Venafi

CASE STUDY

Global Technology Provider Secures Code Signing Process to Safeguard Its Brand

Venafi Process Secures Company's Code Signing Workflows

Executive Summary

Industry: Computer Technology

IT Environment: As a technology solutions provider, the company makes extensive use of security certificates for code signing as well as SSL/TLS, VPN and wireless access.

Business Challenges

- Inability to deploy consistent, automated IT security to maintain the company's brand
- Difficulty securing globally dispersed cryptographic keys and digital certificates
- Lacking the ability to support production with centralized code signing certificate security
- No means to support millions of code signing activities each week

Solution's Business Impact

- Safeguards brand reputation using consistent security policies and practices
- Establishes a central, secure repository for code signing certificates
- Automates security to support cloud deployments, time and resources, self-service and consistent protection
- Conducts interdepartmental training for companywide code signing, SSL/TLS, and other key and certificate security processes

Business Profile

This solutions provider delivers technologies for computers and communications. With its heritage of innovation, the company continues to expand the reach and promise of computing while advancing the ways in which people work and live worldwide.

IT Environment

The company's IT environment supports over 100,000 employees and has billions of dollars in annual revenue. With employees in over 200 countries writing code, digital certificates for code signing have a significant impact on production, operations and security. The organization also uses certificates for SSL/TLS, wireless and VPN access.

Business Challenge

The company realized it needed consistent, automated key and certificate security to maintain its brand. Many of the organization's IT departments would benefit from this security, but the code signing team took the lead. When the company's code is signed using certificates, this is meant to confirm both the company as the author and the integrity of the software. Customers of this solution provider expect products signed with the company's code signing certificates to be secure—they must be able to rely on the brand to deliver safe products.

With the company's code being created by international development teams, keys and certificates for code signing were dispersed across the globe, often with one-off creations for particular projects. The code signing team was faced with the challenge of securing all keys and certificates and ensuring consistent, secure processes moving forward. These challenges included ensuring attempts at automation did not copy the certificates inappropriately, managing certificate lifecycles, tracking certificate owners after people switch roles or companies, and providing a mechanism for provisioning new certificates. After Heartbleed, the team realized it needed a solution that could quickly refresh and replace its key and certificate infrastructure.

"Because we had teams writing code in over 200 countries, our code signing certificates were all over the place—and this negatively impacted production," said the company's solution architect. "The code signing team needed a centralized system for key and certificate management and distribution."

More important than these operational challenges, the code signing team had to verify the security of certificates. The solution architect added: "Malware uses a number of vectors to infiltrate systems. We don't want to be the owner of a certificate that was used to sign malware. We need to secure our business and brand as a trusted technology and security company—and securing the certificate signing process needs to be part of that effort."

"People trust our brand and know that trust is part of all of our product sales. To maintain this trust, we use Venafi as a gateway that imposes consistent, predictable key and certificate security across the enterprise," said the company's solution architect.

Solution: Venafi

When the company decided that key and certificate security was critical to its code signing project, the team reached out to their partners to ask what they were doing. Based on these recommendations, the team met with and evaluated three of the companies, including Venafi.

"One of the solutions we considered was a distant third. Another needed more work, which would have meant waiting for additional development with APIs," said the solution architect. "But with Venafi, the capabilities and agents we needed were already there. Out of the box, we got what we needed instead of having to write our own interfaces, and we knew it was only going to get better."

Solution Business Impact

Central, Secure Repository and Policy Enforcement

The primary business driver for acquiring the Venafi solution was the need to take the keys and certificates dispersed across the company's IT environment and put them into a central, secure repository protected by consistent policy enforcement. The code signing team funded the Venafi solution, so the initial focus was to automate consistent key and certificate security for the code signing managers.

At the company, the code signing certificate mechanisms used in production are restricted for most use cases. Very few people at the company understand these restrictions or how to properly include code signing certificates in the development process. To better manage this process, the code signing team integrated Venafi with their Hardware Security Module (HSM). Using this integration, the company centralized its key and certificate repository, enabling visibility and control, policy enforcement and distribution for improved security.

"With Venafi, the code signing managers can ensure that requests for code signing certificates go through the sanctioned signing engine," said the solution architect. "This gives us the control to do it the right way, the secure way."

"We wish we'd had Venafi in place to remediate Heartbleed. At least now we know that we're ready when a future vulnerability is discovered. Venafi lets us replace our infrastructure quickly when needed. Other departments outside of the code signing team want to deploy Venafi to ensure they are also secure for the future," said the solution architect.

Comprehensive Visibility and Control

With Venafi, the company now could establish a complete inventory of all keys and certificates. With this comprehensive visibility, the organization could validate key and certificate security.

"Before Venafi, we were not doing a good job of remediating certificate expiration," said the solution architect. "Certificates would expire, and no one was managing it. Entire services would go down. With Venafi, we can see which certificates are about to expire and take a proactive approach."

Workflows to Enforce Security

IT teams are also using workflows and approval processes to enforce policies, especially when it involves individuals outside of the immediate managing group. Before Venafi, the workflow practices were very basic. However, with Venafi, the teams can create more granular associations for ownership, actions and approvals to confirm secure processes.

For example, application owners may be restricted to controlling the keys and certificates for their applications. Additional layers of restrictions may be established, such as limiting certificate authorities (CAs), expiration dates, applied algorithms and other criteria that impact secure key and certificate enrollment, provisioning and management. Also, the ability to associate a group instead of an individual to a particular certificate helps expedite a disaster recovery plan when needed.

Cross-Team Training and Security

The code signing team first engaged with the Venafi training team to view demos and confirm implementation for particular certificate security use cases. Now they are looking forward to getting more comprehensive training.

"We'll be looking at detailed workflow capabilities and notifications during our upcoming training. Our team looks forward to Venafi training because it always goes beyond the questions we can think to ask," said the solution architect. "We want to really kick the tires and spark some ideas of other ways Venafi can help our team."

A broader view of the Venafi solution will also help to support internal sales pitches for funding—not only for staffing resources for Venafi implementation but for the entire code signing project.

The code signing team wants to enable the Venafi benefits beyond their deployments. They struck a deal with other departments, agreeing to train a couple of people on their teams if they agree to implement and own the Venafi solution in their environments. This has resulted in several other departments expressing interest in deploying the Venafi platform.

Network Team

Currently, the network team is applying a patchwork of scanning and manual tools to manage their SSL/TLS environment and getting different results across these tools. Addressing these results requires multiple iterations of scan and remediate. They want to use Venafi as a centralized key and certificate security tool that conducts holistic scans and provides near real-time information for their SSL/TLS environment.

Cloud Team

The cloud team plans to leverage the automated processes in the Venafi solution. Currently, the team conducts key and certificate processes manually, which is slowing down the organization's dynamic use of cloud computing. They want to define policies in the Venafi solution and then use the solution's automated processes to securely provision and manage keys and certificates.

PKI Team

The PKI team is interested in developing a self-service portal that will enable others to provision their own certificates. With policies and workflows, they can implement consistent security and policy enforcement companywide, while freeing other teams to meet their own certificate needs.

SAP Team

As a team that hosts a large deployment of applications, the SAP team wants to streamline key and certificate provisioning and distribution. They deliver IT as a service, which means they own the infrastructure piece. Also, they need to help application owners with their key and certificate security.

The SAP team also supports applications with local and global load balancing, tying in the network team and requiring additional certificates across F5 LTMs. With application servers and load balancers, the team manages thousands of keys and certificates. They want the easy, automated and secure certificate distribution and management processes delivered through Venafi.

"Venafi goes beyond enrollment to provisioning. The management team can configure the certificate options to ensure security and consistency, but then our internal customers can get their own certificates. This saves a lot of time; I don't even have to touch it. When I heard that we could use Venafi for our SSL, code signing and my F5 load balancers, I said, 'Sign me up!'" said the company's solution architect.

Automated Key and Certificate Security

The various teams consider automation to be a critical feature of key and certificate security because automation enables consistent deployment of secure processes and delivers time savings that can benefit all business groups. The cloud services team needs automation to fully realize the dynamic benefits offered through a cloud environment. Meanwhile, other departments share a similar need for automated key and certificate security to support the capabilities of underlying technologies.

Next Steps—SSL/TLS Certificate Portal

For its next key and certificate security project, the company plans to use Venafi for an enrollment and provisioning portal. Early on, the code signing team used a smart card provisioning tool, but it was limited to user certificates and did not help with pushing the certificates out to users. The team then attempted to develop a homegrown portal with certificate options and approval workflows, but this portal failed to provide distribution and control of certificates. Ultimately, the company understood it lacked the resources to address these issues manually. The company will soon replace its current portal with Venafi.

"Currently we have a small team that manages all of the SSL/TLS certificate distribution. With the new Venafi portal, the team will maintain the automated structure, but the portal will provide self-service certificate provisioning," said the solution architect. "Not only will it help us save time and resources, we'll also have better security and control by restricting options in the portal. For example, if we need to get rid of a CA, we go into the tool and eliminate it as a choice. We can also see where this CA is already in use and take action."

The Venafi portal will provide self-service SSL/TLS certificate enrollment, provisioning and management while ensuring policy enforcement and security. As the company expands its use of Venafi beyond code signing certificates, it further protects its brand reputation, securing the trust that keys and certificates establish as the foundation of safe business communications and authentication.

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