Case Study

# Thales and SignPath Help Software Development Company Protect Against Supply-Chain Attacks

cpl.thalesgroup.com

THALES
Building a future we can all trust


**SignPath together with Thales Luna Cloud HSM on the Data Protection on Demand (DPoD) marketplace provide end-to-end software supply chain security, from source code repository to deployment.**

## The Organization

Based in the United States, the company develops software that helps businesses manage networks and IT infrastructures.

The company serves customers worldwide, including many Fortune 500 customers and US government agencies.

## Business Need

Following an extensive, targeted supply-chain attack, the company sought to overhaul their security posture. Critical to meeting a defense in depth requirement is the usage of FIPS certified HSMs.

What happened? A build server was captured and code was injected through the build process. During the attack, the hackers injected malicious code in the software production pipeline. The attack went undetected for months and was extremely destructive.

The most important discovery coming out of this attack was that traditional code signing is not enough to protect your software supply chain. The company had a code signing infrastructure in place, but the hack happened elsewhere in the build process. The code signing gave a false sense of security that the software was to be trusted when it was already infiltrated.

## The Solution

The company selected SignPath's end-to-end software development security solution, which provides the customer a simple way to make sure that every signed and published release of their software can be traced back to a specific source code version.

At the core of the solution is Thales Luna Cloud Hardware Security Modules (HSM) on the Data Protection on Demand (DPoD) cloud-based marketplace. The Luna HSM product family represents the highest-performing, most secure, and easiest-to-integrate HSM solution available on the market today. Luna HSMs offer flexible deployment options, including on-premises, as-a-service, in the cloud or across multiple environments to create a hybrid HSM solution. Within DPoD, the customer is assured its own dedicated Luna Cloud HSM instances to store and manage the keys and establish a common root of trust across all applications and services within the software supply chain. The Luna Cloud HSM services are hosted in a data center with physical and logical access controls. Every signing operation takes place on the HSM ensuring that the private key is never exposed.

SignPath is fully integrated with Luna Cloud HSMs, and when you combine features from two proven platforms, you find the perfect balance of agility and security. SignPath.io is built with DevSecOps in mind and integrates seamlessly with your software pipeline without compromise to cybersecurity.

## Benefits

After implementing the SignPath code signing backed by Thales Luna Cloud HSMs, the company is assured its software development is secure every step of the way. Every signed and published release of their software can be traced back to a specific source code version without room for manipulation, and meets all policy requirements, including reviews and testing.

The foundation for the code signing process is the secrecy of the private key, and the company is provided its own dedicated Luna Cloud HSM instances to store and manage the keys. DPoD can be readily deployed, without procurement, installation, configuration, and training delaying deployment.

"With DPoD, our total cost of ownership is considerably lower than it would have been purchasing on-premises HSMs," the customer said. "And because the service is fully managed, there is less room for human errors that could lead to a security breaches or key loss."

DPoD Luna Cloud HSMs provide high availability and disaster recovery by default.

SignPath

## About SignPath

SignPath is dedicated to Software Supply Chain security, providing best-in-class end-to-end software development security solution that ensures code integrity every step of the way. SignPath serves customers worldwide, from small development teams to large enterprises.

## About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.