DATA SHEET

nShield Container Option Pack

Deploy containerized applications integrated with high assurance nShield hardware security modules.

HIGHLIGHTS

- Allows customers to build their containerized deployments in conjunction with an nShield HSM, for dynamic application scalability and maximum HSM utilization
- Provides a well-architected containerized deployment model with associated scripts for creating application container images
- Creates images from a variety of Linux platform base templates
- Integrates with FIPS and Common Criteria certified, tamper-resistant network attached nShield HSM delivering high assurance protection for business-critical cryptographic keys
- Compatible with nShield as a Service deployments

nShield Container Option Pack

Developers working with containerized applications may not be familiar with the complexities of how to integrate with high assurance hardware security modules (HSMs). When the time from staging to production is critical, you need a proven deployment model and scripts to help reduce the overall development cycle. nShield Container Option Pack (nCOP) makes it easy to build HSM support into these containerized solutions and provides a template deployment model that allows you to focus on the containerized application without having to worry about the HSM integration.

A member of the Entrust nShield family of software option packs designed to work seamlessly with our nShield network-attached HSMs, nCOP enables the straightforward and secure integration of HSMs via standard interfaces to containerized applications.

ENTRUST

SECURING A WORLD IN MOTION

High-level Architecture

The nCOP provides easy access to a flexible and scalable containerized architecture that interoperates with an existing nShield HSM and Security World environment.

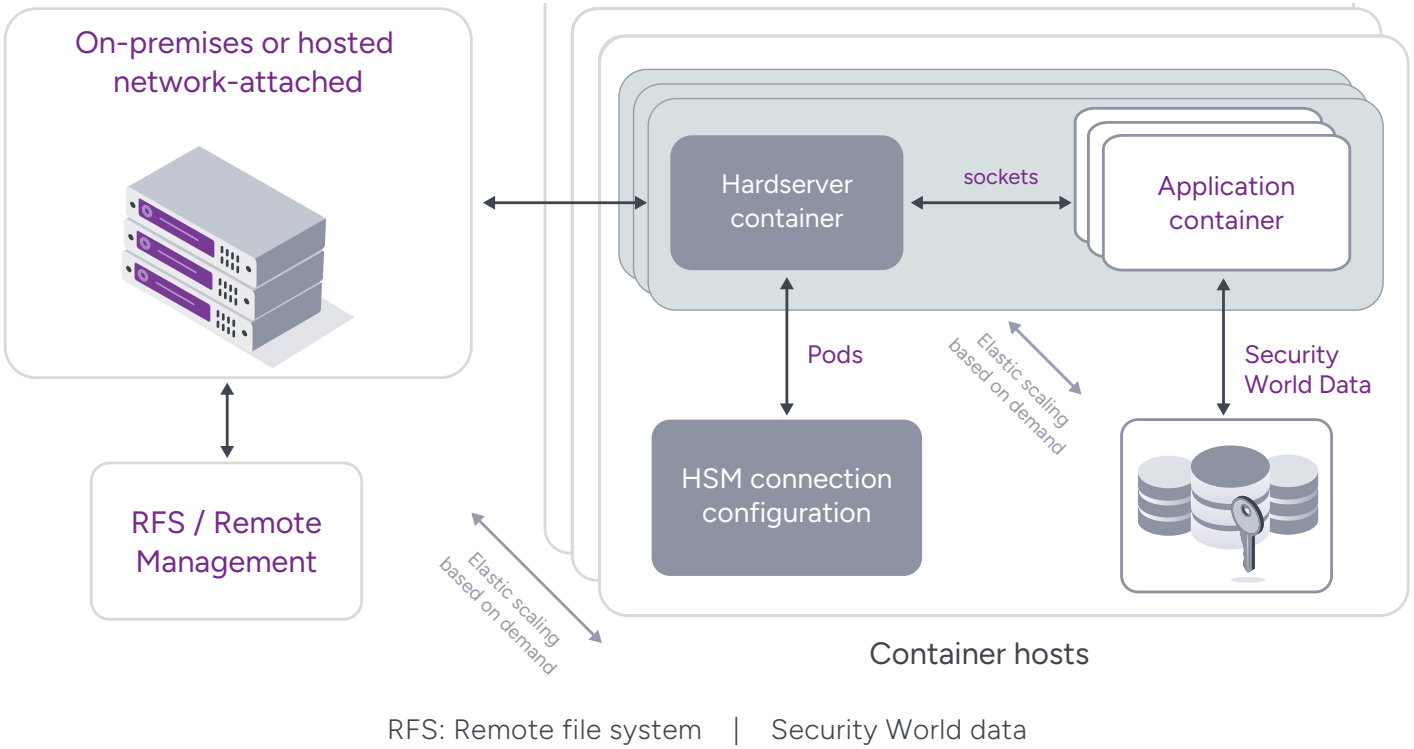

Figure 1: High level architecture of nCOP

Technical Specifications

Operating system support	Supported HSMs	Scalability & licensing
Linux distributions only	• Compatible with all nShield network-attached HSM models • Compatible with nShield as a Service for cloud-hosted HSM deployments	• nCOP supports any number of hardserver or application containers, and can work with any number of container hosts (physical or virtualized server instances) • When used in conjunction with network-attached nShield HSMs, client licenses will be required depending on the scale of deployment. The option pack includes a weighting factor for calculating the number of client licenses required based on the maximum number of running application containers to be deployed. Refer to Figure 2 for guidelines on the number of client licenses required for different sized deployments.

Number of client licenses per HSM	Maximum number of container pods	Maximum number of application containers permitted
5	5	50
10	10	100
15	15	150
20	20	200
>25	25	>250 Recommend purchase of enterprise client licenses

Figure 2: Required number of client licenses per HSM based on container pod and application container sizing

Note 1: The hardserver is the daemon service component of the nShield Security World software - which is responsible for secure communication with nShield devices across the network. Client components including PKCS#11 and Java libraries use sockets to interface with this process.

Learn more

To find out more about Entrust nShield HSMs, email HSMinfo@entrust.com or visit entrust.com/HSM.

To learn more about Entrust's digital security solutions for identities, access, communications, and data, visit entrust.com.

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

ENTRUST
SECURING A WORLD IN MOTION