

CASE STUDY

Tech Customer Secures DevOps Machine Identities and Helps Developers Work Faster

Challenge: Outages caused by application teams

A longtime technology customer that owned the Venafi Platform for many years started to experience a rash of SSL/TLS certificate-based outages after launching several digital transformation initiatives. When Venafi experts met with the company's InfoSec team, they learned the reason behind the problem: Application development teams were going around the certificate infrastructure InfoSec had established and using SSL/TLS certificates from certificate authorities (CAs) that weren't approved by corporate policy. As a result, the InfoSec team had no visibility into when these certificates were issued or when they expired.

InfoSec had tried to talk with the application teams—even briefly to the head of application development—but as in many companies, the two sides had no idea how to talk to each other. Developers saw InfoSec as the voice of “no,” and assumed Venafi was yet another security platform that would gum up their DevOps pipelines. Meanwhile, InfoSec, for their part, didn't understand, let alone have any influence, over the platforms and tools that DevOps teams were using or how to best automate DevSecOps.

Moreover, InfoSec knew that everyone in the company rightly saw the application teams as primary revenue generators, building apps and services that were the driving force of the organization's digital transformation strategy. And although InfoSec knew Venafi could help, they just weren't sure how. “Frankly, we've been feeling like crazy uncles screaming into a void,” one InfoSec manager said. “We just don't understand how Venafi fits into their CI/CD pipeline.”

Solution: Venafi DevOps Expertise

The customer turned to Venafi's professional services organization to seek help. Venafi offers a holistic way to deal with CI/CD, including:

- Ready-made blueprints, templates and patterns for popular DevOps tooling and processes
- Extensive out-of-the-box integrations between leading DevOps, cloud and security technologies
- Single-vendor support of integrations
- Deep professional services expertise for strategy and implementation of DevSecOps

The customer appreciated the comprehensiveness of the Venafi solution; however, its most immediate selling point was the expertise Venafi's Professional Services (PS) team could provide in bridging the communication gap between InfoSec and developers. In effect, Venafi could act as translator between the two sides so that each could see, from their unique perspectives, how the Venafi Platform could make them more secure and faster at the same time.

Translating value in language both InfoSec and developers understand

InfoSec understood intuitively that developers needed to work fast and that existing security processes were continual roadblocks to their progress. In a series of workshops, Venafi went from giving InfoSec a big-picture overview for best practices and DevSecOps strategy to low-level technical implementation plans for integrating the tools that DevOps teams were already using.

During the initial InfoSec workshop, Venafi showed how the Venafi Platform would secure machine identities in this new world of fast app creation. For one thing, Venafi's prebuilt integrations with HashiCorp Vault, the developers' preferred certificate creation tool, enabled developers to use HashiCorp just as they always have. The only difference was that Venafi worked under the hood enforcing such policy parameters as limiting certificate issuance to corporate-approved CAs, automating and validating certificate lifecycles and giving InfoSec centralized visibility into what application teams were doing with machine identities. The InfoSec manager was floored. "It was almost too easy. The only thing that made it seem like it wasn't a pipe dream is that there's always at least a little work involved setting up integrations—although Venafi helped us with that every step of the way," he said.

Venafi makes application teams faster

The attendees of the first developer workshop were skeptical at best. They couldn't see how using Venafi to get their certificates, rather than OpenSSL or Let's Encrypt, would do anything but slow them down. But as Venafi described that developers could use Vault and the rest of their toolset to issue certificates, the attendees listened on. They finally understood that the Venafi Platform comes with hundreds of out-of-the-box API integrations for commonly used DevOps tools, including HashiCorp Vault. Not only would the Venafi Platform not disturb their work, it would make the entire certificate lifecycle easier to deal with than they could have anticipated.

With Venafi, they could issue publicly trusted certificates without having to do any custom coding, while at the same time, InfoSec would have visibility into all certificates issued. To prove his point, the Venafi team member set up a workshop that

included a demo to let them see for themselves. The attendees were impressed that they could better manage their certificates using Venafi than with the templates they had been building for that purpose.

The workshop also went over the many out-of-the-box integrations Venafi provides for a host of DevOps tools, including all three major cloud providers (AWS, Azure, GCP), OpenStack, Ansible Role and Pivotal Cloud Foundry; it also worked seamlessly with Kubernetes using Jetstack cert-manager. Said the PS team member leading the workshop: "Venafi's belief is that, if it can work in the Platform, it can work through our API," adding that all prebuilt integrations are vetted, validated and supported by Venafi.

The team member went on to say that Venafi's goals, through its blueprints and integrations, is to make it easier than ever for DevOps teams to integrate all their technologies. No longer do they have to search for or build any security infrastructure each time they start using a new technology or switch to a different CA or cloud provider. An application developer who attended the session said, "I can help with network security by ignoring it entirely? Count me in!"

Venafi: Bringing InfoSec and DevOps together

Subsequent workshops started bringing in developers and InfoSec people to strategize the blueprints and come up with best practices as they moved forward with digital transformation strategies. There were still times when communication broke down between InfoSec and developers—but Venafi was always there translating as needed. Said one InfoSec team member: "Our relationship with app development has transformed from a cage match to a dance. Venafi taught us how to be a good partner."

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**