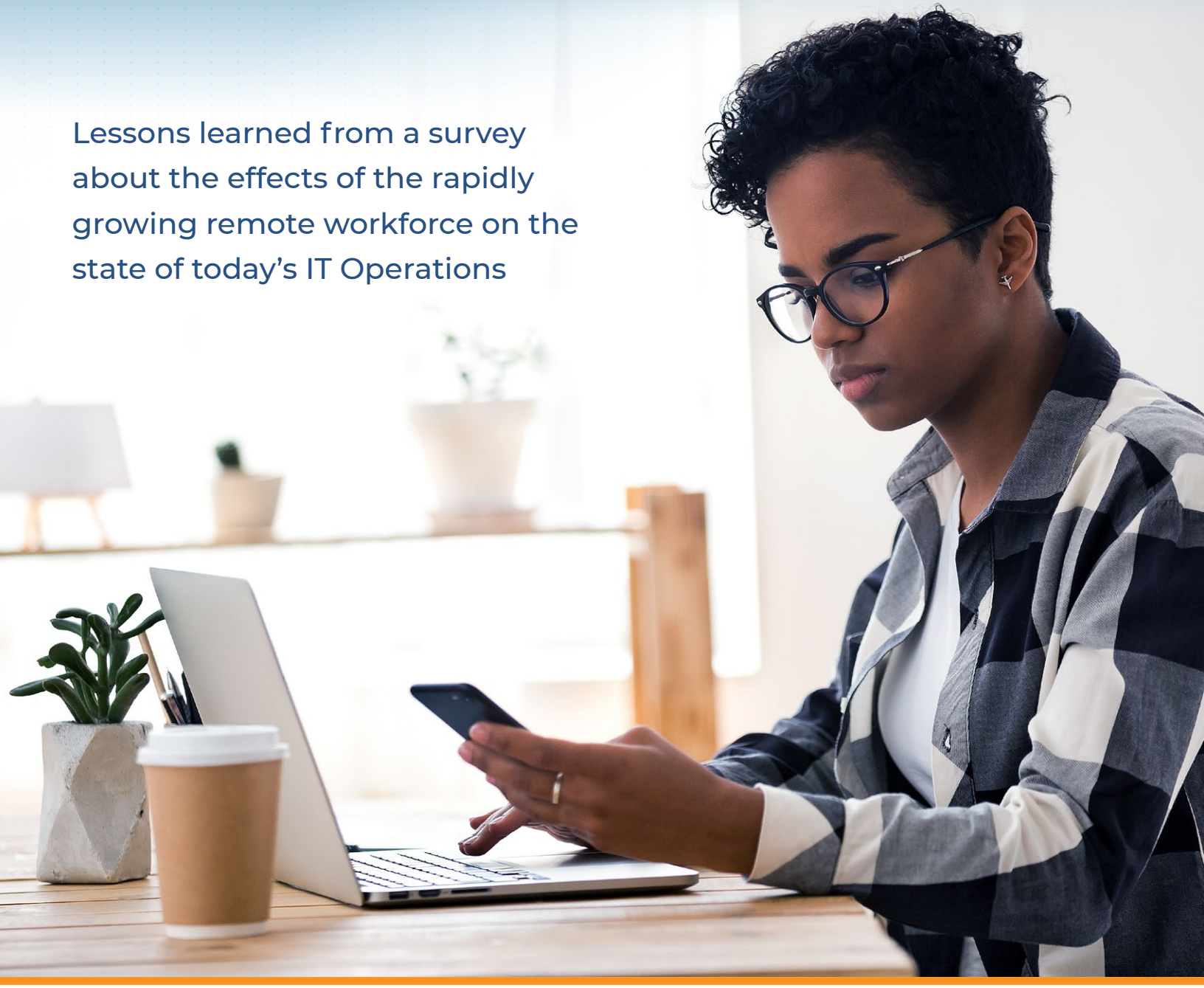
AimPoint Group
high-impact marketing

2021 STATE OF IT OPERATIONS

THE RISE OF THE REMOTE WORKFORCE

Lessons learned from a survey about the effects of the rapidly growing remote workforce on the state of today's IT Operations



SPONSORED BY AUTOMOX

Contents

IT Operations in a Remote World

Doing business in 2021 looks dramatically different than in years past. Few could have imagined that within the span of a few months, the majority of organizations would have their business and technology models completely upended.

To adapt and survive in this new normal, companies took swift action in 2020 to implement and support an almost entirely remote workforce. The effort companies made to keep employees and customers safe while maintaining business operations has been truly inspirational. But that effort was rushed, leaving IT Operations with the overwhelming, if not impossible, task of managing thousands of new devices, endpoints and support requests remotely.

FROM CHAOS TO OPPORTUNITY

We enter 2021 on much more solid footing, but also with the understanding that we will not be returning to what we once considered "business as usual." The remote workforce is here to stay, and businesses are finding there can be tremendous upside to embracing this new way of working, including huge cost savings and happier, more productive employees. But there is also tremendous work to be done to effectively manage, maintain and support a distributed, remote workforce long term.

This report sheds light on how organizations are responding to this new normal, using data from a survey of 501 IT operations and security professionals at enterprises with between 500 and 25,000 employees, across more than 15 industries and government agencies. Our goal is to help readers benchmark the performance of their organizations against peers and develop insights into how to make improvements that will pay off.

MOVING BEYOND PHYSICAL CONSTRAINTS

Organizations are now moving to a position of proactive strategic decision making. It is no longer about stemming the tide but instead finding ways to operationalize and optimize the remote workforce to improve business outcomes.

User experience is now essential to success — remote employees need 24x7 access across devices to the corporate information, systems and tools they need to do their jobs. But this experience is eroded due to the difficulties or burden of physically reaching a device in a remote-only world. As organizations push outside the boundaries of their traditional networks with remote workers and increased use of mobile, solutions that rely on on-premises tools will fail to keep up.

WHY CLOUD-NATIVE IS THE FUTURE OF IT OPS

Today's infrastructure needs to reflect the way we now work and conduct business — on-demand and without boundaries. Traditional on-premises, cloud-hosted and hybrid cloud infrastructures lack the agility and flexibility to meet the 24x7 needs of a remote workforce. In all of these approaches, companies are weighed down because at some point in their infrastructure, they will require ongoing physical maintenance, upgrades, troubleshooting and more.

Our new normal requires a new approach — automating remote IT operations capabilities using cloud-native approaches to enable real-time visibility and control over diverse, shifting IT environments. Cloud-native is an on-demand, elastic, multi-tenant service, accessible anywhere from any device, and with usage that is measured and monitored. An agile native-cloud approach is different from all other on-premises, hybrid and cloud approaches because it:

- Offers quick deployment
- Requires zero maintenance
- Provides the scalability for organizations to evolve and grow without boundaries
- Enables real-time visibility and control over diverse, shifting IT environments

WHAT THE DATA SHOWS

These are important advantages in theory, but are they on the minds of today's IT Operations professionals? Is there really a need to replace on-premises and non-cloud-native approaches to gain visibility and control over diverse IT environments? This survey data explores how participants see today's companies struggling with their existing models to manage their IT Operations, and what they need to optimize the remote workforce experience.

Summary of Findings

- **Enterprises expect the remote workforce is here to stay and are making investments to optimize remote IT operations management.**

  Survey insights show that organizations have largely accepted that a mostly remote workforce has become the new standard. Having added more endpoints that are increasingly diverse and distributed, a clear majority of enterprises are struggling to effectively manage remote IT operations using traditional models built for on-premises management. Responses show that many businesses are investing in cloud-native solutions to drive greater automation and visibility across operations and reduce reliance on physical hardware and appliances.

- **Tools, not people, are hindering IT Operations' ability to perform essential remote management functions.**

  Organizations responded quickly to mobilizing the rising remote workforce, providing workers with 24x7 access to the necessary corporate resources required to maintain productivity and business operations. Insights from the survey reveal that the scale and scope of requirements for effective remote IT management have gone beyond the limitations of organizations' manual-based processes and on-premises tools. The difficulty of managing and maintaining multiple, inflexible tools across distributed sites has resulted in inconsistent uptime for remote employees and a lack of visibility for IT Operations.

- **Enterprises are least confident in their ability to manage IT Operations beyond the perimeter.**

  Whether it's managing IT components, patching endpoints, or responding to critical vulnerabilities, organizations face more challenges when it comes to remote IT management operations.

- **Automation is underutilized and deemed critical to enabling the remote workforce without boundaries.**

  The majority of organizations admit they are not currently leveraging the full value of automation for remote operations management. However, they believe automation holds the key to driving greater agility, security, productivity and visibility across remote IT operations, and they are making investments to reap those benefits.

- **Enterprises are embracing cloud-native solutions to better enable and empower the remote workforce.**

  Organizations find themselves struggling to support the new demands of the remote workforce with traditional management models. As a result, cloud-native adoption is on the rise, expected to more than double over the next two years. Participants likely see the value of adopting a cloud-native model over legacy on-premises or hybrid approaches being real-time visibility, quick deployment, zero maintenance and the ability to easily scale.

The Effects of the Rapidly Growing Remote Workforce

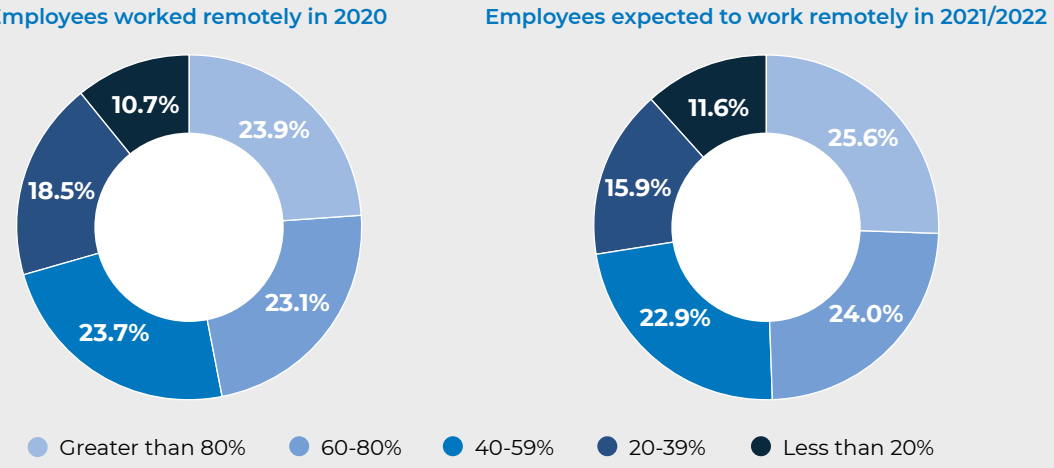
The rapid rise of the remote workforce has created a ripple effect across employees, employers, departments and technology decisions. Knowing the full impact of this chain of events is critical to determining next steps to optimize remote IT Operations.

IS THERE EVIDENCE THAT THE REMOTE WORKFORCE IS HERE TO STAY?

Absolutely! As we know, unprecedented numbers of employees ended up working remotely in 2020 in response to the forced quarantines. Survey results show that respondents don't anticipate things will go back to "normal," instead expecting a larger percentage of employees will work remotely in 2021/2022 vs. 2020.

FIGURE 1: REMOTE WORKING IS THE NEW STANDARD

What percentage of your organization's employees worked remotely (either part or full time) in 2020, and what percentage is expected to work remotely in the future? (n=497)



Specifically, half of all survey participants expect that over 60% of their organizations' employees will be working remotely in 2021/2022. These results are consistent with market analysis that finds employees and employers alike support the continuation of a larger remote workforce.

A recent survey[1] from Global Workplace Analytics found that over half of adults want to work remotely most of the time after the pandemic, and close to one-third of the workforce is expected to be working from home multiple days a week by the end of 2021. Aside from increased worker satisfaction, the financial upside for employers is the ability to save up to $11,000 per year for each employee that works remote at least 50% of the time. That translates into millions of dollars saved for companies with over 100 employees.

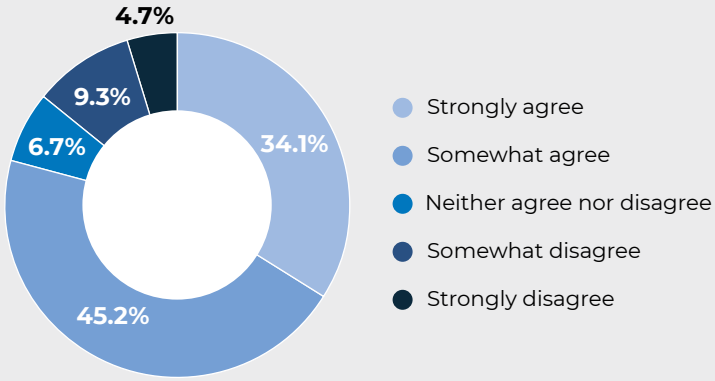
1. https://globalworkplaceanalytics.com/work-at-home-after-covid-19-our-forecast

HAS THE SUDDEN SHIFT TO A MOSTLY-REMOTE WORKFORCE CREATED NEW DIFFICULTIES FOR IT OPS?

Definitely, yes. Close to 80% of those surveyed agree that the process of managing endpoints has become harder as a result of the shift to more employees operating remotely. The challenges are markedly greater for smaller organizations because they have fewer mature tools, standard processes, and IT resources in place to manage a dynamic workforce.

FIGURE 2: THE IMPACT OF THE GROWING REMOTE WORKFORCE ON MANAGING ENDPOINTS

Describe your agreement with the following statement: "The process of managing our endpoints (i.e., patch, re-configure, and inventory software for laptops and desktops) has become harder as a result of the shift to more employees operating remotely." (n=493)



The fact that most organizations maintain several tools in house to manage their endpoints already poses a challenge to IT Operations. The growing remote workforce has exacerbated and further complicated the situation as organizations have added more endpoints that are increasingly diverse and distributed with a continuous growing list of issues to remediate.

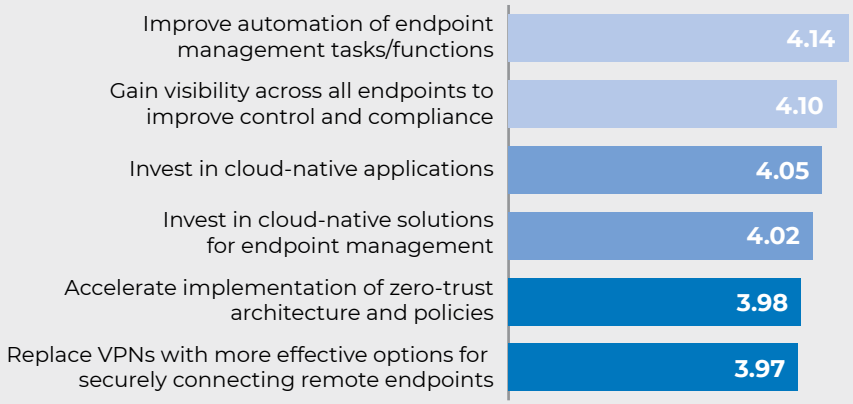
IT Operations now has numerous tools to manage endpoints across multiple operating systems. These systems are built upon largely on-premises architectures, which limits the possibility of using automation for repetitive tasks. This clunky, slow and on-premises approach to endpoint management is a huge barrier to organizations looking to streamline and optimize the remote workforce and improve the user experience.

HAS THE GROWTH OF THE REMOTE WORKFORCE MOTIVATED ORGANIZATIONS TO MAKE TECHNOLOGY CHANGES AND NEW INVESTMENTS?

Remote workforces operate in a digital world where continuous access to information, tools and systems is critical to maintaining business continuity and productivity. In response to this new reality, participants ranked automation of endpoint management tasks/functions and visibility across all endpoints as the top investments they plan to make in 2021.

FIGURE 3: TARGETED AREAS FOR IMPROVEMENT AND INVESTMENT IN 2021

On a scale from 1-5 with 5 being the highest, rate the extent that having an increasingly remote workforce is influencing your organization to make the following changes / improvements in 2021. (n=501)



Many participants see cloud-native applications as the key to providing the automation and visibility necessary to enable a continuous and streamlined remote user experience. Already hamstrung by on-premises and hybrid cloud architectures, organizations feel the pain and limitations associated with trying to manage endpoint connections for a workforce no longer within the four walls of the office.

With a cloud-native approach, organizations can use cloud-based tools to manage and apply the latest software updates to servers, desktop computers, and laptops across an organization without complex infrastructure or VPN requirements. This approach saves significant time and money compared to traditional management solutions.

Current State of Automation

Automation of IT management processes can address the challenges described above by dramatically speeding up IT management tasks, thereby:

- Enabling existing IT operations staff to manage more systems with less effort
- Reducing the amount of system and application downtime needed for IT management and maintenance

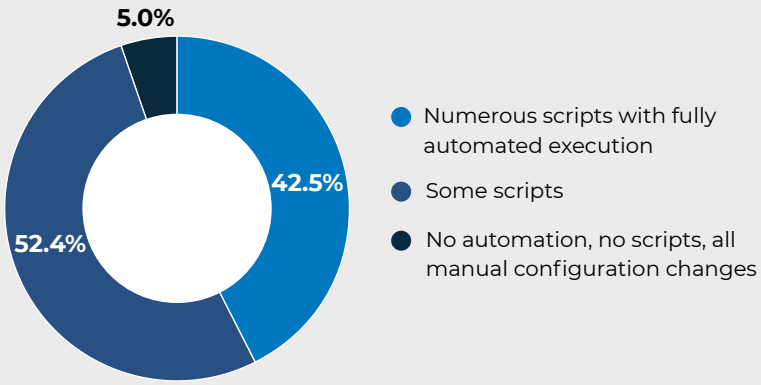
Part of automation in this context means scheduling and automatically managing activities like scanning systems for software and vulnerabilities, collecting data, analyzing what needs to be done, and reporting on successful and unsuccessful tasks. But the other critical, and in practice more challenging, aspect of automation involves managing scripts for tasks like installing and configuring software updates on endpoints and for performing tasks like fixing misconfigurations and closing ports.

ARE ORGANIZATIONS LEVERAGING THE VALUE OF AUTOMATION WHEN IT COMES TO ENDPOINT MANAGEMENT OPERATIONS?

Close to 60% of respondents are either using no automation at all or have only developed some scripts. The degree of automation is progressively less for smaller organizations compared to larger ones, likely due to fewer resources and solutions.

FIGURE 4: CURRENT LEVEL OF AUTOMATION FOR MANAGING ENDPOINTS

Which option best describes your organization's level of automation for endpoint management operations such as patching, changing configuration settings, and inventorying software? (n=494)



A surprising 42% of participants say their organizations are fully automated — which begs the question: What is considered true automation in 2021?

Many organizations create ad hoc scripts to automate a specific task. They may even chain a few scripts together to mimic the idea of automation. While this may be useful for the short term, it can cause tremendous confusion and vulnerabilities in the long term. What happens when the architect of that script leaves the company or goes on vacation? Are these scripts fully documented and easily visible to others?

True automation implies systematic, programmatic support. It involves not just workflow, but orchestration engines and the tools and techniques to achieve that outcome.

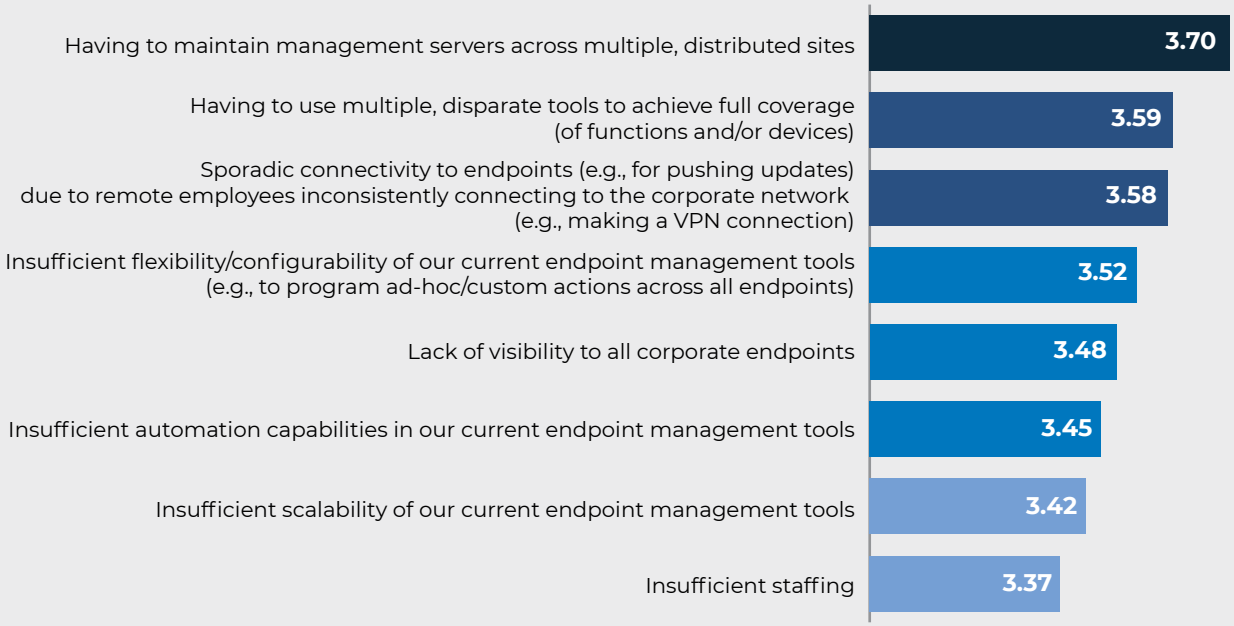
WHAT FACTORS ARE HINDERING IT OPERATIONS' ABILITY TO PERFORM ESSENTIAL ENDPOINT MANAGEMENT FUNCTIONS?

Survey data shows that the biggest issues impacting IT Operations aren't related to people, but to tools. For years, insufficient staffing has been considered one of the largest impediments to effective IT operations management: too many alerts, too many patches, too many vulnerabilities, too many requests, and never enough people to manage them all. However, the survey results show that this paradigm has been turned upside down, with insufficient staffing now falling to the very bottom of the list.

Instead, respondents cited their biggest issues being the difficulty of managing and maintaining multiple, inflexible tools across distributed sites and the resulting inconsistent uptime for remote employees and a lack of visibility for IT Operations.

FIGURE 5: IMPEDIMENTS TO PERFORMING ESSENTIAL ENDPOINT MANAGEMENT FUNCTIONS

On a scale of 1 to 5, with 5 being the highest, rate how the following negatively affect the ability of your organization's IT and Security Operations teams to perform essential endpoint management functions — such as patching, making configuration changes, and inventorying software for desktops and laptops. [n=501]



Many, if not most, employees are now working remotely via the Internet and using mobile devices. The workplace has moved beyond the perimeter of the physical office, but traditional infrastructure models weren't built to support this new reality.

According to Forrester, in a normal year, just 5% of global information workers (people that use a smartphone, PC, or tablet for work) primarily work from home.[2] With that number skyrocketing in 2020, so too did the number of endpoints IT Operations is now responsible for managing, including both personal-owned and corporate-issued desktops, laptops, mobile devices and wearables. The sheer volume of these new endpoints is enormous and requires a more sophisticated, automated approach to management.

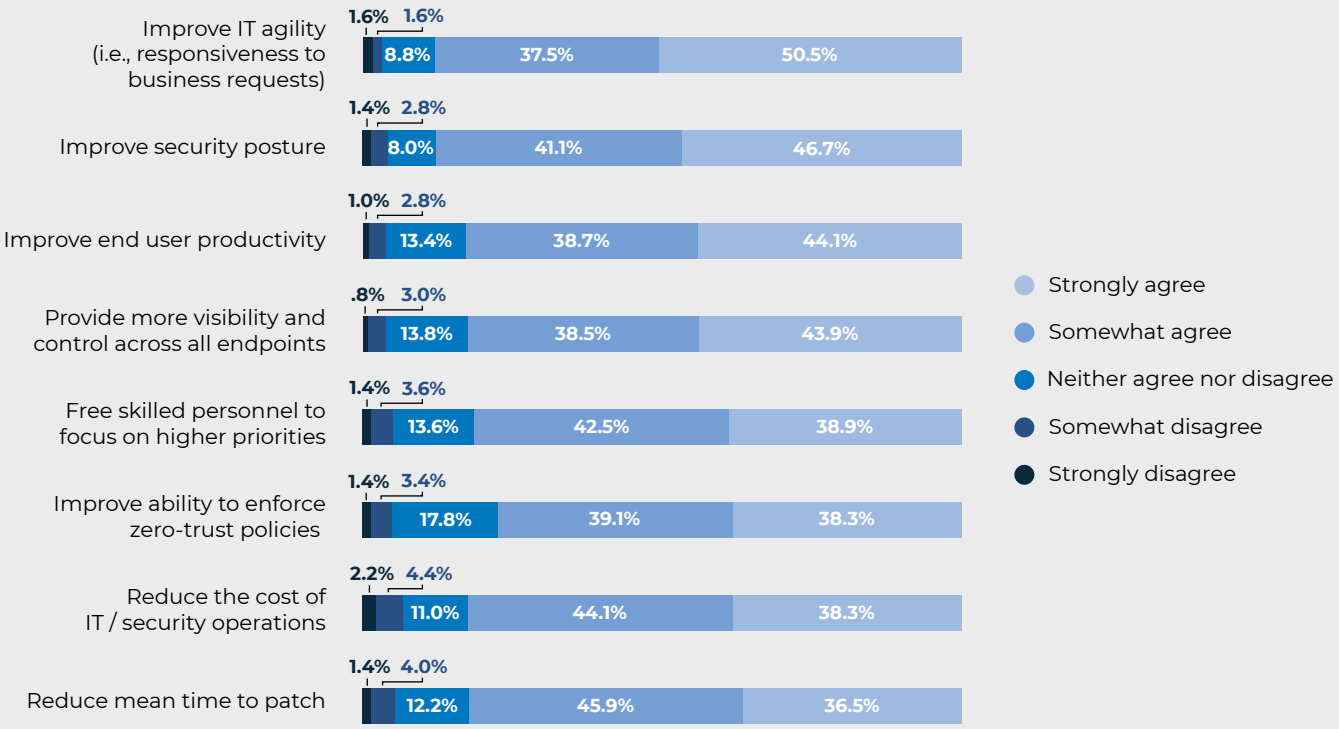
2. https://www.forrester.com/report/The+State+Of+Remote+Work+2020/-/E-RES139899

DO PARTICIPANTS BELIEVE AUTOMATION WILL HELP IMPROVE THE STATE OF IT OPERATIONS?

Yes. Participants clearly connect automation with the ability to optimize performance and the remote end user experience. The agility to respond to business requests, improve security posture, improve user productivity and provide more visibility ranked as the top four benefits automation can deliver.

FIGURE 6: ANTICIPATED BENEFITS FROM AUTOMATION

Describe your agreement that increased automation of endpoint management capabilities can deliver each of the following benefits to your organization. [n=501]



Each of the top four benefits is essential to supporting the new demands of the growing workforce.

- **Agility:** In light of the unexpected changes and upheaval of last year, businesses recognize the importance of being able to quickly respond, adapt and pivot to market and business demands.
- **Security:** As businesses rushed to implement the technology and services needed to support their growing remote workforce, cybercriminals jumped on the opportunity to exploit the gaps within this increased attack surface.
- **User Productivity:** Improving end user productivity is one of the biggest competitive differentiators and challenges for today's businesses. It requires enabling all employees with the on-demand access they need to do their jobs — anywhere, anytime and on any personal-owned or corporate-issued device.
- **Visibility:** While existing approaches can provide great visibility, that visibility degrades as soon as the device is moved outside of the network. With workers and endpoints distributed across the country or the globe, real-time, comprehensive visibility is critical to maintaining performance, security and revenue growth.

State of IT Operations Efficiency Prompting Move to Cloud

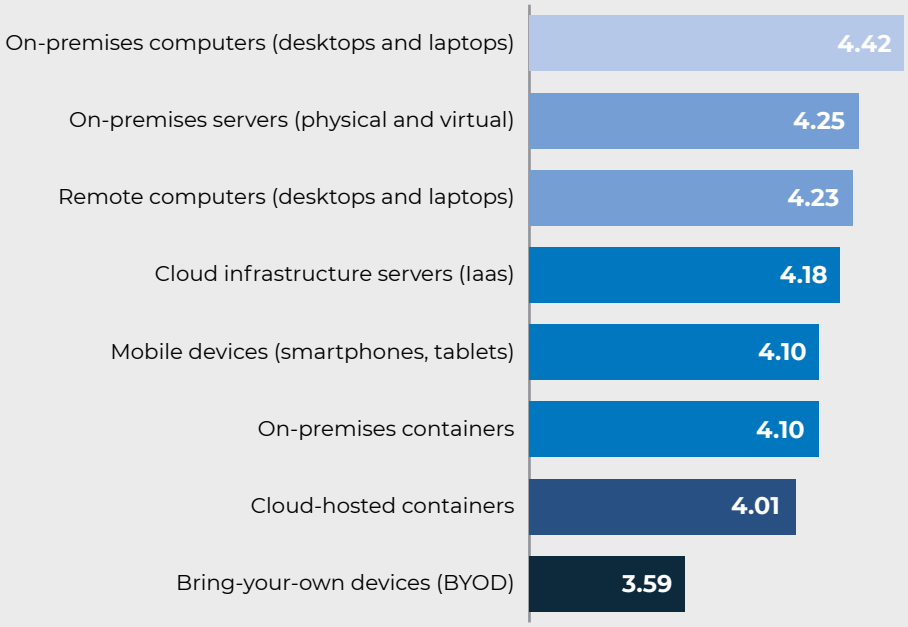
Supporting and enabling the remote workforce is demanding more from IT Operations than it can provide with current on-premises and cloud architectures.

HOW WELL ARE ORGANIZATIONS ABLE TO MANAGE REMOTE OR MOBILE IT COMPONENTS?

Survey insights show there is still a lot of progress to be made when it comes to managing components beyond the physical corporate office. Overall, participants are less optimistic about the ability to manage remote computers and cloud-based servers vs. on-premises computers and servers. A concerning insight from the survey found that organizations are struggling the most with managing bring-your-own devices (BYOD). This is a critical weakness for IT Operations, as more workers than ever before are using their own devices (smartphones, tablets, laptops, wearables) to conduct business.

FIGURE 7: OVERALL ADEQUACY OF MANAGING AND PATCHING VARIOUS ENDPOINTS

On a scale of 1 to 5, with 5 being highest, rate your organization's overall ability to manage (i.e., patch, re-configure, and inventory software for) each of the following IT components. [n=501]



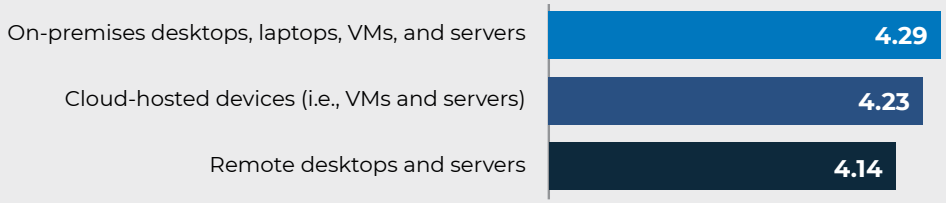
With the remote workforce expected to continue to grow, industry studies show that workers will likely accelerate their adoption of BYOD. This new way of working also demands a new way of managing IT components using automation — one with the flexibility, scalability and speed to deliver the seamless and secure, 24x7 access remote workers need to be productive.

HOW WELL ARE ORGANIZATIONS ABLE TO PATCH REMOTE AND CLOUD ENDPOINTS?

Participants say their ability to patch on-premises endpoints including desktops, laptops, virtual machines and servers is higher than their ability to patch cloud-hosted devices and remote desktops and servers. But the largest pain point by far is the ability to effectively manage endpoints for remote employees.

FIGURE 8: ADEQUACY OF PATCHING REMOTE AND CLOUD ENDPOINTS

On a scale of 1 to 5, with 5 being highest, rate the adequacy of your organization's capabilities for patching each of the following categories of endpoints. [n=501]



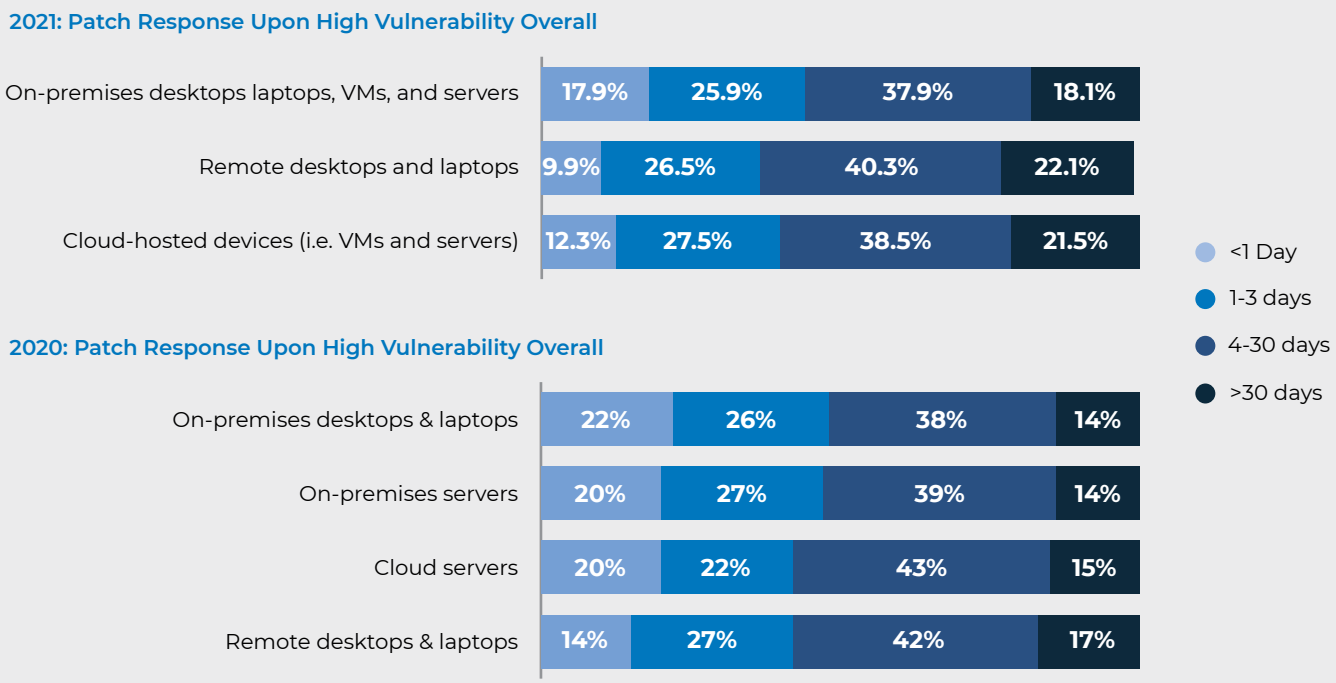
The requirements to effectively manage remote, mobile and cloud IT components and endpoints are scaling well beyond current capabilities, to a degree where adding more staff will never fix the problem. Organizations need an automated way to continuously manage, maintain and secure endpoints to support the remote workforce. By doing so, IT Operations can focus on more strategic and innovative initiatives to support ongoing market shifts and deliver better business outcomes.

ARE ORGANIZATIONS ABLE TO REACT QUICKLY ENOUGH TO CRITICAL VULNERABILITIES?

No, in fact the survey data shows that in some instances, reaction time is longer when compared to 2020. Patching times and speeds are progressively worse for cloud-hosted and remote devices, compared to on-premises devices. The year-over-year findings show that more participants, around 60%, report it takes their organization more than three days to patch cloud and remote devices. And over 20% report it still takes over 30 days to patch remote laptops, remote desktops and cloud servers.

FIGURE 9: RESPONSE TIME TO CRITICAL VULNERABILITIES

Upon announcement of a new, critical/high-severity vulnerability, how quickly on average do you patch your affected systems? (Select one option in each row.) [n=501]



Business is now conducted in a dynamic mobile-first and cloud-first world. But in many cases, IT Operations continue to support and protect the remote workforce with on-premises hardware and appliances like VPNs — designed to support users with corporate devices accessing applications and systems primarily within the physical office. These legacy solutions are complex and costly and lack the agility, flexibility and zero-maintenance demands of the digital world.

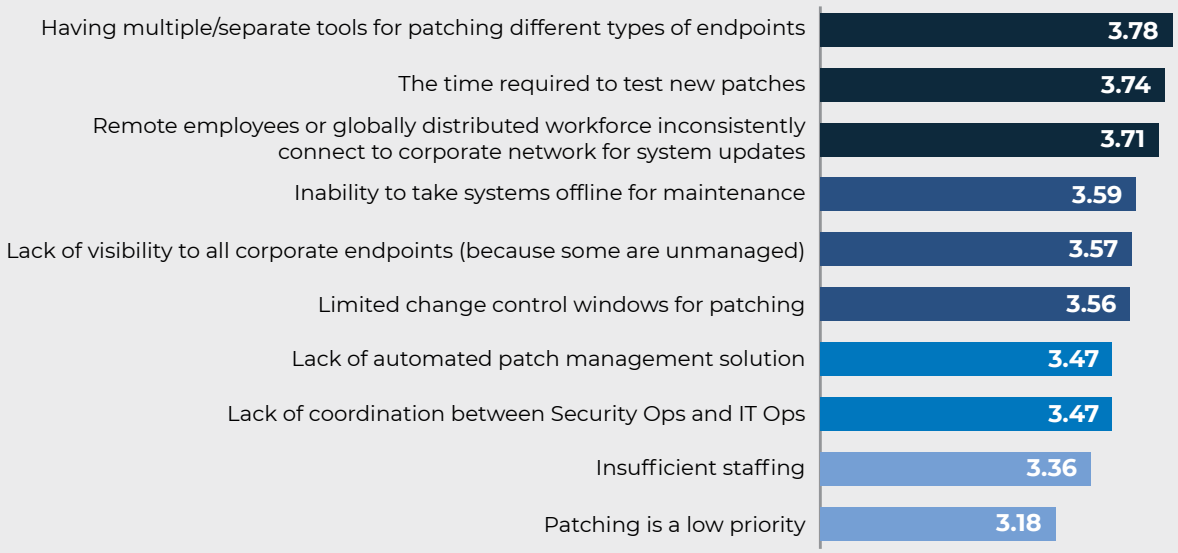
Over 20% report it still takes over 30 days to patch remote laptops, remote desktops and cloud servers.

WHAT FACTORS IMPACT THE ABILITY TO PATCH SPECIFIC REMOTE OR CLOUD ENDPOINTS?

With organizations using so many different endpoint management tools, many of which are built on legacy on-premises technology, results show that testing and patching take a considerable amount of time. This inability to keep pace with the security needs of the digital business and on-demand requirements of the remote workforce is a significant obstacle to locking down vulnerabilities as soon as possible. Exacerbating the problem is that the remote employees of a distributed workforce aren't consistently connected to the corporate network to receive the patches and updates, leaving endpoints vulnerable and out of IT Operations' control.

FIGURE 10: IMPEDIMENTS TO PATCHING REMOTE OR CLOUD ENDPOINTS

Upon announcement of a new critical/high severity vulnerability, on a scale of 1 to 5, with 5 being the highest, rate how the following inhibit your ability to patch affected remote or cloud endpoints (desktops, laptops, VMs, and servers). [n=501]



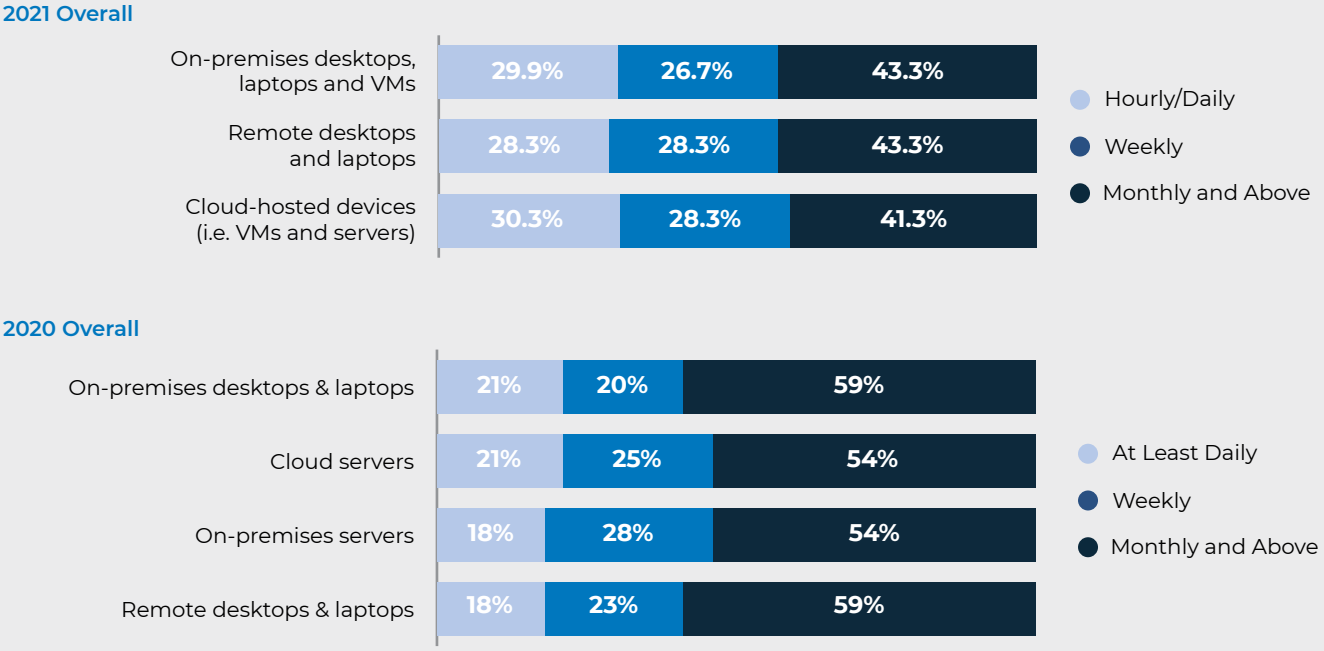
These survey results again speak to the reality that on-premises solutions that require some form of manual intervention can no longer meet the needs of a digital business. Speed to patching for severe vulnerabilities is critical and requires a level of automation most IT Operations don't have in place.

IS A LACK OF AUTOMATION CREATING GAPS AND INCREASED RISK?

Yes. Survey insights show that more than 40% of organizations harden configurations for on-premises and remote endpoints no more often than monthly. This is evidence that either patching workloads is beyond the capacity of current staff and tools, or that patch management processes are broken in a significant number of enterprises. In either case, a significant percentage of endpoints consistently remain vulnerable.

FIGURE 11: FREQUENCY OF HARDENING ENDPOINTS

Which choice best describes how frequently your organization hardens configurations for on-premises and remote endpoints? For this question, hardening involves making changes to configuration settings to improve cyber resilience, but excludes patching software or the OS. (Select one option per row.) [n=501]



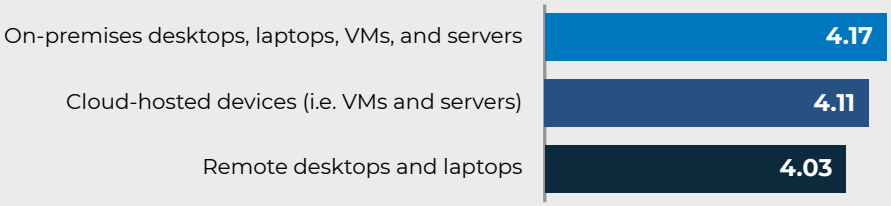
HOW ADEQUATE ARE ORGANIZATION'S ENDPOINT MANAGEMENT CAPABILITIES OTHER THAN PATCHING?

Similar to our findings in Figure 7, participants are most confident in their ability to manage endpoints (other than patching) for on-premises desktops, laptops, VMs and servers. Confidence declines with their ability to manage cloud-hosted devices, but the biggest struggle is trying to manage remote desktops and laptops.

When we compare the data of Figures 7 and 12, it's clear there is no significant difference in the minds of survey participants regarding perceived capabilities for patching versus other endpoint management functions. In either instance, managing remote endpoints is the most significant challenge and obstacle.

FIGURE 12: ADEQUACY OF ENDPOINT MANAGEMENT CAPABILITIES

On a scale of 1 to 5, with 5 being highest, rate the adequacy of your organization's endpoint management capabilities other than patching (e.g., changing configuration settings, provisioning/updating software, troubleshooting operational issues) for each of the following categories of endpoints. (n=501)

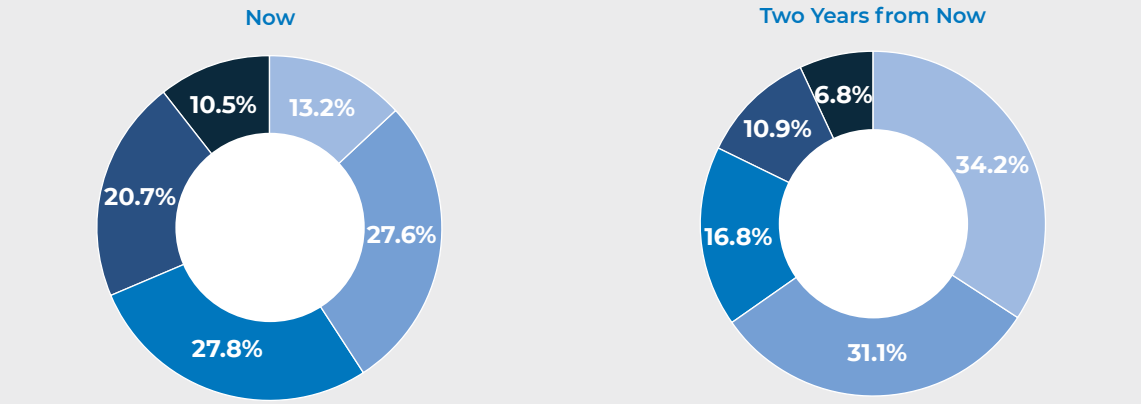


IT Operations are clearly still struggling with the ability to support the new demands of the digital world with traditional management models. In response, survey results in Figure 13 show that some organizations have already adopted a cloud-native strategy, and that number is expected to more than double over the next two years.

WHAT IS THE ADOPTION RATE FOR CLOUD-NATIVE SOLUTIONS TODAY? HOW IS THE ADOPTION RATE EXPECTED TO CHANGE IN THE FUTURE?

FIGURE 13: THE RISE OF CLOUD-NATIVE SOLUTIONS

Which option best describes the extent to which your organization currently uses and plans to use cloud-native solutions for endpoint management — including patching, making configuration changes, and inventorying software? (n=492)



The data clearly signals that participants see the value of adopting a cloud-native model over on-premises or hybrid approaches, most likely because cloud-native:

- Offers quick deployment
- Requires zero maintenance
- Provides the scalability for organizations to evolve and grow without boundaries
- Enables real-time visibility and control over diverse, shifting IT environments

Brief Introduction to the IT Operations Cloud

Not all clouds are created equal. Cloud-native is the next evolution of cloud computing designed to deliver the performance, agility and scalability the digital world requires. True cloud-native is an on-demand, elastic, multi-tenant service, accessible anywhere from any device, and with usage that is measured and monitored. How does this differ from other types of clouds?

With traditional cloud-hosted approaches:

- Software installation can be a lengthy and complex process.
- The network must be configured to enable the "cloud" application.
- Developer level resources are required to make the tool fit the specific use case.
- The application has a subscription-licensing model but is still installed locally.
- The cloud application is delivered via the organization's hosted version that is different than other customer's instances.
- Upgrades and enhancements need to be scheduled.
- Technical expertise or professional services are required to increase capacity or deploy new capabilities.
- There is no inherent method to calculate individual usage of the application.

Cloud-native is designed to meet the unique demands of today's anytime, anywhere IT. It eliminates all of the above requirements and investments, enabling IT to automate operations management at scale. Cloud-native empowers IT Operations with continuous insight into all endpoints to automatically patch remote systems, configure every endpoint, and dynamically deploy software — all without the hassles of hardware and appliances like VPNs.

A Word from the Sponsor

Today's modern, increasingly remote workforce has accentuated the need for real-time, complete visibility and control over diverse, highly-distributed IT environments. On-premises, legacy tools are disjointed and ill-equipped to meet these needs. Automox delivers a cloud-native platform for centralizing IT operations to solve complex IT workflows for modern business.

Automox is the cloud-native IT Operations Cloud platform that supports Windows, macOS, and Linux from a single console, delivered immediately and everywhere through a single agent. It enables continuous connectivity for local, cloud- hosted, and remote endpoints with no need for on-premises infrastructure or VPN connections to a corporate network. This unified platform gives IT the ability to continuously see their entire diverse environment to execute insight-driven actions at scale without complex, cumbersome tools.