Securing Mainframe Access in an Era of Advanced Threats and Evolving Regulations

Barbara Ballard

Principal Product Manager

Rocket® software

Agenda

1. Introduction: Laying the Groundwork
2. Emerging Threat Landscape
3. Identity and Access Management (IAM) vs. Mainframe Security
4. Regulatory Drivers Impacting Mainframe Security
5. Practical Security Approaches
6. Best Practices and Recommendations
7. Q&A and Discussion

Introduction: Laying the Groundwork

As organizational leaders strive to meet regulatory requirements, there is a noticeable **gap** that has proven to create non-compliance and **incidents** that are creating significant **costs**

Not extending risk management initiatives to host systems.

IBM zSystems

90%

All credit card transactions run on MF

3

Trillion

In daily commerce

92 of 100

Top banks use mainframe

IBM i

Over 30,000

Organizations using IBM i

115 Countries

99.9999% Availability

COBOL-Based Applications

800

Billion

Lines of active COBOL code

The State of Security and Compliance

Verizon Data Breach Investigations Report

80%

of cyber incidents involve use of stolen or compromised credentials

IBM Cost of a Data Breach Report 2025

Average cost of a breach related to compromised credentials

$4.67M

IBM Cost of a Data Breach Report 2025

$4.44M

Global average data breach cost ($10.22M average data breach cost in the US)

IBM Cost of a Data Breach Report 2025

53%

of attacks target PII

IBM Cost of a Data Breach Report 2025

276

Days it took to identify & contain data breach across environments

Rocket software

Why Securing Access is Mission-Critical

One criminal, 50 hacked organizations, and all because MFA wasn't turned on

Crim used infostealer to get cloud credentials

Jessica Lyons — Tue 6 Jan 2026 // 07:01 UTC

If you don't say "yes way" to MFA, the consequences can be disastrous. Sensitive data belonging to about 50 global enterprises is listed for sale – and, in some cases, has already been sold – on the dark web following a major infostealer campaign, with apparent victims including American utility engineering firm Pickett and Associates; Japan's homebuilding giant Sekisui House; and Spain's largest airline Iberia.

The thief, who goes by the moniker Zestix or Sentap, steals data from corporate file-sharing portals by using compromised cloud credentials obtained from information-stealing malware. And none of the purported victims enforced multi-factor authentication (MFA), according to Hudson Rock, an Israeli cybersecurity company that specializes in infostealers.

SC Media — A CRA Resource

CISO STORIES | TOPICS | TOPIC HUBS | EVENTS | PODCASTS | RESEARCH | SC AWARDS

Vulnerability Management, Patch/Configuration Management, Malware, Ransomware, Threat Intelligence, Exposure management

State-sponsored attacks now make up 53% of vulnerability exploits

August 29, 2025 — Share

By Laura French

Emerging Threat Landscape

Insider Threats

Malicious insiders

Individuals who deliberately steal data, sabotage systems, or leak sensitive information.

Negligent insiders

People who accidentally cause damage through careless actions, like falling for phishing scams or mishandling data.

Compromised insiders

Those whose credentials are stolen or who are manipulated by external attackers.

Spoofed Digital Identity

Email spoofing

Sending emails that appear to come from a trusted sender, often used in phishing attacks.

IP address spoofing

Faking the source IP address in network communications to hide the origin or impersonate another device.

Website spoofing

Creating fake websites that mimic legitimate ones to trick users into providing sensitive information.

Stolen or Compromised Credentials

Stolen or Compromised Credentials

Okta, with a bruised reputation, rethinks security from the top down

CSO David Bradbury detailed to Cybersecurity Dive what the identity and access management company got wrong and the security pledges it's making to customers.

Published Feb. 27, 2024

Matt Kapko
Senior Reporter

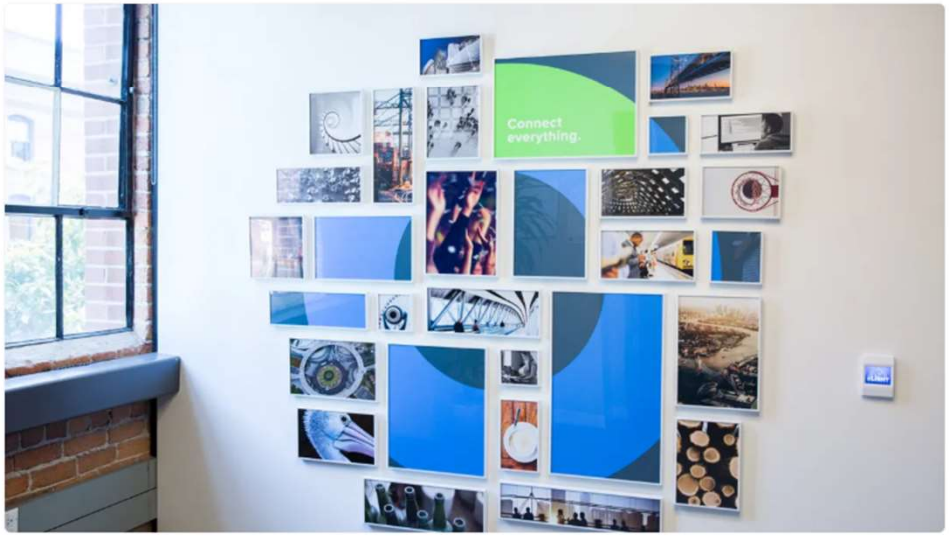


Photo collage on a wall in an Okta office. *Courtesy of Okta*

Common Techniques for Obtaining Credentials

- Advanced phishing campaigns
- Malware
- Social engineering
- Brute force
- Credential stuffing attacks
- Data breach
- Unsecure Public Wi-Fi
- Purchase from the dark web

AI’s Impact on Automation of Attacks

Phishing & Spear Phishing	Password Cracking	Vulnerability Discovery	Malware Creation
AI can generate highly convincing, personalized phishing emails by analyzing publicly available data about targets, making social engineering attacks more effective.	AI-powered tools can rapidly guess or crack passwords using machine learning models trained on common password patterns, drastically speeding up brute-force attacks.	AI systems can scan large codebases or networks to identify vulnerabilities automatically, helping attackers pinpoint weak spots faster than manual methods.	AI can help create polymorphic malware that changes its code or behavior to avoid signature-based detection.

AI’s Impact on Evasion of Detection

Adversarial AI	Behavior Mimicking	Adaptive Malware	Spam & Bot Management
Attackers use AI techniques to manipulate or "fool" security systems like antivirus software, intrusion detection systems, or biometric authentication by exploiting their weaknesses.	AI can analyze normal user behavior and replicate it, making malicious activities look legitimate and thus bypass anomaly detection systems.	AI-powered malware can dynamically change its tactics based on the environment, disabling or modifying its behavior if it detects sandboxing or forensic analysis.	AI-driven bots can manage large-scale spam or fake account generation campaigns more effectively, ensuring they look like human users and evade simple detection rules.

Identity and Access Management (IAM) vs. Mainframe Security

IAM vs. Mainframe Security: A Growing Divide

Enterprise

- Credentials: Corporate IAM
- Authorization: User Directory or other data source
- MFA widely adopted
- Single Sign On

Mainframe

- Credentials: RACF/TopSecret/ACF2
- Authorization: RACF/TopSecret/ACF2
- MFA currently being adopted especially for privileged or remote users

The Gap between IAM & Mainframe Security Controls

Decentralized and Fragmented Identity Management

This separation makes it difficult to apply consistent identity policies across mainframes and enterprise systems.

Limited Support for Modern Authentication Methods

Modern authentication like MFA is often unavailable or involves complex, fragile integrations and is separate from the enterprise.

Lack of Single Sign-On (SSO) Capabilities

This leads to multiple credentials, increasing the risk of reuse, poor management, and higher chances of credential theft.

Inadequate Integration with Identity Federation

This limits integration of mainframe access into enterprise identity ecosystems, making centralized policy enforcement and auditing more difficult.

Restricted Visibility and Auditing for Enterprise IAM Tools

This results in limited centralized visibility of mainframe user activities or policy violations, making detection of insider threats or anomalous behavior more difficult.

Complexity and Legacy Interfaces

This reduces agility in managing identities across the enterprise and introduces risk of orphan accounts or delays in enforcing updated access policies.

Why traditional terminal emulation and authentication mechanisms may no longer suffice

Limited Security Controls

- Lack of multifactor authentication (MFA)
- Weak encryption

Poor IAM Integration

- Lack of support for identity federation
- Lack of SSO
- Increased risk of poor password hygiene

High User Burden & Inefficiency

- Separate credentials = multiple login steps, reduced productivity
- Increased password resets
- Slow access provisioning/de-provisioning

Insufficient Monitoring and Auditing

- Poor SIEM integration and analytics
- Increased blind spots and threat detection

Inability to Defend Against Advanced Threats

- Lack of adaptive, risk-based authentication
- Limited defense against hijacking, replay attacks, spoofing

Challenges in Supporting Remote and Hybrid Work

- Lack of flexibility, security, usability for off-site access
- Lack of VPN-less zero trust access

Risks from this disconnect and why it demands attention

Risk	Description
Inconsistent Access	Mismatched permissions create unauthorized access opportunities
Overprivileged Accounts	Users retain excessive rights beyond their job needs
Orphan/Duplicate Accounts	Unused or duplicate accounts increase vulnerability
Poor Visibility	Fragmented monitoring delays threat detection
Compliance Failures	Non-compliance with audit and security mandates
Credential Compromise Ripple	Easier lateral movement for attackers with stolen credentials
Operational Burden	More manual work, errors, and delays in access management

Regulatory Drivers Impacting Mainframe Security

Regulatory Frameworks Impacting Mainframe Access

NYCRR 500 Compliance

DORA Digital Operational Resilience Act

PCI DSS COMPLIANT

HIPAA Health Insurance Portability and Accountability Act

ISO 27001

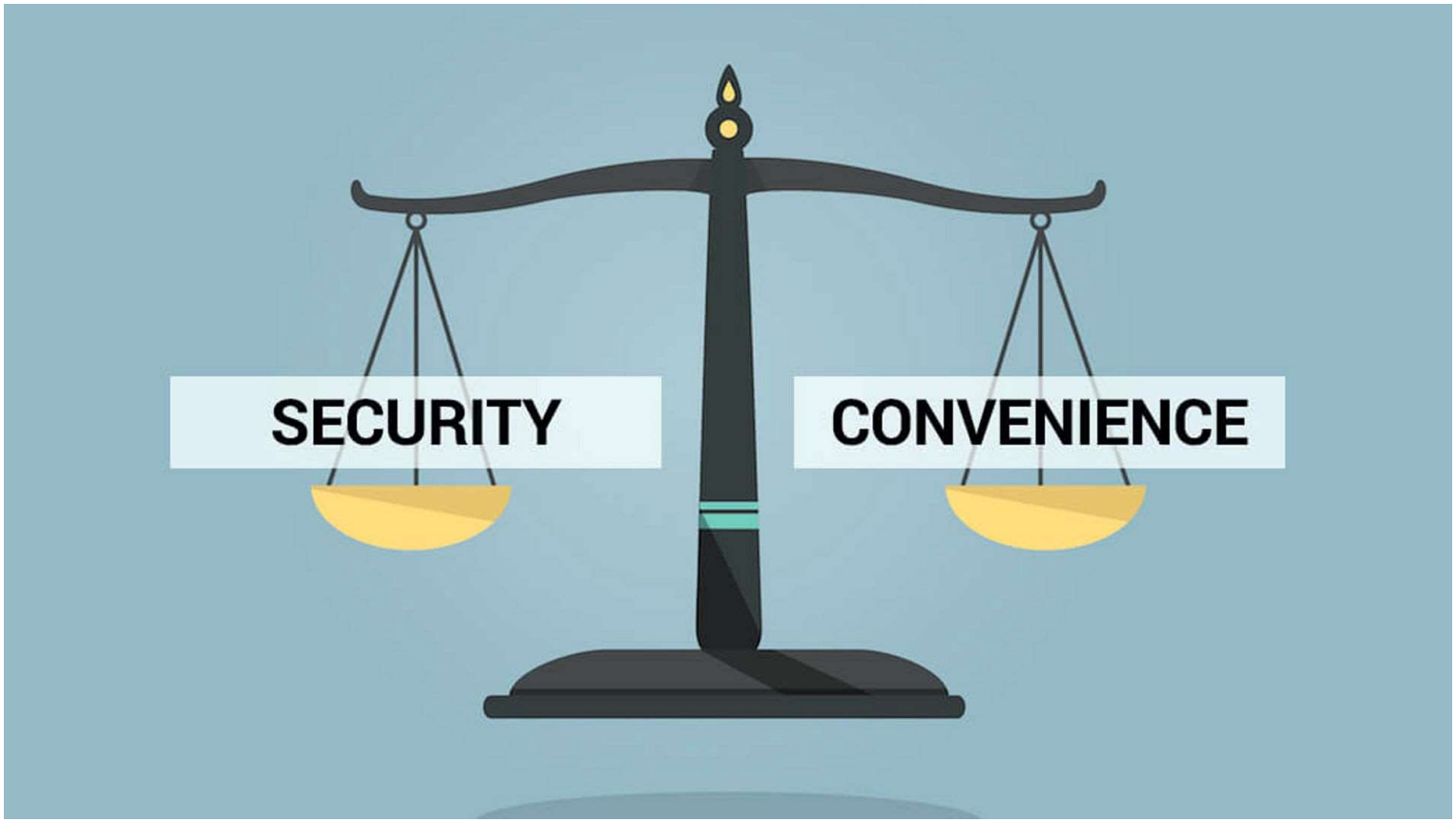
GDPR

NIST National Institute of Standards and Technology

FISMA FEDERAL INFORMATION SECURITY MANAGEMENT ACT

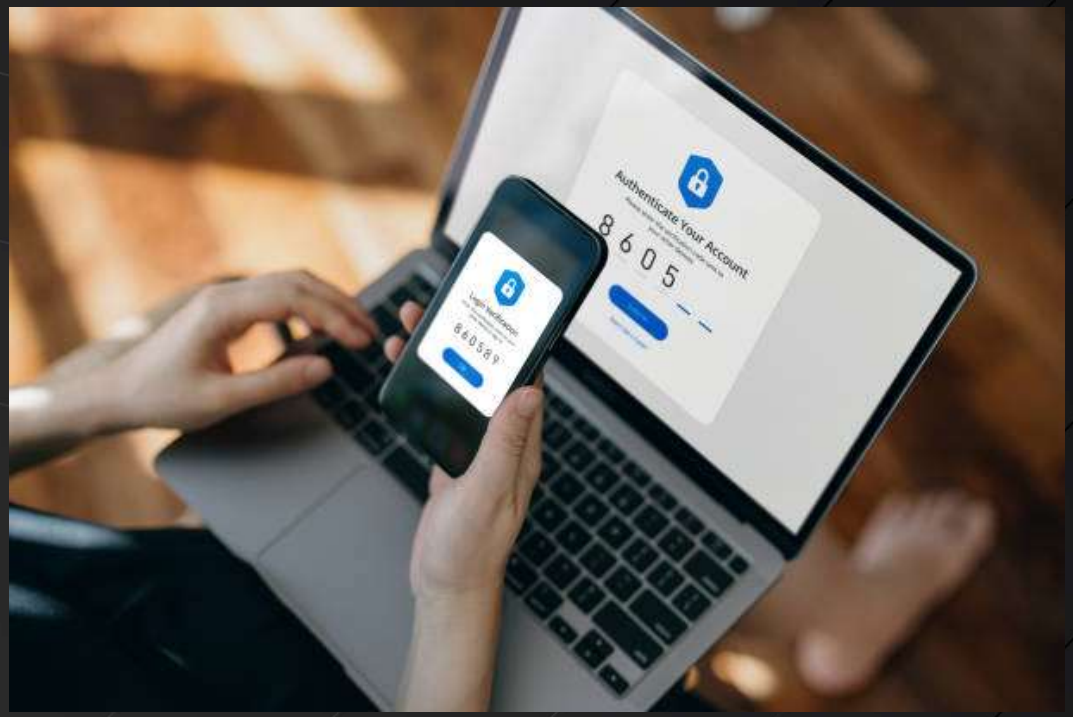
HSPD-12 Interoperability Consortium

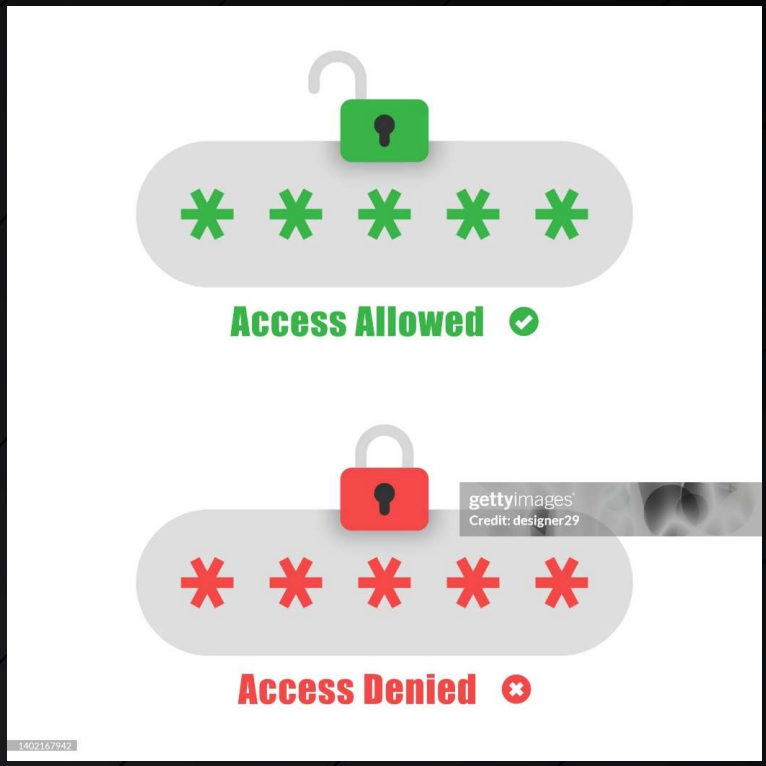
Meeting Compliance Without Disruption



Practical Security Approaches

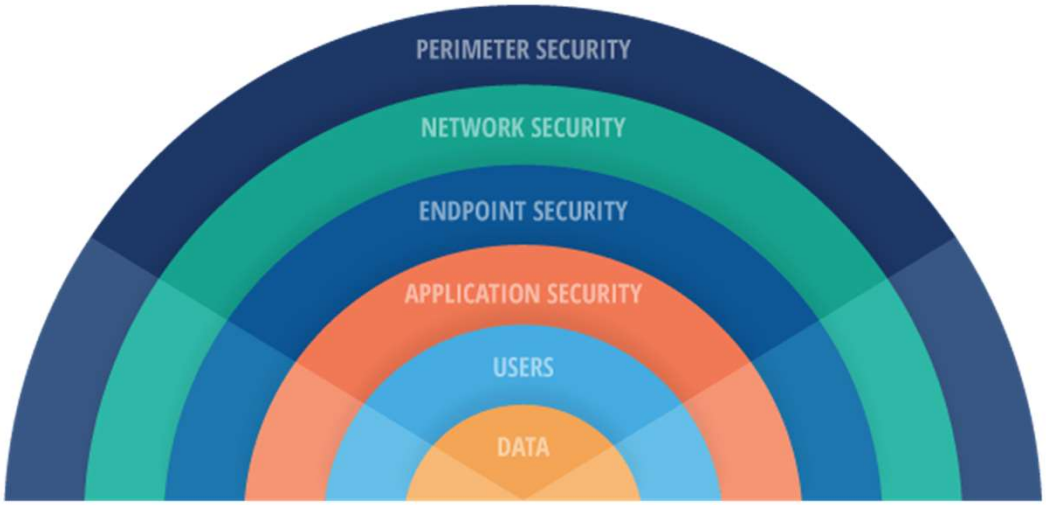
Strong Authentication and Role-based Access





Defense in Depth

A security principle that involves implementing multiple layers of security controls and measures throughout an information system. The idea is to create a series of defensive barriers so that if one layer is compromised, others still provide protection.



Benefits of integrating these controls with IAM solutions and centralized policy management

Benefit	Description
Enhanced Data Security	Encryption and redaction protect sensitive data; IAM controls access and decryption rights
Improved Access Control	Granular IAM policies with centralized management enforce strict and compliant access control
Strengthened Endpoint Security	Ensures only secure, hardened devices are granted system access
Comprehensive Visibility	Monitoring/auditing with IAM logs user and device actions for better detection & compliance
Reduced Insider Threat Risk	Limits data exposure and tracks suspicious activities, mitigating internal breaches
Simplified Management	Centralized, automated policy enforcement reduces errors and operational complexity

Additional terminal-based access security controls

Encryption	Redaction	Endpoint hardening	Monitoring & auditing
• Ensuring data in transit is secure and any sensitive data at rest is encrypted	• The process of redacting sensitive information for users who do not have a legitimate need to view it based on their role in your organization	• Lock down the emulator using PoLP • User data should only be stored in trusted locations, and use User Account Control where applicable	• Understand who is accessing the mainframe, from where, and when

Balancing Security with Usability

Balance security and workflow by:

- Giving users just enough access to do their jobs efficiently (least privilege)
- Applying strong protections like MFA where needed
- Continuously monitoring activity to detect risks without disrupting daily work

This helps keep operations running smoothly while meeting compliance requirements and protecting critical systems.

Best Practices and Recommendations

Best Practices to Mitigate Threats and Comply with Regulations

Key recommendations:

- Add layers of defense between the end user and mainframe
- Implement MFA and strong authentication controls
- Apply least-privilege access models rigorously
  - For authorization and end point hardening
- Use continuous auditing and anomaly detection
- Bridge IAM and mainframe security through unified management

Preparing for the Future

- Emerging trends – AI-driven defenses, adaptive authentication, deeper integration of endpoint posture checks
- Anticipate evolving regulatory requirements and threat sophistication
- Emphasize ongoing reviews and upgrades to mainframe access security practices

Rocket Secure Host Access

Phishing resistant, password-less, secure host access

Easily integrate host application access into your IAM to extend security best practices like SSO, SSH, OIDC, Kerberos, LDAP, SAML, and MFA

Keep your host applications as secure as the rest of the business with minimal additional effort.

The only security-first host access solution to help you:

- Easily stay compliant with DORA, 23 NYCRR 500, US PCI DSS, Federal MFA mandates, and more.
- Mitigate the threat of fake workers, AI, and other cyber attacks

Rocket® software

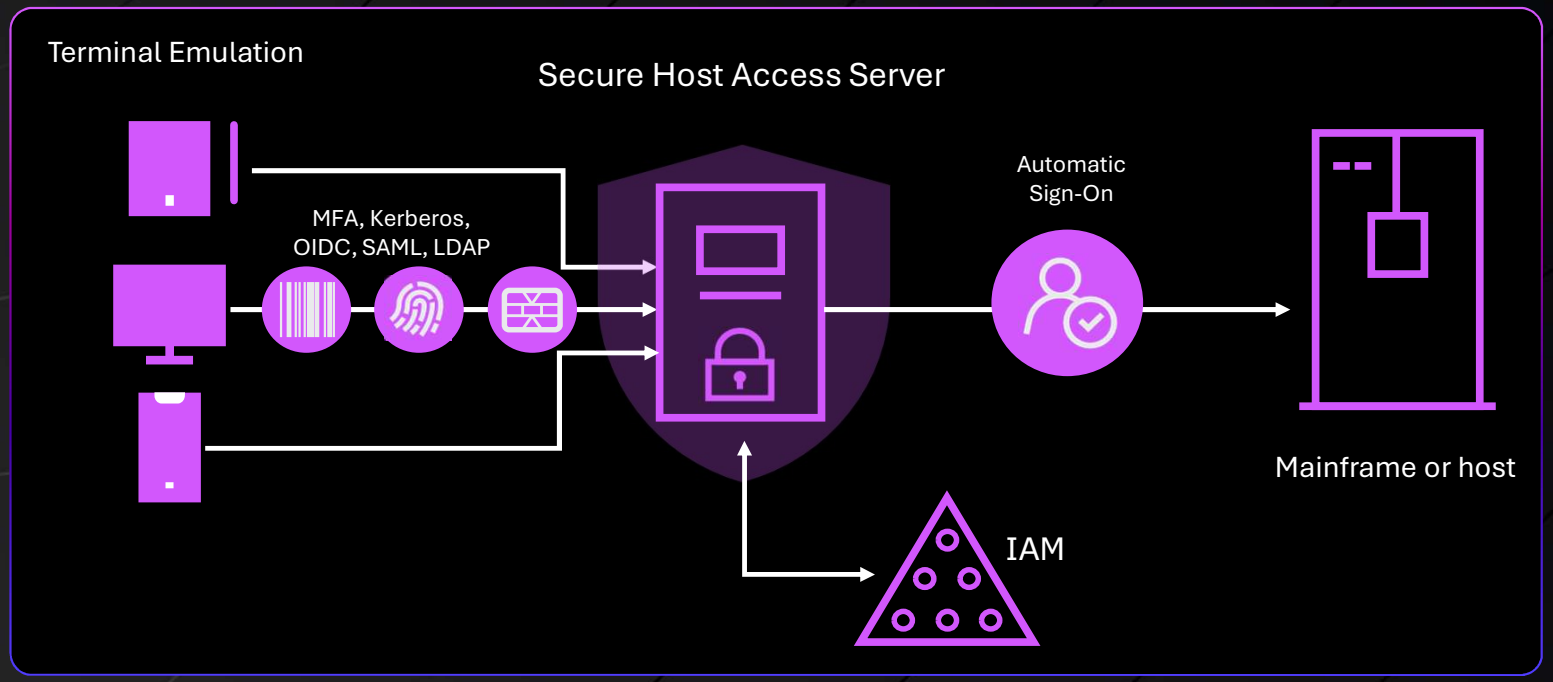
Secure Host Access

Phishing resistant, password-less, secure host access

Easily integrate host application access into your IAM for password-less, phishing resistant, secure host access.

Stay compliant with DORA, 23 NYCRR 500, US Federal MFA mandates, and more.

Mitigate the threat of fake workers, AI, and other cyber attacks.



Summary & Takeaways

A quick recap:

- Cybersecurity threats are evolving
- Gaps between your IAM and mainframe security strategy pose significant risk
- Regulatory pressures
- Practical security strategies
- Securing mainframe access is both achievable and essential
- Proactive security protects both systems and business reputation

Q&A and Discussion

Thank you

bballard@rocketsoftware.com

Rocket® software