

SOLUTION BROCHURE

Secure Privileged Credentials. Control the Keys That Protect Them.

Delinea privileged access security with hardware-rooted cryptographic protection from Entrust nShield HSMs



Delinea



ENTRUST
SECURING A WORLD IN MOTION



Privileged credentials can unlock an organization's most sensitive systems, applications, and data. Delinea finds AI agents, humans and machines with privileged access, ranks the risk and authorizes what each can do, while Entrust nShield® hardware security modules protect the cryptographic keys underpinning that security.

Together, Entrust and Delinea help organizations:

- **Reduce the risk of privileged credential compromise** by protecting critical cryptographic keys within tamper-resistant, certified hardware
- **Retain control of key material** across on-premises, cloud, and hybrid privileged access management deployments
- **Support sovereignty and compliance objectives** with controlled, accountable, and auditable cryptographic operations
- **Adopt the deployment model that fits their strategy** without giving up hardware-backed protection for their cryptographic root of trust

Layered protection for privileged access

Delinea controls what AI agents, humans and machines can do and for how long, extending privileged access management from the point of access to the moment of action. Entrust strengthens the cryptographic foundation protecting the credentials behind that access.

Delinea Secret Server and the cloud-native Delinea Platform integrate with Entrust nShield HSMs to provide hardware-rooted protection for the encryption keys securing privileged credentials.

The combined solution supports Secret Server On-Premises, Secret Server Cloud, the Delinea Platform, and hybrid deployments that combine the cloud-based Delinea Platform with an on-premises Secret Server vault. This gives organizations flexibility to align privileged access security with their infrastructure, cloud, sovereignty, and regulatory requirements.

The risk does not stop at the credential vault

Privileged accounts provide elevated access to critical systems, applications, and data. This makes privileged credentials highly valuable to attackers. If compromised, these credentials can allow an attacker to appear to be a trusted user, move laterally through the organization, and gain access to additional systems and information.

Privileged access management helps organizations discover, secure, control, and audit these credentials. But encryption is only as strong as the protection applied to its cryptographic keys. If the keys securing the credential vault are exposed or insufficiently controlled, the protection around the credentials may also be undermined.

The challenge is becoming more complex as organizations manage growing numbers of human, machine, and AI identities across on-premises, SaaS, and public-cloud environments. Security teams must consider not only who can use privileged access, but also:

- Where the keys protecting privileged credentials reside
- Who controls and administers those keys
- How cryptographic operations are authorized and audited
- Whether key protection supports sovereignty, regulatory, and separation-of-duties requirements

One Solution for Privileged Access and the Keys That Protect It

Entrust and Delinea provide complementary layers of protection.

Delinea secures identities from the point of access to the moment of action

Delinea extends the privilege access controls you already invested in to the moment of action. We continuously discover AI agents, humans and machines, measure actual behavior against entitlements and enforce just-in-time authorization when they act, for a domain admin, a vendor, a service account or an AI agent, without getting in the way of legitimate work.

Entrust protects the cryptographic foundation

Entrust nShield HSMs protect critical cryptographic keys and operations within a tamper-resistant hardware boundary. Strong access controls govern how keys are administered and used.

Together, these capabilities help reduce the risk that compromising a software environment, administrator account, or cloud service also exposes the keys protecting the privileged credential vault.



Control privileged access with Delinea

Delinea secures privileged access for AI agents, humans and machines across on-premise, hybrid and multi-cloud environments. At Delinea's core is the enterprise-grade vault, Secret Server. Delinea continuously discovers, secures, manages, monitors, and audits privileged accounts, including administrator, service, application, and root accounts.

The Delinea Platform extends privileged access management using just-in-time authorization to reduce standing privilege across hybrid, multi-cloud and short lived infrastructure, without adding friction for legitimate users.

Delinea provides visibility across every identity type, scores the risk each one carries, and preserves the context behind access decisions, making them auditable and defensible. It supports both static and ephemeral access, letting teams apply Zero Standing Privilege where risk demands it without replacing existing infrastructure.

Protect critical keys with Entrust nShield HSMs

Entrust nShield HSMs provide a hardened environment for cryptographic processing, key protection, and key management. Critical key material and sensitive cryptographic operations are protected within certified, tamper-resistant hardware.

For Secret Server On-Premises, nShield HSMs integrate directly with the vault to protect the Master Encryption Key. This key protects the Secret Encryption Keys that secure stored credentials.

For Secret Server Cloud and the Delinea Platform, AWS Key Management Service External Key Store provides an integration path to customer-controlled Entrust nShield HSMs. Relevant cryptographic operations depend on external key material protected within the customer-controlled nShield security boundary.

A hybrid deployment allows organizations to use the Delinea Platform as a cloud control plane while retaining the Secret Server vault and its protected Master Encryption Key within their own environment.



Customer-Controlled Key Protection Across Deployment Models

Organizations can apply hardware-rooted key protection while selecting the Delinea deployment model that best fits their infrastructure, cloud, and sovereignty requirements.

Delinea Deployment	How nShield Protects It	Customer Value
Secret Server On-Premises	Direct integration protects the Master Encryption Key within an Entrust nShield HSM.	Retain the credential vault and its cryptographic root of trust within the customer environment.
Secret Server Cloud	AWS KMS External Key Store connects cloud key operations to customer-controlled Entrust nShield HSMs.	Combine a SaaS PAM deployment with external control of critical cryptographic key material.
Delinea Platform	AWS KMS External Key Store provides the integration path to customer-controlled Entrust nShield HSMs.	Add hardware-rooted key control to a cloud-native identity security model.
Hybrid: Delinea Platform With Secret Server On-Premises	The cloud control plane uses an on-premises vault whose Master Encryption Key is protected directly by an Entrust nShield HSM.	Support requirements such as data sovereignty, network segmentation, and local control of the credential vault.

For cloud deployments, AWS KMS External Key Store externalizes relevant cryptographic operations to customer-controlled infrastructure backed by Entrust nShield HSMs. For on-premises and hybrid deployments, nShield HSMs directly protect the Secret Server Master Encryption Key.

In each model, the combined solution strengthens control of the cryptographic keys underpinning privileged credential security.



Why Add Hardware-Rooted Protection?

Strengthen the root of trust

Encryption protects privileged credentials, but the keys used for that encryption are themselves critical security assets.

Entrust nShield HSMs isolate critical key material and sensitive cryptographic operations within a hardened, tamper-resistant hardware environment. This provides a strong cryptographic foundation for protecting privileged credentials and the access they unlock.

Separate privileged access from key control

Customer-controlled HSMs help separate administration of the privileged access environment from control of the cryptographic keys protecting it.

This avoids relying solely on the application, credential vault, or cloud service to control both encrypted information and its associated key material. It also supports stronger separation of duties between privileged access administrators and cryptographic key custodians.

Maintain control through cloud adoption

Organizations should not have to choose between the benefits of cloud-based privileged access management and greater control of critical cryptographic keys.

Through AWS KMS External Key Store, customers using the Delinea Platform or Secret Server Cloud can protect external key material inside customer-controlled Entrust nShield HSMs. Organizations with additional sovereignty, segmentation, or regulatory requirements can use the Delinea Platform with an on-premises Secret Server vault protected directly by nShield HSMs.

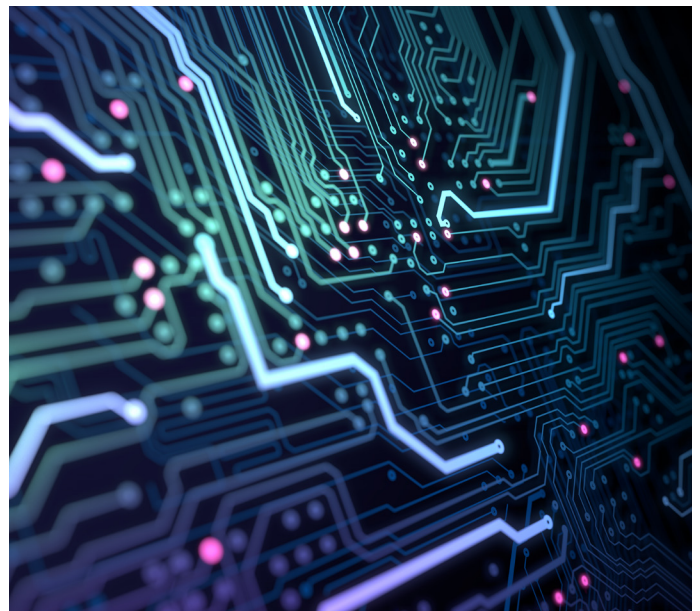
Support assurance and compliance objectives

Entrust nShield HSMs are available with FIPS 140-2 Level 3, FIPS 140-3 Level 3, and Common Criteria EAL4+ certification.

Their hardware-based security controls help organizations demonstrate how sensitive cryptographic keys are protected, administered, and governed. This can support broader security, audit, sovereignty, and regulatory compliance objectives.

Deploy without creating a security dead end

Entrust nShield HSMs are available as physical appliances or through nShield as a Service. They support on-premises, cloud, and hybrid deployment strategies, enabling organizations to strengthen key protection while adapting their privileged access architecture as requirements evolve.



Combined Solution Benefits

With Entrust and Delinea, organizations can:

- Protect the cryptographic keys securing privileged credentials within certified, tamper-resistant hardware
- Maintain control of critical key material across on-premises, cloud, and hybrid environments
- Separate privileged access administration from cryptographic key control
- Support sovereignty, audit, and compliance objectives with controlled and accountable key operations
- Apply consistent hardware-rooted protection across different Delinea deployment models
- Scale privileged access and key protection as infrastructure and identity requirements evolve



Entrust nShield HSMs

Entrust nShield HSMs provide a hardened, tamper-resistant environment for generating, protecting, and using cryptographic keys.

Available as physical appliances or through nShield as a Service, nShield HSMs support on-premises, cloud, and hybrid deployments. Their Security World key management architecture provides granular control over access to and use of keys while supporting resilient and scalable HSM deployments.

Entrust nShield HSMs are available with FIPS 140-2 Level 3, FIPS 140-3 Level 3, and Common Criteria EAL4+ certification, helping organizations protect critical cryptographic assets and support regulatory compliance requirements.

For more information, visit entrust.com/HSM.

About Delinea

Delinea is the identity security platform that continuously controls what AI agents, humans and machines can do and for how long. It extends privileged access management from the point of access to the moment of action., using just-in-time authorization to reduce standing privilege across on-premises, multi-cloud and short-lived infrastructure, without adding friction for legitimate users.

Delinea provides visibility across every identity type, scores the risk each one carries, and preserves the context behind decisions, making them auditable and defensible. It supports both static and ephemeral access, letting teams apply Zero Standing Privilege where risk demands it without replacing existing infrastructure.

Learn more at delinea.com.



Strengthen the Cryptographic Foundation of Privileged Access

Learn how Delinea and Entrust nShield HSMs can help your organization secure privileged credentials, retain control of critical cryptographic keys, and support on-premises, cloud, and hybrid deployment strategies.

[Contact Entrust to discuss your privileged access key protection requirements](#)

SECRET SERVER ON-PREMISES	SECRET SERVER ON DELINEA PLATFORM	HYBRID DEPLOYMENT
Delinea Secret Server On-Premises → Entrust nShield HSMs Direct integration protects the Master Encryption Key.	Delinea Platform / Secret Server Cloud → AWS KMS → External Key Store → Entrust nShield HSMs Cloud deployment with critical external key material protected within customer-controlled HSMs.	Delinea Platform identity security platform → Secret Server On-Premises vault → Entrust nShield HSMs Cloud-based identity security with an on-premises credential vault and hardware-rooted key protection.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com.