Rocket software

Simplifying Secure Mainframe Access

Centralizing identity controls with Rocket® Secure Host Access

CHALLENGE

Adapting to evolving security mandates

The organization needed to replace outdated password systems with modern Personal Identity Verification cards. **They faced a complex challenge updating access protocols for thousands of users** across external hardware while managing a sprawling 50-server infrastructure.

- **Evolving security mandates**
  The provider needed to replace outdated password systems with Personal Identity Verification (PIV) and Common Access Cards (CAC) to meet new federal guidelines and protect against insider threats.
- **Complex ICAM policies**
  New Identity, Credential, and Access Management (ICAM) policies required a zero-trust framework for automated provisioning across a large network of unmanaged external hardware.
- **Infrastructure bloat**
  Managing access to host systems demanded a sprawling internal setup of 50 physical servers, making maintenance and system management inefficient and expensive.

SOLUTION

Centralizing control with Rocket® Secure Host Access

01 Modern authentication

The platform enabled OIDC and SAML protocols for seamless integration with existing identity management systems, securing access to IBM® and Unisys mainframe environments.

02 Unified management console

Administrators could now manage desktop and web clients from a single console, simplifying system oversight and daily IT operations.

03 Granular security controls

The IT team gained the ability to apply specific security controls and enforce session lockdowns from a central point to prevent unauthorized access.

04 High-availability design

Deployed across three distinct data centers, the solution guaranteed continuous uptime and system resilience for essential government operations.

RESULTS

Achieving compliance and reducing infrastructure

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

Regulatory compliance
Ensured federal security compliance by implementing workflows aligned with FIPS standards.

Strengthened security
Improved data security with features that hide host IPs and disable risky macros entirely.

MAR-17670_ShortUC_FederalGovernment_V2