nCipher AN ENTRUST DATACARD COMPANY

www.ncipher.com

nCipher HSMs wrap and protect master keys used by HashiCorp centralized secrets management solution

- Enable secure generation, encryption, and decryption of secret assets
- Support organizations' computing needs across myriad of environments
- Mitigate risks created by centralizing/aggregating secrets management
- Address the regulated market needs for reduced risks and compliance
- Provide a FIPS 140-2 Level 3 and Common Criteria EAL4+ root of trust

HashiCorp

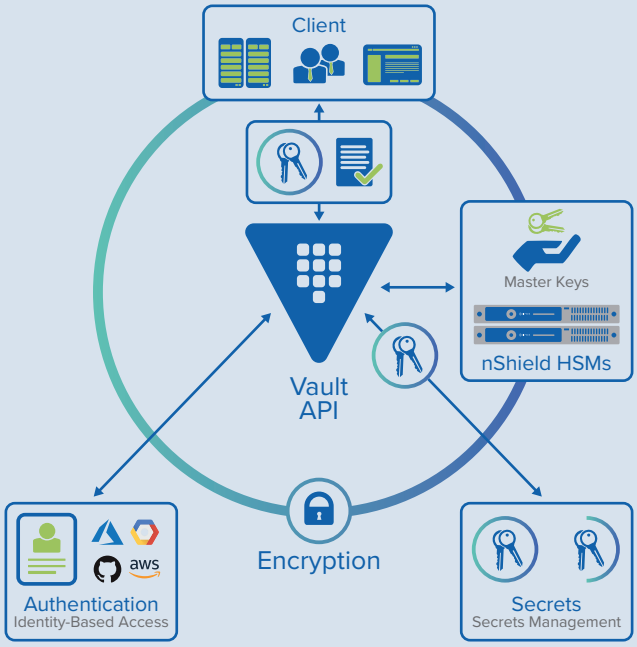
nCipher and HashiCorp deliver highly secure centralized enterprise secrets management

THE PROBLEM: SECRETS MANAGEMENT LACKS CONSISTENT SECURITY POLICIES

As more enterprise applications offer their own secure repositories to store secret assets, organizations are uncovering silos, each holding different secrets with varying lifecycle management and protection policies. Unless centrally managed, secrets such as tokens, passwords, certificates, and API keys, can exist in various locations. Not knowing where these are maintained, and applying inconsistent management policies, creates risks and audit challenges. Centralizing secrets management across the organization enables uniform policy enforcement and facilitates auditing and regulatory compliance, but requires high security.

THE CHALLENGE: MANAGING RISKS ACROSS A CENTRALIZED SECRETS MANAGEMENT ARCHITECTURE

Centralizing secrets management across the organization enables consistent security policy enforcement and eliminates secrets sprawl. However, aggregation of secrets in one place requires high security. Establishing a root of trust that protects the centralized secrets management repository is critical to enable enterprise access to computing resources across a variety of on-premises and multi-cloud environments.



nShield hardware security modules (HSMs) secure the key used to unseal HashiCorp Vault by wrapping the Vault master key that encrypts the organization's secrets, credentials, and other confidential assets.

nCipher and HashiCorp deliver highly secure centralized secrets management

THE SOLUTION: HASHICORP VAULT CENTRALIZED SECRETS MANAGEMENT WITH NCIPHER HIGH SECURITY HSM ROOT OF TRUST

HashiCorp Vault brings organizational secrets into a single centralized secure repository, enabling consistent lifecycle management and policy compliance. The solution ensures organizations can protect their secrets while enabling applications to access data. By centrally storing, accessing, and distributing dynamic secrets, HashiCorp Vault keeps applications and the data they process secure, while ensuring that a consistent security policy can be easily audited for compliance.

To mitigate potential risks created by aggregating secrets under a centralized management model, HashiCorp Vault integrates with nCipher nShield Connect on-premises and nShield as a Service (nSaaS) cloud-based HSMs to establish a robust root of trust protecting the Vault master keys. The combined solution eliminates secrets sprawl with centralized controlled access, based on trusted identities and policy enforcement.

WHY USE NCIPHER NSHIELD HSMs WITH HASHICORP VAULT?

Encryption keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attack, which can lead to compromise of critical keys. HSMs are the only proven and auditable way to secure valuable cryptographic material. nCipher nShield HSMs integrate with HashiCorp Vault to provide comprehensive logical and physical protection of master keys used to unseal the Vault content. The combination delivers an auditable method for enforcing security policies and facilitate regulatory compliance.

nCipher nShield Connect and nSaaS enable HashiCorp customers to:

- Secure the Vault master key within a carefully designed cryptographic boundary that uses robust access control mechanisms, so the key is only used for its authorized purpose
- Ensure master key availability by using sophisticated management, storage, and redundancy features to guarantee it is always accessible when needed by HashiCorp Vault
- Deliver superior performance to support demanding multi-cloud applications

nCipher nShield Connect and nSaaS provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. With nCipher HSMs, customers can:

- Provide a tightly controlled tamper resistant environment for safekeeping and managing cryptographic keys
- Enforce key use policies, separating security functions from administrative tasks
- Interface with applications using industry-standard APIs (PKCS#11, OpenSSL, JCE, CAPI, and CNG)

NCIPHER

nCipher, an Entrust Datacard company, is a leader in the general purpose HSM market, empowering world-leading organizations by delivering trust, integrity, and control to their business critical information and applications. By using the same proven technology customers depend on today to protect against threats and meet compliance, nCipher underpins the trust of tomorrow.

HASHICORP

HashiCorp is a leader in multi-cloud infrastructure automation software. The company's software suite enables organizations to adopt consistent workflows to provision, secure, connect, and run any infrastructure for any application. HashiCorp open source tools are broadly adopted by Global 2000 companies. Enterprise versions of the products enhance the open source tools with features that promote collaboration, operations, governance, and multi-data center functionality.

For more information visit www.ncipher.com and www.hashicorp.com

Search: nCipherSecurity

nCipher AN ENTRUST DATACARD COMPANY