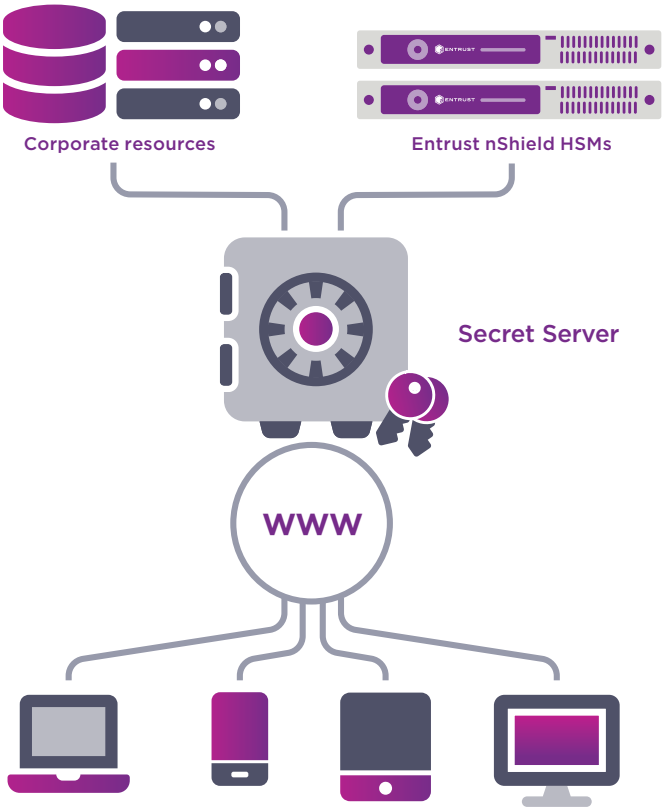
Entrust and Delinea Bolster Security of Privileged Access Management

An integrated solution providing layers of protection

HIGHLIGHTS

- Secure credentials for service, application, root, and administrator accounts across your organization on-premises or in the cloud
- Quickly identify, secure, manage, and implement privileged account controls with turnkey implementation and out-of-the-box auditing and reporting tools
- Manage multiple databases, software applications, hypervisors, network devices, and security tools, even in large-scale, distributed environments
- Protect cryptographic keys used to access privileged account credentials within a tamper-resistant FIPS 140-2 or FIPS 140-3 and Common Criteria certified Entrust nShield® hardware security module (HSM)
- Facilitate auditing and compliance with data security regulations



Entrust nShield HSMs provide an additional layer of protection by controlling the encryption key used by the Delinea Secret Server to secure access credentials.

Entrust and Delinea Integrated Solution

The Problem

Privileged user accounts are a top target of cybercriminals seeking access to enterprise IT systems and sensitive data.

Attacks on IT infrastructures target privileged user account credentials. These credentials are highly attractive to attackers because a compromise can open an easy path to an organization's most sensitive information. Bad actors use stolen credentials to move laterally, gaining access to more accounts with more privileges until they get the most sensitive data. The stolen credentials allow them to go undetected, sometimes for extended periods, because the attacker appears to be a trusted user.

The Challenge

Privileged account credentials need to be encrypted and further secured by high assurance protection.

Organizations establish privileged accounts for highly trusted individuals. These accounts provide unique access and privileges based on the roles and responsibilities of the trusted individuals. 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.

Because cyberattacks frequently target privileged accounts, organizations require full visibility and 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. Encrypting privileged account credentials protects them from unauthorized access. Securing the underpinning cryptographic keys used to encrypt these credentials is critical to protect an organization from attacks.

The Solution

Delinea's Secret Server privileged access management vault adds additional layers of security by integrating Entrust nShield HSMs to secure underpinning encryption keys.

Delinea's Secret Server simplifies the ability to discover, secure, manage, delegate, monitor, and audit privileged accounts across the organization. The solution gives security and IT teams the agility to secure and manage all types of privileges, protecting administrator, service, application, and root accounts from cyberattacks. Secret Server enables rapid deployment and gives enterprises direct control to customize as they grow. Organizations can strengthen their IT security, protect their data within global governance requirements, and scale across on-premises and cloud systems as their requirements change.

To achieve the highest assurance protection, Delinea's Secret Server integrates with Entrust nShield HSMs to protect the root encryption keys. nShield HSMs offer FIPS 140-2 Level 3, FIPS 140-3 Level 3, and Common Criteria EAL4+ protection for the keys that protect privileged account credentials. The combined solution provides an added layer of security that protects privileged credentials and the access they unlock for authorized privileged users.

Entrust and Delinea Integrated Solution

A Closer Look

Why use nShield HSMs with Delinea's Secret Server?

Entrust nShield HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. They are specifically designed to safeguard and manage cryptographic keys and processes within a certified hardware environment to establish a root of trust.

Critical keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attacks that can compromise confidential information. Entrust nShield HSMs, offered as an appliance deployed at an on-premises data center or leased through an as-a-service subscription, provide enhanced key generation, signing, and encryption to protect sensitive data and transactions. Using HSMs as part of an encryption and/or key management strategy is considered a best practice among cybersecurity professionals.

Integration of Entrust nShield HSMs with Delinea's Secret Server:

- Secures keys within carefully designed cryptographic boundaries that use robust access control mechanisms, so keys are only used for their authorized purpose
- Ensures availability by using sophisticated key management, storage, and redundancy features to guarantee keys are always accessible when needed
- Delivers high performance to support increasingly demanding transaction rates
- Complies with regulatory requirements for public sector, financial services, and enterprises

Entrust nShield HSMs

Entrust nShield HSMs are among the highest-performing, most secure, and easiest-to-integrate HSMs available. They help facilitate regulatory compliance and deliver 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. For more information visit **entrust.com/HSM**.

About Delinea

Delinea is a leading provider of Privileged Access Management (PAM) solutions for the modern, hybrid enterprise. The Delinea Platform seamlessly extends PAM by providing authorization for all identities, granting access to an organization's most critical hybrid cloud infrastructure and sensitive data to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. The company's customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. Learn more at **delinea.com.**

For more information

888.690.2424
+1 952 933 1223
sales@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust is an innovative leader in identity-centric security solutions, providing an integrated platform of scalable, AI-enabled security offerings. We enable organizations to safeguard their operations, evolve without compromise, and protect their interactions in an interconnected world — so they can transform their businesses with confidence. Entrust supports customers in 150+ countries and works with a global partner network. We are trusted by the world's most trusted organizations.

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