

Your Ultimate Guide to Mainframe Vulnerability Management: How to Protect Your Systems

By Rocket Software
13 min. read

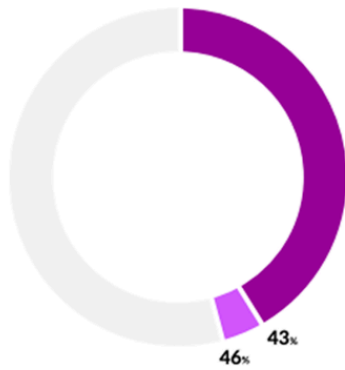
1. What is mainframe vulnerability management?

What is mainframe vulnerability management?

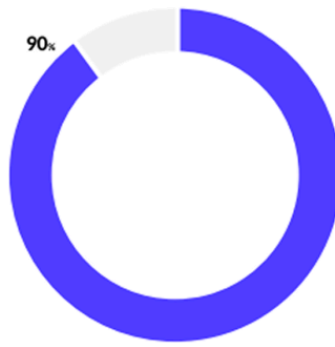
Mainframe vulnerability management is the process of locating, assessing, and addressing your threats on the mainframe to ensure the security and integrity of critical systems and data.

Why does your mainframe vulnerability management matter?

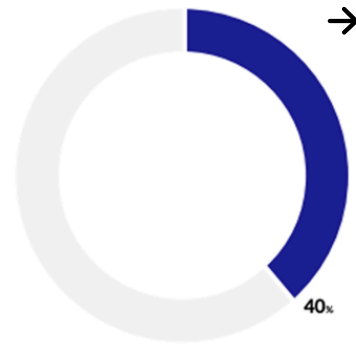
Cyberthreats are evolving at a hair-raising pace, making the security of your mainframe more important — and precarious — than ever. Mainframes are the unsung heroes of enterprise operations, powering critical applications and safeguarding sensitive information. But with great responsibility comes great risk. These systems are a prime target for cyberattacks. Did you know that 76% of organizations experienced a cybersecurity breach in the last year, with many attacks exploiting unpatched vulnerabilities?



46% of data breaches involved customer personally identifiable information (PII), 43% involved intellectual property (IP).



90% of credit card transactions take place on mainframes.



40% of security incidents involve application-level attacks in 2024.

Effective vulnerability management is no longer optional; it's essential. This means continuously monitoring for potential threats, assessing vulnerabilities and understanding their severity, and taking decisive action, through steps like patches, software updates, and tightening access controls.

Every proactive step is a shield against unauthorized access, data breaches, and costly operational disruptions. The mainframe powers your work — until an unmanaged vulnerability weakens it.

2. Regulatory compliance

How does mainframe vulnerability affect your regulatory compliance?

Vulnerability management is key to staying compliant by identifying and addressing security weaknesses. Many regulations require secure systems and data protection, including:

- **GDPR:** Mandates data protection and privacy for individuals in the EU.
- **HIPAA:** Requires safeguarding sensitive healthcare information.
- **PCI DSS:** Ensures secure handling of payment card data.

Effective vulnerability management helps reduce your data breach risks, apply regular patches, and show proactive security during audits. Neglecting it can lead to fines, legal issues, and reputational damage. The stakes couldn't be higher: non-compliance costs nearly three times more than compliance.

3. Rising threats

What are rising threats to today's mainframe?

New risks are surfacing as technology evolves, posing challenges that weren't significant in the past. Today's cybercriminals compromise your mainframe's data security with:

- **Sophisticated cybercriminals:** Attackers are deploying tactics with an intensifying ruthlessness, growing more skillful with malware, ransomware, and exploiting zero-day vulnerabilities, to target mainframe systems. These attacks are becoming more difficult to detect and mitigate, posing significant risks to critical infrastructure.
- **Insider threats:** Employees, contractors, or other insiders with legitimate access misuse their privileges intentionally or unintentionally, leading to internal security risks. These threats are particularly challenging as they stem from trusted individuals already within the system.
- **Integration with cloud and APIs:** As mainframes are increasingly integrated with cloud services and APIs to support modernization efforts, they experience greater exposure to external threats. This expanded attack surface requires robust security measures to prevent unauthorized access and breaches.
- **AI-driven threats:** Cybercriminals are leveraging artificial intelligence to develop more sophisticated and adaptive attacks. From automated vulnerability scans to highly targeted adaptive malware, AI is being weaponized to breach even the most secure environments.
- **Regulatory pressures:** The growing complexity of compliance requirements in industries like finance, healthcare, and government adds significant pressure to keep mainframes secure. Organizations must ensure their systems meet stringent regulations, while maintaining robust defenses against evolving threats.
- **Financial backing for cybercriminals:** The increasing financial support for cybercriminal organizations has exacerbated the threat landscape. Well-funded attackers can invest in advanced technologies, hire skilled professionals, and develop sophisticated tools to exploit

vulnerabilities in critical mainframe systems. This influx of resources enables persistent and targeted attacks, raising the challenge for organizations to defend their infrastructure effectively.

Staying ahead of these evolving challenges is critical to maintaining the security and stability of mainframe operations.



'Ghost employees' may pop up on company payrolls, created by internal fraudsters who have the access and ability to falsify payroll and other records, generating paychecks that they then cash.

[Read full study](#) →

How does a vulnerability management program address threats to the mainframe?

To address mainframe threats, implement a structured, continuous process to identify, assess, prioritize, and mitigate vulnerabilities within the mainframe environment. Here's how:

- **Asset discovery and inventory:** Your first step is to maintain an up-to-date inventory of all mainframe systems, applications, and connected components. This ensures that any vulnerabilities are identified in the correct context and no system is overlooked.
- **Vulnerability identification:** Using automated scanning tools tailored for mainframes or manual assessments, the program identifies security vulnerabilities, including outdated software versions, misconfigurations, and unpatched operating system components.

Emerging threats like zero-day vulnerabilities or new exploit techniques are flagged through real-time threat intelligence feeds integrated into the program.

- **Risk assessment:** This step evaluates the severity and potential impact of detected vulnerabilities. This involves analyzing the likelihood of exploitation and the potential consequences on critical business operations, data integrity, and compliance requirements. Mainframes often host mission-critical data, so prioritizing risks is crucial.
- **Patch management:** Mainframes require careful handling of updates due to their importance and complexity. The program applies patches and software updates provided by vendors to mitigate known vulnerabilities, but only after thorough testing in a controlled environment to avoid disrupting system stability.
- **Configuration management:** Misconfigurations are a common attack vector. Your regular audits of mainframe configurations ensure they align with security best practices and compliance standards, such as limiting administrative privileges, enforcing encryption, and securing network interfaces.
- **Monitoring and threat intelligence:** Continuous monitoring is essential to detect new threats as they emerge. Integrating real-time threat intelligence allows the program to adapt quickly to evolving attack techniques, such as ransomware, advanced persistent threats (APTs), or insider threats targeting mainframes.
- **Incident response:** If a threat is detected, the program includes a well-defined incident response plan. This ensures rapid containment, investigation, and remediation of vulnerabilities to minimize damage or disruption.
- **Compliance management:** Mainframes often operate in industries with strict regulatory requirements like banking and healthcare. The program ensures that security measures align with frameworks like GDPR, HIPAA, or PCI-DSS, reducing legal and financial risks from non-compliance.
- **Employee training and awareness:** Human error is often a factor in security breaches. A robust program also educates administrators, developers, and users about secure practices to reduce the likelihood of introducing vulnerabilities.

By combining automated tools, threat intelligence, and best practices, a vulnerability management program enables organizations to proactively address emerging threats, protect sensitive mainframe environments, and maintain operational resilience

4. Critical needs

Why are mainframes critical to include in your vulnerability management program?

The mainframe no longer means guaranteed security — and hackers will exploit this. (You should treat your mainframe with the same level of security as any other system.)

\$4.9M

the average cost of a data breach in 2024

67%

of organizations to overlook rigorous security measures

Source: IBM and Ponemon Institute, 2024

Mainframes are often seen as impenetrable, leading 67% of organizations to overlook rigorous security measures, according to a report by Key Resources Inc. Cybercriminals capitalize on this misconception, targeting mainframes because they store 70% of the world's data and run 90% of global credit card transactions. Failure to include mainframes in a comprehensive vulnerability management program exposes your organizations to significant risks. With IBM reporting that the average data breach costs \$4.45 million in 2023, prioritizing mainframe security as part of your strategy is more critical than ever. As technology evolves, so do your vulnerabilities.

Your vulnerability management program must be too dynamic for surprises.

5. Best practices

What are some tips and best practices for mainframe vulnerability management?

The challenge of organizing mainframe security best practices arises from the mainframe's undeniable importance. An enterprise's valuable tool is a cybercriminal's valuable target. This is why vulnerability management is imperative.

And this is why vulnerability management involves more than just uploading some risk management software. Strategic vulnerability management is the building block you need for success with your risk management tools. Otherwise, you leave your organization open to the hazards of relying on a narrow: security infrastructure: When the only tool you have is a hammer, every challenge must be treated like a nail.

Tips and best practices for effective vulnerability management:

- **Know your vulnerability types:** Understand the various types of vulnerabilities that could impact your organization. These include software flaws, misconfigurations, outdated systems, and human errors. Knowing these helps you prioritize and address them effectively.
- **Understand regulatory requirements:** Familiarize yourself with the stringent vulnerability management requirements outlined in industry regulations and standards like GDPR, HIPAA, PCI DSS, or ISO 27,001. Compliance ensures both legal adherence and enhanced security.
- **Hire a security architect:** Skilled security architects are vital for robust security strategies. They navigate legal, regulatory, and operational requirements, assess cybersecurity risks, and design effective security solutions. While architects select the right tools for your organization, they are not responsible for daily operation.
- **Establish code-level policies and scanning:** Implement clear, code-based policies for vulnerability scanning. Use these policies to ensure every line of code is reviewed for potential risks. Additionally, install a vulnerability scanner for proactive and continuous monitoring of your systems.

- **Produce real-time compliance checks:** Ensure your compliance policies are enforced through real-time compliance checks. Use tools that automatically monitor your systems and flag any deviations from your established policies.
- **Conduct annual penetration tests:** Perform annual penetration tests on all critical environments, including your mainframe systems. This helps identify hidden vulnerabilities and validates the effectiveness of your security measures.
- **Implement multi-factor authentication (MFA):** Fully implement MFA across all systems and applications. This adds an additional layer of protection against unauthorized access, significantly reducing the risk of breaches.
- **Review your budget periodically:** Regularly assess your cybersecurity budget to ensure it aligns with your organization's digital operational resilience needs. This allows you to allocate resources effectively and address emerging threats without compromising security measures.

By following these best practices, you can build a comprehensive vulnerability management strategy that protects operations, ensures compliance, and strengthens resilience against evolving cybersecurity threats.



We never even thought we could have vulnerabilities on the mainframe, but once we began automated scanning, we found the volume and the severity to be much greater than anticipated.

Chief Information Security Officer

Major Global Bank

6. Mainframe integrity

What's the difference between mainframe integrity and mainframe security?

Another reason your organization needs vulnerability management for mainframe security is to preserve your mainframe's integrity:

Mainframe integrity is about:

- Making decisions based on the established accuracy and consistency of your data
- Having complete confidence in the logical correctness of your mainframe
- Trusting the system to perform as expected

Mainframe integrity is about:

- Making decisions based on the established accuracy and consistency of your data
- Having complete confidence in the logical correctness of your mainframe
- Trusting the system to perform as expected

Together, integrity and security form the backbone of a resilient and trusted mainframe ecosystem.

The importance of vulnerability management is that, without it, you can only start with mainframe integrity — but you won't have the security to keep it. Integrating vulnerability management protects both sides of your mainframe and the entirety of your organization with the following results:

- Aligned security initiatives with business goals
- Ensured smooth operations
- Strengthened stakeholder confidence

02:41

Strategic vulnerability management also means answering the question of open-source software, a powerful addition to your mainframe which can also present numerous and far-reaching vulnerabilities to your mainframe. The many points of exposure through open source can be assisted by an internal team member falling prey to phishing or an external team member uploading ransomware. Other threats include:

- **Outdated libraries with security flaws:** These can leave your system vulnerable to known exploits if not updated regularly.
- **Unvetted code from unknown contributors:** Using such code increases the risk of introducing bugs or malicious elements into your software.
- **Intentional insertion of backdoors or other exploitable features:** These can provide attackers with unauthorized access to compromise your system.

Vulnerability management is critical to your mainframe's success because open source isn't a threat to your operations; unmanaged open source is.

7. Penetration testing

Why is penetration testing crucial to your vulnerability management strategy? How is it different from vulnerability management scanning?

Penetration testing is a crucial part of any strong vulnerability management program. Here's why it matters:

- **Goes beyond scanning:** Unlike vulnerability scanning, penetration testing shows exactly how attackers could exploit your system. It provides detailed reports and actionable steps to fix vulnerabilities before bad actors use them.
- **Reduces security risks:** 71% of organizations that conduct regular penetration testing report significant reductions in security risks.
- **Proactive Approach:** Conducting mainframe penetration testing at least once a year helps uncover weaknesses and strengthens your defenses.

Compliance standards require both vulnerability scanning and penetration testing:

- **Vulnerability scanning** identifies weaknesses and their types.
- **Penetration testing** demonstrates how those weaknesses could be exploited.

Studies show that 43% of cyberattacks exploit vulnerabilities that proactive testing could have identified. Together, these practices are essential for a comprehensive approach to mainframe security.

8. Vulnerability types

What's the difference between code-based and configuration-based vulnerabilities, and how do you identify them?

When considering mainframe vulnerabilities through the broad lens of “configuration-based versus code-based” vulnerabilities, configuration-based vulnerabilities often receive the bulk of ¹ attention and resources. This is partially due to the underestimated consequences and

overlooked prevalence of code-based vulnerabilities. However, ignoring code-based vulnerabilities is as costly as ignoring their configuration-based counterparts.

Configuration-based vulnerabilities from the faulty setup (or management) of systems:

- Weak or absent passwords
- Misconfigured firewalls
- Overly permissive directory access

Options for configuration-based fixes:

- The skill set of an experienced administrator
- Redundant safeguards implemented during an update or a system's initial setup
- Changing a program's settings

The consequences of code-based vulnerabilities include:

- An impact that can be more widespread than the localized configuration-based infractions
- Specialized developers needed to close the vulnerability, siphoning organization resources
- Advanced vulnerability scanning technology to identify vulnerabilities effectively

Actionable insight: Regularly assess your mainframe environment for these vulnerabilities.

Addressing configuration issues and keeping code up to date lowers your risk of an attack and raises your mainframe security to zero trust levels.

Why are no two mainframe vulnerability regulators alike?

A common requisite among regulators for the mainframe, like DORA, 23 NYCRR Part 500, PCI DSS, and NY State, is to minimize risk through continuous assessment. But the differences between just these three regulators highlight the complexity of mainframe compliance:

- DORA prioritizes a broad scope that includes operational resilience and third-party oversight.
- [Twenty-three NYCRR Part 500](#) emphasizes cybersecurity governance, which is overseen by a CISO (Chief Information Security Officer).
- PCI DSS 4.0 focuses on payment card data security over both resilience and governance.
- NY State requirements include robust data privacy measures and protection against unauthorized access to sensitive information.

These four regulators are part of a larger and even more diverse community. Mainframe vulnerability management is how you keep up with the variety of your regulators, while surpassing your industry competition that can't.

9. Mainframe vulnerability management checklist

Before you build your program, make sure you're checking these boxes:

Step 1: Implement code and configuration vulnerability management

A key aspect of mainframe security is maintaining code and configuration integrity. Code-based vulnerability management analyzes application code for flaws, while configuration-based management ensures system settings follow security best practices. Without these measures, a single bad line of code or misconfiguration can lead to costly breaches. Regular reviews and automated tools can help identify and fix these risks.

Step 2: Conduct frequent mainframe penetration tests

Vulnerability scanning identifies weaknesses by comparing z/OS® standards to security policies. However, regulations often require penetration testing multiple times a year for a deeper assessment. Penetration tests simulate real-world attacks to uncover vulnerabilities and how they might be exploited. These insights are vital for building strong defenses and staying ahead of evolving threats.

Step 3: Secure and update open-source software

Many organizations use open-source software on mainframes, but outdated or unsupported versions can create risks. Remove unauthorized software, support approved tools, and keep them updated. Apply fixes for known CVEs (Common Vulnerabilities and Exposures) and patch security gaps to maintain system integrity and regulatory compliance.

Step 4: Regularly update passwords

Passwords are often the last line of defense, but outdated ones increase the risk of security failures through phishing, malware, or brute-force attacks. Enforce policies for regular password updates, require strong password complexity, and educate users on best practices to reduce risks tied to weak credentials.

Step 5: Hire a security architect

A security architect oversees and integrates security protocols across your mainframe environment, including infrastructure, applications, and user access. This role ensures a proactive, strategic approach to mitigating risks and strengthening your organization's defenses.

Step 6: Implement multifactor authentication (MFA)

MFA adds an extra security layer beyond passwords. By requiring multiple authentication methods — like a password paired with a one-time code sent to a trusted device — MFA reduces the chances of unauthorized access. Fully deploy MFA across systems, especially those handling sensitive data or administrative access.

Step 7: Conduct regular user access reviews

Over time, users may gain excessive access rights, increasing vulnerabilities. Regularly audit access to ensure that employees, contractors, and third parties only have permissions necessary for their roles. Apply the principle of least privilege (PoLP) to limit exposure and minimize breach risks.

By following these streamlined steps, your organization can build a strong vulnerability management program and effectively protect your mainframe systems.

10. How to start a mainframe vulnerability management program

Effective vulnerability management is no longer optional; it's essential. This means continuously monitoring for potential threats, assessing vulnerabilities and understanding their severity, and taking decisive action, through steps like patches, software updates, and

tightening access controls.

Every proactive step is a shield against unauthorized access, data breaches, and costly operational disruptions. The mainframe powers your work — until an unmanaged vulnerability weakens it.



Share

Table of contents

- [1. Introduction](#)
- [2. Mainframe Vulnerability Management](#)
- [3. Regulatory Compliance](#)
- [4. Critical Needs](#)
- [5. Best Practices](#)

[6. Mainframe Integrity](#)

[7. Penetration Testing](#)

[8. Vulnerability Types](#)

[9. Checklist](#)

[10. Get started](#)

More solutions for Mainframe Vulnerability Management

Your future success with mainframe vulnerability management depends on your assortment of those potential solutions, from mainframe audit tools to a data recovery manager. Risk management software, AI-based tools, and mainframe security services can all be aligned to produce a strong defense against bad actors and routine compliance with standards set by regulators.

Rocket® z/Assure® Vulnerability Analysis Program

Fortify defenses without the oversights but with scans for code-based vulnerabilities boasting an industry-best 99% rate of accuracy



Rocket® Mainframe Security Services

Enhance Your Mainframe Security with Vulnerability Assessments, Penetration Testing, and Compliance Support



Rocket® Data Recovery for Dell GDP

Ensure your critical mainframe data assets are protected and recoverable



Resources

How to Start a Mainframe Vulnerability Management Program

[Read whitepaper](#)

Bringing Vulnerability Scanning into Penetration Testing

[Read the case study](#)

From Green Screen to Red Alert: Fortifying Your Mainframe Security

[Read whitepaper](#)

Related insights

What to Expect in Cybersecurity in 2025

The cybersecurity landscape is evolving rapidly, driven by new technologies and increasingly sophisticated threats, forcing organizations to reassess their security strategies.



Three Key Strategies to Enhance Mainframe Security and Resilience

Building a secure and resilient infrastructure is not just a best practice – it's a necessity.



The DORA Deadline Is Here: Is Your Mainframe Ready?

What you need to know to meet DORA's requirements seamlessly when it comes to the mainframe, in addition to a helpful mainframe compliance checklist.



Talk to an expert

[About us](#)

[Resources](#)

[Products A-Z](#)

[Insights Hub](#)

[Product documentation](#)

[Partner portal](#)

[Community](#)

[Careers portal](#)

[Contact us](#)

Support portal

English

Trust center

Accessibility

Terms of use

Trademarks

Unsubscribe



77 4th Avenue
Waltham, MA 02451 USA

Privacy Notice

Cookie notice

Security practices

Manage your email preferences

©2025 Rocket Software, Inc. Rocket® is a registered trademark of Rocket Software, Inc. All other trademarks mentioned herein are the property of their respective owners.

"Micro Focus®" is a trademark of OpenText; Rocket Software is not affiliated with OpenText.