Venafi

CASE STUDY

Manufacturing company returns to Venafi after ill-fated switch to low-cost competitor

Challenge

A manufacturing customer purchased the Venafi Platform but was not actively using it when the InfoSec team lead had a proposal: Why use Venafi when a low-cost competitor appeared to offer the same functionality for a fraction of the price?

This proposal appealed to the firm's senior leadership, especially once the CISO backed it. The company was planning to launch several digital transformation initiatives, including the migration of a large portion of their infrastructure to the cloud and increased adoption of IoT devices. As part of this initiative, the organization was seeking ways to trim their operating budget wherever they could. Switching to a bargain machine identity management solution, which promised the same results, seemed a painless way to free up funds for these important projects.

Initially, this low-cost platform appeared to be effective, discovering certificates and providing intelligence about them. Some of the company's app developers grumbled that the bargain vendor's API was not robust enough to automate certificate management using their preferred toolsets. But the CISO chalked it up to the inevitable adjustments that happen when switching solutions.

Then in early 2021, the company suffered an outage that shut down part of their manufacturing floor for several days. Initially, the company thought the outage was caused by a hardware failure or a misconfiguration. After losing several million dollars in revenue, the company finally found the culprit: an expired, rogue Let's Encrypt certificate. An IT admin had procured the certificate; he knew development teams were using Let's Encrypt to save time, so he decided to do the same. The problem was that the bargain platform failed to discover the unauthorized certificate before it expired.

Realizing that there likely were more undiscovered Let's Encrypt certificates on the network, the company feared there were more serious outages on the horizon. The company contacted the bargain vendor's customer support team for help. But getting help to remediate the problem was next to impossible. In addition to language barriers, the bargain vendor's offshore support team was unable to discover unauthorized certificates consistently enough to solve the overarching visibility problem.

Solution: Venafi Platform

The outage inflicted serious, long-term financial and reputational damage, forcing the company's executive team to act. First, they fired the CISO and the InfoSec team lead for pushing the ill-fated switch. Then the CIO reached out to the Venafi team for help.

He told the Venafi sales team that the company needed comprehensive discovery of their entire certificate inventory as soon as humanly possible. Two days later, the Venafi support team was onsite and working. Venafi discovered more than a dozen Let's Encrypt certificates throughout the network—including one on a critical manufacturing machine that would expire inside a week—and helped the firm replace it before another devastating outage could occur. They also immediately replaced all the Let's Encrypt certificates with new certificates from the company's approved certificate authority (CA).

Because eliminating outages was the company's top priority, Venafi recommended the customer follow the VIA Venafi program, which provides a step-by-step methodology that combines people, process and technology to completely eliminate outages.

VIA Venafi includes a "No Outage Guarantee," which appealed to an executive leadership team spooked by the consequences of the recent outage.

In addition to this project, the customer wanted better direct integration with DevOps toolsets, direct integration into ServiceNow, and discovery and management of the certificates being used in their IoT devices. The Venafi team assured the customer they could solve all these challenges.

Eliminating Outages

Using the eight-step VIA Venafi methodology, Venafi helped the customer create enterprisewide machine identity management policies. These policies encompassed such best practices as limiting certificate procurement to approved CAs, as well as required configurations for key lengths, algorithms and expiration dates. Then Venafi set up automated enforcement of these policies. Now, if anyone tries to procure a certificate from an unauthorized CA like Let's Encrypt, the certificate is automatically removed and replaced.

Then the Venafi team automated machine identity lifecycles from procurement to retirement using a "certificates-as-a-service" approach that made it possible for anyone to quickly access compliant certificates from within the customer's ServiceNow implementation—no specialized PKI knowledge required.

Helping developers work fast while staying in compliance

The Venafi support team then focused on helping the company's developers stay in compliance with the firm's machine identity policies without slowing them down. The company was moving application development into AWS, and Venafi's powerful API made certificate procurement in this environment easy to accomplish. Moreover, Venafi's robust ecosystem enabled direct integrations to a wide range of developer toolsets, including HashiCorp Vault, Ansible, Istio and Kubernetes with the help of Jetstack cert-manager.

Venafi provided the company's development teams with ready-made blueprints, templates and patterns for popular DevOps tooling and processes, and showed them where they could find more on GitHub. And when the teams had questions, Venafi's customer support team, which had the technical depth and expertise to support both developers and InfoSec, troubleshot with them until the issue was resolved.

A machine identity management platform for now and tomorrow

In addition to helping the firm address their immediate machine identity challenge, Venafi spent the time necessary to partner with the firm to build a vision for the future of their machine identity management strategy. Working together, Venafi and the customer defined how the entire lifecycle of TLS certificates used by IoT devices could be automated from server to device. This ensures that sensitive data remains protected and that the IoT certificates could be managed in the same way as all other machine identities.

Venafi also showed the customer how they could reduce risks posed by the SSH keys used by their robots and other IoT devices. Adding SSH Protect to their Venafi implementation would give them a complete inventory of their SSH keys, so they could easily remove those that were no longer being used. In addition, SSH Protect could automate management of the entire SSH key lifecycle, thereby removing potential backdoors that could be exploited by SSH malware that has become increasingly popular with cyberattackers. The customer plans to deploy SSH Protect in 2022.

Said the CIO after returning to Venafi: "We learned an expensive but important lesson: When it comes to machine identities, it's more cost-effective to get a solution and a partner that really solves these critical security problems. And Venafi has proven to us that not only do they provide the best-in-class machine identity management offering, but they also understand—and are anticipating—our future challenges. I can't think of a better partner to have going forward."