Case Study

Key and Certificate Protection Bolsters IT Security and Performance

Delivering Consistent, Proactive Security in a Decentralized Management Model

Executive Summary

Industry | Insurance

IT Environment

Uses certificates for SSL/TLS encryption and authentication

Business Challenges

- Implement consistent security across distributed digital certificate ownership
- Deploy a secure, centralized key and certificate repository
- Streamline certificate renewals to avoid outages and financial loss
- Reduce risk with stronger, uniform key and certificate security

Solution Business Impact

- Enabled a secure, central repository for keys and certificates
- Delivered consistent, integrated workflow to enforce security policies
- Reduced manual practices by 80%
- Lowered risk with inventory visibility, consistent processes, automation and role-based access

Business Profile

This Venafi customer has grown to be one of the largest insurance companies in the United States and is now expanding internationally, offering coverage for a wide range of insurance options. The company's success comes, in part, by staying one step ahead in the insurance industry. It was one of the early adopters in the industry to offer 24/7 service and the ability to purchase insurance online. It now joins other leading global companies using key and certificate security.

IT Environment

The company's IT environment supports tens of thousands of independent insurance agencies and the company website. Its IT environment includes both internal and external web-based services, including quote services and policy access over the web. The company uses digital certificates to secure these web-based services and for strong authentication.

Business Challenge

With both certificate usage and certificate-related security threats on the rise, the company's PKI team needed to ensure that the organization's keys and certificates remained protected. Of course, the company had other security controls in place, but the PKI team did not want cybercriminals to compromise unprotected keys and certificates which are often used to bypass these security controls via trust-based attacks.

SSL/TLS certificate management became more challenging when the company changed from centralized application control to a more distributed model where different groups control their own applications. The different groups did not implement the same security processes and some did not know how to secure keys and certificates for their applications. The loss of central visibility and consistent processes resulted in weakened security and long delays in, or even missed, SSL/TLS certificate renewals. This caused outages, brand damage and financial loss.

After these organizational changes, the company's PKI team no longer knew where all of its certificates were or how they were being used: the team had no inventory system or centralized, secure key and certificate repository.

The PKI team also knew it needed consistent processes for the different application teams to follow if it was to implement an effective certificate and key management system and ensure that keys and certificates remain protected. At the time, the team's certificate tracking efforts were all manual, using either a spreadsheet or SharePoint site. And the PKI team did not have firm workflow processes to improve operational efficiency, conduct certificate lifecycle management and enforce security practices, relying instead on email and other ad hoc communications.

The team knew it needed another solution, but it also knew it did not want to create and maintain custom code in internal, home-grown scripts for SSL/TLS certificate management. It decided to look for a vendor solution that would meet its needs, including the ability to establish a comprehensive inventory; a secure and centralized repository; consistent, enforceable workflow; and automated processes—all of which were required to strengthen the company's key and certificate security and prevent compromise.

> *"We turned to Venafi to find all of our cryptographic keys and digital certificates companywide. And we needed to include root and intermediate certificate control as well as safeguard our work with external vendors—all with a goal of reducing risk and protecting the business. Venafi delivered this security."*
>
> *Systems Engineer Lead*
> *Insurance Company*

Solution: Venafi

After deciding not to create a solution in house, the PKI team started looking at outside vendors. It turned to Venafi as a vendor known for digital certificate and private key security. In the spirit of due diligence, the team also looked at other vendors, but found that these vendors' solutions did not have sufficient security capabilities to safeguard the company's keys and certificates—unlike the Venafi offering, these products could not conduct discovery to locate all certificates nor could they provide the breadth of capabilities needed for effective protection.

After narrowing down the solution vendors to one—Venafi—the PKI team conducted a proof of concept (POC). The Venafi product met all test requirements and worked as advertised. The company purchased Venafi for SSL/TLS, initially to help with inventory and consistent security-process workflow, and later to fold in other key and certificate security features.

Not only did Venafi have the most capabilities of all solutions considered, the Venafi team was also open to talking about its plans for the future. This allowed the company's PKI team to show the value of Venafi key and certificate security now and moving forward.

Solution Business Impact

Comprehensive Inventory and Secure, Central Repository

To start, the company turned to Venafi to find where its certificates were located and how they were being used. The PKI team had previously tracked ownership by embedding emails into the certificates, but it did not have a central repository for the visibility and control it needed to secure keys and certificates.

"With Venafi, we now know what the certificate is, where it is and the group associated to it," said the organization's systems engineer lead. "Even if the group gets disbanded, we can still figure out how to renew by following the normal renewal operations in place and find out the 'who' later. This helps us keep all certificates current and up to date with the latest security practices."

The PKI team is inventorying all of the company's keys and certificates, but is focusing on the largest use cases first—Windows servers and F5 Local Traffic Managers (LTMs). Then the team will turn to other, secondary platforms.

"We will have 100% of our certificates in the Venafi inventory," said the systems engineer lead. "We'll use Venafi automated processes through network discovery and use the Venafi agent to secure the highest percentage and important use cases right out of the gate and then pick up the remaining niche cases as needed. Securing keys and certificates is a hot topic, as always, but this year even hotter."

Consistent Workflow Enforces Security

After company reorganizations created distributed application management, the company needed a consistent certificate-security process that could be followed across all departments companywide. Before Venafi, the company used manual methods such as email, spreadsheets and SharePoint sites to track keys and certificates. This created inconsistent efforts, lack of visibility and no structure to enforce policies. With these holes in processes, the company was missing important security practices.

"One of the key benefits of Venafi platform is the workflow processes. It allowed us to set up workflows for security practices that anyone can use and we can pull in other teams," said the systems engineer lead. "This gives us documented and hardcoded workflow processes for consistent certificate security across the company."

Automated Security

"When we started with Venafi, we updated inventory and applied workflow processes for security practices," said the systems engineer lead. "And we found that the Venafi automated processes reduced our manual efforts by 80%."

With Venafi, the company's PKI team was able to load its key and certificate inventory with automated network scans. And now the team is moving toward what its members call "Complete Automation," which enables certificate renewals without human interaction other than a manual check of the certificate and its associations prior to its scheduled renewal date and time, which is preconfigured in the Venafi platform. The PKI team will also be leveraging the automated certificate provisioning processes in Venafi to ensure efficient and secure deployment.

> *"With staff and organizational changes, we want to make sure key and certificate security is not forgotten until it's broken. We don't want certificates to expire and lose our services or, worse yet, suffer a breach. With Venafi automated processes, we know key and certificate security is continually covered."*
>
> *Systems Engineer Lead*
> *Insurance Company*

"Before when a certificate request came in, we'd use an SMS package to deploy it," said the lead engineer. "Now we can instruct Venafi to deploy to all servers, for example, all of our LTM load balancers. I'm looking forward to having this automation from a PKI management and security perspective."

The company is also planning to use Venafi to monitor its certificate revocation lists (CRLs). It has an offline root CRL that it must create every 120 days. Now with Venafi, the company has an automated method for generating the CRL when it comes due, helping to ensure that revoked certificates cannot be misused by cybercriminals.

Role-based Access

With the changes in organizational structure, the PKI team discovered that connecting keys and certificates to a single owner was problematic. Venafi gives the team the flexibility to assign particular certificates to groups while maintaining security by designating different levels of access across groups.

"Reorganizations wreaked havoc in the certificate renewal process," said the systems engineer lead. "But now Venafi allows us to break down the access controls for each application. Each application team has its own access limited to its application while the operations team has access to everything. We can also allow a team to view the certificates of other teams, but not change them. This role-based access for certificate owners helps to ensure certificate security within our decentralized management model."

Improved Security and Reduced Risk

"As the PKI team, the Enterprise Security team is our direct customer. They create our standards and policies and we need to meet them," said the systems engineer lead. "Venafi is one of those tools that allows us to meet and exceed the standards and policies they have put in place. And Venafi lets us monitor our efforts to ensure we stay in compliance."

In addition to inventory, workflows, automation and role-based access for improved security and risk reduction, the PKI team will also use Venafi whitelisting and blacklisting capabilities to designate trusted connections. With Venafi, the team can identify root certificates in use and update CAs that are trusted, while blacklisting those that are not.

The Venafi policy framework also helps the company reduce risk by ensuring proper key and certificate configuration as well as use of only current, strong cryptography—including attributes such as key length, validity period and cryptographic hash type. For example, the company is using Venafi to meet SHA-2 requirements.

Right now, the PKI team is using Venafi to meet internal security requirements, but will look to Venafi to meet external compliance requirements as well. Venafi monitoring and reporting capabilities provide visibility into the company's ongoing state of security and compliance.

Evolving Capabilities

With Venafi sharing the project roadmap, the PKI team has been able to align project expansion with new Venafi capabilities. For example, when the team heard that the custom fields feature was going to be released, the team prepared to use it both to further automate processes and improve vendor communications, allowing these changes to be quickly implemented following the release.

Venafi Professional Services

The company's PKI team turned to Venafi Professional Services to assist with its deployment of the Venafi platform. The company had three engagements during implementation and has one planned in the near future to train its PKI and operations teams.

The PKI team is looking forward to the training so it can learn the intricacies of the product. Otherwise, its members have been learning about Venafi platform during deployment sessions and on their own. "I've been actively learning the product. I found the product intuitive and the documentation is good at bringing you where you need to go," said the systems engineer lead. "Support is also top notch with very good responsiveness. They've quickly answered the tickets I've opened while exploring the product's capabilities."

"Before Venafi, my favorite system error was 'Intermittent Certificate Issues,'" said the systems engineer lead. "That could mean so many things and would take hours to troubleshoot—potentially leaving us vulnerable in the meantime. But now with Venafi, we can figure it out. And more importantly, we take a proactive approach to securing our keys and certificates that doesn't wait until something breaks."

TRUSTED BY THE TOP

5 OF 5 Top U.S. Health Insurers
4 OF 5 Top U.S. Retailers
4 OF 5 Top U.S. Airlines
4 OF 5 Top U.S. Banks
3 OF 5 Top AU Banks
4 OF 5 Top U.K. Banks
4 OF 5 Top S. African Banks

ABOUT VENAFI

Venafi is the cyber security market leader in protecting cryptographic keys and digital certificates which every business and government depends on to deliver safe encryption, authentication and authorization. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access.

To learn more, visit www.venafi.com

Share this case study: