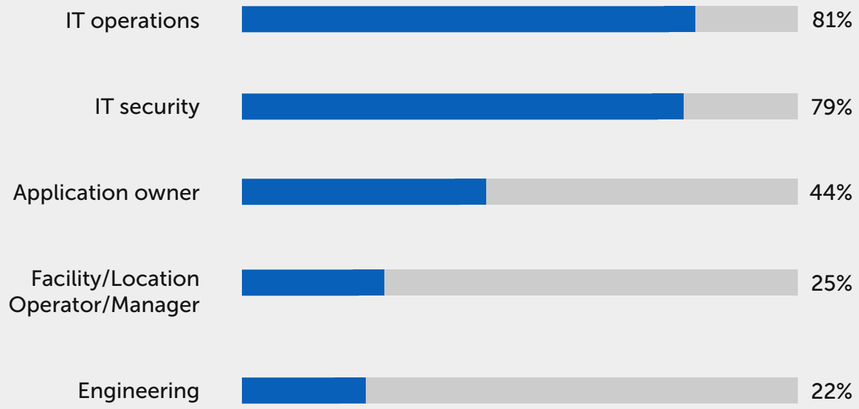
The time required for patch deployment is influenced by the approval process, which can require involvement from other cross-functional stakeholders.

**More than 40% of this study's participants report that application owners must approve patch deployment, as shown in Figure 7.**

The approval process for patch deployment has the potential for significant improvement. Involving application owners and other cross-functional stakeholders is essential to prevent disruptions to business-critical systems. However, reliance on manual approvals outside of an automated system can create bottlenecks and delays that can leave systems vulnerable. Organizations can benefit from streamlining the approval process with integrated approvals built into patching workflows.

Figure 7

Who is required to approve patch deployment?



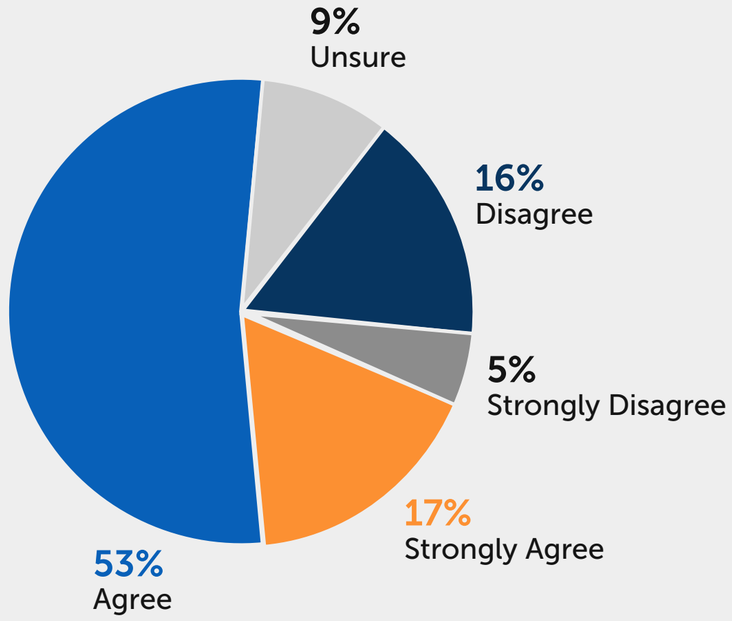
# Network Resource Constraints

**More than two-thirds of IT and security professionals (70%) report that limited network resource bandwidth makes patching more difficult, as Figure 8 shows.**

Low bandwidth in these environments further complicates the process, making it challenging to distribute updates efficiently. IT teams often hesitate to deploy large patches during peak business hours, which could strain already limited bandwidth and disrupt normal operations. As a result, the time it takes to deploy patches can be extended, increasing the window of vulnerability for unpatched systems and exposing the organization to heightened security risks.

Figure 8

Low network resource bandwidth makes patching more difficult.



# IT Involvement in the Patching Process

**For most organizations, patch management remains resource-intensive, demanding considerable IT bandwidth.**

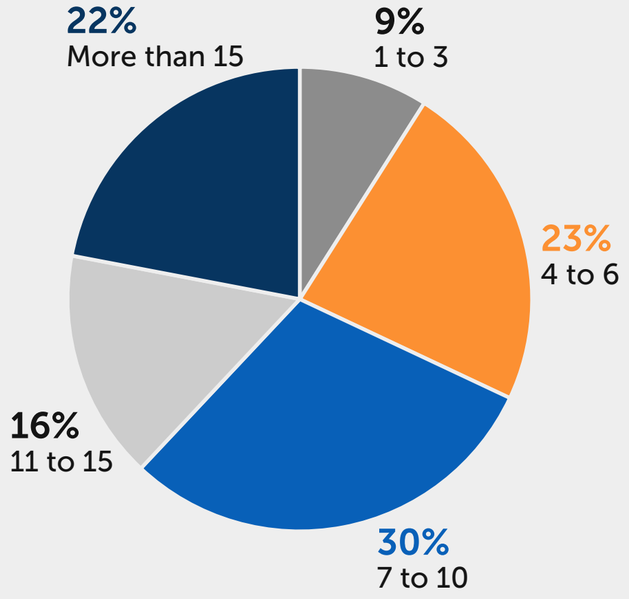
This study shows that fewer than 10% of IT and security professionals report that only 1-3 people are involved in the patching process, while a significant majority—90%—require 4 to 15 or more people, as **Figure 9** shows.

The involvement of a larger team often reflects the complexity of coordinating patch deployments, managing approvals, testing patches, and handling various devices and business units. This high level of resource allocation can slow down patch deployment and increase operational overhead, particularly in environments where automation is limited.

For organizations relying on manual or partially automated processes, the need for a larger team also increases the potential for inefficiencies and delays, as more personnel are required to coordinate and manage the process, leaving less time for them to focus on strategic initiatives.

Figure 9

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



# Enterprise-Wide Patch Deployments

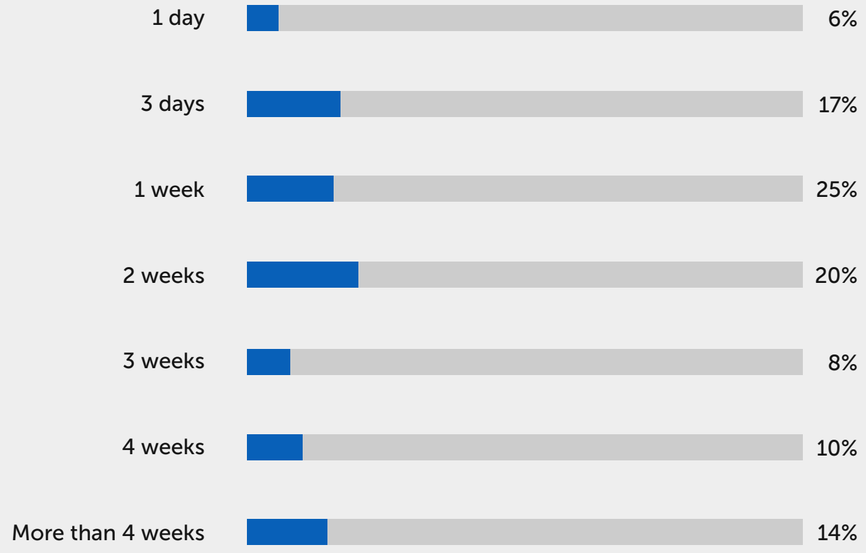
More than three-quarters of IT and security professionals report that deploying a patch across their entire organization takes one week or more. This extended deployment timeline is often the result of several interrelated factors, including the complexity of large, distributed environments with diverse device types and configurations, the need to schedule patching during maintenance windows, and the coordination required between IT, security teams, and other business units. Manual and siloed processes further exacerbate these challenges, as they are time-consuming and difficult to scale in complex environments. Ensuring minimal disruption to critical business operations adds another layer of complexity, compounding delays and slowing the overall deployment process even further.

**The longer patch deployment window increases the organization's exposure to potential security vulnerabilities, heightening the risk of cyber attacks or compliance failures**.

Reducing these timelines through better automation, streamlined processes, and improved collaboration is critical for enhancing security and minimizing risks.

Figure 10

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



# Automated Elements of Patch Management

**Figure 11** shows that the most commonly automated elements in patch management are scans, patch and version identification, and patch testing.

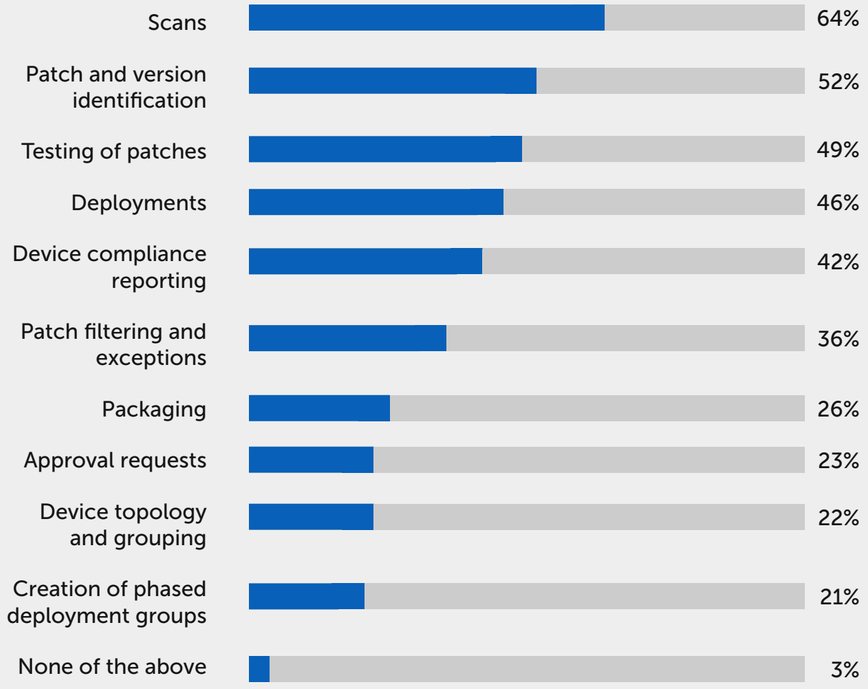
**While some respondents may be taking a siloed approach to automation, this study reveals promising progress: Participants who automate patch management report automating an average of 3.9 elements.**

This finding demonstrates a growing recognition of automation's potential to streamline processes and pave the way for more integrated and comprehensive strategies in the future.

By automating patch testing, organizations can assess a patch's potential impact before deployment, reducing the risk of introducing new issues or disrupting critical operations. These automated steps significantly reduce the time and manual effort required, relieving IT and security teams, who can focus on more strategic tasks while ensuring that patches are applied promptly and effectively.

Figure 11

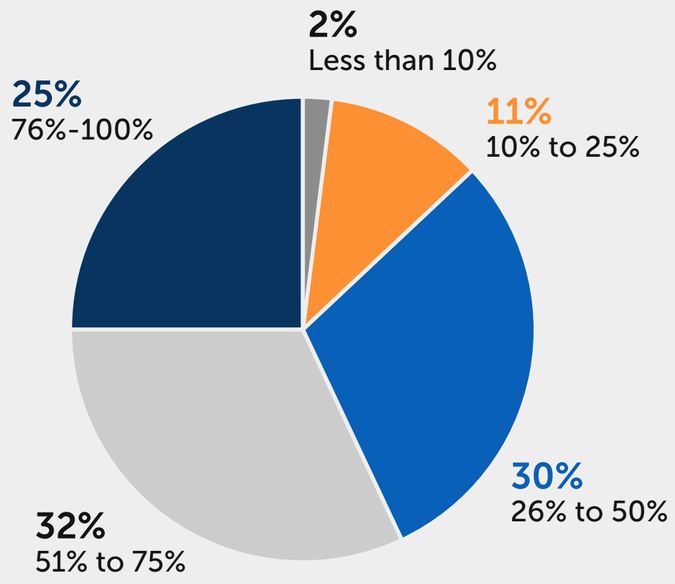
Select the elements of your patch management that are automated:



# Distribution of Application Patches Using Automation

Figure 12

What percentage of application patches are distributed using automation?




Automation is essential for managing the growing demands of patch management, with adoption rates steadily increasing. This survey revealed that 79% of IT and security professionals have already automated the distribution of application patches, and 57% of those who haven't automated plan to do so within the next year.

**This means an impressive 94% of organizations have either adopted automation, are expanding its use, or intend to implement it soon—reflecting a significant shift toward more efficient and secure patch management.**

Despite this progress, there is still room for improvement. Only one-quarter of IT and security professionals report that they are taking a more autonomous approach (with 75% or more of their application patches are distributed using automation). Vulnerabilities in third-party applications continue to require timely patching, while network limitations, organizational complexities, and the need for tailored patching strategies can hinder efficient deployment.

**The next section of this report will explore the benefits of an autonomous approach.**

# The Benefits of Automation

Automation is revolutionizing patch management, offering significant benefits to organizations that have embraced advanced, autonomous systems.

**Compared to more limited forms of automation, this study found that "Autonomous Adopters," organizations that report 75% or more of their application patches are distributed using automation, experience fewer disruptions, higher efficiency, and reduced risks.**

**The following insights highlight the differences between organizations with limited automation and those leveraging autonomous automation, emphasizing the advantages of adopting a more sophisticated approach.**

# Better Collaboration

As noted earlier, one major challenge in patch management is coordination and visibility between IT, security teams, and other stakeholders. 72% of IT and Security professionals report that different business units, locations, and devices require different patch handling, approval processes, and timelines.

However, as **Table 2** shows, "Autonomous Adopters" are far less likely to report collaboration challenges related to lack of process, visibility, tools, and coordination than their counterparts using limited automation.

**By streamlining workflows and improving communication, automation platforms reduce team friction, ensuring patches get deployed consistently and with fewer miscommunications.**

This leads to better alignment between IT and security teams, which is essential for timely patch deployment and reducing vulnerabilities across the organization.

Table 2

Collaboration challenges between the security and IT teams that negatively impact the speed of remediation include the following:

| Lack of process | Agree | Neutral | Disagree |
|---|---|---|---|
| Limited Automation | **46%** | **38%** | **26%** |
| Autonomous Adopters | **15%** | **31%** | **54%** |

| Lack of visibility | Agree | Neutral | Disagree |
|---|---|---|---|
| Limited Automation | **50%** | **28%** | **22%** |
| Autonomous Adopters | **30%** | **22%** | **48%** |

| Lack of tools | Agree | Neutral | Disagree |
|---|---|---|---|
| Limited Automation | **44%** | **26%** | **30%** |
| Autonomous Adopters | **20%** | **26%** | **54%** |

| Lack of coordination | Agree | Neutral | Disagree |
|---|---|---|---|
| Limited Automation | **53%** | **29%** | **18%** |
| Autonomous Adopters | **28%** | **28%** | **44%** |

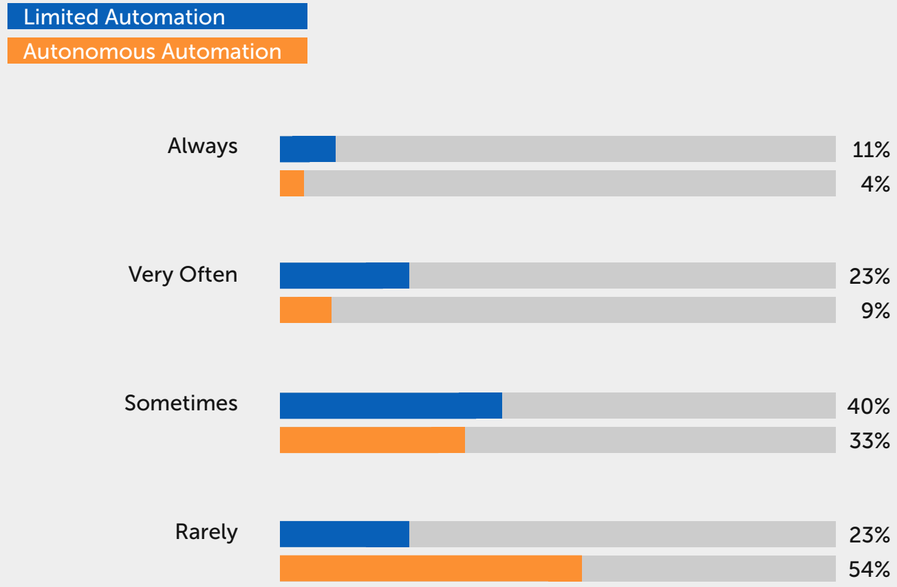
# Fewer Patch Rollbacks

The need to quickly roll back problematic patches is universal, as only 3% of this study's participants reported never having encountered a situation where their IT team wished they could roll back a patch after deployment.

**However, as Figure 13 shows, "Autonomous Adopters" are much less likely to report the need to roll back patches after deployment than those with less sophisticated automation.**

Figure 13

In your experience, how often have you encountered situations where your IT team wished they could roll back patches after deployment?



# Faster Patch Deployment

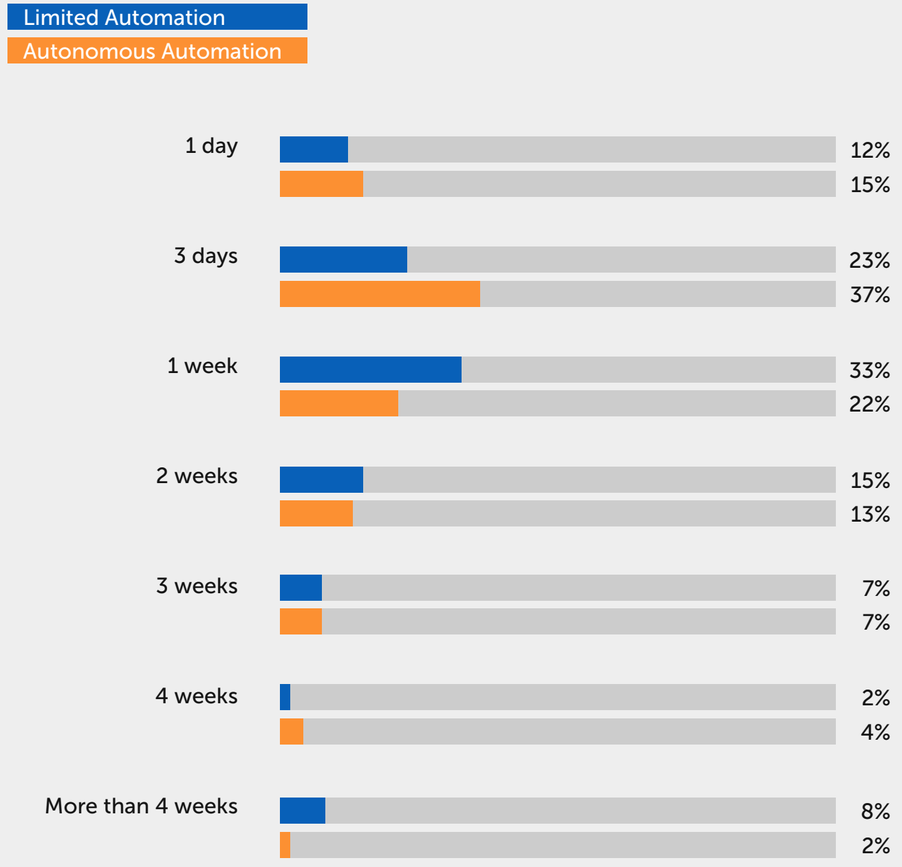
Regarding patch deployment, more than three-quarters of IT and Security professionals report that it takes one week or more to deploy a patch across the entire organization.

**In contrast, Autonomous Adopters are far more likely to deploy patches in three days or less than their more manual counterparts, as shown in Figure 14. Organizations using Autonomous Automation begin deploying patches nearly 50% faster within the critical 1- and 3-day windows compared to those using Limited Automation.**

This faster deployment cycle allows organizations to address vulnerabilities more quickly, significantly reducing the window of exposure to potential cyber threats.

Figure 14

How long does it take to begin a patch deployment after the manufacturer releases one?



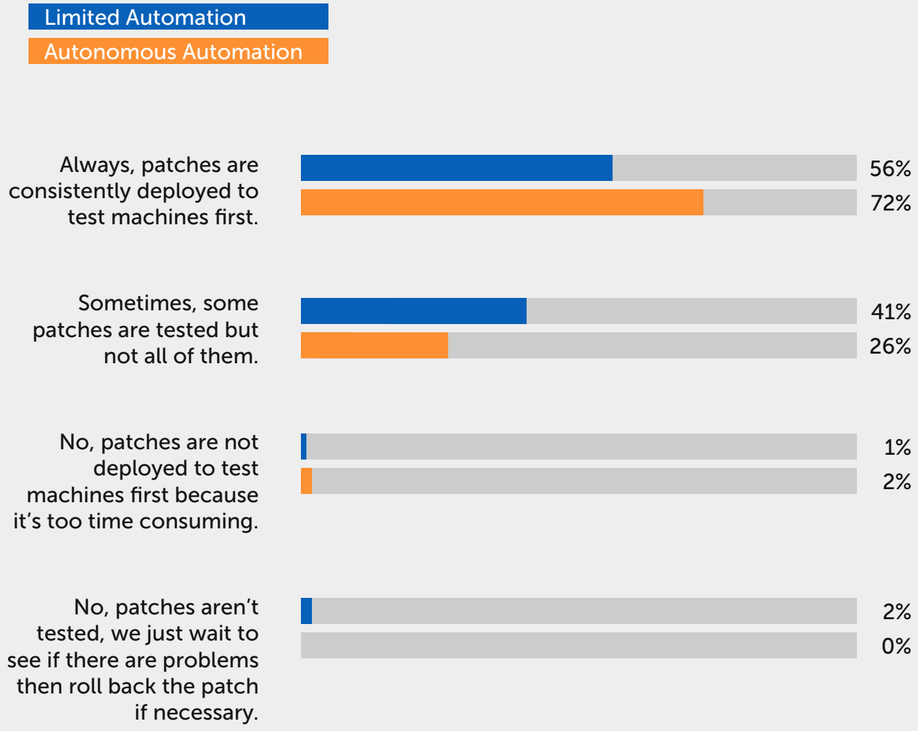
# Consistent Testing

Testing patches before deployment is critical to avoid introducing new operational issues. However, only 61% of this study's participants report routinely testing patches before deploying them.

**However, Autonomous Adopters are far more likely to test patches as part of their automated processes, ensuring that patches are deployed quickly and safely.**

Figure 15

Do you test patches before deploying them?



# Improved Compliance

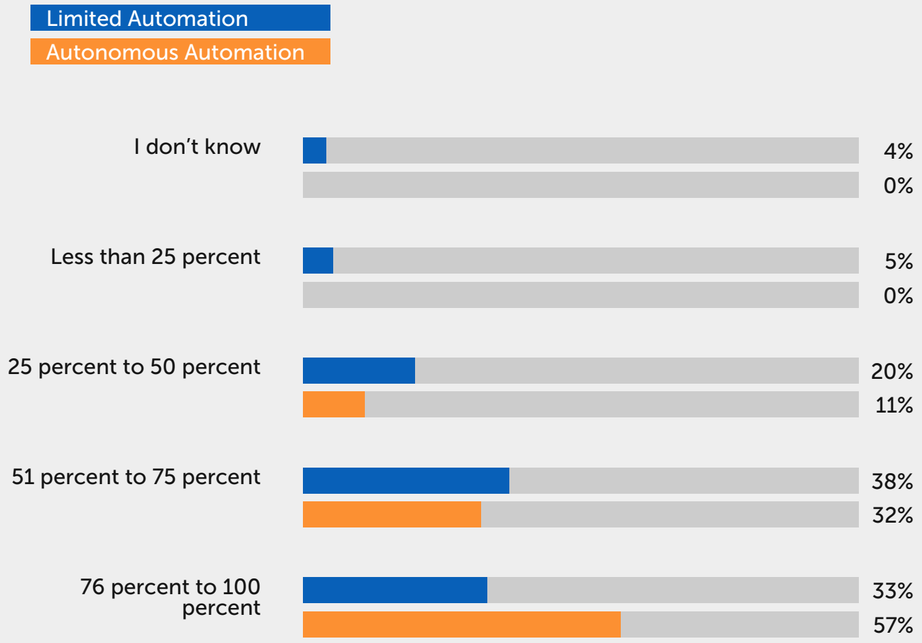
In addition to testing, only 38% of IT/Security professionals surveyed report that their applications are updated to the latest version.

**However, Autonomous Adopters are significantly more likely to keep their systems up-to-date, monitoring and deploying the latest application versions, as Figure 16 shows.**

This capability helps organizations avoid emerging security risks and ensures their systems run the most secure and stable software versions.

Figure 16

What percentage of the applications tracked are on the latest version?



# Conclusion

Accelerating the management and security of devices requires moving beyond traditional approaches to a fully adaptive platform for Autonomous Endpoint Management. By leveraging adaptive and autonomous capabilities, organizations can achieve faster patch deployment, enhanced control, and greater reliability, ensuring their endpoints are secure and their operations remain uninterrupted.

Looking ahead, the future of endpoint security lies in embracing intelligent, integrated solutions that leverage automation and enable organizations to address vulnerabilities proactively, predict potential threats, and optimize patch deployment with minimal human intervention.

**By shifting from reactive, manual processes to predictive and autonomous systems, businesses can accelerate their patch management cycles and reduce operational disruptions**. This forward-thinking approach positions organizations to stay ahead of security challenges and maintain seamless and secure operations.

# Action Plan

1 2 3 4 5 6

## Step 1: Audit Your Current Patch Management Process

It's crucial to review your patch management practices against a maturity model. This model, consisting of four phases, provides a clear roadmap for improvement and helps you assess your organization's current state. **Conduct your own assessment here**.

### PHASE 1: MANUAL

In this stage, the IT team manually manages each stage of patching, which leads to a slow and often inefficient process, increasing the organization's exposure to vulnerabilities. According to recent findings, more than three-quarters of IT and security professionals report it takes one week or more to deploy patches, highlighting the risks of manual processes.

### PHASE 2: AUTOMATED

As organizations begin to automate, patch deployment accelerates, but this may result in less control over the process. However, 79% of IT and security professionals have automated some portion of their patch distribution, improving efficiency but often introducing complexity in oversight.

### PHASE 3: ADAPTIVE

Adaptive technologies play a vital role in this phase, reintroducing control and improving efficiency. They incorporate responsive and customizable automation to specific organizational needs, helping manage different patch handling, approvals, and processes across diverse business units.

### PHASE 4: AUTONOMOUS

Autonomous patching technology takes it a step further, proactively responding to risks and network conditions. "Autonomous Adopters" are more efficient.

**Use the following assessment tool to evaluate your organization across key dimensions: Speed, Control, and Reliability.**
**Identify pain points, such as delays in deployment, high manual workloads, or insufficient visibility into endpoint vulnerabilities.**

# Action Plan

1 2 3 4 5 6

## Step 2: Assess Patching Vendors

Evaluating potential platform vendors is a critical step that requires careful consideration of their capabilities and alignment with your organizational needs.

A **checklist of key questions** will help you ensure the selected vendor is equipped to handle your patch management demands. Developing a strategy for vulnerability remediation is crucial, particularly as 72% of IT/Security professionals report that different business units and locations require different handling and approval processes.

Your strategy should include vulnerability management integration and risk-based prioritization to ensure that critical vulnerabilities are patched quickly while maintaining operational continuity across the organization.

Learn more about best practices to reduce risk fast with autonomous vulnerability patching here: **The 5 best practices to reduce risk fast with autonomous vulnerability patching.**

## Step 3: Model Your Vulnerability Remediation and Patching Strategies

Evaluating potential platform vendors is a critical step that requires careful consideration of their capabilities and alignment with your organizational needs. A checklist of key questions will help you ensure the selected vendor is equipped to handle your patch management demands.

Pay particular attention to features such as automation, customization, and rollback capabilities—areas where Autonomous Adopters excel, with faster deployment and rollback times than limited automation solutions. Learn more about best practices for a proactive approach to remediation **here**.

# Action Plan

1 2 3 4 5 6

## Step 4: Automate Patch Deployments from Testing to Installation

Automation is a key driver of efficiency and security. You can reduce human errors, streamline workflows, and significantly reduce patching times by automating the entire patching process–from testing to deployment.

Autonomous Adopters are more likely to involve fewer IT resources to manage the process than less automated environments requiring more IT bandwidth.

See how one organization managing 5500 endpoints across 190 locations accelerated patching without manual effort **here**.

## Step 5: Monitor the User Experience and Ensure Controls for Failure Scenarios

Even with automation, it's essential to continuously monitor the user experience and ensure robust controls are in place for when things go wrong.

For example, 58% of IT and security professionals report experiencing delays due to stakeholder involvement outside IT, highlighting the importance of **streamlining approval processes** and addressing potential bottlenecks.

Additionally, ensure your system has a quick and reliable **rollback process** to minimize downtime or security exposure when patches fail, providing a safety net for unexpected situations.

# Action Plan

1 2 3 4 5 6

## Step 6: Analyze Patching Results and Vulnerability Remediation Compliance

Once patches are deployed, **regularly analyze your results** to ensure compliance and effectiveness. Measure how quickly patches are applied across the organization.

Autonomous Adopters typically report faster patching times—often deploying in 1-3 days—compared to manual or limited automakers, which may take a week or more, ensuring your organization remains secure and compliant at all times.

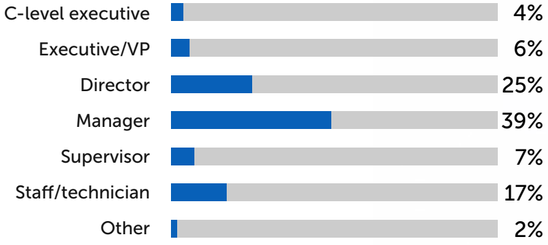
# Methodology

The State of Patch Management survey was administered online from August until September 2024. During this period, 456 complete and partial responses were collected of which 252 were included in the analysis. Only valid or correlated findings are shared in this report.

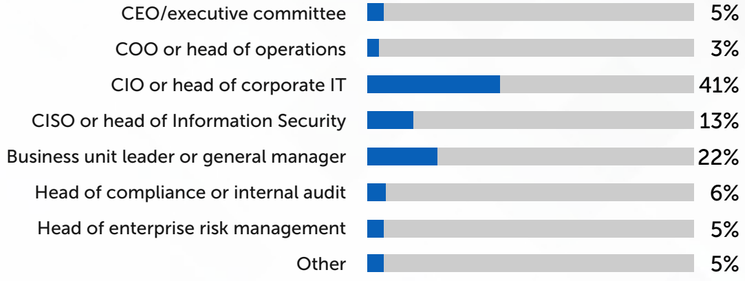
The representativeness of this study's results depends on the similarity of the sample to environments in which this survey data is used for comparison or guidance. Findings based on small sample sizes are noted and should only be used for informational purposes.

**Summarized below is basic categorization data collected about the 252 study participants to enable filtering and analysis of the data:**

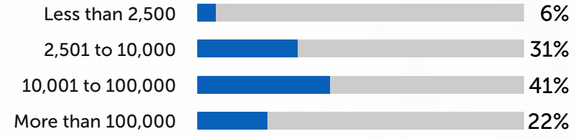
### What best describes your position level within the organization?



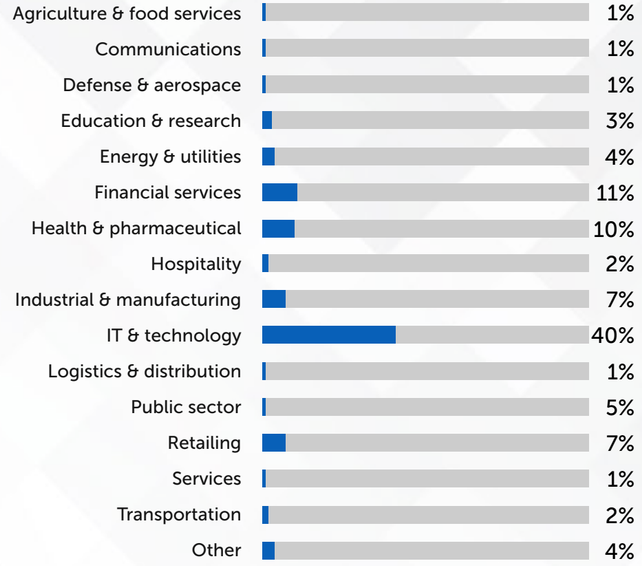

### What best describes your reporting channel or chain of command?




### What is your organization's headcount?




### What best describes your organization's primary industry classification?



adaptiva

# About

Adaptiva, the autonomous endpoint management company, delivers the fastest way to patch and manage endpoints at scale.

We offer OneSite, the first fully adaptive autonomous endpoint management platform. IT and cybersecurity leaders use OneSite to gain a hands-free, fully automated approach to speeding the continuous delivery of software, patches, and vulnerability remediations.

Founded two decades ago, hundreds of today's largest global organizations rely on Adaptiva to increase operational efficiency, reduce risk, and maximize patching velocity across millions of endpoints.

Adaptiva is headquartered in the Greater Seattle area—in Kirkland, Washington—and has team members around the world with deep expertise in enterprise endpoint management and innovation.

Our philosophy is simple: Humans should define strategy and process, and software should do the rest.

Learn More

DEMAND METRIC

# About

Demand Metric is a global research and advisory firm that helps organizations empower their people with the expertise, insights, and resources they need to unlock customer value and achieve sustainable growth.

Through strategic partnerships with the AMA, ANA, and AIPMM, Demand Metric's resources have become the industry standard for business professionals. Over the past 18 years, they have helped 6,000+ businesses worldwide rapidly build their in-house capabilities.

Enable your team with access to cutting-edge research, experienced experts, and the world's most trusted set of playbooks, tools, and templates.

Learn More