cpl.thalesgroup.com

THALES

Securing the DevOps Lifecycle with Continuous Trust

Establishing End-to-End Trust with Thales Luna Hardware Security Modules and CipherTrust Data Security Platform

By Farallon Technology Group for Thales Digital Identity & Security

White Paper

Contents

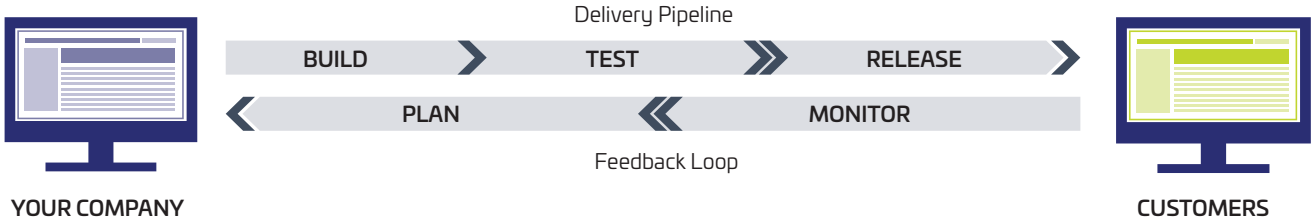
Securing the DevOps Lifecycle to Accelerate Software Delivery and Efficiency

What is DevOps?

DevOps is a set of practices and tools that enables teams to develop and deliver software applications faster and more reliably. DevOps, which blends the words "development" and "operations," is a cultural movement that breaks down organizational barriers by bringing software engineers and operations managers together to deliver the best possible application user experience.

> " DevOps is a cultural and professional movement, focused on how we build and operate high velocity organizations, born from the experiences of its practitioners. "
>
> - Nathen Harvey, Developer Advocate, Google

While there are many business advantages to DevOps, security remains a significant challenge that impacts the integrity and trustworthiness of code, software builds, firmware, and data. As a result, security and quality assurance teams must be tightly integrated with DevOps to make the software development lifecycle both efficient and secure. **Secure DevOps ensures the trustworthiness of code, finished software, and data throughout the DevOps lifecycle.**



DevOps teams use practices that automate historically manual and slow software development, testing, and release processes using purpose-built DevOps tools that help team members to code, build, test, release, and operate applications faster and more reliably. Furthermore, DevOps teams are often responsible for provisioning compute infrastructure, virtual machines (VMs), containers, storage, and load balancing in an automated fashion to help applications scale efficiently.

Benefits of a DevOps Approach

There are many benefits of adopting a DevOps approach, including speed, reliability, scalability and collaboration, each of which has unique security challenges.

Speed

Moving at a high velocity to innovate and adjust to changing markets is critical to business competitiveness. The DevOps model allows developers and operations teams to increase the frequency and pace of software updates, enabling a constant flow of new features. In fact, according to a study[1], top-performing DevOps teams deploy code to production 208 times more frequently than low-performing adopters. DevOps requires trusting that the code has not been tampered with and malware has not been introduced during the build process. Securing a fast DevOps pipeline relies on code signing, secrets management, container security, authentication, and IaaS/PaaS cloud security.

Reliability

DevOps deployments are more reliable and resilient, experiencing less downtime. In fact, skilled DevOps teams experience one-third of the failure rates of low-performing DevOps teams[1]. Security, such as code testing and software composition analysis, are implemented early in the DevOps lifecycle to reduce the cost and time to address security bugs and breakdowns later in the delivery process. Manual and automated testing and software scanning tools require strong authentication, authorization, and access controls.

Scalability

DevOps models leverage automation and orchestration that allow teams to rapidly scale compute resources, load balancing, and application services. For example, infrastructure as code allows companies to manage development, testing, and production environments more efficiently and programmatically using APIs. Scaling DevOps deployments securely requires strong key management, PKI and certificate management, encryption of data-at-rest and data-in-motion, authentication, and access controls.

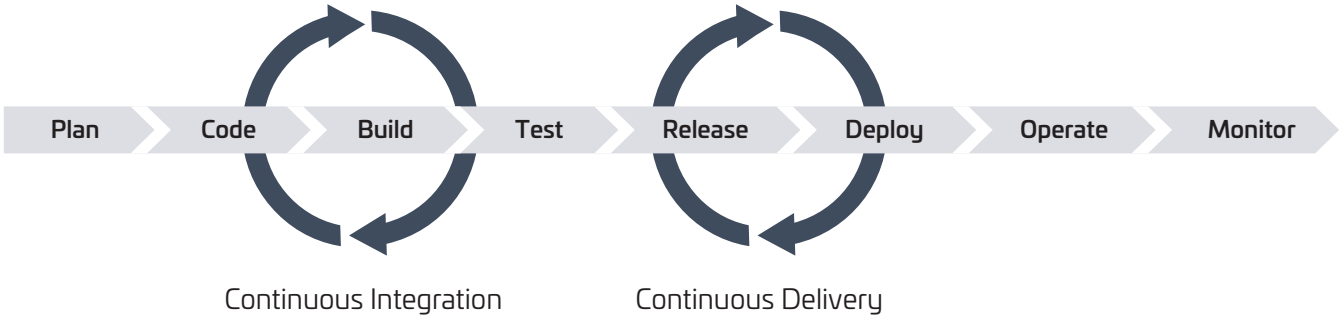
Collaboration

DevOps promotes a culture of collaboration and sharing between the software development and operations teams. The use of common tools and shared goals allows teams to work together efficiently to develop and deploy. Trusted collaboration requires end-user and machine-to-machine authentication, roles-based access controls, and secure communications.

Ensuring that businesses realize the speed, reliability, scalability, and collaborative benefits of DevOps requires securing the environment and continuous integration and continuous delivery (CI/CD) pipeline.

The DevOps Lifecycle and CI/CD Pipeline

The DevOps lifecycle can be broken down into eight stages: plan, code, build, test, release, deploy, operate, and monitor. Across these stages, DevOps embraces practices for continuous integration and continuous delivery (CI/CD) to ensure consistent, reliable, and automated development, verification, and delivery.



Continuous integration

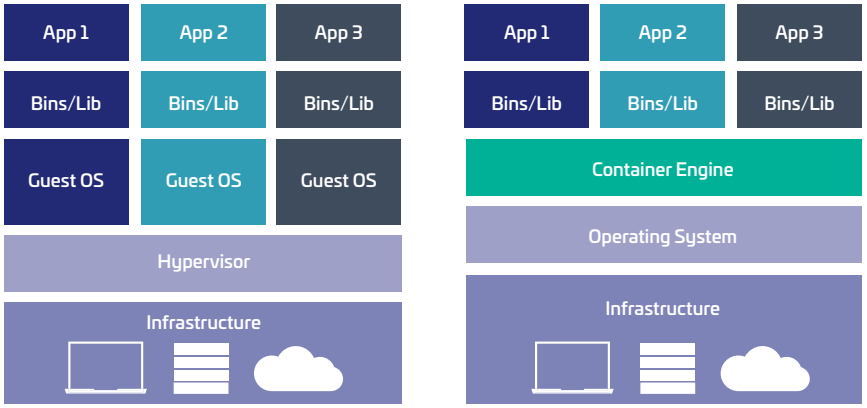
Continuous integration (CI) is a software development practice where developers regularly merge their code changes into a central repository, after which automated builds and integration tests are run. CI typically uses a build server to implement continuous processes applying quality control, static analysis, performance measurement, and updating documentation. The key goals of CI are to find and address bugs quicker, improve software quality, reduce the time it takes to validate and release new software updates, and speed up QA processes.

Continuous delivery

Continuous delivery (CD) is a software engineering and operations practice where code changes are automatically built, tested, and prepared for release into production. It expands upon continuous integration by deploying all code changes to a testing environment, verifying code signing signatures, testing the software, and readying the code for a manual release into environment after the build stage. When CD along with deployment into production are automated, it is called continuous deployment. The goal of CD is to release software with greater speed, frequency, and reliability.

Microservices

The microservices architecture is a design approach to build a single application as a set of small services running in containers. An application container encapsulates only the necessary files, dependencies, and libraries for a specific part of an application. Each service runs in its own process and communicates with other services through a well-defined interface using a lightweight mechanism, typically an HTTP-based application programming interface (API). Unlike a virtual machine that runs a full OS on a hypervisor, a container runs on a container engine, such as Docker, and is made up of only the processes and services required for the application container's purpose. This makes containers much more efficient than virtual machines, enabling greater economies of scale and a more cost-effective use of compute resources.



Virtual Machines

Containers

Infrastructure as Code

Infrastructure as code is a practice in which infrastructure, such as compute, memory, storage, and networking, is provisioned and managed using code and software development techniques, rather than physical or manual configuration. The cloud's API-driven model enables developers and system administrators to interact with infrastructure programmatically. Because they are defined by code, infrastructure and servers can quickly be deployed and terminated based on an application's requirements during the software development and DevOps lifecycle.

Monitoring & Logging

DevOps teams monitor metrics and logs to see how an application update or change in infrastructure impacts the end user experience. By capturing and analyzing data and logs generated by applications and infrastructure, organizations can better understand the impact on performance and user behavior while shedding light onto the root causes of problems or unplanned incidents.

With such a broad scope of responsibility, DevOps is extremely vulnerable to cyber-attacks that compromise the development, deployment, and operation of applications. Secure DevOps, known as DevSecOps, must secure machine identities, secrets, keys and certificates to prevent bad actors from gaining access to systems that allow malware and manipulated data to be deployed.

Securing DevOps and CI/CD Pipeline

Securing the DevOps environment is critical to the success of business-driven digital transformation projects that require a nearly constant stream of new features and fixes, delivered in small increments. Digital transformation and DevOps leverage cloud computing to scale development, testing, and production operations. 80% of DevOps practitioners1 said that the primary application or service they supported was hosted on a hybrid multi-cloud platform.

Secure DevOps requires strong key management, certificate management, authentication, PKI, access controls, code signing, and signature verification to ensure the trustworthiness and integrity of software, VMs, and containers. **While DevOps teams can use dynamic and static application security testing to check the code and binaries for misconfigurations or the presence of known vulnerabilities, if the system does not have a consistent and centralized approach to key and certificate management, the DevOps configuration management and orchestration tools will be very difficult to trust.**

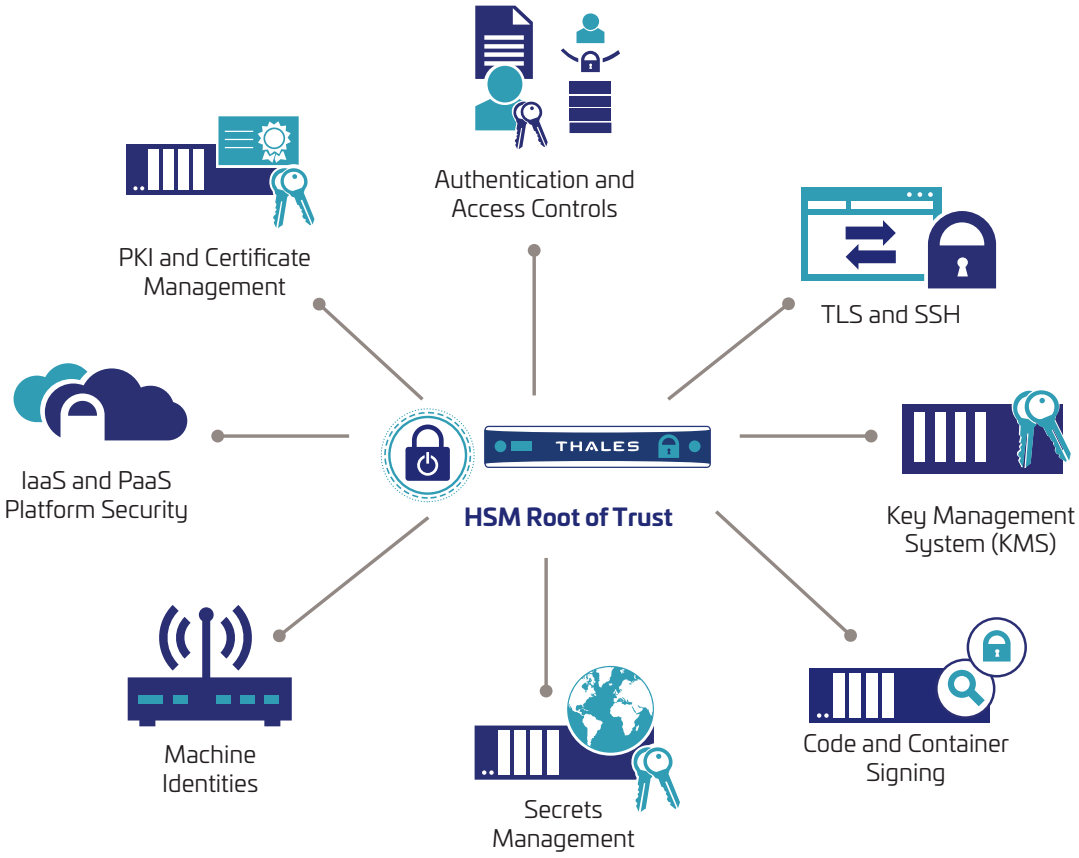
For example, if the signatures used to sign code were created based on a self-signed digital certificate using keys that were generated insecurely, then a sophisticated and persistent attacker could impersonate the author of the code and potentially introduce malware.

Similarly, if the configuration management tools used to manage the CI/CD pipeline, IaaS infrastructure, Kubernetes clusters, and network encryption are using secrets, machine identities, certificates, and tokens that are based on insecurely generated private keys, then the deployed software and containers should not be trusted.

It is critical that the DevOps environment is built on a foundation of digital trust with hardened key and certificate management for each stage of the DevOps lifecycle.

> " The DevOps process is vulnerable to cyber-attacks that compromise the development, deployment, and operation of applications. Secure DevOps, also known as DevSecOps, is a practice to help ensures the trustworthiness of code, associated data, and the resulting application, throughout the lifecycle. "

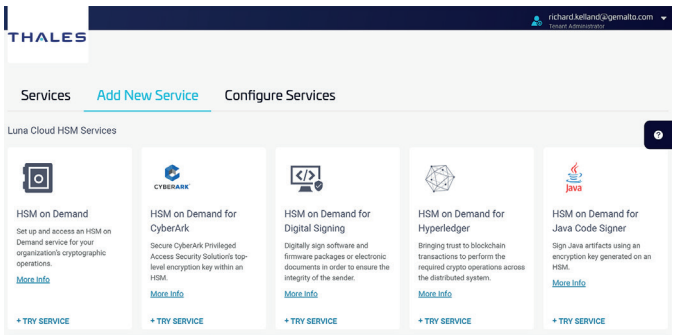
Establishing a Chain of Trust Across DevSecOps



Establishing a chain of trust across the DevSecOps tool chain requires a consistent and centralized approach to key and certificate management. Development, testing, and production environments rely heavily on machine identities, secrets, tokens, keys, and digital certificates that must be trusted. Hardware security modules (HSM) and key management systems (KMS) are able to support advanced security features supported by DevOps tools that manage the CI/CD pipeline, cluster orchestration, TLS ingress, and code signing.

An HSM is a device containing a dedicated crypto processor that is specifically designed for the protection of the crypto key lifecycle. HSMs act as trust anchors that protect the cryptographic infrastructure of some of the most security-conscious organizations in the world by securely managing, processing, and storing cryptographic keys inside a hardened, tamper-resistant device. HSM services can be consumed from dedicated hardware, from a Cloud HSM as a Service, or from a hybrid mixture of both.

Luna Network HSM



Luna Cloud HSM as a Service

The following DevSecOps systems require strong key and certificate orchestration and management that can be provided by an HSM and integrated KMS systems:

- **IaaS and PaaS Platform Security:** Public and private cloud platforms often use open source software to generate key pairs and self-signed certificates that are more easily hacked. Using an HSM to generate key pairs will make it virtually impossible for attackers to compromise.
- **Machine Identities and Containers:** Deploying a VM or container with an encrypted tunnel to other containers are often implemented using default settings. Kubernetes supports advanced KMS functions that are well-suited to integrate with HSMs and third-party KMS platforms.
- **Public Key Infrastructure (PKI) and Certificate Management:** Managing PKI infrastructure is oftentimes the weak link in a layered network defense strategy. A PKI management system simplifies the generation of public/private key pairs and digital certificates and supports device enrollment, key rotation and revocation. Access controls, machine to machine (M2M) mutual authentication, data encryption, and TLS require strong PKI and certificate management.
- **Secrets Management:** Secrets managers (aka vaults) contain application credentials and tokens that are used frequently by applications and IaaS platforms. It is critically important for these secrets to have been generated using private keys that are generated, managed, stored and remain in hardware.
- **Authentication, Authorization and Access Controls:** Software supply chains and agile development teams can be comprised of hundreds of software developers that contribute code and software builds. Authenticating users and machines; enforcing access controls; and enabling privileged escalation require a sound authentication and authorization system built on bulletproof key and certificate management systems.
- **TLS and SSH:** Public and private cloud platforms often use open source software to generate key pairs and self-signed certificates for SSH access and TLS/SSL. While convenient and fast, using open-source cryptographic software with insufficient entropy, or randomness, for key generation can introduce vulnerabilities or weaknesses in the cryptographic control system. Using an HSM simplifies the enforcement of strong key management principles.
- **Code and Image Signing:** Code should be signed with a verified digital signature during development and before it is submitted into the CI/CD pipeline. Orchestration and configuration management tools should be integrated with platforms that are monitoring and scanning code. Using strong keys in the code and image signing process will reduce the risk of impersonation, IP theft, and counterfeiting.

Using an HSM and KMS will provide a chain of trust across the DevOps lifecycle in a consistent manner that will simplify management and harden systems to withstand persistent attacks from well-funded bad actors with malicious intent.

Thales impact on the DevOps lifecycle

Code Stage:

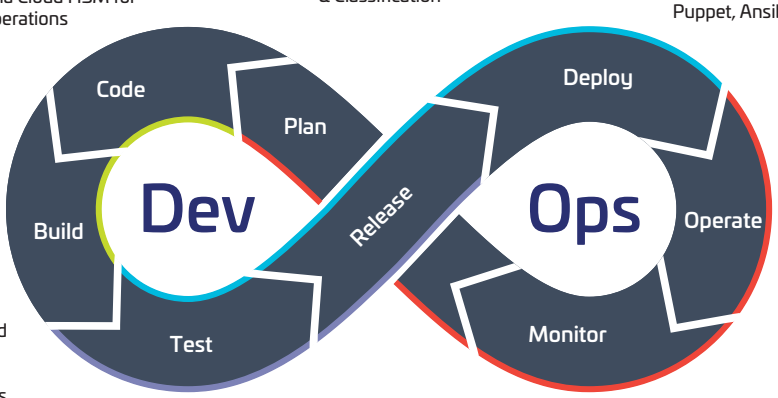
- CipherTrust Application Data Protection for app layer encryption
- CipherTrust Tokenization to tokenize sensitive data, vaulted or vault-less
- CipherTrust Batch Data Transformation for static data masking
- Luna HSM and Luna Cloud HSM for app level crypto operations

Plan Stage:

- CipherTrust Data Discovery & Classification

Deploy Stage:

- Via integrations with CI/CD Tool Chain, such as Chef, Puppet, Ansible



Build Stage:

- Luna HSM code and container image signing via integrations such as RedHat Openshift, Docker, KeyFactor, Venafi, Garantir

Test Stage:

- CipherTrust Batch Data Transformation enables you to remove the sensitive information before sharing with internal or third-party developers

Monitor Stage:

- Luna HSM and Luna Cloud HSM
- CipherTrust Manager
- CipherTrust Cloud Key Manager (CCKM)
- Via integrations with SIEMs, such as IBM Qradar, Splunk, ArcSight

Operate Stage:

- CipherTrust Manager
- CipherTrust Transparent Encryption
- CipherTrust Container Security extends controls for data encryption, access control, and data access audit logging to data within or linked to containers
- CipherTrust Transparent Encryption Live Data Transformation (LDT) for live data encryption for data-at-rest
- CipherTrust Cloud Key Manager (CCKM) for AWS, Azure, IBM, Salesforce.com, Cloud BYOK
- Luna HSM and Luna Cloud HSM for Root of Trust (RoT) for certificate authorities, secrets management, and certificate management

Continuous Integration (CI)

Continuous Delivery (CD)

Continuous Deployment (CD)

Continuous Feedback (CF)

Thales Across the DevSecOps Lifecycle

Thales provides continuous trust across the DevOps lifecycle and CI/CD pipeline, enabling fast, secure and reliable operations for hybrid multi-cloud deployments. By leveraging Thales Luna hardware security modules (HSM) and the CipherTrust Data Security Platform, DevSecOps practitioners are able to address the need for strong key generation, storage and management and data encryption across all stages of the DevOps lifecycle.

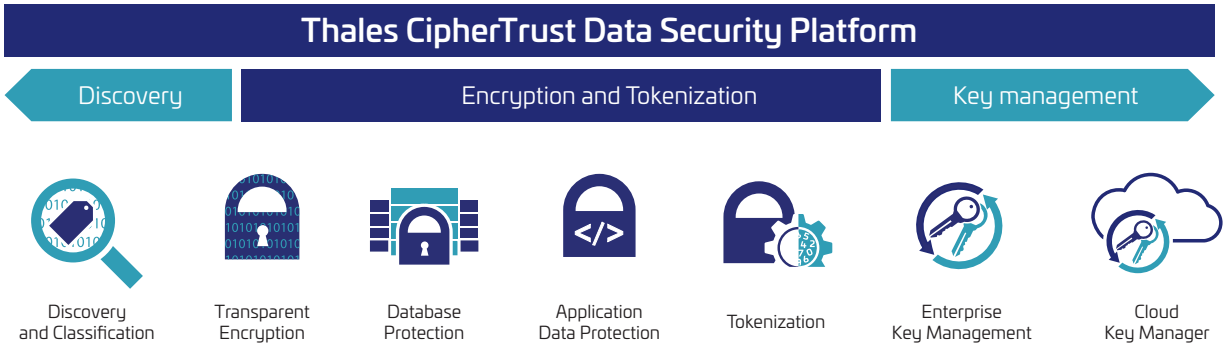
Thales Luna HSMs

Luna Network HSM is a FIPS 140-2 Level 3 validated and Common Criteria certified, tamper-resistant network-attached HSM that provides high assurance cryptographic key protection for governments, financial institutions and large enterprises worldwide. Luna HSMs establish confidentiality and trust between devices, identities and transactions. HSMs simplify integration and development with a wide variety of APIs with hundreds of out-of-the-box technology partner integrations providing a strong foundation of digital trust.

Luna Cloud HSM services are available on Thales Data Protection on Demand (DPoD), a cloud-based platform that provides a wide range of Cloud HSM and key management services through a simple online marketplace. With Luna Cloud HSM, there is no hardware to buy, and integration with other cloud-based IaaS and DevOps platforms is simple.

The Luna Network HSMs and Luna Cloud HSMs provide a hardware root of trust, secure key generation, and key storage for the coding, building, monitoring, deployment and operating stages of the DevOps lifecycle and CI/CD pipeline seamlessly across on-premises, hybrid and multi-cloud environments.

Thales CipherTrust Data Security Platform enables DevOps teams to centralize and simplify data security policies and key management anywhere. The CipherTrust Platform unifies data discovery, classification, and protection with unprecedented granular access controls, including centralized key management – all on a single platform. The comprehensive platform reduces the need for resources dedicated to data security operations while providing ubiquitous compliance controls and significantly reduced risk across the business.



The following is a description of the core CipherTrust Data Security Platform products.

CipherTrust Manager

- CipherTrust Manager enables organizations to centrally manage encryption keys for Thales and third-party products. It simplifies key lifecycle management tasks, including secure key generation, rotation, backup/restore, clustering, deactivation, and deletion while offering developer friendly REST APIs. CipherTrust Manager is the central management point for the CipherTrust Data Security Platform. It is available in both virtual and physical appliances that are FIPS 140-2 compliant for securely storing keys with an elevated root of trust. **CipherTrust Manager is an essential solution for key management across the end-to-end DevOps lifecycle.**

CipherTrust Application Data Protection

- Simple-to-use, powerful software tools for application-level key management, signing, hashing and encryption of sensitive data through APIs, so that developers can easily secure data at the application server or big data node. The solution comes with supported sample code so that developers can move quickly to securing data processed in their applications. CipherTrust Application Data Protection accelerates development of customized data security solutions, while removing the complexity of key management from the developer's responsibility and control. In addition, it enforces strong separation of duties through key management policies that are managed only by security operations. The solution is flexible enough to encrypt nearly any type of data passing through an application. **CipherTrust Application Data Protection helps to secure the coding and operating stages of the DevOps lifecycle.**

CipherTrust Tokenization

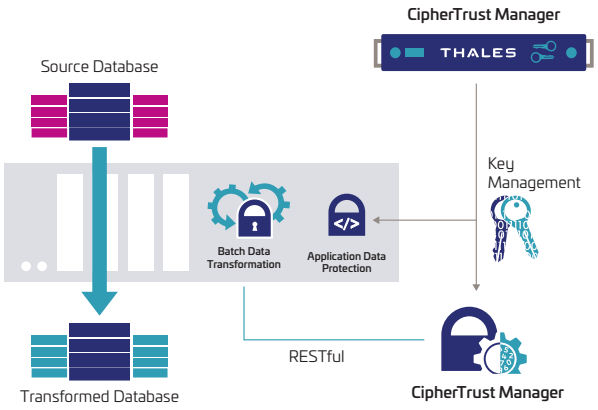
- CipherTrust Tokenization is offered both vaulted and vaultless and can help reduce the cost and complexity of complying with data security mandates such as PCI DSS. Tokenization replaces sensitive data with a representative token, so that the sensitive data is kept separate and secure from the database and unauthorized users and systems. The vaultless offering includes policy-based dynamic data masking. Both offerings make it easy to add tokenization to applications. **CipherTrust Tokenization protects sensitive data during the coding stage and at runtime.**

CipherTrust Batch Data Transformation

- Software tool that provides high-performance static data masking. It leverages the power of CipherTrust Application Data Protection and CipherTrust Tokenization to protect vast quantities of data quickly. **CipherTrust Batch Data Transformation helps to secure the testing stage of the DevOps lifecycle.**

CipherTrust Data Discovery and Classification

- Allows you to discover and classify sensitive data to meet data privacy and security regulations. This enterprise-wide data privacy solution is simple to deploy and scale. It provides ready-to-use templates and a streamlined workflow to help you quickly discover your regulated data across traditional and modern repositories. **CipherTrust Data Discovery and Classification helps to secure the planning stage of the DevOps lifecycle.**



CipherTrust Transparent Encryption

- CipherTrust Transparent Encryption delivers data at rest encryption, privileged user access control and detailed data access audit logging. This protects data wherever it resides, on-premises, across multiple clouds and within big data, and container environments. CipherTrust Transparent Encryption Live Data Transformation, with zero downtime encryption deployments, allows for encrypting and re-keying data without taking applications offline. This allows deployment of data security controls to applications along with business continuity and high availability. CipherTrust Container Security extends CipherTrust Transparent Encryption to containers, enabling security teams to establish data security controls inside of containers. With this extension, you can apply encryption, access control, and data access logging on a per-container basis. Encryption can be applied to data generated and stored locally within the container and to data mounted in the container by network file systems. **CipherTrust Transparent Encryption helps to secure the operating stage of the DevOps lifecycle.**

CipherTrust Enterprise Key Management

- Enterprise Key Management solutions enable organizations to centrally manage and store cryptographic keys and policies for third-party devices including Microsoft SQL TDE, Oracle TDE, and KMIP-compliant encryption products. **CipherTrust Enterprise Key Management helps to secure the operating stage of the DevOps lifecycle.**

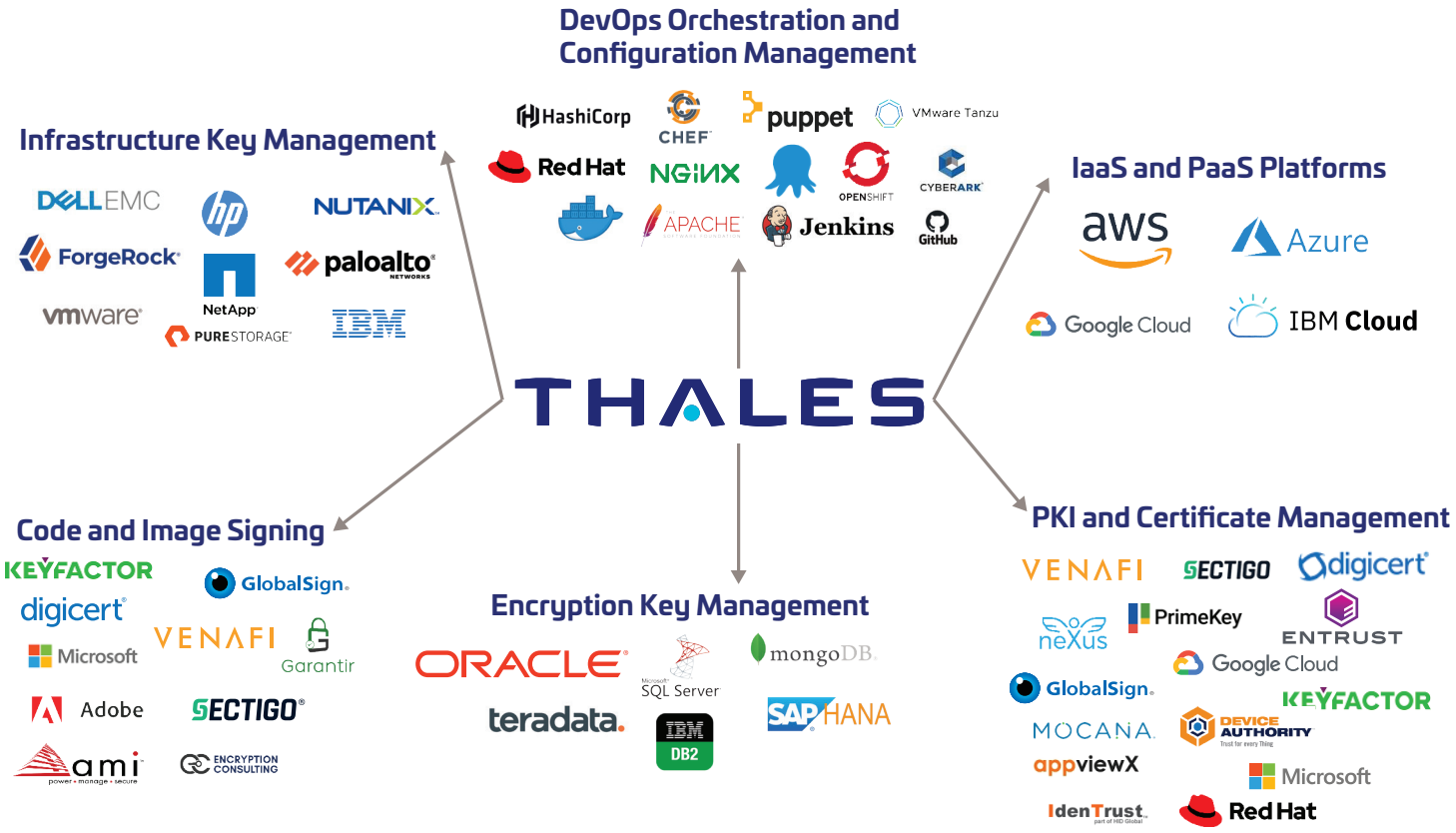
CipherTrust Cloud Key Manager

- CipherTrust Cloud Key Manager centralizes encryption key management from multiple environments, presenting all supported clouds and even multiple cloud accounts in a single browser window, including: AWS, Microsoft Azure, Google Cloud, IBM Cloud, and Salesforce. **CipherTrust Cloud Key Manager helps to secure the monitoring stage of the DevOps lifecycle.**

Thales DevSecOps Ecosystem Partners

Thales Luna HSMs and CipherTrust Data Security Plaform simplify the implementation of trustworthy DevSecOps practices. Thales solutions are broadly integrated with open-source platforms and DevOps tools to accelerate the implementation of security at every stage of the DevOps lifecycle.

Thales DevSecOps Partners



Summary and Recommendations

DevOps has accelerated the software delivery process and made it more reliable and resilient. Using practices such as agile software development, continuous integration and continuous delivery (CI/CD), microservices, infrastructure as code, and modern DevOps tools organizations are realizing significant improvements in:

- Deployment frequency
- Lead time for change
- Time to restore service
- Change failure rate.

The rapid adoption of DevOps and DevSecOps has created a complex software development environment that is fraught with vulnerabilities and risks. Gaps in DevOps security can lead to application vulnerabilities that result in:

- Code injections
- Broken authentication
- Using components with known vulnerabilities
- Stolen machine identities, keys and certificates
- Sensitive data exposure
- Weak authentication
- Insecure key generation and storage
- Lack of a chain of trust
- Man-in-the-middle attacks.

Protecting the DevOps lifecycle requires implementing layered network defenses, code verification, strong security controls and mature key and certificate management. IaaS and PaaS platform security, PKI, authentication, TLS, secrets management, container security, and code signing all require trustworthy key generation, storage and management. All of these defenses require a consistent approach to key and certificate management.

Why Thales Luna HSMs and CipherTrust Data Security Platform

- Thales Luna HSM and CipherTrust Data Security Platform solutions for hybrid and multi-cloud environments provide security across all stages of the DevOps lifecycle
- Developers can secure applications managing sensitive data with RESTful APIs and installable libraries for encryption and/or tokenization
- Test teams can ensure that sensitive production data is not made accessible for testing by leveraging batch data transformation tools
- Application release teams can secure code/container image signing and signature verification with hardware-based Root of Trust (RoT)
- Operations teams can ensure data-at-rest encryption requirements are met by leveraging transparent encryption when app-level encryption/tokenization is not feasible
- Operations teams can secure crypto keys and certificates by leveraging centralized software-based enterprise and cloud key management
- Operations teams can secure PKI, SSH, TLS, and certificate management infrastructure and tools by leveraging hardware-based RoT for key generation and storage
- Operations teams can monitor access to sensitive data and keys via centralized encryption and key management solution's integration with their SIEM tools
- Thales Luna HSMs provide a wide variety of APIs and hundreds of common technology partner integrations that simplify integration and development.

High-performing DevOps teams and organizations that are still maturing their DevOps practices can benefit from implementing a consistent and centralized approach to policy-based data encryption, crypto keys, and certificate management using Thales Luna HSMs and CipherTrust Data Security Platform.

About Thales Digital Identity and Security

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

About Farallon Technology Group

Farallon Technology Group is technology research and advisory firm focused on embedded, operational technology (OT), and cloud native cybersecurity. We deliver technical market and vendor research that covers key security technologies for cloud, IoT and edge computing. Farallon helps industrial companies, OEMs, and cybersecurity vendors to navigate business and technology risks and opportunities to reduce cost, drive digital transformation, and manage supply chains. www.farallontech.com

THALES

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <