REVERSINGLABS

SPEC SHEET

Securing the DoD Software Supply Chain

START HERE

ReversingLabs delivers visibility into software supply chain risks starting with the most comprehensive Software Bill of Materials (SBOM).

Get a complimentary SBOM for your software or third-party package (.exe, .dll, etc.) to comply with Executive Order (EO) 14028 and White House memos on improving the Nation's Cybersecurity. It's a simple, cost effective way to start with SBOMs and get visibility into what's in your software package.

Why ReversingLabs for your SBOM?

- Comprehensive report including; Component name, version, license, dependencies, and known vulnerabilities.
- Delivered in the Cyclone DX delivery format approved by the U.S. government.
- Prioritized vulnerability mitigations mandated by CISA for software used by government.
- Validation of third-party and open source component integrity.
- Ability to demonstrate conformance for every software update through automation and differential analysis, which makes it easy to understand what's changed.

REGISTER HERE

FOR YOUR FREE SBOM REPORT, VALUED AT $1995

The fastest and most reliable software supply chain security platform for DoD dev and SOC teams

The U.S. military's technology assets are constantly threatened by sophisticated cyber attacks, but its software components are not adequately tested. From weapon systems to classified data, these unknown gaps in cyber performance represent a very real danger to military branches and throughout the Department of Defense (DoD). An attacker can take advantage of a single vulnerability in software and have a severe negative impact on military operations.

The President's Executive Order (EO) 14028, M-22-18, "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices" requires software developers to securely develop, deliver, and verify all code to harden DoD IT environments. All suppliers have a critical responsibility to ensure the security and integrity of their software is free of malicious code.

ReversingLabs empowers modern software development and security operations center teams to protect their software releases and organizations from sophisticated software supply chain security attacks, malware, ransomware, and other threats. The ReversingLabs Reverse Engineer Platform analyzes any file, binary or object including those that evade traditional security solutions.

The solution is delivered through a hybrid-cloud, VM, Container, or Appliance, to help unify and provide an end-to-end approach for Software Development Teams and SOC/ Infrastructure Teams with transparent and human readable threat analysis to confidently respond to software tampering and security incidents.

Our solution provides:

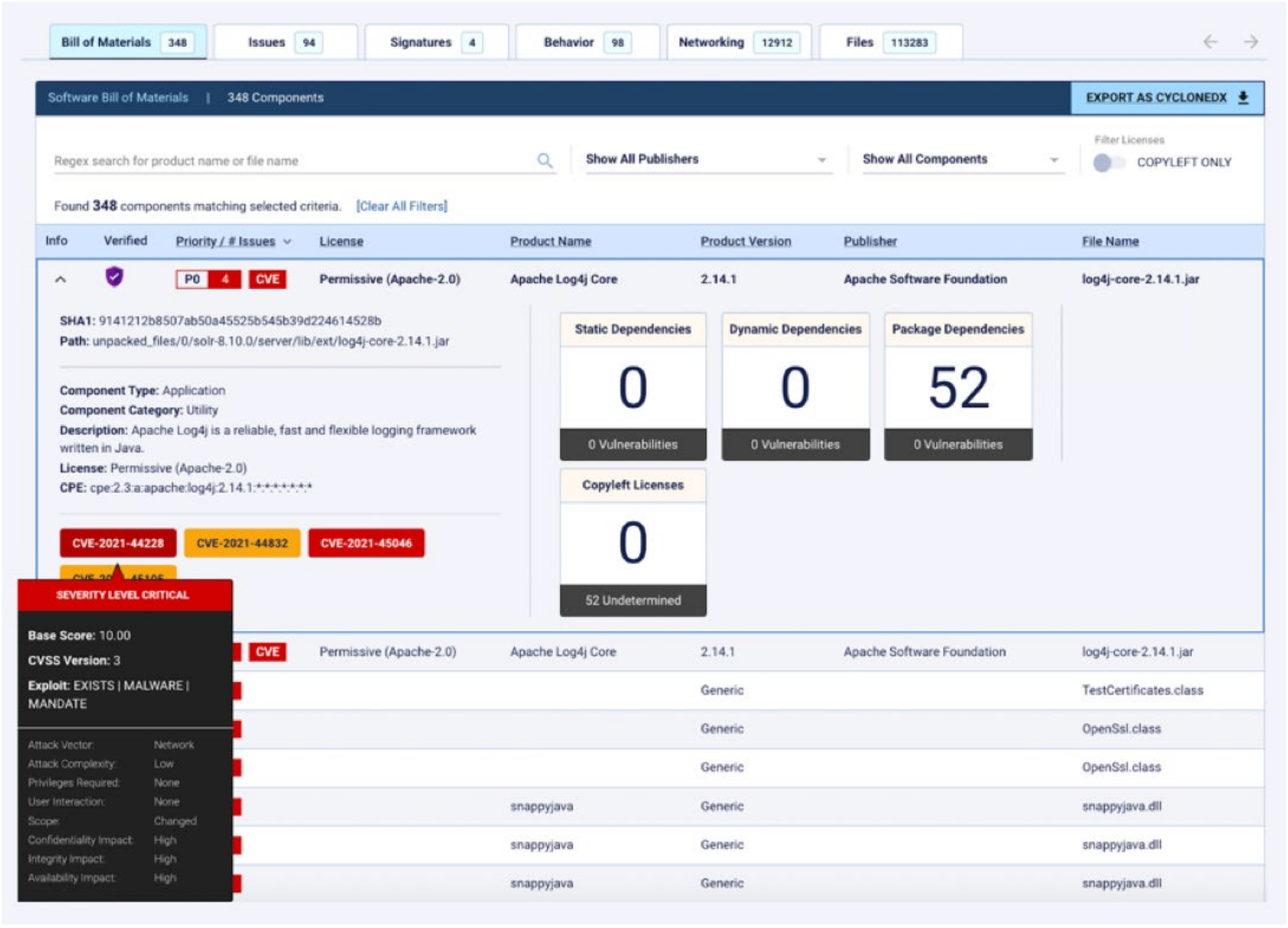
- Software to analyze over 4,000 file formats from diverse platforms to understand the reputation and risk related to your software.
- File reputation databases to compare your binaries using the world's largest database of curated malware, cyber threats, and known goodware to identify and remediate against cyber-attacks.
- Active feeds and continuous updates.

A ReversingLabs SBOM and Supply Chain Risk Report: A Cut Above

ReversingLabs data is used by more than 65 of the world's most advanced security vendors and their tens of thousands of security professionals. ReversingLabs enterprise customers span all industries, leveraging integrations with popular DevSecOps and SOC platforms that enable teams to access the analysis they need to make quick security verdicts, eliminate threats, and release software with confidence.

Its latest software latest solution provides a single snapshot view into the securing of each enterprise software tool and provides a grade much like a food label. These labels are designed to inform the C suite and product teams with immediate risk and remediation insights.

ReversingLabs provides up-to-date file reputation services, threat classification, and rich context derived from the world's largest repository of over 15 billion known malware and goodware files. Files are automatically reverse engineered and are accessible via a powerful set of REST APIs that provide ultra-fast threat identification, analysis, intelligence development, and threat hunting services to any external system.



Product Capabilities

ReversingLabs software speeds detection of files and objects through automated static and dynamic file analysis, determining file reputation and prioritizing the highest risk files with actionable details, in only milliseconds.

ReversingLabs Threat Analysis & Hunting: In-Depth Rich Context and Threat Classification

ReversingLabs' Threat Analysis platform enables an organization to profile and classify large volumes of files in real-time to create relevant data for advanced analytics platforms to support threat correlation, hunting and response. Conventional malware products focus on detecting malware while treating unknown files as good, essentially overlooking them. As the amount of malware that evades detection grows, the need to profile, track and correlate undetected files becomes imperative to limit the impact of incidents and breaches. This intelligence data helps close the visibility gap between malware detection and tedious and expensive post-breach reconstruction.

ReversingLabs' Threat Analysis platform helps enterprises form a comprehensive assessment of millions of files from web traffic, email, file transfers, endpoints, and storage. ReversingLabs file decomposition technology extracts detailed metadata, while adding global reputation context to rapidly classify threats. The ReversingLabs File Reputation Repository is the industry's most comprehensive solution with up-to-date, threat classification and rich context on over 15 billion known goodware and malware files.

ReversingLabs does not depend on crowdsourced collection but instead curates the harvesting of files from multiple software vendors and diverse sources of malware intelligence. All files are processed using unique the file decomposition (FD) technology to derive detailed context and input from over 40 antivirus scanners providing industry reputation consensus.

Product Discriminators

- All-in-one solution with easy onboarding
- Customer supplied YARA rule matching
- Seamless integration for automated operations
- Processes files sizes 10X larger than competition & faster
- Files analyzed in milliseconds to support real-time, high-volume processing
- Cloud based and on-premise

TRUSTED BY

U.S. AIR FORCE

REVERSINGLABS

www.reversinglabs.com
Russell Jacobs
russell.jacobs@reversinglabs.com
1-703-403-8843