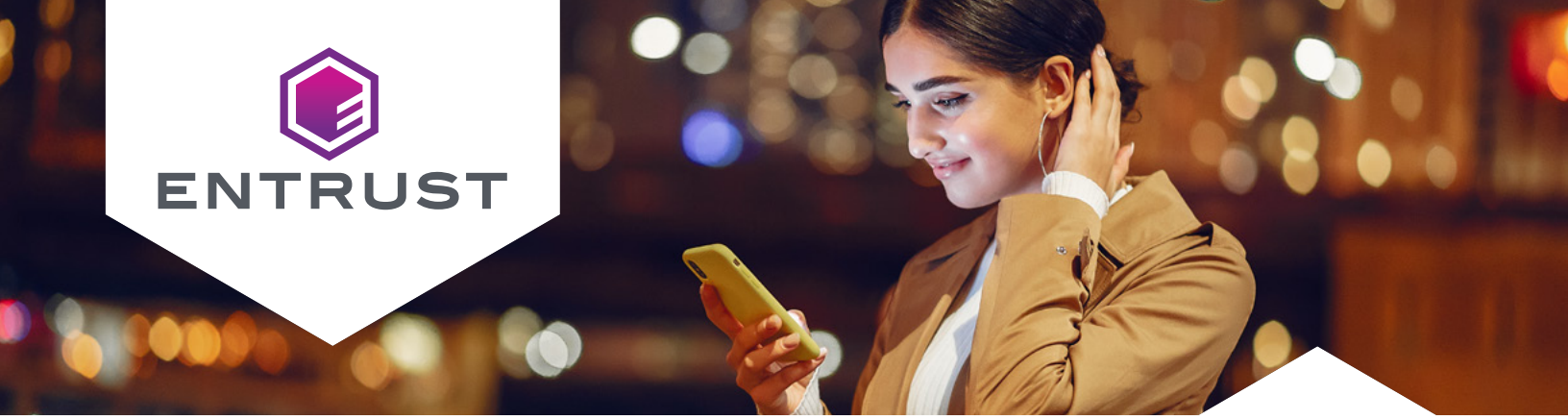


CyberArk Conjur and Entrust nShield HSMs Secure Enterprise Secrets

Integrated solution delivers comprehensive secrets management secured by a certified root of trust.

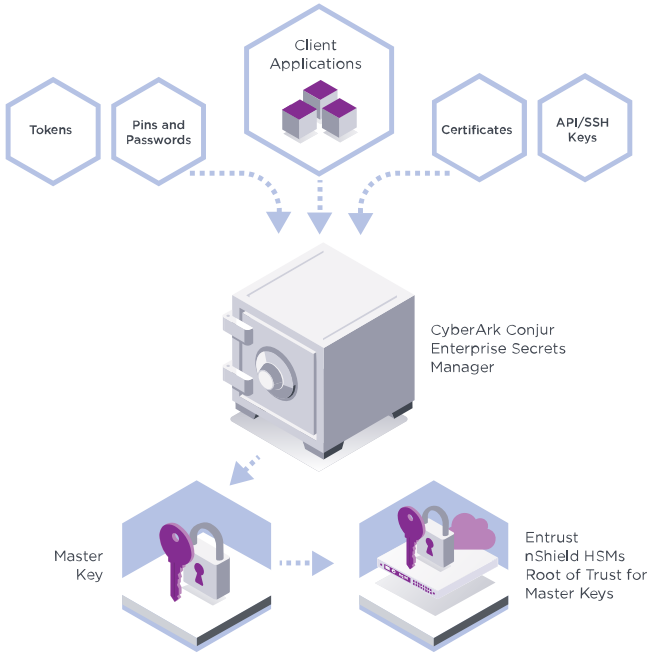
HIGHLIGHTS

- Provide complete management for secrets and privileged credentials including PINs, passwords, tokens, and API and SSH keys
- Support organizational computing needs across myriad of environments including containerized applications and DevOps
- Leverage native cloud deployments with continuous integration and continuous delivery (CI/CD) tools such as Ansible, Jenkins, and Kubernetes container orchestration software
- Protect against risks created by centralizing and aggregating secrets and privileged credentials
- Facilitate auditing and regulatory compliance with a FIPS 140-2 Level 3 and Common Criteria EAL4+ root of trust

The Problem:

Organizational secrets are attractive targets of cybercriminals

Applications use different types of credentials including PINs, passwords, tokens, certificates, and keys to control access and secure sensitive resources. Because these secrets hold the keys to organizations' critical processes and data, they can be the target of attackers. To protect from this threat, not only must the secrets used by the applications be secured, but also the credentials used by the tools themselves, and by the people managing them.



Entrust nShield HSMs, deployed on-premises or as a service, integrate with CyberArk Conjur secrets management solution to protect and manage the master cryptographic key used to secure enterprise secrets.

Learn more about our HSMs at entrust.com/HSM

Entrust and CyberArk Integrated Solution

The Challenge:

Securing workloads across multiple environments without impacting development flow

As enterprises adopt DevOps and automate other IT infrastructures leveraging the cloud to achieve CI/CD, securing dynamic workloads is critical. Configuration management tools use secrets to interact with other resources, and therefore access must be managed for DevOps administrators and developers. Doing this in a way that does not slow down development processes is necessary in order to meet the needs of both security teams and developers.

The Solution:

CyberArk Conjur and Entrust nShield® Hardware Security Modules (HSMs) provide high assurance secrets protection and management.

CyberArk Conjur Enterprise is a purpose-built secrets management solution engineered to address the security needs of cloud-native, containerized applications, and of the DevOps environments under which they are developed. Conjur Enterprise safeguards, rotates, and manages device and application secrets and other credentials throughout their lifecycle, ensuring these important security processes are transparent to developers working in fast-paced CI/CD environments.

As containerization has become the new standard for software development, Conjur Enterprise delivers scalable support and seamless integration with widely used DevOps, container, and Kubernetes platforms. The solution enables organizations to secure applications and automated processes by integrating secrets management best practices into the developer workflow.

Conjur Enterprise integrates with Entrust nShield Connect HSMs and nShield as a Service cloud-based HSMs to enhance the security of the secrets management process. The integration establishes a robust root of trust protecting cryptographic master keys encrypting the secrets server. The combined solution provides centralized, controlled access, based on trusted identities and policy enforcement. In addition, the integrated solution:

- Protects privileged credentials within a secure, encrypted environment
- Limits access to specific systems based on user role
- Can grant access for a specified time period and automatically revoke it upon expiration
- Monitors and audits each privileged activity

Entrust nShield HSMs offer FIPS 140-2 Level 3 and Common Criteria EAL4+ protection for the keys that protect privileged account credentials. This provides an added layer of security protecting both access credentials and the doors they open to privileged accounts and the sensitive data they hold.

Entrust and CyberArk Integrated Solution

A Closer Look:

Why use Entrust nShield HSMs with CyberArk Conjur Enterprise?

Entrust nShield HSMs 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. 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 enterprise encryption and/or key management strategy is considered a best practice among cybersecurity professionals.

nShield HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. Integration of nShield HSMs with Conjur Enterprise:

- Secures cryptographic keys used to access the secrets manager within a tamper-resistant FIPS 140-2 and Common Criteria-certified HSM
- Protects and manages large numbers of enterprise secrets within the protected hardware boundary
- Facilitates auditing and compliance with data security regulations
- Improves accountability and control over enterprise secrets

About Entrust nShield 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.

About CyberArk

CyberArk delivers privileged access security and secrets management, critical layers of IT that protect data, infrastructure, and assets across the enterprise, in the cloud, and throughout the DevOps pipeline. CyberArk offers a complete solution to reduce risk created by privileged credentials and secrets. A global company, CyberArk is headquartered in Petah Tikva, Israel, with U.S. headquarters located in Newton, Massachusetts. The company also has offices throughout the Americas, EMEA, Asia Pacific, and Japan.

For more information visit **cyberark.com.**

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

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

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