opentext™

Case Study

Federal Agency

Major federal agency validates OpenText security investment.

Overview

With the advent of a serious security breach at the Office of Personnel Management (OPM) affecting over 22 million people, the federal government needs to enhance cybersecurity across its agencies. As part of a 30-day cybersecurity sprint, agencies were directed to further protect federal information, improve the resilience of their networks, immediately patch critical vulnerabilities, review and tightly limit the number of privileged users with access to authorized systems, and dramatically accelerate the use of strong authentication, especially for privileged users.

> **"Micro Focus (now part of OpenText™) gave us a depth of security capabilities, including end-to-end support for HSPD-12, support for automatic single sign-on to the mainframe, and a dedicated sales and support organization known through the U.S. federal government for its security expertise."**

SPOKESPERSON
Federal Agency

Challenge

This particular federal agency is heavily reliant on a mainframe infrastructure integrated with close to 20 mission-critical applications. Over 40,000 individuals will access the mainframe daily. The agency has to comply with the HSPD-12 initiative[1], in particular multifactor authorization, FIPS 140-2, and TLS 1.2 encrypted communication. Also, as a shared resource, the mainframe is not under the agency's direct control, so data encryption cannot be enabled. Data encryption on the mainframe would be controversial in any event, as the federal government has a continuous monitoring requirement that data encryption would inhibit. Instead, the agency relies on log files rather than inspecting the data itself.

The federal government is moving away from user ID and password combinations, which are inherently nonsecure. They are enforcing the use of multifactor authentication to access applications; i.e., a combination of a user PIV card and PIN code.

[1] *The Homeland Security Presidential Directive 12 is a government-wide mandate to safeguard the federal community, information, systems, and facilities through identity certification and access management.*

At a Glance

- **Industry**

  Government—Federal

- **Location**

  USA

- **Challenge**

  The agency's existing terminal emulation solution was old, nonsecure, and noncompliant with HSPD-12 security requirements. It needed a replacement solution flexible enough to meet its architectural needs and provide strong security.

- **Products and Services**

  Reflection Desktop
  Reflection for the Web
  Host Access Management and Security Server (MSS)
  MSS Automated Sign-On for Mainframe Add-On

- **Success Highlights**

  + Enabled HSPD-12 compliance for mainframe access
  + Improved usability with single sign-on to the mainframe
  + Leveraged existing infrastructure within a defined security framework
  + Opened the door to a Java-free browser environment
  + Encrypted communications and enabled content inspection

> "We regard Micro Focus (now part of OpenText™) as trusted advisors, and with its broad range of solutions, from mobile to mainframe, we expect the relationship to go from strength to strength."

SPOKESPERSON
Federal Agency

Connect with Us
OpenText CEO Mark Barrenechea's blog

The agency's existing terminal emulation solution was old, nonsecure, and noncompliant with HSPD-12 security requirements. It needed a replacement solution flexible enough to meet its architectural needs and provide strong security.

Managing X.509 security certificates directly on the mainframe is impractical. Certificates are linked to individuals and require maintenance and renewal, creating too much overhead with a user base of over 40,000 individuals.

Solution

The agency looked for a repeatable, commercial solution, flexible enough to meet its unique demands. OpenText™ presented the Reflection family of products, which would leverage the existing Active Directory and PKI infrastructure. The agency can authenticate mainframe users with X.509 certificates from their smart cards and enforce this level of access. This tight access control for terminal sessions leverages multiple levels of security. Authentication and authorization takes place at the perimeter rather than on the mainframe itself. The Reflection security proxy is a true reverse proxy that leverages a JITC-certified token to ensure that TFA is enforced. The proxy also allows users to connect via TLS encryption and then is able to break that encryption behind the firewall to securely allow for content inspection of the data stream.

Once authenticated using their PIV card[2] and PIN, users are automatically logged onto the mainframe with appropriate credentials. The solution provides seamless sign on to the mainframe without the user ever having to enter a password. This methodology provides a frictionless ease-of-adoption that agencies are striving to create for their end users as they implement more secure methods of access.

The agency has a long-term plan to eliminate Java from its browser environment and minimize the number of applications running on the desktop. They are pushing towards a centralized identity-based access solution that will allow centrally controlled access to mission-critical applications. It is now possible for them to do this with their mainframe applications.

Results

The Reflection suite of products enabled the agency to leverage its current infrastructure and integrate this into a defined security framework. With Reflection, the agency can provide multifactor authentication in support of HSPD-12, meet continuous monitoring requirements, and eliminate passwords with complete single sign-on. The same security requirements can be applied across other platforms, providing a uniform approach across the agency. The solution also enables the agency to eventually transition to a Java-less browser environment.

An agency spokesperson concludes: "Micro Focus (now part of OpenText™) gave us a depth of security capabilities, including end-to-end support for HSPD-12, support for automatic single sign-on to the mainframe, and a dedicated sales and support organization known through the U.S. government for its security expertise. We regard Micro Focus (now part of OpenText™) as trusted advisors, and with its broad range of solutions, from mobile to mainframe, we expect the relationship to go from strength to strength."

Learn more at
www.microfocus.com/opentext

[2] *Personal Identity Verification is a United States federal smart card that contains the necessary data for the cardholder to be granted access to federal facilities and information systems and assure appropriate levels of security for all applicable federal applications.*