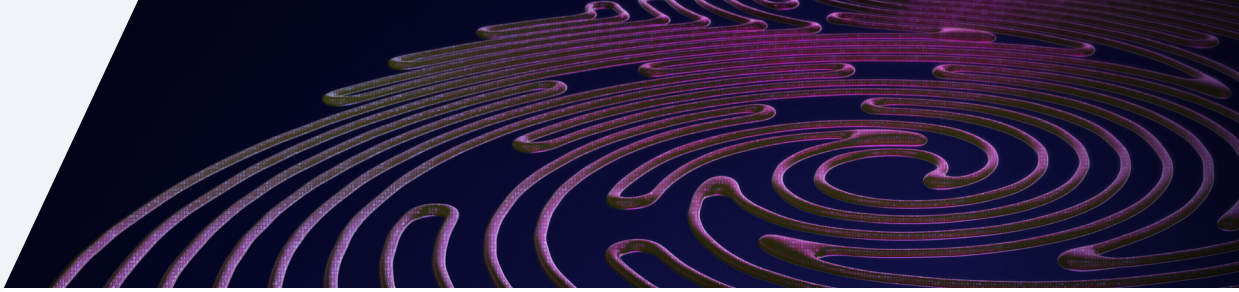
Venafi



CASE STUDY

Technology Provider Reduces Costs to Secure Code Signing Processes

Venafi CodeSign Protect Increases Security for Development Team

Executive Summary

Industry: Technology

Dev Environment: The company develops enterprise Windows and SaaS applications for Fortune 500 companies. Its global stable of developers is responsible for millions of lines of code.

Business Challenges

- Securing code signing keys required duplicate environments, increasing costs and complexity.
- Insufficiently protected code signing keys heightened risk.
- Passing audits was problematic.

Solution's Business Impact

- Reduces costs by eliminating dual build environments.
- Secures code signing processes without hampering developer productivity.
- Safeguards private code signing keys through both process and authorization.
- Automates code signing approval workflows to fit code signing processes and corporate security policies.
- Audits against all code signing operations.

Business Profile

The company is a leading enterprise technology provider that supplies mission-critical, cloud-based and on-premises software to global organizations. Its customers depend on the reliability and security of its software to run business operations.

Development Environment

The technology company builds enterprise applications that are deployed to a variety of operating systems, including Windows, Linux, Unix, macOS, iOS and Android. The company follows DevOps methodologies to deliver frequent software releases that improve on feature set and functionality. A cadre of developers is responsible for writing and iterating millions of lines of code, with more than 150,000 code signing operations taking place each month.

The company runs both Windows and Linux servers for development platforms, using Jenkins and Buildbot for build automation. Additionally, it utilizes both internal and external certificate authorities (CAs) to generate code signing certificates. Even though hardware security modules (HSMs) were used for other PKI, the company couldn't use them to store code signing keys because of the difficulties developers had in accessing those keys.

Business Challenge

The company embraced DevOps processes to build out the types of features its Fortune 500 customers needed to operate more quickly and effectively. But as its product portfolio—and consequently, the amount of code being developed—continued to grow, the company needed a way to sign code in an automated fashion without slowing down its software build processes.

The company's original solution to secure their code signing keys was to create dual build environments—a general one used by the development and engineering teams and a second "secure" environment where a limited number of people could access their private code signing keys to sign their software builds.

This dual build environment was less than ideal. For one thing, maintaining two environments was expensive and complex, requiring additional hardware to duplicate the general build, as well as the human resources needed to maintain it. Upkeep of this dual infrastructure took engineers away from their core job of rolling out new features. And this expense would only increase as development teams built more code and scaled to grow with the business.

In addition to cost, these multiple build environments introduced additional complexity to the development environments. If changes were needed for one environment, those same changes would have to be duplicated in the other environment. This approach also required dedicated resources to have PKI and code signing expertise because there wasn't a self-service way for developers to easily procure the machine identities they needed for their code.

Also, this setup still required development teams to manually manage the entire lifecycle of its code signing certificates, including issuance, rotation and revocation. Development teams were responsible for monitoring certificate expirations, anticipating and planning engineering work hours around key rotation activities, maintaining a written step-by-step procedure for renewing the certificate, and testing everything in all environments with the new key.

"Venafi has proven they will have our backs regardless of any issues we might face with this new solution, so we had trust in them that CodeSign Protect could work for us," said the company's chief developer.

Even with this expense and complexity, the company failed to adequately protect private code signing keys from all risks. Access to these private keys was still being protected with usernames and passwords for specific individuals. In other words, these individuals had access to the private keys and could conceivably create copies of them. "Because it was file-based, any person or machine on the network had access to secure information and could sign code of any type. We didn't have a way to monitor or limit inappropriate actions from happening," said the company's lead DevOps engineer.

Solution: Venafi

In the past, the company investigated solutions to solve this problem but couldn't find any that offered high-performance value without forcing upheaval to their developers. "We were resigned to building something ourselves that wasn't ideal for our needs," said the lead DevOps engineer.

The company had been using Venafi Trust Protection Platform for several years to manage and protect their SSL/TLS machine identities. "We wanted something that could take care of the code signing certificate lifecycle and securely store code signing keys on our HSM without the ballooning costs we were facing," said the company's chief developer. "Venafi has proven they will have our backs regardless of any issues we might face with this new solution, so we had trust in them that CodeSign Protect could work for us."

Because Venafi CodeSign Protect integrated directly with the Venafi Platform they were already using, the company was able to evaluate the product quickly and easily. And the DevOps pilot project was so successful that the company started rolling it out to other teams soon afterward.

Solution Business Impact

Costs reduced significantly by eliminating duplicate build environments

Venafi CodeSign Protect has allowed the company to migrate away from their dual-build environment strategy. Because the second build environment is no longer necessary, it provides tremendous economic savings. For example, the company no longer needs to:

- Maintain a duplicate build environment with its associated costs.
- Maintain scripts that kept the secure build environment in sync with the actual build environment.
- Funnel away engineers from their core competencies of rolling out, installing and configuring software to maintain the secure build environment.

The company's leadership was concerned about the prospect of having to divert more capital expenditures (in the form of more hardware) and operational expenses (in the form of full-time employee hours) to the previous setup. With CodeSign Protect, those concerns have been eliminated, and according to the lead DevOps engineer, the finance team is "elated" about the immediate and long-term economic benefits from these savings.

Code signing processes secured without hampering developer productivity

Development teams also like how CodeSign Protect enables them to procure code signing keys without having to use special tools and scripts or needing PKI and code signing expertise. In addition, the private keys are significantly more secure now that they are permanently stored in the company's HSMs rather than the secure build server, where they could have been easily copied. The jump in productivity was immediately noticeable.

"With CodeSign Protect, I don't have to rely on engineers to help me secure code signing," said the company's lead developer. "It's in my environment, and I don't have to do anything special for it to just work."

Code signing private keys completely protected by both process and authorization

In addition to making the code signing process easier than ever before, CodeSign Protect allows the InfoSec team to secure private code signing keys based on the principle of least privilege rather than by usernames and passwords. InfoSec now has the ability to secure private keys in a granular fashion by customizing the level of access based on such factors as the type of project the code is being used for, acceptable risk and from where the IP request originates. InfoSec and the project managers can even establish which individuals are needed to approve the use of a specific code signing key.

Said the lead DevOps engineer: "Even I no longer have access to these keys—and that's a relief! There's no reason for anyone to have access to those keys and put our company at unnecessary risk."

Code signing lifecycle now automated

A significant benefit for the DevOps team is that CodeSign Protect has made it possible for them to automatically manage the code signing certificate lifecycle, saving many hours of manual effort. CodeSign Protect, in conjunction with the Venafi Platform, manages the corresponding private keys without the engineering team having to be involved. These automated workflows provide the flexibility of using different keys for different code, as well as the ability to use certificates with shorter validity periods. By design, the whole code signing process is now more scalable and secure.

In addition, certificate issuance and even revocation are automated and no longer require development teams to have PKI expertise. CodeSign Protect handles that without the need for human intervention.

InfoSec team able to audit against all code signing operations

CodeSign Protect gives InfoSec the ability to monitor code signing usage and automate processes across the development organization—enabling them to effectively audit against all code signing operations.

InfoSec now can generate reports showing detailed intelligence into the developers who signed code, the people who approved requests for the signed code, the CA that procured the code signing certificate, and the time these actions took place.

As a result, the company is now able to generate a detailed audit trail of all code signing activities. And CodeSign Protect can generate compliance and audit reporting for InfoSec to use in proving to the company's customers that they can comply against all relevant code signing security standards. "CodeSign Protect has eliminated the problem areas that our audits had previously identified," said the company's vice president of risk and compliance.

Overall, CodeSign Protect transformed the way this technology company manages its code signing processes. Its ability to keep private keys secure and inaccessible has dramatically lowered the company's risk profile, while providing InfoSec the ability to monitor and enforce enterprise security policies and best practices. And CodeSign Protect did this by improving processes for development teams, making it easier and faster than ever before to perform their core coding tasks.

Finally, CodeSign Protect can easily scale. As a result, the immediate economic benefits that came with ridding themselves of the secure build environment has continued to compound as the company's development teams continue to grow in employee size and in the amount of produced code. "As a DevOps engineer, I was skeptical of any solution that our InfoSec team suggested because sometimes they just don't get the pressures that we are under in getting product updates out the door. However, CodeSign Protect has reduced our expenses while speeding up our overall release process!" the company's lead developer concluded.

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 machine identity management, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access. **To learn more, visit venafi.com**