FORRESTER®

The Essential Holistic Security Strategy

Mainframe Security Is Dangerously Absent From Enterprise Strategy

A FORRESTER CONSULTING THOUGHT LEADERSHIP PAPER COMMISSIONED BY BMC, DECEMBER 2021

Table Of Contents

Project Director:
Madeline Harrell,
Market Impact Consultant

Contributing Research:
Forrester's security and risk research group

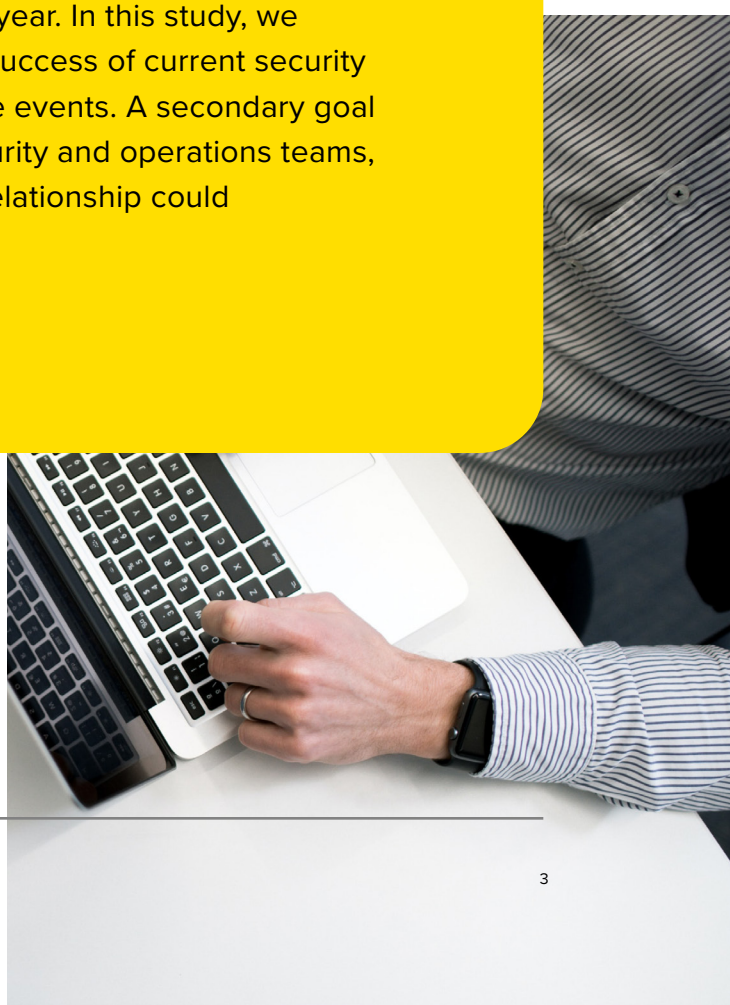
ABOUT FORRESTER CONSULTING

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.

Executive Summary

Previously in 2020, BMC commissioned Forrester Consulting to conduct a study that sought to understand the mainframe and security readiness of businesses and their priorities for change.[1] However, with the unexpected emergence of the COVID-19 pandemic — and the work-from-home employment model taking center stage — companies found themselves scrambling to secure trust between internet-connected devices and open devices in order to protect against untold amounts of risk. This involved companies forcing themselves to examine their lack of effective mainframe security practices and tools, which was created by making the mistake of trusting their mainframe as being inherently secure. Additionally, the increased adoption of Zero Trust challenged this perception and forced many to begin seeing the mainframe as something that is securable. The reality is that mainframe security — whether managed onsite or remotely — must scale in the same ways it has for other systems handling sensitive data.

In September 2021, BMC commissioned Forrester Consulting to conduct a second analysis of mainframe and security readiness with an online assessment of 310 respondents and four interviews with security and mainframe decision-makers. The purpose was to determine if companies have advanced their security readiness since last year. In this study, we primarily explored security events, as well as the success of current security operations tools and practices in addressing these events. A secondary goal was to understand the relationships between security and operations teams, when it comes to their integration, and how that relationship could be improved.



Key Findings

Companies know they must optimize their mainframe security strategy to scale with increased risk, but they aren't sure where to begin. As organizations scramble to properly manage any and all security events, many are leaning on a reactive strategy of increased headcount and budget with no real strategy or internal alignment amongst teams. Ninety-one percent of organizations with mainframes have experienced a compromise or breach of sensitive data in the last five years.

Companies are adopting a Zero Trust approach to mitigate risk as part of larger adjustments to their security strategy. Companies that are optimizing their security strategy are seeing improved internal alignment amongst teams and improved security technology. They are also benefitting from a Zero Trust approach, which should inherently include the mainframe as an internet-connected device. Seventy-one percent of respondents indicated that Zero Trust is a high or critical security priority for their organization over the next 12 months. Including mainframe security in this will be critical; 84% agree it is important to include mainframe security as part of a holistic Zero Trust strategy.

As companies pivot to a security-led approach, mainframe strategy is still slipping through the cracks. The 2020 study revealed how mainframes were considered to have a lower priority due to their perceived *secure* nature. Unfortunately, some firms still take this position in 2021. Others though are aware of this pitfall, and they are instead moving toward automation and orchestration to stack on top of their existing mainframe technology and processes.

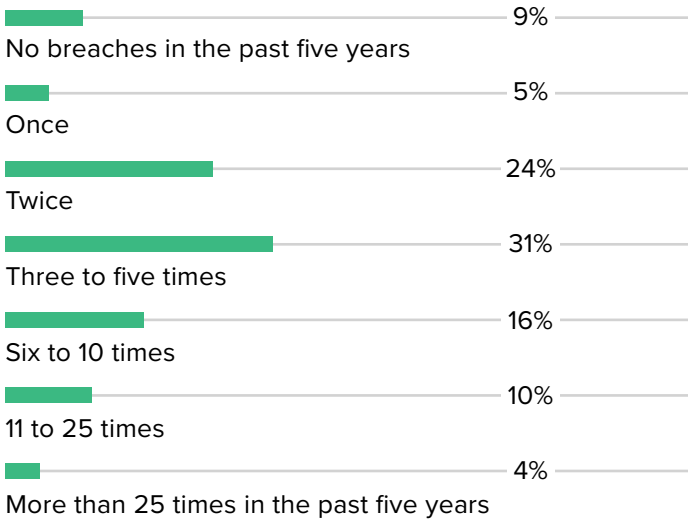
Increased Security Incidents Drive Organizations To Be Security-Led

As companies come to grips with the understanding that their previous approach to mainframe security was lacking, they must pivot multiple points in their strategy to remedy the issue. Depending on how forward-thinking their strategic practices are, companies have had to start reprioritizing their initiatives. Savvy security leaders will address their security program in a newly holistic way by improving security technologies, leadership and personnel changes, and internal alignment between teams. In surveying 310 security decision-makers with insights into mainframe security in EMEA and North America, we found that:

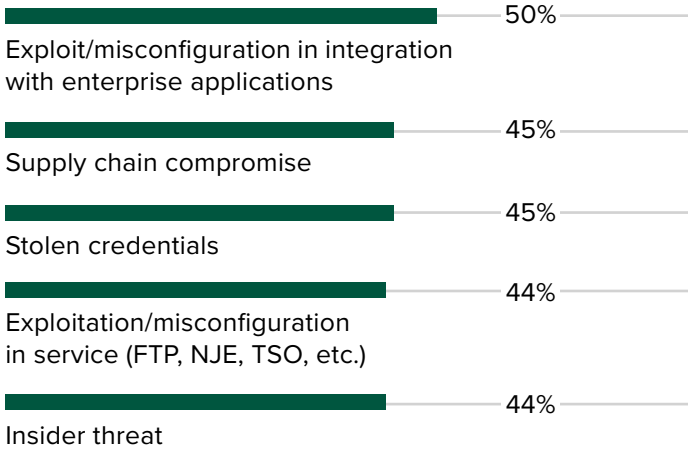
- **Frequent security events — that have included the mainframe — are driving urgency for companies to become security-led.** Ninety-one percent of organizations with mainframes have experienced a compromise or breach of sensitive data in the last five years; 26% have experienced compromises or breaches between six and 25 times. The most common attacks were exploitation or misconfiguration in integration with enterprise applications (see Figure 1). With the regular occurrence of security events seen in 2020, organizations are expanding their approach to overall business security. Integration of a Zero Trust approach will deepen security culture at the enterprise level while encouraging safety in the

Figure 1

"How many times do you estimate that your organization's sensitive data was potentially compromised or breached in the past five years?"



"How was the attack carried out?"

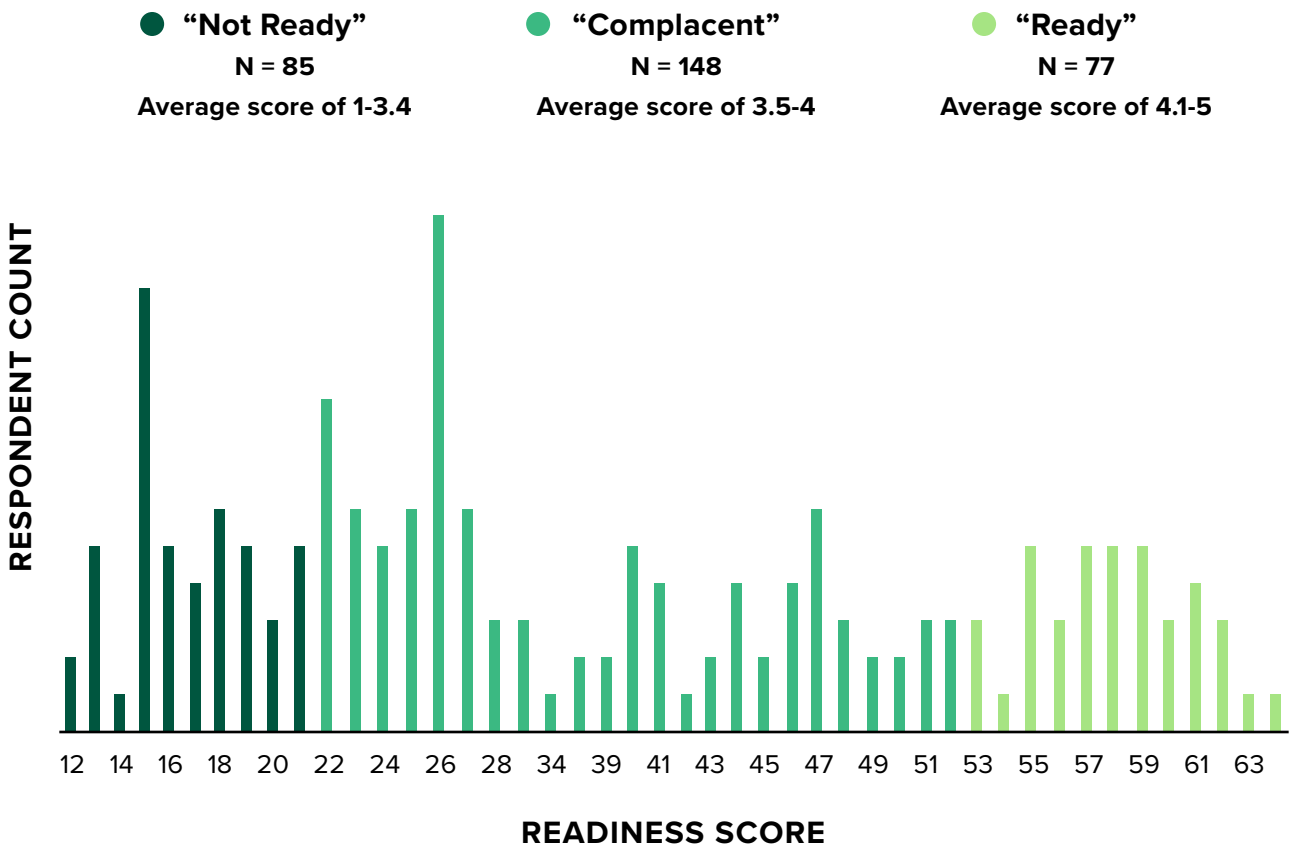


Base: 310 security decision-makers in North America and EMEA with insights into mainframe security
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, September 2021

mainframe as well. These security events have led to an increase in spending on mainframe security, security monitoring, and additional IT security staff. But are companies going about these investments in a strategic way?

- In order to understand the overall trend of security strategy optimization overall, we scored respondents based on several variables to understand their readiness to respond to mainframe-related security events. “Ready” organizations are performing key security tasks more often than those in the “Complacent” and “Not Ready” groups, and it shows. “Not Ready” organizations were twice as likely to have experienced 11 or more breaches of sensitive data in the last five years vs. “Ready” organizations (see Figure 2).

Figure 2

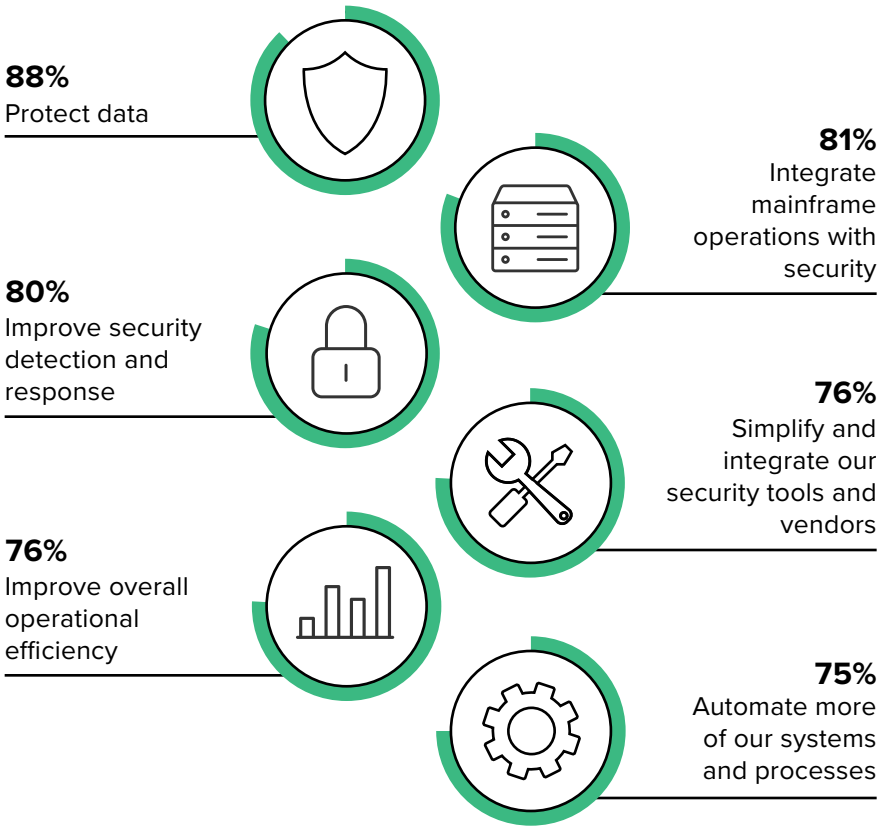


Base: 310 security decision-makers in North America and EMEA with insights into mainframe security
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, September 2021

- **Mainframe decision-makers are seeing the need to secure their mainframes, but enterprise actions are still playing catchup.** While some firms are actively working on a holistic security approach, those may not include strategies geared toward mainframes just yet. Respondents' number-one priority for the next 12 months is the same as it was last year: protecting data (88%). They are also prioritizing the integration of security functions (81%) and improving security detection and response (81%). This bodes well for improved alignment of internal teams that have previously not seen eye to eye (mainframe and security) — it also ensures protection against active threats (see Figure 3).

Figure 3

"How important are the following IT priorities to your organization over the next 12 months?"



Base: 310 security decision-makers in North America and EMEA with insights into mainframe security
Note: Top six responses shown out of 12 that were collected; additional options in appendix
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, September 2021

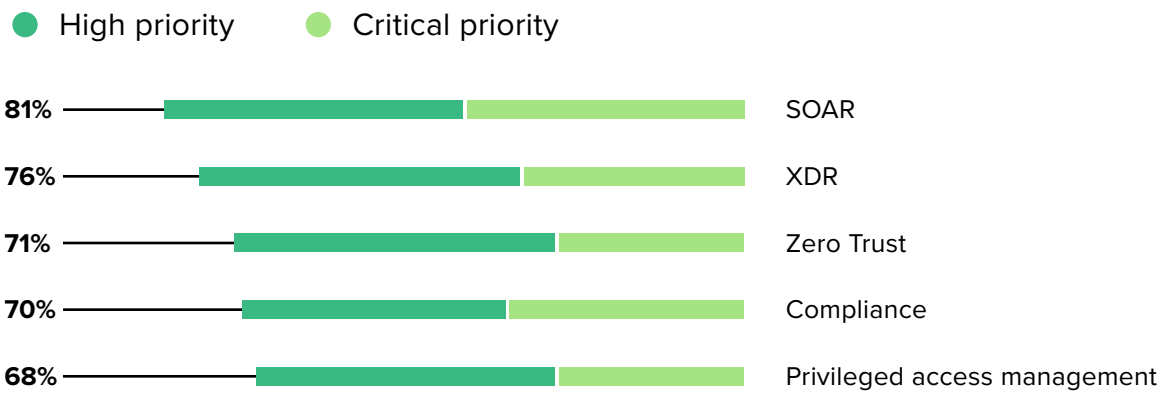
- **Taking mainframe security for granted? Big mistake.** We found that companies overall have decreased their mainframe security readiness. This is likely due to companies scrambling to protect their expanding attack surfaces, deprioritizing mainframe security in the process. However, mainframe security isn't going anywhere, and while the reputation of them being inherently secure exists, companies are realizing they need to fill in the persistent security gap with improved protections. Over the last year, the perception of mainframe security fell, so now there is a new, clearer understanding that mainframes still need to be actively secured. Companies are seeing the vast benefits of leaning into a Zero Trust approach that includes mainframe security. Seventy-one percent of respondents indicated Zero Trust is a high or critical security priority for their organization over the next 12 months. This priority is behind extended detection response (XDR) and security orchestration automation and response (SOAR) (see Figure 4).

91%

of organizations with mainframes have experienced a compromise or breach of sensitive data in the last five years.

Figure 4

"How important are the following security priorities to your organization over the next 12 months?"



Base: 310 security decision-makers in North America and EMEA with insights into mainframe security
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, September 2021

Leadership Must Produce Mainframe Champions To Encourage Top-Down Change

As companies cope with their expanded attack surfaces, they are laying the groundwork to advance their security strategy practices in the long term to avoid any future security events. With remote work being the norm for most people now and in the future, companies are seeing the need to continue investing in security. The mainframe is often one of the most critical systems to business operations, yet it is often overlooked in security strategies. A large part of prioritizing mainframe security will involve aligning security operations and mainframe security teams, that are tasked with securing the full company, with those that manage the mainframe.

- **Most teams are realizing their data isn't safe, but they aren't prioritizing mainframe security in response.** Only 29% of respondents are taking steps to actively secure their mainframes; this is down 12% from last year. The mainframe as a piece of technology is typically the most critical business server for companies, whereby it stores mission-critical data and workloads; so the urgency is there. Companies' key mainframe security priorities are led by: monitoring and threat detection (71%); data backup and recovery (66%); and database activity monitoring (66%). With this focus on resiliency and data, they will need the right tools and expertise for the mainframe to get the job done (see Figure 5).
    - The prioritization of mainframe security is exacerbated in "Complacent" and "Not Ready" organizations. To deal with the onslaught of security events, those "Not Ready" organizations are increasing spending on threat intelligence capabilities and focusing on managing the risk of third-party relationships. However, they should be focusing on direct mainframe activities: The categories of highest investment over the last five years for those "Ready" organizations include direct mainframe security practices (like increasing collaboration between security and operations teams), hiring additional IT security staff, and investing in mainframe

security. Meanwhile, the top response for "Not Ready" organizations has been to increase spending on security monitoring alone.

- While "Not Ready" organizations are building the framework for their security strategy, "Ready" organizations are focusing on the mainframe and ensuring they have the internal culture of collaboration to support these top-down changes. Additionally, "Ready" organizations report improved security mainframe management as the number one expected benefit of having a more aligned relationship between security and operations teams, while "Not Ready" organizations are simply expecting more efficient operations (see Figure 5).

> "Normally, if you ask internal people, they feel [the mainframe is] secure because it's contained. But when you start talking more from the leadership perspective, they feel that we have to continue doing more because we are opening the can of worms that is called cloud."
>
> **Senior director, IT Architecture at a financial services company**

Figure 5

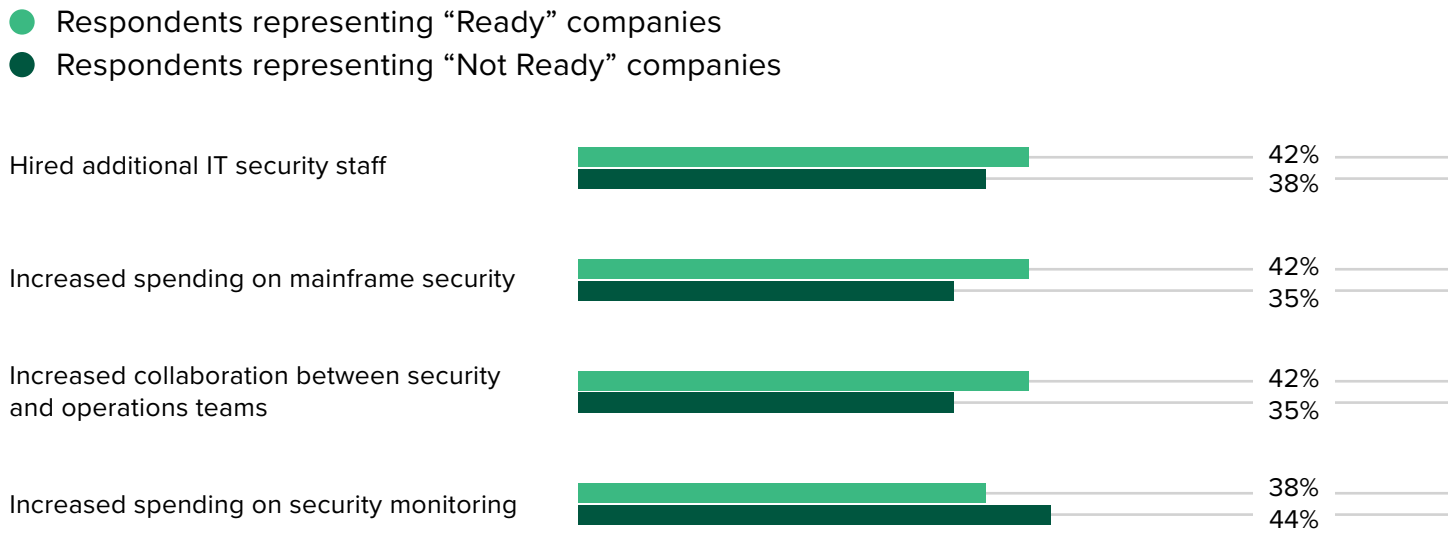
"What components of mainframe security is your organization most focused on?"

71%	66%	66%	61%	61%
Monitoring and threat detection	Data backup and recovery	Database activity monitoring	Identity access management	Incident response

Base: 310 security decision-makers in North America and EMEA with insights into mainframe security
Note: Top five responses shown
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, September 2021

Figure 5 (Cont'd)

"What has changed at your organization as a result of the breaches occurring in the past five years?"



Base: 77 "Ready" respondents and 85 "Not Ready" respondents out of 310 security decision-makers in North America and EMEA with insights into mainframe security
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, September 2021

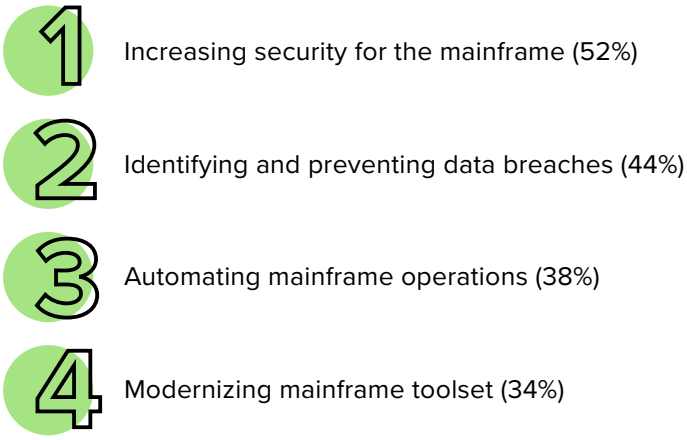
- **Companies are looking to expand resources via employee training and managed services.** In order to avoid the number of exposures organizations have faced over the last five years, information technology decision-makers (ITDMs) are currently focusing on increasing security for the mainframe, identifying and preventing data breaches, automating mainframe operations, and modernizing the mainframe toolset (see Figure 6). As part of the charge to keep their mainframes secure, 85% of respondents agree that their organizations look to managed services to help them manage their mainframe security. As for increased protection via internal resources, they also agree that it is easier to reskill existing employees than it is to hire new ones. However, 85% also agree that they are prioritizing hiring and training recent graduates to help with mainframe operations. It's a never-ending challenge to find the right personnel within the existing market, and it is easier to either train a new workforce from the start or reskill existing employees. With this in mind, organizations need the right tools in place

to start off on the right path toward modernizing mainframe operations and security. Recommended tools include: 1) those that deliver the same capabilities as distributed security tools (with a better user experience) and 2) those with contextualized data to allow non-mainframe security teams the visibility to take action.

> "If anybody tells you that they are not having challenges locating mainframe people, they're lying to you."
>
> **Senior director, IT architecture at a financial services company**

Figure 6

Mainframe Priorities



Base: 310 security decision-makers in North America and EMEA with insights into mainframe security
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, September 2021

- **Organizations are struggling to get mainframe and security teams aligned both on culture and goals.** Over half (55%) of companies say there is friction between their security and operations teams. Similarly, 55% also agree their security and operations teams are too siloed to effectively work together. This is specifically true at the practitioner level, while higher level leadership doesn't feel the same degree of disconnect. For there to be increased alignment, leadership needs to recognize the challenges in removing siloes between teams and

make strides toward collaborative strategic decision-making. Top-down changes to improve internal collaboration and mainframe security will need to be spearheaded by leadership in both security and operations departments.

- **Mainframe security needs to be included in Zero Trust.** Despite the lack of attention given to mainframes in the past, and the low numbers of respondents that are currently securing their mainframes, companies are beginning to realize that mainframe security is not bulletproof. In fact, 84% agree it is important to include mainframe security as part of a holistic Zero Trust strategy. In order to secure the system from the inside out, companies are making the move from a perimeter-based security model to one that is based on minimizing trust by continuously verifying that access is secure, authenticated, and authorized. Additionally, 68% of companies indicate that privileged access management is a high or critical security priority in 2022. This directly addresses the user error and insider risk challenges that companies have seen rise over the last 12 months. It is up to enterprise leadership to lead the change in company security strategy by breaking down team siloes and encouraging the creation of a healthier security culture that includes both Zero Trust and mainframe security.

> "All these practices and controls that [security leadership is] putting in place are not well received by my mainframe people. So it has been more of an educational process, telling them what exactly the implications are if we don't follow those protocols."
>
> **Senior director, IT architecture at a financial services company**

Work Smarter Not Harder To Reduce Risk

Firms are being forced to either modernize or migrate their mainframe workloads due to pressures of risk exposure. And unfortunately, those "Not Ready" companies are dealing with detection issues; while "Ready" companies are in the beginning stages of rolling out a more proactive approach. With these changes taking place across the market, companies must not forget the security risks that come with data migration and their lack of detection capabilities. It's worth noting that the more advanced companies are already experiencing the benefits of securing their mainframes, with the largest benefits matching up with most companies' 2022 priorities.

- **To improve efficiency and reduce risk and cost, secure your mainframes now.** While companies strive to improve detection, prevention, and employee productivity, their strategy so far has been to throw money and headcount at the issue — in the form of detection technologies and new FTEs, respectively. A key action they should be taking is investing in the security of their full data environment, which naturally includes the mainframe. Rather than solely relying on onboarding new FTEs to fill the space, they can invest in Zero Trust and mainframe-specific security practices to protect their data and reap business benefits. In this study, we have seen that "Ready" companies are investing in and expecting to benefit from: 1) monitoring and detection/response capabilities and 2) improved collaboration between security and operations teams. Mainframe security could stand to benefit from compounding increased collaboration with both mainframe operations automation and mainframe toolset modernization across all maturity levels.
- **Easing the burden on internal personnel while also increasing internal alignment on strategy activation is expected to improve security overall.** Respondents indicate that after securing the mainframe, they expect and have seen reduced risk to the business (61%), protection of corporate brand identity (61%), and reduced technology-related risks (52%). While the benefits of an optimized

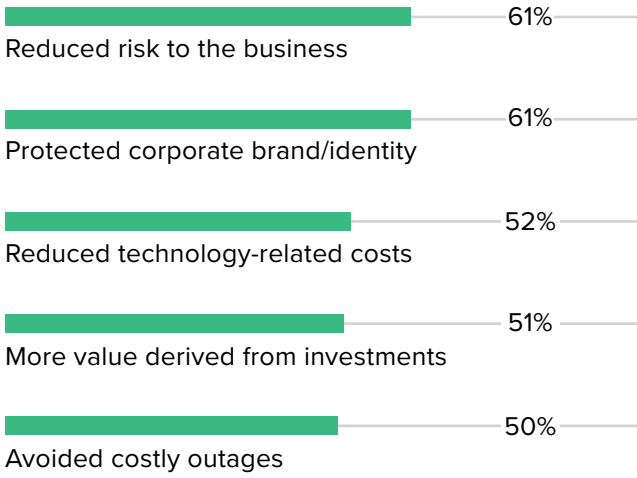
security strategy are clear, the availability of new FTEs is still a concern for the market. Companies need to get creative with filling neccesary headcount by either training existing employees or upping the ante for potential hires with new tools that'll better enable their future success. Mainframe security needs internal champions to remind the larger company of its power, relevance, and vulnerability to attack (see Figure 7).

- "Ready" companies are experiencing more advanced benefits overall, such as improved security monitoring (64%), reduced security risks (63%), and improved operational efficiency (58%). On the other hand, "Not ready" companies are still reaching for more basic benefits like reduced cyberattacks/breaches (43%), reduced security risks (43%), and consistent performance (39%).

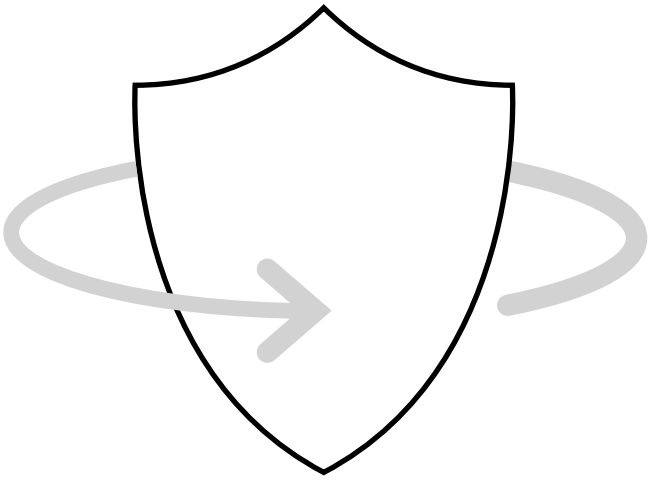
- **Aligning mainframe and security teams via respective champions improves efficiency and the overall security culture.** Better team relations are especially good for mainframe security, but this is a lofty goal for those without leadership guiding the way. In order for security and operations teams to effectively collaborate, they will need champions from both teams leading the way to improved security and efficiency. Over half of organizations that have increased alignment between security and operations teams have seen improved mainframe security management and more efficient operations, while nearly half have seen faster incident response times.

Figure 7

"What benefits have you seen/ would you expect from having a secure mainframe?"



Base: 310 security decision-makers in North America and EMEA with insights into mainframe security
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, September 2021

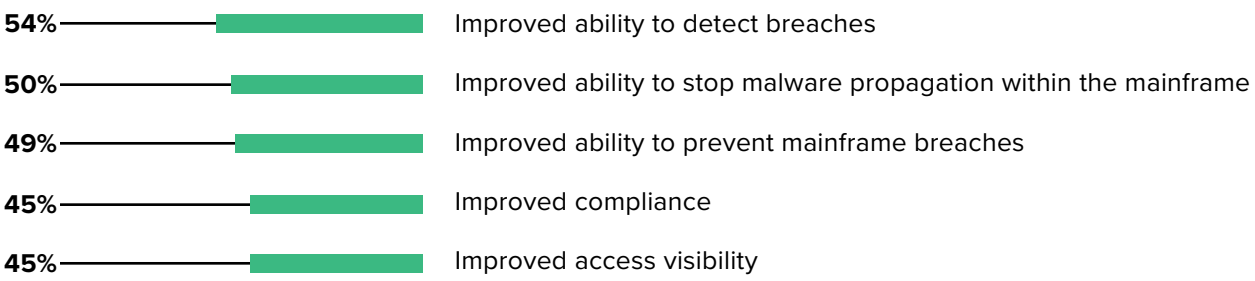


- **Carefully and thoughtfully including mainframe security in Zero Trust strategies delivers a clear ROI.** As companies turn to improved methods of day-to-day mainframe management and security, the need to include it in their burgeoning Zero Trust strategies is paramount. Those organizations that are expecting to adopt a Zero Trust approach for their mainframe, or have already adopted one, have seen an improved ability to: detect breaches (54%); stop malware propagation within the mainframe (50%); and prevent mainframe breaches (49%). This speaks to their intention of improving both incident response and prevention. While the benefits of adopting Zero Trust are clear, it is important to note that proper implementation and employee onboarding to new practices is prioritized. It will be crucial to approach this shift with thoughtful change management and eyes and ears open to feedback from employees for successful adoption to take place (see Figure 8).

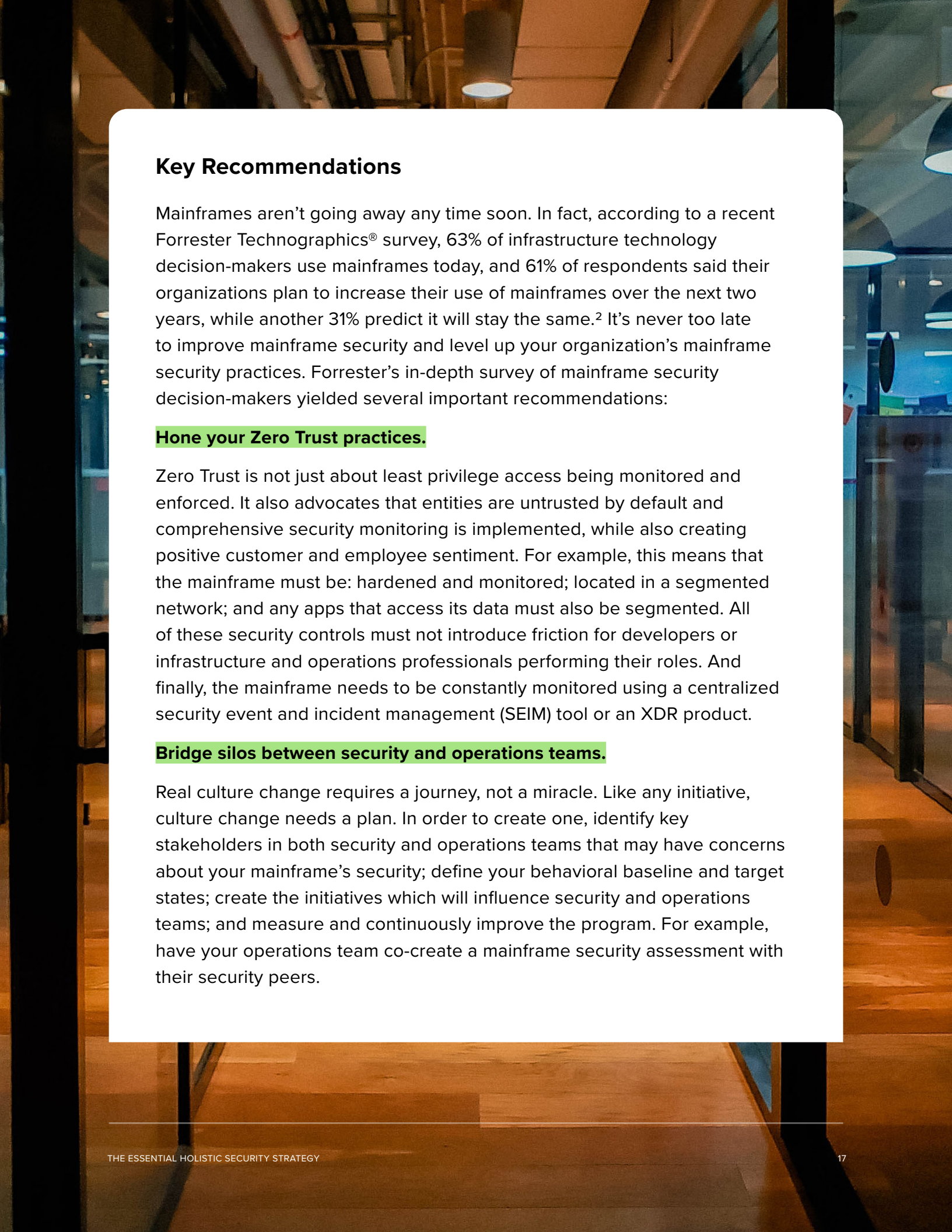
> "Everyone is talking about [Zero Trust] architecting but understanding the real benefits around [Zero Trust] and how to apply it, the framework gives you many flexibilities. It gives you better compliance, it gives you better audits so you can actually demonstrate to your auditors in the case that something happens."
>
> **Senior director, IT architecture at a financial services company**

Figure 8

"What technology benefits would you expect to see or have you seen from adopting a Zero Trust security approach for your mainframe?"



Base: 310 security decision-makers in North America and EMEA with insights into mainframe security
Note: Showing top five responses out of 11 that were collected
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, September 2021



Key Recommendations

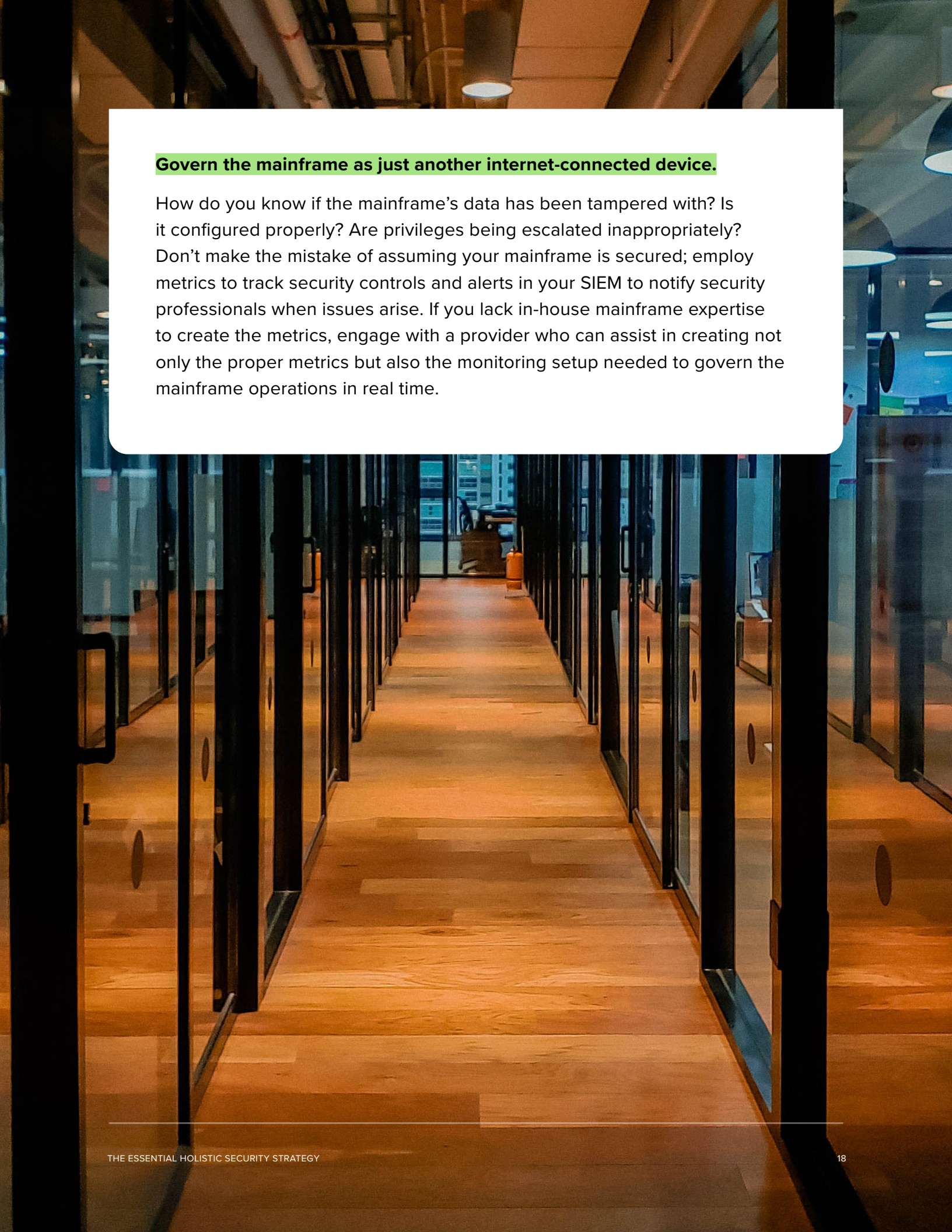
Mainframes aren't going away any time soon. In fact, according to a recent Forrester Technographics® survey, 63% of infrastructure technology decision-makers use mainframes today, and 61% of respondents said their organizations plan to increase their use of mainframes over the next two years, while another 31% predict it will stay the same.[2] It's never too late to improve mainframe security and level up your organization's mainframe security practices. Forrester's in-depth survey of mainframe security decision-makers yielded several important recommendations:

Hone your Zero Trust practices.

Zero Trust is not just about least privilege access being monitored and enforced. It also advocates that entities are untrusted by default and comprehensive security monitoring is implemented, while also creating positive customer and employee sentiment. For example, this means that the mainframe must be: hardened and monitored; located in a segmented network; and any apps that access its data must also be segmented. All of these security controls must not introduce friction for developers or infrastructure and operations professionals performing their roles. And finally, the mainframe needs to be constantly monitored using a centralized security event and incident management (SEIM) tool or an XDR product.

Bridge silos between security and operations teams.

Real culture change requires a journey, not a miracle. Like any initiative, culture change needs a plan. In order to create one, identify key stakeholders in both security and operations teams that may have concerns about your mainframe's security; define your behavioral baseline and target states; create the initiatives which will influence security and operations teams; and measure and continuously improve the program. For example, have your operations team co-create a mainframe security assessment with their security peers.



Govern the mainframe as just another internet-connected device.

How do you know if the mainframe's data has been tampered with? Is it configured properly? Are privileges being escalated inappropriately? Don't make the mistake of assuming your mainframe is secured; employ metrics to track security controls and alerts in your SIEM to notify security professionals when issues arise. If you lack in-house mainframe expertise to create the metrics, engage with a provider who can assist in creating not only the proper metrics but also the monitoring setup needed to govern the mainframe operations in real time.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 310 respondents and four interviews with security and mainframe decision-makers at organizations in North America and EMEA to determine if companies have advanced their security readiness since last year. It also sought to understand the nature of the relationship between their security and operations teams. Survey participants included decision-makers in security and IT. The study began and was completed in September 2021.

Appendix B: Demographics

GEOGRAPHIES	
US	**43%**
Canada	**9%**
UK	**12%**
Spain	**7%**
Italy	**10%**
France	**11%**
Germany	**10%**

COMPANY SIZE	
>$5B	**14%**
$1B to $5B	**31%**
$500M to $1B	**36%**
$400M to $499M	**12%**
$300M to $399M	**7%**

INDUSTRY (TOP 5)	
Technology and/or tech services	**11%**
Financial services and/or insurance	**9%**
Retail	**7%**
Manufacturing and materials	**7%**
Telecommunications services	**6%**
Consumer product goods and/or manufacturing	**6%**

RESPONDENT LEVEL	
C-level executive	**18%**
Vice president	**21%**
Director	**28%**
Manager	**33%**

DEPARTMENT	
Security	**41%**
IT	**59%**

RESPONSIBILITY FOR MAINFRAME SECURITY	
Final decision-maker	**25%**
Part of a team making decisions	**45%**
Influences decisions	**30%**

Appendix C: Endnotes

[1] Source: "A False Sense Of Mainframe Security," a commissioned study conducted by Forrester Consulting on behalf of BMC, July 2020.
[2] Source: Forrester Analytics Business Technographics Infrastructure Survey, 2021.


FORRESTER®