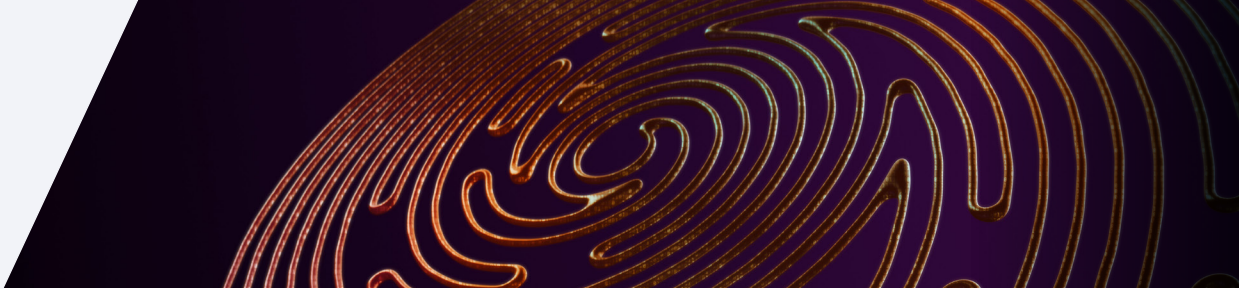
Venafi



SOLUTION BRIEF

Insert Machine Identity Management into DevOps Workflows and Automate Security

Accelerate access to policy-enforced certificates for DevOps by offering a certificate service compatible with automated workflows

Who should read this: InfoSec leaders who want to enable development and operations (DevOps) teams to use proper machine identity management policies and practices.

InfoSec teams are challenged with securing application software development. With fast delivery requirements, DevOps practitioners want to avoid security processes that can bog down development and delay production.

Digital certificates are critical to security, serving as machine identities that enable authentication and encryption for the many virtual systems and containers created by DevOps automation. Yet most organizations take days to procure a certificate, relying on manual certificate issuance and installation or the patchworking of homegrown processes.

Many DevOps teams seek ways to quicken this process, taking shortcuts that can create vulnerabilities or bypass the use of certificates entirely. For DevOps to embrace secure certificate processes, InfoSec must offer seamless certificate lifecycle management that inserts within DevOps builds, delivering policy-driven, effortless security.

The Disconnect: DevOps and InfoSec

DevOps has been fundamental in creating the exploding number of machines that support our current digital transformation. Virtual machines, cloud instances, containers and microservices can be spun up in seconds. InfoSec leaders working to protect machine identities have come to realize these three things:

- Unbridled DevOps projects often use unauthorize certificate sources and experience certificate related outages due to poorly managed keys and certificates.
- DevOps can't and shouldn't be slowed down if teams are to deliver on the promise of digital transformation.
- InfoSec teams need a way to make their certificate and key management policies and processes compatible with automated DevOps workflows.

Risks Created Without Team Alignment

DevOps teams must deliver quickly. When faced with a security practice that slows them down, they often take shortcuts or bypass security altogether. When DevOps teams skip issuing digital certificates, the risks are apparent—the machine-to-machine connections and communications for their IT services cannot be encrypted or authenticated as trusted systems.

However, shortcuts with certificate issuance also create vulnerabilities. These are some common shortcuts DevOps teams take:

- Creation of their own certificate authority (CA) to issue certificates.
- Use of CAs outside of policy.
- Use of improperly signed certificates.
- Not following practices for secure issuance, configuration or installation.

CISOs and CIOs know that DevOps practices tend to inspire the use of security shortcuts that weaken key and certificate usage. In fact, 79% of CIOs expect the speed of DevOps to make it more difficult to know what is trusted and what is not.[1] As the reliance on DevOps increases, the problem only worsens.

"Don't force information security's old processes to be adopted by DevOps developers. Instead, plan to integrate continuous security assurance seamlessly into the developer's continuous integration/continuous development (CI/CD) toolchain and processes. This is a significant mindset change for information security professionals accustomed to forcing developers to conform to our processes, so it will require several changes, such as never making developers leave their native toolchain environment. This means integrating your testing with their integrated development environment (IDE) and CI/CD toolchain tools."

MacDonald, Neil and Head, Ian. Gartner.
10 Things to Get Right for Successful DevSecOps.
3 October 2017 ID: G00341371

The Threat From Poor Certificate Practices

The following breaches and outages highlight the need for sound machine identity management strategies that safeguard the certificates and keys responsible for machine-to-machine authentication and encryption:

- Equifax 2017: A prime factor in the scale, severity and length of the Equifax breach was a failure to protect one machine identity. An expired certificate blinded security tools for months, transforming a manageable incursion into a catastrophe.[2]
- O2 and Ericsson 2018: In December of 2018, more than 30 million mobile customers of the U.K. company O2 lost network access and services. Ultimately, this was due to yet another expired TLS certificate.[3]
- Microsoft and Sennheiser 2018: In November 2018, Microsoft issued a security advisory warning that two applications by Sennheiser had accidentally installed root certificates on users' computers, and then leaked the private keys. Hackers could extract private keys from the applications, use them to issue forged certificates and spoof the identities of legitimate sites and services.[4]

In response to this, the need for strong policies to protect certificates and digital keys has driven new guidance. This is exemplified by NIST's recently released draft special publication, *Securing Web Transactions: TLS Server Certificate Management*.[5]

DevOps Machine Identity Management from Venafi

The challenge now becomes: How do we align emerging machine identity management policies with lean, fast DevOps practices? InfoSec and DevOps leaders need a machine identity management platform that is accessible through comprehensive APIs and has deep integration with existing DevOps toolsets and services. Venafi fully automates key and certificate provisioning as a central part of the DevOps environment. The Venafi API integrates with any DevOps platform—such as Kubernetes, Ansible, Chef and Terraform—ensuring that key and certificate policy enforcement, access control, workflow processes and audit logging are all part of the automated build process. The Venafi Platform also supports the broader DevOps ecosystem through native integrations with over 1,000 applications and common APIs.

InfoSec and PKI leaders have long relied on Venafi to establish, assure and manage policies for the appropriate protection of machine identities. This policy enforcement can be extended to DevOps using just a few lines of code in the automated build processes, managing this usage and providing the same level of assurance that internal PKI teams require—without interrupting automated workflows or adding burden to DevOps processes.

InfoSec teams need to "leverage automation lessons from DevOps... as infrastructure becomes increasingly software-defined and administrators evolve into becoming developers, they can leverage some of the same tools and processes that drive development and operations (DevOps) efficiency."

Gardner, Chris; Blankenship, Joseph; and Cunningham, Chase. Forrester. Reduce Risk And Improve Security Through Infrastructure Automation June 22, 2018.

Venafi Platform

Inventory	Policy Controls
Audit and Reporting	Automation Workflows
CA Connectors	Agentless Drivers

Venafi Platform for Visibility, Intelligence, and Automation for Machine Identities

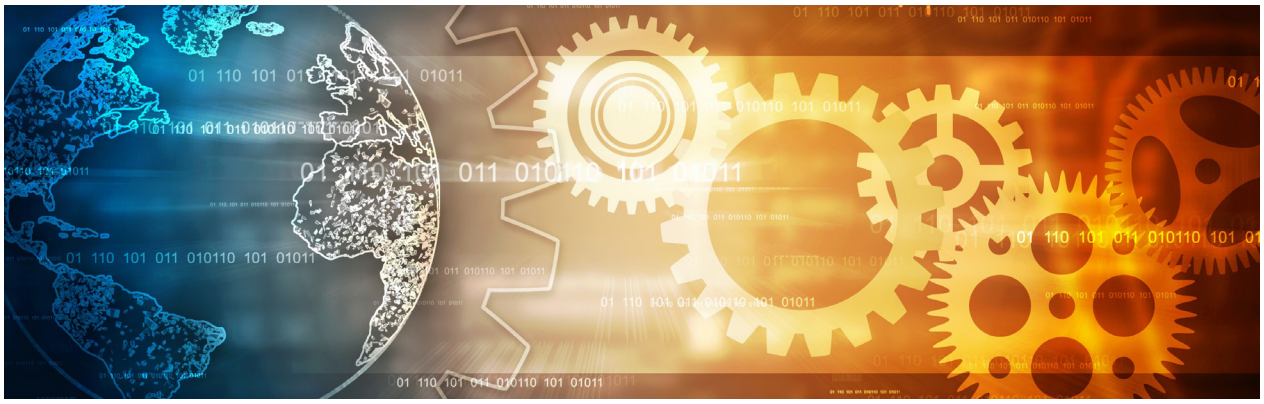
Integrations and Supporting Services for Embedding Certificates ito DevOps Workflows

DevOps Integrations

CHEF · openstack. · kubernetes · RED HAT ANSIBLE · RED HAT OPENSHIFT · JETSTACK · SALTSTACK · urban{code} · docker · HashiCorp Terraform · HashiCorp Vault · HashiCorp Consul

VCert	Venafi API	ACME
SDK in Go, Python, Java, Ruby Command Line	REST API / SDK	Venafi ACME Service

DevOps Tooling Integrations



But how does Venafi machine identity management align with DevOps practices? Venafi supports the new DevOps "shift" model. "Shifting Left" means moving practices earlier in the development process to allow teams to focus on quality, to work on problem prevention—instead of detection—and to begin testing earlier. "Shifting Right" means taking processes that typically happen before application release and moving them into production. This allows teams to catch post-release issues before end users notice them, allowing for continuous assessment and testing, even in production.

Venafi integration supports both shifting left and shifting right. When shifting left, the Venafi Platform can test machine-to-machine authentication systems earlier and ensure the robustness of keys and certificates before they are deployed by orchestrating TLS certificate expiry dates, certificate ownership and certificate use, as well as policy enforcement of key length, algorithm type and CA usage.

When shifting right, the Venafi Platform goes beyond policy-enforced provisioning of keys and certificates to support the full life cycle—including renewal, replacement and revocation—per policy. Venafi real-time assessment protects the same kind of machine identities that failed at Equifax, O2 and Microsoft. Instead of the "set and forget" approach to creating machine identities, the same rigor is applied to their life cycles as is applied to vulnerability assessment, application monitoring and configuration management.

DevOps Can Automate Certificate Requests for

Traditional Infrastructure
- Servers
- Load Balancers

Modern Infrastructure
- Containers
- Service Mesh
- Serverless
- IaaS

Located in
- Physical Data Centers
- Virtual Data Centers
- Hybrid Cloud
- Public Cloud

And from within CI/CD Pipelines, across all environments

Development | **Test** | **Staging** | **Production**

Test Only Certificates — Internal and Externally Trusted Certificates

When provisioning keys and certificates becomes part of the automated build process, DevOps teams can significantly reduce IT service delivery time. In a third-party survey, over half (57%) of Venafi customers used the Venafi Platform to improve their SLAs for internal IT services, and over one-third (34%) were able to change their SLAs from days to just hours. By empowering your developers to comply with corporate policies without delaying development, Venafi helps your DevOps teams excel at both security and agility.

Visit **venafi.com/DevOps-Solutions** for more resources and product info.

References

1. Venafi. 2016 CIO Study Results: The Threat to Our Cybersecurity Foundation. 2016.
2. U.S. Government Accountability Office. Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach. GAO-18-559: Sep 7, 2018.
3. Reichert, Corinne. ZDNet. Ericsson: Expired Certificate Caused O2 and SoftBank Outages. December 8, 2018.
4. Cimpanu, Catalin. ZDNet. Microsoft Warns About Two Apps That Installed Root Certificates Then Leaked the Private Keys. November 28, 2018.
5. National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide Special Publication (SP) 1800-16, Securing Web Transactions: TLS Server Certificate Management. Draft open for public comment through December 31, 2018 (Delivery of final version anticipated in Spring 2019).

Trusted by

5 OF THE 5 Top U.S. Health Insurers
5 OF THE 5 Top U.S. Airlines
3 OF THE 5 Top U.S. Retailers
3 OF THE 5 Top Accounting/Consulting Firms
4 OF THE 5 Top Payment Card Issuers
4 OF THE 5 Top U.S. Banks
4 OF THE 5 Top U.K. Banks
4 OF THE 5 Top S. African Banks
4 OF THE 5 Top AU Banks

Venafi is the cybersecurity market leader in machine identity management, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access. **To learn more, visit venafi.com**