SafeNet and Xceedium
Access Controls for the Cloud, Compliance, and Security
SOLUTION BRIEF

Benefits

Through their integrated solutions, SafeNet and Xceedium provide joint customers with a range of benefits:

- **Ensure compliance.** These solutions offer the robust security controls that are in alignment with the most stringent security policies and mandates.

- **Boost security.** Through the solutions' capabilities, organizations can more effectively guard against unauthorized access, mitigate the risk of abuse by privileged insiders, and eliminate the exposure presented by unprotected credentials.

- **Expand cloud initiatives.** These solutions provide the security controls and auditability that organizations need to move forward with their virtualization and cloud initiatives—without making any compromises in security and compliance.

With SafeNet and Xceedium, even organizations with the most stringent security policies and mandates can leverage cloud services.

Introduction

In recent years, many companies have adopted cloud services and delivery models. They have realized enhanced agility, reduced capital expenditures, and improved productivity. However, for many organizations, these benefits have been out of reach due to unaddressed security questions and challenges. Traditionally, organizations have had to choose between high assurance and regulatory compliance or moving to the cloud—doing both wasn't an option. Ultimately, many applications and assets remain solely on premise and the organization suffers, or organizations move forward with their cloud objectives, and jeopardize their security and compliance status.

Solution Introduction

With joint solutions from SafeNet and Xceedium, federal agencies, financial services institutions, healthcare establishments, and other organizations can adhere to stringent compliance requirements and protect sensitive assets as they leverage virtualized, hybrid cloud, and cloud infrastructures. These solutions include:

- **Xceedium Xsuite.** Xceedium Xsuite is an appliance-based platform that enables control over the access, activities, and credentials of privileged users. In addition, Xsuite's AWS cloud extension enables organizations to deliver these security controls to cloud and hybrid-cloud architectures.

- **SafeNet Authenticatin Service (SAS).** SafeNet Authentication Service makes two-factor or strong authentication easy to implement and manage. SAS is available in cloud-based or on-premise versions for both enterprises and service providers.

- **SafeNet smart cards.** SafeNet's single- and multi-domain smart cards deliver highly secure, two-factor authentication capabilities that help ensure only authorized users can access sensitive corporate networks and online business applications.

- **SafeNet Luna SA HSM.** The SafeNet Luna SA HSM ensures the integrity and security of cryptographic operations in a robust, high-availability appliance.

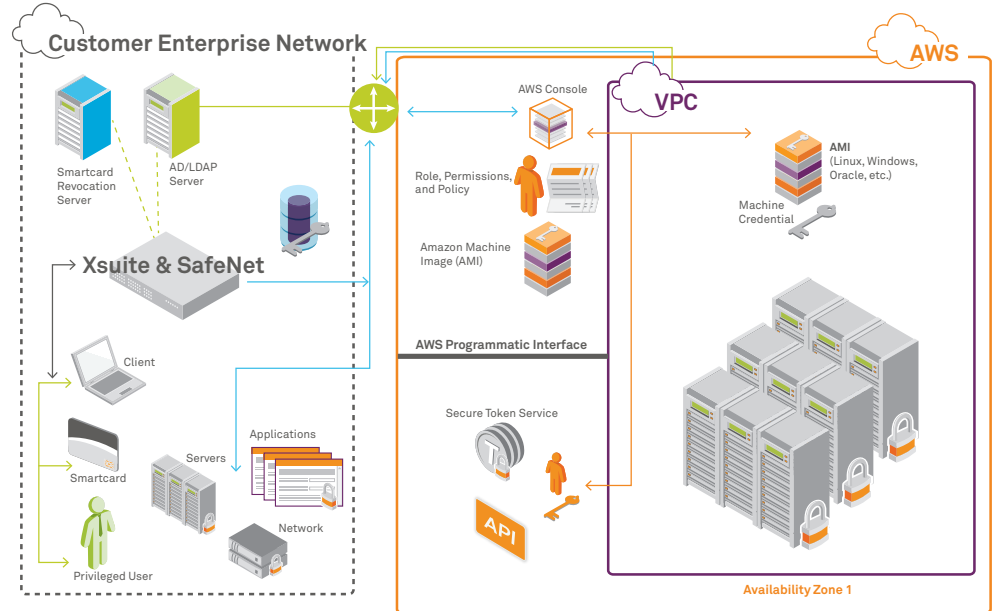## Multi-factor Authentication-based Access Controls

With the integration of SafeNet smartcards and SAS, organizations can leverage high-assurance extensions to the Xsuite solution.

These integrated solutions offer the following key features:

- **Extensive access controls.** The integration between SafeNet's smart cards and Xsuite will enable organizations to positively identify and authenticate elevated-privilege users, such as system, network, database, virtualization, and cloud administrators, before they are allowed to perform administrative functions. This integrated solution enables secure access controls over all accounts, including administrative accounts and cloud infrastructure management systems, such as the AWS Management Console.

- **Compliance with U.S. agency requirements.** This solution addresses a U.S. federal government agency mandate for Common Access Card (CAC)/Personal Identity Verification (PIV) access controls.

- **Support for on-premise and cloud deployments.** Organizations can use SafeNet smart cards to authenticate users to the Xsuite appliance, whether on-premise or in the cloud.

- **Identity federation.** These solutions enable security teams to federate identities within AWS environments so privileged users can have secure access to the AWS-based infrastructure and the AWS Management Console without the extra work required to add and maintain individual users or groups within the AWS identity and access management (IAM) database.

- **Comprehensive auditing.** Xsuite monitors and records all privileged user sessions.

Mitigating the Exposure of AWS Administrator Privileges

The ability to provide greater certainty in user authentication is especially critical when managing access to cloud administrator consoles. Through these consoles, administrators can add, delete, copy, and modify entire servers or systems running in the AWS EC2 environment. Not only does this pose security risks, but direct financial exposure; these changes can entail additional charges, which can create concerns for organizations trying to keep tight controls over procurement.

The Amazon Web Services team has enabled separation of duties for administrators using the AWS Management Console. However, this requires organizations to define and maintain user and group roles in a separate AWS IAM directory. The Xsuite extension for AWS enables organizations to leverage identity and role information contained in their current enterprise directory and federate these identities into the AWS IAM services on the fly—eliminating the need to manage separate identity stores and role definitions. With the integration of Xsuite and SafeNet smart cards, organizations can positively authenticate these critical users and enforce separation of duties, without the cost and complexity of managing multiple identity databases.

FIPS-compliant Appliances and Key Storage

The FIPS 140-2 Level 3 conformant version of Xsuite hardware appliances now features the SafeNet Luna SA HSM. With this integrated solution, security teams can realize maximum security of privileged user access, and of the cryptographic keys and permissions that guard this access. This solution offers administrators the flexibility to store critical cryptographic keys in the SafeNet Luna SA HSM within the customer's enterprise or within AWS's CloudHSM offering, which leverages SafeNet HSMs.

This solution provides a range of features:

- **Robust security mechanisms**—providing secure, vault-based storage of passwords and credentials.

- **Granular controls**—including fine-grained control over the execution of commands through application access.

- **Comprehensive auditing**—enabling security teams to get complete monitoring, recording, and playback of privileged user sessions.

About SafeNet

Founded in 1983, SafeNet, Inc. is one of the largest information security companies in the world, and is trusted to protect the most sensitive data for market-leading organizations around the globe. SafeNet's data-centric approach focuses on the protection of high-value information throughout its lifecycle, from the data center to the cloud. More than 25,000 customers across commercial enterprises and government agencies trust SafeNet to protect and control access to sensitive data, manage risk, ensure compliance, and secure virtual and cloud environments.

About Xceedium

Xceedium, Inc. is a network security software company, and the leading provider of privileged identity and access management solutions for hybrid-cloud enterprises. Large companies and global government agencies use Xceedium's products to reduce the risks that privileged users and unprotected credentials pose to systems and data. Xceedium Xsuite, the company's award-winning product, enables customers to implement a zero-trust security model. Xsuite vaults privileged account credentials, implements role-based access control, and monitors and records privileged user sessions. With privileged identity management, the Xsuite platform enables the seamless administration of security controls across systems, whether they reside in a traditional data center, a private cloud, on public cloud infrastructure, or any combination thereof.