CASE STUDY

Venafi Zero Touch PKI frees healthcare company from mounting costs and risk

Challenge

A healthcare company found themselves without a PKI lead administrator to manage their increasingly rickety collection of Windows Active Directory Certificate Services. The previous PKI lead had warned that properly patching and updating the Windows PKIs was too much work for him to manage. These internal CAs proved to be a constant drain on the IT team's resources because no one had any clue how they were originally set up years earlier. In addition, everyone who needed machine identities from these CAs, including those working on mission-critical projects, faced expensive delays.

The previous PKI lead quit after stumbling on a group of TLS certificates and private keys sitting unprotected on a server. "He basically said, 'I'm out of here,'" noted the company's director of InfoSec. "His decision to leave was a wakeup call to us that our machine identity management program needed a complete overhaul. No one even knew how to quantify the security and availability risks let alone how much money and time we were wasting."

The company ruled out hiring a replacement PKI administrator. The budget wasn't there, and no one knew the real size of the problem and risk. In addition to the cost of a full-time replacement, it would have taken a year to refresh their current PKI. This was time the company did not have; the organization needed to change to meet the demands of multiple digital transformation initiatives. They also needed to increase automation pronto.

As they explored alternatives, the company's external, publicly trusted CA pushed their own solution as a replacement for the Windows PKIs—but it seemed like a devil's bargain. The user interface looked like something from the Y2K era, and it required an overwhelming number of steps to onboard anyone. Worse, it didn't work natively with Active Directory, which meant deployment would take too long.

At best, the solution would neither reduce costs nor meet the immediate need for automation.

"We were in a bad place, if I'm being honest," admitted the director of InfoSec.

Solution: Venafi Zero Touch PKI

On learning about the company's PKI emergency, Venafi suggested they consider Zero Touch PKI. This fully managed, cloud-native, "PKI-as-a-service" solution wouldn't require any physical or virtual infrastructure, specialized security hardware, or licenses for operating systems and Windows Servers. It wouldn't require any specialized staff to maintain legacy systems or monitor security. Instead, Zero Touch PKI would be a turnkey service leveraging automation and speed to prevent potential compromise.

With Zero Touch PKI, the company could replace their current Microsoft PKIs with a fast and secure cloud service designed by the experts in machine identity management. This managed service would immediately reduce operational and compliance risks and significantly lower costs without introducing complexity for end users. In fact, end users wouldn't notice any change because Zero Touch PKI is 100% compatible with Active Directory, Windows desktops and laptops, Microsoft Intune, and more.

And the time to value was incredibly fast. When Venafi said their SLA from purchase order to production was three weeks, the company's leadership team decided to go for it. "Everything about Zero Touch PKI screamed 'too good to be true,' but it was a fraction of the cost of hiring a new PKI lead and trying to do it ourselves. Hundreds of others like us already use Venafi for machine identity management, so it was a simple decision," reasoned the director of InfoSec.

Lightning-fast deployment and bulletproof security

Venafi met their SLA, deploying Zero Touch PKI in just 19 days. Beyond the sheer speed, the deployment was amazingly easy and delivered an immediate improvement in security.

The ultra-fast start consisted of four one-hour meetings. The first meeting addressed the scope of Zero Touch PKI, setup and handoff. The second meeting, which took place after Zero Touch PKI became available to the business, was a walkthrough of the service. The third meeting focused on specific use cases, such as Active Directory auto enrollment for Windows devices, IIS servers, remote desktops and the like—which enabled the company to seamlessly transition away from their Microsoft PKI. The final step involved connecting the service with the Venafi Platform, providing the healthcare organization with a complete machine identity management solution.

"Zero Touch PKI didn't change anything in our current environment, except of course eliminate the cost, headaches and risk," said the director of InfoSec. "The auto-enrollment proxy took a half hour to configure and prove out, and then Zero Touch PKI was issuing certificates easy-peasy. We eliminated enormous security risks and were immediately able to automate everything that used to be a pain."

Instant scalability

In addition to taking over the tasks previously assigned to the PKI team, Zero Touch PKI also could scale on demand, no matter the use case.

The true test came when the company launched a new application utilizing certificates issued by the new service. Zero Touch PKI's OCSP service handled the load without breaking a sweat and without deploying anything.

"We didn't have to worry about adding load balancers or servers to handle any of this. It was fast, easy and completely automatic," said the director of InfoSec.

Better security and efficiency with lower costs

Most importantly, Zero Touch PKI dramatically reduced the overall risk of a compromise—a constant worry in the old Microsoft PKI setup. The significant security risks were eliminated; private keys were now kept safe in an HSM rather than being secured haphazardly on file shares scattered across the enterprise. This eliminated the constant worry that a threat actor might infiltrate the network, steal private keys, obtain a trusted identity or initiate a man-in-the-middle attack.

Because Zero Touch PKI is a modern cloud service, several other risks inherent to the old Microsoft PKI were no longer a concern. And all this was accomplished in less than a month.

The InfoSec team delivered huge improvements to the business. Response times for new certificates were faster. Operating expenses were lower. And machine identity lifecycles were automated for efficiency in ways not possible before.

Said the director of InfoSec: "I feel like a huge weight has been lifted, and I can't quite believe it. Zero Touch PKI did everything we needed almost instantly and then some!"