Rocket® software

Think Your Mainframe Is Secure? Think Again.

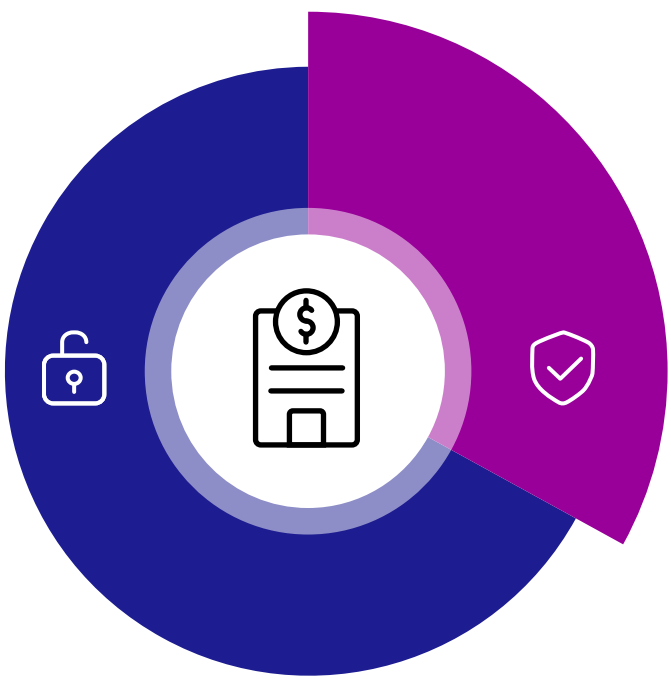
91% of all cyber attacks begin with phishing[1]

The mainframe is the most enduring IT system, well-regarded for its processing speed and high degree of security. But just because the mainframe is secure, doesn't mean it's impenetrable. The myth of the mainframe as a secure powerhouse has meant that the system is often overlooked or ignored in corporate IT security strategy.

Only 33% of organizations always or often factor security into their mainframe decisions[2].

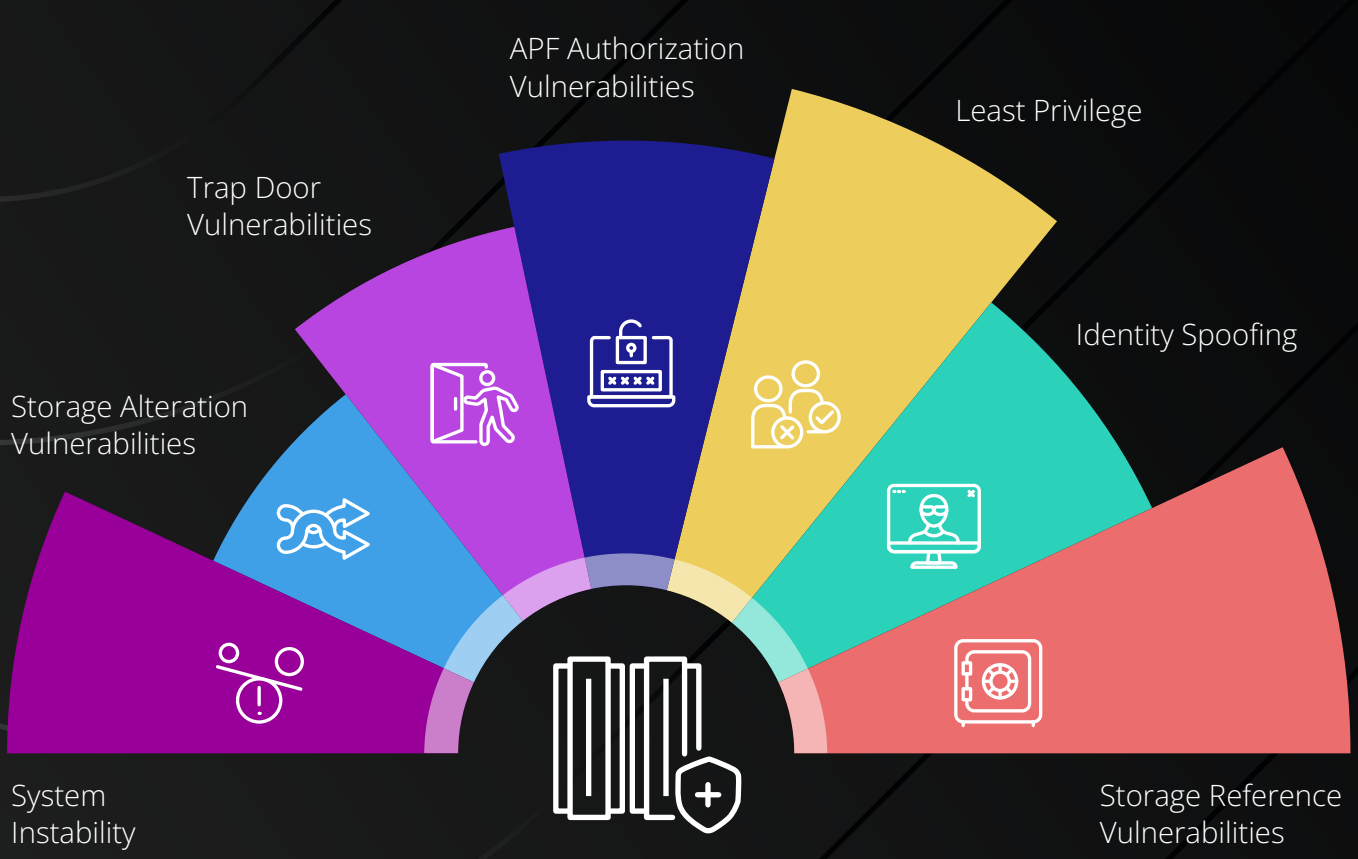
That leaves it exposed to security threats that could bring an organization to its knees.

Forfeiture of revenue, remediation expenditures, diminished market share, business disruption, and legal and regulatory repercussions are some of the many consequences you can face in the event of a threat.



Mainframe Vulnerability Management

A critical piece of your mainframe security strategy is mainframe vulnerability management. Application and network scanning alone isn't enough – you must scan for Integrity Vulnerabilities in operating system (OS) layer code and continuously assess security configurations – and it's necessary to be aware of the mainframe vulnerability categories that could severely impact the security of your mainframe.



Trap Doors, Storage Alteration, and System Instability vulnerabilities are several of the many you need to be aware of that can impact the integrity of your mainframe.

As a Security leader, it's important to have a strong mainframe vulnerability management program in place.

As a suggested first step, we recommend you:

Leverage a Security Architect for the mainframe that understands the organization's mission, objectives, stakeholders, and activities, and understands the policies, procedures, and processes required to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements.

Include the mainframe in your Vulnerability Management Program. Install a vulnerability scanner, like Rocket® z/Assure® Vulnerability Analysis Program, for proactive monitoring, and scan all software before going to production. This enables you to identify vulnerabilities, perform forensics analysis, prioritize risks, and report the location of the exploitable code for ease of remediation.

z/Assure® Vulnerability Analysis Program scans the operating system layer in real-time to look for integrity-based code vulnerabilities, using proprietary algorithms and advanced intelligence to detect threats. It conducts runtime analysis of operating system level code, memory, and data flows to identify vulnerabilities, perform forensics analysis, prioritize risks, and then reports the location of the exploitable code for ease of remediation.

Learn more about z/Assure® Vulnerability Analysis Program

1. 91% of all cyber attacks begin with a phishing email to an unexpected victim. Deloitte Malaysia, Risk Advisory, Press releases.
2. Research Reveals Pervasive Complacency Around Mainframe Security. KRI Security thought paper.

Rocket® software

MAR-8019_Mainframe-Security-VAP_Infographic_V10