



WHITE PAPER

Secure Financial Services Applications in Virtualized and Cloud Environments with Gemalto and Xceedium

Securely move financial services applications to virtualized environments and the cloud with Xceedium and Gemalto.

Introduction

Financial institutions are now considering moving resources to the cloud and virtualized environments because of the advertised efficiencies and performance gains. The cloud's pay-as-you go approach means firms can expand quickly without having to make significant capital investments as the number of account and transaction records grows. Additionally, financial organizations using a cloud-based approach can streamline operations as offices in financial centers such as Shanghai, Frankfurt, London, and New York have access to centrally stored information.

To move their resources to the cloud, financial institutions must have confidence that their information is in trustworthy hands, since trust is at the center of the operations that they conduct daily. Both customers and regulators demand that firms protect sensitive account and cardholder information from external and internal threats. That protection is particularly hard to achieve when it comes to privileged users in the hybrid cloud. These trusted insiders and contractors enjoy wide-reaching administrative-level access to information, systems, and the actual infrastructure on which applications operate. As a consequence of this unfettered access and power—which often bypasses routine business controls—successfully managing risk and ensuring compliance demands specialized controls. Rigorous protection of passwords and credentials and strong authentication represent the crucial foundation of a comprehensive set of privileged user management capabilities.

Yet, despite the benefits of the cloud and virtualization, security risks are off-putting as potential damage to an institution's reputation can cost millions in lost business, eroded market share, and possible regulatory violations leading to fines and legal liability. As a result, financial sector

Benefits

By harnessing solutions from Gemalto and Xceedium, financial services customers can realize a range of significant benefits:

- > **Boost security.** Additional layers of authentication and controls isolate data from users responsible for the cloud infrastructure where sensitive financial information is stored.
- > **Expand cloud initiatives.** Firms can take advantage of the technical and business benefits of cloud and virtualization without worrying about undue access to data.
- > **Demonstrate compliance.** Strong authentication and detailed activity logs allow financial services firms to more easily demonstrate compliance with regulatory requirements.

IT and security teams are faced with two highly unappealing options—either failing to capitalize on the benefits of virtualization, or moving critical workloads into these environments and incurring significant risk.

Financial institutions can address the privileged user risk to sensitive workloads in the cloud.

Solution Introduction

Now, financial services institutions can address the privileged user risk to sensitive workloads in virtualized and cloud environments. With Gemalto and Xceedium, organizations know that data access is restricted only to authenticated users with the appropriate permissions. The companies deliver two offerings:

Gemalto's SafeNet Authentication Service and SafeNet smart cards combined with Xceedium's Xsuite. SafeNet authenticators from Gemalto provide identity verification for Xceedium's Xsuite privileged identity management system. Xsuite examines all privileged user activity and compares commands to policies prior to execution, preventing unauthorized and malicious activities. Its role-based access controls, separation of duties and recorded sessions ensures that users only have access to the information they need and that all activity is fully monitored. Implemented together, organizations can verify identities, restrict access to sensitive data by privileged users, and go above and beyond in meeting the PCI DSS's unique identification requirements. This solution deploys on-premises, and in virtualized and Amazon Web Services (AWS) environments.

Xsuite with Gemalto's SafeNet Luna SA hardware security modules (HSMs). Xsuite hardware appliances are available with SafeNet Luna HSMs—Federal Information Processing Standard (FIPS) 140-2 Level 3, tamper-resistant hardware appliances—for additional security. Xsuite can store the cryptographic keys, certificates, and permissions that guard access in hardware to protect valuable cryptographic materials from the vulnerability of traditional software storage. Vault-based storage of cryptographic materials enforces separation of duties so those maintaining servers cannot decrypt the data stored in their environments. SafeNet Luna SA and Xsuite can be deployed on-premises in physical servers, on virtualized servers running VMware vSphere, and in Amazon Web Services (AWS) environments.

Financial institutions can address the privileged user risk to sensitive workloads in the cloud. Customers can store cryptographic keys and credentials in a tamper-resistant appliance for maximum security.

Features

Solutions from Gemalto and Xceedium offer these key features:

Top-of-the-line hardware protection. Customers can store cryptographic keys and credentials in a tamper-resistant appliance for maximum security. Software stored materials can easily be copied, corrupted, or decrypted, ultimately rendering an organization's security ineffective. By storing cryptographic materials in hardware, important keys and certificates are protected from prying eyes and are available only to authenticated, authorized users. The physical separation of encryption keys makes it easier to divide privileges so IT professionals can manage the virtualized environment without gaining access to the keys for the encrypted data within the environment.

Granular access control. Xsuite operates on a zero-trust basis so network and application access is denied unless specifically granted from within Xsuite's management console. Gemalto's SafeNet authenticators add an additional layer of security so only the appropriate users – internal or at third-party service providers – gain access to financial information or administrative functions. The combination of granular access controls and strong authentication offers a robust yet nuanced approach to identity management.

Convenience of federation. Financial firms can implement identity federation with Xsuite and Gemalto's strong authentication for secure, yet streamlined, access to server environments and applications. Xsuite connects to identity and role information located in the existing enterprise directory, eliminating the need to manage separate identity stores and role definitions. As a result, users enjoy single sign-on convenience while organizations enjoy higher levels of security and the cost-savings of streamlined administration.

The solution operates on a zero-trust basis so network and application access is denied unless specifically granted.

Flexible implementation and maintenance. Customers enjoy flexibility during both initial deployment and over the long term. Xsuite's access management logically segments the network, creating isolated, tightly controlled data islands. Additionally, Xsuite fits existing network topologies so administrators need not change their network structures to achieve data isolation. SafeNet Luna HSMs can be deployed in the cloud and feature upgradeable software so they can remain in use longer. Further, SafeNet Luna SA supports a wide range of configurations, supporting up to 20 partitions. This solution is easy to implement and provides the type of efficiencies that organizations are searching for in using the cloud.

Complete data isolation. Xsuite eliminates application-to-application passwords from scripts, codes, and configuration files connected to cardholder data processing systems. Data stays isolated as Xsuite eliminates the threat of application developers and testers stealing administrative passwords in plaintext as they pass from one application to another.

Use Case: Wealth Management Application

Challenge

A bank needed to support an online wealth management application for its corporate clients. Further, they were incurring increasing infrastructure costs to support periodic spikes in demand. Corporate clients and partners needed access to the information provided by the application. And application developers and system administrators needed access to the servers and application to maintain it. How could they meet the higher demand while still keeping access to the application, and the back-end accounts and credentials, segregated and secure?

Solution

The bank's IT team migrated to AWS, which enabled the organization to quickly and economically scale the capacity required to support fluctuating traffic. The organization leveraged SafeNet Authentication Service from Gemalto and Xsuite in order to deploy robust, multi-factor authentication controls.

Benefit

Through its migration to the AWS platform, the bank was able to enjoy increased agility and cost efficiency in accommodating fluctuating usage of its e-banking platform. At the same time, with Gemalto and Xceedium, the organization was able to reduce its exposure to internal abuse and external attacks, and the associated cost and brand damage associated with breaches.



The solution eliminates application-to-application passwords from scripts, codes, and configuration files.

About Xceedium

Xceedium, Inc., is a network security software company and the leading provider of privileged identity management solutions for hybrid cloud enterprises. Large companies and global government agencies use Xceedium's products to reduce the risks privileged users and unprotected credentials pose to systems and data.

About Gemalto's SafeNet Identity and Data Protection Solutions

Through its acquisition of SafeNet, Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions – from the edge to the core. Gemalto's newly expanded portfolio of SafeNet Identity and Data Protection solutions enables enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Contact Us: For all office locations and contact information, please visit www.safenet-inc.com

Follow Us: [data-protection.safenet-inc.com](https://twitter.com/data-protection.safenet-inc.com)

 GEMALTO.COM

gemalto
security to be free