Venafi

SOLUTION BRIEF

Stop Unauthorized Code

Reduce your attack surface and harden security by preventing the execution of unauthorized code across all environments

Stop Unauthorized Code solution components

- **Venafi CodeSign Protect.** Secures the code signing process while enforcing enterprise-wide code signing policies.
- **Venafi CodeGuard Service.** Delivers comprehensive, ongoing support and guidance to maintain a robust cybersecurity posture.

Malicious code is evolving quickly, and while most organizations invest heavily to secure critical software infrastructure, they tend to overlook the protection of their internal software against attack. This oversight can leave macros, PowerShell scripts, applications, and containers exposed to tampering and malware attacks. To prevent these types of attacks, it's crucial that your security strategy permit only authorized code to execute across your enterprise.

To tackle this challenge, large enterprises—particularly in highly regulated environments—are prioritizing their security efforts to prevent unauthorized code from executing. Many are adopting protective strategies such as application control, a security measure that allows only approved applications and processes to run in their environments.

This approach is not just a matter of internal policy, as major security frameworks emphasize the importance of application control as an indispensable practice for defending systems, networks, and data from cybersecurity threats and unauthorized intrusions.

Application control is recommended by a variety of security standards, including:

- NIST
- CIS
- PCI DSS
- CMMC
- OWASP
- ISO/IEC 27001
- Essential Eight
- Zero Trust Security Framework

Traditional application control is useful, but with its static list of approved applications, can suffer from drift, where the list of approved applications gets quickly outdated – meaning IT and security teams take on the additional burden of maintaining this list, in order to ensure business processes continue uninterrupted.

Solution overview

Venafi provides an end-to-end solution to streamline and enhance the benefits of traditional application control. Our unique Stop Unauthorized Code solution prevents the execution of unauthorized code, while overcoming the common challenges of traditional application control. It maintains rigorous control over code execution by verifying trusted signers and enforcing strict code execution policies, ensuring the protection of data and systems. This process is crucial because if intrusion detection systems can't spot hidden malicious code, your company might be at a higher risk of malware attacks, zero-day exploits and the like.

Venafi's integrated solution for stopping unauthorized code combines the power of Venafi CodeSign Protect and Venafi CodeGuard Service. Together, they create a solution designed specifically for stopping unauthorized code within your unique security environment. Combined with Venafi's expansive integrations with your current security vendors, this approach is the optimal method to ensure that only the code you authorize is permitted to run.

Stop Unauthorized Code Across All Environments

Solution highlights:

- **Secure code signing process:** Information security teams can automate and secure the entire code signing lifecycle, reducing the burden on development teams. Code is signed using private digital certificates or those issued by trusted Certificate Authorities. Afterward, a cryptographic hash is attached to the code before it is encrypted with a private key linked to the code signing certificate. This ensures that only verified and authenticated code can execute.
- **Dynamic certificate-based application control:** A dynamic and authorized list of certificates reduces the workload on InfoSec teams, while improving compliance and security. Teams can maintain the list with utmost flexibility through their operating system or existing security solutions such as endpoint protection platforms with built-in capabilities to manage certificate-based allowlists.
- **Certificate verification:** Before code or software can execute, the solution actively checks the digital signature against trusted code signing certificates. The integrated solution allows only valid signatures associated with trusted certificates, which indicate authentic and unaltered software.
- **Execution policy control:** To prevent unauthorized software from running, the solution blocks code that doesn't employ valid, a trusted code signing certificate or isn't on the approved certificates list.
- **Ongoing tailored support and guidance:** Comprehensive, ongoing support and guidance from Venafi's trusted team of security experts helps customers tailor the solution to specifically meet their organization's needs. This includes configuring and optimizing third-party technology integrations with your existing security vendors and workflows. This includes configuring and optimizing third-party technology integrations with your existing security vendors and workflows.

Solution benefits:

- **Mitigate risk:** Reduces the risk of unauthorized code execution, mitigating systems intrusions, data breaches, system vulnerabilities and compliance violations.
- **Tamper detection:** Preserves code integrity by detecting any modifications made to the code after signing, preserving system and data integrity.
- **Regulatory compliance:** Aligns with regulatory standards and industry best practices, simplifying compliance requirements for application control and code signing.
- **Low maintenance:** Automates the creation and upkeep of a dynamic certificate-based allowlist, minimizing maintenance efforts and enhancing compliance and security.
- **Rapid response:** Allows for swift response to emerging threats through the revocation of code signing certificates to block unauthorized software execution in a dynamic threat landscape.
- **Proactive threat prevention:** Ensures that malicious code, zero-day exploits, and known vulnerabilities are unable to execute and compromise the system or network.
- **Scalable, flexible and seamless integrations:** Integrates smoothly with existing systems, minimizing workflow disruptions, and scales and adapts to diverse platforms and organizational needs.

Solution components

Using an end-to-end approach, the Venafi Stop Unauthorized Code solution is built on a strong product foundation that secures and streamlines the code signing process and is accompanied by professional services that optimize your infrastructure to enable third-party technologies to prevent unauthorized code execution.

Product: Venafi CodeSign Protect

Venafi CodeSign Protect secures enterprise code signing processes by providing centralized and secure key storage along with role-based policy enforcement. Using a code signing-as-a-service approach, it alleviates the workload 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.

- **Ensure code authenticity and integrity:** CodeSign Protect maintains the code signing trust chain, ensuring both the authenticity and integrity of the code, assuring that software originates from an approved source and hasn't been altered since signing.
- **Prevent private keys from being stolen or misused:** Code signing private keys never leave the designated secure storage location, either in Venafi's trusted vault or a connected HSM.
- **Maintain code signing visibility across the enterprise:** Using the detailed intelligence it gathers, CodeSign Protect provides compliance and audit reporting that includes all code signing activities.
- **Define and enforce code signing policies:** Using 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.
- **Streamline code signing for development teams:** 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.

Ongoing professional services: Venafi CodeGuard

Included as an essential element of the Stop Unauthorized Code solution, Venafi CodeGuard Service delivers comprehensive support to stop unauthorized code in your environment. This service component ensures that organizations can not only configure and enable 3rd-party advanced unauthorized code prevention technologies, but also receive ongoing support and guidance necessary to maximize their investment and maintain a robust cybersecurity posture.

With access to Venafi's experienced security professionals and tailored solutions, Venafi CodeGuard Service ensures organizations can effectively stop unauthorized code, without disruption to existing systems and workflows.

Services include:

Expert guidance and solutioning

- Ongoing access to experienced security professionals who provide expert advice and recommendations tailored to meet organizational requirements.
- Assistance in designing and implementing a solution that best aligns with your organization's unique IT infrastructures, business processes, and security requirements—while still adhering to best-practice principles and standards.

Training and knowledge transfer

- On-the-Job training sessions for IT and information security teams to effectively manage and utilize the Venafi solution.
- Ongoing knowledge transfer to keep staff updated on the latest features, best practices and security strategies.

Compliance and regulatory support

- Assistance in navigating complex regulatory environments and to ensure compliance with various cybersecurity standards during the deployment of your Stop Unauthorized Code solution.
- Scheduled reviews to support compliance efforts and provide guidance on emerging trends.

Scalability and futureproofing

- Services designed to scale with the future needs of your organization, ensuring the solution remains effective as your business needs evolve.
- Guidance to help navigate the complexities inherent in updates and changes to reliant systems, while maintaining the existing security framework.

Long-term security planning

- Assistance developing long-term security strategies that align with your business objectives.
- Ongoing consultancy to adapt and evolve these strategies as the business and threat landscapes change.

The ongoing professional services element of Venafi's Stop Unauthorized Code solution focuses on providing continuous, expert-level support and guidance to enhance the effectiveness and efficiency of unauthorized code prevention strategies.

Start now to stop unauthorized code

The Venafi Stop Unauthorized Code solution empowers organizations with a comprehensive approach to code execution security that is designed to reduce risks and enhance compliance. Find out how you can get enterprise-wide visibility into your code signing operations and start building the foundation you need to stop unauthorized code from running across any environment.

Learn more about
Venafi's Stop Unauthorized Code Solution

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, mobile and user access. **To learn more, visit venafi.com**