nCIPHER
AN ENTRUST DATACARD COMPANY

www.ncipher.com

Integrated solution provides secure, high-speed orchestration of machine identities using certified hardware security modules (HSMs)

- Automate lifecycle management of keys and certificates
- Protect identities of devices and applications securing critical data
- Enable trust in machines that are supporting critical business
- Apply consistent security policies to put you in complete control
- Establish a FIPS 140-2 and Common Criteria EAL 4+ root of trust

VENAFI®

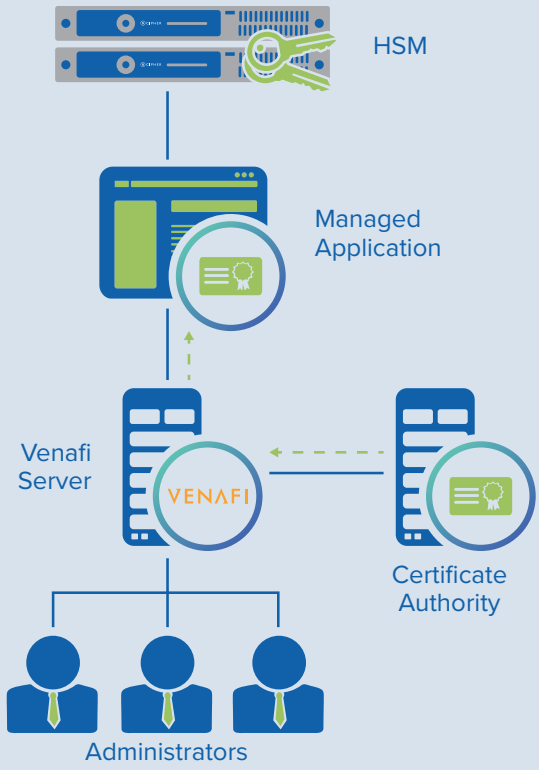
Venafi and nCipher deliver automated and secure cryptographic key orchestration

THE PROBLEM: IDENTITIES OF MACHINES THAT MANAGE CRITICAL ENTERPRISE SYSTEMS AND DATA ARE AT RISK

Organizations are increasingly dependent on machines, including devices and applications, to communicate and manage vital systems and process critical data. To discover and validate the identities of machines and protect the data they process, machine identities (digital certificates and encryption keys are used.) As increasing number of attacks target signing and encryption keys, the need for strong private keys for TLS certificates, SSH, and code signing throughout the enterprise becomes more acute. Keys stored in software are susceptible to file and memory scraping, as well as side-channel attacks, both exploit information gained from system operation.

THE CHALLENGE: ORCHESTRATING ROBUST HARDWARE-BASED CRYPTOGRAPHIC KEYS AT ENTERPRISE SCALE

Generating keys in an HSM addresses risks by producing strong FIPS-compliant signing and encryption keys with maximum entropy, using random number generation and secure hardware protection. While HSMs provide a way to secure machine identities, many organizations still opt to create custom scripts and use other manual processes to generate and provision keys, leaving them vulnerable to attack and introducing new risks to the enterprise.



The Venafi Trust Protection Platform delivers key and certificate orchestration with the key pairs securely maintained by the nCipher nShield HSM, deployed on-premises or as a service.

Venafi and nCipher deliver automated and secure cryptographic key orchestration

THE SOLUTION: VENAFI MACHINE IDENTITY PROTECTION WITH NCIPHER NSHIELD HSMs

Venafi and nCipher have joined forces to help address the machine identity protection challenge faced by today's enterprise customers. Venafi delivers an out-of-the-box solution that integrates with industry-leading nCipher nShield HSMs, on premises or as a service, to leverage strong hardware-based signing and encryption keys throughout the enterprise. Together Venafi and nCipher allow organizations to generate, store, and use keys securely – without private key material ever having to leave the HSM. These capabilities make it possible for enterprises to ensure the consistent use of the strongest cryptographic keys possible.

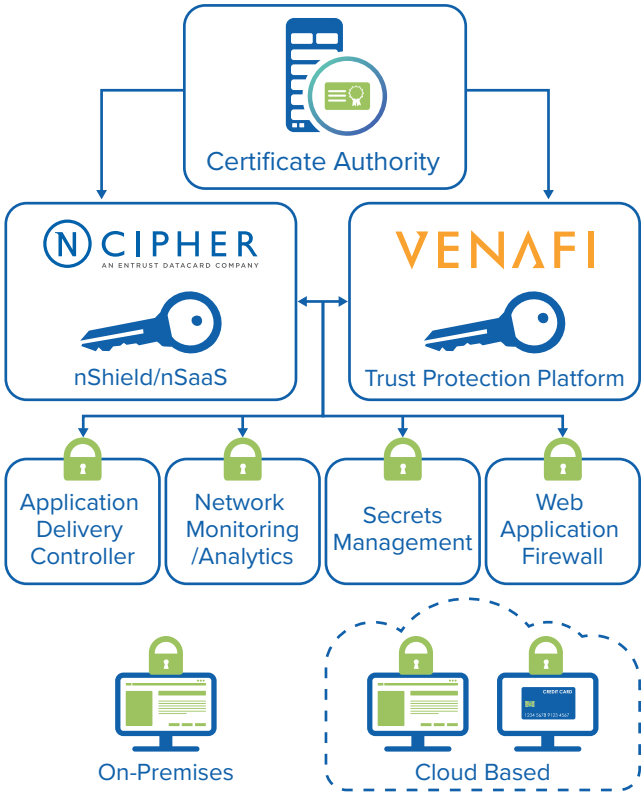
WHY USE NCIPHER NSHIELD HSMs WITH VENAFI?

Cryptographic keys underpin the security of enterprise IT systems. Keys handled outside the protected boundary of a certified HSM are significantly more vulnerable to attack, which can lead to compromises. HSMs are the only proven and auditable way to secure valuable cryptographic material. nShield Connect on-premises HSMs, and nShield as a service (nSaaS), secure the generation and storage of the private keys used by the Venafi Platform. nShield HSMs enforce key use policies, separating security functions from administrative tasks. Doing so provides the highest level of security and assurance against key compromise and theft, while delivering scalability, flexibility, and efficiency.

PROTECTING THE BIGGER ECOSYSTEM: MACHINE IDENTITIES ARE VULNERABLE AND UNDER ATTACK

Todays' authentication and encryption landscape includes a multitude of applications. Machine identities ensure trust across on-premises and cloud based deployments, from virtual private networks (VPNs), to application delivery controllers (ADCs), web application firewalls (WAFs), and performance monitoring and analytics software. A variety of attack vectors including downloadable code, weak or compromised keys and expired certificates protect organizational secrets and control access to systems, applications, and data. Not only are these vectors a growing target of exploitation, but adoption of cloud, containers, and DevOps models can make it even harder to protect these ecosystems.

Venafi Trust Protection Platform and nCipher nShield HSMs, deployed together with leading machine identity providers like CAs, and machine identity consumers like ADCs, WAFs, network monitoring and analytics software, and secrets management applications, can significantly enhance the orchestration and security of machine identities.



The Venafi Trust Protection Platform together with nCipher nShield HSMs orchestrates secure machine identities across today's distributed computing deployments.

NCIPHER - AN ENTRUST DATACARD COMPANY

nCipher 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 our customers depend on today to protect against threats and meet compliance, we underpin the trust of tomorrow. To learn more visit www.ncipher.com

VENAFI

Venafi is the cybersecurity market leader in machine identity protection, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access. To learn more, visit www.venafi.com

Search: nCipherSecurity

www.ncipher.com

nCipher An Entrust Datacard Company