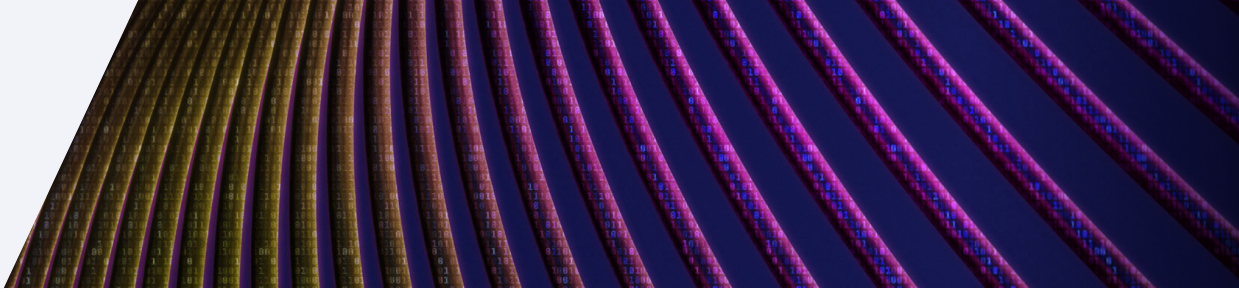
Venafi



CASE STUDY

FinServ company deploys SSH certificates, cutting time to harden SSH defenses

Challenge: Leading insurance company needed to quickly mitigate decades of SSH key sprawl

A large insurance company desperately needed to get their SSH security under control. They were concerned that in the decades since the company first deployed their IT environment, they had amassed millions of SSH keys, most of which needed to be removed. These "rogue" keys ranged from clones of a golden key on countless VMs to keys that predated corporate SSH security policies or were simply orphaned. The director of IAM (Identity and Access Management) likened the situation to a fraternity house. "Imagine piles of old pizza boxes and crushed beer cans in every nook and cranny—and then multiply it by a factor of 10. That was the level of sprawl we were facing," he said.

The company realized that not only did they need complete visibility into their SSH key inventory, but they also needed an automated way to remove unsecured SSH keys. They asked several SSH security vendors about implementing such a solution and learned that it would take two years to complete such a thorough process—which was too long to remain vulnerable.

As the company evaluated alternative tactics, they learned SSH certificates could accelerate the process. Instead of having to find and remove every unnecessary key, they could simply disallow keys and replace them with SSH certificates. However, the migration to SSH certificates was not without its challenges. Without expert help, setup and deployment was so convoluted that few organizations had succeeded, despite SSH certificates having been around since 2010. The company needed to find a vendor whose solution could effectively deploy SSH certificates in a reliable manner.

Solution: SSH Protect

The company was already a longstanding Venafi TLS Protect user, so they asked Venafi SSH experts to demo SSH Protect as part of a due diligence process. Venafi started their PoC by performing a free SSH Risk Assessment on a selection of the company's servers. Venafi found twice as many keys as the company had estimated, including an uncomfortable number of previously unknown duplicate and shared private keys.

In contrast, none of the competing solutions delivered complete visibility into existing key inventories. "They seemed to work on the assumption that deploying SSH certificates was a greenfield project, but our IT infrastructure is decades old and represents our greatest risk," the IAM director said. "It's valuable to us to fix this as fast as we can."

In addition to complete visibility into SSH keys using SSH Protect, Venafi could help them cut deployment times for SSH certificates from two years to a matter of months. Said the IAM director: "They offered us the whole package that an enterprise of our size needed to be successful with SSH. And they demonstrated to us that they, better than anyone else, would lead us to success."

Streamlined configuration of SSH policies

Once the company gained complete visibility into their key inventory and removed the most problematic keys, Venafi helped them set up the necessary infrastructure for SSH certificates. The templates included in SSH Protect allowed them to set up an SSH Certificate Authority (CA) that could be managed within the larger Venafi Control Plane for Machine Identities. These templates use parameters that define settings and permissions for the CA in an easy-to-use GUI and could be set up so that all Linux systems knew to trust it. This centralized SSH CA would streamline trust configurations for all users across all the company's systems.

"It was a one-and-done configuration that ensures consistency and reliability," said the IAM director. "Now whenever a user requests an SSH certificate, certain security specifications will always be embedded on that cert."

Improving security using SSH certificates

In addition, SSH Protect also automated policy around how SSH certificates were being used, along with access controls. Once the company deployed it in production, they could disallow SSH keys in favor of SSH certificates issued by the CA simply by editing a configuration file on the server.

This ability "just about broke my brain," said the IAM director. Every administrator, past and present, had placed their own public key on servers for easier access. "The very notion of removing or rotating the thousands of keys littered on servers without disrupting services really troubled me," he added. Instead, the company could use SSH Protect to safely migrate or remove these keys without inadvertently causing an unknown server to go down.

With Venafi's help, the company began their rollout of SSH certificates by onboarding interactive sessions where root-level accounts were being used. Admins now had to procure an SSH certificate to access the server—and those certificates could be set to expire in an appropriate timeframe within days, hours or even minutes after issuance.

"SSH Protect works especially well for these interactive user sessions because you can make the certificate valid just long enough to establish the connection; it doesn't affect what the admins are doing once they're logged in," said the IAM director. "But after five or 10 minutes, depending on how we've set it, they expire, so any bad guy trying to use it will be out of luck."

Improving operational efficiencies using SSH certificates

The company soon saw how deploying SSH certificates improved operational efficiencies as well. Key rotation took minutes rather than several hours or days, because the SSH CA deployed the same public key to access all onboarded servers. "Instead of having to rotate all those public keys in the past, you can just issue a new certificate from the CA that is automatically trusted," said the IAM director.

After some initial grumbling, the admins saw the value of SSH certificates and preferred using them to their old messy processes. Said the IAM director: "They appreciate having less to do and less to worry about. And they're sure happy to get rid of the hassle of juggling passwords. We can't wait to roll out SSH certificates across our entire infrastructure, and we're thrilled at how Venafi has helped us throughout the journey."