Rocket® software

The State of Mainframe Security

2023 Survey Report

Contents

Introduction

In the era of rapid digital transformation, mainframe systems—often deemed the bedrock of enterprise infrastructure—remain as relevant as ever. Mainframes remain unmatched when it comes to reliability, scalability, and security when processing vast amounts of data.

With the integration of new-age methodologies like DevOps, the embrace of open-source philosophies, and the move towards hybrid cloud solutions, the digital terrain is undergoing an unprecedented surge in activity. Each brings its own set of obstacles and opportunities, reshaping the way businesses operate and innovate. Yet, this dynamic evolution also magnifies potential vulnerabilities and security risks. With constantly changing rules and shifts in how software is developed and used, it's more important than ever to focus on mainframe security.

To gain a better understanding of how IT leaders view mainframe security – and the actions they plan to take to keep the mainframe secure – Rocket Software, a global technology leader that develops enterprise software for some of the world's largest companies, conducted a survey of 250 global IT directors and vice presidents in companies with more than 1,000 employees. Respondents were asked about their current mainframe security plan, if they are integrating security into their DevOps processes, and their thoughts on introducing open-source software into workflows.

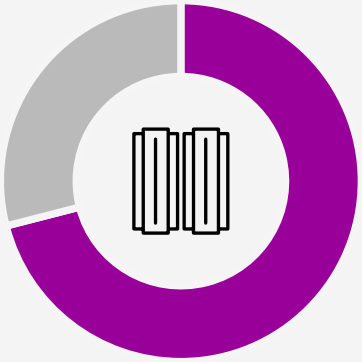
← Back to contents

The State of Mainframe Security

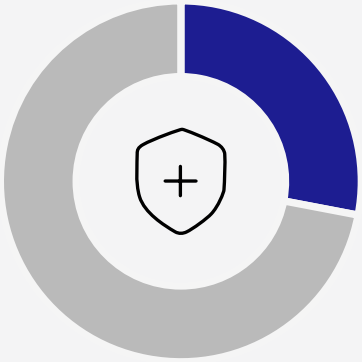
Mainframes continue to be an integral component in the technology infrastructure of many enterprises. Notably, they are leveraged by 71% of Fortune 500 companies, underlining their pivotal role in large-scale business operations. IT leaders have also voiced their trust in mainframes, particularly in their capability to handle core business applications; over half, or precisely 51%, have indicated that they run either all or the majority of these applications on the mainframe.

A deep dive into the reasons behind this reliance revealed that security is the paramount consideration for organizations. Security, in fact, topped the list of reasons, followed closely by factors such as reliability, efficiency, availability, and the total cost of ownership (TCO). However, while mainframes are lauded for their benefits—security chief among them—they are not without challenges. When respondents were asked about the main challenges their organizations face in ensuring effective mainframe security, they noted:

Amidst these challenges, there's an overarching concern regarding the confidence in addressing mainframe security vulnerabilities. A mere 28% of organizations feel **extremely confident** in their proactive response to these vulnerabilities. Such a confidence gap underscores the potential risks these organizations face, especially when considering the potential loss or leakage of invaluable data, be it financial records, trade secrets, or even sensitive customer information. According to one report, the global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years. The findings accentuate the need for improved resource allocation and talent sourcing to fortify security across the board.



Mainframes are leveraged by 71% of Fortune 500 companies.



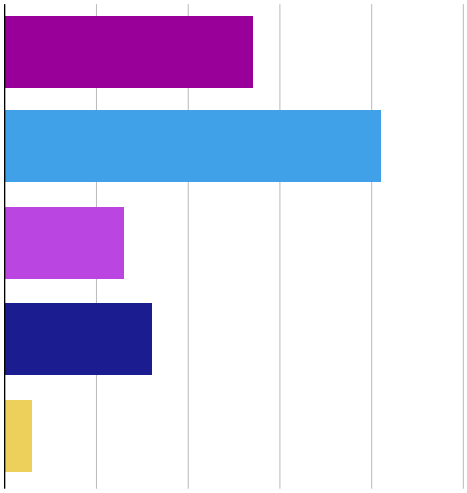
Only 28% of organizations feel extremely confident in their proactive response to mainframe security vulnerabilities.

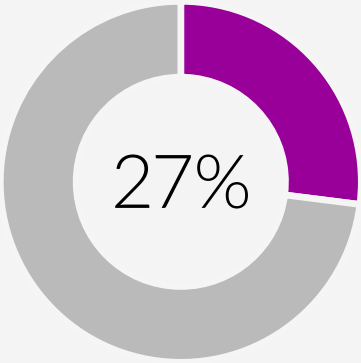
← Back to contents

Measures Being Taken to Protect the Mainframe

Thankfully, 68% of respondents noted that mainframe security is an area that their organizations take seriously. However, 27% of respondents know it's important but don't have enough funding or resources to contribute as much as they feel they should. With the mainframe holding so much mission-critical data, it's more important than ever to make sure it is secure. When asked which of the following best describes their organization's attitude to mainframe security, respondents noted:

27%	IT security is our most important priority, but we do not have enough funding or resources to contribute as much as we should to mainframe security
41%	Mainframe security is one of our top priorities and we contribute significant funding and resources to it
13%	We actively work to meet mainframe compliance standards, but it is not a top priority
16%	Our mainframe security is primarily an administrative function based on authentication and authorization needs
3%	Mainframe security is not a priority for our organization





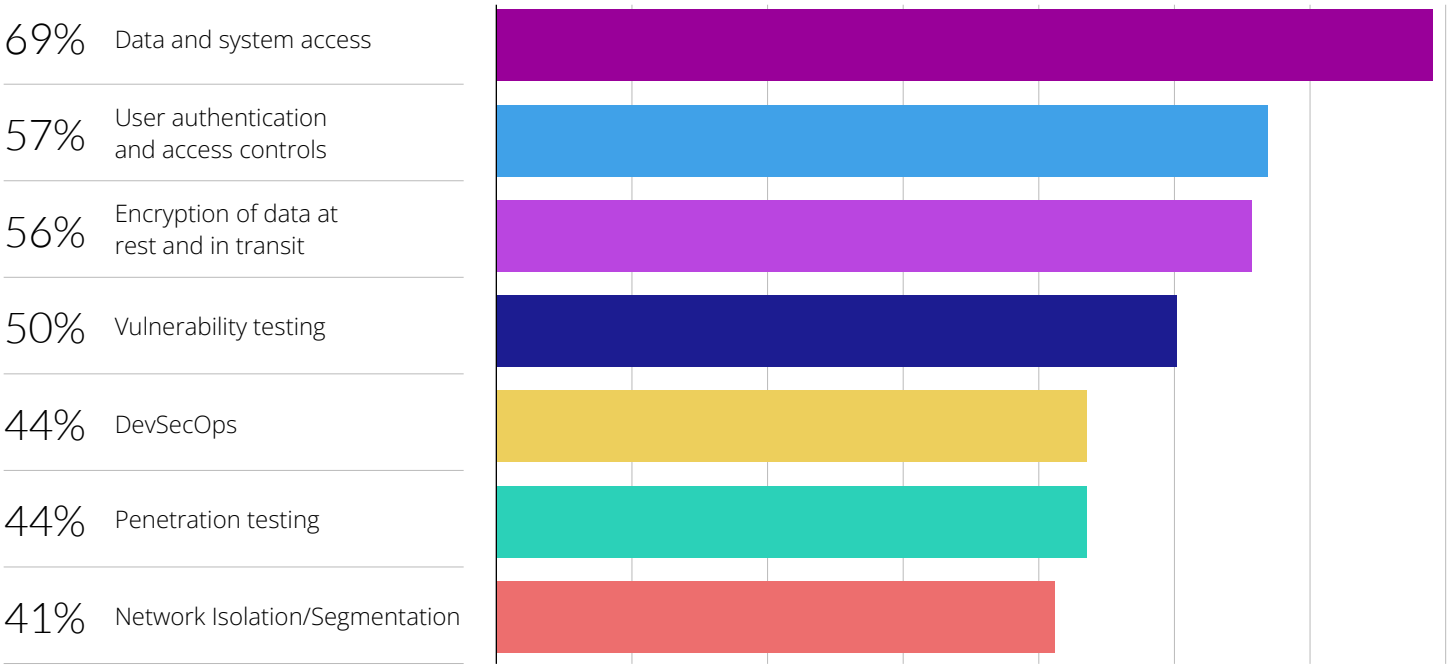
Twenty seven percent of respondents know mainframe security is important, but their organizations don't have enough funding or resources to contribute as much as they feel they should.

The frequency of security assessments varies among organizations: 33% conduct these vital compliance assessments for their mainframes every 1-2 years, whereas a more proactive 56% undertake them annually.

When it comes to bolstering the security consciousness of an organization's workforce, the landscape again presents a mixed bag. Sixty two percent of organizations consistently offer training or educational initiatives aimed at heightening security awareness among their teams, which is standard industry practice. On the flip side, 31% limit such endeavors to a one-to-two-year interval.

← Back to contents

Delving into the practical measures organizations adopt to shield their mainframes, respondents shared how their organizations are focused on:



The key takeaway, however, is that the most resilient defense mechanism for mainframes is not a singular strategy. Instead, a holistic approach, blending multiple security methods, stands as the most effective buffer against both internal and external threats.

The Risk of a Breach

In the realm of mainframe security, adhering to regulatory and industry standards isn't just a box to check—it's a non-negotiable imperative. The rise in rules and regulations, such as the GDPR and PCI DSS, reflects the global push for greater data protection and privacy in the digital age.

Organizations are now required to maintain more stringent standards for collecting, processing, and storing personal data, ensuring the rights of individuals are at the forefront of digital interactions. These evolving regulations underscore the need for businesses to be transparent, accountable, and proactive in safeguarding user data in an increasingly interconnected world.

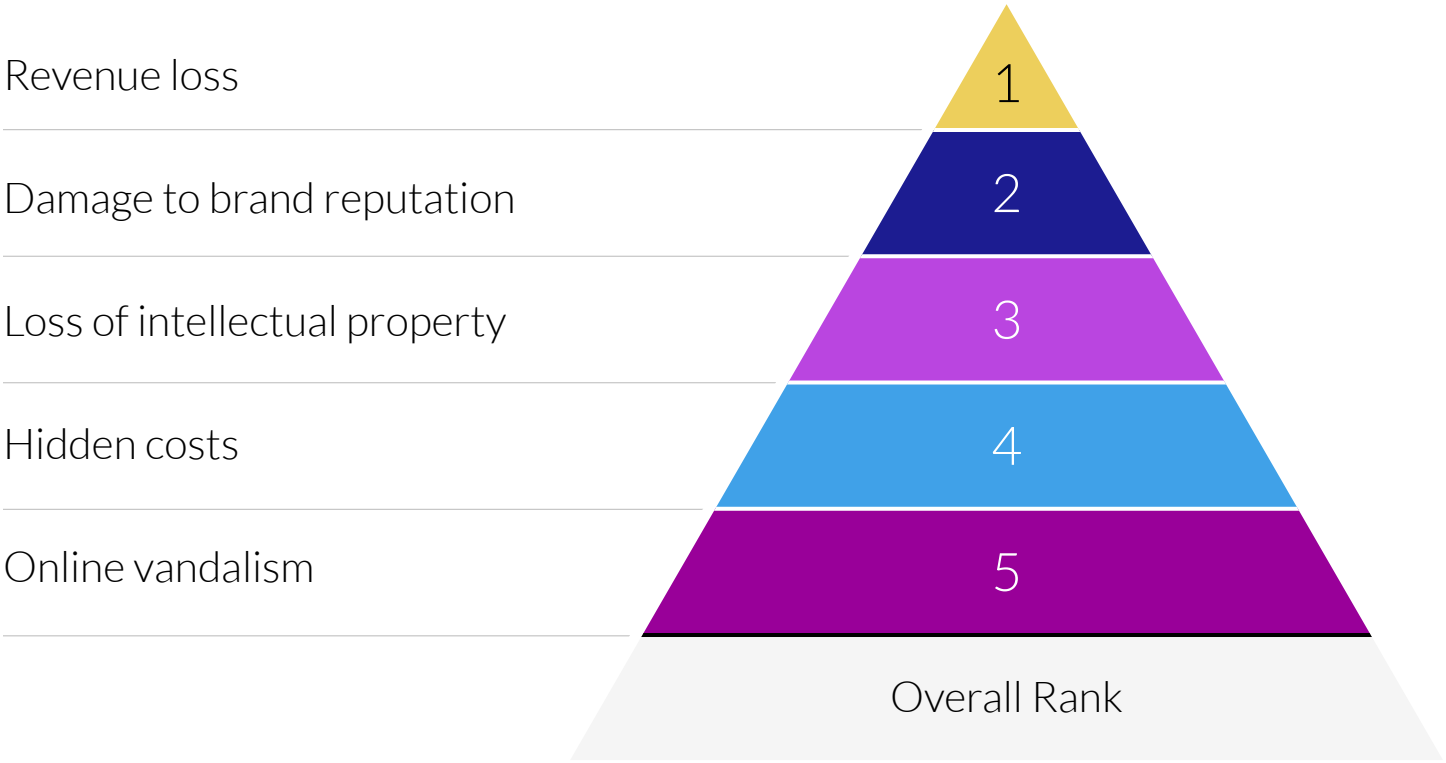
Only 27% of respondents believe their organization is **extremely effective** at ensuring compliance as it pertains to mainframe security.

Compliance isn't just an internal endeavor. Businesses must also keep an eye on their third-party suppliers. Why? Making sure suppliers meet quality standards (QA) is as important as internal compliance, especially for heavily regulated industries like banking and healthcare. Yet, only 31% of respondents are fully convinced of their organization's effectiveness in making certain that vendors stick to these rigorous QA benchmarks.

Quality assurance (QA) is any systematic process of determining whether a product or service meets specified requirements.

← Back to contents

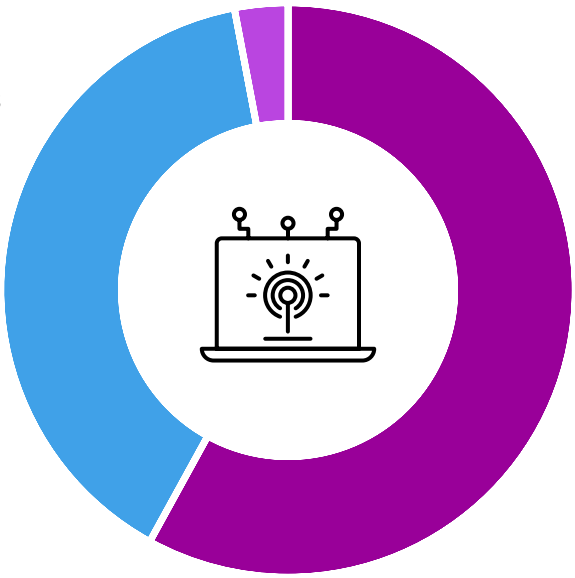
The repercussions of a security breach can be staggering. Surveyed respondents were unequivocal in their rankings of the potential aftermaths of a security threat:



While the threat of a breach looms large, how prepared are businesses in its wake? The respondents' feedback paints a mixed portrait. Ninety seven percent of organizations believe they can isolate workloads, but 39% acknowledge that isolating workloads takes precious resources and lengthy cycles internally – and that can quickly translate into lost dollars and a damaged brand reputation. This data brings forward the pressing need for organizations to not just bolster their mainframe defenses but also equip themselves for rapid, effective responses when breaches occur.

3%
No, we have no way to isolate workloads in the event of a breach

39%
Yes, but it takes several steps and time to isolate workloads



58%
Yes, we can isolate workloads quickly

← Back to contents

Risk and Opportunity: Open Source and DevOps

Open source and DevOps are not merely buzzwords anymore; they're invaluable assets in the arsenal of mission-critical organizations that are modernizing in place with the mainframe. While open source paves the way for myriad benefits, it does come with its fair share of risks. It allows for community collaboration and transparency, but that also means that potential attackers can examine the code for vulnerabilities. A predominant concern centers around the security and integrity of open-source components embedded within mainframe applications. While open-source communities can quickly apply patches and fixes to critical vulnerabilities and exposures (CVE), these fixes generally aren't applied to z/OS®-ported instances of the tools and languages. Applying updates and CVE fixes is incumbent on users within organizations or the vendors who have ported the languages and tools for use on z/OS. For that reason, vendor support is critical when leveraging open source on the mainframe.

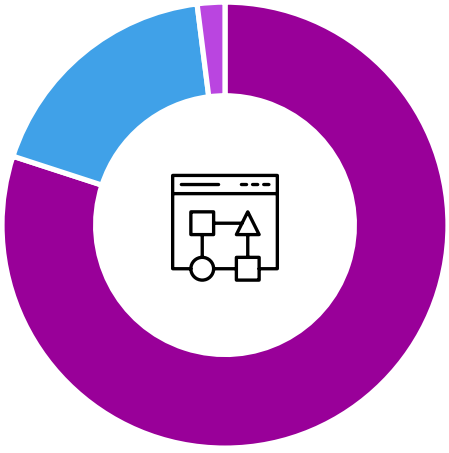
The good news is that organizations are taking open source and mainframe security seriously. Proactive measures dominate the landscape, with 62% of organizations routinely conducting vulnerability assessments and security audits, leveraging solutions like z/Assure VAP. Furthermore, 58% of respondents noted they engage in continuous monitoring and updating of open source to address security patches promptly. Fifty-four percent noted they are training developers on best practices for secure coding and popper usage of open-source components.

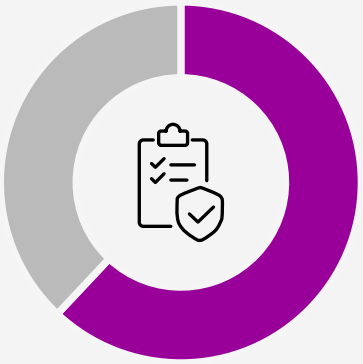
Does your organization have a well-defined process for managing and monitoring the usage of open-source software in mainframe environments?

2%
No, we do not have a well-defined process and no plans to implement one in the next 12 months

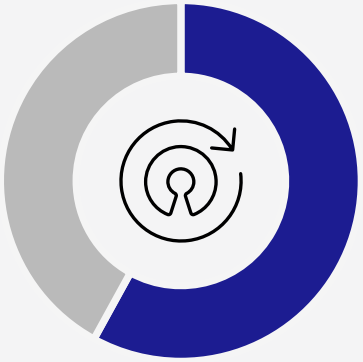
18%
No, but we are currently looking to implement one

80%
Yes, we have a well-defined process





62% of organizations routinely conduct vulnerability assessments and security audits.



58% of respondents engage in continuous monitoring and updating of open source to address security patches promptly.

Learn more

← Back to contents

While this is a positive development, the scalability of maintaining security and compliance with unsupported open-source software, as it evolves and expands within an enterprise, remains a major concern. It warrants investigating the benefits of vendor-supported open-source languages and tools to ensure security is never compromised for the sake of modernization.

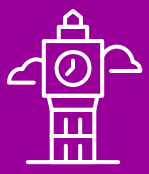
In the rapidly evolving landscape of cyber threats, the reflexes of the open-source community are paramount, **but even more important is ensuring the updates and fixes those communities make are applied to their open-source tools and languages that have been ported to z/OS**. A heartening 78% of survey participants displayed high confidence—ranging from extreme to considerable—in the open-source community's capacity to act promptly, underlining its pivotal role in the holistic security framework. **Ensuring you work with a vendor who can extend that promptness to open-source tools and languages ported to z/OS is equally important.**

At the same time, incorporating security best practices into your DevOps toolchain—also known as DevSecOps—helps ensure security remains a consistent, shared responsibility throughout the software development life cycles and that security updates are added quickly and smoothly, reducing the chance of threats. However, seamlessly integrating mainframe security with DevOps presents its own set of intricacies. Respondents to the survey shed light on these hurdles, spotlighting limited automation and integration capabilities within DevOps pipelines as the prime concern.

When asked to rank potential barriers, respondents said:

1. Limited automation and integration capabilities for mainframe security in DevOps pipelines
2. Incompatibility between legacy mainframe security tools and modern DevOps toolchains
3. Auditability and tracking of changes and actions, such as when someone requests authorization
4. Resistance to change from traditional security practices
5. Lack of specialized skills and expertise in mainframe security within a DevOps team

Breaking it Down by Industry and Location



By far and away, the United Kingdom relies on the mainframe for security purposes – with 56% of U.K. respondents citing it as the number one ranked reason for the mainframe.

When asked about challenges organizations face in ensuring effective mainframe security – respondents in the United States noted a lack of awareness about mainframe security risks – more than any other country.

Interestingly, respondents who work in manufacturing, more than any other industry, feel very to extremely (80%) confident in their organizations ability to detect and mitigate potential data breaches caused by insider threats.

Respondents in heavily regulated industries including finance, insurance, and real estate, noted that risk of non-compliance with privacy-regulations is the biggest challenge their organization faces when it comes to security.

← Back to contents

What's Next for Mainframe Security

In this age of rapid technological change, mainframe systems remain a cornerstone for businesses. With digital transformation projects well underway in nearly every enterprise, modernizing mainframe systems will enable them to better adapt to new security risks and data management needs. Organizations must consider hybrid cloud solutions that leverage the security and reliability of the mainframe, while also allowing users to store and manipulate data in the cloud. A resilient defense mechanism for mainframes is not a singular strategy, but instead, a holistic approach.

As data makes its way into a multitude of environments, sometimes leaving behind the safety of its on-premises home, data management and governance operations have become essential steps in the modernization process. The same security infrastructure that keeps data safe in the mainframe needs to be able to extend into those new environments. To better support a hybrid cloud approach to modernizing, businesses can adopt a variety of monitoring tools, improved data storage, and intelligent automation solutions that help IT teams keep track of their data, lighten workloads, and stay on top of regulatory guidelines.

Mainframes are around to stay – it's time to protect them.

Learn more

Methodology

Rocket Software partnered with independent research firm Researchscape to survey 250 U.S. IT directors and vice presidents in firms with more than 1,000 employees. The survey was conducted between August 18, 2023 and September 8, 2023, and focused on the opinions of IT professionals in seven countries (US & EMEA).

About Rocket Software

Rocket Software partners with the largest enterprises, in all industries, to solve their most complex IT challenges, across infrastructure, data, and applications — with solutions that simplify, not disrupt their modernization journey. Trusted by over 10,000 customers, Rocket Software helps enterprises modernize in place with a hybrid cloud strategy, so they don't need to re-platform or build from the ground up. The company's 2,600 global employees work with customers to accelerate and optimize their modernization journey while meeting evolving market needs. Rocket Software is a privately held U.S. corporation headquartered in the Boston area with centers of excellence strategically located throughout North America, Europe, Asia and Australia. Rocket Software is a portfolio company of Bain Capital Private Equity. Follow Rocket Software on LinkedIn and Twitter or visit RocketSoftware.com.

The future won't wait—modernize today.

Visit RocketSoftware.com ›

Rocket software

MAR-7498_TheState-of-MainframeSecuritySurvey2023_WP_V8