Rocket® software

From Green Screen to Red Alert: Fortifying Your Mainframe Security

How to arm green screens against rogue AI, fake IT workers, and expensive auditory fines

Contents

Introduction

IT teams have long relied on the idea that the mainframe is more "securable" than, for example, a Linux box and have considered that to be "good enough."

No more.

Data breach challenges and costs are rising. Threats are becoming more expansive and bolder, cyber-attackers better armed, and AI increasingly complicit. It's no wonder that only 28% of IT leaders surveyed felt extremely confident in their proactive response to mainframe vulnerabilities.[1]

In this whitepaper, you'll read how to reduce growing mainframe risk and protect operations without a major overhaul of your mainframe security.

You'll discover:

- Three significant risks threatening your mainframe today.
- A five-point, best-practices strategy to fix these risks.
- Technologies and techniques that can help.

There are simple things you can do today to sleep better at night. **Start right now.**

← Back to contents

Why mainframes are (increasingly) a risky business

In our sophisticated, hyper-connected world, mainframes are sitting ducks.

Users often connect directly to mainframe applications using terminal emulators. The login authentication is usually an eight-character, case-insensitive password. (Yes, you read that right.) This routine has worked well historically, but today, it's no longer a match for protecting the crown jewel — your critical mainframe data.

And the job's an intense, high-stakes one:

- Data breach costs increased 10% from last year — the largest jump since the pandemic — reaching a global average cost of US$4.88 million per breach in 2024.[2] Nearly half of the breaches (46%) involved customer personally identifiable information (PII), and 43% involved intellectual property (IP) records, both increasing targets of legislation and fines.[3]

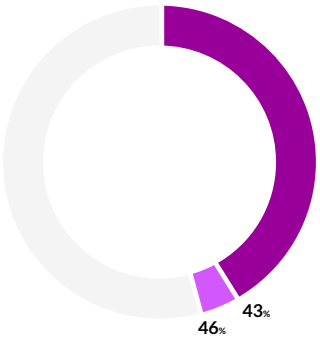
- An estimated 90% of credit card transactions take place on mainframes. The amount of PII stored on mainframes is substantial (if not exactly quantifiable), including Social Security numbers, dates of birth, addresses, phone numbers, and credit card numbers. Financial services, government, utilities, and not-for-profit organizations tend to have the most PII.

- Cyberattacks using stolen or compromised credentials increased 71% year-over-year in 2024.[4] Forty percent (40%) of security incidents involve application-level attacks in 2024.[5] Meanwhile, finding passwords and authenticated browser session tokens is increasingly easy on the Dark Web.[6]

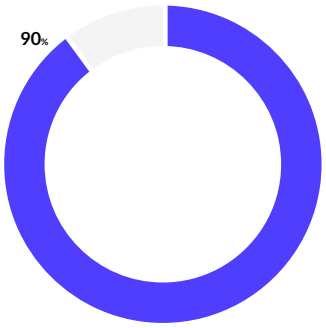
- Compared to other vectors in 2024, malicious insider attacks resulted in the highest costs, averaging US$4.99 million, according to IBM®'s 2024 Cost of a Data Breach report. Other expensive attack vectors included business email compromise, phishing, social engineering, and stolen or compromised credentials. GenAI may be playing a role in creating some of these phishing attacks.[7]

New technologies, such as ubiquitous AI, are lowering the bar for hackers and thieves. They can mutate identities, enable password cracking in seconds, and even identify passwords by the sound of keys being pressed.

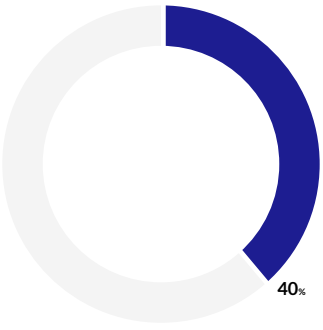
Organizations need new best practices to keep the bad guys out, your data and operations intact, and your mainframe running smoothly.



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



90% of of credit card transactions take place on mainframes.



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

← Back to contents

Three significant risks threatening your mainframe

Mainframe access presents an enticing target — for everyone from determined hackers and disgruntled employees to competitors and state-funded actors intent on disruption. Today, credential stuffing, password spraying, phishing, and other easily accessible tools are available.

Meanwhile, new data-security regulations involving access are proliferating, with real penalties for non-compliance.

All of this comes at an excessive cost to CISOs wrangling complex IT environments, including mainframes.

Here are three risky areas to watch for:

01 Insider threats and fake workers.

02 AI, ChatGPT, CoPilot, and beyond.

03 Compliance creep.

← Back to contents

Insider threats and fake workers

"It's coming from inside the house!" may sound like the stuff of bad horror films, but insider threats are very real and getting more rife and more sophisticated. Here's the usual scenario: Unintentional errors by authorized employees or contractors who accidentally compromise security. Then, there are disgruntled employees who turn on the harm. A single bad hire, depending on their position within the organization, can often run rampant for personal gain or payment. (Even lateral moves can be devastating.)

Lost, shared, stolen, or outdated credentials are often involved, and it happens more often than you may think.

And it gets worse.

"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.

At the extreme (but not far-fetched) end of the spectrum are elaborate, targeted schemes like the Korean "laptop farm" scandal. Armed with thousands of stolen credentials, organized perpetrators allegedly placed more than 300 overseas information technology (IT) workers — posing as U.S. citizens and residents — in remote positions at U.S. companies to benefit North Korea (DPRK).[8]

The perpetrators allegedly defrauded the companies using U.S. payment platforms, online job site accounts, proxy computers in the United States, and witting and unwitting U.S. persons and entities. A U.S. government advisory noted that workers also used privileged access obtained through their employment to enable malicious cyber intrusions, an observation corroborated by cybersecurity expert Mandiant and other organizations.

In the State of Massachusetts, a convincing fake payroll website tricked some state employees, stealing their personal or financial data. The likely culprit was an active "credential harvesting campaign" involving the state's employee-self-service time and attendance system.[9] Phishing at its phinest.

Even sophisticated technology companies aren't immune. Russian state actors hacked Microsoft using password-spraying, which leverages weak passwords and other weaknesses, eventually penetrating some company email accounts.[10]

The bottom line is that insider threats are increasing, becoming ever easier to create, and benefiting a broad spectrum of actors.

"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.

← Back to contents

AI, ChatGPT, CoPilot, and beyond

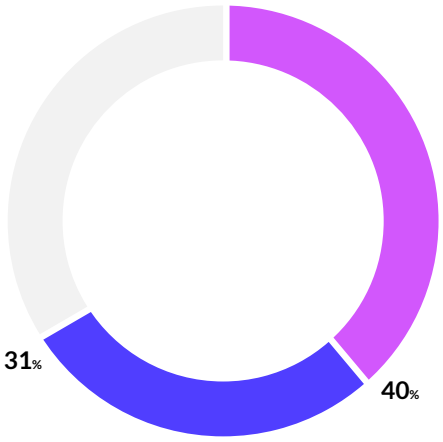
AI is rewiring business: everything from how we design, develop, build, sell, and service products to how we interact with customers, prospects, employees, vendors, and partners. Businesses are racing to adopt AI (GenAI and otherwise) throughout operations, including software development.

AI is finding its way into technology-driven attacks as well as social engineering tactics. Social engineering uses people's humanity to get them to give up confidential information or personal data (including credentials), pay or deposit money, or otherwise be victimized. Verizon Business documented over 3,600 social engineering incidents in 2023, with 3,032 confirmed data disclosures.[11] Leading the way with more than 40% of social engineering attacks was pretexting, followed by phishing (31%), extortion, and baiting.[12]

In pretexting, social engineers create a pretext (scenario) that lures a victim into a vulnerable situation and tricks them into giving up private information. (In reverse social engineering, the attacker tricks the victim into contacting the attacker first.)

Increasingly accessible, AI is lowering humans' resistance to identity fraud. It's getting ever easier to spoof humans, from constructive Help Desk bots to Tik-Tok "influencers" or LinkedIn profiles with large followings who seem to appear overnight. Identity theft or appropriation by AI can result in new insider threats, scams, financial fraud, social and political re-engineering, and worse — resulting in financial and reputation losses.

Of course, smart businesses and organizations continually update their security to keep ahead of data infiltration and exfiltration. But previously sheltered mainframe owners need to be vigilant about AI-enabled human shapeshifting by perpetrators.



40% of social engineering attacks was pretexting, followed by 31% phishing, extortion, and baiting.

← Back to contents

Compliance creep

Even if you think you've covered all your bases, the current regulatory climate will likely give you a run for your money. The typical financial organization must, on average, deal with 223 regulatory developments every day, according to Thomson Reuters.[13]

Data and IT security regulations are steadily advancing, with mandated deadlines and penalties for noncompliance, including mainframes.

Currently, mainframes are subject to regulations such as the Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA) — all of which now or very soon will require more stringent protection of personal information, like multi-factor authentication (MFA). As does the Digital Operational Resilience Act (DORA), which takes effect Jan. 17, 2025. DORA mandates data encryption for financial institutions that do business in the European Union.

States are getting into the act. The State of New York's cybersecurity regulation, known as 23 NYCRR Part 500, is designed to protect customer data and the IT systems of financial institutions operating in New York, including state-chartered, private, and international banks, mortgage brokers, and insurance companies.[14] It requires MFA, and non-compliance can result in civil money penalties for violations.[15]

The US Government has a spectrum of compliance regulations. As part of its Cybersecurity National Action Plan, it mandates MFA for all federal government websites. Similarly, the IRS requires MFA key protection for tax professionals to safeguard sensitive data.

These are just a few examples of regulations that affect the mainframe, with increasing emphasis on user authentication requirements.

← Back to contents

Five new best practices, ready to go

While challenges continue to grow, here are five simple actions you can take to help protect your organization going forward.

01

When you hear “green screen,” start thinking of “security”

This should be automatic. Green-screen applications provide critical data to users, including PII and other sensitive data. We need to be as overprotective of green-screen applications as we are of other parts of IT.

Make sure you’re either offering an inherently secure, web-based terminal emulator or making users hop on a VPN to access it. Also, ensure your terminal emulator supports standard security capabilities such as TLS 1.3 and MFA.

If you haven’t already, join and participate in IT-ISAC, the Information Technology-Information Sharing and Analysis Center, at the national and topical level. It will help you stay on top of threats and learn from colleagues.

02

Integrate your green screen login authentication into your current IAM solution

IAM is a framework of policies, technologies, and processes that ensures controlled access to company resources and data. It’s a crucial component of modern cybersecurity, enabling secure access to sensitive data, systems,

and applications. IAM includes identity management, access management, authentication, authorization, provisioning/de-provisioning, governance/compliance, and monitoring/reporting. IAM improves security, helps ensure regulatory compliance, provides operational efficiency, and improves user convenience.

A standard part of IAM systems, multi-factor authentication (MFA) is a security method that requires users to provide more than just a password to access an account. Users must provide two or more forms of authentication: typically, (1) something you know (like a password or PIN) or (2) something you have (e.g., a token). The third factor is often something you are, for example, a fingerprint, iris scan, or other biometric. Typically, MFA prompts users for the second factor when they sign in to an account on a device or app.

MFA can help prevent unauthorized access to accounts if a password is compromised. It can also protect against online criminals who use weak or stolen passwords to try to gain access to data.

By leveraging IAM in the enterprise, you add one more layer of defense between the world and your mainframe connection.

03

Watch for behavior that moves off baseline

Use automated monitoring and behavior analysis to continually identify behavior changes. For example, a worker in India suddenly logs in from a new location in the middle of the night. Extend your monitoring to encompass all direct-connected mainframe users. Preconfigure access guardrails and keep them current.

Your corporate Identity and Access Management system can usually help with this by empowering you to set up granular rules for blocking or enabling behavior based on credentials. Moreover, if you leverage IAM for mainframe access, you can block bad actors before they ever connect to your mainframe.

← Back to contents

04

Always create an audit trail

To identify and prevent future malicious behavior patterns, you need to know who connected when, where, why, how, and what they did. Good IAM systems have metering capabilities that can be used for this purpose. Run-time process discovery tools that run in the background of mainframe operations can also track user navigation at a fine-grained level in real time using heat maps and other technology.

Why not let your IAM do the work of logging green screen user activity and aggregating it into the reporting it already does across your organization?

05

Look for vendors that already have robust SDLs.

Collaborate with vendors who can demonstrate robust and documented secure development cycles (SDLs). You want to know: *During development and when doing updates, what doors did they open? What doors did they close? How do we know?*

Software vendors must be secure partners in businesses' supply chains. This includes monitoring new security regulations in their areas and their customers' (you) effects.

In its 2024 Cost of a Data Breach report, IBM® found that using security AI and automation extensively in prevention is paying off, saving those organizations who do so an average of US $2.22 million in annual cost savings.[16]

← Back to contents

New risks. New rules. New rewards.

Mainframes no longer have the luxury of staying under the radar of hackers, thieves, or criminals.

We live in an open, rapidly evolving online world where identities are increasingly easy to spoof, steal, and sell. Passwords alone are not enough to protect and access information. Organizations' threat profiles continue to get worse, and hackers — human and AI — are ever more inventive.

Securing green screen access is a vital but often overlooked part of modernization strategies.

You can close this security gap and reduce growing risks by taking advantage of readily available technologies and some of the best practices above.

The tools and techniques are at hand, and it's easier than you may think.
Get started today.

[1]The State of Mainframe Security, 2023 Survey Report by Rocket Software

[2]Cost of a Data Breach Report 2024, IBM

[3]Cost of a Data Breach Report 2024, IBM

[4]IBM X-Force Threat Intelligence Index 2024

[5]Gartner

[6]"Stolen passwords are a goldmine now," Axios, March 5, 2024

[7]Cost of a Data Breach Report 2024, IBM

[8]"Charges and Seizures Brought in Fraud Scheme, Aimed at Denying Revenue for Workers Associated with North Korea," Office of Public Affairs/U.S. Department of Justice, May 16, 2024

[9]"State employees fooled by fake payroll website farming their data," Boston.com, October 10, 2024

[10]"Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard," Microsoft, March 8, 2024

[11]Verizon Business 2024 Data Breach Investigation Report

[12]Verizon Business 2024 Data Breach Investigation Report

[13]"Establishing Resiliency through a Modern Regulatory Change Management Strategy," IDC blog, March 22, 2021. https://blogs.idc.com/2021/03/22/establishing-resiliency-through-a-modern-regulatory-change-management-strategy/

[14]New York Department of Financial Services, https://www.dfs.ny.gov/system/files/documents/2023/03/23NYCRR500_0.pdf

[15]"DFS Announces $1 Million Cybersecurity Settlement With First American Title Insurance Company" https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202311281

[16]Cost of a Data Breach 2024, IBM https://www.ibm.com/reports/data-breach

← Back to contents

Rocket® Secure Host Access

With Rocket® Secure Host Access, you can provide secure, phishing-resistant, password-less access to critical host applications. Leverage your existing enterprise IAM and integrate host application access into your larger IT security strategy with little effort.

Secure Host Access lets you:

- Extend security best practices like SSO, SSH, and MFA.
- Redact sensitive data based on the end user's role in the organization.
- Mitigate the threat of cyberattacks and auditory fines.

Rocket is the only terminal emulation partner committed to a security-first approach to mainframe application access, helping you secure your green screen login with the strategy and tools already at your disposal.

About Rocket Software

Rocket Software is the global technology leader in modernization and partner of choice that empowers the world's leading businesses on their modernization journeys, spanning core systems to the cloud. Trusted by over 12,500 customers and 750 partners, and with more than 3,000 global employees, Rocket Software enables customers to maximize their data, applications, and infrastructure to deliver critical services that power our modern world. Rocket Software is a privately held U.S. corporation headquartered in the Boston area with centers of excellence strategically located around the world. Rocket Software is a portfolio company of Bain Capital Private Equity. Follow Rocket Software on LinkedIn and X.

Speak to an expert

Modernization.
Without Disruption.™

Rocket® software

Visit RocketSoftware.com ›

MAR-12201_WP_SecureHostAccess_V4