SOLUTION BROCHURE

Entrust nShield as a Service for OpenText Data Privacy and Protection (Voltage)

Simplified access to cryptography as a service

ENTRUST

SECURING A WORLD IN MOTION

The problem: controlling cryptographic keys as enterprises migrate to the cloud

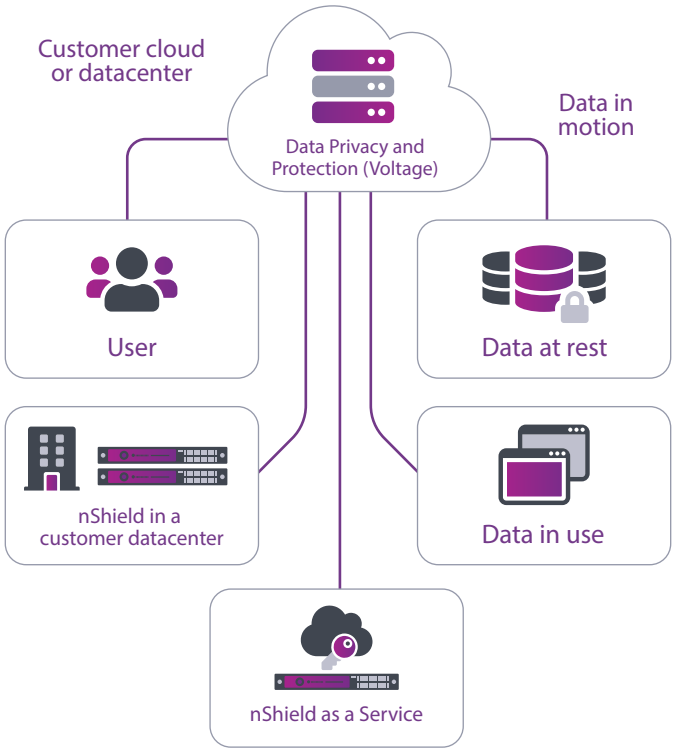
In today's fast-moving enterprise IT environment, "cloud first" is a common strategic aim. By shifting to the cloud, organizations benefit from its scale, flexibility, and resilience. Organizations seek reduced maintenance burdens and predictable monthly operational expense. Maintaining control of the keys that protect applications and the sensitive data processed is mandatory for security and compliance.

Highlights

- Keep full control of keys, regardless of where applications are running
- Provide high-performance nShield hardware security module (HSM) dedicated to each client
- Maintain FIPS certification within nShield HSM protected boundary
- Support multiple datacenters for security compliance and high availability
- Migrate existing nShield Security World seamlessly to nShield as a Service

The challenge: maintaining high assurance security in the cloud

Traditionally housed in on-premises datacenters and managed by on-site security teams, HSMs secure corporate data and form an important part of the organization's critical infrastructure. With the shift to the cloud, organizations seek to continue to use the enhanced security offered by HSMs. Efficient access to the services of a dedicated cloud-based HSM is necessary to ensure robust security and compliance as enterprises shift to this new business paradigm.



Data Privacy and Protection (Voltage) customers using Entrust nShield® HSMs on premises can easily migrate cryptographic services to nShield as a Service to protect encryption keys and establish a root of trust.

The solution: Data Privacy and Protection (Voltage) and Entrust nShield as a Service

Data Privacy and Protection (Voltage) addresses the confidentiality and privacy needs for data at rest, in motion, and in use by enterprise critical processes and analytic applications. The solution employs next-generation technologies such as Hyper Format Preserving Encryption (Hyper FPE), Hyper Secure Stateless Tokenization (Hyper SST), Format-Preserving Hash (FPH), and data masking to encrypt and de-identify data, while preserving original formats. Structured Data Manager (Voltage) maintains referential integrity for processes, applications, and services, while rendering data valueless to cyberattackers. The solution significantly reduces administrative staff burden and IT costs, allowing enterprises to focus on their business with data protection and privacy compliance enabled. Using Voltage Stateless Key Management, keys are derived on the fly, eliminating the need for a key database, storage, replication, and backup.

Data Privacy and Protection (Voltage) integrates nShield as a Service to enable customers to easily migrate cryptographic keys from existing nShield on-premises deployments. nShield as a Service is a subscription-based solution for generating, accessing, and protecting key material separately from sensitive data. Using dedicated and certified nShield HSMs, the cloud-hosted model gives organizations the option to either supplement or replace HSMs in their datacenters, while retaining the same benefits as owning the appliances.

Deployed globally in geographically dispersed datacenters, nShield as a Service integrates seamlessly with Stateless Key Management, providing trust assurance by hosting the master root key for the key derivation function in a hardened device.

Critical encryption, decryption, and key management processes run using CodeSafe, a unique capability that enables secure code execution inside the physical FIPS 140 Level 3 hardened tamper-resistant environment, away from possible malware or insider attacks. Only nShield as a Service allows customers to seamlessly migrate, on-demand, their secure code execution from an on-premises HSM to the cloud.

Why use nShield as a Service with Data Privacy and Protection (Voltage)

nShield as a Service allows enterprises to budget for security more predictably, manage capacity based on demand, reduce their datacenter footprints, and decrease the time spent on routine maintenance and monitoring. Subscribed customers interact with the cloud-based nShield HSMs in the same way that they would with appliances in their datacenters, but no longer need to receive, install, and maintain physical hardware. This results in faster deployment of secured applications. nShield as a Service offers customers a subscription to a dedicated HSM with full control of their cryptographic keys and full separation of duties for enhanced security.

The Self-Managed nShield as a Service option enables customers to use the remote administration capabilities just as if they were managing their own nShields in their datacenter, even when choosing one or more cloud services. Customers wishing to leave management and maintenance to the experts at Entrust can chose the Fully-Managed option, while still maintaining control over their keys. The managed service readily supports hybrid cloud deployments and offers easy key migration should data repatriation from a cloud service provider (CSP) to on-premises deployment be required.

Regardless of the option chosen, customers own their keys and may utilize these across their entire nShield environment using the nShield Security World key management architecture. nShield HSMs are certified to FIPS 140 Level 3, Common Criteria EAL4+, and eIDAS (EN 419 221-5 protection profile).

nShield Features	Cloud based	On-premises
Scalable, flexible, cost-effective deployment (replaces CapEx with OpEx)	●	
Decrease maintenance / monitoring time	●	
Free-up internal security resources	●	
Support multiple datacenters	●	
Maintain full control over critical keys	●	●
Transfer security officer role to trusted Entrust personnel	Fully-managed	
Access to high-performance nShield HSMs	●	●
Secure keys and execution code within FIPS 140-2 certified physical boundary	●	●
Ensure high availability, guaranteeing keys are always accessible when needed	●	●

nShield as a Service delivers extended benefits over nShield on-premises deployments. As Structured Data Manager (Voltage) customers increasingly migrate storage and workloads to cloud-based environments, they are looking to establish an HSM-based root of trust in the cloud that can maintain the highly available, highly performant data-centric solution they enjoy.

Entrust HSMs

Entrust nShield HSMs are among the highest-performing, most secure, and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial, and government organizations. Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

OpenText Structured Data Manager (Voltage)

OpenText is an information management software company that helps companies organize, store, and protect their data. We provide integrated solutions in analytics, business networks, content services, cybersecurity, DevOps, IT management, and more. Our software is designed to propel businesses forward with cloud, security, and AI tools that facilitate enterprise-level growth and innovation.

Structured Data Manager (Voltage) includes next-generation technologies: Hyper Format-Preserving Encryption (FPE), Hyper Secure Stateless Tokenization (SST), Format-Preserving Hash (FPH), Stateless Key Management, and data masking. Structured Data Manager (Voltage) "de-identifies" data, while maintaining referential integrity for data processes, applications, and services.

For more information, please visit us at www.opentext.com

Learn More

To find out more about Entrust nShield HSMs visit entrust.com/HSM. To learn more about Entrust's digital security solutions for identities, access, communications, and data, visit entrust.com

ABOUT ENTRUST

Entrust fights fraud and cyber threats with comprehensive identity-centric security that protects people, devices, and data. Our solutions help enterprises and governments safeguard critical systems from every angle, enabling secure onboarding and issuance, providing everyday identity protection, and empowering them with 360-degree visibility and orchestration across keys, secrets, and certificates so they can transact and grow with confidence. Building on our decades as a pioneer and innovator in establishing trust, Entrust has a global partner network and supports customers in over 150 countries. For more information, visit www.entrust.com.

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION