Secure privileged access management with nShield HSMs

NFINITY STRATEGIC TECHNOLOGY PARTNER PROGRAM

High assurance protection of privileged account credentials

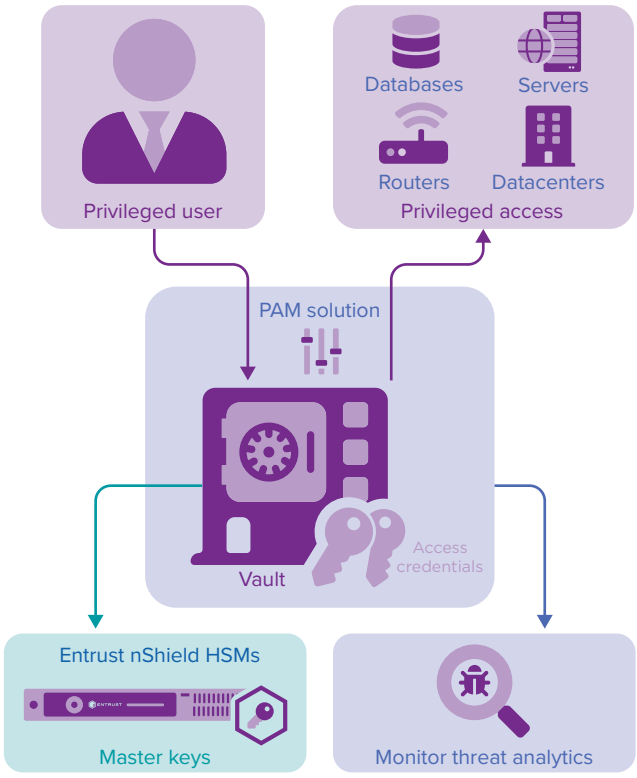
HIGHLIGHTS

- Cryptographic keys used to access the vault are secured within a tamper resistant FIPS 140-2 Level 3-certified HSM
- Protect and manage large numbers of privileged account keys within protected hardware boundary
- Integrate with privileged account credentialing and management solutions
- Facilitate auditing and compliance with data security regulations
- Enhance security of privileged access
- Improve accountability and control over privileged passwords

The challenge: attackers seek opportunities to exploit privileged accounts

Organizations establish privileged accounts for highly trusted individuals that provide unique access and privileges based on their roles and responsibilities. For example, a privileged user might be able to upgrade an operating system, add or remove software, or access files and directories that are inaccessible to typical users.

Attacks on enterprise IT infrastructures increasingly seek access to privileged user account credentials. These credentials are highly attractive to attackers, as a compromise can open an easy path to an enterprise's most sensitive information. Privileges can also be abused to gain access to more accounts, and compromised credentials can go undetected for an extended period because the attacker appears to be a trusted user.



LEARN MORE AT ENTRUST.COM/HSM

Secure privileged access management

Organizations require full control over privileged account credentials, including the ability to audit their use, impose automatic time restrictions and instantly revoke access as needed. Such capabilities are not available when managing privileged credentials via spreadsheet or other manual processes.

Similar to other essential enterprise systems and credentials, privileged accounts require cryptographic protection secured by high assurance protection of the underpinning encryption keys.

The solution: privileged access management solutions integrated with nShield HSMs

Enterprises deploy privileged access management (PAM) tools to authorize, manage and audit account and data access by specific users and applications. PAM tools allow customers to:

- Protect privileged credentials within a secure, encrypted vault
- Limit access to specific systems based on the user's role
- Grant access for a specified time period and automatically revoke it upon expiration
- Monitor and audit each privileged activity

As with any use of cryptography, the highest assurance protection of the encrypted vault incorporates a hardware security module (HSM) to protect the root encryption keys.

Entrust nShield® HSMs are integrated with leading PAM solutions to offer FIPS 140-2 Level 3 and Common Criteria EAL 4+ protection for the keys that protect privileged account credentials. The combined solution provide an added layer of security protecting both access credentials and the doors they open to privileged accounts and the sensitive data they hold.

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.

Secure privileged access management

nFinity Partners

BeyondTrust Password Safe unifies privileged password and privileged session management, providing secure discovery, management, auditing, and monitoring for any privileged credential. Password Safe enables organizations to achieve complete control and accountability over privileged accounts.

BeyondTrust Password Safe integrates with Entrust nShield HSMs to safeguard and manage encryption keys used to protect stored privileged access credentials.

Broadcom Privileged Access Manager 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 administrative 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.

The Broadcom Privileged Access Manager integrates with the Entrust nShield HSMs to encrypt and decrypt stored credentials.

CyberArk Privileged Access Security Solution is an enterprise-class, unified platform that allows organizations to manage and secure all privileged accounts. The solution secures credentials, including passwords and SSH keys, controls access to these accounts, and isolates and records privileged sessions that are used for auditing and forensics analysis.

Combined with nShield Connect HSMs, these solutions maximize the security afforded to the cryptographic keys used to access privileged accounts.

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**

STRATEGIC TECHNOLOGY PARTNER PROGRAM

To find out more about Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

Entrust is a trademark, registered trademark, and/or service mark of Entrust Corporation in the United States and/or other countries. ©2020 Entrust Corporation. All rights reserved. October 2020 • PLB9576

ENTRUST

Contact us:
HSMinfo@entrust.com