nShield as a Service Direct

Easy, efficient access to cryptography as a service

HIGHLIGHTS

- Use 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 with performance-based pricing to meet critical security needs
- Decrease time spent on maintenance and monitoring tasks
- Meet geo-fencing requirements for cloud data security and data sovereignty mandates via regional data centers
- Use Cloud Disaster Recovery (CDR) option to increase redundancy and reliability of on-premises deployments

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-premises 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 Direct 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 Entrust.

Learn more about nShield as a Service Direct at entrust.com

nShield as a Service Direct

Cryptography as a service

nShield as a Service Direct is a subscription-based solution for generating, accessing, and protecting cryptographic key material, separately from sensitive data. The solution uses dedicated FIPS 140-2 and eIDAS (EN 419 221-5) 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 Direct 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 Direct 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 Direct 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 Direct and on-premises HSMs. nShield 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 Direct allows customers to seamlessly migrate their secure code execution from an on-prem HSM to the cloud.

The nShield as a Service Direct difference

nShield as a Service Direct offers several key advantages over competing options:

- Ensures customers own their Security World resources and keys and may use these across their nShield environment, whether as-a-service or on-premises
- Provides customers on-demand control to migrate and expand their secure code execution from an on-prem HSM to the cloud
- Delivers FIPS 140-2 Level 3 and eIDAS (EN 419 221-5 protection profile) certified security of keys, which is not available with some cloud key protection solutions

[1] Note 1. See our nShield Security World white paper for additional details.

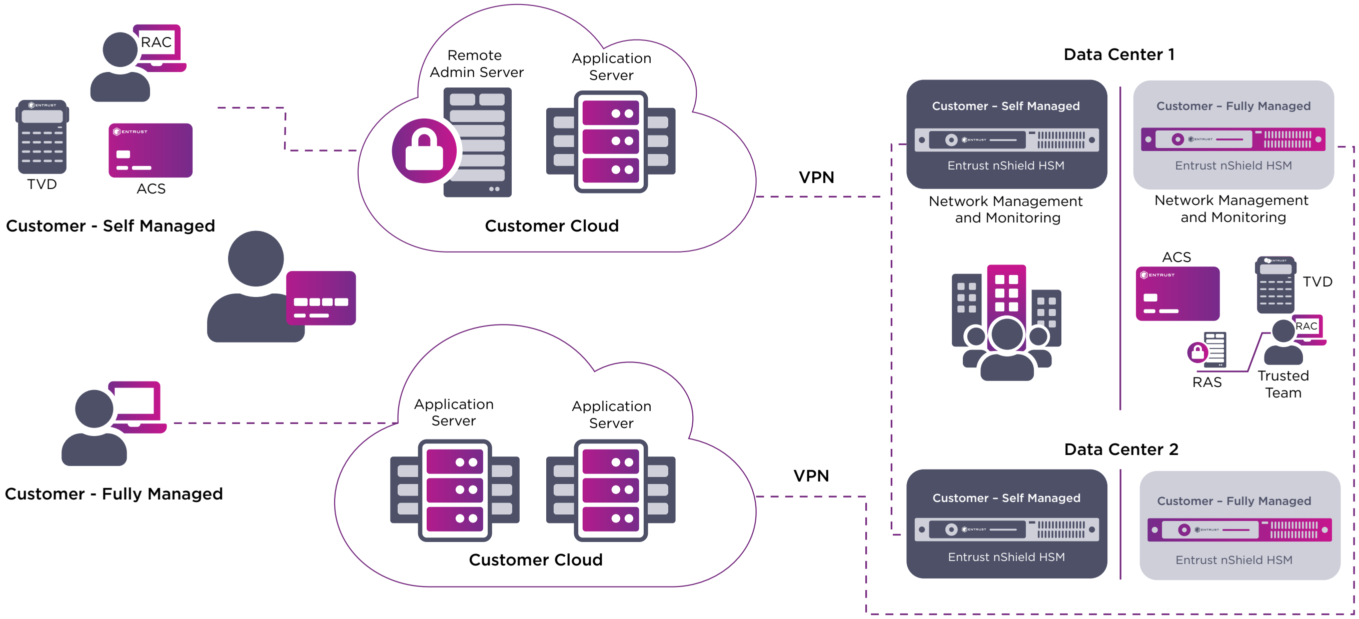
Learn more about nShield as a Service Direct at entrust.com

nShield as a Service Direct

- Enables customers to 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
- Deploy with multiple cloud service providers, in contrast to HSM services offered by individual providers that can lock customers into their own cloud environments. Supports hybrid cloud deployments and offers easy key migration should data repatriation from a cloud service provider to on-prem be required
- Offers customers a dedicated HSM service. Customers have full control of their cryptographic keys - full separation of duties ensures no individual can single-handedly change key use policies

nShield as a Service Direct deployment options and features

nShield as a Service Direct is available in a range of different feature/performance levels to enable customers to match capabilities to their operational, disaster recovery, and data sovereignty needs while choosing the optimum performance and price point. Self-managed or fully-managed deployment options are also available for greater flexibility
(see diagram).



Key ACS: Administrator Card Set TVD: Trusted Verification Device
RAS: Remote Administration Server RAC = Remote Admin Client

nShield as a Service Direct

nShield as a Service Options/Features

Features	Basic	Standard	Premium	Enterprise
Indicative performance (2K RSA signatures per second)	150 tps	450 tps	3,000 tps	16,000 tps
Number of HSM instances	x1 HSM	x2 HSMs	x2 HSMs	x2 HSMs
High Availability – multi-geographical locations		●	●	●
Committed SLA	99%	99.9%	99.9%	99.9%
Number of application integrations	3	10	100	1,000
Available as a fully managed option		●	●	●

A Cloud Disaster Recovery solution is also available, enabling organizations with in-house HSM estates to easily increase the redundancy and resiliency of their deployments, without having to add in-house equipment and personnel resources. Offered as a cost-effective, subscription-based solution, the Cloud Disaster Recovery solution has a 99% SLA, multi-geographical locations, and 10 application integrations.

nShield as a Service Direct 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 – nShield Security World creation – HSM enrollment – Signing ceremonies		✓
• ISO/IEC 27001: 2013 compliant policies & procedures (certificate of registration available on request) • Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) - Level 1 & CSA Trusted Cloud Provider	✓	✓
• All operational staff BS7858 cleared (non-U.S. data centers only)	✓	✓

Learn more about nShield as a Service Direct at entrust.com

nShield as a Service Direct

Technical Specifications

Connectivity

- IPsec tunnel w/ pre-shared keys
- Between customer Cloud IP space(s and dedicated, managed nShield HSM environment
- Transparent to client hosts
- Takes entire path out of control scope

Certified Hardware Solutions

nShield as a Service Direct is built with nShield Connect HSMs, which help our customers to demonstrate compliance while also giving them the assurance that their HSMs meet stringent industry standards.

nShield Features

nShield as a Service delivers the same features as on-premises nShield HSMs, including CodeSafe, Web Services Option Pack, Container Option Pack, and Database Option Pack.

Security Compliance:

- FIPS 140-2 Level 3

Safety and Environmental Standards Compliance:

- UL, CE, FCC, RCM, Canada ICES
- RoHS2, WEEE

Data Center Certifications

Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) - Level 1

Wide Support for APIs, Cryptographic Algorithms, and Platforms

Supported APIs

- PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI/CNG and Web Services

Supported Cryptographic Algorithms

- Asymmetric public key algorithms: RSA, Diffie-Hellman, ECMQV, DSA, KCDSA, ECDSA, ECDH, Edwards (X25519, Ed25519ph), Secp256k1
- Symmetric algorithms: AES, AES-GCM, ARIA, Camellia, CAST, RIPEMD160 HMAC, SEED, Triple DES
- Hash/message digest: SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160
- Full Suite B implementation with fully licensed ECC including Brainpool and custom curves

nShield HSMs offers support for the majority of these cryptographic algorithms as part of the standard feature set. For organizations wishing to use ECC or South Korean algorithms, optional activation licenses are needed.

Supported Platforms

Microsoft Windows and Linux operating systems including distributions from Red Hat, SUSE, and major cloud service providers running as virtual machines or in containers.

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