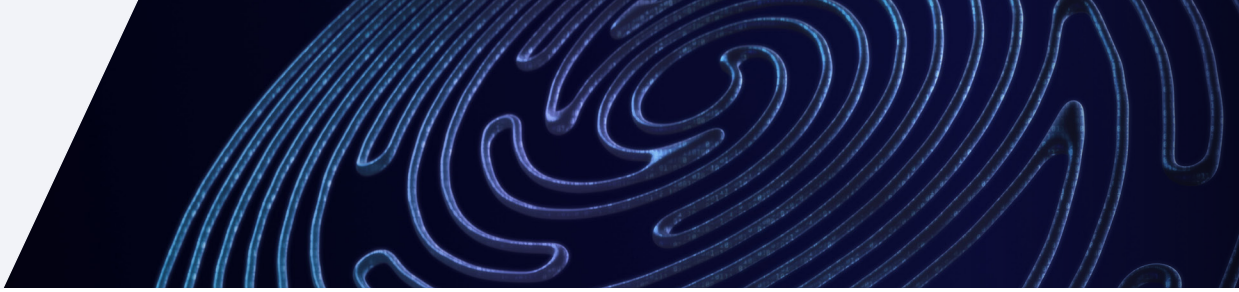
Venafi



DATA SHEET

Venafi CodeSign Protect

Secure the code signing process across your enterprise that is fast and easy for developers to use

Key Features

Secure Private Keys
Code signing keys never leave secured, encrypted storage, even during a code signing operation.

Enforce Code Signing Policies
InfoSec defines corporate code signing encryption and certificate policy for the organization.

Automate Code Signing Workflows
Development teams establish code signing key approval and usage workflows.

Maintain Enterprisewide Visibility
An irrefutable record of all code signing activity is available to InfoSec and compliance teams.

Easy Code Signing
Developers continue to use the same tools, including those for DevOps. Code signing certificate management is automatically handled.

Fast Code Signing
Developers do not need to upload large applications to be signed on a central server as code signing occurs locally on their build machines.

For decades, companies have used code signing to ensure that their customers can trust the software they deliver. Properly signed software is intended to prove creatorship of the software and prevent unauthorized changes from being made to it (such as malware being added by a third party).

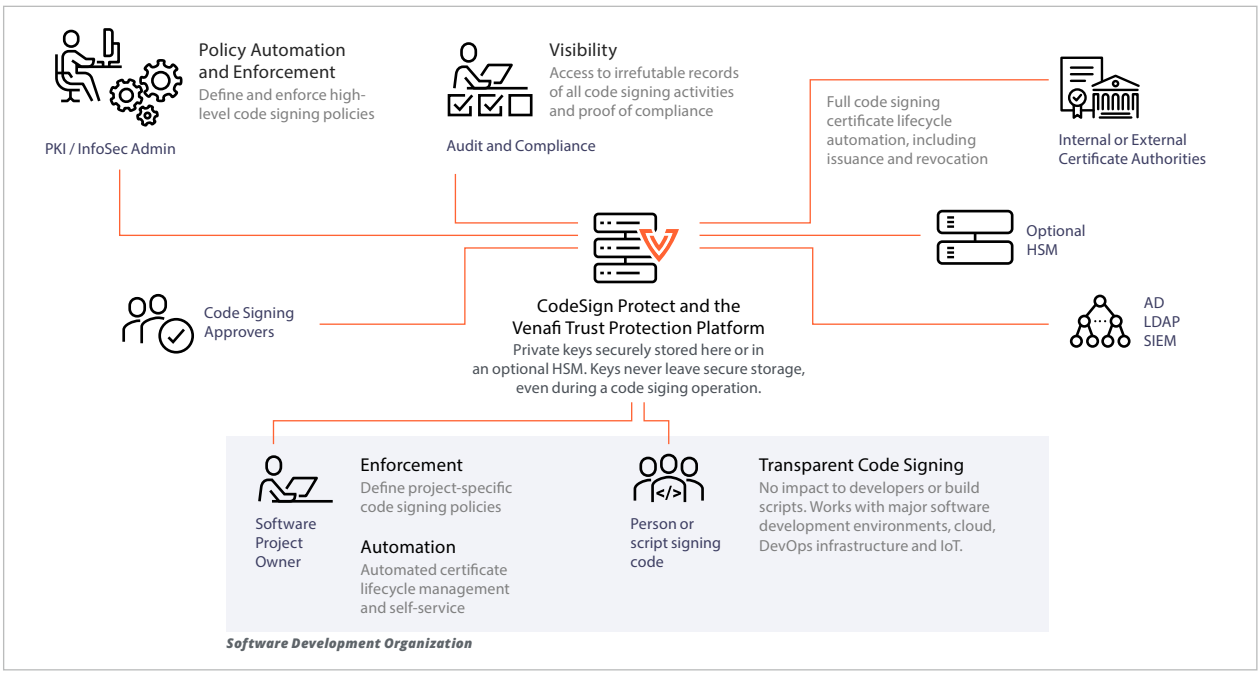
Numerous high-profile incidents have been reported where cybercriminals have stolen or misused unprotected code signing credentials. As a result, businesses down the software supply chain can get infected with malware that exposes them to additional security breaches.

Software developers often do not take the necessary precautions to protect the code signing credentials they use to sign their software. According to NIST's Security Considerations for Code Signing paper, not only should code signing keys be stored in an encrypted and secure location, but secure code signing processes should be created to establish who has access to the keys and under what circumstances.

Venafi CodeSign Protect

Venafi CodeSign Protect secures enterprise code signing processes by providing centralized and secure key storage along with role-based policy enforcement. Providing code signing-as-a-service, it reduces the burden on development teams by integrating with the tools and processes they already use.

By combining visibility and intelligence with workflow automation and controls, CodeSign Protect guards against unauthorized use of code signing certificates while providing an audit trail of all code signing activities.



CodeSIgn Protect offers a role-based approach to securing the code signing process. InfoSec defines high-level policy. Development team leads establish the approval and usage process for a code signing certificate. All code signing keys are stored in the Venafi encrypted trusted store or an attached hardware security module (HSM). CodeSign Protect automates the certificate lifecycle process.

Why use Venafi CodeSign Protect?

Never worry about your private keys being stolen or misused

Code signing private keys never leave the secure storage location that InfoSec specifies, either in Venafi's trusted vault or a connected HSM.

Maintain visibility across the enterprise

Using the detailed intelligence gathered, Venafi CodeSign Protect provides compliance and audit reporting that includes all code signing activities.

Ensure that code signing policies are defined and enforced

Using Venafi CodeSign Protect, project owners can control code signing policy definitions. They can define who approves requests, who can access the certificates and what code signing tools can be used.

Provide value to your development teams

Venafi CodeSign Protect plugs directly into native code signing tools provided by most software development environments. By providing an automated code signing service, the hassle and overhead of personally managing and requesting code signing certificates is eliminated, improving efficiency.

For more information about this product, its features, and how other customers use it, scan this QR code or go to:

venafi.com/platform/codesign-protect

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**