Venafi

CASE STUDY

Energy company prevents TLS machine identity misuse and compromise

Expired TLS certificate leads to damaging data breach

Last year, an energy company experienced a data breach. During the aftermath and resolution, a third-party digital forensics provider made multiple recommendations to reduce the risk of future breaches—one of which was to better manage TLS machine identities. The investigation had revealed that an expired certificate rendered a network traffic inspection device inoperative, enabling bad actors to stay inside the company's network undetected for an extended time.

The breach already had led to serious repercussions. A portion of the company's intellectual property was found on the dark web, including plans for future drilling operations. Company leadership was dismayed. Said the company's CISO: "This can't happen again under my watch—because if we don't fix this, I won't have a job anymore."

Their method of managing TLS certificates— a patchwork of tools from their primary Certificate Authority (CA) combined with spreadsheets—made them vulnerable to another data breach. Lacking visibility into their enterprisewide certificate inventory, they had missed the alerts warning about the expiring certificate. It didn't help that these alerts had gotten lost in the deactivated email address of an administrator who had left the company months earlier.

To prevent future incidents, the company researched several machine identity management providers including Venafi. Venafi pointed them to a **free TLS Protect Cloud trial**. They were up and running within minutes and immediately saw how quickly and easily TLS Protect Cloud could solve their challenges.

Solution: TLS Protect Cloud with a 'No Outage Guarantee'

The company was pleased that TLS Protect Cloud could spin up and discover certificates without having to install any data center software. But they were stunned at the solution's ability to identify all of the company's private- and public-facing certificates, no matter which CA the certificate originated from. TLS Protect Cloud quickly revealed several expired TLS certificates across the enterprise, as well as several that were about to expire.

"TLS Protect Cloud keeps an inventory of *all* certificates, no matter where they came from. CA-based tools simply can't do that," said the CISO.

But what put TLS Protect Cloud across the finish line was Venafi's philosophy in stopping outages, which includes changing people and processes, as well as deploying the technology itself. The company also purchased a Professional Services package to help them implement a methodology for machine identity management that would result in a "No Outage Guarantee." Said the CISO: "Venafi clearly had the expertise to make such a promise—and they could help us do so at a pace we couldn't have done on our own."

Building an Outage Safety Net

The first step was to build what Venafi calls an "Outage Safety Net," an enterprisewide alarm for expiring certificates. They helped the company identify key teams, processes and data points so that whenever a certificate was about to expire, the appropriate people would be alerted to mobilize a coordinated response.

And Venafi helped the company get an outage safety net up and running within a month. "Having this capability gives us a lot of breathing room to set up consistent outage prevention," the CISO said. "And we dodged a lot of bullets in the process."

Making TLS certificate management consistent and reliable

Venafi next aligned the enterprise organization around a service-based approach. Using best practices based on NIST 1800-16B and Venafi's experience helping other companies do the same thing, Venafi helped the team define policies and codify roles and responsibilities across the company. NIST 1800-16B provided guidance on appropriate TLS key lengths and signing algorithms, defining operational and security policies specific to TLS keys and certificates, reporting for audit purposes and limiting certificate procurement to authorized CAs, among many other things. Venafi set up TLS Protect Cloud to automate enforcement of these policies and processes.

In addition, Venafi showed all the areas that were prime candidates for TLS Protect Cloud automation, including keeping an accurate inventory of all deployed certificates, tracking ownership of these certificates, revoking ownership of reassigned or terminated employees using the principle of least privilege, and streamlining vulnerability remediation. Moreover, TLS Protect Cloud enabled automation of the TLS certificate lifecycle, from procurement and issuance to renewal and revocation, so that these processes became consistent and reliable.

Venafi met with stakeholders across the company, including security and operations, to educate them on how to work together to further strengthen machine identity security. This education built on the initial work done for the outage safety net, with Venafi going into more depth about the responsibilities of certificate owners and security's role in overseeing the management of machine identities. Venafi helped the company implement a control plane for machine identities that helped them move toward enterprisewide deployment.

Turning early adopters into influencers

The next step was to onboard a group of early adopters. The company chose the network device management team, a group that was especially motivated to prevent any future data breaches like the one caused by that undiscovered expired certificate. Because this team was responsible for the largest concentration of certificates, it was important to test and validate all work to this point to ensure TLS Protect Cloud was functioning as intended.

The network device management team appreciated how TLS Protect Cloud could automate certificate procurement and renewal, turning what was once a tedious and error-prone process into something consistent and reliable. And thanks to the outage safety net, the team uncovered another expiring certificate that would have otherwise been lost in another former employee's email account, and they were able to renew it with plenty of time to spare.

"The team's attitude completely transformed from cynicism to excitement at what TLS Protect Cloud enabled them to do," said the CISO. "Getting this real-world win really cemented the value of implementing machine identity management across our organization."

Trusted by

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

Venafi is the cybersecurity market leader in identity management for machines. From the ground to the cloud, Venafi solutions automate the lifecycle of identities for all types of machines—from physical devices to software applications, APIs and containers. With more than 30 patents, Venafi delivers innovative solutions for the most demanding, security-conscious organizations in the world. **To learn more, visit venafi.com**