Solution Brief

THALES

CYBERSECURITY

The End-to-End Software Integrity Solution

Together, SignPath and Thales create an end-to-end trusted release process: fully automated, fully auditable, and built for modern DevOps.

cpl.thalesgroup.com

THALES

CYBERSECURITY

The End-to-End Software Integrity Solution

Together, SignPath and Thales create an end-to-end trusted release process: fully automated, fully auditable, and built for modern DevOps.

Key benefits

Security

- Prevents compromised builds from receiving valid signatures through pipeline verification.
- Keys never leave the HSM, eliminating risk of theft and misuse.
- Resistant to insider threats with enforced approvals and role-based controls.

Developer Velocity

- Seamless integration with leading CI/CD tools.
- No manual key handling: developers remain focused on coding.
- Nested signing and artifact validation reduce build complexity.

Compliance & Auditability

- Complete, exportable audit trails: who signed what, when, and under which policy.
- Built-in support for NIS2, Cyber Resilience Act (EU), NIST SSDF, Executive Orders 14028 and 14144 (U.S.); and SLSA.
- Long-term artifact and log retention, structured approval workflows.

Scalability & Flexibility

- Available as SaaS, self-hosted, or hybrid deployment.
- Modular architecture: start with Semantic Code Signing, extend to Pipeline Integrity and Software Attestation.
- Supports a wide range of formats: apps, drivers, containers, macros, SBOMs.

The Challenge

In today's escalating threat landscape, software supply chain attacks have become one of the most damaging and fastest growing risks.

Incidents like the breaches of SolarWinds and 3CX show how attackers target the development process itself - injecting malicious code before release, and getting it signed as if it were alongside legitimate software updates.

Yet, many organizations still assume that code signing equals security. But if the signing process is compromised, even malware can carry a valid signature - enabling it to evade protections that organizations rely on, making detection nearly impossible.

As a result, software teams are forced to secure not just their code, but the entire CI/CD pipeline - without slowing down delivery.

Key challenges include

- Manual, inconsistent signing workflows
- Insecure key handling and limited access
- Lack of enforcement of policies, reviews, or scan results
- No centralized visibility or traceability
- Growing audit and compliance pressure

Traditional signing tools and even isolated use of HSMs alone can't solve these problems. What's needed is an end-to-end software integrity platform built for modern development and release pipelines.

The Solution

The SignPath Software Integrity Platform goes far beyond traditional code signing.

It ensures that only verified, policy-compliant, and traceable artifacts are signed and released - by securing both the what and the how of software delivery.

The SignPath Software Integrity Platform combines three core capabilities:

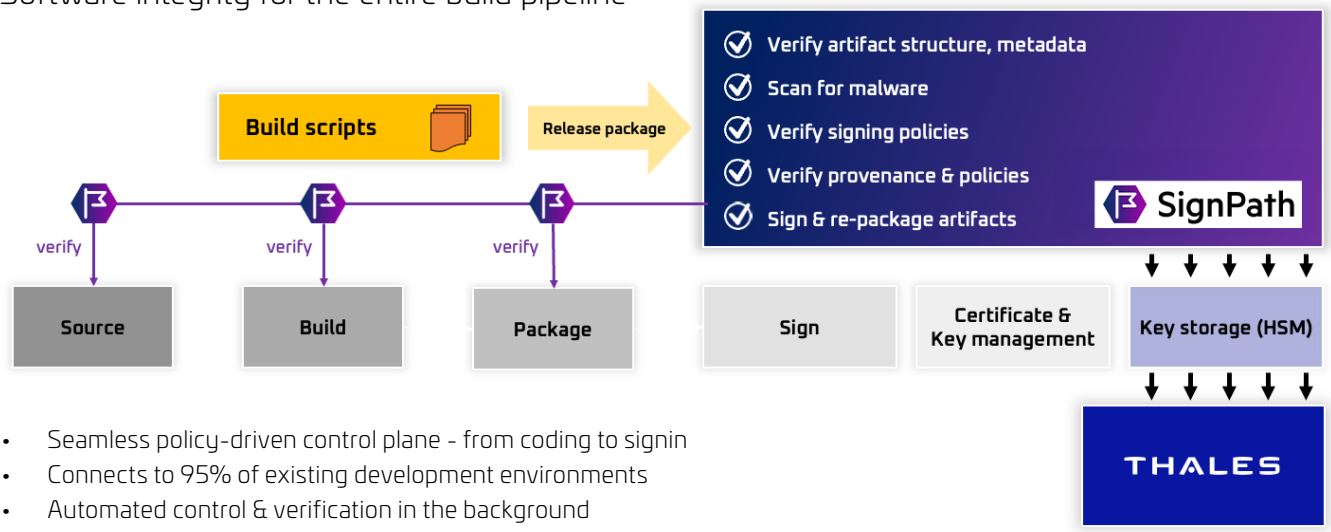
- **SignPath Pipeline Integrity**
  Validates the entire build process: origin, source branch, test results, and approvals – before signing.
- **SignPath Semantic Code Signing**
  Signs only compliant artifacts via automated workflows with policy enforcement, structural checks, and nested signing support.
- **Software Attestation**
  Creates signed evidence for every release. It captures build provenance, policy conformance, release integrity, and compliance-relevant information in attestations that can be verified by machines, auditors, customers, and partners.

At the core of the solution is **Thales Luna Cloud Hardware Security Modules (HSMs)** on the **Data Protection on Demand (DPoD)** cloud-based marketplace. 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 Software Integrity Platform

Software integrity for the entire build pipeline



- Seamless policy-driven control plane - from coding to signin
- Connects to 95% of existing development environments
- Automated control & verification in the background
- Rule- and policy-based
- End-to-end coverage
- Audit-proof documentation of all signing requests

Solution Key Features and Benefits

- **Policy Enforcement**
  Only reviewed code from approved pipelines gets signed - fully automated
- **Deep CI/CD Integration**
  Native support for GitHub Actions, Azure DevOps, Jenkins, GitLab, and TeamCity
- **Secure HSM-backed Signing**
  Keys stored and used exclusively within Thales HSMs (DPoD or on-prem)
- **Artifact-level Verification & contextual metadata checks**
  Build provenance, artifact structure, and approval status
- **Broad Format Support**
  Sign installers, containers, drivers, Office macros, scripts, and SBOMs
- **Audit-Ready**
  Full traceability with exportable records for each signed artifact

Summary

By combining SignPath's best-in-class software development security solution with top-of-the-line private key security from Thales, you get an unparalleled software supply chain security solution.

About SignPath

SignPath is a European provider of software integrity solutions, headquartered in Vienna.

The SignPath Software Integrity Platform enables policy-controlled and fully traceable software release processes that go beyond traditional code signing.

With the SignPath Software Integrity Platform, organizations ensure that only verified, authorized, and fully traceable releases are signed.

SignPath serves enterprises and critical infrastructure providers across multiple industries, including finance, healthcare, industrial, and public sector organizations.

About Thales

Thales is a global leader in cybersecurity, helping the most trusted organizations protect critical applications, data, identities, and software anywhere, at scale. Through Thales' integrated platforms, customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

cpl.thalesgroup.com

Contact us – For contact information, please visit cpl.thalesgroup.com/contact-us

© Thales - September 2026 • AC v6