Entrust nShield HSMs and Mirantis Kubernetes Engine Enhance the Security of Containerized Applications

Integrated solution enables application developers to easily access high assurance cryptographic services

HIGHLIGHTS

- Support today's fast-paced application container deployment environments
- Provide secure access to Entrust nShield® hardware security modules (HSMs)
- Allow critical cryptographic key management to run transparently
- Establish a FIPS 140-2 and Common Criteria certified root of trust
- Help facilitate auditing and compliance with data security regulations

MIRANTIS CERTIFIED

THE PROBLEM

Developers lack ability to access cryptographic functions for their applications

Modern application development uses containers and Kubernetes to standardize software design and facilitate continuous integration and continuous delivery (CI/CD).

The process enables developers to deploy new applications with the assurance that they'll run reliably in any user environment. A critical component of the software development process is the security of the CI/CD software supply chain. To date, adding an HSM root of trust for container deployments has been difficult.

Enhancing the security of containerized applications

THE CHALLENGE

Enabling access to cryptographic services without impacting development process

While the security of applications developed using containers and Kubernetes is critically important, it's also essential to maintain the accelerated pace that these technologies offer. Robust cryptographic services – including key creation, signing, verification, and encryption – need to integrate with the software development process easily and transparently.

Solutions that enable this integration not only protect the integrity of applications, but also of the data they process, helping facilitate security auditing and regulatory compliance.

THE SOLUTION

Mirantis Kubernetes Engine and Entrust nShield HSMs

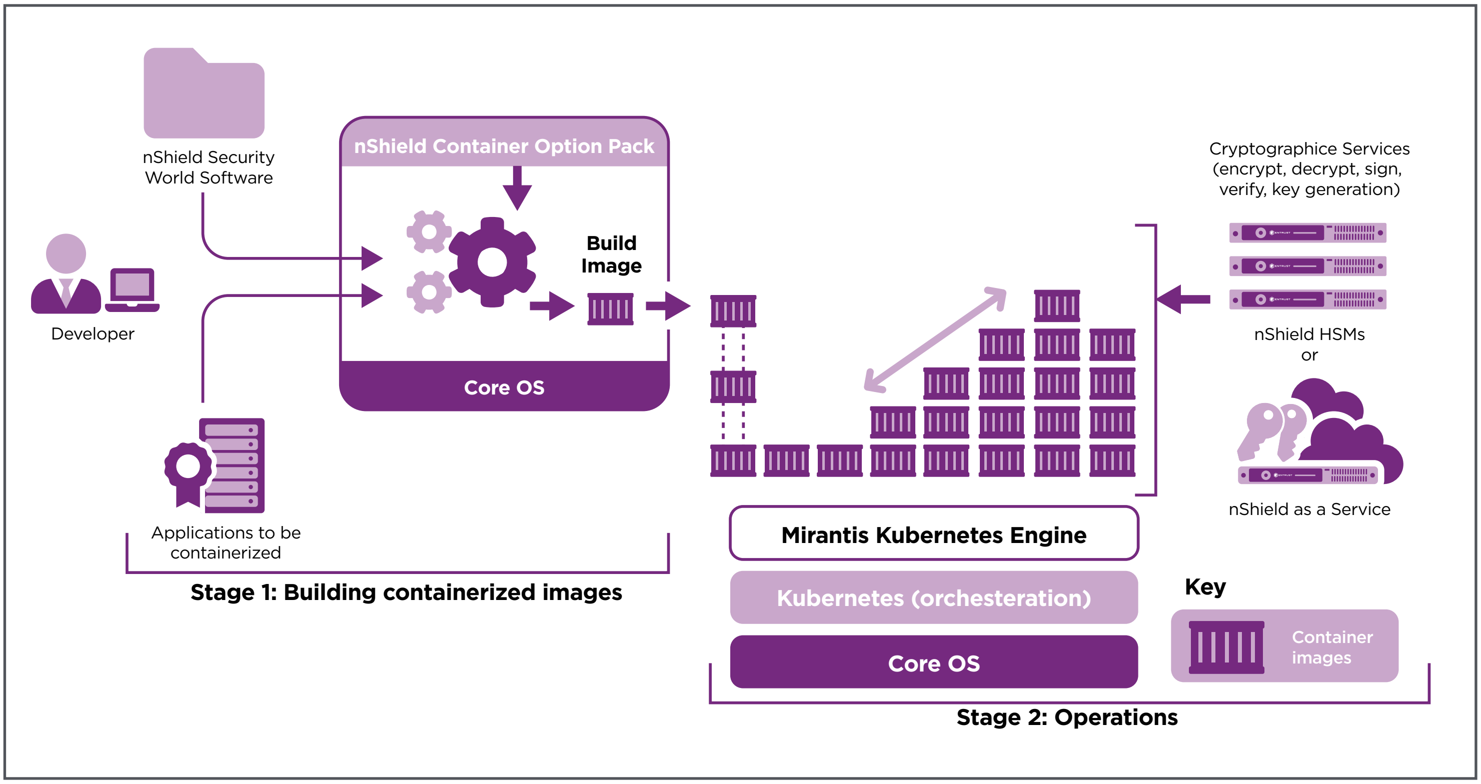
Mirantis Kubernetes Engine is a market-leading container platform for accelerating the development and delivery of modern applications. The platform provides developer choice, simple onboarding, and automation across DevOps. It also enables a secure pipeline to Kubernetes environments that run anywhere without losing operational flexibility and agility. Mirantis Kubernetes Engine provides:

- **Consistent Kubernetes clusters:** Deploy with Mirantis Kubernetes Engine across bare metal, private clouds, and public clouds; simplifies creation of CI/CD and automation that works everywhere
- **Docker trusted registry:** A private container registry with external registration mirroring, image security scanning, signing, and promotion policies; lets you quickly identify and mitigate vulnerabilities in curated images
- **Docker content trust:** Strict policy management preventing execution of inappropriately signed images; ensures process and oversight compliance in preparing workloads for test, staging, and production
- **FIPS-140-2 certified encryption and DISA STIG compliance**

Integration of Mirantis Kubernetes Engine with Entrust nShield Container Option Pack gives application developers the ability to access the cryptographic functionality of a robust, industry-leading nShield HSM within a container-based environment.

Enhancing the security of containerized applications

HOW IT WORKS


nShield Security World Software
Developer
nShield Container Option Pack
Build Image
Core OS
Applications to be containerized
Stage 1: Building containerized images
Cryptographice Services (encrypt, decrypt, sign, verify, key generation)
nShield HSMs or
nShield as a Service
Mirantis Kubernetes Engine
Kubernetes (orchesteration)
Core OS
Key
Container images
Stage 2: Operations

Mirantis Kubernetes Engine streamlines the application development process

1. Developers build containerized images using the Entrust nShield Security World software and the nShield Container Option Pack.
2. The Mirantis Kubernetes Engine provides the tools to test and deploy the containerized applications, abstracting the complexities of the Kubernetes layer.
3. Cryptographic services including encryption, decryption, signing, verification, and underpinning key generation are enabled using Entrust nShield HSMs on premises or nShield as a Service.
4. Containerized images with high assurance cryptographic functions can be built in a flexible and scalable manner.

A CLOSER LOOK

Why use nShield HSMs with Mirantis Kubernetes Engine?

Entrust nShield HSMs are specifically designed to safeguard and manage cryptographic keys and processes within a certified hardware environment to establish a root of trust. Critical keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attacks that can compromise confidential information.

Entrust nShield HSMs, offered as an appliance deployed at an on-premises datacenter or leased through an as-a-service subscription, provide enhanced key generation, signing, and encryption to protect sensitive container data and transactions. Using HSMs as part of an enterprise encryption and/or key management strategy is considered a best practice among cybersecuity professionals.

Entrust nShield HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management.

Why nShield Container Option Pack for Mirantis Kubernetes Engine?

Entrust nShield Container Option Pack provides a set of scripts for seamless development and deployment of containerized applications, underpinned by a high assurance Entrust nShield HSM. For DevOps and DevSecOps, Entrust nShield Container Option Pack provides the tools and proven architecture to deploy containers at scale as part of a CI/CD process. When the time from development to deployment is tight, Entrust nShield Container Option Pack accelerates the development of container images with cryptography provisioned by an Entrust nShield HSM root of trust.

About Entrust nShield HSMs

Entrust nShield HSMs are among the highest-performing, most secure, and easiest-to-integrate HSMs available. They help facilitate regulatory compliance and deliver 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.

For more information visit entrust.com/HSM.

About Mirantis

Mirantis helps organizations ship code faster on public and private clouds. Mirantis Kubernetes Engine provides one cohesive cloud experience for delivering consistent Kubernetes anywhere, providing a single pane of glass for metrics, and fully automated lifecycle management with continuous updates.

Open-source Lens, the leading Kubernetes IDE (sponsored by Mirantis), complements Container Cloud by providing unique insights into objects and containers across a fleet of clusters, dramatically simplifying Kubernetes complexity. Mirantis serves leading global enterprises, including Adobe, DocuSign, Liberty Mutual, Nationwide Insurance, PayPal, and Splunk.

For more information visit mirantis.com

Learn more at
entrust.com

ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com