nShield as a Service

- Uses hosted, managed HSMs for cloud deployments
- Maintain full control over key material regardless of where application workloads are running
- Extend cloud-based cryptography and key management across multiple clouds
- Support secure code execution for cloud-based workloads
- Simplify budgeting for business critical security
- Decrease time spent on maintenance and monitoring tasks

nShield as a Service

Easy, efficient access to cryptography as a service

nShield as a Service

Easy, efficient access to cryptography as a service

In today's fast moving enterprise IT environment, "cloud first" is a common strategic aim of many organizations. Gone are the days when companies automatically host their critical IT infrastructure on premises. With the shift to the cloud, organizations benefit from the scale, flexibility and resilience a cloud service provider can deliver while enjoying reduced maintenance burden and a more predictable monthly operational expense. This business shift results in tension when cloud applications rely on hardware security modules (HSMs), physical appliances that protect the cryptographic keys that act as the root of trust for an organization's encrypted data. Traditionally housed in on-premise data centers and managed by an on-site security team, HSMs help customers meet regulatory or certification requirements and are an important part of an organization's critical infrastructure. Given the increasing demands on enterprise security teams, finding skilled security professionals to administer HSMs is an ongoing challenge. nShield as a Service provides the same features and functionality as on-premises HSMs combined with the benefits of a cloud service deployment. This allows customers to fulfill their cloud first objectives and leave the management and maintenance of these appliances to the experts at nCipher.

CRYPTOGRAPHY AS A SERVICE

nShield as a Service is a subscription-based solution for generating, accessing and protecting cryptographic key material, separately from sensitive data, using dedicated FIPS 140-2-certified nShield Connect HSMs. This cloud-hosted model gives organizations the option to either supplement or replace HSMs in their data centers while retaining the same benefits as owning the appliances. nShield as a Service allows enterprises to budget for security more predictably, manage capacity based on demand, reduce their data center footprints and decrease the time spent on routine maintenance and monitoring tasks.

Subscribed customers interact with the cloud-based nShield HSMs in the same way that they would with appliances in their own dark data centers, but have no need to receive, install and maintain physical hardware. This often results in a shorter time between initial procurement and use of the HSM and, therefore, faster deployment of secured applications.

ALIGNS WITH YOUR SECURITY STRATEGY AND DEMANDS

nShield as a Service is well-suited to align with any security strategy, whether an organization is adopting a cloud-first approach for its cryptographic functions, selectively migrating specific services to the cloud, or enhancing HSM capacity to handle occasional workload spikes.

Because nShield as a Service benefits from the same unique Security World architecture as on-premises nShield deployments, customers can use a hybrid approach, mixing both nShield as a Service and on-premises HSMs. Security World is a scalable key management framework that spans the customer's nShield estate and provides a unified administrator and user experience and guaranteed interoperability across all devices, whether subscription-based or owned on-prem.[1] This allows customers to easily and efficiently scale their HSM operations with their specific environment, operational approaches and security needs.

Additionally, the unique CodeSafe secure execution capability gives customers on-demand access to expanded secure computing capacity. Only nShield as a Service allows customers to seamlessly migrate their secure code execution from an on-prem HSM to the cloud.

THE NSHIELD AS A SERVICE DIFFERENCE

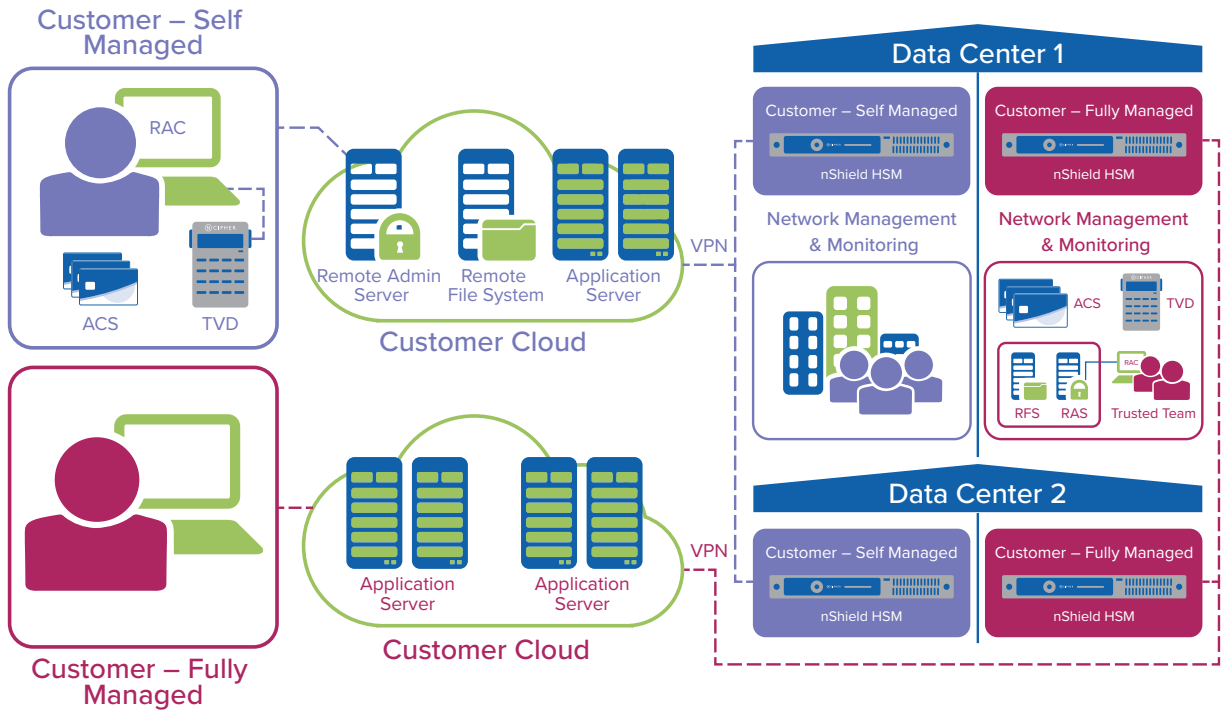nShield as a Service offers several key advantages over other options:

- Customers own their Security World resources and keys and may use these across their nShield environment, whether as-a-service or on-premises.
- Only nShield as a Service provides customers on-demand control to migrate and expand their secure code execution from an on-prem HSM to the Cloud.
- nShield as a Service delivers FIPS 140-2 Level 3 protection of keys, which is not available with some cloud key protection solutions.
- Customers can continue using the same business applications with their cloud-based nShield HSMs and have the option to access enhanced HSM capacity to handle occasional workload spikes.
- nShield as a Service can be used with multiple cloud service providers, in contrast to HSM services offered by individual providers who strive to lock customers into their cloud environments.
- nShield as a Service readily supports hybrid cloud deployments and offers easy key migration should data repatriation from a Cloud Service Provider to on prem be required.
- nShield as a Service offers customers a dedicated HSM service. Customers have full control of their cryptographic keys - dual control and full separation of duties.

NSHIELD AS A SERVICE DEPLOYMENT OPTIONS AND FEATURES

nShield as a Service is available as either a Self-managed or Fully-managed deployment, as detailed in diagram.

nShield as a Service deployment options

Customer – Self Managed

RAC

ACS   TVD

Customer Cloud

Remote Admin Server   Remote File System   Application Server

Customer – Fully Managed

Application Server   Application Server

Customer Cloud

VPN

VPN

Data Center 1

Customer – Self Managed
nShield HSM

Network Management & Monitoring

Customer – Fully Managed
nShield HSM

Network Management & Monitoring

ACS   TVD

RFS   RAS   Trusted Team   RAC

Data Center 2

Customer – Self Managed
nShield HSM

Customer – Fully Managed
nShield HSM

KEY ACS: Administrator Card Set   TVD: Trusted Verification Device   RAS: Remote Administration Server   RFS: Remote File System

nShield as a Service deployment features	SELF-MANAGED	FULLY-MANAGED
Customer has access to dedicated nShield Connect hardware hosted in secure data center	✓	✓
The nShield Remote Administration kit lets you securely connect to and interact with your cloud-based nShield HSM(s)	✓	✓
Maintenance & Support ○ Service monitoring ○ Pre-tested upgrades/patches applied during annual or emergency maintenance windows ○ 24/7 Support	✓	✓
Full Management of installation ○ Security Officer role fulfilled by trusted personnel • Security World creation • HSM enrollment • Signing ceremonies ○ ISO 27001 compliant policies & procedures ○ All operational staff BS7858 cleared		✓

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**

N CIPHER

nCIPHER
AN ENTRUST DATACARD COMPANY

About nCipher Security

nCipher Security, an Entrust Datacard company, is a leader in the general-purpose hardware security module (HSM) market, empowering world-leading organizations by delivering trust, integrity and control to their business critical information and applications. Today's fast-moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency – it also multiplies the security risks. Our cryptographic solutions secure emerging technologies such as cloud, IoT, blockchain, and digital payments and help meet new compliance mandates. We do this using our same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensure the integrity of your data and put you in complete control – today, tomorrow, always. www.ncipher.com

Search: nCipherSecurity

TRUST. INTEGRITY. CONTROL.