Entrust and Leading Container Solution Providers Enable Secure Enterprise Software Development

HIGHLIGHTS

- Develop and deploy secure containerized applications
- Access the strong cryptographic functionality of Entrust nShield® HSMs
- Accelerate the development of container images
- Deploy containers at scale in a continuous improvement/continuous development process
- Facilitate compliance with government and industry security standards

THE CHALLENGE

Ensuring containerized applications are secure

As modern application development and deployment evolves to meet demands for flexibility and scalability, application development teams have come to rely increasingly on containers and Kubernetes.

"Containers have become popular because they provide a powerful tool for addressing several critical concerns of application developers, including the need for faster delivery, agility, portability, modernization, and lifecycle management."[1]

Containerization helps developers ensure applications will run reliably no matter the user environment. As an open-source container orchestration platform, Kubernetes meet development teams' need for managing resources as containers dynamically scale.

However, when applications require an enhanced level of protection, developers need to be able to incorporate cryptographic operations, such as key generation, digital signing, and data encryption while maintaining the accelerated pace that containerization offers. In addition, adequately protecting these cryptographic operations is vital to ensure the integrity of the applications and data, and to facilitate security auditing and regulatory compliance.

[1]Gartner, June 2020.

nShield HSM integration with container/Kubernetes platform

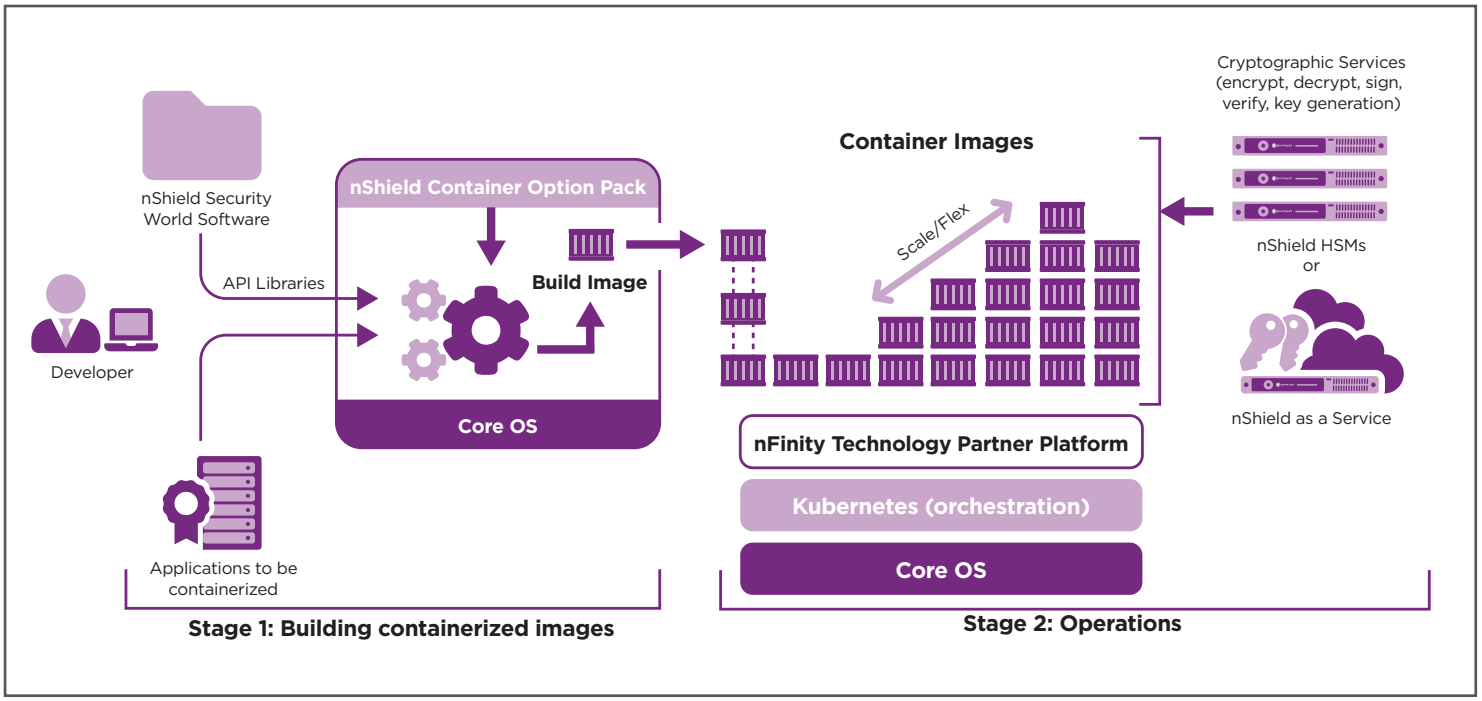
THE SOLUTION

Entrust nShield hardware security modules (HSMs) provide a certified root of trust for containerized applications

Containerized applications that require scalable, dynamic cryptographic services to generate keys, or to sign and encrypt data, can now use nShield® HSMs to deliver these services. Leveraging best practices, the use of HSMs mitigates risks by ensuring underpinning keys are protected within a FIPS 140-2 Level 3 and Common Criteria EAL4+ high assurance boundary, helps meet auditing and compliance requirements.

The Entrust nShield Container Option Pack provides application developers in container-based environments the ability to access the cryptographic functionality of nShield HSMs. nShield Container Option Pack provides a set of scripts for seamless development and deployment of containerized applications, with access to the Entrust nShield HSM's robust cryptography functionality.

For DevOps and DevSecOps, Entrust's nShield Container Option Pack provides the tools and proven architecture to deploy containers at scale as part of a continuous improvement/continuous development (CI/CD) process. When the time from development to deployment is tight, the nShield Container Option Pack accelerates the development of secure container images with cryptography provisioned by an nShield HSM root of trust.



nShield HSM integration with container/Kubernetes platform

THE SOLUTION (CONTINUED)

Developers use nShield Security World software and the nShield Container Option Pack to build containerized images. nFinity Technology Partner solutions provide the tools to test and deploy these images, abstracting the complexities of the Kubernetes layer. Cryptographic services including encryption, decryption, signing, verification, and underpinning key generation are enabled using Entrust nShield HSMs (on-premises or as a service). Containerized images, with high assurance cryptographic functions, can then be rapidly assembled in a flexible, scalable, and repeatable manner to support the customers' operations.

THE NSHIELD HSM DIFFERENCE

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

Using HSMs as part of an enterprise encryption and/or key management strategy is considered a best practice and is recommended by solution providers. Entrust nShield HSMs provide enhanced key generation, signing, and encryption to protect sensitive container data and transactions and are available as an appliance deployed at an on-premises data center or leased through an as-a-service subscription.

Entrust nShield HSMs:

- Easily integrate with containerized/Kubernetes application development platforms
- Are available as an on-premises platform and/or as a service for greater flexibility
- Provide a certified FIPS 140-2 Level 3 and Common Criteria EAL4+ root of trust
- Facilitate auditing and compliance to cybersecurity standards and regulations
- Support organizations' computing needs across a myriad of infrastructure environments
- Secure customer migration between computing environments including on-premises, cloud, and hybrid
- Flex and scale in dynamic, fluid containerized CI/CD software development process

nShield HSM integration with container/Kubernetes platform

NFINITY TECHNOLOGY PARTNERS

Entrust nFinity Technology Partners include leading providers of container/Kubernetes platform solutions that incorporate an Entrust nShield HSM root of trust, ensuring delivery of enhanced security for containerized applications. nShield HSMs are integrated with solutions from the following leading vendors.

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

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
info@entrust.com entrust.com/contact