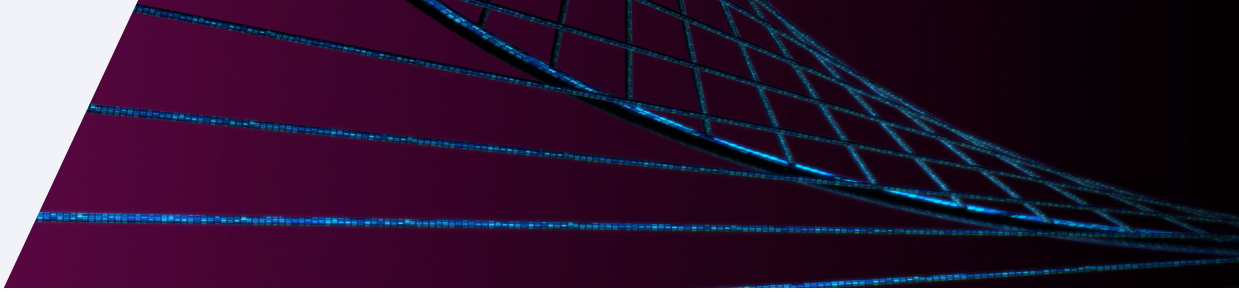
Venafi



CASE STUDY

TLS Protect Cloud stops TLS certificate outages for technology company

Challenge: Siloed management of TLS certificates fueled frequent outages

A fast-growing technology services company had a challenge that no longer could be ignored: outages. In the previous year, the company experienced 27 P1 outages. And the aftermath was painful—bringing down the company's email server for more than a day and preventing customers from accessing their software knowledge base for several hours. Not surprisingly, the downtime and financial losses caused by these outages was unacceptable. Moreover, this jump in outages was 100% greater than the previous year. The company realized that if they wanted to scale successfully, they needed to gain control over how they managed TLS certificates across their enterprise.

An internal audit, led by the chief network architect, uncovered the nub of the problem: The company lacked any sort of coherent TLS machine identity management strategy. The more organized business units used spreadsheets, calendar reminders or OneNote to manage certificates, but these methods not only lacked important details and data, but they would often be incomplete or have data entry errors.

As a result, the network architect found certificates in unexpected locations from a plethora of CAs (Certificate Authorities), including rogue CAs that developers stood up for limited use. The result was no consistency in certificate configuration, including encryption strength, and no central log or inventory for monitoring all these certificates. It was clear the company needed a comprehensive approach to machine identity management as soon as possible.

"If I could have hit the pause button on the company until this was taken care of, I would have," the network architect said.

The company needed to find a way to manage machine identities that accomplished three important goals: 1) discover certificates across the entire enterprise, 2) build a continuous inventory of these certificates and 3) document details including certificate ownership, location and lifespans. After that, they needed to establish a way to create and enforce enterprisewide certificate policies that standardized the way all users procure, access and renew their certificates.

Solution: TLS Protect Cloud

The company wanted a machine identity management solution that they could easily deploy and help them build a foundation for TLS certificate management. This solution would need to stop certificate-related outages while securing machine identities no matter how large the company scaled. They didn't want to be limited by a CA-based one because they wanted to enforce consistent policies across multiple CAs as well as any internal CA.

The company learned about TLS Protect Cloud from a developer who had tried the free TLS Protect Cloud trial and liked how easy it was to use. Venafi demoed TLS Protect Cloud for the company's decision makers,, showing how its single pane of glass provides visibility into certificates across the enterprise, including an interactive dashboard and filters showing which certificates were due to expire. The network architect was surprised how easily TLS Protect Cloud worked with both public and private CAs. And they were pleased to learn that the Venafi Customer Success team would help them set it up and establish processes using industry best practices.

In addition, TLS Protect Cloud provided a way to streamline management for the many internal Microsoft CAs that were draining PKI resources. The solution could pull in all private certificates, alerting owners when they were expiring, and issue compliant certificates for internal use without even needing to create a certificate signing request (CSR).

"Watching the demo, I saw a future where we could finally press play without worrying about outages," said the network architect.

Discovering certificates before they can cause outages

Immediately after TLS Protect Cloud was deployed across the company's network, the solution amassed a central TLS certificate inventory across all regions and business units, eliminating the siloed management that was contributing to all their outages. Moreover, TLS Protect Cloud performed validation to continuously check that certificates were properly installed and that the entire trust chain was healthy.

"Before we deployed TLS Protect Cloud, resolving an outage was a nightmare. We had to figure out if the certificate even existed, find where the server was located and document the server. It was impossible to build a complete inventory, let alone one that stayed up to date," explained the network architect. "TLS Protect Cloud does it instantly."

The network architect admitted he was astonished to learn that TLS Protect Cloud found three times as many certificates as the company had originally estimated. The previously unknown certificates came from a host of different CAs and self-signed certificates. In addition, TLS Protect Cloud showed the company the location of all their certificates, including wildcards that were being used in multiple unexpected places. Finally, TLS Protect Cloud enabled them to see which certificates were due to expire so that they could replace them immediately.

Setting up enterprisewide machine identity policies

The Venafi Customer Success team helped to operationalize continuous updating of the company's certificate inventory and assign owners to certificates to prevent future outages. Venafi next worked to set up a policy that applied industry best practices, which included creating policy templates and simplified workflows for certificate issuance, as well as assigning appropriate ownership. TLS Protect Cloud also allowed teams to effortlessly procure policy-compliant certificates that would optimize the reliability and security of applications. Automated Secure Keypair, a central TLS Protect Cloud feature, also made it easy for users to generate a private key and keep it safe from compromise within TLS Protect Cloud.

TLS Protect Cloud also enforced standards-based security policies for certificate attributes including validity length by application, minimum key strength and private key storage. The solution then verified security compliance by ensuring all newly issued certificates had proper ownership, attributes and configurations and were sourced from CAs that had been vetted and approved.

Said the network architect: "TLS Protect Cloud has transformed our business. We haven't had a single outage since it's been deployed. Not only have we been able to press play on running our business, but with the efficiencies that Venafi gives us, we can now press fast-forward on growth."