Transportation Company Thwarts Ransomware Attack by Locking Down Code Execution

CyberArk Code Sign Manager helps firm streamline key management, improve visibility, and secure script execution—at enterprise scale

↑ Back to Top

Jump to

Summary

A transportation company was hit by ransomware that infected internal virtual servers and halted operations. Rather than comply with the attacker's demands, the company shut down affected systems and restored from backups—then moved quickly to harden its defenses. By deploying certificate-based enforcement with CyberArk Code Sign Manager, the company secured internal scripts and macros to prevent future attacks and regain control over its code execution environment.

Products and services

CyberArk Code Sign Manager →

Solutions

Secure Certificates and PKI →

Company profile

This leading transportation and logistics company delivers mission-critical services across global supply chains and operates under strict uptime and security requirements. With an extensive internal software footprint—including logistics platforms, automation tools, and macros used by employees and partners—the company places a premium on secure and reliable code execution.

Challenge

After a ransomware attack brought operations to a standstill, a leading transportation company faced a wake-up call. Although InfoSec wasn't sure how the servers had been compromised, they did know that a phishing email with an attached malicious Microsoft Office file had been received not long before the ransomware attack took place.

The company's CISO explained, "Employees are required every year to take cybersecurity training, and we also send them fake phishing emails to test them and keep them on their toes. But it only takes one distracted or careless employee to let malware in."

The director of public key infrastructure (PKI) services mentioned his frustration with the company's struggles with phishing—and his suspicion that some connection existed between the malicious payload and internal scripts. One of the solution architects asked if the company knew that internal macros and scripts could be code signed—and that any macro that wasn't signed could be prevented from executing with the proper security controls in place.

Solutions

To manage and protect their macros and scripts, the company used CyberArk Code Sign Manager to automate security controls that detect, disable, and remove all unsigned macros. They also integrated Code Sign Manager seamlessly with users' preferred toolsets, whether they were developers writing apps using DevOps methodologies or IT members writing PowerShell scripts.

Even better, Code Sign Manager automated everything having to do with signing code, including managing the lifecycle of certificates and enforcing security policy. Once the company saw the product in action, their only remaining question was how quickly Code Sign Manager could scale to manage the security of their internal code. Code Sign Manager quickly proved it could deliver.

Results

Using Code Sign Manager, the company's InfoSec team could now define code signing policy configurations that aligned with corporate security policies. These policies could be configured using important parameters, such as:

- Restricting issuance of code signing certificates only to approved certificate authorities (CAs).
- Setting minimum encryption strength of private code signing keys.
- Specifying the management approvals required before a code signing key could be used.

Code Sign Manager enabled the company to set up multiple configurations uniquely tailored for each functional area of the organization. Because Code Sign Manager automatically manages code signing certificate lifecycles—including issuance and renewal—it ensured the right keys and certificates were available to authorized end users based on each use case.

Once initial policies were finalized, the company's IT department configured employees' computers and Microsoft Office suites to require that all shell scripts and macros be signed with a company-authorized code signing certificate before they could execute.

"No more complexity. No more overhead. My team can now support thousands of employees without worrying about their expertise or skill level," said the director of PKI services. "This level of simplicity is essential to ensure widespread adoption across our enterprise—the only way code signing serves as an effective means to help stop future ransomware attacks."

Beyond reducing the risk of third-party scripts and macros spreading malware, Code Sign Manager gave the InfoSec team visibility into every code signing operation across the enterprise—regardless of what was being signed or which tools were used. This single-pane-of-glass view supplied a historical record and an irrefutable audit trail of all code signing activities.

> "Code Sign Manager has enabled us to secure all our code regardless of the type. It's not only easy to use, but it also keeps us safe.
>
> **– CISO, Transportation Company**

Key benefits

- **Security:** Prevented execution of unsigned or unauthorized scripts and macros, minimizing ransomware risk and supply chain exposure.

Related customer stories

Modernized Code Signing Helps Healthcare Innovator Reduce Risk and Speed Up Development

Read Case Study →

Global bank transforms how it secures loan applications

Read Case Study →

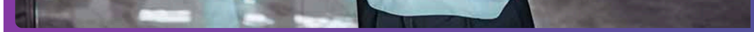
Cisco Protects the Bridge to the Possible by Holistically Securing Human and Non-human Identities

Read Case Study →

Talk to an expert

Understand the key components of an Identity Security strategy

Get a first-hand look at CyberArk solutions



STAY IN TOUCH

Keep up to date on security best practices, events and webinars.

Tell Me How

Support

- Contact Support
- Training & Certification
- CyberArk Community
- Technical Support
- EPM SaaS Register / Login
- Product Security

Resources

- Resource Center
- Events
- Blogs
- CIO Connection
- CyberArk Blueprint
- Scan Your Network
- Marketplace

Partners

- Partner Network
- Partner Community
- Partner Finder
- Become a Partner
- Alliance Partner

Company

- Investor Relations
- Leadership
- Newsroom
- Office Locations
- Environmental, Social and Governance

CYBERARK®
A PALO ALTO NETWORKS COMPANY

Terms and Conditions Privacy Policy Your Privacy Choices Cookie Preferences