AUTOMOX

2023 STATE OF IT OPERATIONS

Learn how nearly 500 ITOps professionals are managing endpoint complexity despite economic uncertainty.

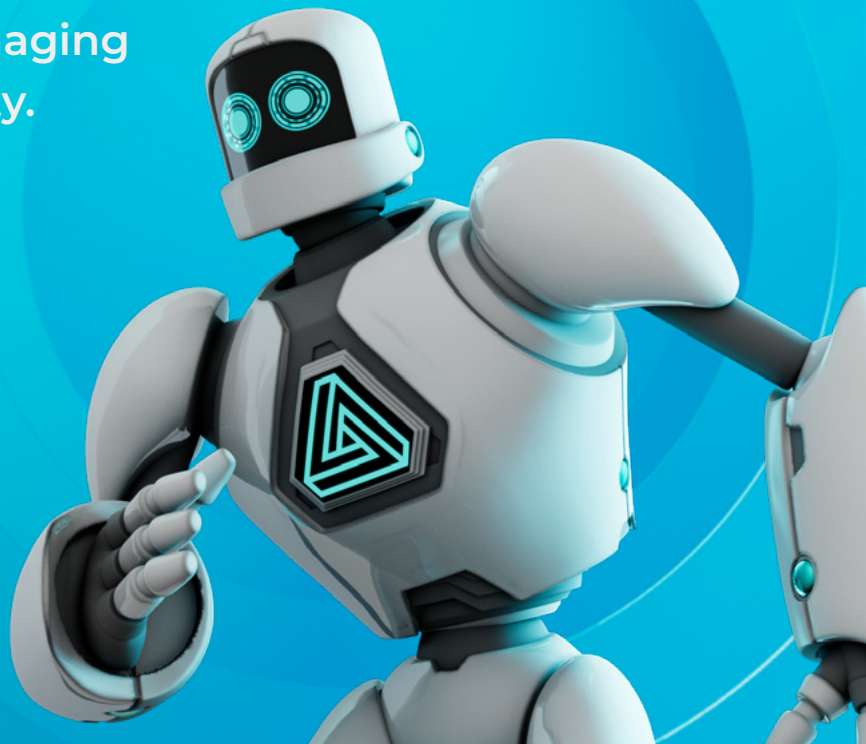


Table of contents

Introduction 3

Top Takeaways and Trends 4

State of the Economy for ITOps Teams 5

Complexity and Scale Continue to Be Hurdles for Endpoint Management 8

How to Increase Endpoint Management Efficiency 11

Automation Trends in ITOps 16

Cloud Trends for ITOps 27

How Companies are Selecting Endpoint Management Solutions 34

End the Complexity 37

Methodology 39

INTRODUCTION

The adage of “do more with less” is pushing ITOps to be more efficient.

In a time of economic uncertainty, the perfect storm may be brewing for IT operations (ITOps) teams. As the amount of data and number of devices continue to rapidly increase and hybrid and remote workplaces become the norm, ITOps teams are tasked with managing an environment with heightened complexity and more diverse endpoints. Compounding these difficulties is a weakened economy that is pushing companies to trim back on hiring, cut costs on tools and budgets wherever possible, and push teams to do more with less.

As we enter our fourth year of producing this report, findings from nearly 500 U.S.-based ITOps professionals show that many are hungry for more efficient ways to centralize and simplify IT operations.

IT teams are looking for scalable solutions that make it faster and easier to manage today’s complex IT environment.

As part of this year’s report, we dug into where the biggest efficiency challenges were for ITOps teams, what’s holding them back, and how automation and the cloud are increasing IT agility, reducing costs, and enhancing ITOps ability to simplify IT management of today’s modern workplace. See what’s working, where ITOps teams are struggling, and how your own team stacks up.

Top takeaways and trends

1

Economic impacts are minimal so far for ITOps teams, but there's still concern

87% of ITOps professionals say their companies are still experiencing rapid or steady growth, but over half worry about reduced budgets, should the economic climate become more challenging.

2

Endpoint management remains complex

55% of organizations do not feel they are managing their endpoints very efficiently.

3

Organizations are moving toward fully automating endpoint management, but most aren't there yet

Only **23%** of organizations have fully automated endpoint management, but **77%** say they are at least mostly automated.

4

Improved security posture, more control across all endpoints, and reduced cost of ITOps are driving investments in automation

Over half of all IT professionals cited these as the top three reasons for increasing automation.

5

Adoption of the cloud and cloud-based solutions continues to increase, but there's still room for significant growth

Only **28%** of organizations are fully cloud-based and only **21%** of organizations fully use cloud-based solutions for endpoint management.

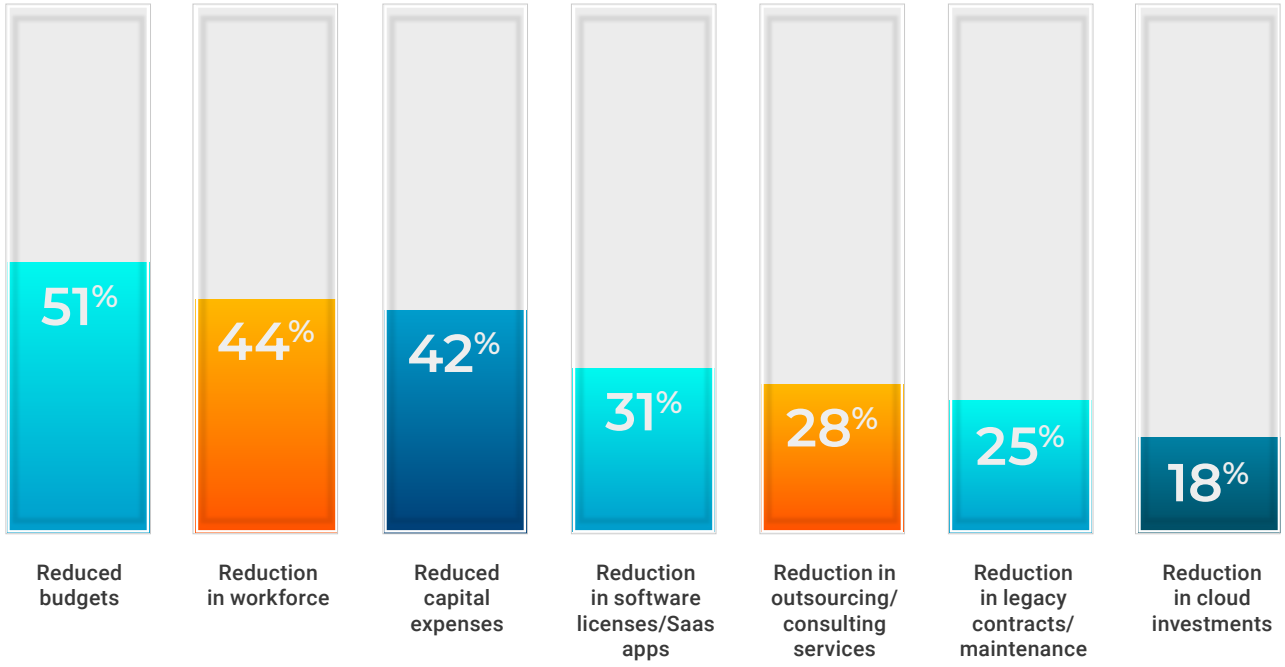
State of the Economy for ITOps Teams

In a world where layoffs and recession worries seem to frequent the headlines, it's notable that ITOps professionals are seeing a much more dynamic and positive picture at the companies they work at. In fact, many are experiencing rapid growth.

However, even with most ITOps teams feeling their companies are doing well, the turbulent economic climate still creates room for concern. The companies that can find ways now – and in the future – to do more with less will emerge as the winners, especially if times should get tougher.

Budgets and layoffs are the biggest concerns if economic headwinds require cutbacks.

Should a recession occur or if the current economic downturn continues, which of the following are you concerned about?

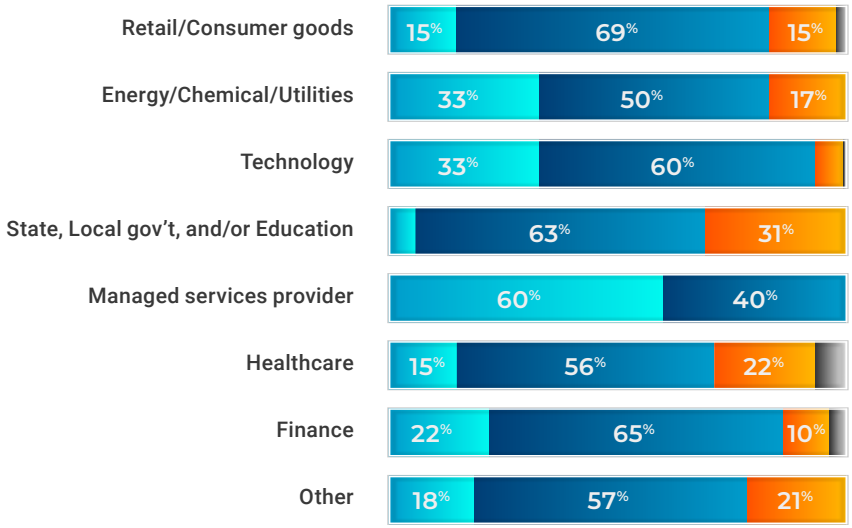


Not all industries are seeing rapid growth

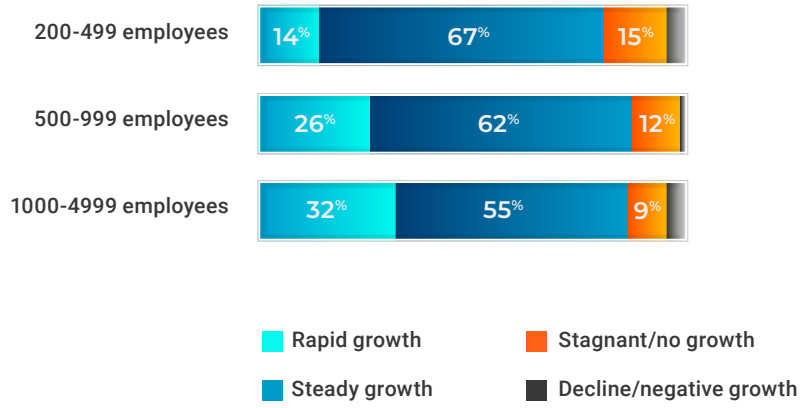
Managed service providers (MSPs) are seeing an exceptional amount of growth with **60%** stating their companies were experiencing rapid growth. This rapid growth may be due to increasingly complex IT stacks that require skilled resources, making it easier in some cases to simply outsource to MSPs.

Approximately one-third (**33%**) of technology and energy/chemical/utility companies are also experiencing rapid growth. However, nearly a third of state, local government, and/or education and healthcare companies are experiencing stagnant or declining growth. Smaller companies are also experiencing slower growth, making any belt-tightening even more challenging – and more of a reason to seek greater efficiencies in IT operations.

Growth by industry



Growth by size of company



Our findings also show that the larger the company size, the more likely they are to be experiencing growth. Smaller companies already have fewer resources – making any belt-tightening even more challenging – and more of a reason to seek greater efficiencies in IT operations.

Complexity and Scale Continue to Be Hurdles for Endpoint Management

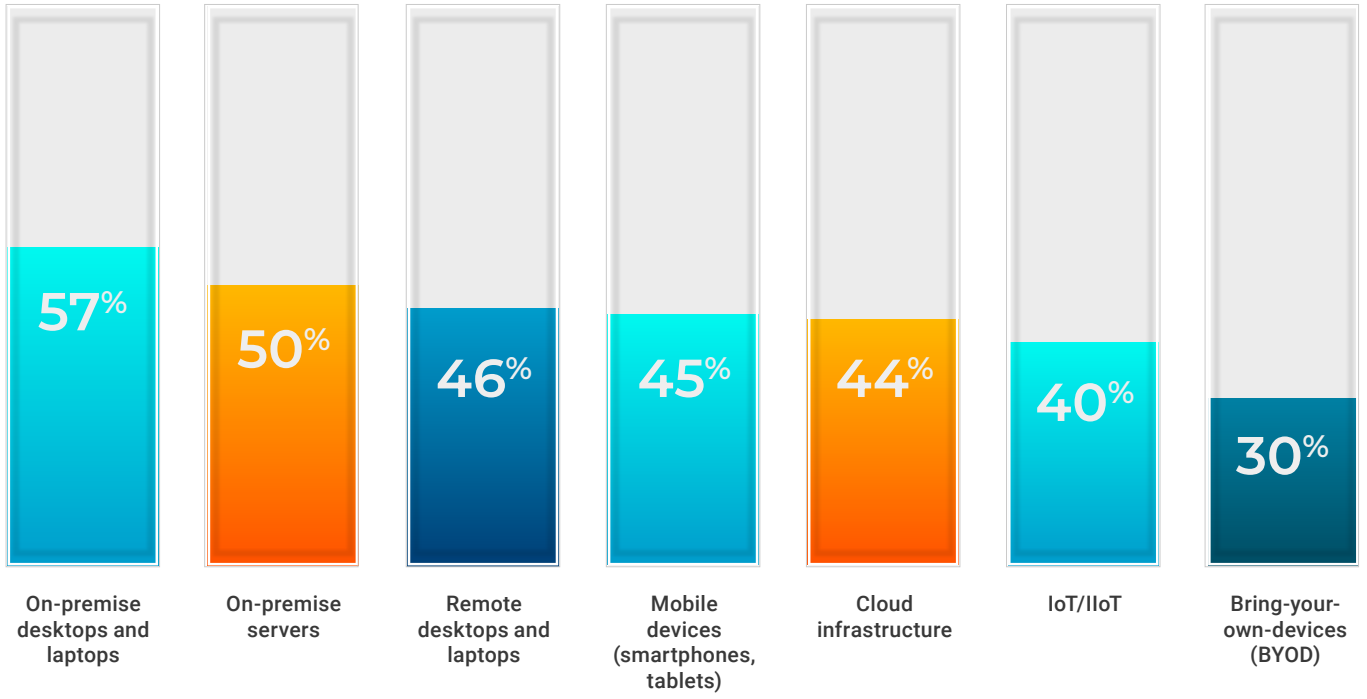
On-premises workloads and devices are easier for IT operations teams to manage, but the increasingly mobile, distributed, and cloud-enabled workforce is bringing more employee-owned devices and distributed endpoints into the mix, creating greater endpoint management challenges.

The complexity of the IT environment means that ITOps teams must manage thousands to hundreds of thousands of endpoints across multiple locations – often with a myriad of tools. While ITOps teams are making progress in reducing complexity, they are far from conquering the issue altogether.

The majority of organizations do not feel they are managing their endpoints very efficiently

The complexity of the IT environment means that ITOps teams must manage thousands to hundreds of thousands of endpoints across multiple locations – often with a myriad of tools. While ITOps teams are making progress in reducing complexity, they are far from conquering the issue altogether.

Organizations that say they can “very efficiently” manage the following endpoints

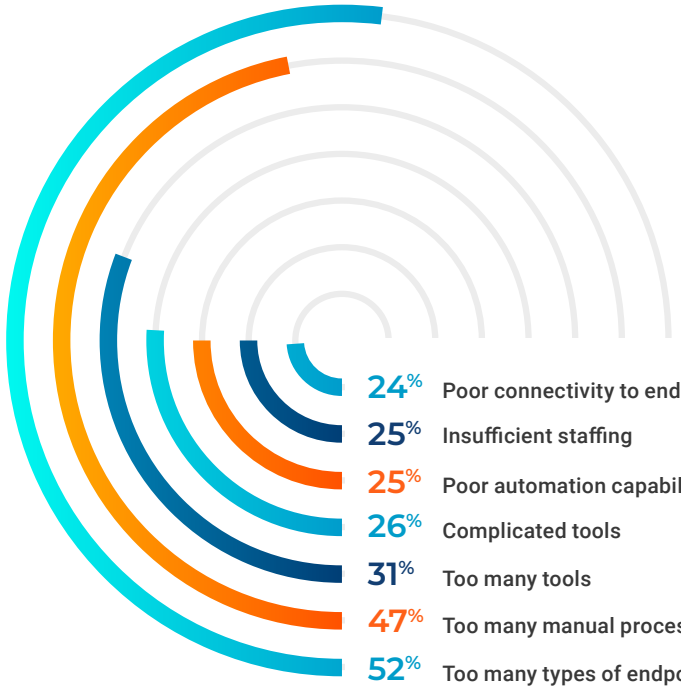


What's holding ITOps back from greater efficiency?

Too many types of endpoints, manual processes, and tools are the biggest obstacles to managing endpoints efficiently. Too many manual processes is an especially surprising finding given that 77% of ITOps professionals say their endpoint management environment is "mostly" automated. One hypothesis could be that what still isn't automated is painful and time-consuming.

The massive shift to remote work and an acceleration of cyberattacks on remote devices means organizations must contend with their attack surface expanding far beyond the corporate walls. This makes securing all parts of a digital environment uniquely challenging with increasingly distributed teams. Too many point solutions for endpoint management further add to the complexity of monitoring and managing the overall digital environment.

The biggest causes of endpoint management inefficiency



- 24% Poor connectivity to endpoints that rely on VPN connections
- 25% Insufficient staffing
- 25% Poor automation capabilities
- 26% Complicated tools
- 31% Too many tools
- 47% Too many manual processes
- 52% Too many types of endpoints (on-premises, remote, hybrid, etc.) being managed

How to Increase Endpoint Management Efficiency

ITOps teams that can implement more efficient tools and processes will enhance their agility and ability to support internal and external customers. Yet, complicated tools, too many tools, and poor automation are all getting in the way. Here's a look at how to overcome these types of hurdles.

View and manage all endpoints from a single console

As organizations grow, tracking the inventory of all the virtual and physical assets becomes increasingly complicated. An endpoint management platform that can provide a complete inventory of all hardware, software, patches, and configuration details for corporate endpoints allows organizations to remediate and patch vulnerabilities, deploy required software, and fix misconfigured systems without the need for multiple tools.

Given the growing shift toward hybrid, flexible, and agile ways of working among today's modern workforce, there's a greater need than ever for solutions that will enable ITOps teams to manage these different endpoints from a single console.

ITOps teams with fewer tools are more efficient than those with more tools

ITOps using 5 tools or fewer see an average of

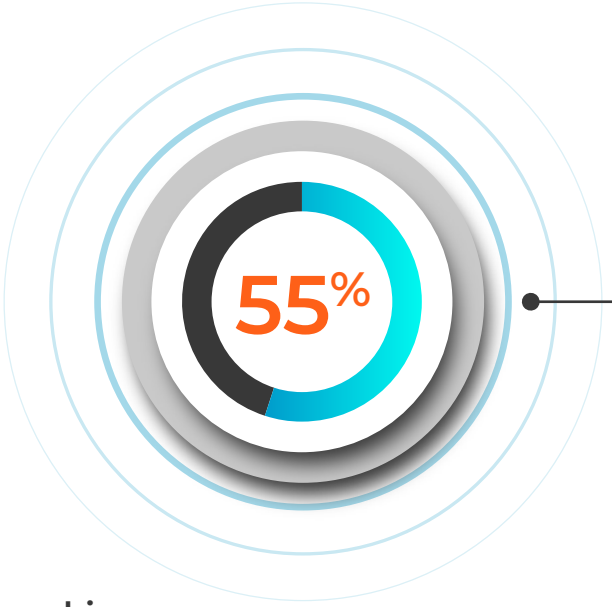
5% to 20%

greater endpoint efficiency than those using 10+ tools

Only 4% of ITOps have streamlined endpoint management to 1 to 2 tools

Many teams have ended up with too many tools because legacy solutions lack the capabilities to manage and monitor increasingly complex and diverse environments, especially as new infrastructure components and device types are added. This sort of tool sprawl is a problem of compounding maintenance and learning for IT teams with diminishing returns.

As emerging technologies continue to be adopted by the modern workforce and cloud services, IoT, and mobile devices also continue to proliferate, the inherent complexity of IT ecosystems will only further increase. What's more, each additional management tool requires more training and increases administrative overhead.



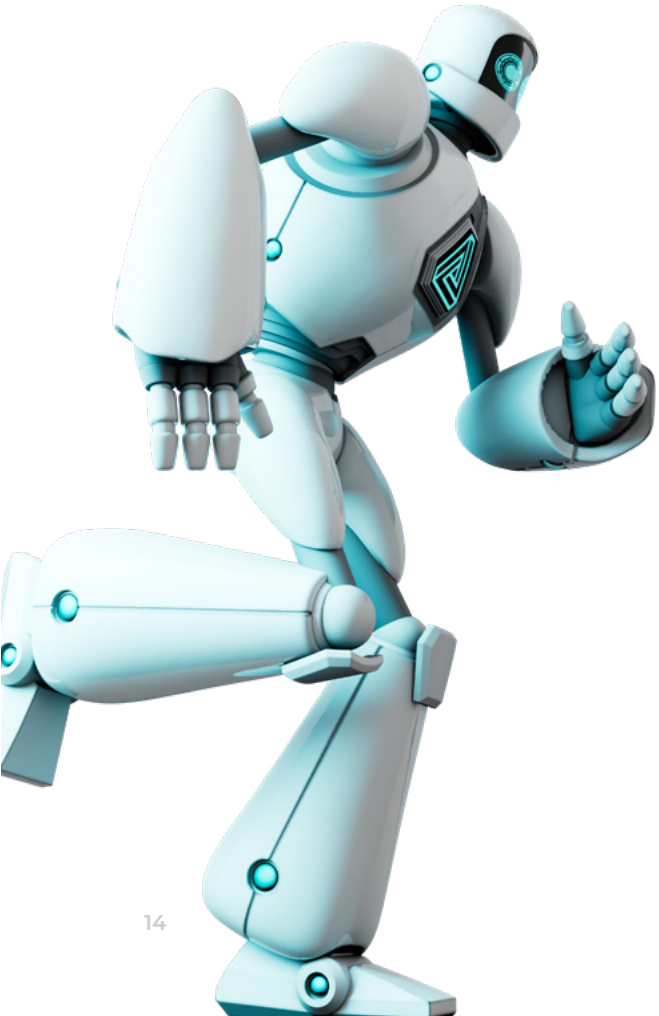
Of respondents use 6 or more applications, tools, and services to manage their organizations
20% use 10+

But ITOps teams are making progress.

In 2022, **60%** of ITOps professionals said they were using over 10 tools for endpoint management. Today, that's dropped to **20%**.

More automation equals more efficiency

Without modern, automated solutions that allow ITOps to manage, maintain, and secure remote endpoints efficiently at scale and from anywhere, manual and repetitive processes will continue to hold IT teams back.



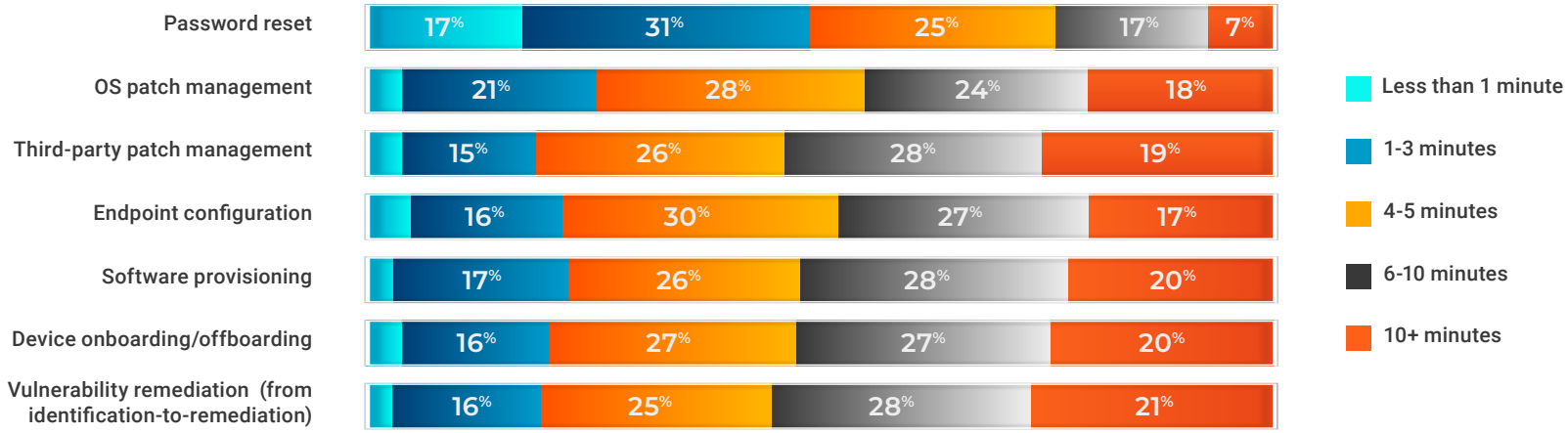
77% **Of ITOps say their endpoint management is automated, but manual processes still hamper ITOps teams from being highly efficient.**

The most time-intensive manual task according to respondents was vulnerability remediation. In 2022, over **22.5 thousand** new common IT vulnerabilities and exposures were discovered. While this number encompasses all types of hardware, software, and IoT devices, even if an organization is only dealing with vulnerabilities from an average Microsoft "Patch Tuesday," they will still have somewhere between 50 to 100 new common vulnerabilities and exposures (CVEs) to address each month. For instance, if the average is 80 new Microsoft CVEs per month across 1,000 devices, that's 8,000 vulnerabilities a month to remediate or 32,000 hours per month if you were to fix them each manually at four minutes per patch.

Manually managing tasks quickly adds up for ITOps professionals

Not surprisingly, many IT teams get bogged down by manual patch policies, arduous success or failure reporting and investigation, and unreachable devices, which results in wasted time and massive burnout. Consequently, many organizations with legacy tools that lack automation only fix the most important devices and the highest-risk vulnerabilities, leaving remaining endpoints often unmanaged and exposed to additional security breaches.

On average, how long do the following tasks take you to do manually per endpoint?



Automation can enable IT operations to fix vulnerabilities much faster across different operating systems and software, collect data that pinpoints what needs to be done next, and report on tasks completed — as well as those that are outstanding – freeing up significant time to focus on higher value work.

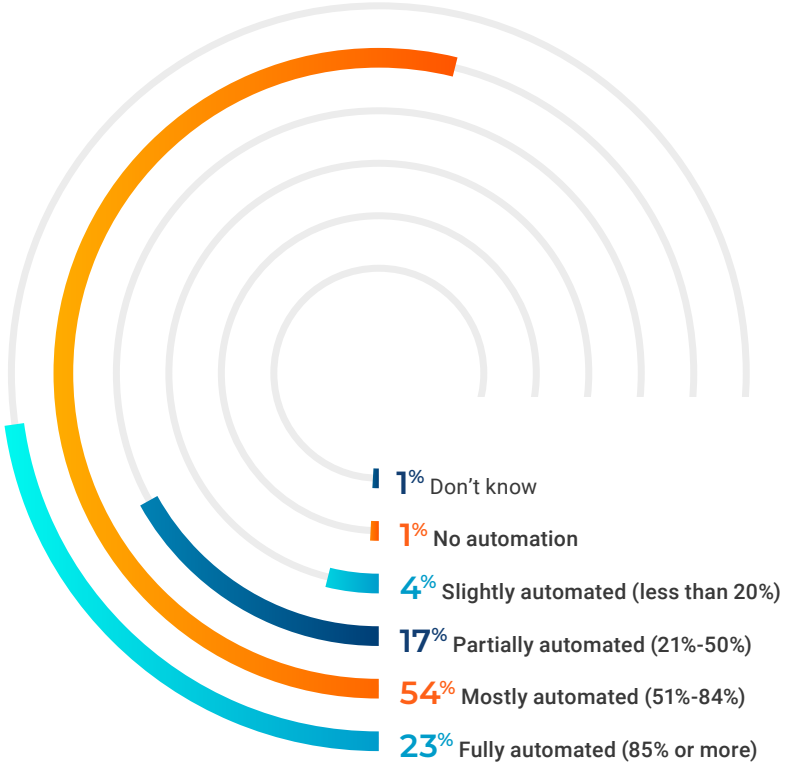
- **77% of those with a fully automated endpoint management solution for on-premises desktops and laptops say they are very efficient**
- **Only 41% of those with less than 20% of their endpoint management automated say they are very efficient**

Automation Trends in ITOps

Our findings clearly show that respondents see the value in adopting modern, automated solutions, particularly those that are scalable, low-maintenance, and that give visibility and control over today's complex IT environments. As a result, automation is becoming more of the norm.

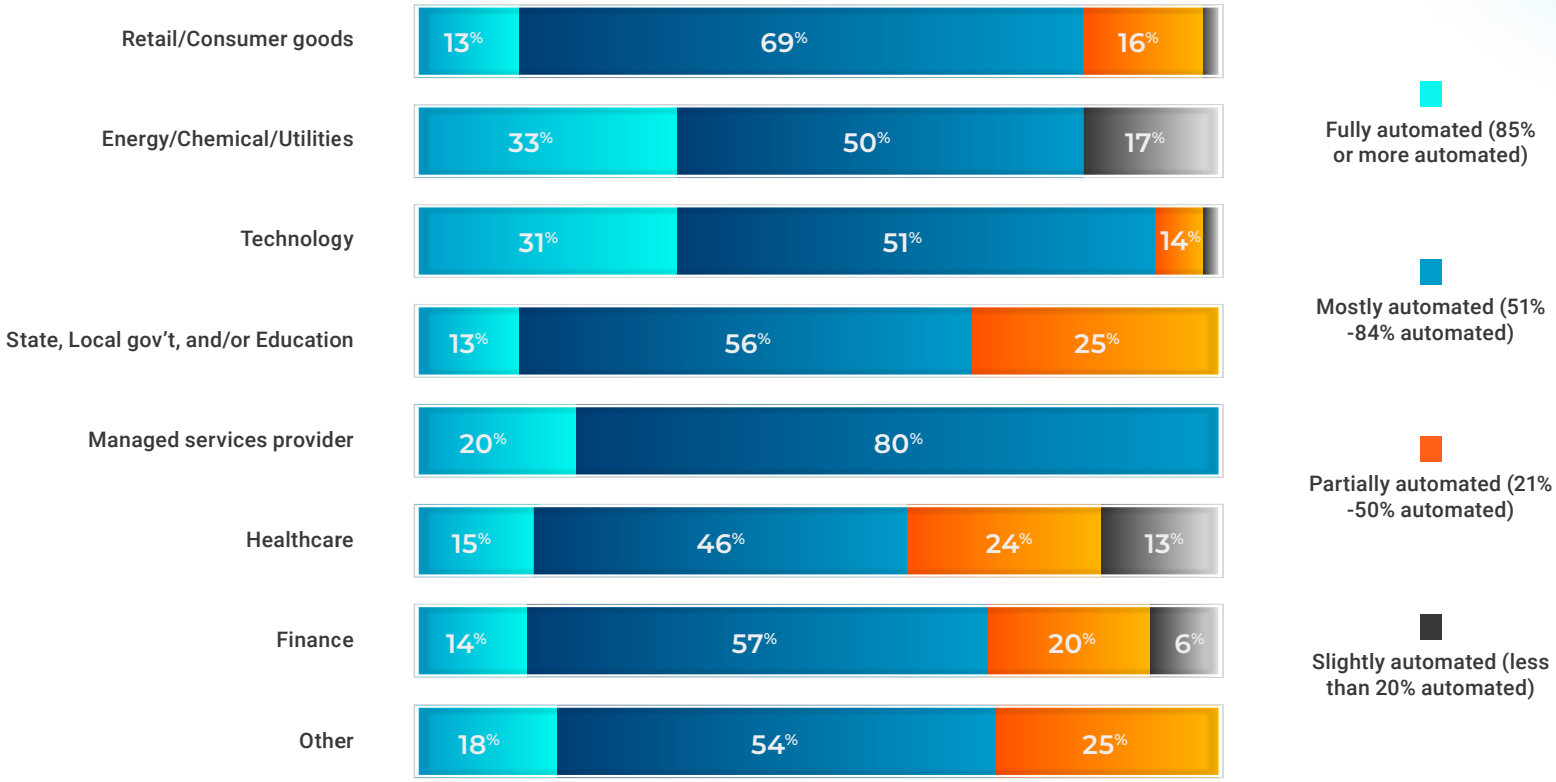
77% of organizations say their endpoint management is mostly (54%) or fully automated (23%)

Which best describes the extent to which your organization's endpoint management operations are automated?



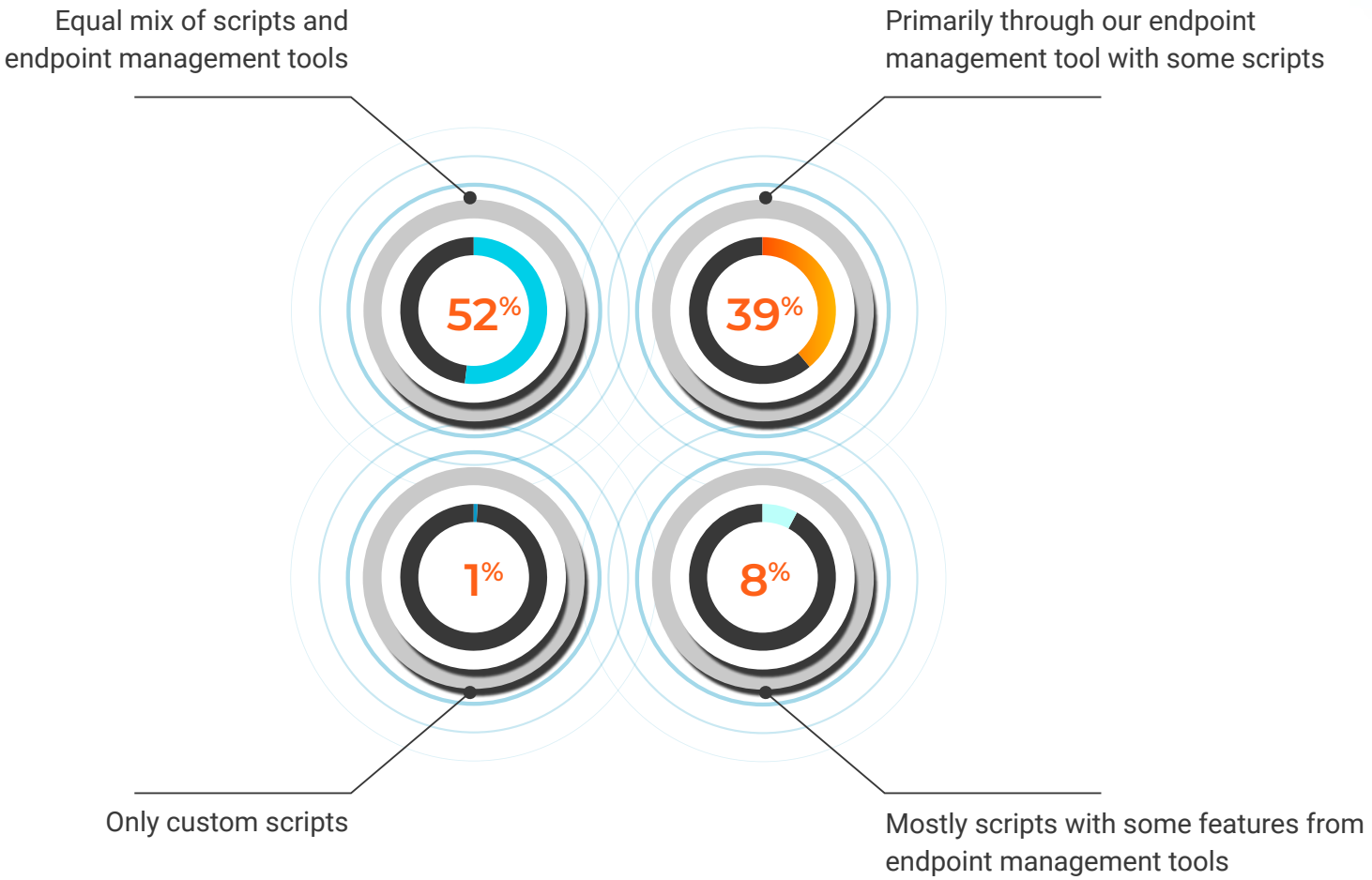
Automation maturity by industry

MSPs, technology, and energy/chemical/utilities are the “most fully” to “mostly automated” industries. Healthcare, state, local government and/or education, and finance present the most areas of opportunity for automation.



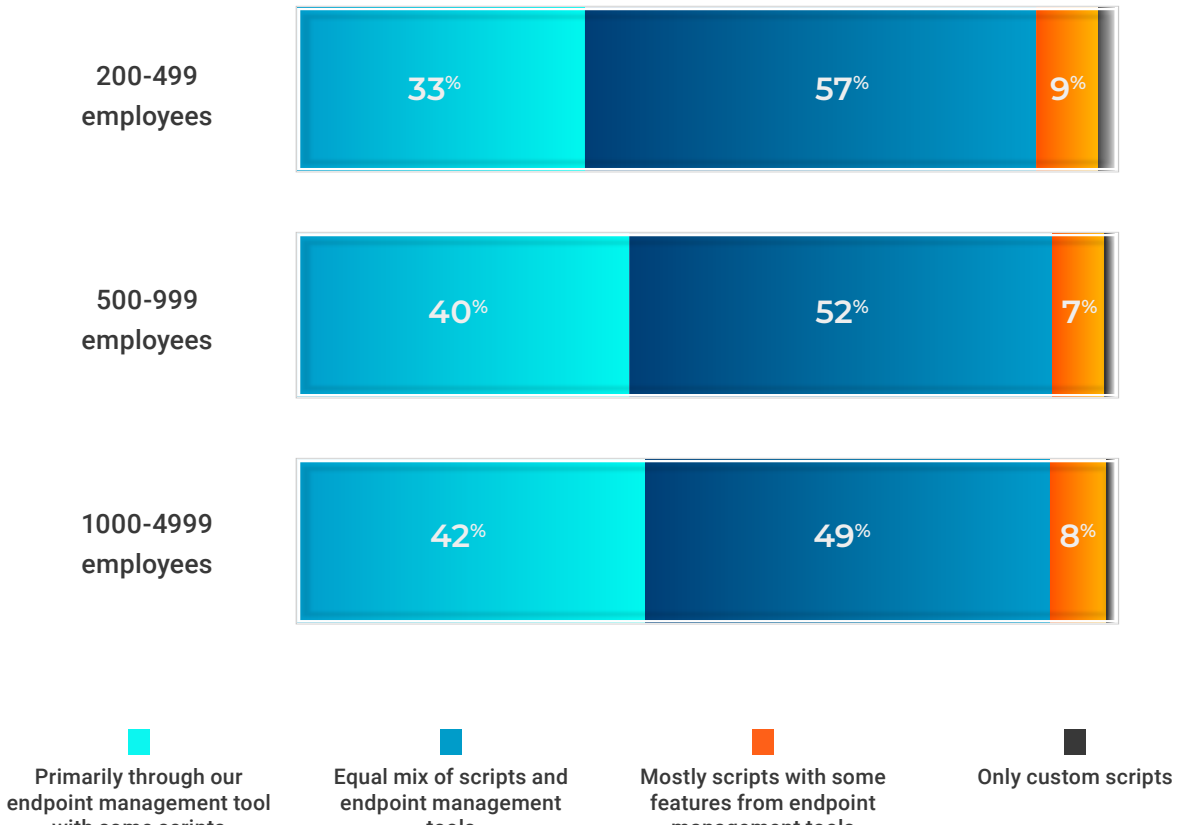
How ITOps are automating endpoints

There isn't one right way to automate endpoint management. While most organizations automate endpoint management through a mix of scripts and endpoint management tools, our findings show organizations are taking multiple approaches to automation.



Endpoint management tools by company size

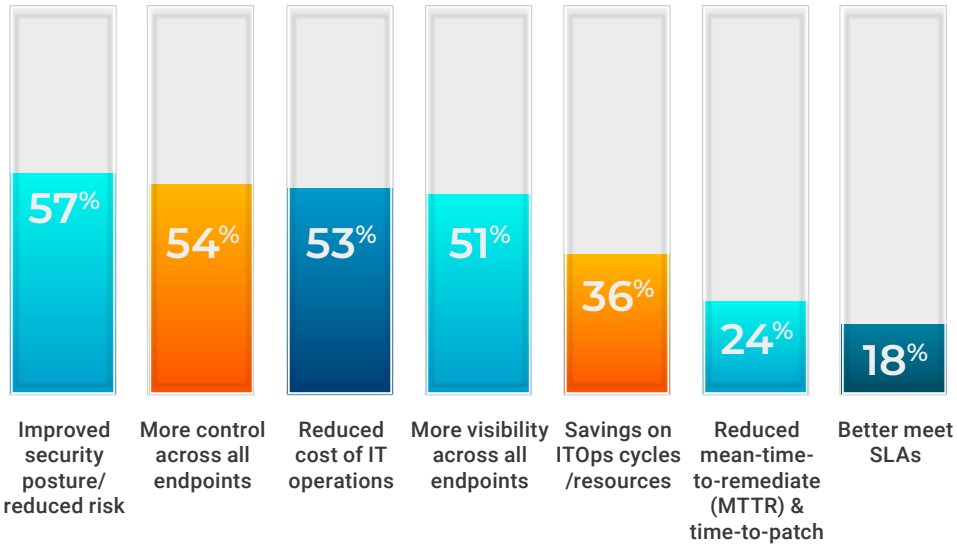
The larger the company, the more likely it is to automate primarily through an endpoint management tool with some scripts.



Benefits of automation

Improved security posture/reduced risk, more control across all endpoints, and reduced cost of IT operations are the biggest benefits ITOps professionals expect from automation. Saving on ITOps resources is also an important benefit of automation in today's current economic climate, not only because it reduces costs, but it can help fill IT staffing shortages. In our 2022 report, staffing shortages were cited as the number one impediment to performing essential endpoint management functions.

Which of the following benefits do you anticipate by increasing the automation of your endpoint management solutions?



The biggest realized benefit for "fully-automated" ITOps teams is agility

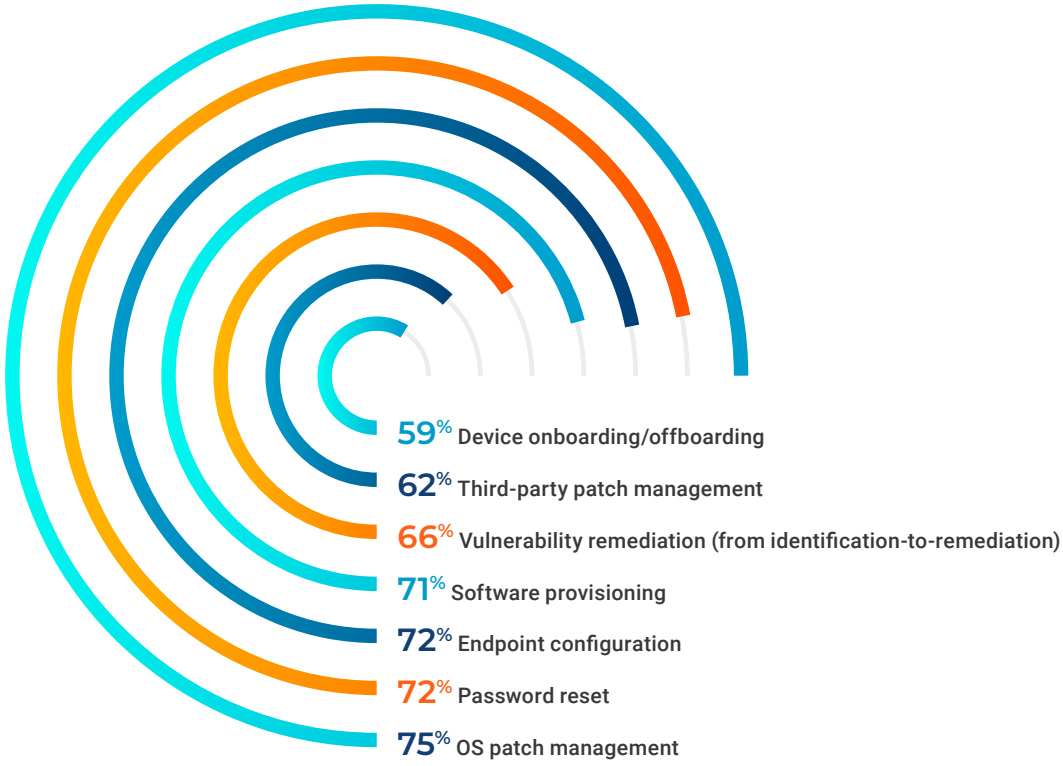
In the modern workplace, IT agility is critical. The greater agility an ITOps team has, the faster and more effectively they can respond to market and business changes. Automation is playing a key role in helping ITOps teams achieve the level of agility necessary to keep up in today's environment.

- **64% of those with full automation say they have greater IT agility vs. only 29% of those in slightly automated environments**

What tasks are being automated?

The most commonly automated tasks are OS patch management, password reset, and endpoint configuration. Third-party patching and device onboarding/offboarding are least likely to be automated.

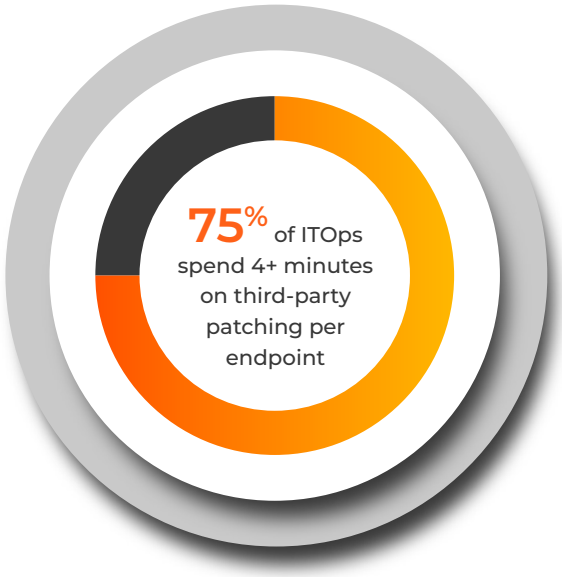
Are the following tasks automated?

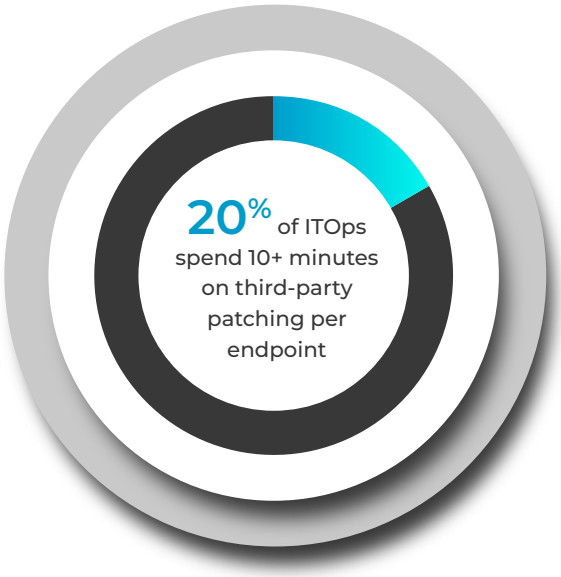


Third-party software patching is a major pain point

While operating systems are the primary focus of most ITOps patching efforts, third-party software is a major source of vulnerabilities in any network. Approximately **60%** of data breaches occur because of third-party software. Vulnerabilities are frequently found in popular software including Chrome, Adobe, and Java, and these applications are often an easy target because of their high market penetration and low patch rate.

Manually patching all third-party vulnerabilities is an extremely time-consuming task. Almost three-quarters of ITOps say they spend four minutes or more manually patching third-party software per endpoint and nearly **20%** spend 10 minutes or more on this task. An automated solution that can patch the most popular third-party applications including Java, Adobe Flash, Google Chrome, and Microsoft Office, can lead to significant time savings and management efficiencies.

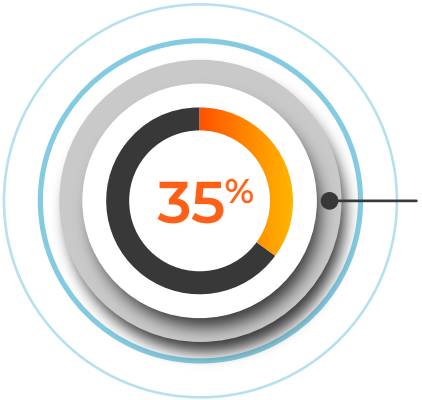




Barriers to automation

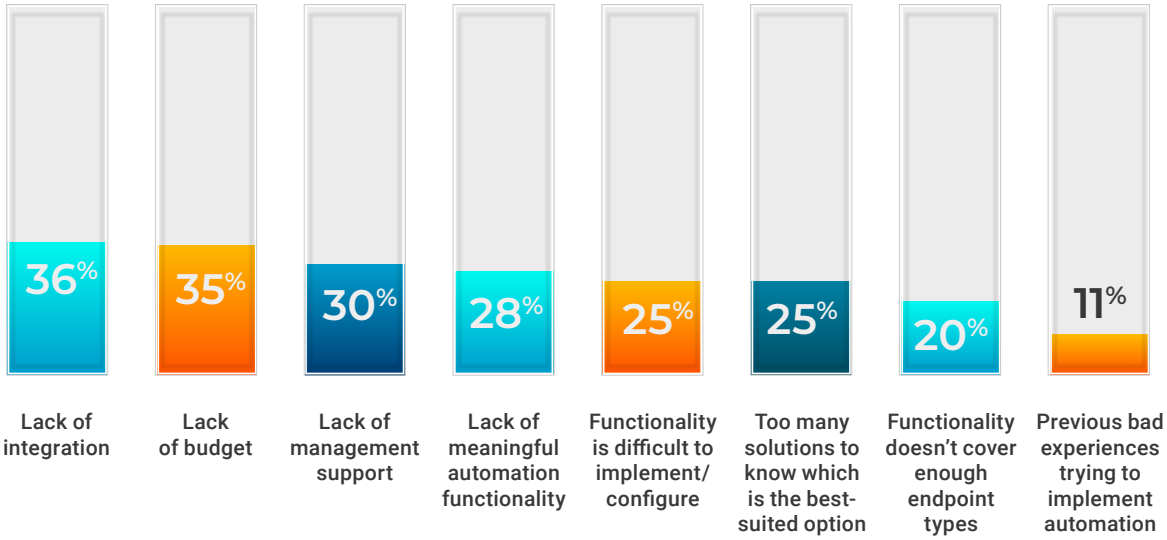
While automation is on the rise, not everyone has embraced it.

The top obstacles keeping organizations from further automating are inconsistent functionality across tools, lack of budget, and lack of management support.



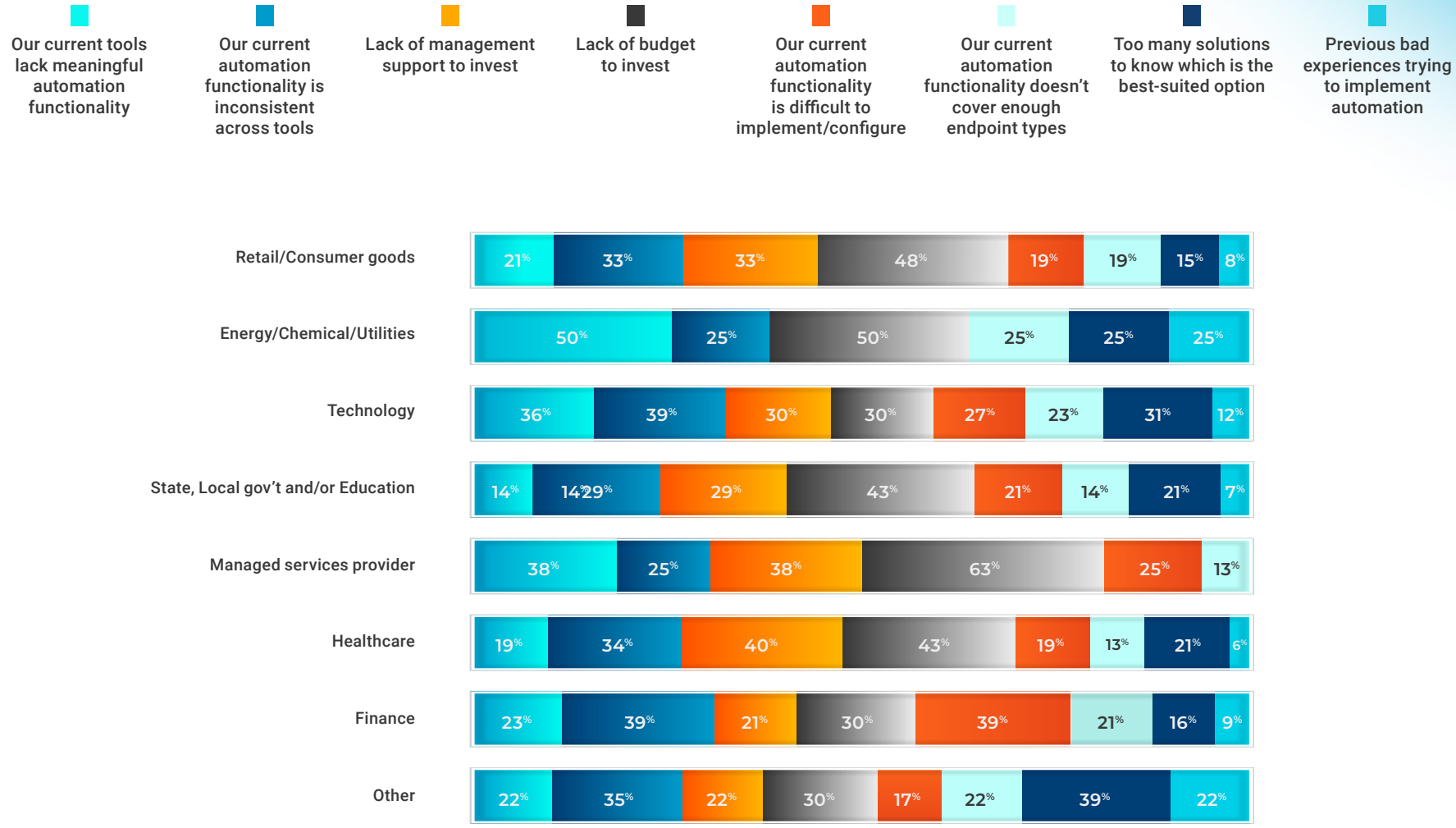
Of ITOps environments are still only partially or slightly automated

What obstacles are keeping your organization from further automating its endpoint management?



While lack of budget is the biggest factor for most industries, the finance and healthcare industries cited their biggest barrier as having current automation functionality that is inconsistent across tools. A lack of management support to invest in new automation solutions was also a key barrier for most industries.

What obstacles are keeping your organization from further automating its endpoint management?



Trust in automation is growing

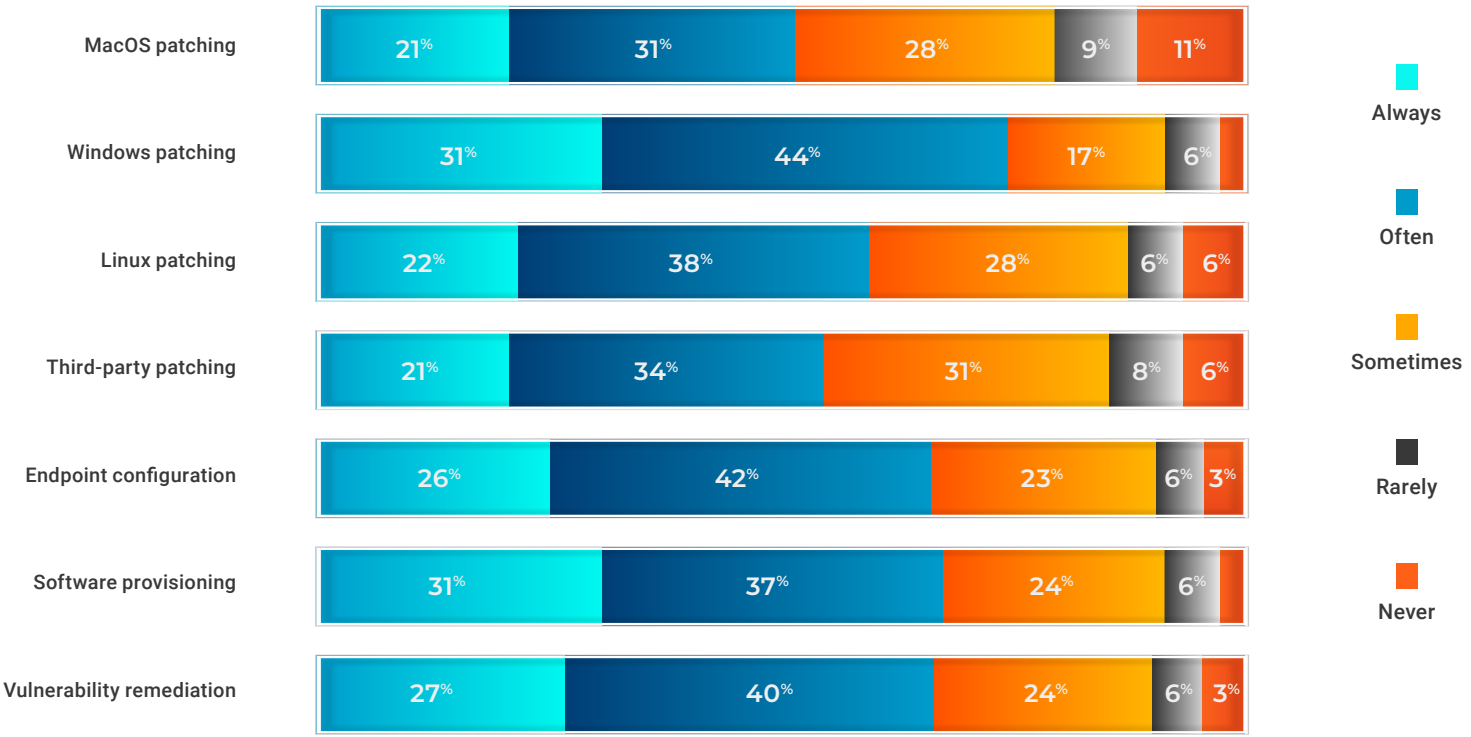
As automation tools have been introduced into the IT environment, winning ITOps trust that automation can be effective and won't create more headaches or errors than manual processes has been an ongoing challenge. However, as adoption of automation continues to increase, so has trust in automated solutions.

- **64% of ITOps professionals always or often trust automation**

Where a lack of trust in automation has stalled some automation efforts, the most common reasons ITOps professionals gave were security concerns, worries that errors wouldn't be caught or caught too late, and a desire to have more control or ability to oversee processes.

Windows patching, endpoint configuration, and software provisioning are the most trusted tasks for automation while macOS and third-party patching are the least trusted tasks.

Do you (or would you) trust automation for the following tasks?



Cloud Trends for ITOps

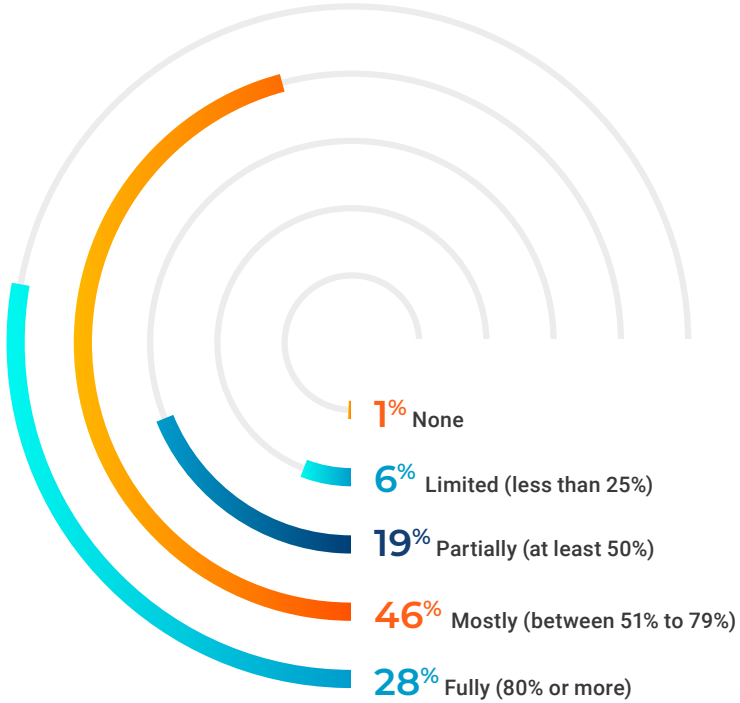
Cloud trends for ITOps

Adoption of cloud-native endpoint management solutions is already strong, with **74%** of organizations saying they are cloud-based. However, there is still room for growth.

- **Only 28% of organizations are fully cloud-based.**

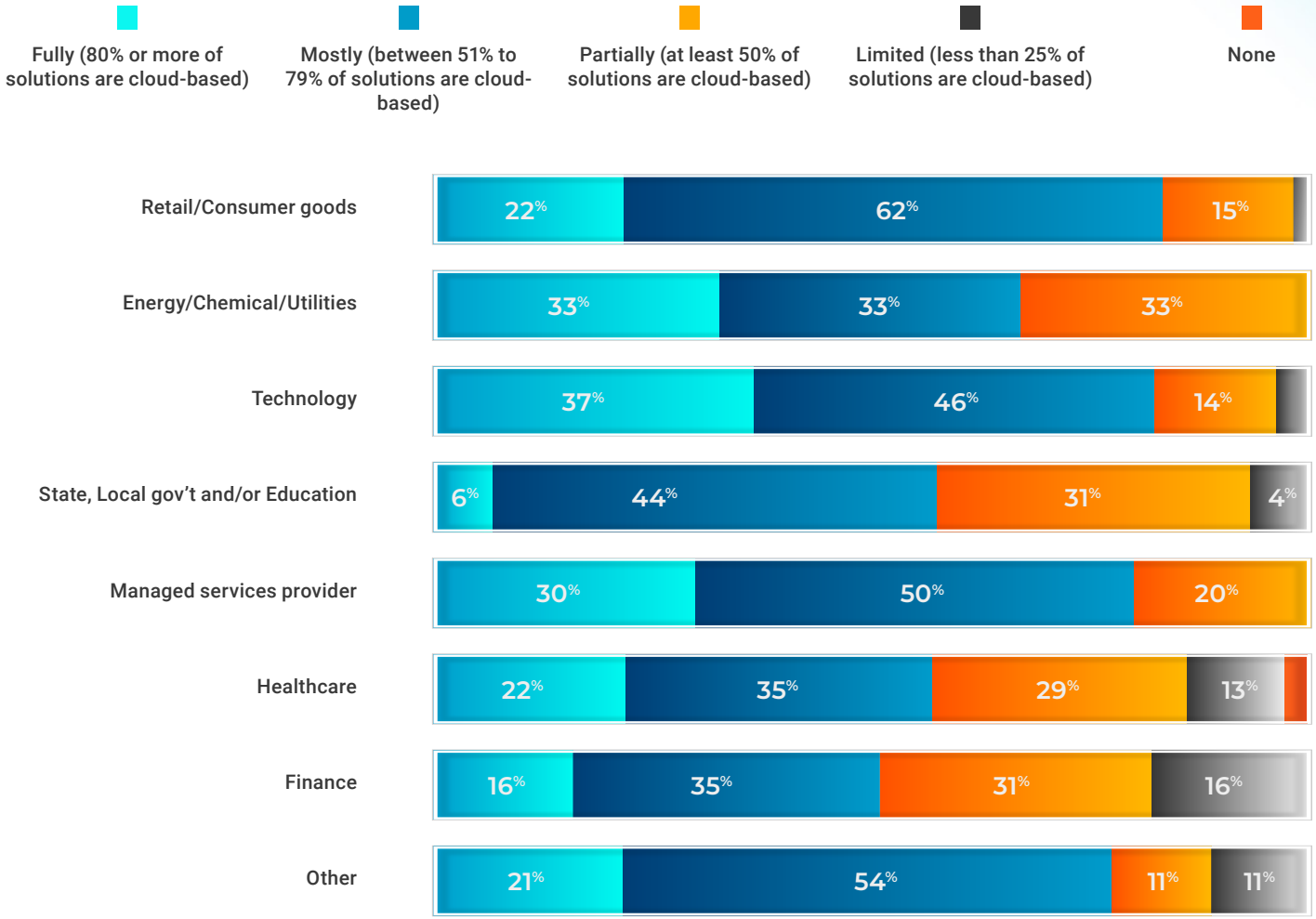
In 2022, only **23%** were extensively cloud-based, which shows there has been growth in full cloud adoption, but it's happening at a very gradual pace.

Currently, to what extent is your organization's overall environment cloud-based?



Cloud adoption by industry

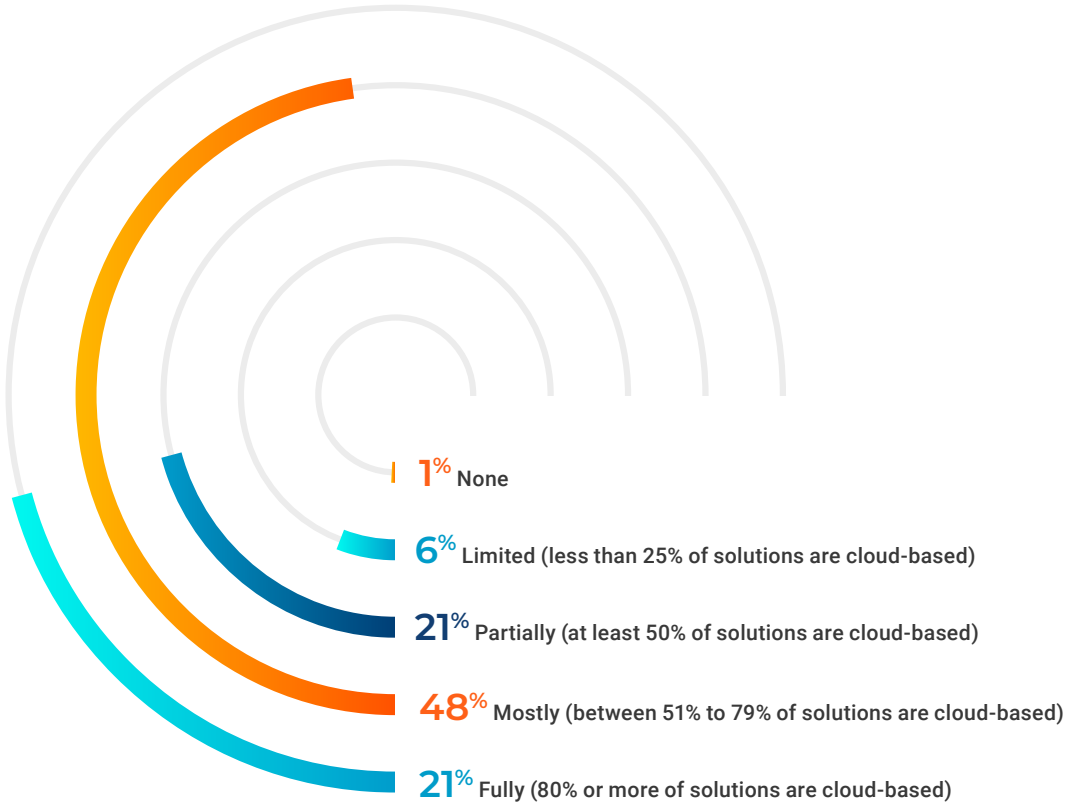
The state/local government, finance, and healthcare sectors are significantly less likely to be fully cloud when compared to retail, technology, and MSP organizations.



ITOps are moving to the cloud for endpoint management

Similar to overall cloud adoption trends, only **21%** of organizations fully use cloud-based solutions for endpoint management. However, **69%** fully or mostly use cloud-based solutions.

Managed services providers, retail, and technology are the top users of cloud-based solutions

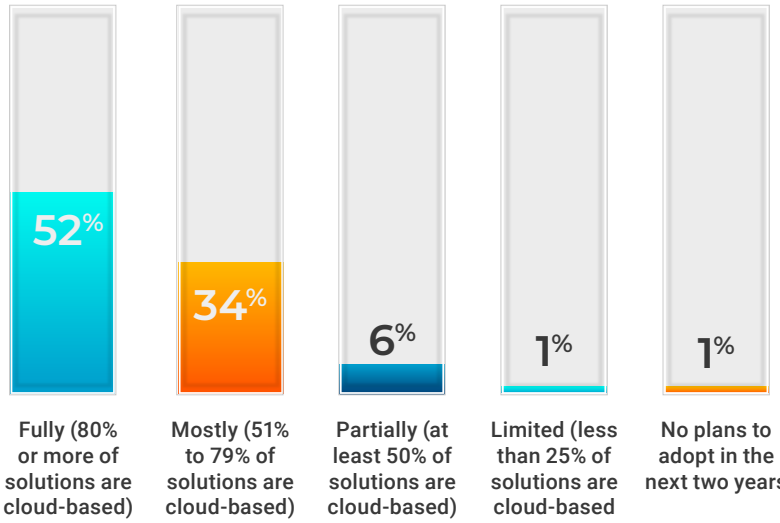


Organizations continue to shift to more cloud-based endpoint management solutions.

Despite full cloud adoption being still less than a quarter of all companies, most organizations plan to continue to increase the use of cloud-based endpoint management solutions

31% more organizations plan to be fully cloud-based within 2 years than are currently

To what extent does your organization plan to increase the adoption of cloud-based solutions for endpoint management in the next 2 years?



Benefits of cloud-native solutions

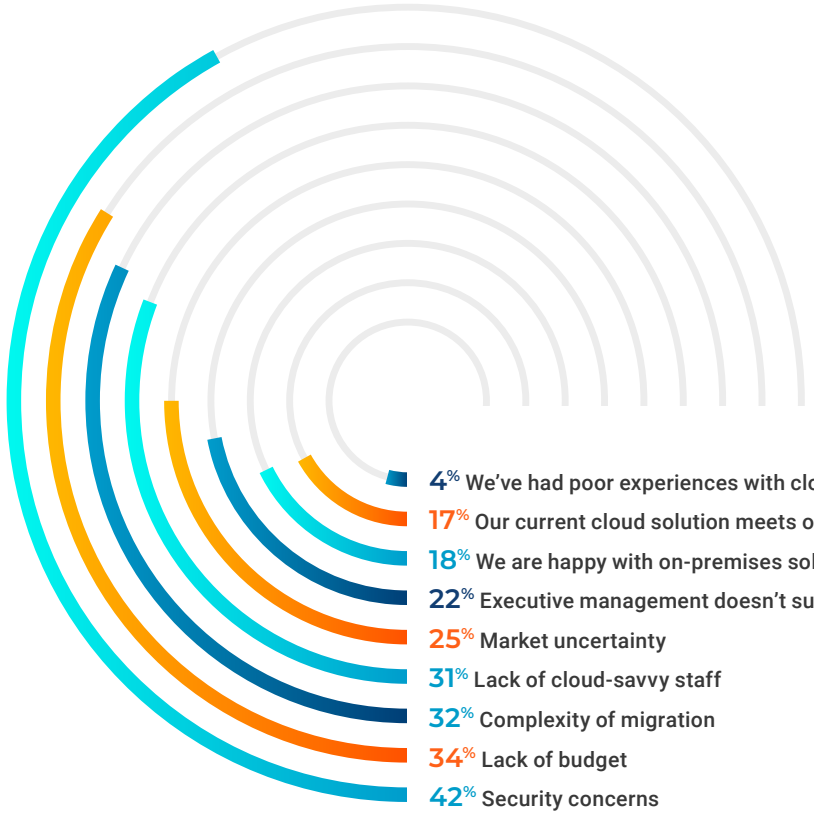
Findings from our survey clearly show that respondents see the value in adopting cloud-native solutions over legacy on-premises tool sets or hybrid models. Key benefits include:

If organizations committed to moving all their IT solutions to the cloud, they would quickly realize that the costs to stay with the same on-premises patching and endpoint management tools are far more expensive than the cost to shift to a modern cloud-native patching and endpoint management solution.

Barriers to greater cloud adoption

Security concerns, lack of budget, and complexity of migration to the cloud are the key reasons organizations aren't increasing the adoption of cloud-based solutions.

What obstacles are currently limiting your organization from increasing the adoption of cloud-based solutions?



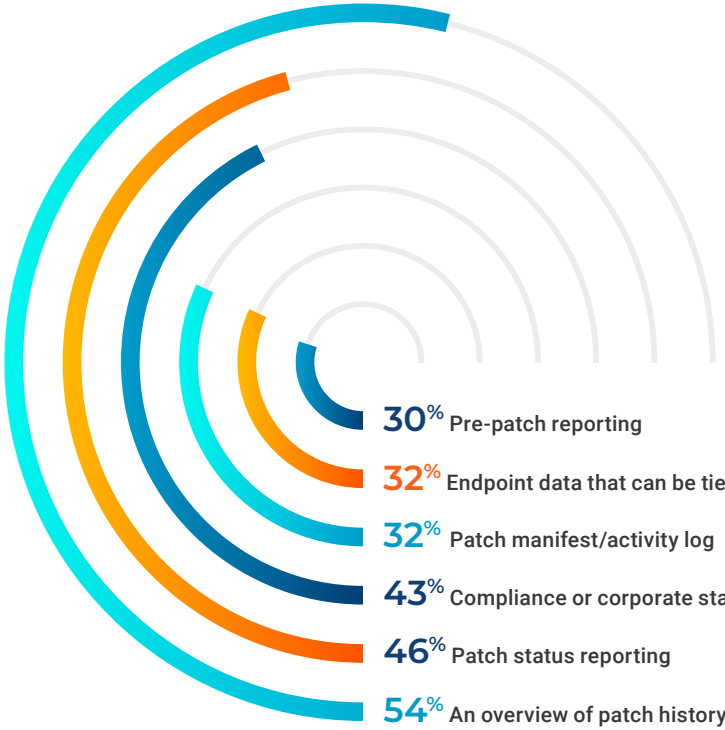
How Companies are Selecting Endpoint Management Solutions

Organizations want an all-in-one solution

Because of the number of endpoints and devices ITOps teams have to monitor, keeping track of it all can get complicated quickly, which is driving more organizations to look for an all-in-one solution that can provide everything from patching to remote access in a single platform.

Reporting features are also important, as they are useful in quickly identifying issues and remediating them. ITOps professionals indicated they used reports on patch history, patch status, and compliance reporting most frequently.

From an endpoint management perspective, what type of reports are most important to you?



30% Pre-patch reporting

32% Endpoint data that can be tied to other data sources

32% Patch manifest/activity log

43% Compliance or corporate standards reporting for executive management

46% Patch status reporting

54% An overview of patch history, applied patches, and outstanding patches by severity and age

Cloud-native, all-in-one solutions for the modern workforce

As organizations look to increase efficiency and reduce complexity, it's important to recognize how certain solution capabilities drive greater efficiency gains and simplify the IT environment. A cloud-native platform enforces OS and third-party patch management, configurations, and custom scripting across on-premises, remote, and virtual endpoints, enabling ITOps teams to dramatically reduce the time, complexity, and effort required to effectively manage endpoints.

In addition, the right solution should also be:

1

Simple

Capabilities that allow ITOps teams to remediate and patch vulnerabilities, deploy required software, fix misconfigured systems, and instantly access devices to assist users from anywhere — without the need for multiple tools or connections via VPN — significantly simplify and speed endpoint management.

2

Efficient

Automation capabilities such as patching, configuring, and vulnerability remediation can deliver significant efficiency gains.

3

Extensible

Extensibility through API reduces the number of tools required, eliminating complexity, and making administrative tasks faster and simpler.

4

Cross-platform

A solution that works across platforms, including Microsoft Windows®, macOS®, and Linux® platforms provides complete visibility no matter the platform.

End the Complexity

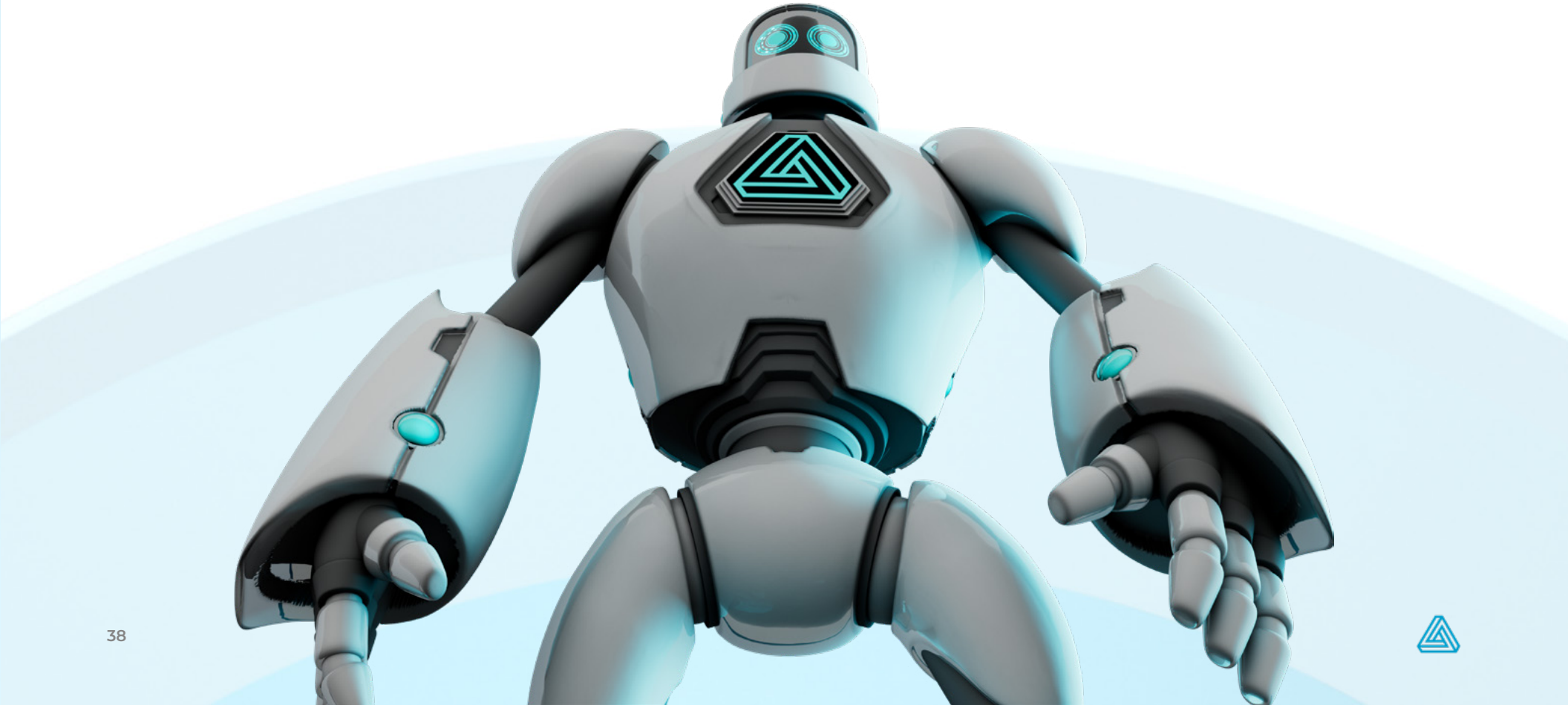
Today's IT teams have been handed a lot to manage: multi-cloud environments, a growing number of devices of varied operating systems, and an increasingly distributed workforce. At the same time, companies are constantly looking for ways to cut costs, increase efficiency, and simply do more with less.

The practicality is that without the ability to add significant efficiency to how endpoints are managed, it becomes near impossible to identify and remediate endpoint issues in a timely enough manner to avoid security gaps and productivity impacts across the modern workplace.

The cloud, combined with automation, is the answer for a secure, scalable, and efficient way to simplify the complexity and stay on top of endpoint management, which is why, as this study has illustrated, almost every organization is continuing to move toward an environment that fully embraces the cloud and automation. Those that do it faster, will have more agility and a competitive edge.

About Automox

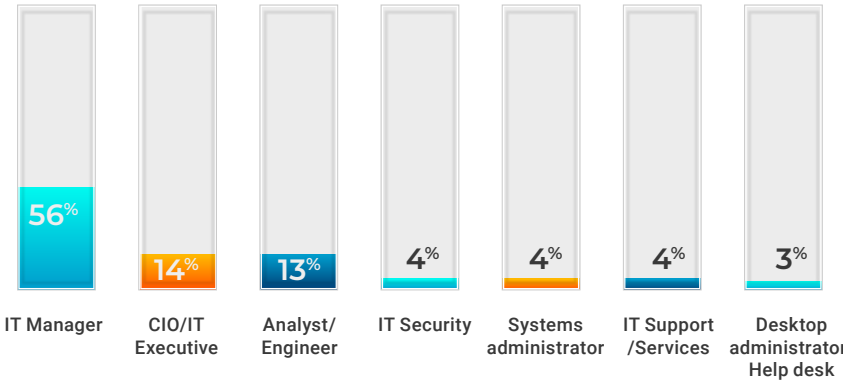
Automox is the cloud-native IT operations platform for modern organizations. It makes it easy to keep every endpoint automatically configured, patched, and secured — anywhere in the world. With the push of a button, IT admins can fix critical vulnerabilities faster, slash cost and complexity, and win back hours in their day. Join thousands of companies transforming IT operations into a strategic business driver with Automox.



Study methodology

Automox surveyed 451 U.S.-based ITOps professionals at organizations with 200-5,000 employees. The survey has a 95% confidence, +/-%5 margin of error and was conducted in November 2022.

Level of responsibility



Industries