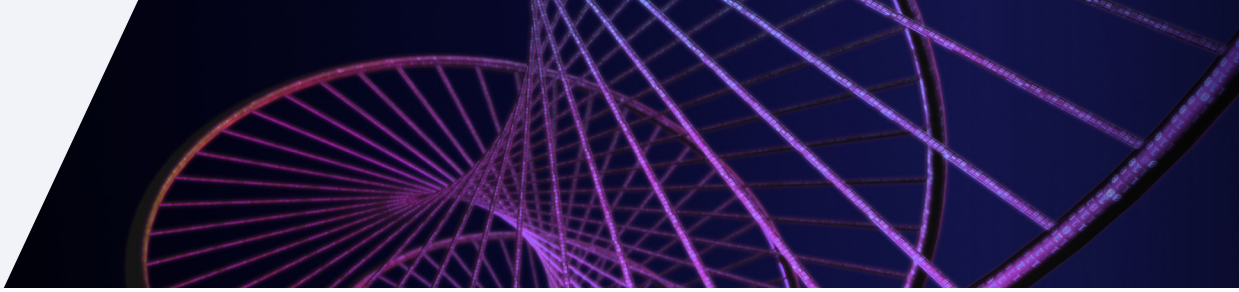
Venafi



CASE STUDY

Insurance Company Eliminates F5-Based Outages; Automates TLS Certificate Lifecycle Across Their Enterprise

Challenge: Outages caused by expired F5 SSL/TLS certificates kicks customers off insurance plans

A large health insurer was already struggling with certificate outages when the unthinkable happened. Their primary mobile app—the one their customers use to find doctors, manage claims and pay deductibles—went down over a holiday weekend. The PKI team discovered the root cause—an expired F5 certificate where the app was being hosted—but not before several customers, unable to pay their deductibles, were accidentally kicked off their insurance plans.

This was not a new problem for the organization. The F5 team had complained about having to wait for InfoSec to issue and renew certificates for a long time, and this incident was their "I told you so!" moment, the senior manager of InfoSec explained.

Despite the obvious problems resulting from this latest outage, the manager hoped the incident would provide the urgency needed to solve this problem. She used Venafi at a previous company and felt her superiors would finally see how essential the Venafi Platform was for securing machine identities *and* for business continuity. "We needed insight into all our TLS certificates, not just our F5s—and we needed to automate certificate management across our enterprise. This problem affected everyone, and we can't keep pretending it's 2013," she said.

Solution: Venafi TLS Protect for F5

Venafi's POC started with a scan of the insurer's entire TLS certificate inventory. This scan found three times the number of certificates as competing vendors. Venafi then showed how TLS Protect uses automation to continually discover certificates, both on-premises and in the cloud, giving InfoSec near real-time visibility into the organization's complete inventory.

Despite these insights, the F5 team was skeptical about trusting their TLS certificates to a third-party platform. After all, F5s were critical business infrastructure. If even a single F5 went down, business continuity suffered, and the company couldn't afford another outage like the last one, especially during the COVID-19 pandemic. "What if a gravely ill customer isn't seen by a hospital because it looked like their insurance had lapsed?" said the manager. "Venafi would have been a no-go if they couldn't support our F5s."

Venafi showed the InfoSec and F5 teams how TLS Protect was literally built into F5's BIG-IQ management platform. BIG-IQ could automate and orchestrate TLS keys and certificates across F5 BIG-IP load balancers using TLS Protect, including the automation of certificate provisioning and renewal for BIG-IPs. In addition, TLS Protect offered tons of out-of-the-box integrations specifically for F5, including several that increased scalability by automating access controls and improved security by identifying all machine identities associated with F5s.

To help smooth the integration of TLS Protect, Venafi recommended adding an F5 automation Professional Services package designed to help deploy the F5-specific portion of TLS Protect within a few weeks. The manager appreciated that the pricing of this PS offering was outcome-based—the cost of it was fixed, no matter how long it took to get TLS Protect integrated with their F5s. The package ensured the team would eliminate F5 outages completely. "This package enabled us to reach this desired outcome ASAP," the manager said.

Eliminating F5 outages while cutting F5 certificate provisioning from days to minutes

The Venafi team worked with the InfoSec and PKI teams to set up automatic discovery of F5 TLS certificates. Then Venafi showed both teams how easy it was to access intelligence about their certificates, including the issuing CA, the owners of the applications and servers with installed certificates, how they were being used and when they would expire. The tight integrations between TLS Protect and F5 BIG-IQ meant that TLS certificate lifecycles could be completely automated, from certificate issuance through renewal and installation.

Then Venafi F5 experts helped the F5 team automate these processes. Instead of having to perform a series of manual actions as they had needed to previously, TLS Protect used API calls and other processes to automate downloading the Certificate Signing Request (CSR), the signing of the certificate by the approved CA and the uploading of the signed certificate. The F5 team cut certificate provisioning from days to minutes.

"In six months, we eliminated F5 outages across the organization. And our F5 guys now can procure certs on their own," the manager said.

F5 automation leads to CaaS template for onboarding of other teams

Although automating certificate lifecycle management for F5s was the insurer's primary goal, the experience also served the senior manager's long-term goal of automating certificate management across the entire enterprise. The company could now use their experience automating certificate lifecycle management of their F5s as a template for a certificates-as-a-service initiative that could be repeated across the organization.

The out-of-the-box integrations that came with TLS Protect covered almost every part of the company's entire tech stack, including internal IIS certificates. TLS Protect also worked seamlessly with a wide range of app development toolsets like Kubernetes, Jenkins, Vault and Ansible. Now InfoSec could set and implement certificate policy for dev teams without slowing them down because the teams could work within their preferred toolsets.

Automating for business continuity and security

In addition to stopping outages and maintaining business continuity, InfoSec discovered additional security benefits that TLS Protect could supply. Because TLS Protect provided unparalleled visibility and intelligence into the company's entire TLS machine identity inventory, InfoSec could now proactively respond to the myriad security threats that TLS keys and certificates might cause—and leverage TLS Protect's automation capabilities to head off a potential problem.

For example, if a TLS certificate didn't conform to the organization's corporate policies, TLS Protect would automatically revoke it. Similarly, it could remove rogue certificates, manage crypto-agility events, such as when a browser no longer trusts certificates from a certain CA, and protect rapidly growing certificate populations in the cloud. TLS Protect even kept logs and generated reports so that the organization could provide proof of effective machine identity management for security audits.

In fact, TLS Protect has been so effective in solving the many problems the insurer faced, executive management is now considering purchasing more parts of the Venafi Trust Protection Platform, including SSH Protect and CodeSign Protect. And the company CISO was so pleased by the transformation brought about by TLS Protect, he promoted the senior manager to director.