REVERSINGLABS

# Global Energy Leader: Securing Third-Party Software at Enterprise Scale with ReversingLabs

90+ terabytes of approved software sat dormant in network file shares, previously vetted through procurement, trusted by policy, and never once scanned for malicious content. For a global energy leader running critical IT and OT infrastructure, legacy security tools fell short of processing the size and complexity of software present. The attack surface wasn't unknown. It was unexamined.

## The Challenge: Managing Third-Party Software Risk Without Source Code

Like many large enterprises, our customer faced a significant and growing challenge, managing the risks associated with third-party software. The fundamental challenge was trust. The organization was forced to rely on vendor assurances for software it had no practical means to independently verify, in an environment where a single compromised package could have far-reaching operational consequences. This included not only newly acquired applications, but also a vast backlog of previously purchased software already deployed across the organization.

Prior efforts to assess the risk presented by commercial off-the-shelf (COTS) software relied on traditional application security testing methodologies. While well-intentioned, these approaches fell short not due to a lack of rigor, but because legacy tools were not designed to handle the realities of modern software.

**CUSTOMER:** Global Energy Leader

**HEADQUARTERS:** North America

**EMPLOYEES:** 50,000+

**INDUSTRY:** Energy

### CHALLENGES:

- Limited visibility into COTS software
- Existing tools fail on large binaries
- Inconsistent security checks
- Reliance on vendor trust

### SOLUTION:

- Binary analysis delivers pass/fail verdicts, enabling fast, policy-driven approval of third-party software at enterprise scale

Many COTS applications procured by the organization were delivered as large, multi-gigabyte packages, exceeding file size limits imposed by conventional security tools. In addition, limited support for diverse file formats made it difficult to analyze software in the form it was distributed by vendors. Compounding the challenge, the company was required to repackage each COTS binary using an endpoint management platform to ensure compatibility with the enterprise technology stack, introducing additional files and artifacts that expanded the attack surface. As a result, security checks became inconsistent, creating stage gates that could not be reliably enforced across all software acquisitions.

This inconsistency posed a growing challenge in their complex environment. Without a scalable way to inspect third-party software artifacts, teams were forced to rely on vendor assurances and point-in-time checks that provided limited visibility into the contents of the software being deployed. Legacy AST tools, designed primarily for first-party development workflows, lacked the coverage and flexibility needed to support enterprise-scale COTS software onboarding.

Internally, this organization also faced resource constraints. The teams responsible for onboarding new software were not malware experts or incident responders. Our customer required clear, decisive "go/no-go" decisions, not raw technical findings that required extensive analysis to interpret.

Decades of digital transformation and acquisitions also introduced unique complexities, most notably a "digital junk drawer" – an accumulation of network file shares containing terabytes of previously approved software. While this software could be reinstalled at any time, it had never been systematically inspected for malicious content, exposing a significant and unaddressed attack surface for the business.

## The Solution: Binary-Level Assurance Across New and Existing Software

The organization adopted ReversingLabs as a core control for managing third-party software risk at scale, focusing on two primary workflows:

**1. Secure Onboarding of Newly Acquired Software**

As new software moves through procurement, artifacts are uploaded into ReversingLabs Spectra Assure® and evaluated using predefined security policies. These policies are designed to surface critical issues, such as malware or tampering, while minimizing noise.

### RESULTS:

- Verified COTS software without source code
- Faster, policy-driven approval decisions
- Verified trust in legacy software at enterprise scale
- Reduced false positives with expert validation

### RL PRODUCTS:

- Spectra Assure
- Spectra Analyze
- Spectra Detect

For the new software onboarding team, the outcome is intentionally simple:

- Clear pass/fail verdicts to facilitate software approvals
- Policy-driven actions, only flagging issues when they exceed organizational tolerance
- An escalation path to ReversingLabs experts when deeper validation is required.

This approach enables the organization to push binary-level assurance directly into procurement workflows, establishing a reliable security stage gate that screens third party software packages before approval, without requiring procurement or onboarding teams to have malware analysis expertise.

This unique blend of advanced detection technologies with human confirmation delivers high-confidence malware verdicts. Offloading this behind-the-scenes investigation work to ReversingLabs helps this global energy leader augment non-technical teams with expert malware analysts, reduce false-positive noise, and free up constrained resources to focus on what matters most.

**2. Visibility Into Existing Software Assets**

To address risk across software already deployed and stored in its extensive “digital junk drawer”, this organization leverages ReversingLabs to inspect large volumes of historical software at scale. This repository spanning more than 90+ TB of software artifacts contains previously approved applications that may be reinstalled at any time, making visibility into dormant threats a critical requirement.

Using ReversingLabs Spectra Detect, our customer was able to scan software directly from network file shares to identify malicious and suspicious files without requiring prior repackaging or manual sorting. The organization evaluated multiple workflows during an on-premises proof of value, including scanning raw contents with and without file sorting enabled, to ensure the approach could scale across diverse environments.

This process surfaced previously undetected risks within legacy software, including packages where critical origin metadata (such as Mark of the Web) had been stripped, revealing gaps in software integrity that had gone unnoticed despite prior approval.

When Spectra Detect identifies suspicious or malicious artifacts, findings are automatically routed into this organization's internal correlation engine, where security teams can quickly triage risk. From there, analysts can pivot directly into ReversingLabs Spectra Analyze to perform deeper inspection of flagged files, enabling rapid confirmation of true threats versus false positives. In cases requiring additional validation, our customer then engages ReversingLabs malware experts to provide definitive verdicts without burdening internal teams.

The Detect-to-Analyze expert validation workflow delivers a managed outcome across the full software estate. Continuous monitoring of legacy repositories surfaces high-risk artifacts for investigation, while human-vetted verdicts provide confidence that security policy is consistently applied across both newly acquired and long-standing assets.

**The Pursuit of Continuous Improvement**

A critical evolution in this organization's workflow was the adoption of mandatory version diffing, where subsequent releases of an application are compared to identify changes, tracking software quality over time. Rather than treating diffing as optional, our customer embedded it into their onboarding process whenever multiple versions of a package existed.

By analyzing how the software changes between updates, Spectra Assure enables:

- Detection of newly introduced files or behaviors
- Identification of tampering or suspicious modifications
- Validation that vendor-provided fixes actually resolved previously identified issues

This approach offers greater assurance by evaluating the software artifact as it is delivered, not just what the vendor's claim has changed. The ability to track and verify these changes over time also provides valuable data for risk management and compliance purposes.

## The Outcome – Confidence, Coverage, and Assurance

By leveraging the power of ReversingLabs' complete product portfolio, this organization gained a level of visibility into third-party software that was previously unattainable:

1. Independent verification of commercial software without requiring source code
2. Consistent, policy-driven decisions for new software onboarding
3. Scalable inspection of massive existing software repositories
4. Expert validation to confirm true threats while minimizing false positives

Instead of building a new capability from scratch, Spectra Assure seamlessly integrated into an existing business process, delivering assurance where it was previously absent.

For this global energy leader, the value lies not in cutting steps, but in eliminating blind spots – ensuring new and existing software meets and maintains clearly defined security standards.

### Why It Matters - From Assumed Trust to Verifiable Assurance

Our customer's strategy reflects a broader shift across large enterprises: moving away from assumed trust in commercial software toward evidence-based assurance.

Achieving that shift requires a platform built to address the full scope of the problem. By inspecting thousands of software packages across terabytes of historical files stored in distributed network directories spanning diverse file types, ReversingLabs helps organizations manage supply chain risk, protect critical environments, and gain confidence that software is safe to use, before it ever reaches production.

Ultimately, as emphasized in JPMorgan Chase's recent discussion on software trust debt, supply chain risk is a shared responsibility. Enterprises are no longer passive consumers of software. They must actively collaborate with vendors to validate, remediate, and continuously improve security outcomes.

### Learn More About RL Solutions

CONTACT US TODAY

**ABOUT REVERSINGLABS**

ReversingLabs is the trusted name in file and software security. We provide the modern cybersecurity platform to verify and deliver safe binaries. Trusted by the Fortune 500 and leading cybersecurity vendors, RL Spectra Core powers the software supply chain and file security insights, tracking over 422 billion searchable files with the ability to deconstruct full software binaries in seconds to minutes. Only ReversingLabs provides that final exam to determine whether a single file or full software binary presents a risk to your organization and your customers.



CS-Rev-04.20.26

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com