cpl.thalesgroup.com

THALES

Enabling Enterprises to Achieve Secure and Compliant DevOps

Integrated DevOps Solution from Thales, Venafi and HashiCorp

The Problem

Today's large enterprises operate across many boundaries, acting as a virtual organization in multiple cities and countries. With recent health issues expanding the need for a remote workforce the corporate perimeter has grown even wider. One department that commonly combines efforts from widely dispersed individuals is software development. DevOps, or the processes that enable application development and operations to be combined, adds complexity and security risks not previously seen when programmers were all on-site, behind a firewall and with access only to development environments. Along with the agility and scale that DevOps brings, if not implemented correctly, DevOps processes can be impeded and hacked, adding development time and security risks to the end product.

Several security solutions are available to maintain trust in the DevOps process, including code signing, secrets management, TLS/SSL keys and machine identity management. At the root of any security solution are the private keys that are at the heart of the PKI environment. If code signing private keys find their way into the hands of an attacker, accidentally or through a breach in the network, they can inflict serious damage on the business. The root of trust is broken, the digital signatures using these keys are suspect and the integrity of the code they sign cannot be assured.

Combining disparate security products into a cohesive solution can be complicated, and may leave it to the organization to figure out how to deploy a compete solution. Without solution components that are tested, optimized, and work seamlessly together, the speed of code development and deployment from DevOps teams can be negatively impacted. In addition, missing one key piece in the solution can leave a trust gap in the final product.

Implemented correctly, all aspects of DevOps can be secured: secrets are safely stored; development and deployment processes and protocols remain the same; compliance requirements are met; the end-to-end the root of trust is maintained; and an organization's InfoSec policies are upheld. The solution must also be transparent to the processes and tools developers are using.

The Solution

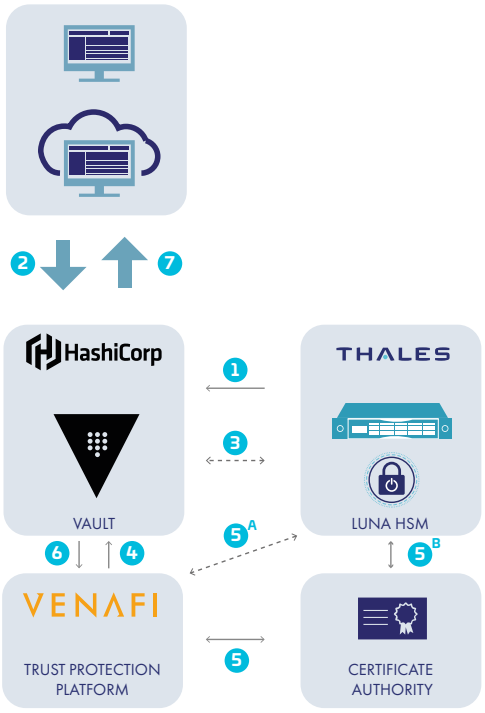
Whether an on-premises or cloud-distributed DevOps team, to be truly effective for deployment in critical business systems, DevOps needs a balance of ease of use, speed and security. In the past, it has been very slow to get compliant certificates as needed by developers as they quickly build new software workflows. The Venafi, HashiCorp and Thales combined solution provides a balance of speed and root of trust for developers. By connecting DevOps tools with certificate authorities, this solution enables an automated and efficient way to provide, enterprise-trusted, compliant SSL certificates that are accessible from within the tools developers use. This cohesive integration enables developers to maintain the speed of the agile development process without sacrificing compliance with security policies.

Venafi Trust Protection Platform manages and automates all PKI certificates while meeting the needs of DevOps to move at speed. Thales Luna HSMs, available on-premises, or as a cloud HSM service using Thales Data Protection on Demand (DPoD), provides the vital HSM key stores to ensure protection from compromise by protecting the HashiCorp Vault and Venafi Trust Protection Platform master keys, as well as provide the public CA with a more secure root of trust for DevOps. PKI infrastructure has been a manual process of generating a private key and CSR, submitting to a CA, then waiting for a verification and signing process to complete. This joint solution simplifies PKI

infrastructure into a single command, or even a fully automated process. Thales and Venafi also work closely with public CAs like DigiCert, Entrust Datacard, GlobalSign, PrimeKey, and Sectigo to ensure customers have the secure, high quality and compliant SSL certificates to meet their compliance and DevOps requirements.

How it all Works

1. Thales Luna HSM automatically unseals HashiCorp Vault
2. DevOps team requests a machine identity for a new application from Vault
3. Vault generates a private key pair using advanced entropy provided by Luna HSM
4. Vault creates a Certificate Signing Request (CSR) and sends to Venafi Trust Protection Platform (TPP)
5. TPP sends the CSR to the CA to be fulfilled and sent back to TPP
   - a. Luna HSMs provide master key protection for the TPP database
   - b. Luna HSMs provide root of trust protection to leading CAs
6. Vault retrieves the certificate from TPP
7. The new machine identity is retrieved from Vault during the CI/CD build process and installed on the app



Thales, Venafi and Hashicorp DevOps Solution Architecture

Key Features and Benefits

- On-premises, hybrid and cloud-based Thales HSM options ensure your critical encryption keys and digital identities are always secure by managing and storing them in a certified root of trust HSM
- Thales HSMs easily and cost-effectively meet compliance needs with the most certifications in the industry, including FIPS 140-2, Common Criteria, eIDAS, GDPR, ITI, Singapore CC NITES, and more
- Venafi seamlessly connects certificate authorities (CAs) to the tools developers are using today, providing secure and compliant certificates while automating the lifecycle of keys and certificates, and maintaining the speed and efficiencies of the DevOps Agile development process.
- Use native Vault commands for requesting certificates while fully complying with corporate security and audit policies.
- HashiCorp Vault PKI streamlines distributing TLS certificates, allowing users to create PKI certificates with a single command or through a fully automated process

In Summary

Selecting a fully integrated and tested DevOps solution from three industry-leading companies like Thales, Venafi and HashiCorp, organizations embracing DevOps practices can implement controls and processes with the security, reporting and auditing features required in an enterprise-class development program. By including root of trust protection with a FIPS 140-2 Level 3 compliant Luna HSM, the application can meet global regulatory requirements while maintaining the tools, speed and flexibility provided by the agile development process.

About Thales

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 Venafi

Venafi is the cybersecurity market leader of machine identity management, securing machine-to-machine connections and communications. Venafi protects machine identity types by orchestrating cryptographic keys and digital certificates for SSL/TLS, code signing, mobile and SSH. Venafi delivers innovative solutions for the world's most demanding, security-conscious Global 5000 organizations and government agencies.

About HashiCorp

HashiCorp is the leader in multi-cloud infrastructure automation software. The HashiCorp software suite enables organizations to adopt consistent workflows to provision, secure, connect, and run any infrastructure for any application. HashiCorp open source tools Vagrant, Packer, Terraform, Vault, Consul, and Nomad are downloaded tens of millions of times each year and are broadly adopted by the Global 2000. Enterprise versions of these products enhance the open source tools with features that promote collaboration, operations, governance, and multi-data center functionality. The company is headquartered in San Francisco and backed by Mayfield, GGV Capital, Redpoint Ventures, True Ventures, IVP, and Bessemer Venture Partners

> cpl.thalesgroup.com <

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

© Thales - September 2020 • DBV3