digicert®

Software Trust Manager Case Study

CASE STUDY

Canon streamlines code signing operations and meets industry regulations using DigiCert Software Trust Manager

Executive Summary

Company name: Canon Inc.
Industry: Technology
Headquarters: Tokyo

Key business requirements:

- Enhance security of code signing processes to protect applications and printer drivers used by Canon printing devices
- Centralize management of code signing across the organization to improve control and efficiency
- Comply with evolving industry regulations and standards, including CA/Browser Forum's 2023 mandate for code signing keys that requires secure hardware storage of private signing keys

Solution:

- DigiCert Software Trust Manager

Key benefits:

- Comprehensive visibility and control over all code signing activities enables prompt detection and response to potential threats
- Role-based access management separates signing and administrative duties, reducing workload and minimizing the risk of human error and security breaches
- Automated workflows and intuitive tools cut code signing time in half, streamlining processes and empowering users regardless of technical expertise.
- Centralized management and strict controls enforce corporate security policies and regulatory compliance while providing a clear overview of the company's security posture.

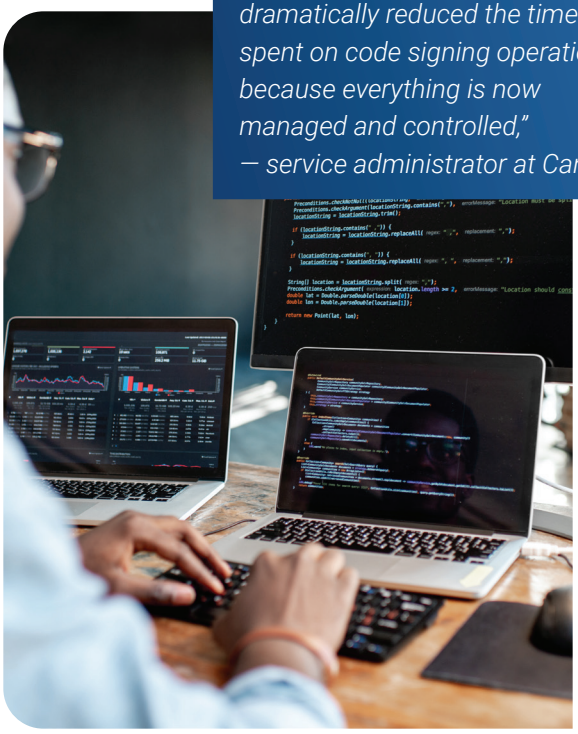
Challenge

Strengthen code signing processes to safeguard printers and meet evolving regulations

Canon Inc., a global leader in digital imaging solutions, faced a pressing need to enhance the security of its code signing processes. Their printing division, which accounts for a large portion of the company's sales, makes an array of multifunction printers (MFPs) and printing-related products for various industries. The applications and printer driver used on these many devices must be secure to ensure the safety of connected devices and compatibility with the latest operating systems.

Until recently, Canon was using an internally developed code signing management solution. Increasingly, however, the company questioned whether their solution could meet either the evolving security landscape or meet changing regulatory requirements. For one thing, the CA/Browser Forum (CA/B) mandated that starting in June 2023, private code signing keys must be stored on hardware that is FIPS 140-2 compliant, Common Criteria EAL 4+, or their equivalent.

Meanwhile, the alarming rise in global software supply chain attacks meant that they needed a solution that could work across the organization to centrally manage and secure code signing processes in an efficient way. Canon knew they couldn't continue to use their current solution without major improvements that might ultimately be too expensive to maintain and update.



> *"Software Trust Manager has dramatically reduced the time spent on code signing operations because everything is now managed and controlled,"*
> *— service administrator at Canon*

Solution

DigiCert Software Trust Manager streamlined Canon's code signing operations while ensuring security and compliance

After an extensive analysis, Canon concluded that they needed a purpose-built solution to resolve the code signing challenges they were facing. The company chose DigiCert Software Trust Manager because its features aligned perfectly with Canon's objectives. Software Trust Manager supplies granular certificate and key access based on role-based permissions, as well as proactive compliance with regulatory requirements.

"Software Trust Manager has dramatically reduced the time spent on code signing operations because everything is now managed and controlled," said a service administrator at Canon. "And it has freed our developers from having to worry about managing keys, in addition to everything else they have to do."

Combining comprehensive visibility with efficient role-based access management

Software Trust Manager provided Canon with visibility and control to track and monitor all code signing activities across the entire organization. This strong management capability meant the company's security team could now see:

- When the code signing operation took place, as well as on which system
- Who initiated the session
- Which certificate and private key was used
- Whether the corporate and industry policies are followed

This granular visibility gave the security team the ability to detect and respond to anomalies and potential threats more quickly than they could in the past.

Moreover, Software Trust Manager provided role-based access controls that enabled Canon to drastically reduce the responsibilities of developers. Now developers only had to worry about the act of signing the code, rather than having to worry about certificate and key management as well. This separation of duties not only reduced the workload for developers but also minimized the risk of human error and potential security breaches.

Cutting code signing actions by half using automation

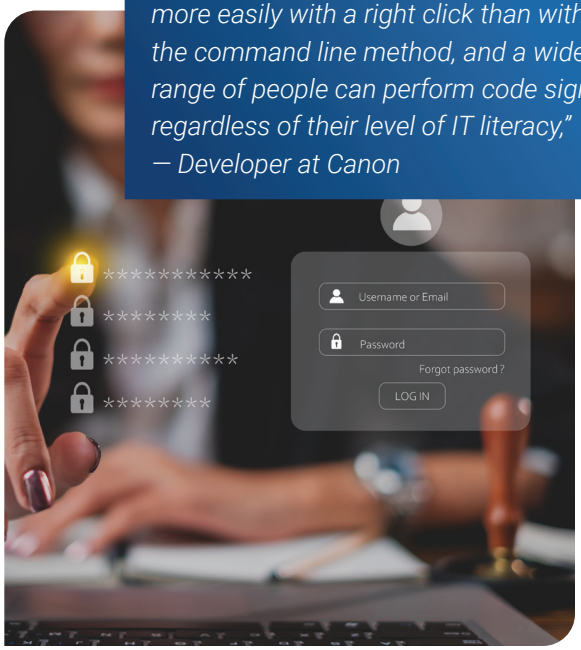
In addition, Software Trust Manager enabled Canon to streamline their code signing workflows, bringing about improved efficiency and productivity. Software Trust Manager comes with multiple code signing methods for each code signing tool and platform that worked seamlessly with the myriad tools used by Canon's development teams.

For example, the DigiCert Click-to-Sign feature directly integrated with Microsoft's SignTool, so that developers could quickly and intuitively sign code without having to learn new tools. Not surprisingly, Canon development teams embraced Click-to-Sign because it so closely resembled normal PC actions. "Code signing can now be performed more easily with a right click than with the command line method, and a wide range of people can perform code signing regardless of their level of IT literacy," one developer commented.

Moreover, Software Trust Manager automated many of the tasks that the previous internal solution required users to do manually. Even better, Software Trust Manager automatically logged each code signing activity, eliminating the need for developers to manually enter the history into the management system. This automation not only saved time but also improved the accuracy and completeness of code signing records.

"Software Trust Manager has reduced developers' workloads by about half for each signing session," said the service administrator. "Now that all code signing operations are centrally managed and controlled, we have been able to streamline our code signing processes, giving us the highest level of security and trust."

DigiCert Click-to-sign



"Code signing can now be performed more easily with a right click than with the command line method, and a wide range of people can perform code signing regardless of their level of IT literacy,"
— Developer at Canon

Ensuring compliance with industry standards and regulations while enabling future security enhancements

In addition to providing centralized management of code signing keys and certificates and strict role-based access control, Software Trust Manager enforces corporate security policies and regulatory compliance, such as the 2023 CA/B Forum mandate for secure key storage, while also providing Canon comprehensive visibility into their security posture. Now the company security teams can promptly identify potential compliance gaps and make sure they stay aligned with industry best practices and regulatory demands.

By deploying Software Trust Manager, Canon now is confident that its code signing processes meet the highest standards of security, protecting its customers and maintaining the trust and reliability associated with the Canon brand. "We look forward to continuing to work with DigiCert and exploring other capabilities of Software Trust Manager to further secure our software development lifecycle," said the Product Security Lead at Canon.

Get started today with DigiCert® Software Trust Manager by contacting us here.