

A Forrester Consulting
Thought Leadership Paper
Commissioned By Dell Technologies
April 2021

Modernize Your Server Infrastructure For Speed And Security

Infrastructure Lifecycle Automation Paves The
Way For An Adaptive, Resilient Organization

Table Of Contents

- 3** Executive Summary
- 4** Security Remediation And Provisioning Sap IT Staff's Time
- 8** New Server Buying Fueled By Infrastructure Automation And Security
- 10** Adding Contemporary Servers Helps Overcome Automation And Security Challenges
- 12** Key Recommendations
- 13** Appendix

Project Director:

Lisa Smith,
Principal Market Impact Consultant

Contributing Research:

Forrester's Infrastructure &
Operations research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

© 2021, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to forrester.com. [E-50141]



Automation and security challenges are driving new server implementation.

New servers reduce time spent on provisioning and remediating security vulnerabilities.

Executive Summary

Every business is now a digital business, regardless of industry. To deliver on the business promise, I&O leaders must focus on platforms and practices that empower employees and delight customers. The speed of infrastructure services and efficiency are just two of the underlying critical capabilities for success. As businesses evolve, they must increasingly rely on infrastructure automation to deliver such capabilities required of them. In 2020, 56% of global infrastructure technology decision-makers surveyed by Forrester reported that they are implementing or have implemented infrastructure automation software; a further 19% said that they were planning to do so in the coming year.¹ To succeed, I&O leaders must strategically implement these automated technologies to power the agility, speed of execution, security, and dependability to delight customers.

Simultaneously, as businesses risk increasing security attacks, the manual approaches of managing security threats do not scale. With increasing attack surfaces, businesses must aim for automated ways to manage every stage of the infrastructure security lifecycle. Enterprises must plan for security and automation as part of their infrastructure from the very beginning of the design phase.²

Dell Technologies commissioned Forrester Consulting to determine what is driving infrastructure upgrades. Forrester conducted an online survey with 613 IT professionals at the manager level and higher in enterprise organizations in North America, Europe, and Asia to explore this topic.

KEY FINDINGS

- › **Automation of infrastructure management often requires manual remediation, sapping IT resources.** As companies continue to automate a wide range of processes, I&O pros face mounting server security threats caused by increased threat vectors and attack surfaces. However, only 22% of IT managers feel their company is efficiently automating security policies. Ongoing server security challenges, such as controlling access, managing threats, and BIOS/firmware exploits, require remediation, which takes important IT resources away from higher-value work.
- › **Automation and security capabilities are driving investments in newer servers.** Our study found that half of IT managers anticipate adopting new servers within the next two years. As they implement this technology, 54% look for automation, 50% seek easier configuration compliance, and 33% desire continuous security innovation.
- › **I&O pros expect new servers to save them time and money.** Using new server technology, IT managers expect time savings of nearly 14% for remediating vulnerabilities and 10% reduction of IT time spent on deployments and routine IT management tasks. In addition, I&O pros estimate that new servers will help trim operating expenses by an average of 6%.

Security Remediation And Provisioning Sap IT Staff’s Time

IT departments are seeking servers with new capabilities as they work to overcome several challenges. Two of the top challenges for IT departments include automation and security. These main challenges lengthen the time and increase the effort that provisioning of IT infrastructure takes.

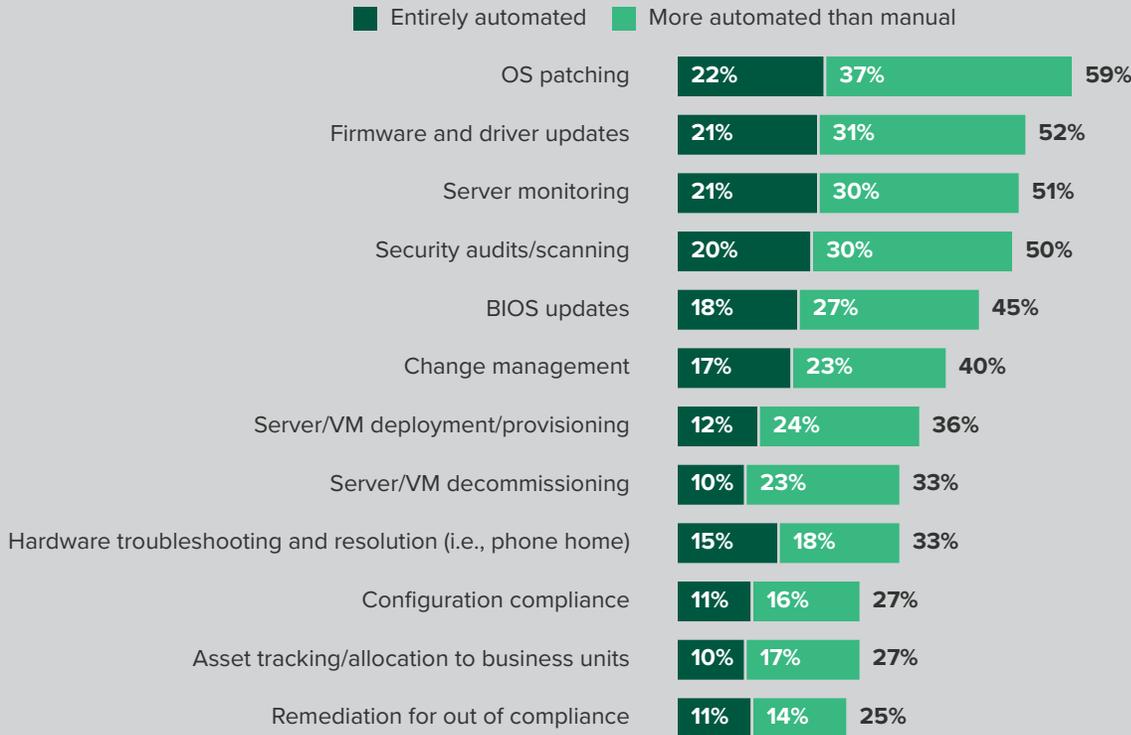
AUTOMATION OF INFRASTRUCTURE MANAGEMENT IS STEADY, BUT THE NEED FOR MANUAL REMEDIATION CONTINUES.

- > **Firms often employ higher levels of automation ...** In this study, more than half of respondents report having entirely or mostly automated their processes for OS patching (59%), firmware updates (52%) and security audits and scanning (50%). But only 27% report automation for configuration compliance (see Figure 1).
- > **... however, lack of automated security remediation increases risks.** While 61% of respondents report their organizations are extremely efficient at identifying misconfigurations, a relatively smaller 27% mention their ability to automate the configuration compliance tasks. Among respondents, 51% claim efficiencies in detecting security threats, 45% in quickly adapting security controls to change, and 40% in patching hardware security vulnerabilities. Less than a quarter report they are efficiently automating security policies across workloads.

Only 22% of IT managers feel their organizations are efficiently automating security policies across workloads.

Figure 1

“To what extent would you say each of the following server infrastructure management tasks is automated within your IT operations team?”



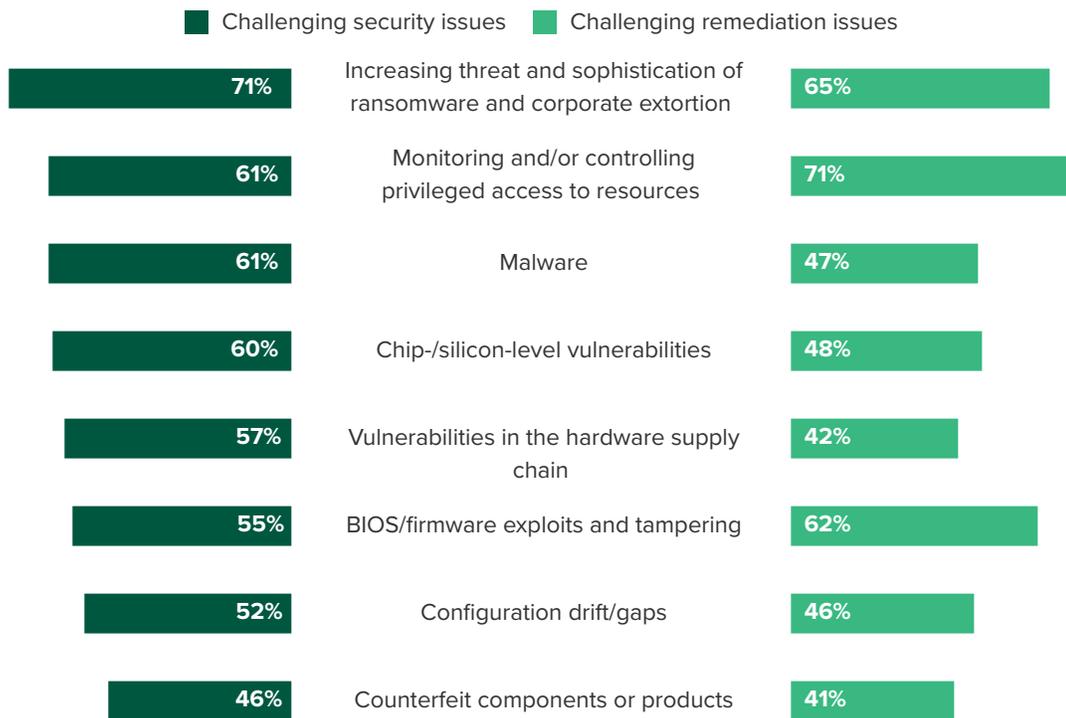
Base: 613 IT managers or above with server responsibilities
 Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, March 2021

> **I&O professionals face increased server security and corresponding remediation challenges.** Increasing threat vectors, more sophisticated ransomware and extortion risks are creating challenges as IT departments work to secure servers; 71% report this as a challenge while 65% feel challenged by the remediation of these security vulnerabilities (see Figure 2).

- More than half of respondents highlight the lack of security risk awareness and skills. Organizational factors impact security vulnerabilities as 69% of IT pros say they lack visibility across the infrastructure environment, and 61% lack a cohesive security strategy.
- Monitoring and controlling privileged access are challenging for 61%, with more than seven out of 10 decision-makers finding remediation challenging.
- More than half (55%) of respondents report challenges with BIOS/firmware exploits and tampering; 62% find remediation challenging.

Figure 2

Security And Remediation Challenges (Percentages represent 4 and 5 out of 5 where 5 is “Very challenging”)



Base: 613 IT managers or above with server responsibilities

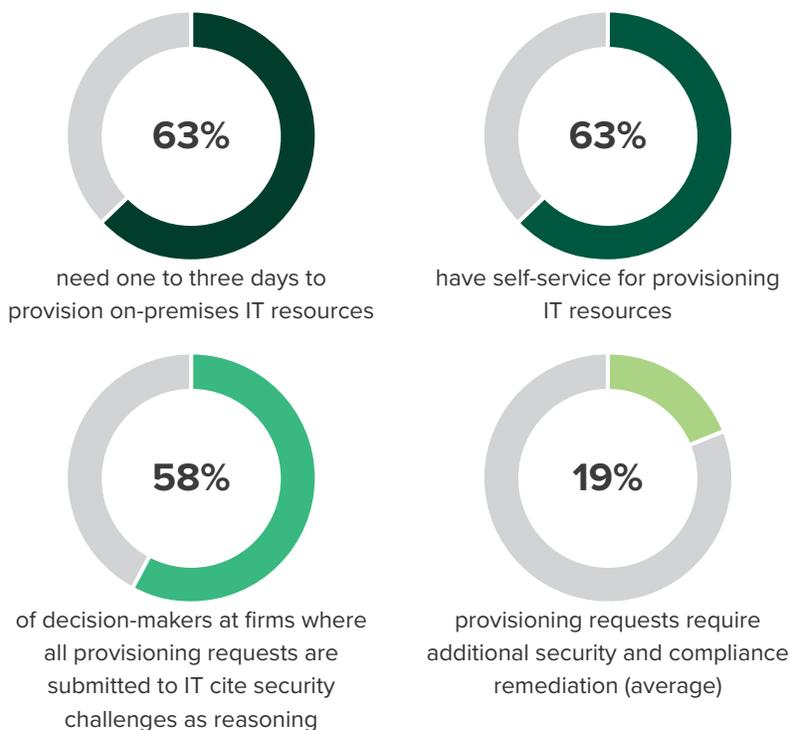
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, March 2021

Provisioning saps time and resources and often requires additional remediation for security and compliance issues.

- › **Provisioning is quick, but compliance enforcement takes longer.**
Around three-fourths of the provisioning requests can be completed in a max of three days. But their readiness for business use takes longer than that, as the I&O pros report that they spend additional time to ensure the provisioned resources follow organizational policies. IT teams report that an average of 19% of provisioning requests require the infrastructure team to remediate for security and compliance (see Figure 3). In addition, 65% report delivering servers/VMs to application developers or line-of-business teams after checking for configuration drift.
- › **Security challenges can restrain the implementation of self-service capabilities.** Many decision-makers (63%) report their firms allow for some level of self-service for provisioning on-premises IT resources. But self-service capabilities are not without challenges. More than half of professionals at organizations not currently providing self-service capabilities report security and technology challenges, and more than 40% anticipate compliance challenges (see Figure 3).

Figure 3

Provisioning Is Time-Consuming And Often Requires Security Remediation



Base: 613 IT managers or above with server responsibilities

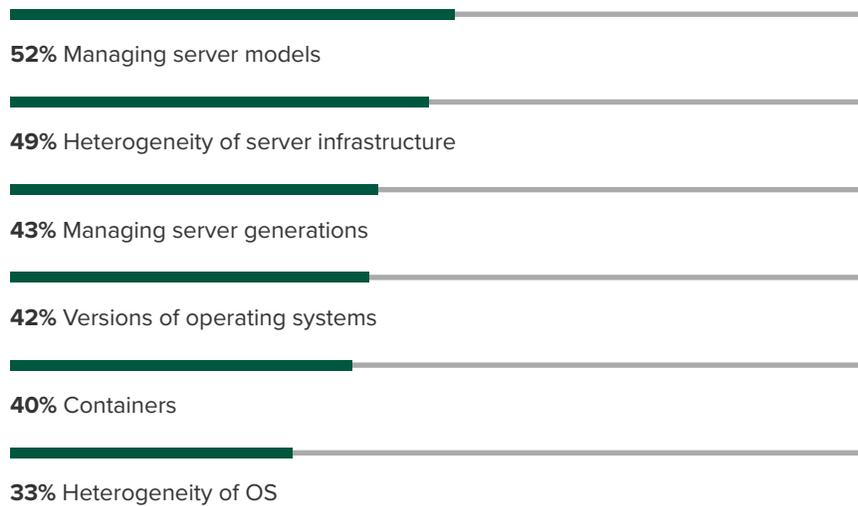
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, March 2021

> **Unmanaged configuration drift adds to infrastructure management woes.** Nearly half of respondents perform daily or weekly checks for configuration drift. As they perform these checks, 52% are challenged with server models, and 49% grapple with the heterogeneity of server infrastructure. More than 40% have difficulties managing multiple server generations and operating system versions (see Figure 4).

In retrospect, I&O professionals would do things differently if starting their infrastructure management, provisioning, and configuration journey over again. Half (51%) say they would better align infrastructure and security priorities, and 48% would have implemented policy engines that could be leveraged by both infrastructure management and compliance.

Figure 4

“What challenges do you face as your organization manages and checks for configuration drifts?”



65% of IT managers deliver servers/VMs to app dev or LOB teams after checking for configuration drift.

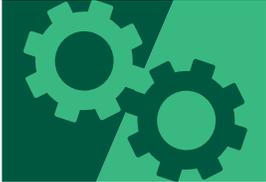
45% indicate their organizations manually perform daily or weekly checks for configuration drift.

Base: 613 IT managers or above with server responsibilities
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, March 2021

New Server Buying Fueled By Infrastructure Automation And Security

Enterprises continue to upgrade and modernize their server infrastructure. As they add contemporary server technology, companies are improving system performance, adding capabilities, and enhancing server security. In surveying I&O professionals at the manager level and above, we found that:

- > **New servers are in demand.** By deploying new server infrastructure, I&O pros expect improved capabilities, like higher system reliability, reduced infrastructure complexity, faster deployment or delivery of services, and improved security and compliance of servers. Fifty percent of decision-makers plan to add new server technology within the next two years, and 19% plan to add servers in more than two years (see Figure 5).
- > **Automation and easier configuration compliance are capabilities in demand.** Roughly half of I&O professionals seek automation and easier configuration compliance with their next server purchases. Two out of five are looking for faster deployments and delivery of services, and a third are seeking continuous security innovation (see Figure 6).
- > **Imperatives for server implementation – modern infrastructure, ease of integration, and skilled IT staff.** As enterprises consider new infrastructure, the technology is only one piece. Three-quarters (75%) of I&O professionals report that modernized infrastructure, such as programmable hardware or infrastructure-as-code, is extremely important when implementing new server technology. However, 81% report integration is extremely important, and 76% say that having IT staff with the right skill sets and training is necessary for a successful implementation.



54% of I&O professionals seek automation capabilities in their next server purchases.

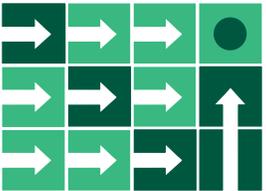
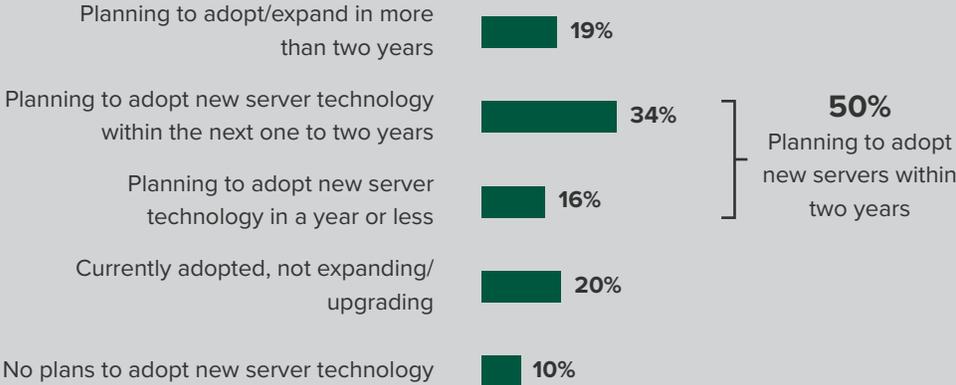


Figure 5

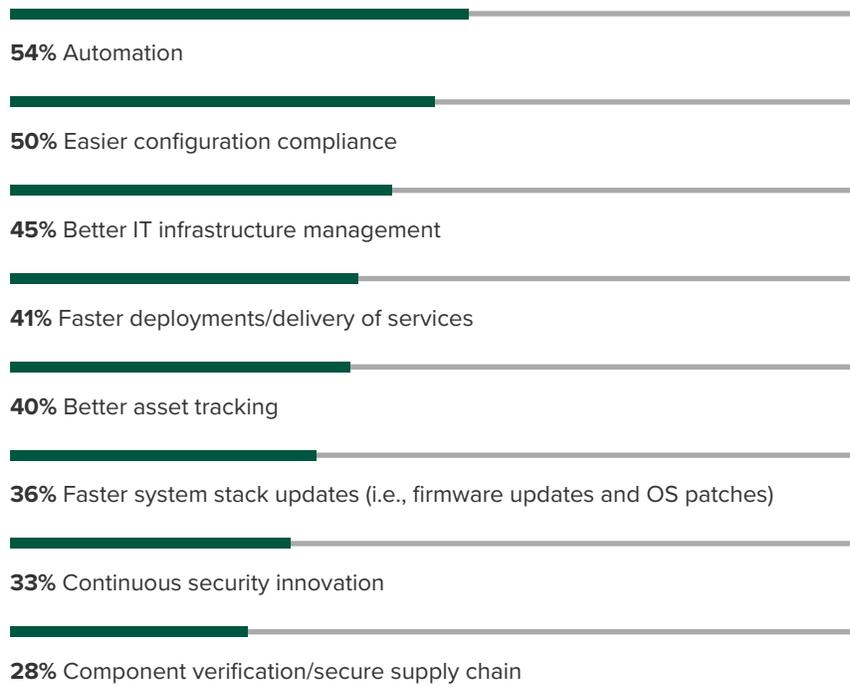
“What are your firm’s plans to adopt new server technology?”



Base: 613 IT managers or above with server responsibilities
 Note: Percentages do not total 100 because of rounding.
 Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, March 2021

Figure 6

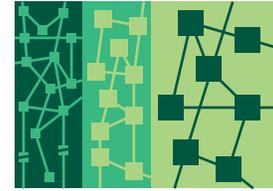
“If adopting new server technology, what new capabilities is your organization seeking with your next server purchase?”



Base: 549 IT managers or above with server responsibilities adopting or planning to adopt new server technology
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, March 2021

Adding Contemporary Servers Helps Overcome Automation And Security Challenges

Enterprises work to overcome these challenges by adding new server technology. Not only are they able to overcome their automation and security issues, but new servers also lead to measurable results. Our study found that adding new server technology can:



- › **Improve reliability and security and reduce complexity.** Roughly half of I&O pros whose firms have adopted new servers have already reaped the benefits. More than half (55%) have higher system reliability and have reduced infrastructure complexity. In addition, 54% cite improved security and compliance as a result of the new technology, and 38% report reduced time spent on remediating issues due to proactive security audits and scanning. A third of respondents were able to lower operating expenses (see Figure 7).
- › **Save IT departments time and money.** As companies implement new servers, they reap clearly quantifiable benefits, and these savings can be reinvested into innovation that can drive a competitive edge for the organization (see Figure 7).
 - Saving time.
 - On average, I&O pros estimate a 10% savings in time spent on provisioning and infrastructure delivery and routine or repetitive IT management tasks.
 - They also estimate that implementing new server technology saves an average of 13.7% of time spent on remediating vulnerabilities.
 - Saving money.
 - IT teams estimate that new server technology can trim operating expenses by an average of 6.3%.
 - The impact on capital expenses is an anticipated reduction of 3.4%.

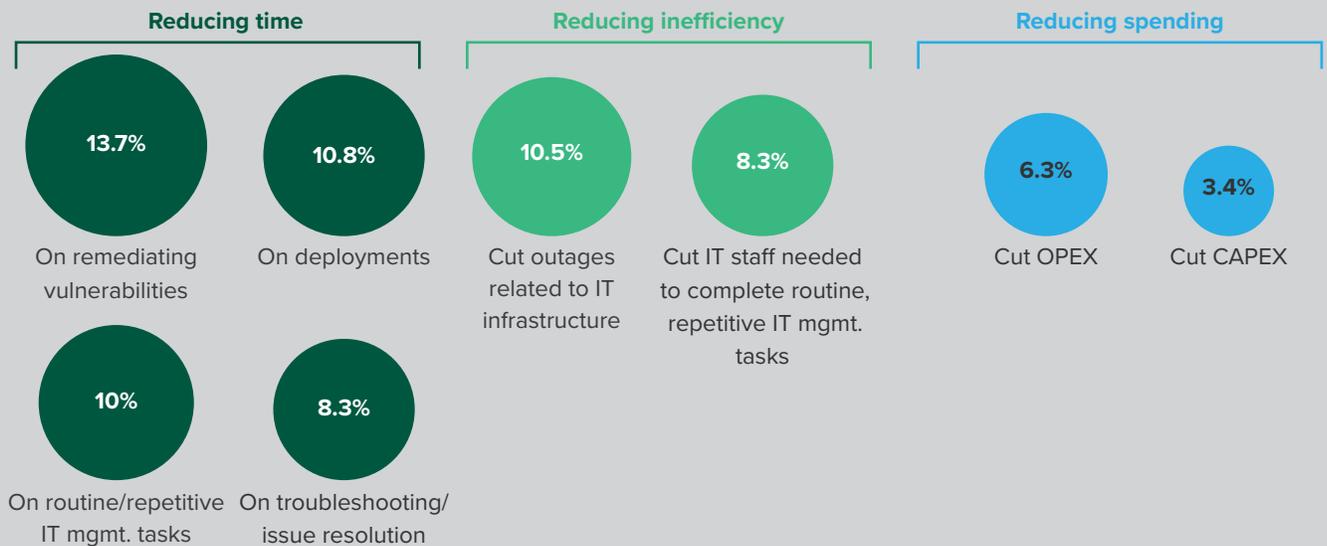
Figure 7

Benefits Realized By Adopting New Server Technology



Base: 125 IT managers and above with server responsibilities whose orgs have adopted new server technology

Quantified Outcomes Of Adopting New Servers



Base: 613 IT managers or above with server responsibilities

Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, March 2021

Key Recommendations

As enterprises aim for digital transformation, I&O leaders must take multiple steps to develop a secure and automated technology infrastructure. Implementing new server technology is one of those first steps. Forrester's in-depth survey of I&O professionals yielded several additional important recommendations:



Refine IT processes. A bad process automated is still a bad process. Before purchasing automation tools, inventory your workflow around IT infrastructure. Can some manual steps be made more efficient? Are some steps no longer required with modern infrastructure? Can some change management steps be removed as governance becomes code?



Keep the business objectives in mind. Businesses depend on end-to-end service automation to improve their speed of service: app development, testing, and rolling out new services in production. Self-service capabilities have taken a lot of friction out of the process; however, it's far from frictionless. Technology infrastructure must stay compliant and be governed by organizational guardrails. Automated enforcement and remediation of those policies should be a key focus given the volume and complexity of today's infrastructure.



Focus relentlessly on automating infrastructure services. Developers focus on application logic and don't want to worry about infrastructure intricacies. On-premises infrastructure will remain relevant in tomorrow's business model, but only if technology leaders automate and abstract the infrastructure services across silos and lifecycle stages and take care of all interdependencies.



Be cognizant of the security holes in hardware. Businesses are being attacked from all sides and must guard against all attack vectors to minimize risk. It's not just software that has security vulnerabilities; vulnerabilities also exist at the hardware layer. Infrastructure — especially when heavily distributed — can increase the attack surface by orders of magnitude. Tech leaders face considerable pressure to embrace infrastructure innovation and serve business requests without compromise — even as they need to maintain or improve the overall security posture.

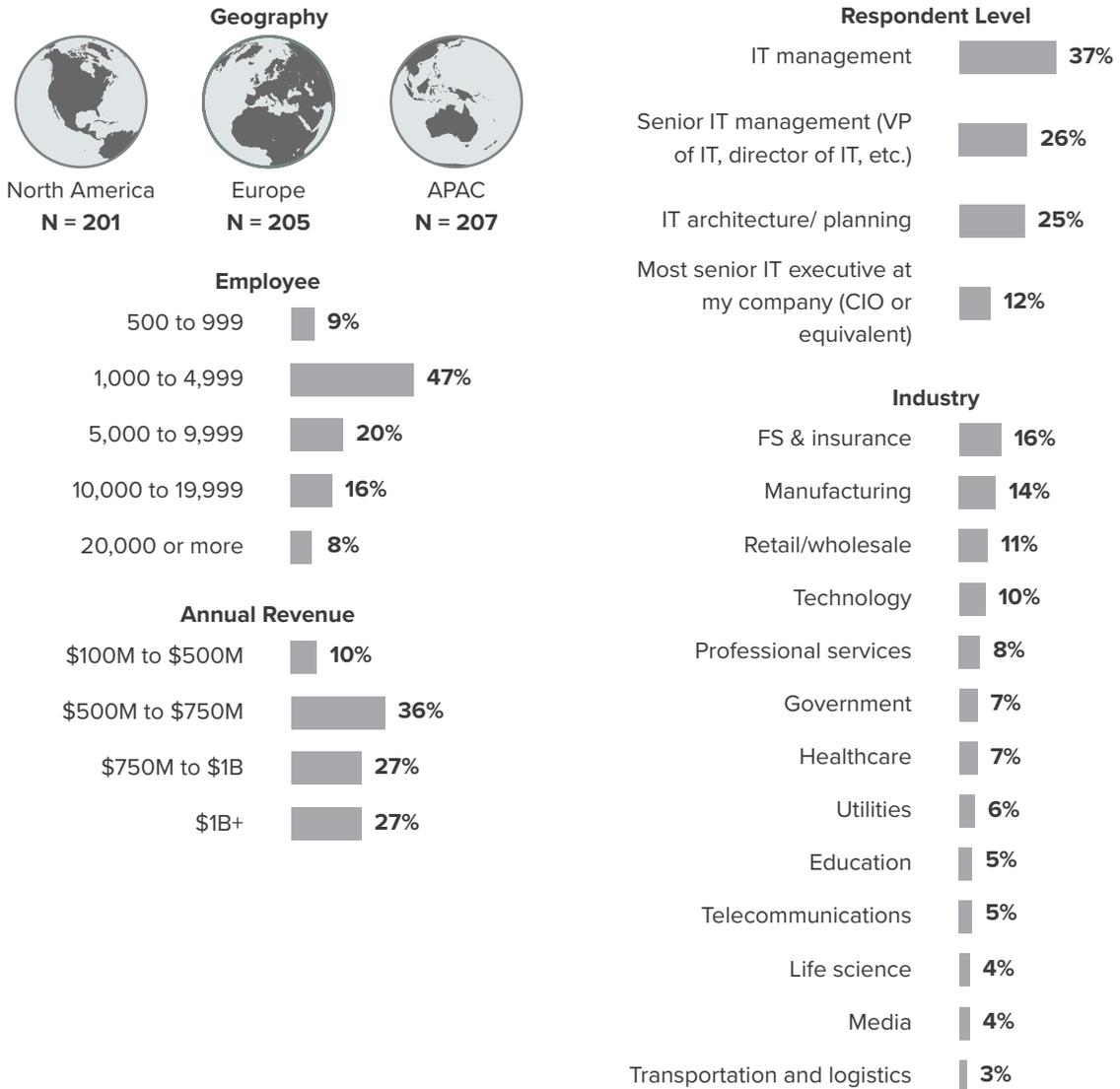


Work with a trusted IT services partner. Modernized IT organizations recognize the importance of a trusted IT services partner to guide the automation journey. Bringing in a partner also ensures that the automation of IT optimizes your strategy, ensures it is holistic, and smooths out any bumps over the long term.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 613 IT managers and above in North America, Europe, and APAC to understand new server buying. Survey participants included decision-makers in infrastructure and security operations. The study began in February 2021 and was completed in March 2021.

Appendix B: Demographics



Base: 613 IT managers or above with server responsibilities
 Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, March 2021

Appendix C: Supplemental Material

RELATED FORRESTER RESEARCH

“Automation Drives The I&O Industrial Revolution,” Forrester Research, Inc., February 9, 2021

“Research Overview: Infrastructure Technology For 2020,” Forrester Research, Inc., February 14, 2020

“Gauge Your Infrastructure Automation Maturity,” Forrester Research, Inc., July 17, 2020

Appendix D: Endnotes

¹ Source: Forrester Analytics Business Technographics Infrastructure Survey, 2020.

² Source: “Research Overview: Infrastructure Technology For 2020,” Forrester Research, Inc., February 14, 2020.