Rocket software

Streamlining Agency Operations

Driving efficiency and security with Rocket® Secure Host Access

COMPANY OVERVIEW

This IT provider manages some U.S. federal government systems, processing data for numerous agencies and external partners. For over two decades, they have relied on robust IBM® and Unisys® mainframe environments to ensure national operational continuity.

CHALLENGE

Securing diverse users amidst evolving federal mandates

The organization became aware of the inherent vulnerabilities of its traditional, password-based access methods. This event served as a catalyst for change, effectively requiring the replacement of traditional password-only systems with Personal Identity Verification (PIV) cards or Common Access Cards (CAC) for the Department of Defense. Much later, the organization had to adapt its security posture again to comply with new Identity, Credential, and Access Management (ICAM) policies, which requires far more than just possessing a CAC or PIV card. While these cards are the primary authenticator, ICAM is a comprehensive framework that integrates identity management, automated provisioning, and access policies designed for a zero-trust environment.

CHALLENGE

Transitioning thousands of users to multi-factor authentication (MFA) and ICAM protocols while reducing the complexity of a 50-server infrastructure.

This presented a complex modernization challenge: the provider had to update access protocols for thousands of users across a wide array of external hardware, some of which they had no control over. Compounding this issue was their sprawling internal infrastructure, which consisted of 50 physical servers, to deliver access to host systems and corresponding applications. This extensive setup made routine maintenance, hardware procurement, and general system management increasingly cumbersome, inefficient, and expensive. By adopting Rocket® Secure Host Access, the organization was able to achieve high availability with significantly less infrastructure than their previous products allowed, streamlining their operations and reducing overhead.

SOLUTION

Centralizing control and identity with Rocket® Secure Host Access

Leveraging a deep partnership, the organization collaborated with Rocket Software to implement Rocket® Secure Host Access as a comprehensive solution. This platform was instrumental in centralizing control over their entire system by enabling modern authentication standards like OIDC (OpenID Connect) and SAML (Security Assertion Markup Language) protocols. This key change allowed for a seamless and secure integration with their existing enterprise-wide identity management systems, securing critical access to both their IBM and Unisys mainframes.

For administrators, this meant a significant improvement in day-to-day operations. They gained the ability to manage both desktop and web terminal emulation clients from a single, unified console, which greatly simplified system oversight. From this central point, they could apply granular security controls and enforce session lockdowns as needed across the user base. To guarantee continuous uptime for essential government operations, which could not afford any disruption, the solution was strategically deployed across three geographically distinct data centers, ensuring high availability, resilience, and scalability.

SOLUTION

Rocket® Secure Host Access integrated with the organization's existing Identity and Access Management (IAM) system and consolidated server nodes to ensure secure, high-availability access to applications and data on host systems.

RESULTS

Achieving full compliance and significant infrastructure reduction

Transitioning to Rocket® Secure Host Access was a pivotal move that allowed the provider to meet the government's strict deadlines for authentication modernization. This strategic shift did more than just satisfy immediate requirements; it also dramatically simplified their complex IT environment. By moving away from traditional, often vulnerable, password-based systems and implementing robust ICAM workflows, they successfully achieved full regulatory compliance, including meeting rigorous FIPS (Federal Information Processing Standards) standards. The solution's centralized management approach was key to improving their overall security posture against insider threats, while also creating a more consistent and reliable access experience for their essential external collaborators.

RESULTS

Simplified infrastructure by 90%

Slashed hardware footprint by 90%, consolidating 50 physical servers to just five nodes.

Regulatory compliance

Ensured federal security compliance by implementing MFA, OIDC, and SAML workflows aligned with FIPS standards.

Strengthened data security

Improved data security with features that hide host IPs and disable risky macros, reducing the risk of data leaks.

Guaranteed business continuity

Ensured 24/7 continuity for critical government operations via a high-availability architecture across three data centers.

PRODUCT HIGHLIGHTS

Rocket® Secure Host Access

Key features

- Multi-factor authentication and modern protocol support for secure access.
- Centralized management for all clients from one console.
- High-availability architecture for resilient operations.

At a glance

- 90% reduction in hardware footprint.
- Ensured regulatory compliance.
- Enhanced data security.

Rocket® software

Modernization. **Without Disruption.**™

Visit RocketSoftware.com

Explore more

MAR-17669_LongUC_FederalGovt_V2