Enhancing the Security of Credentials and Secrets with Entrust nShield HSMs

High assurance protection of privileged account credentials and corporate secrets

CHALLENGE

Attackers seek opportunities to exploit privileged credentials and corporate secrets

Organizations today depend on an increasingly diverse set of infrastructures and applications, some of which contain sensitive data that requires high assurance protection.

Many organizations establish privileged accounts for highly trusted individuals who are responsible for these systems. Others offer their own repositories to store secrets such as tokens, passwords, certificates, and API keys.

Both privileged account credentials and application secrets call for special protection.

Privileged accounts

Organizations require full control over privileged account credentials, including the ability to monitor and audit each privileged activity, grant access for a specified time period, and automatically revoke it upon expiration. Such capabilities are critical to defend against insider attacks, and are not possible when managing privileged credentials via manual processes.

HIGHLIGHTS

- Protect and manage keys that secure privileged accounts and secrets vaults within a certified, protected boundary
- Mitigate risks associated with centralizing/aggregating credentials and secrets
- Provide a FIPS 140-2 Level 3 and Common Criteria EAL4+ root of trust
- Facilitate auditing and compliance with data security regulations

Enterprises increasingly use privileged access management (PAM) tools to authorize, manage, and audit account and data access by specific users and applications.

Learn more about Entrust HSMs at entrust.com

Entrust nShield HSMs and Privileged Access/Secrets Management

Corporate secrets

Using more applications, each with their own repositories of secrets access credentials, not only proliferates secrets across the organization, but also results in silos with varying lifecycle management and protection policies. Managing these sprawling secrets across environments creates an administrative burden and increases exposure due to user error and/or deliberate attacks.

As a result, organizations use secrets management solutions to ensure centralized and consistent policy enforcement and reduce secrets sprawl.

The concentration of high-value corporate assets within privileged account and secrets management vaults and repositories make them attractive targets for both malicious insiders and external attackers. Therefore, high assurance security is a must.

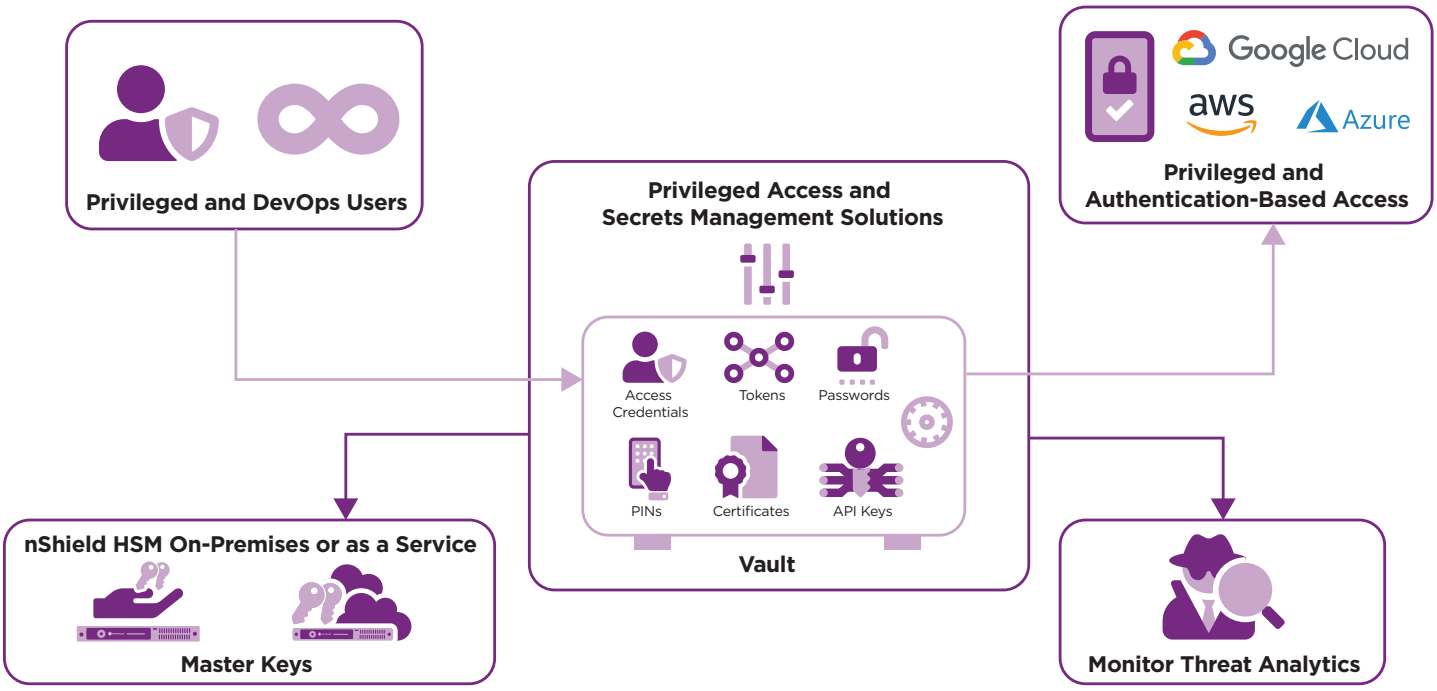
SOLUTION

Privileged access and secrets management solutions integrated with HSMs

Privileged access and secrets management solutions use cryptographic keys to lock the vaults and repositories that house assets such as critical credentials, passwords, PINs, and tokens.

Entrust nShield® Hardware Security Modules (HSMs) integrate with leading privileged access and secrets management solutions to protect the keys that secure these vaults and repositories. The integration with PAM solutions provides an added layer of security for privileged account credentials, the doors they open to privileged accounts, and the sensitive data they hold.

HOW IT WORKS



Learn more about Entrust HSMs at entrust.com

Entrust nShield HSMs and Privileged Access/Secrets Management

The integration of nShield HSMs with secrets management solutions helps mitigate potential risks created by aggregating secrets under a centralized management model. This eliminates secrets sprawl with centralized controlled access, based on trusted identities and policy enforcement.

THE nSHIELD DIFFERENCE

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

Available as network-attached appliances or PCIe cards, as well as via a subscription-based service, Entrust nShield HSMs:

- Secure keys and certificates within a carefully designed cryptographic boundary, using robust access control mechanisms to ensure keys are only used for their authorized purpose
- Ensure availability with sophisticated key management, storage, and redundancy for constant, reliable key access
- Deliver high performance to support increasingly demanding transaction rates
- Comply with regulatory requirements for public sector, financial services, and other enterprises that process sensitive data

ENTRUST READY TECHNOLOGY PARTNERS

Entrust Ready Technology Partners include leading solution providers that incorporate an HSM root of trust in their offerings, ensuring delivery of enhanced security for all data and applications. nShield HSMs are integrated with privileged access and secrets management solutions from the following providers.

CYBERARK

BeyondTrust

WALLIX
CYBERSECURITY SIMPLIFIED

BROADCOM

HashiCorp

Delinea

Learn more about Entrust HSMs at entrust.com

For more information

888 690 2424
+1 952 933 1223
sales@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling strong identities, secure payments, and protected data. We offer an unmatched breadth of solutions that are critical to the future of secure enterprises, governments, the people they serve, and the data and transactions entrusted to them. With our experts serving customers in more than 150 countries and a network of global partners, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com entrust.com/contact