Fortune 500 Chemical Manufacturer Implements Best Practice Security to Defend Against Code Manipulation and Cyberattacks

An international Fortune 500 chemical manufacturer that uses software allowing its customers to make custom requests needed to protect that software from tampering and manipulation. In doing so, it found it could use the same Entrust solution to help raise its security posture and protect its business from cyberattacks.

Business challenge

Despite the chemical manufacturer providing many thousands of standard options, there is still significant demand for custom mixes to suit customer needs. In order to fulfill these requirements, customers download software provided by the manufacturer, enter their custom requirements, and send the information back to the manufacturer for processing. The challenge was to ensure the authenticity of the software as it's delivered to the customer and then back to the manufacturer, determining that it hasn't been modified since it was published, potentially for malicious purposes.

> **“Using an HSM to protect cryptographic keys is a requirement for code signing and a recognized best practice for privileged access management. By implementing Entrust nShield as a Service across both of these use cases, we've significantly improved our security posture.”**
>
> IT Manager, Fortune 500 Chemical Manufacturer

LEARN ABOUT nSHIELD AS A SERVICE AT ENTRUST.COM/HSM

Chemical Manufacturer Case Study

Technical challenge

Code signing is a recognized method of identifying software and assuring users of the code's origin and that it has not been tampered with since publication. Digital signatures provide a proven way to establish authenticity and expose any attempt to tamper with the code, protecting end-users from cybersecurity dangers such as advanced persistent threats (APTs). All modern operating systems look for and validate digital signatures during software installation and provide warnings about unsigned code. However, the security provided by a digital signature is directly related to the measures taken to protect the cryptographic keys on which they are based.

Like virtually every IT department, the chemical manufacturer's IT department was resource-constrained. This meant the solution would need to be a centralized system that was easy to implement and manage. In addition, the company was in the process of moving much of its IT infrastructure to the cloud, so it required a cloud-based solution.

Solution

The chemical manufacturer deployed Entrust Code Signing Gateway together with Entrust nShield® as a Service Hardware Security Modules (HSMs).

For an organization that needed an enterprise-grade, controlled software signing approval process, the Entrust Code Signing Gateway provided a range of flexible and centralized workflow automation functions that helped the chemical manufacturer meet its strong security requirements.

The Code Signing Gateway manages authorization workflow, accepts requests, notifies approvers via email, manages time-outs, acknowledges approvals, logs activity, and delivers signed code to the staging area.

Entrust nShield as a Service uses cloud-based HSMs to protect the private key used to sign the code, providing a root of trust. The signing keys reside in the FIPS 140-2 certified HSMs and are mapped to multiple signing profiles that can be created in the Code Signing Gateway. This prevents the potential loss of valuable signing keys – the keys to the code's authenticity and integrity.

The Code Signing Gateway integrates with Microsoft Active Directory to provide user authentication and manage approval groups. It can be accessed through a traditional web-based portal or through a RESTful API, allowing integration into automated build process or customer workflow engines.

The Entrust Code Signing Gateway is customized for each customer's unique environment by the Entrust professional services team.

Chemical Manufacturer Case Study

Protecting against cyberattacks

As a large, international enterprise with many employees, consultants, and contractors – all needing to access the company's data – how do you ensure they can do so without compromising the security of that data? As one IT manager for the company notes, "For a large organization, security is a big issue, and getting hacked is a big problem. It's a big reputation issue. It's a big image issue. So, we need to protect both our customers and ourselves."

The chemical manufacturer was working with HashiCorp, an Entrust technology partner, to deploy privileged access management (PAM) tools to authorize, manage, and audit account and data access by specific users and applications. PAM tools allow customers to:

- Protect privileged credentials within a secure, encrypted vault
- Limit access to specific systems based on the user's role
- Grant access for a specified time period and automatically revoke it on expiration
- Monitor and audit each privileged activity

HashiCorp Vault manages and protects sensitive data by securing, storing, and tightly controlling access to tokens, passwords, certificates, and encryption keys for protecting secrets and other sensitive data. The security foundation of HashiCorp Vault is the encryption and decryption of secret assets with the master key protected by an Entrust nShield HSM.

Having already deployed Entrust nShield as a Service to secure its code signing requirements, the chemical manufacturer was able to deploy the same Entrust HSM service to provide a robust root of trust to its HashiCorp Vault PAM solution.

> **"For a large organization, security is a big issue, and getting hacked is a big problem. It's a big reputation issue. It's a big image issue. So, we need to protect both our customers and ourselves."**
>
> IT Manager, Fortune 500 Chemical Manufacturer

Chemical Manufacturer Case Study

CUSTOMER PROFILE

Business need

- A way to secure software downloads to customers who need the software to customize the end product
- Enterprise digital security that accommodates multiple users from inside and outside of the organization
- Keep overhead low and manageable

Technology need

- A secure code signing solution
- A secure privileged access management system
- A centralized, easy-to-implement, easy-to-use cloud-based system

Solution

- Entrust nShield as a Service cloud-based HSM
- Entrust Code Signing Gateway
- HashiCorp Vault

Result

- Compliance with code signing standards
- A significantly improved security posture
- Simple, pain-free implementation

Result

Entrust nShield as a Service is a subscription-based solution for generating, accessing, and protecting cryptographic key material – separately from sensitive data – using dedicated FIPS 140-2 Level 3 certified Entrust nShield HSMs. The solution delivers the same features and functionality as on-premises HSMs combined with the benefits of a cloud service deployment. This allows customers to fulfill their cloud-first objectives and leave the maintenance of these appliances to the experts at Entrust.

Customers can easily migrate their cryptographic operations from on-premises to the cloud, or use a hybrid approach, mixing both cloud-based and on-premises nShield HSMs.

According to the chemical manufacturer's IT manager, "Using an HSM to protect cryptographic keys is a requirement for code signing and a recognized best practice for privileged access management. By implementing Entrust nShield as a Service across both of these use cases, we've significantly improved our security posture."

"The implementation of HashiCorp Vault was super easy. Two team members accomplished it in an afternoon. The Entrust professional services team onboarded us with nShield as a Service and customized and installed the Code Signing Gateway. The overall implementation process for both of these projects was pain-free. I'm happy and my team is happy."

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223