REVERSINGLABS

SOLARWINDS

CUSTOMER: SolarWinds

HEADQUARTERS: Austin, Texas

EMPLOYEES: 2,300

INDUSTRY: IT Software & Services

SolarWinds: Building a Path to Excellence in Software Supply Chain Security with Spectra Assure

Building an exemplary, leading program devoted to securing a complex, modern software supply chain was the critical objective for SolarWinds after the Sunburst incident. While SolarWinds continued to leverage legacy application security testing tools, they embarked on a mission to identify new tools that could provide novel and deeper insights that identify risks and threats.

That's when SolarWinds added Spectra Assure™ to its development and deployment pipeline. Spectra Assure provides "a final check," CISO Tim Brown said. "ReversingLabs always plays that important final check to say, 'Is anything else in here that is suspect?' that could include unexplained changes to the build process, or unexpected additions to the software. By comparing new builds with previous, known good builds, SolarWinds can "make sure nothing nefarious got into a release," Brown said.

Malware, tampering, suspicious behavior changes, and more can be identified within proprietary, commercial, and open-source components, plus artifacts added during compilation. In addition, Spectra Assure determines if software components or artifacts behave as expected – flagging anomalies, unusual patterns, or changes in behaviors, which is critical for seeing and stopping novel supply chain attacks before release.

Automated prioritization helps product and security teams organize remediation projects for development teams, which is critical for balancing security improvements with delivery timelines.

> **"Securing the software supply chain is one of the biggest challenges that we face as an industry. We need to know how much we can trust each piece of software,and that's where Spectra Assure comes in."**
>
> Tim Brown, CISO, SolarWinds

CHALLENGES:

- Final check of complex software releases
- Comprehensive SBOMs to drive business
- See and stop software supply chain threats
- Manage risk in software components

SOLUTION:

- Spectra Assure assesses software builds before release, providing a comprehensive SBOM, risk assessment, and remediation feedback

SBOMs That Drive Transparency and Business

SolarWinds sees an increasing number of requests for software bills of materials (SBOMs) before purchase. This marks a critical milestone for enterprise procurement where vendor transparency is implemented as a best practice. These prospective customers need software inventory information to effectively manage third-party risk.

"ReversingLabs is what we use to generate that SBOM," Brown said. "Our customers are requesting them. Our customers need them. The ability to produce SBOMs helps us close our deals."

Spectra Assure generates a comprehensive SBOM by analyzing the entire software release that customers will receive, including proprietary, commercial, and open-source components. Assessing software in its final executable state creates a more comprehensive software inventory than tools focused on just open-source components, or rely solely on build manifests specifying the expected software contents rather than the actual contents. SBOMs are exported in CycloneDX or Software Package Data Exchange (SPDX), the two industry-standard formats, to respond to customer requests.

"ReversingLabs is what we use to generate that SBOM. Our customers are requesting them. Our customers need them. The ability to produce SBOMs helps us close our deals," said Tim Brown, CISO, SolarWinds.

Manage Risk in Software Components

As a software developer, SolarWinds must manage risks from third-party, commercial, and open-source components being used within its products. This requires new levels of transparency with third parties creating software components SolarWinds includes in its products. The Spectra Assure SAFE Report simplifies this effort, bringing awareness to the most imminent security issues and expedites remediation. The reports can be used to meet both internal and external compliance requirements and prove due diligence in assessing risks in software components provided by third parties.

RESULTS:

- Improved software supply chain security with rapid analysis of large, complex software before release
- Increased security assurance for prospective customers with a securely shareable, comprehensive SBOM
- Enabled remediation without encumbering speed-to-market with actionable feedback
- Improved risk management for commercial and open-source software components

> **"ReversingLabs always plays that important final check to say, 'Is anything else in here that is suspect?'"**
>
> Tim Brown, CISO, SolarWinds

RL PRODUCTS:

- Spectra Assure

Next Step: Third-Party Commercial Software Risk

Like the rest of the industry, SolarWinds is working to improve its third-party risk management and process for the commercial software they use. “It’s very common practice for people to look for SOC 2s, ISOs, questionnaires, spreadsheets, and that's a lot of the way evaluation is done today. But that evaluation doesn't really give you enough to be able to truly assess the risk of the product that you're buying,” Tim Brown, CISO.

SolarWinds would like to identify any risks or threats in the commercial software they use prior to acquisition or deployment. ReversingLabs makes this risk assessment possible, because Spectra Assure’s complex binary analysis engine does not require access to source code to provide transparency.

Brown shared, “The ideal case is that you're running ReversingLabs on everything prior to purchase. I not only get the SBOM, I also get insights into malicious code or tampering.”

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