REVERSINGLABS

CUSTOMER: Large Global Bank

HEADQUARTERS: United Kingdom

EMPLOYEES: 75,000

INDUSTRY: Financial Services

Global Bank: Surfacing Risk in Third-Party Commercial Software with Spectra Assure

A global financial institution recognized a requirements gap in its software supply chain security practices — third-party commercial software. Spectra Assure™ provided visibility and governance to the organization's software acquisition process by ensuring that software embedded with suspicious or malicious components was barred from being deployed in their environment.

Spectra Assure enabled the bank to take a comprehensive approach to assessing and managing software supply chain risk by identifying malware, tampering, suspicious behaviors, and vulnerabilities. This deeper level of insight allowed the bank to set repeatable policies and guardrails for new software procurements.

Securing the Software Acquisition Process

The IT Security team at this Fortune Global 500 financial institution recognized a major risk associated with third-party software. With an end-user population of about 75,000 employees, the bank realized they did not have the visibility they needed into commercial software deployments. Ultimately, the team wanted to implement a solution to properly identify the risks in commercial software, and provide a repeatable process to demonstrate that they had proper safeguards embedded within their commercial software procurement process.

> **"We have almost every cybersecurity tool, but Spectra Assure showed us risks we couldn't see before. That was huge."**
>
> Global Head of Windows,
> Large Global Bank

CHALLENGES:

- Limited vetting for third-party applications
- No insight into software threats beyond CVEs
- Strict regulatory requirements

SOLUTION:

- Spectra Assure enables security and risk managers to make informed procurement decisions by identifying embedded software risks and threats

Spectra Assure provided a primary control for the bank's third-party software risk management program by analyzing all incoming commercial software binaries for embedded threats. It filled a major gap in the bank's existing strategy by assessing software binaries to determine whether third-party applications are safe to use without requiring access to vendor source code. Spectra Assure aids in securing the bank's end-to-end procurement process by analyzing software packages before deployment, release updates — and assessing for novel software supply chain threats.

Going Beyond Vulnerability Detection

When it came to assessing third-party software, the bank's existing tool stack consisted primarily of vulnerability and malware scanners — neither of which provided the richness of data that they needed to make educated procurement decisions. Both of these solutions provided inconsistent and often messy results. The IT Security team recognized that they were not accounting for the broader scope of software threat categories. While the bank had controls in place to detect and contain vulnerabilities, it had no such controls for threats like malware, tampering, and suspicious behaviors.

Using complex binary analysis, Spectra Assure can analyze software in minutes without source code. It aggregates the risk and threat findings into the Spectra Assure SAFE Report - a digestible, comprehensive risk assessment providing a summary of the most critical software risks along with recommended actions to fix them. The IT Security team then shares their SAFE reports directly with vendors through a secure, time-bound, password-protect link to solicit the required remediation actions. Sharing SAFE reports directly with vendors enables active collaboration with the bank's vendor partners, drastically reducing median-time-to-fix.

RESULTS:

- Binary analysis provides comprehensive risk assessment to instill governance into all new deployments
- Full visibility into a wider range of software threats like malware, tampering, and suspicious behaviors
- Third-party software security policies aligned with organizational risk appetite and compliance regulations

> **"Our goal is nothing comes in dirty or unknown."**
>
> Global Head of Windows,
> Large Global Bank

RL PRODUCTS:

- Spectra Assure

Implementing Policies and Controls to Third-Party Software Risk

Being a global financial institution comes with the obligation to meet a host of strict regulatory and compliance standards — namely the EU's Digital Operational Resilience Act (DORA) and Cyber Resilience Act (CRA). However, the IT Security team had to strike a balance between instituting proper guardrails for new commercial software procurements while not encumbering the needs of the bank's various business units.

Spectra Assure also reports on a SAFE Level of any software. The SAFE Levels are a series of predetermined and increasingly strict policy requirements that organizations can use to gradually raise the bar in how they scrutinize commercial software. The bank uses the Spectra Assure SAFE Levels as a guide to set policies that meet their risk tolerance, keep them in compliance with regulators, while avoiding bottlenecks with their end-users. Since SAFE Levels are fully customizable, the IT Security team was able to fine tune its policy requirements to account for threats that were considered a non-starter for deployment, making communication with the vendor on necessary fixes much more manageable. Furthermore, this approach provided the team the runway it needed to ensure that mitigating controls were in place for findings that were within acceptable levels of risk.

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, the ReversingLabs Spectra Core powers the software supply chain and file security insights, tracking over 40 billion searchable files daily 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-12.13.24

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com