



Whitepaper

Simplify DevOps Security: Integrating Your Cryptographic Framework with Your CI/CD Pipeline

Integrated DevOps Solution from Accutive Security,
Thales, Venafi and HashiCorp

The Problem

In today's globalized era, large corporations function beyond geographical limitations, behaving as virtual entities spread across various cities and nations. Recent health crises have further accelerated the need for a remote workforce, thereby stretching the corporate boundaries even further. One domain where collaboration from individuals scattered across diverse locations is typically seen is software development. DevOps, a practice that merges application development and operations, introduces unique complexities and security threats that were previously absent when developers operated on-site, within the safety of a firewall, and had access only to development environments. While DevOps offers the advantage of agility and scalability, improper implementation can lead to security breaches and slow down the development process, thus escalating security risks associated with the final product.

There is a range of accessible security measures to ensure the trustworthiness of the DevOps process, such as code signing, secrets management, TLS/SSL keys, and machine identity management. Fundamental to any security framework are the private keys, the lifeblood of the PKI environment. If these code-signing private keys fall into an attacker's hands, either unintentionally or through a network breach, they can severely compromise the organization. The root of trust is shattered, digital signatures relying on these keys become dubious, and the integrity of the signed code cannot be guaranteed.

Integrating varied security products into a unified solution can be a complex task, potentially leaving the organization to discern how to deploy a comprehensive solution. The absence of solution components that have been tested and optimized and function harmoniously can hinder the pace of code development and deployment by DevOps teams. Additionally, omitting a critical element in the solution could result in a trust gap in the end product.

However, with the right implementation, every aspect of DevOps can be safeguarded: secrets remain securely stored, development and deployment procedures and protocols are preserved, compliance standards are met, the root of trust is maintained end-to-end, and the organization's InfoSec policies are upheld. The solution must also be transparent to the tools and processes that developers employ.

Accutive Security steps in to fortify this solution by offering its data discovery and masking product, along with professional services for Thales and Venafi. Along with Accutive Security, these additions aim to streamline and safeguard the entire DevOps process, making sure all components work seamlessly together, leaving no room for trust gaps, and ensuring the highest standards of security and compliance are met.

The Answer

Whether it's an on-premises team or one distributed across multiple cloud platforms, effective DevOps for critical business system deployment necessitates a balance of user-friendliness, speed, and security. In the past, acquiring compliant certificates was a time-consuming process that hindered the rapid development of new software workflows. The consolidated solution from Venafi, HashiCorp, Thales, and now, Accutiv Security, provides a perfect blend of speed and foundational trust for developers. By connecting DevOps tools with certificate authorities, this solution delivers an automated and efficient approach to provisioning SSL certificates that adhere to enterprise trust standards and are readily accessible right from developers' toolkits. This seamless integration enables developers to maintain the momentum of agile development processes without violating security policy compliance.

Venafi's Trust Protection Platform supervises and automates all PKI certificates, keeping pace with DevOps' demand for speed. Thales' Luna HSMs, available both on-premises and as a cloud HSM service through Thales' Data Protection on Demand (DPoD), supply the essential HSM key stores required to avert compromises. They do this by protecting the master keys of HashiCorp Vault and Venafi Trust Protection Platform, and providing the public certificate authority (CA) with a more secure root of trust for DevOps.

Business Impact

Traditionally, managing PKI infrastructure has been a manual process, involving the generation of a private key and CSR, submission to a CA, followed by a waiting period for a verification and signing process to complete. This collaborative solution simplifies PKI infrastructure into a single command or potentially an entirely automated process. Thales and Venafi also work closely with public CAs like DigiCert, Entrust Datacard, GlobalSign, PrimeKey, and Sectigo, ensuring that customers receive secure, high-quality, and compliant SSL certificates meeting their compliance and DevOps requirements.

To this robust security mix, Accutiv Security brings its prowess in data discovery and masking, along with professional services. By offering additional layers of security and compliance measures, Accutiv's contributions aim to further reinforce this integrated DevOps solution, ensuring all components work together seamlessly for a safer, more efficient DevOps environment.

The Integrated Workflow

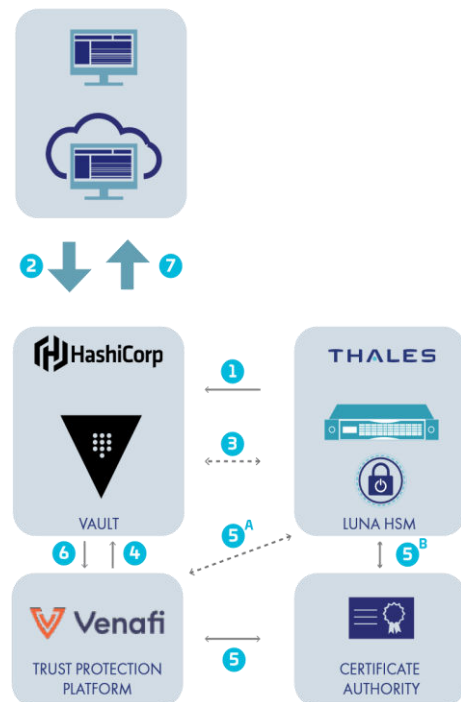
1. Thales Luna HSM autonomously unseals the HashiCorp Vault.
2. The DevOps team submits a request to Vault for a machine identity for a new application.
3. Utilizing the advanced entropy provided by Luna HSM, Vault generates a private key pair.
4. Vault then formulates a Certificate Signing Request (CSR) and forwards it to the Venafi Trust Protection Platform (TPP).
5. TPP sends the CSR to the Certificate Authority (CA) for fulfillment and returns it to TPP.
 - Luna HSMs offer master key protection for the TPP database.
 - Luna HSMs provide a secure root of trust protection to leading CAs.
6. Vault retrieves the certificate from TPP.
7. During the CI/CD build process, the new machine identity is retrieved from Vault and installed on the application.
8. Throughout this process, Accutiv Security's data discovery and masking product works seamlessly, contributing towards the secure and compliant execution of DevOps operations. Furthermore, Accutiv's professional services for Thales, Venafi, and HashiCorp ensure that each stage of the workflow is optimized and secure, reinforcing the end-to-end trust and security of the integrated DevOps solution.

Key Features and Benefits

- Thales HSMs, available in on-premises, hybrid, and cloud-based options, ensure the security of your critical encryption keys and digital identities by managing and storing them in a certified root of trust HSM.
- Thales HSMs address compliance needs efficiently and economically, boasting a broad range of industry certifications including FIPS 140-2, Common Criteria, eIDAS, GDPR, ITI, Singapore CC NITES, and more.
- Venafi effortlessly connects CAs to the tools developers use, offering secure and compliant certificates. It automates the lifecycle of keys and certificates while maintaining the rapidity and efficiencies of the DevOps Agile development process.
- HashiCorp Vault allows the use of native commands for certificate requests, while ensuring full compliance with corporate security and audit policies.
- HashiCorp Vault PKI simplifies the distribution of TLS certificates, enabling users to generate PKI certificates with a single command or through a fully automated process.
- Accutiv Security enhances the solution with its data discovery and masking product, along with professional services for Thales, Venafi, and HashiCorp. By providing additional security and compliance layers, Accutiv's contributions aim to bolster this integrated DevOps solution, ensuring all components cooperate seamlessly for a safer, more efficient DevOps environment.

In Summary

Choosing a thoroughly integrated and tested DevOps solution from four industry-leading companies like Thales, Venafi, HashiCorp, and Accutiv Security allows organizations adopting DevOps practices to establish controls and processes endowed with the security, reporting, and auditing features necessary for an enterprise-grade development program. By incorporating root of trust protection with a FIPS 140-2 Level 3 compliant Luna HSM, the application can satisfy global regulatory requirements while preserving the tools, speed, and flexibility offered by agile methodologies. Accutiv Security, with its expertise in data discovery and masking, along with professional services, further ensures that the solution meets all security and compliance benchmarks, thereby enhancing the overall robustness of the DevOps environment.



About Thales

The entities you trust with your privacy turn to Thales to safeguard their data. In the realm of data security, organizations are encountering an escalating array of pivotal moments. Be it constructing an encryption strategy, migrating to the cloud, or fulfilling compliance requirements, Thales is your reliable partner in securing your digital transformation journey.



About Venafi

Venafi is the frontrunner in the cybersecurity industry specializing in machine identity management and safeguarding machine-to-machine links and exchanges. Venafi assures protection for various machine identity types by managing cryptographic keys and digital certificates for SSL/TLS, code signing, mobile, and SSH. Serving the government agencies and the most security-sensitive organizations in the world, Venafi brings to the table inventive solutions that align with their unique demands.

About HashiCorp

HashiCorp stands at the forefront of multi-cloud infrastructure automation software. Their comprehensive software suite equips organizations to adopt uniform workflows for provisioning, securing, connecting, and operating any infrastructure for any application. HashiCorp's open-source tools - Vagrant, Packer, Terraform, Vault, Consul, and Nomad - enjoy widespread adoption among the Global 2000, with tens of millions of downloads each year. The enterprise editions of these products augment the open-source versions with features that encourage collaboration, streamline operations, enable governance, and facilitate multi-data center operations. The company, with its headquarters in San Francisco, is supported by esteemed backers including Mayfield, GGV Capital, Red point Ventures, True Ventures, IVP, and Bessemer Venture Partners



About Accutive Security

At Accutive Security, we are a trusted leader in Auth + Crypto solutions. Founded in California in 2009 by FinTech engineers and consultants, our expertise is focused on safeguarding essential data and software systems. Partnered with the world's leading Auth + Crypto companies, we deliver a comprehensive range of services and products to our mutual customers, including data discovery, data masking, key management, PKI management, certificate lifecycle management, hardware security module management, and more.

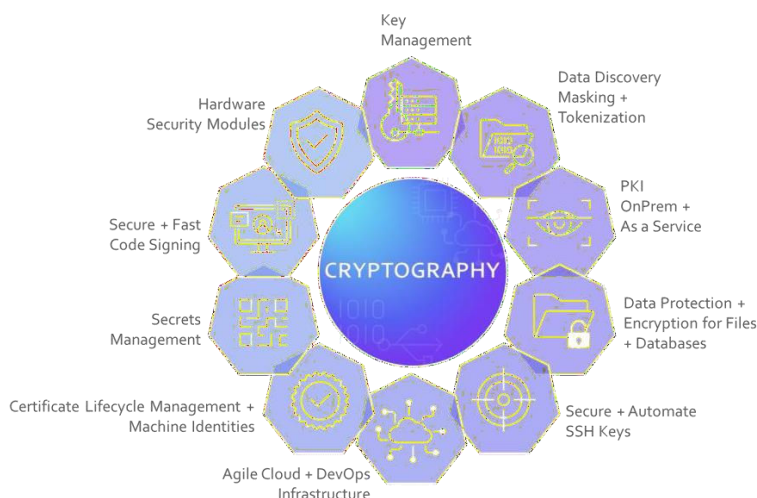
Our cutting-edge solutions are trusted by globally recognized organizations to protect their most sensitive data, regardless of its location. From cloud infrastructures to data centers, we ensure information remains secure and accessible. With our commitment to security, we empower organizations to confidently navigate their digital transformation and realize their full potential in a digitally connected future. Visit our website to learn more about our security solutions and services at <https://accutivesecurity.com/adm-platform/>

We are your Center of Excellence. Domain experts delivering

- Software engineering & professional services
- Strategic insights
- Effective training & research
- Deep experience
- Necessary solutions & products

Professional Services

Increase Security + Improve Operations



CONTACT INFORMATION

27068 La Paz Road, Suite 245 Aliso Viejo,
CA 92656

Toll Free 888.666.8315

[Contact Us](#)

<https://accutivesecurity.com/>



Accutive Security provides comprehensive information technology solutions which includes enterprise security; IT application development; systems integration; lending platform services; and professional services to clients in industries ranging from financial services, healthcare, technology, entertainment, and retail. Accutive Security is a specialized team of experienced professionals with years of industry, business, and IT expertise dedicated to developing IT solutions that exceed our clients' expectations.