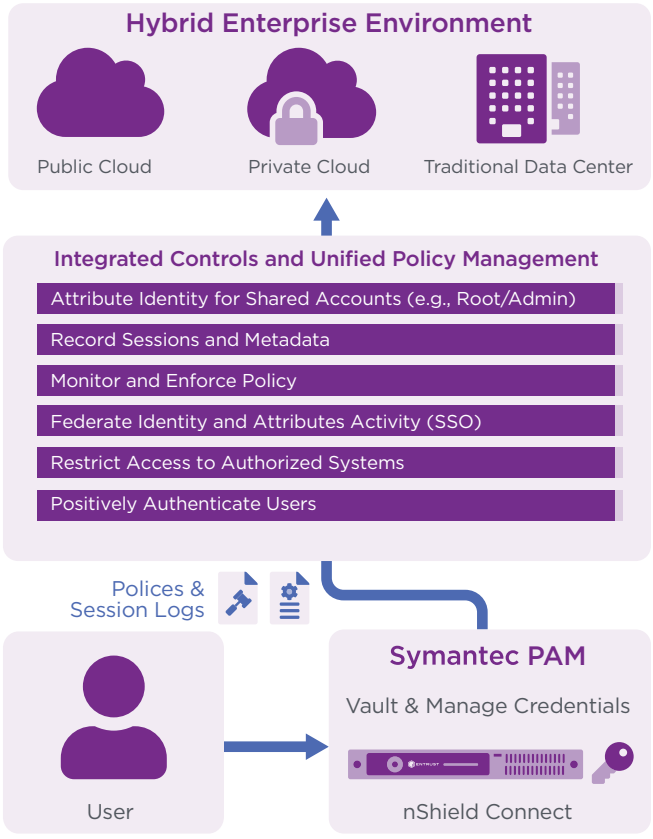
Entrust and Broadcom Protect Privileged Access Credentials and Associated Keys

Security solution provides hardware-based encryption and management of stored credentials

HIGHLIGHTS

- Manage privileged credentials and provide positive user authentication
- Protect privileged credentials from external and internal threats
- Monitor, audit, and record sessions
- Provide root of trust for encryption and decryption keys
- Facilitate security auditing and compliance with FIPS 140-2 L3 certified hardware



Symantec Privileged Access Management uses Entrust® nShield Connect hardware security modules (HSMs) to encrypt and decrypt privileged account credentials.

Learn more about our HSMs at entrust.com

Entrust and Broadcom Integrated Solution

The Problem

Privileged credentials can be exploited to gain access to systems and their sensitive data

Compromised privileged accounts are the culprit of many data breaches. Holding the organizations' keys to the kingdom, privileged account credentials are a preferred target of external and internal attacks. The protection of these credentials is thus an imperative to successfully defend organizations and facilitate compliance with ever more stringent data security regulations.

The Challenge

Defending enterprise privileged account credentials and the data they protect without impacting operational efficiency

Privileged credentials open doors to accounts and the sensitive data they hold, and underpin the security of entire privileged access systems. Finding and guarding external and internal conduits to these accounts can be difficult when implementing across multiple points in the enterprise. A centralized solution that enables visibility and control of accounts without affecting operational efficiency is necessary for comprehensive security.

The Solution

Broadcom's Symantec Privileged Access Management with Entrust nShield HSMs

Broadcom's Symantec Privileged Access Management is an automated solution for privileged access management in physical, virtual, and cloud environments. Available as a physical hardened appliance or virtual machine instance, the solution enhances security by protecting sensitive credentials such as root and administrator passwords, controlling privileged user access, proactively enforcing policies, and monitoring and recording privileged user activity across all IT resources.

Broadcom's Symantec Privileged Access Management integrates with Entrust nShield HSMs to encrypt and decrypt stored credentials.

The joint solution delivers an added layer of security, protecting access credentials and the doors they open to privileged accounts and the sensitive data they hold. Entrust nShield HSMs provide FIPS 140-2 Level 3 and Common Criteria EAL4+ certified key protection, which enables organizations to deliver a high assurance environment to comply with industry best practices.

Why use Entrust nShield HSMs with Broadcom's Symantec Privileged Access Management?

Entrust nShield HSMs encrypt and decrypt privileged account credentials and protect associated keys in a dedicated environment. Keys handled outside the protected boundary of certified HSMs are significantly more vulnerable to attacks, which can lead to disclosure of confidential information. HSMs provide a proven and auditable way to secure valuable cryptographic material. HSMs:

- Provide added layer of security with a root of trust for privileged account management
- Ensure cryptographic key operation is smooth, easy to manage, and secure
- Protect keys within a carefully designed boundary using robust access controls so keys are only used for their authorized purpose
- Ensure availability using sophisticated key management, storage, and redundancy features to guarantee keys are always accessible when needed
- Deliver high performance to support increasingly demanding transaction rates
- Comply with regulatory requirements for public sector, financial services, and enterprises

nShield Connect is a high-performance, network-attached HSM for high-availability data center environments.

Entrust and Broadcom Integrated Solution

Entrust HSMs

Entrust nShield HSMs are among the highest-performing, most secure, and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial, and government organizations. Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

Broadcom

Broadcom is a global technology leader that designs, develops, and supplies a broad range of semiconductor and infrastructure software solutions. Broadcom's category-leading product portfolio serves critical markets including data center, networking, enterprise software, broadband, wireless, storage, and industrial. Our solutions include data center networking and storage, enterprise, mainframe, and cybersecurity software focused on automation, monitoring and security, smartphone components, telecoms, and factory automation.

To learn more, please visit:
broadcom.com/products/cyber-security/identity/pam

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications, and data visit **entrust.com**.

Learn more at
entrust.com/HSM

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223