REVERSINGLABS

DATA SHEET

ReversingLabs Managed Software Assurance Service

Introduction: Managing New Risks Requires New Approach

The strategic importance of securing software that enriches our daily lives - our banking systems and ATMs, medical records, utilities and even our connected homes and cars - cannot be understated. Malicious actors are actively targeting software supply chains with new levels of sophistication and patience. They look for weaknesses to exploit, subvert the established trust in patch updates, and gain unauthorized access through an unchecked software supply chain. Only by improving how we assure the integrity of software as we build, deploy and adopt it can we mitigate the risk of future supply chain attacks.

Key Benefits

- **Improve visibility and verification of your software supply chain**
- **Reduce brand risk due to compromise and data loss that jeopardize your customer's trust**
- **Increase confidence by auditing software releases and updates**
- **Comply with new secure software directives or policies**
- **Increase auditability of large and complex software release packages**
- **Improve prioritization of remediation efforts**
- **Reduce code maintenance with the removal of vulnerable code**

How it works

1. **Submit software package or release binary for analysis**
2. **Receive your comprehensive assessment report**
3. **Review the results and plan remediation with one of our experts**

Assuring That Your Software Is Reliable and Trustworthy

ReversingLabs Managed Software Assurance Service inspects software packages before their release, deployment or adoption by an organization. It inspects every application layer to automatically deliver the most complete software bill of materials to eliminate issue detection gaps. Every component is audited for a wide range of software vulnerabilities, malware injection, unexpected or malicious software behaviors, and ineffective security mitigations.

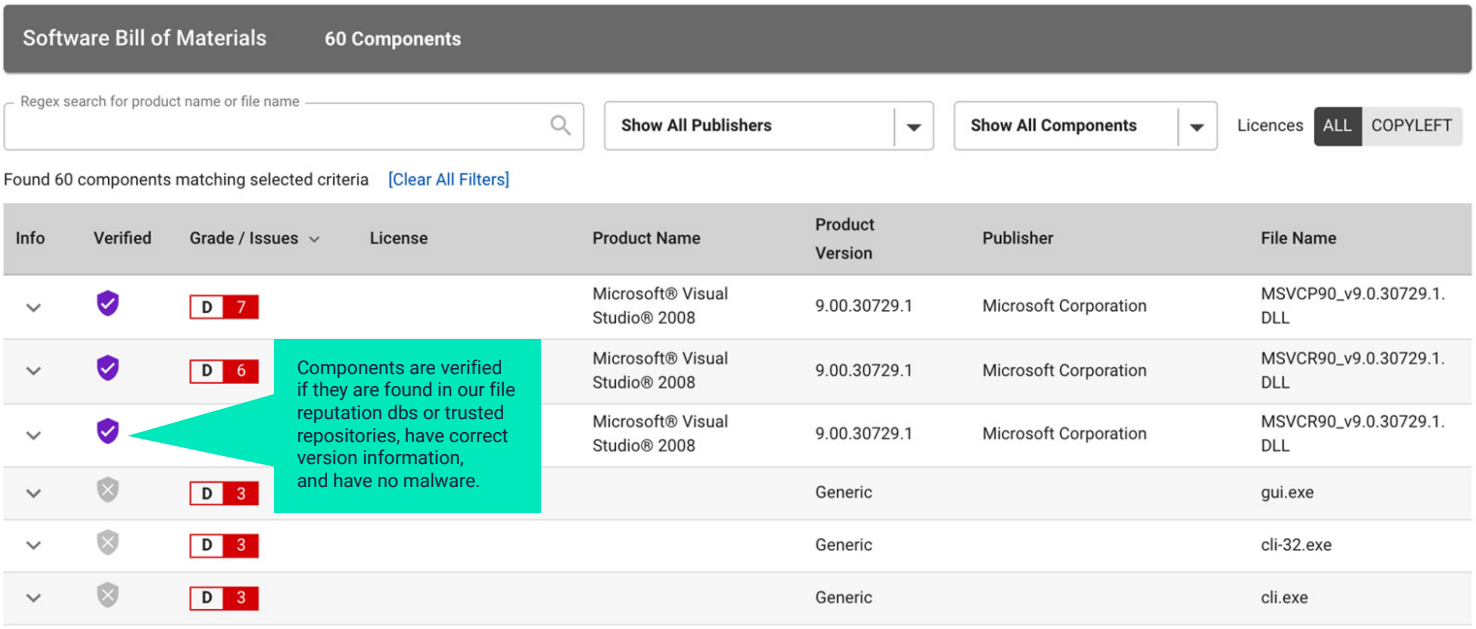
It assigns grades to quality issues to enable developers, auditors, and customers to quickly gauge security practices of any software package. The reporting informs users of hidden software risks before deployment and also provides context and details needed by developers to spearhead security innovation in their organization. Together we drive the security forward, by improving visibility, auditability, issue detection, and remediation prioritization.

Solution Capabilities

Software Bill of Materials (SBOM) with Verified Components

Visibility gaps within a Software Bill of materials can hide preventable security issues, simply put - if you cannot see it, you cannot analyze it for issues. Unlike traditional software composition analysis scans, our analysis process:

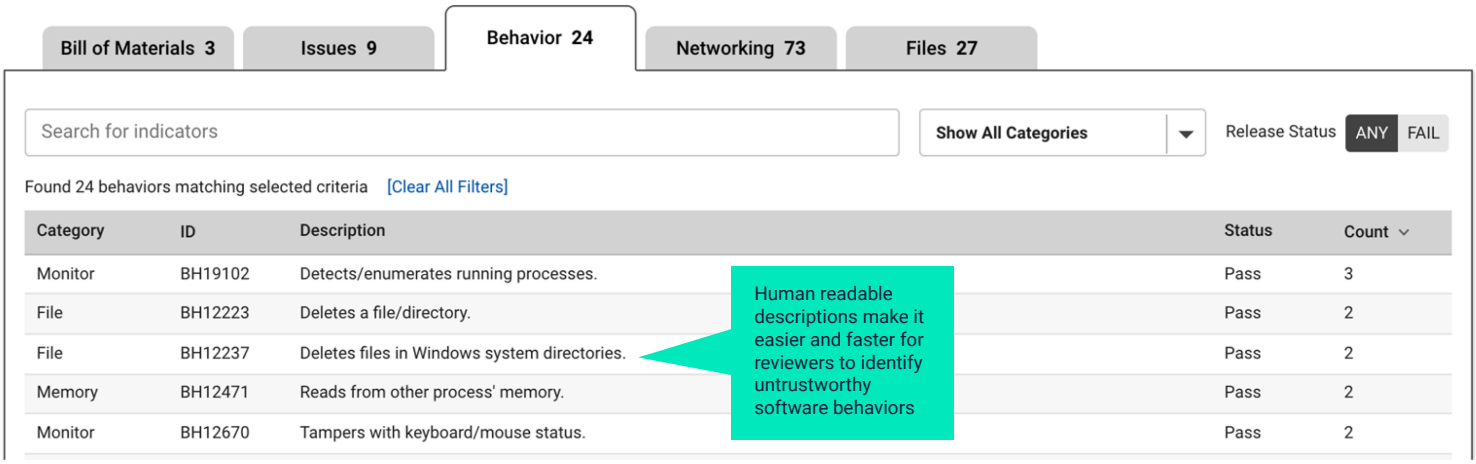
- Looks for over 400 file formats that may be embedded within a package to compile a far more complete list of in-house, open source and third-party software components
- Extracts origin, version, and licensing meta-data for each component
- Components are verified if they are found in our file reputation dbs or trusted repositories, have correct version information, and have no malware
- Constructs an accurate software dependency tree by examining static, dynamic, package, resource and transient dependencies
- Does not require source code, debugging symbols, or any special package preparation steps, making it easy for independent customers, auditors and application security teams to validate software quality



Audit Software Behaviors

The ability to inspect large and complex software packages for unexpected behaviors can be a key indicator of compromise in modern software supply chain attacks. However, traditional application security tools typically depend on having access to the source code to understand the intended software behaviors and are unable to glean behavioral insights from software binaries alone. Our solution applies years of malware behavior analysis experience and proprietary techniques (such as static binary code analysis and explainable machine learning classification) to this challenge so that we can extend traditional vulnerability analysis with:

- Detailed look into the underlying software behaviors is generated without source code or special debug builds
- Human readable interpretation of software intent for compiled binaries and script languages

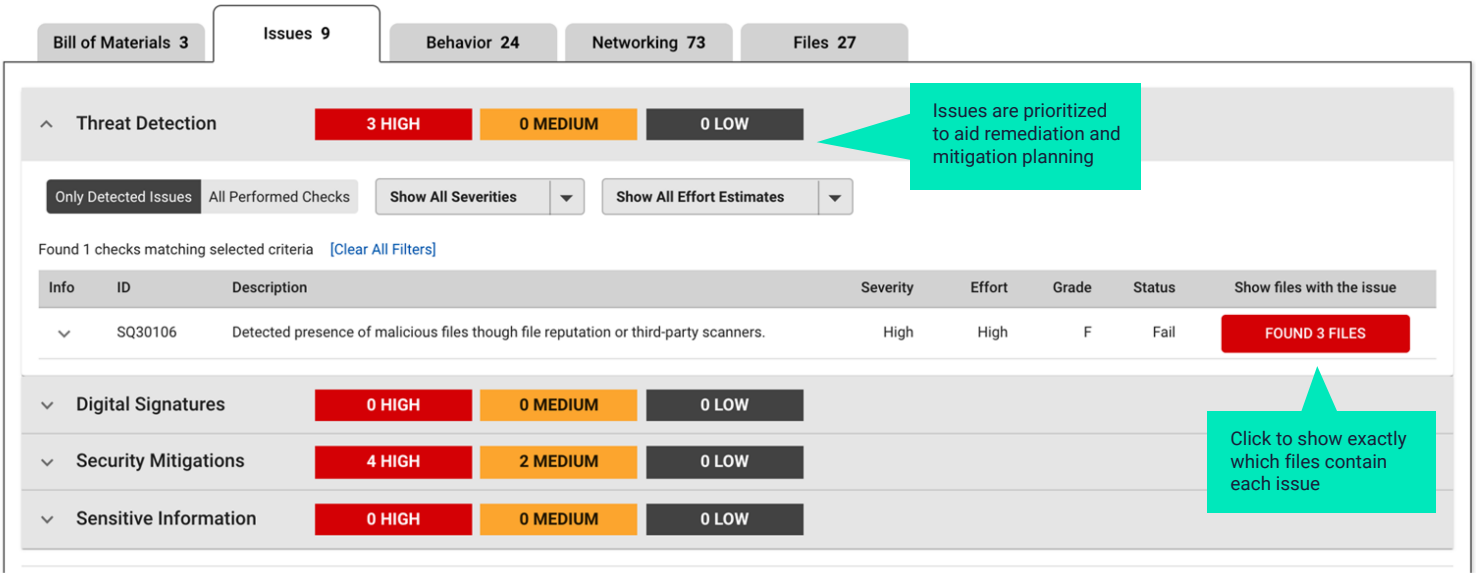


Fortify vulnerability mitigations and secure sensitive information

The risk of active malicious exploitation rises exponentially when vulnerability mitigation techniques are not implemented properly or if sensitive information is accidentally embedded within the software package.

Our ability to unpack and analyze over 400 file formats delivers unmatched visibility and analysis depth to:

- Uncover a comprehensive range of malware threats, software vulnerabilities, and indicators of compromise
- Detect accidental inclusion of source code, debug symbols, private keys, internal certificates, access tokens, etc. to enable changes that protect intellectual property and maintain user privacy
- Identify ineffective and misconfigured protections to empower development leaders and application security teams to enforce vulnerability mitigation practices
- Simplify vulnerability remediation by prioritizing the issue impact based on severity, exploit prevalence, and known malware use.



Expert Report Review

As with any new and expanded security controls, most enterprise software providers and consumers face unique challenges in establishing a new baseline and roadmap prioritization for their application security and assurance programs. As large and complex packages can have hundreds of newly discovered issues, every analysis includes a review with one of our security experts. These review sessions help teams:

- Understand the reported results
- Obtain guidance on remediating software supply chain issues
- Prioritize remediation efforts
- Monitor remediation progress

Annual Subscription Options

Organizations with higher-volume and more frequent analysis requirements, can take advantage of our on-demand subscription options that include:

- Identification of indicators of software supply chain attacks, such as SunBurst-type backdoor code injection, by comparing differences in version code behaviors
- Custom number of software analysis reports defined by the organization
- Report review calls are available on a regular basis to review groups of reports
- Based on the organization's needs, scanning policies can be customized, adjusting the report outputs

REVERSINGLABS
Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com
www.reversinglabs.com