nCIPHER
AN ENTRUST DATACARD COMPANY

www.ncipher.com

nCipher and ADC providers ensure the availability, security and performance of your critical applications

- Secures keys and certificates within cryptographic boundaries with robust access control mechanisms, so keys are only used for their authorized purpose
- Supports virtual and cloud-based environments
- Provides FIPS-certified, centralized protection of keys and certificates
- Meets the demand for high application performance
- Ensures availability by using sophisticated key management, storage, and redundancy to guarantee keys are always accessible when needed
- Facilitates compliance with regulatory requirements across industries

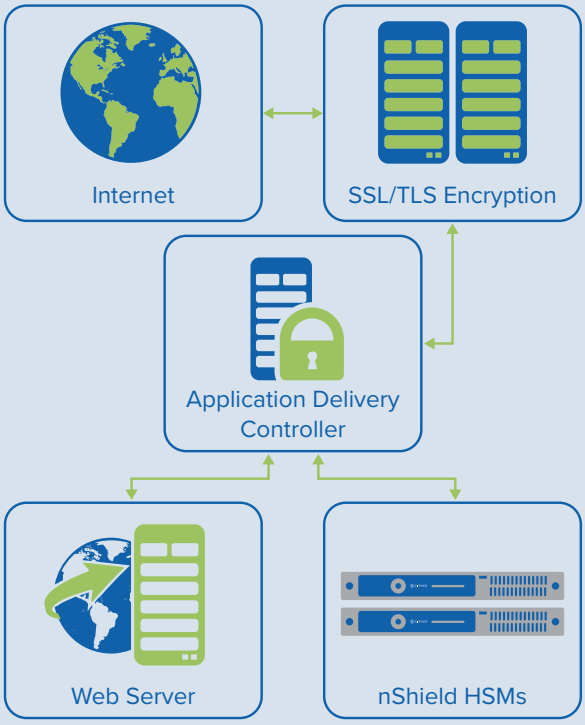
NFINITY
STRATEGIC TECHNOLOGY PARTNER PROGRAM

Enhanced security of application delivery controllers with nShield HSMs

THE CHALLENGE: ATTACKERS SEEK OPPORTUNITIES TO EXPLOIT WEB APPLICATIONS

The rapid rise of online transactions has resulted in similar growth of sensitive and confidential information exchanged online and in the cloud. And where there is valuable information, there are cybercriminals attempting to intercept and exploit it.

Transport Layer Security (TLS)/Secure Sockets Layer (SSL) connections encrypt information but are resource-intensive. They demand high server utilization to meet application performance and availability requirements. This results in higher costs. In addition, encrypting the data is not enough to truly secure it. A compromise of TLS/SSL encryption keys can lead to compromised sessions, potentially exposing the encrypted data flowing between end user devices and web servers. And the increased encrypted traffic over multiple channels and simultaneous connections creates a key management nightmare. Encryption keys must be protected and managed in a trusted manner for security and compliance with regulations.



nShield protects SSL/TLS encryption/decryption keys and certificates within its high security environment.

Enhanced security of application delivery controllers with nShield HSMs

THE SOLUTION: APPLICATION DELIVERY CONTROLLERS INTEGRATED WITH NSHIELD HSMs

Application delivery controllers (ADCs) are designed to optimize web application performance by providing load balancing and management of sensitive traffic. nCipher partners with ADC providers to deploy high-security TLS/SSL systems that enable customers to deliver secure connectivity while meeting operational demands.

nCipher network-based hardware security modules (HSMs) deliver both operational efficiency and certified security for encryption keys and operations. nCipher nShield Connect HSMs protect critical TLS/SSL encryption keys and certificates within a dedicated, hardened device. This ensures keys are never exposed to unauthorized entities.

THE NSHIELD DIFFERENCE

nShield HSMs protect encryption keys in a certified, tamper-resistant environment. Keys handled outside the cryptographic boundary of nShield HSMs are significantly more vulnerable to attacks, which can lead to disclosure of confidential information. HSMs are the only proven and auditable way to secure valuable cryptographic material. nShield HSMs:

- Protect keys and certificates within carefully designed cryptographic boundaries
- Use robust access control mechanisms so keys are only used for their authorized purpose
- Ensure availability by using sophisticated key management, storage and redundancy features to guarantee keys are always accessible when needed
- Deliver high performance to support increasingly demanding transaction rates
- Comply with regulatory requirements for financial services, retail and other industries

NFINITY PARTNERS

appviewX

CITRIX®

f5®

A10®

radware

LEARN MORE

To find out more how nCipher Security can deliver trust, integrity and control to your business critical information and applications, visit ncipher.com

Search: nCipherSecurity

nCIPHER
AN ENTRUST DATACARD COMPANY