DATA SHEET

// Venafi Cloud DevOpsACCELERATE

Automatically enforce certificate policy and connect trusted certificate authorities to DevOps tooling

Venafi Cloud DevOpsACCELERATE at a Glance

Venafi Cloud DevOpsACCELERATE™ is a SaaS solution that centralizes and standardizes policy controls for SSL/TLS certificates by baking them directly into DevOps tooling.

DevOpsACCELERATE provides an easily consumed, common service for certificates via an API that is integrated with a broad range of DevOps tooling out-of-the-box. It improves security and availability by standardizing and centralizing certificate workflows. As a result, businesses are able to accelerate software development and reduce complexity.

Benefits

- Delivers policies-as-code to increase developer productivity
- Automates consistent certificate workflows, improving agility and speed
- Enhances security and flexibility across multicloud and hybrid environments

Challenges

Digital SSL/TLS certificates serve as machine identities for authentication and encryption. As DevOps dramatically increases the number of machines (including virtual machines, service mesh and containers), the need for a standardized approach to certificates becomes essential. When DevOps teams use inconsistent solutions for certificates, it increases complexity and creates lock-in to DevOps tooling and cloud providers. This often results in the use of rogue certificates, unauthorized certificate authorities (CAs) and application downtime caused by poorly configured or expired certificates.

Until now, the process of incorporating trusted certificates into DevOps environments has been slow and complicated. As a result, organizations adopting cloud services and containers have increasingly had to choose between agility and security. Developers spend valuable time either creating security infrastructure or waiting for certificates, both of which delay innovation.

Inefficient Use of Developer Time

Because corporate certificate issuance processes are too slow, application development teams often build custom solutions for certificates. This introduces complexity and heterogeneity across environments—from development and testing to production—and in individual applications. Because all custom code must be tested and maintained, this approach creates a burden on developers and slows down software innovation.

Cloud Lock-In

Most organizations develop applications in a way that is not cloud-agnostic. This approach makes it impossible to run workloads across more than one cloud provider without having to recreate the application or underlying security layers. Even though this problem is well understood, most organizations still rely on built-in certificate offerings from cloud providers.

Negative Compliance Findings

Because of the critical security role machine identities play, they are increasingly subject to policies and regulations that specifically focus on certificate management and protection. However, auditors often find that organizations lack visibility over both certificates and their configurations, and this in turn leaves them short on the intelligence needed to enforce certificate policies in modern applications. Unwelcome audit findings are often the result.

Outages

With the increase in encryption use, the explosion in the number of devices, availability of free certificates and shorter certificate lifecycles, the complexity of managing certificates continues to increase. Without sufficient controls in place unexpected certificate expirations often result in outages. When a certificate is installed on more than one system, the certificate needs to be replaced everywhere it is used and before it expires. Unfortunately, many large organizations don’t have visibility into all of their certificates or intelligence about all locations where they are installed.

No Crypto-Agility

Most organizations lack the ability to quickly replace digital certificates in response to business and security events such as CA compromises, vulnerable algorithms or cryptographic library bugs. Even with advance notice, most organizations are not able to replace certificates quickly and reliably.

The Solution:
Venafi Cloud DevOpsACCELERATE

DevOpsACCELERATE delivers a common service for certificates via an API that is integrated with DevOps tooling. This easily consumed solution improves security and availability, ensures compliance, and accelerates software development by reducing complexity.

Enterprise Security at DevOps Speed

DevOpsACCELERATE defines and enforces enterprise security policy for issuance and use of TLS-certificates-as-code with prebuilt DevOps tooling and cloud provider integrations. Supporting services—such as a well-documented API, VCert utility, and SDK and ACME servers—provide added flexibility to incorporate a common service for any application or CI/CD pipeline.

Regulatory and Policy Compliance

DevOpsACCELERATE improves regulatory and policy compliance through automated intelligence and visibility into the technical and procedural controls in place, ensuring TLS security across the hybrid enterprise.

Flexibility and Crypto-Agility

DevOpsACCELERATE provides security teams with a single point of control to quickly and rapidly change TLS certificate configuration parameters and policies, as well as CAs/sources to meet changing business needs. With a single lever, security teams can change cryptographic parameters without impacting application development teams or the underlying applications.

69% of surveyed IT professionals agree that policy enforcement with Venafi automation helped improve security.

Large Enterprise Transportation Services Company

Source: TechValidate. TVID A58-783-4E2

Centralized Security Policy Definition and Enforcement	
Define and Enforce Policies	• Define and configure certificate policy in a common location, including key length, CAs, validity period, etc. • Automatically enforce policies and restrict certificate creation and configuration to authorized sources. • Lock policies to govern certificate usage by application and environment.
RBAC	• Apply a least-privileged access model and set granular permissions for roles and access. • Use a web-based UI for establishing users, groups and workload-specific policies.
Certificate Authorities	• Connect to third-party CAs to streamline certificate enrollment from automated DevOps workflows. • Request internal certificates from the DevOpsACCELERATE built-in CA.

Improved Security, Availability and Compliance	
Visibility	• View issued certificates to demonstrate due care for compliance audits by application and environment with application-specific certificate dashboards. • Get single pane-of-glass visibility into all issued certificates to meet audit and compliance requirements. Filter by: • Domain name • Issuer • Owner • Key strength/type, hash algorithm and validity.
Certificate Lifecycle Automation	• Automate certificate lifecycles for certificates in Kubernetes and OpenShift clusters. • Automate certificate management for external-facing infrastructure, such as load balancers, with the Venafi ACME server.
Expiration Tracking	• Associate certificates by application and environment in order to optimize prevention and remediation actions. • Track upcoming certificate expirations using the web interface and receive expiration alerts via email.

Easy for Development Teams to Adopt and Use	
Recipes and Sample Code	• Use recipes and sample code provided in the web interface to speed adoption and integration. • Use a common framework for certificates across environments, applications and cloud providers to reduce complexity and enable cloud and crypto-agility.
DevOps Tooling Integrations	• Use prebuilt open source integrations for the modern application stack. • Scale certificate issuance as part of CI/CD pipelines. • Secure modern infrastructure like containers and microservices to harden applications in zero-trust environments with prebuilt integrations. • Request policy-compliant certificates from third-party CAs and built-in CA with native integrations for: • Kubernetes (supports auto-renewal with Jetstack cert-manager) • OpenShift (supports auto-renewal with Jetstack cert-manager) • Docker • SaltStack • Ansible • Terraform • Vault (also supports policy enforcement for Vault-issued certificates) • OpenStack • Pivotal • CredHub • Chef Infra and Chef Habitat • And more
Cloud Provider Integrations	• Obtain certificates from leading CAs and deploy them directly to Azure Key Vault and Azure web apps. • Use AWS Private CA for certificates while complying with policy and audit requirements.
API, VCert and SDK	• Use the REST API to request certificates, review certificate issuance policies, view issued certificates and push certificates directly to Microsoft Azure web apps as well as many other applications. • Generate keys to simplify certificate issuance by using VCert and eliminate the need to write code that interacts with the Venafi REST API. • Allow application developers to integrate key generation and certificate management tasks into custom applications with VCert SDK, a cross-platform software development kit written in Go, Java, Ruby and Python.

Venafi Cloud DevOpsACCELERATE

Venafi Cloud DevOpsACCELERATE was designed from the ground up to allow developers to get their TLS certificates from a single place. It also works seamlessly with many of the tools that they use today. For security teams, DevOpsACCELERATE provides centralized visibility into certificate issuance, policy enforcement and control over which CAs issue certificates.

By taking control of the certificate management process, organizations can prevent outages and, at the same time, provide developers with the flexibility to get certificates quickly without disrupting existing workflows.

DevOpsACCELERATE makes it easy to increase the speed of secure development:

- **SaaS Delivered**
  No hardware or software required
- **Open Source**
  Prebuilt integrations for modern application stacks
- **Consistency**
  Easy-to-use sample code and recipes
- **Portability**
  PKI that works across environments
- **Outage Prevention**
  Reporting and expiration tracking
- **Compliance**
  Smart policy enforcement and visibility

As a solution built for DevOps and designed to deliver improved security, DevOpsACCELERATE automates compliance for application development teams without slowing down existing workflows.

Next Steps

Are you using trusted certificates for your applications? Venafi Cloud DevOpsACCELERATE can simplify certificate workflows for DevOps environments and ensure that your certificates comply with policy through a common service that's automatically integrated. Give it a try and start your 30-day free trial today.

To learn more, visit **venafi.com/cloud**

Trusted by the Top

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

About Venafi

Venafi is the cybersecurity market leader in Machine Identity Protection, 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/cloud