Enterprise Strategy Group™
by TechTarget

2024 Mainframe Market Pulse:

Cybersecurity and Compliance Insights

Strengthening Modern Mainframe Resilience in Hybrid Cloud Environments

Mainframe Market Pulse research by Enterprise Strategy Group was commissioned by Broadcom and is distributed under license from TechTarget, Inc.

“**Mainframes continue to be the backbone of many organizations**, providing unmatched reliability, scalability, and security.”

Introduction

As a technology, mainframes have existed for more than half a century. During this period, they have delivered essential computing and processing capabilities, powering the world’s economy by managing vast amounts of data for enterprise organizations of all sizes and types. Mainframes have demonstrated tremendous value in their consistency to perform at high levels for some of the most sensitive and voluminous computing operations. Mainframes are widely viewed as being not only reliable and continually available but also highly secure. This is evidenced by the pervasive dependence on mainframes by banks, financial services, governments, and healthcare organizations to perform many of their most critical IT functions.

Mainframes continue to be the backbone of many organizations, providing unmatched reliability, scalability, and security. As businesses navigate challenges and emerging threats, the robust performance of mainframes ensures seamless operations. Today, organizations operate in the cloud as well. Consequently, many enterprises are embracing a hybrid environment, strategically balancing applications and workloads between the cloud and their indispensable on-premises mainframes.

TechTarget’s Enterprise Strategy Group was commissioned by Broadcom Inc. to generate research and explore some of the challenges, drivers, and benefits of mainframe architectures. The results of the research are highlighted in this eBook.

OBJECTIVES

This comprehensive analysis delves into the evolving role of mainframes in the modern IT landscape, addressing how, when properly using the available tools, they help organizations continue to adapt and thrive amid the rise of cloud computing and hybrid environments. The goal of this research is to provide IT professionals and decision-makers with valuable information to optimize their mainframe strategies. Whether an organization is looking to enhance performance, improve security, or integrate with other cutting-edge technologies, this eBook offers a wealth of knowledge to help navigate the complexities and unlock the full potential of mainframe systems.

This study, conducted in March 2024, surveyed over 100 stakeholders and IT leaders involved in purchasing network infrastructure and services. Respondents came from large enterprises (5,000+ employees) in North America (U.S.) and Western Europe (U.K.), operating in the financial services (FinServ) and government (Gov't) sectors. After passing a thorough vetting process, 100 respondents remained, all of whom received incentives in the form of cash or cash equivalents for their participation and insights.

KEY FINDINGS

The mainframe market isn't going anywhere:

79%
expect more investment in mainframe technology over the next two years.

73%
plan to keep using mainframes for at least 5-10 years, or in perpetuity.

ONE-QUARTER
of all investments in mainframe solutions made by the FinServ sector were made over the last 3 years, highlighting the value consistently found in mainframes.

Monitoring mainframes remains fundamental to strong security postures:

94%
reported some continuous security monitoring in their mainframe environment.

90%
reported some continuous compliance and regulation monitoring in their mainframe environment.

Compliance and security challenges are distinctly affecting Gov't and FinServ sectors:

4.7x MORE
observed security vulnerabilities (without proper controls in place) due to outside technologies integrating with the mainframe.

88%
were challenged in keeping pace with changes in cybersecurity-related compliance.

Mainframe Solutions Aren’t Going Away

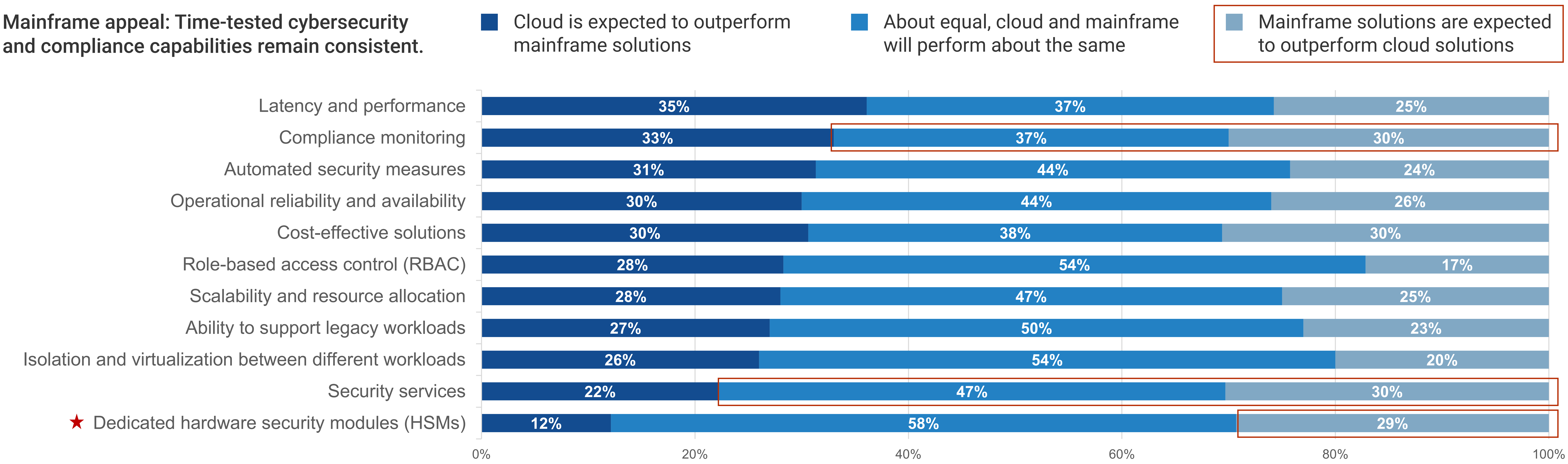
Operating in a Hybrid Environment Is the New Normal

At the onset of cloud computing, there was excitement (mixed with cautious trepidation), momentum, and a fear of missing out for business leaders considering moving to the cloud. Fast-forward 10-15 years later, and there are more case studies as well as cloud-based challenges and threats that have muted some of the aggressiveness of past mass migration, as this report shows application repatriation back to mainframes continues to be substantial.

Today, most companies operate in the cloud as well as on premises, in a hybrid environment Yet, when respondents were asked whether they believed their apps and workloads would likely perform better in the cloud, on premises in a mainframe environment, or equally in both, most benchmarks and capabilities were viewed rather evenly.

Optimism about mainframe environments is even more pronounced in the case of hardware security modules (HSM). Dedicated HSM on mainframe were reported to be 2.5x as likely to outperform cloud-based dedicated security modules.

Mainframe appeal: Time-tested cybersecurity and compliance capabilities remain consistent.



In Spite of Cloud-Related Options, Strategic Use of Mainframes Remains Strong

Mainframes remain vital for sectors requiring immense compute and transactional power. Given their heightened data sensitivity and massive volumes, both the FinServ and Gov't sectors require such capabilities.

With today's sophisticated threats and heightened security and compliance demands, mainframes are more attractive than ever.

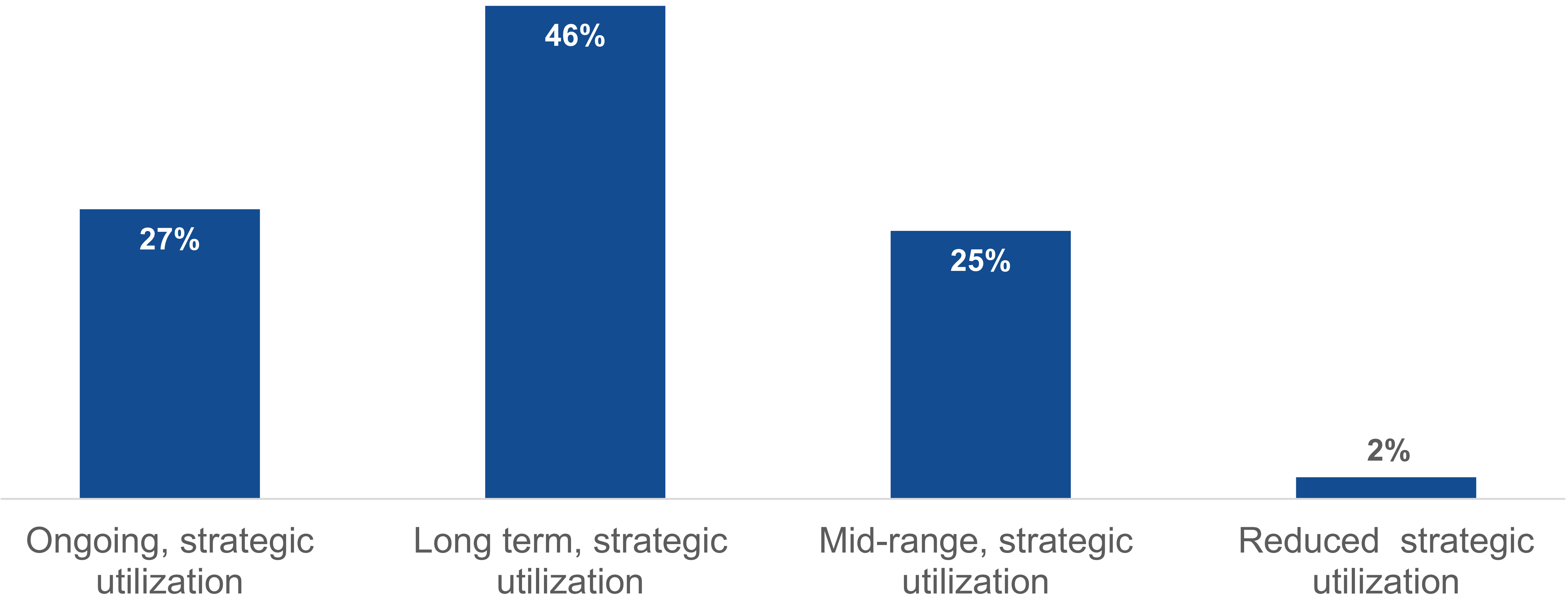
Utilization rates are expected to remain high, as 98% of respondents foresee continued strategic use of mainframes for workloads over the next 5 -10 years, if not in perpetuity.

FinServ organizations lead the charge to new mainframe purchases, while Gov't organizations are prone to extended retention (see *Appendix*):

22% of FinServ mainframe purchases were made in the last one to three years.

Gov't respondents purchased no mainframes in that time but were **40% more likely** to have been operating their current mainframe solutions for longer than eight years.

Mainframe solutions continue to enjoy strategic utilization.



***Ongoing,* strategic utilization:** We view our mainframes as stable and anticipate use in perpetuity for wide range of workloads.

***Long term,* strategic utilization:** We anticipate reliance and usage over next 5 to 10 years for significant amount of workloads.

***Mid-range,* strategic utilization:** We anticipate continued usage over the next 5 to 10 years but with minimal workloads (i.e., business-critical only).

***Reduced* strategic utilization:** We anticipate continued usage over the next 3 to 4 years but with reduced workloads (i.e., business-critical and legacy only).

Not strategic: We anticipate continued usage over the next 3 to 4 years but with minimal workloads (i.e., business-critical only).

Sunset: We anticipate sunsetting our mainframe solutions within the next 5 years.

Previously Migrated Apps and Workloads Are Returning to Mainframes

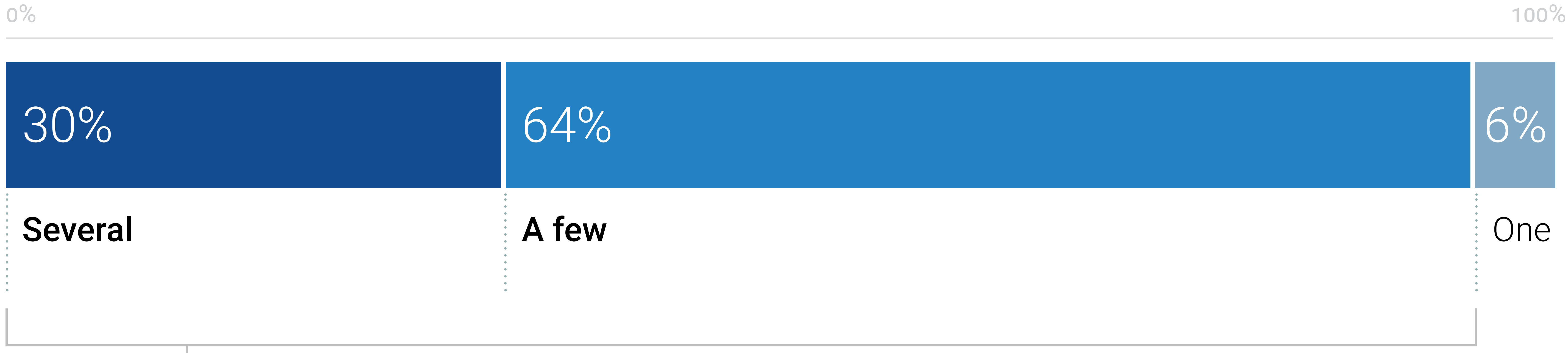
Unexpected Costs and Compliance Concerns on Cloud Are Principal Reasons Cited

94% of all respondents reported moving numerous workloads back on prem (aka repatriation) for a variety of reasons. Operational costs (41%) was one, but many other top reasons were compliance-oriented.

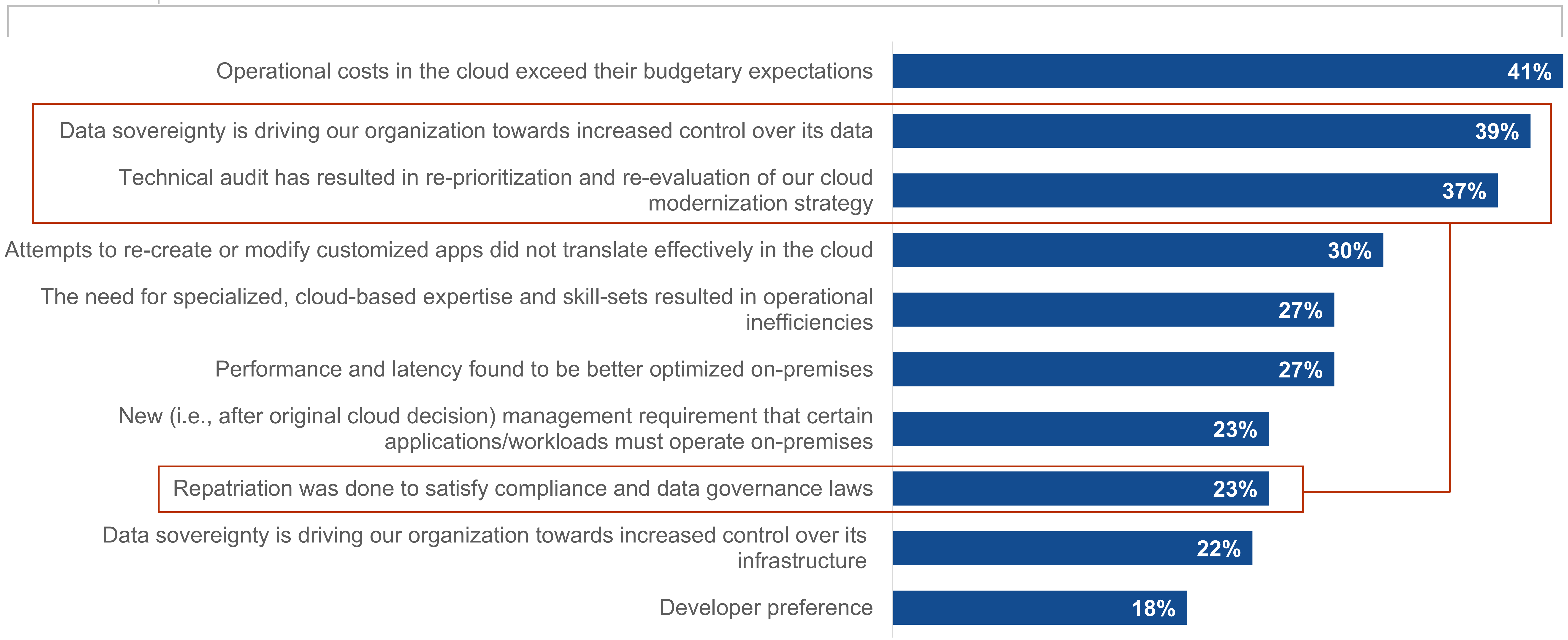
Compliance concerns are real and always evolving. A growing compliance concern is data sovereignty. Data sovereignty essentially means that data is governed by the laws and regulations of the country or region where it's located. 39% of all respondents expressed this concern. Mainframe solutions featuring continuous compliance monitoring are aptly suited to address this.

37% cited technical audits, predicated on internal reviews of cloud modernization strategies versus mainframe benefits (i.e., enhanced security, real-time alerts, advanced reporting), paved the way for workload mainframe repatriation.

Workloads once migrated to the cloud are now migrating back on prem.



What do you believe to be the principal reasons for the repatriation of workloads from public cloud to on-premises mainframes within the last 12 months?



Empower Cybersecurity and Compliance:

Optimize Security Continuous Monitoring on Mainframes

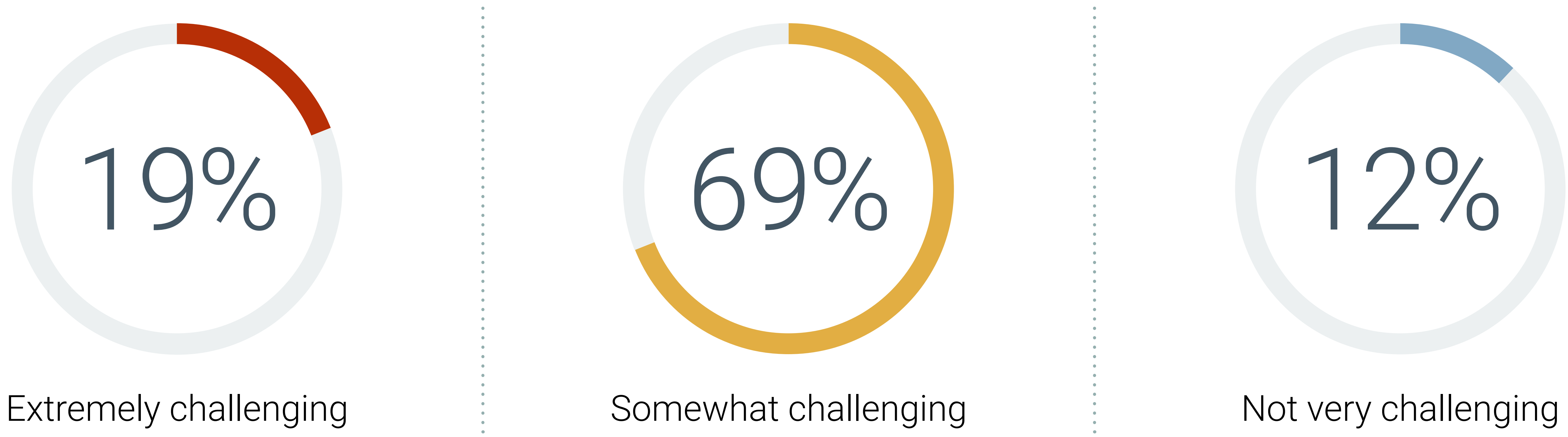
Keeping Pace With Compliance Changes Around Cybersecurity Is Crucial

The volume of cybersecurity compliance regulations, and the pace with which they change, is daunting, as noted by 88% of respondents.

Cybersecurity compliance involves adhering to regulations such as GDPR, DORA, NIST, and PCI DSS, to name a few. These standards mandate data protection, incident response, access controls, and security training, helping organizations safeguard sensitive information and build a strong security framework.

Failure to meet cybersecurity compliance results in far-reaching consequences. There is the potential for financial, legal, regulatory, and reputational penalties. Conversely, organizations that successfully navigate these waters can maintain a competitive advantage from a perspective of cost savings, increased security, operational efficiency, and vaunted customer trust.

Cybersecurity compliance changes prove to be a challenge.



> “The volume of cybersecurity compliance regulations, **and the pace with which they change, is daunting,** as noted by 88% of respondents.”

Compliance Pain Points Include Financial Regulations and Security Guidance

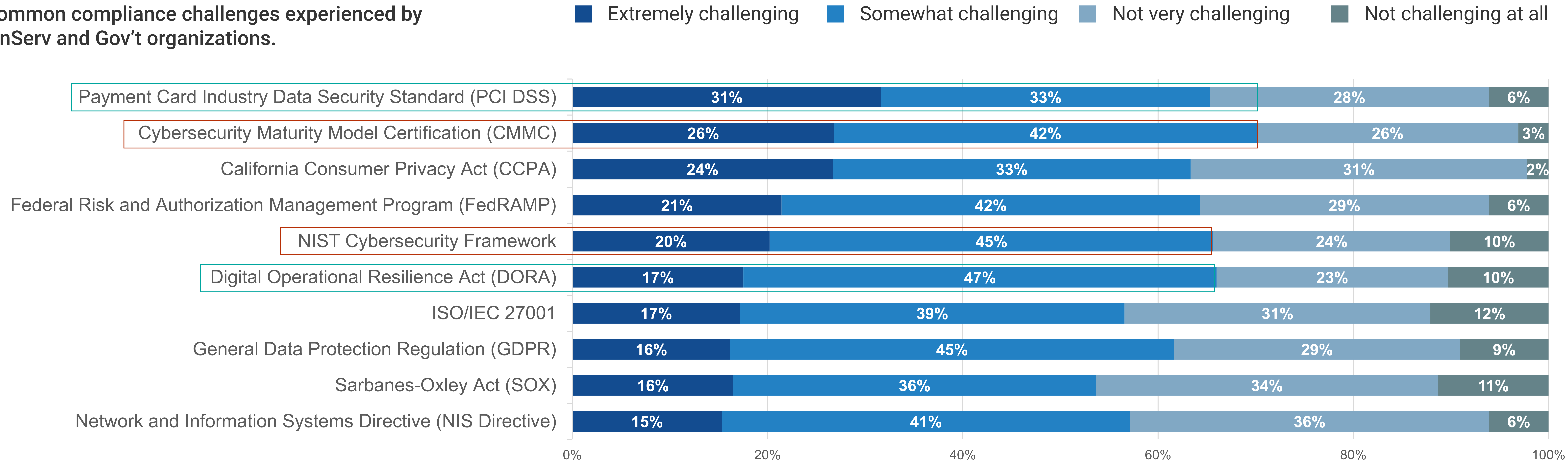
Security Ranks as Most Challenging

To say there are an immense number of regulations would be an understatement. It also goes without saying that compliance challenges (and prioritization) should differ between FinServ and Gov't sectors. Enterprise Strategy Group sought to uncover commonalities between 10 of the most FinServ- and Gov't-related compliance challenges.

In reviewing common sector-associated compliance challenges, two of the top four were security-based: 68% of organizations found CMMC standards challenging to meet, and 65% found the NIST Cybersecurity Framework challenging. The next two were financial regulations: 64% of organizations found both PCI DSS and DORA challenging to comply with.

This list represents merely a fraction of the overwhelming number of compliance regulations and frameworks, each with its own rules and guidelines. Falling outside of compliance can result in regulatory as well as commercial consequences. Maximizing compliance monitoring solutions can help mitigate potential compliance issues.

Common compliance challenges experienced by FinServ and Gov't organizations.



Organizations Remain Ever Watchful as They Increasingly Adopt More Comprehensive Security Continuous Monitoring Solutions

With FinServ and Gov't dominating the mainframe market, continuous monitoring is a must. Critical data (e.g., payment transactions, tax records, etc.) demands stringent security, leading 94% to report continuous monitoring mainframes for security. Likewise, 90% also continuously monitor for changes in compliance and regulatory guidelines.

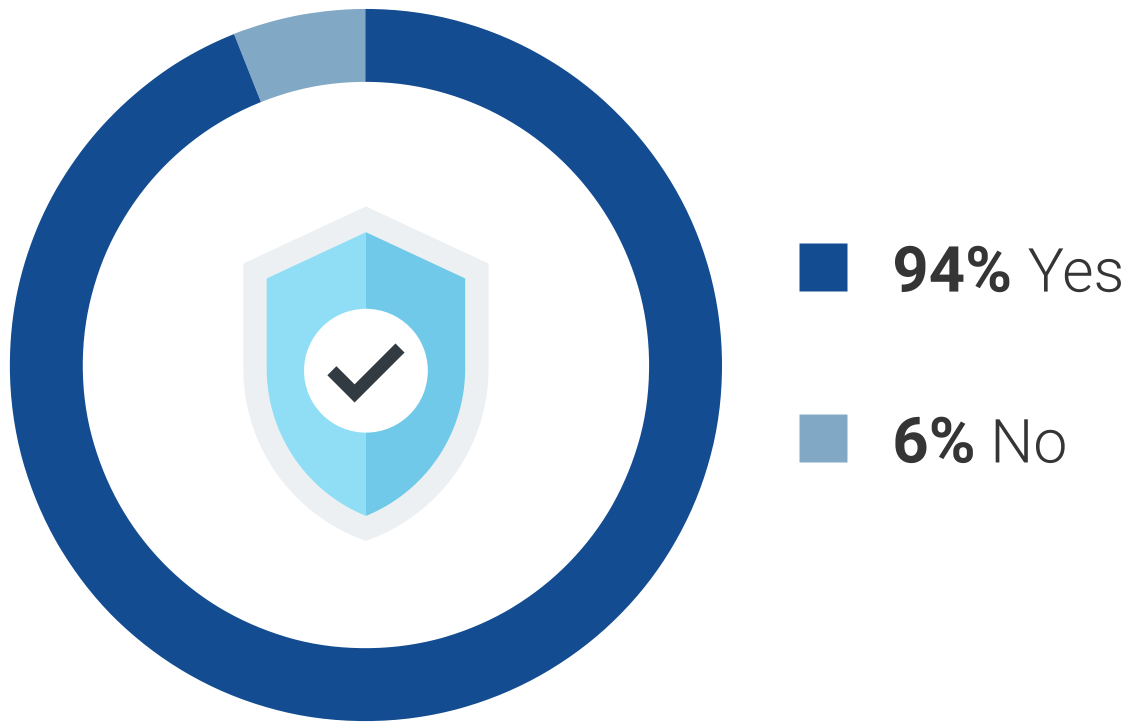
It's vitally important to identify areas critical to one's organizational security continuous monitoring needs (technical audits can help identify these areas). Vulnerability management, access controls, incident/event management, network security, and data protection are prime examples of areas that would benefit from appropriate levels of continuous monitoring.

Therefore, it's not enough to continuously monitor for security events; organizations must employ a more comprehensive approach to continuous security monitoring across the entire mainframe environment.

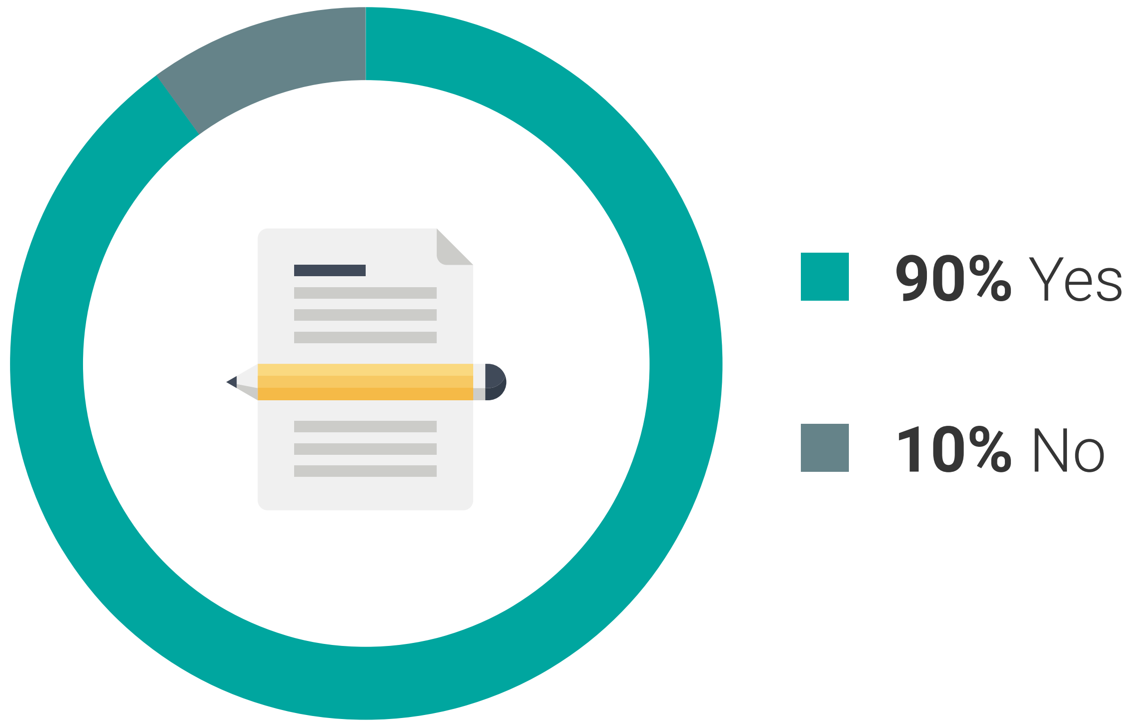
The swift and constant changes in regulatory frameworks and guidance are daunting. Continuous compliance monitoring helps organizations stay ahead, ensuring adherence to standards and avoiding penalties. This proactive approach mitigates risk, enhances security, boosts stakeholder confidence, and maintains the integrity of critical systems and data.

Continuous monitoring for security and compliance is the norm.

Does your organization currently utilize solution(s) that continuously monitor mainframes for security issues?



Does your organization currently utilize a solution to continuously monitor for changes to compliance and regulatory guidelines?



Organizations must employ **a more comprehensive approach to continuous security monitoring** across the entire mainframe environment.

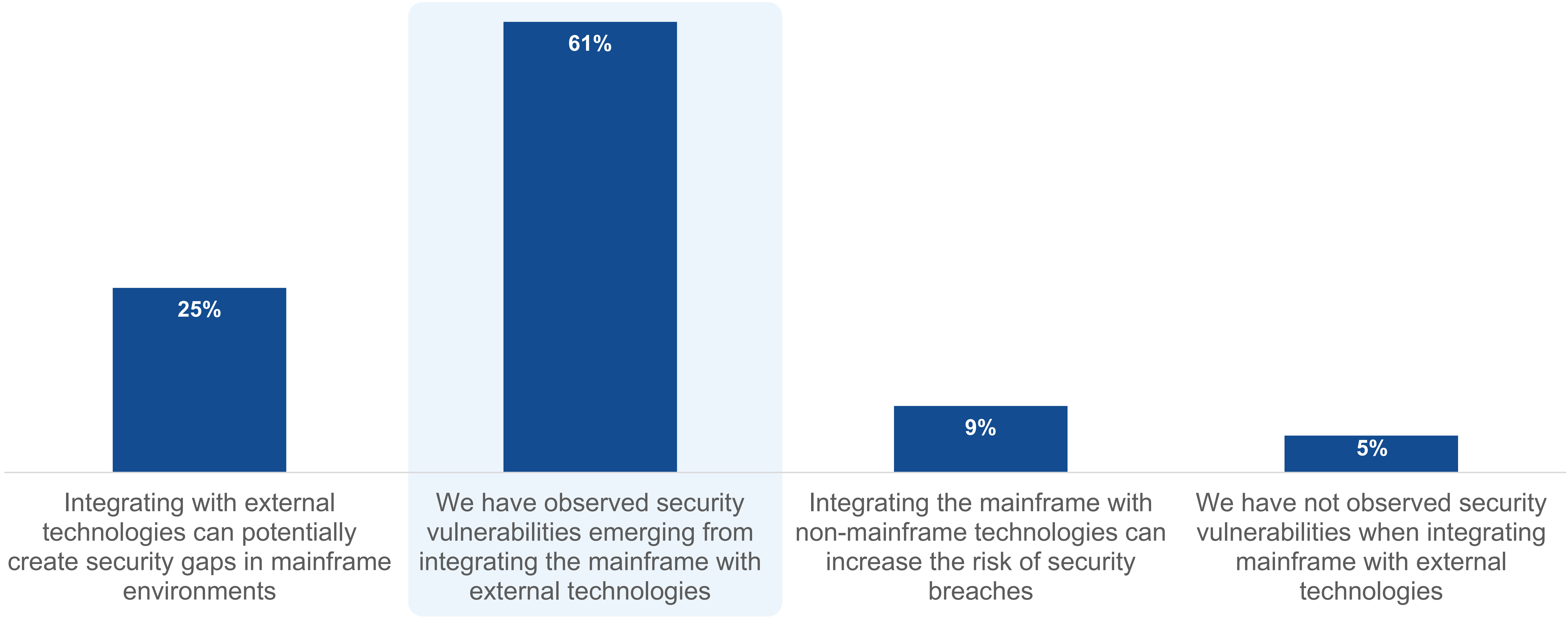
Cloud-Connected Mainframes Should Implement Continuous Security Monitoring to Minimize Vulnerabilities

Mainframes have been reliable for decades but face new threats as they are increasingly opened up and integrated into hybrid architectures. Integrating outside technologies into the mainframe led to 4.7x more observed security vulnerabilities (without proper controls in place).

The top reported challenge related to operating core business systems with current mainframe security technologies was updating legacy components (cited by 43%; see *Appendix*). As mainframe solutions are updated with new technologies, new exposures could arise, especially when challenged with integrating new solutions as part of legacy modernizations efforts.

Cybersecurity continuous monitoring can reduce threat exposure, while identifying potential breaches and providing real-time alerts. However, continuous monitoring alone might not be enough; it can be elevated by operating in tandem with just-in-time (JIT) privileged access management (PAM) capabilities.

Integrating mainframes with external technologies increases exposure to security risks.



> "Integrating outside technologies into the mainframe led to **4.7x more observed security vulnerabilities** (without proper controls in place)."

Implementing PAM and Adaptive Authentication Strengthens Compliance, While Reducing Risk

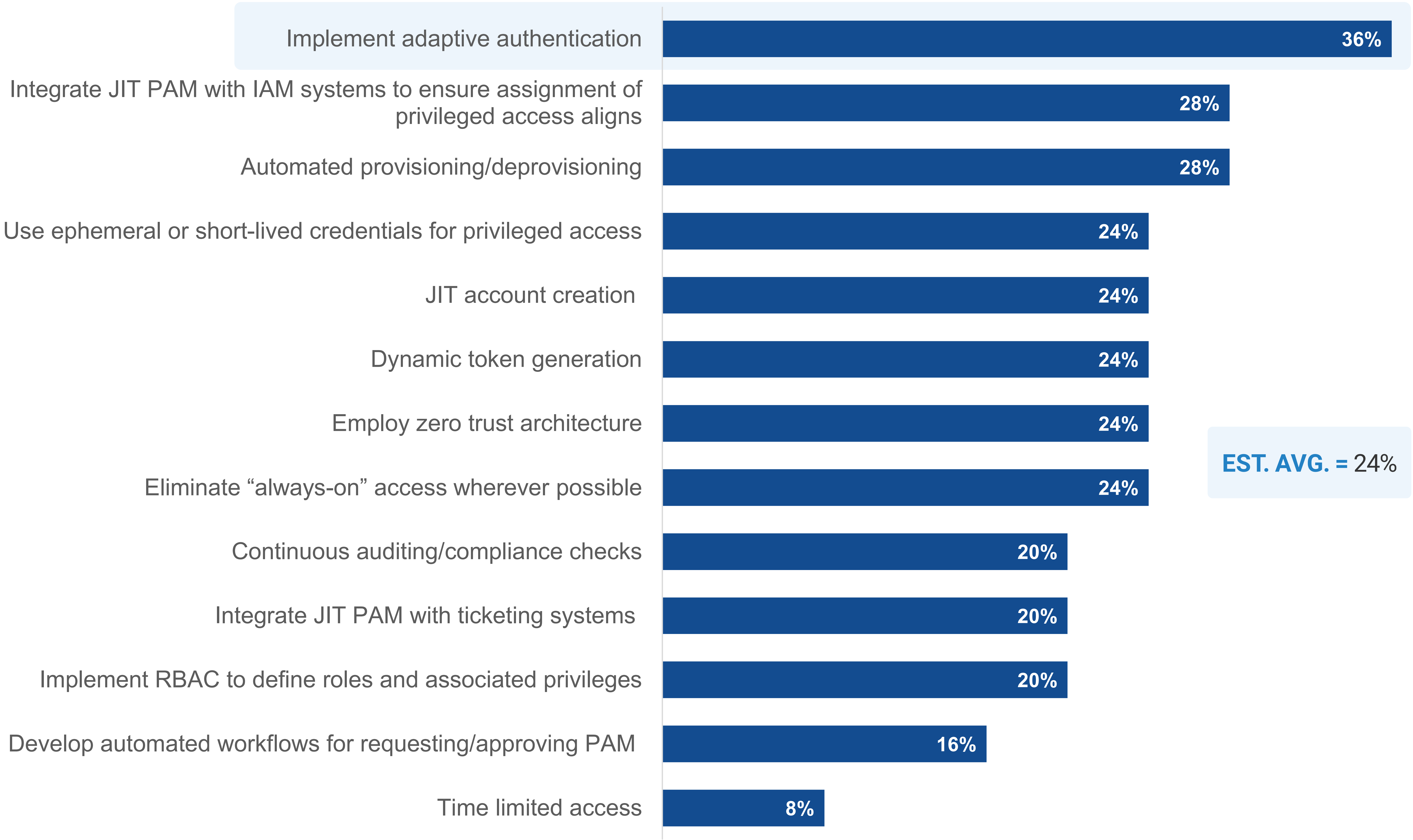
Implementing a comprehensive PAM solution improves organizational compliance by relying on best practice access and controls to secure critical data and infrastructure. In doing so, businesses mitigate risk by reducing threat landscapes.

Adaptive authentication (i.e., risk-based multifactor authentication) builds trust in privileged user identity and provides JIT access. This is especially important for Zero Trust initiatives, which aim to minimize threat exposure. These measures help limit unnecessary or malicious access to mainframes integrated with external technologies.

As such, respondents were 50% more likely to consider adaptive authentication to reduce unauthorized access risks, as compared with the average of all other elements combined.

**This data point is considered directional due to a low sample size (N>30).*

Using MFA and PAM mitigates threats.



Mainframes Are Not Intrinsically Secure; Mitigating Risk Requires a Variety of Approaches

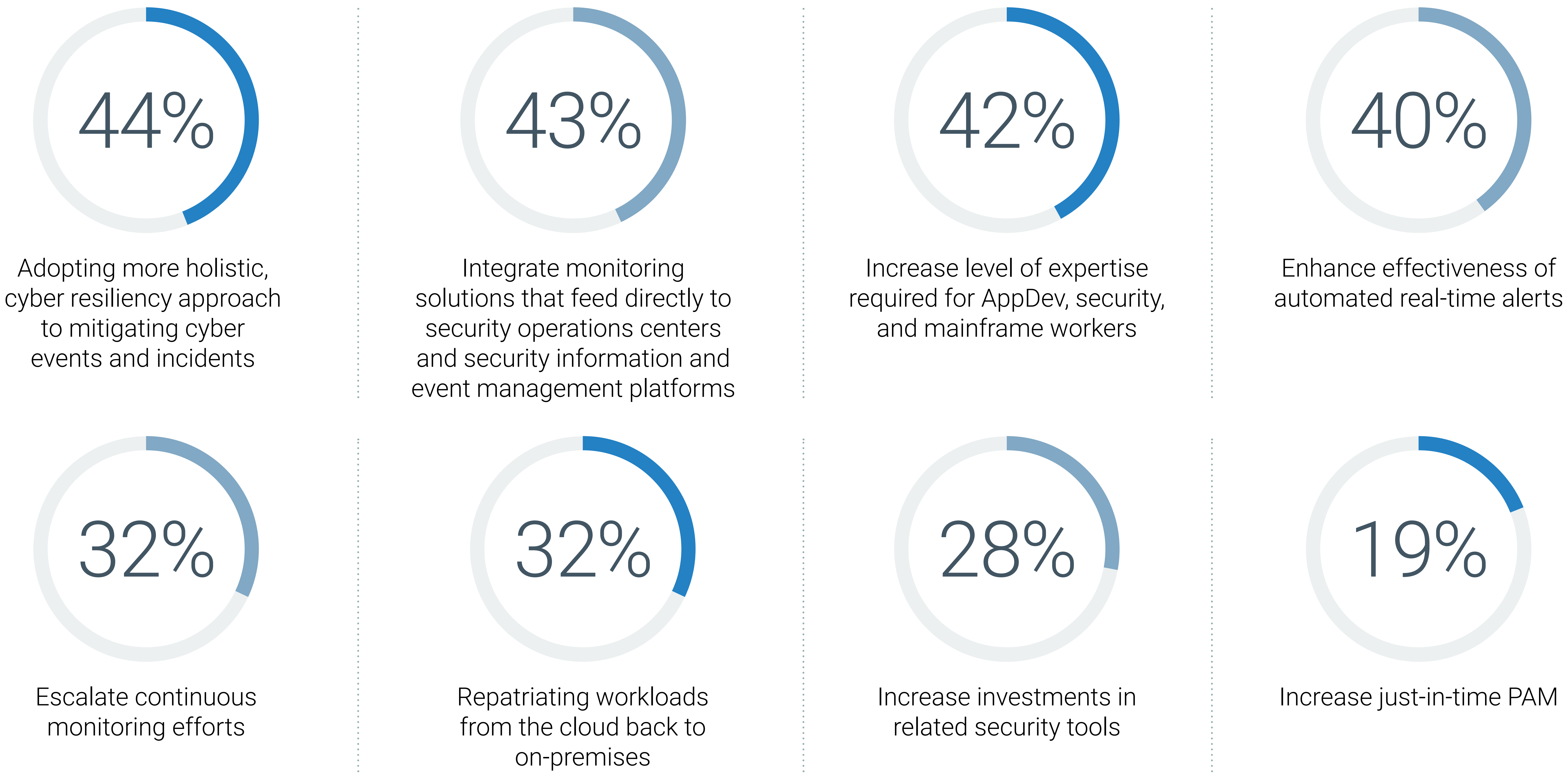
Combatting business-critical cybersecurity incidents requires a comprehensive approach to threat management, according to 44% of respondents. No singular control point is likely to effectively secure mainframes operating in a hybrid environment. Strategies should be multipronged to address the complex attack surface.

Implementing security continuous monitoring remains a principal recommendation, and 43% of all respondents reported integrating the solutions directly into their security and information event management (SIEM) platform. Of course, effective use of automated alerts is necessary (40%), or the effort around continuous monitoring is almost for naught.

What should not be taken for granted is ensuring that employees managing mainframe environments are adequately skilled and supported. Training, certification, and instruction might be necessary. Broadcom Mainframe Education can offer such support.

Suffice to say, the best employee training available has little value if employees lack the proper tools. Broadcom's Mainframe Cybersecurity and Compliance portfolio offers a myriad of robust tools and software around compliance event management, data protection, advanced authentication, systems audits, and more—all of which can enhance an organization's mainframe environment.

Organizations are taking a balanced approach to combatting the rise in business-critical cybersecurity incidents.



78%

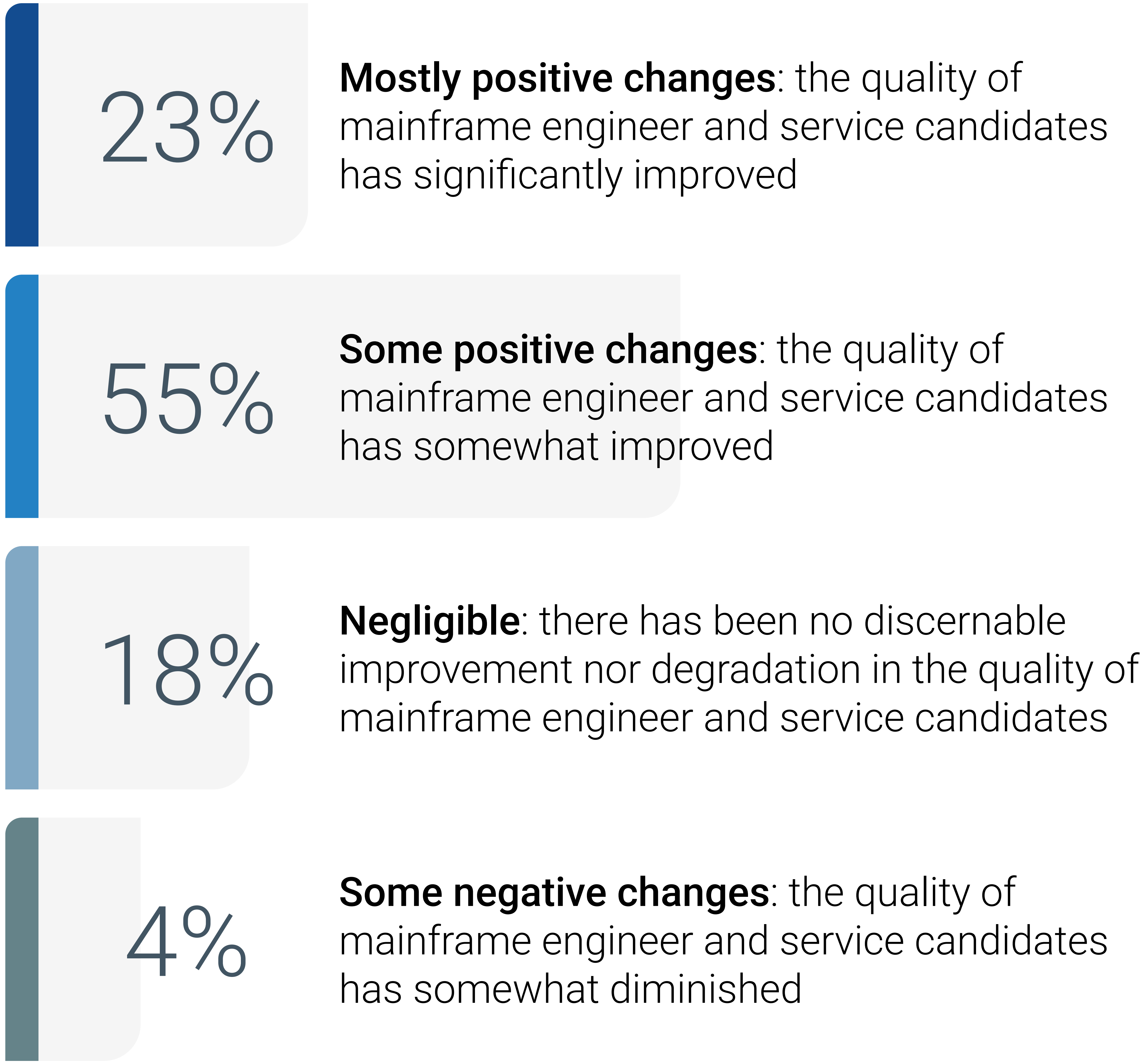
of all respondents felt there were **positive changes** around the quality of such candidates.

The Outlook on the Mainframe Engineer Job Market Is Optimistic, as Is Anticipated Mainframe Innovation

Despite challenges in skill gaps, organizations are bullish on the quality of mainframe candidates. Fortunately, there is optimism in this job space trajectory, as 78% of all respondents felt there were positive changes around the quality of such candidates.

This optimism is not limited to candidates; the future state of mainframe innovation also looks bright. Robust security (60%), data suitability (54%), and high compute capabilities (50%) were reported as having experienced innovation in mainframes over the last two years, among other categories (see *Appendix*).

Future state of mainframe engineers, service providers, and mainframe innovation is bright.



23% **Mostly positive changes**: the quality of mainframe engineer and service candidates has significantly improved

55% **Some positive changes**: the quality of mainframe engineer and service candidates has somewhat improved

18% **Negligible**: there has been no discernable improvement nor degradation in the quality of mainframe engineer and service candidates

4% **Some negative changes**: the quality of mainframe engineer and service candidates has somewhat diminished

Conclusion

Technology is amazing in that it always continues to evolve. Some technologies and tools stand the test of time better than others. Mainframe solutions fall into this category and continue to flourish. They also continue to set the standard where computability, compliance, security, and ability-scope are IT architecture priority requirements.

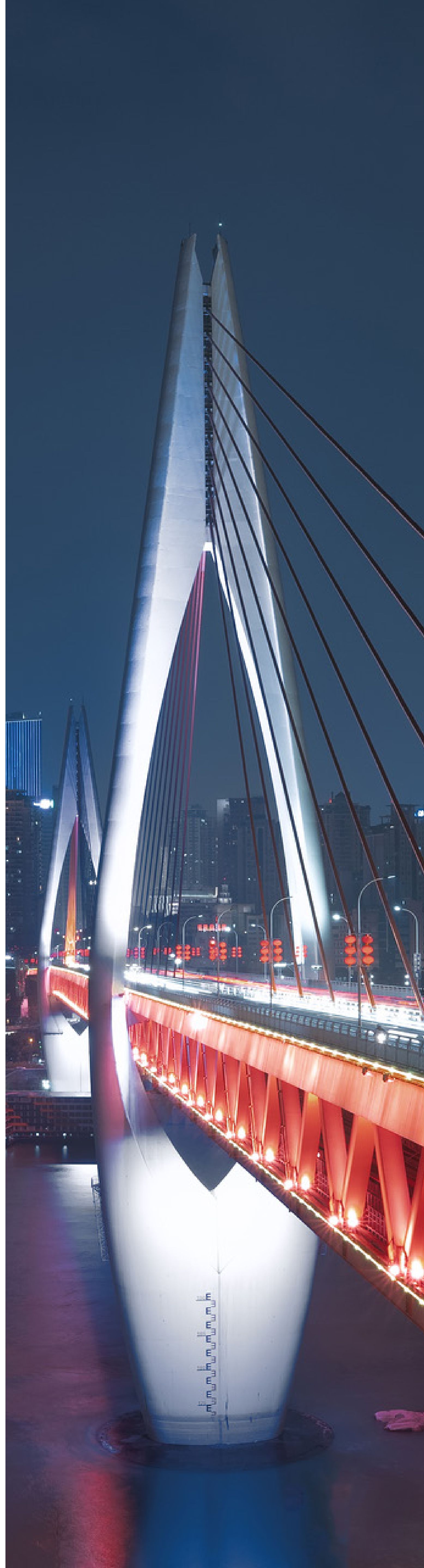
Suffice to say, cloud computing is an equally impactful innovation within the evolution of technology. Fast forward from its inception to today, and the evolutionary result is the hybrid cloud. For organizations to thrive in a hybrid cloud, optimizing mainframe efficiency is imperative, as the two environments function more symbiotically than divergently. While integrating with new technology has its challenges, fortunately there are solutions. To achieve mainframe optimization, organizations should do the following:

- **Maximize security continuous monitoring** for both cybersecurity threat mitigation and compliance alerts and updates. Ensure that continuous monitoring penetrates all necessary levels of threat.
- **Take a multipronged approach to manage mainframe security.** Identify the appropriate solutions and technology to stack as part of mainframe efficiency and security improvements. This includes providing employees responsible for mainframe operations adequate competencies, training, and associated tools.
- **Implement solutions with robust PAM and MFA.** Solutions with PAM and MFA capabilities are crucial for enhancing access controls and ensuring compliance with corporate mandates, security frameworks, and regulatory guidelines.
- **Optimize expert technology audits.** Secure mainframe environments with expert technology audits to formally assess mainframe performance and potential threat horizon. Additionally, ensure any such review satisfies all requisite compliance, framework, and regulatory guidance.

When integrating new solutions into your mainframe environment, be cognizant of new potential vulnerabilities and the expanded attack surface.
Seek out those solutions that integrate directly into SIEM platforms.

LEARN MORE

BROADCOM®



RESEARCH METHODOLOGY AND DEMOGRAPHICS

This study—fielded between March 20, 2024 and March 26, 2024—included IT leaders influential in the purchase process for network infrastructure and services at their organization.

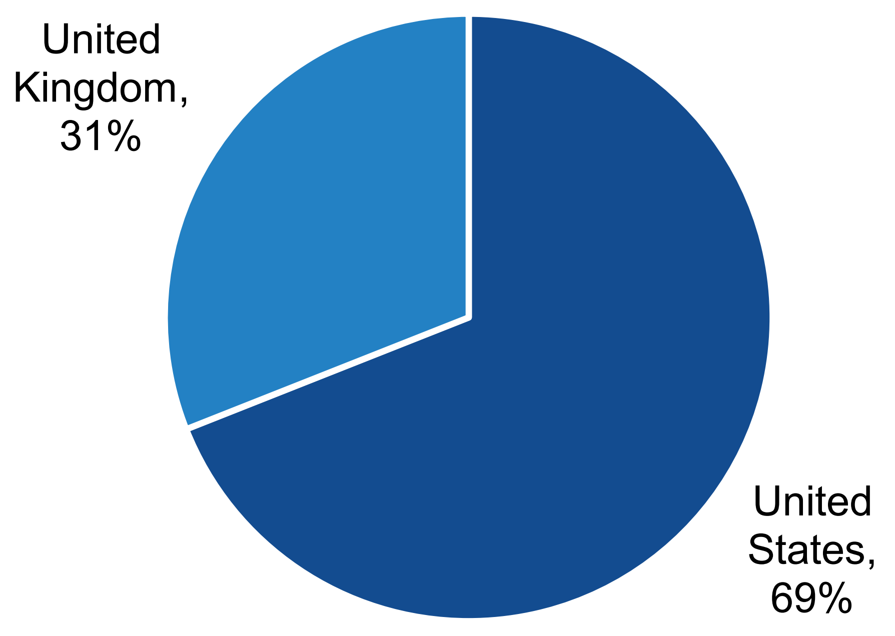
Respondents in the study came from organizations designated as large enterprises (i.e., 5,000+ employees). These organizations were based in North America (U.S.) and Western Europe (U.K.) and operated in the financial services and government sectors.

After applying data quality control best practices and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 100 respondents remained. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

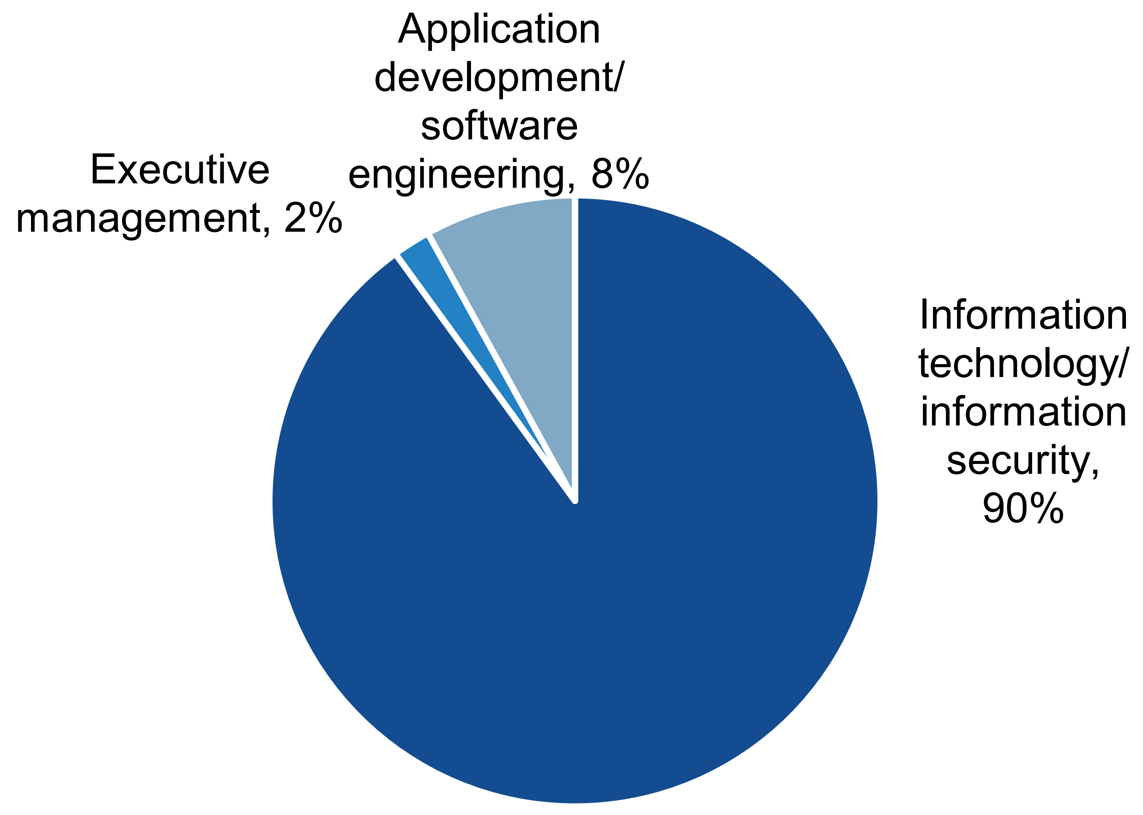
The survey confidence level is 95%, with a margin of error of +/-9.8%.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

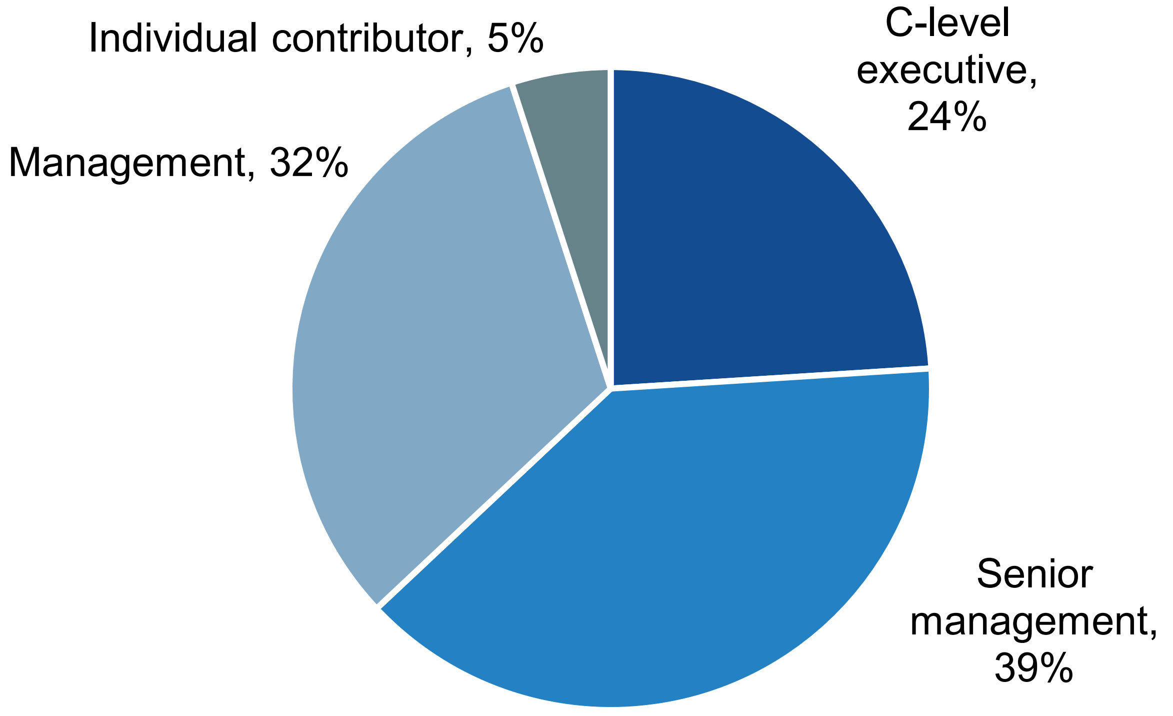
Respondents by country (Percent of respondents, N=100)



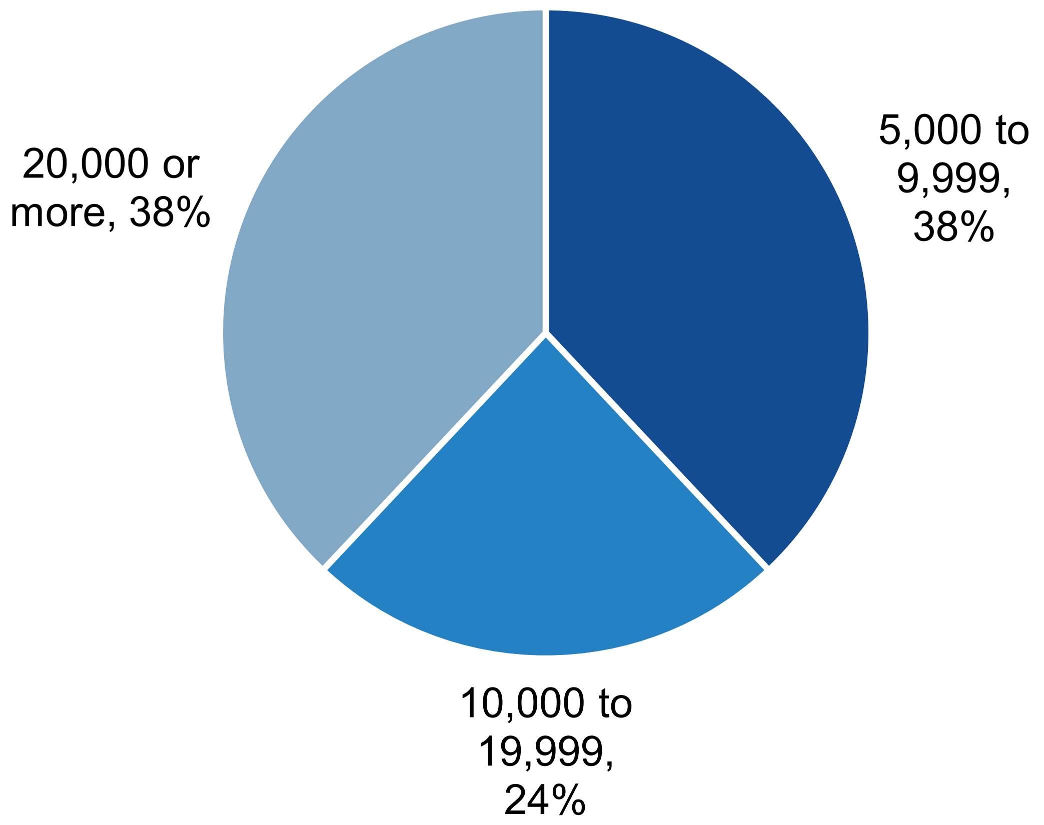
Which of the following best describes your current job function? (Percent of respondents, N=100)



Which of the following best describes your current job title/level? (Percent of respondents, N=100)



How many total employees does your organization have worldwide? (Percent of respondents, N=100)



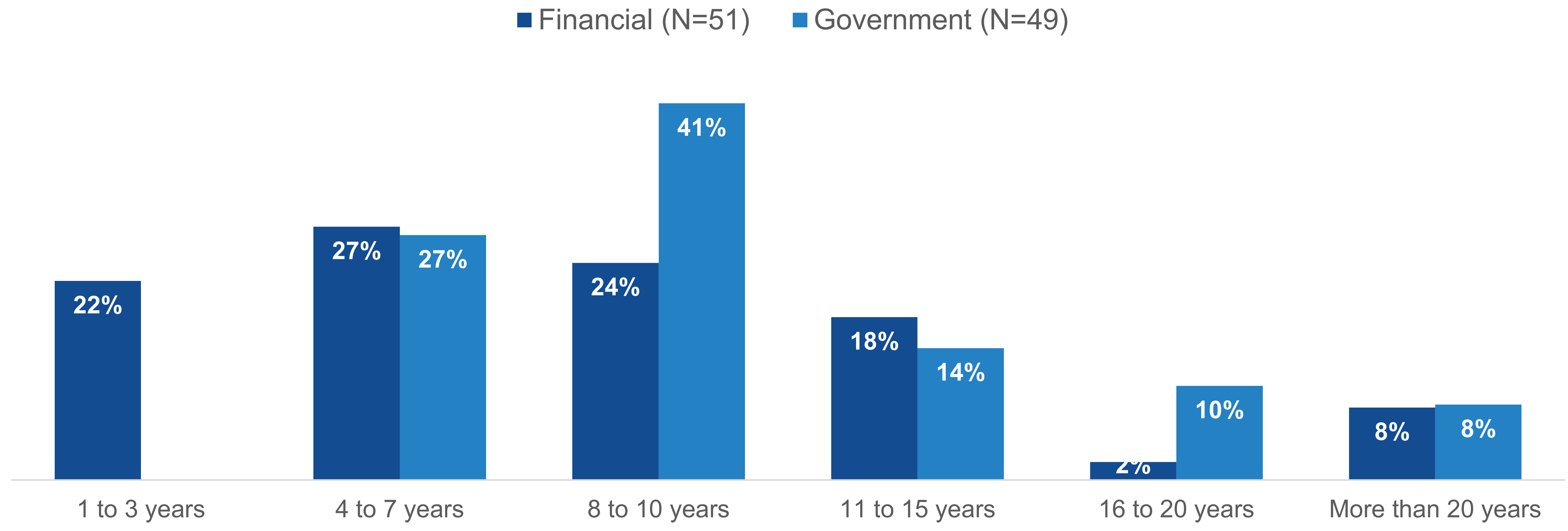
About Broadcom

Broadcom's Mainframe Software Division empowers enterprises to amplify the value of their mainframe investments in ways that drive their business forward. The company's market-leading AIOps, cybersecurity and compliance, data management, DevOps, and core infrastructure solutions enable clients to adopt common tools using industry standards and integrate mainframes as part of their hybrid cloud. Broadcom's commitment to partnership extends beyond software and features Beyond Code programs that give customers the power to achieve greater business success with the platform.

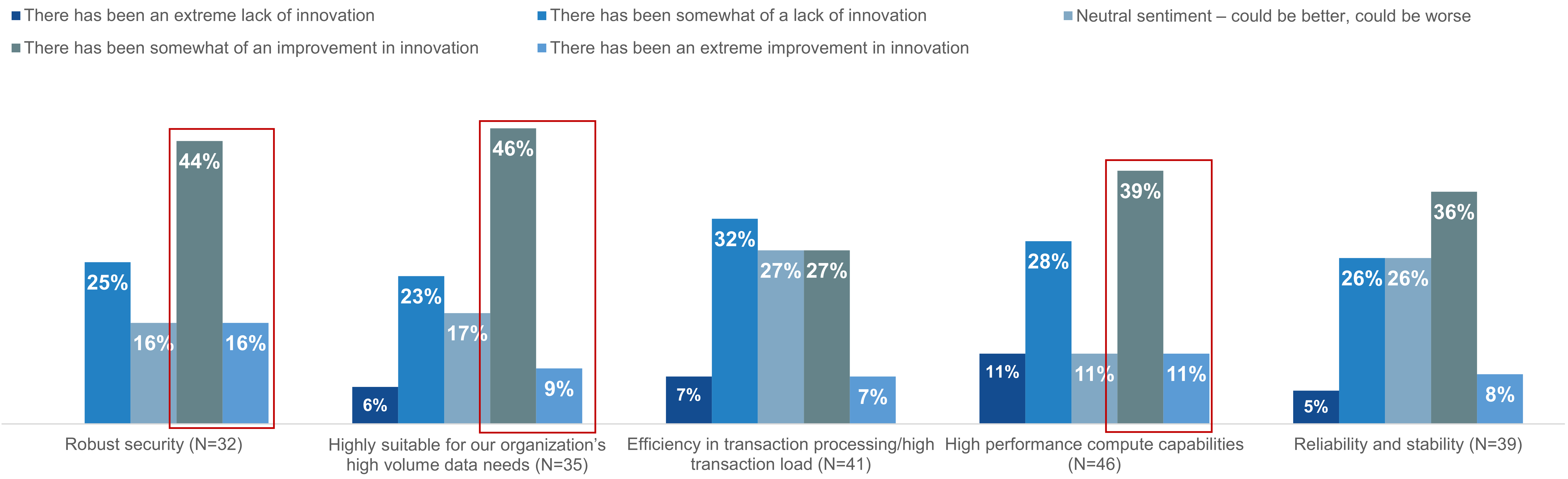
BROADCOM®

APPENDIX

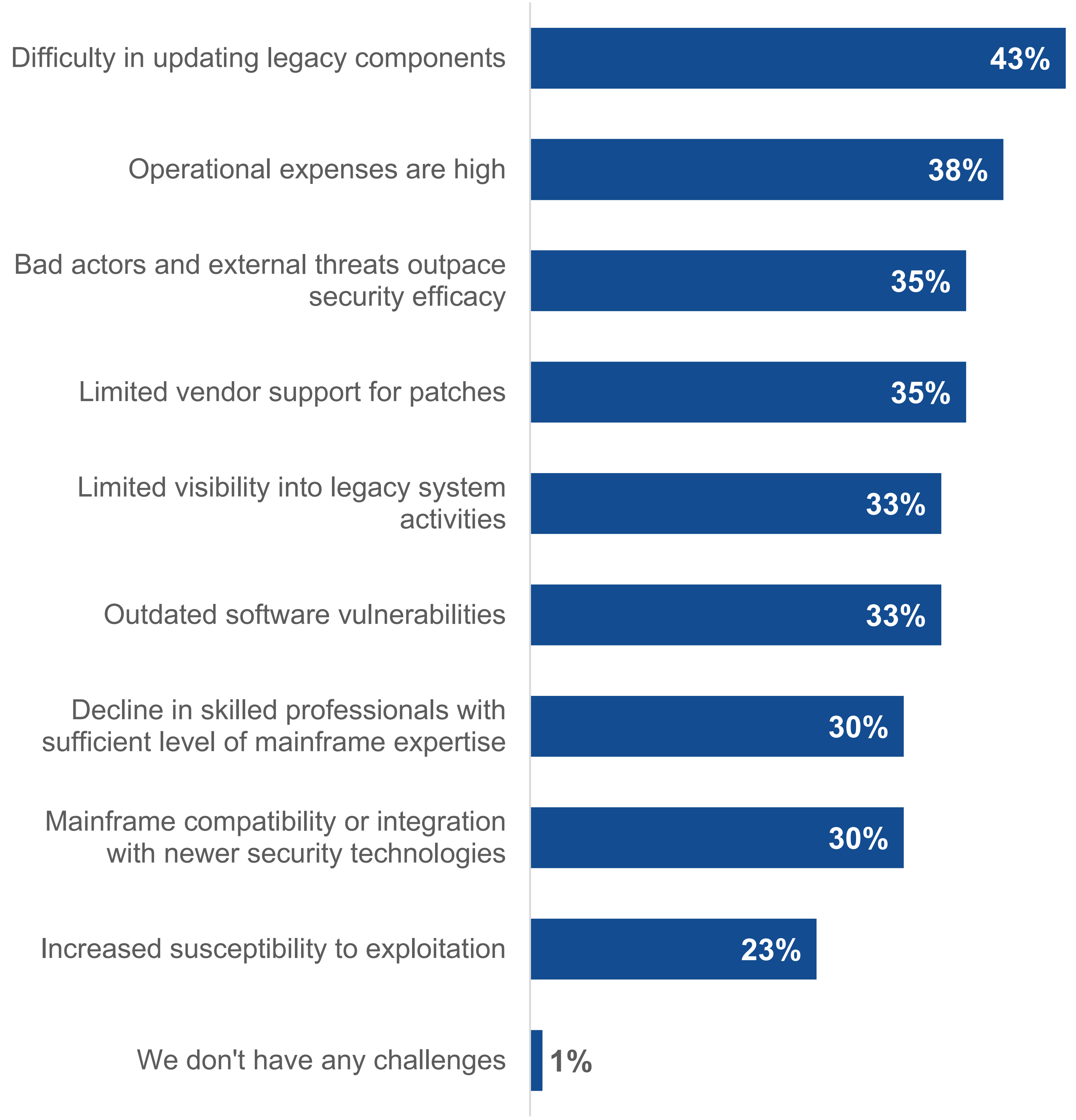
How long has your organization been operating its current mainframe software?



How do you feel about mainframe innovation over the last 2 to 3 years? (Respondents by perception on innovation, five responses accepted)



What are your organization's top challenges related to operating core business systems with current mainframe security technologies? (Percent of respondents, N=100, five responses accepted)



All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Enterprise
Strategy Group™
by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.