CODESentry®

The Software Supply Chain Challenge

The use of open source components in software development is common practice. The challenge for software developers and organizations consuming software is understanding what is actually in the software and are vulnerabilities hiding in those components. Diligently managing the software supply chain is essential to ensuring software integrity and security to reduce risk and prevent threats.

Why CodeSentry:
CodeSentry rapidly scans binary files to deliver application intelligence and actionable information enabling you to:

- Establish stronger application security posture
- Approve or reject applications based upon risk
- Accept and manage application risk
- Work with vendors to remediate vulnerable software
- Improve the security of software you are developing

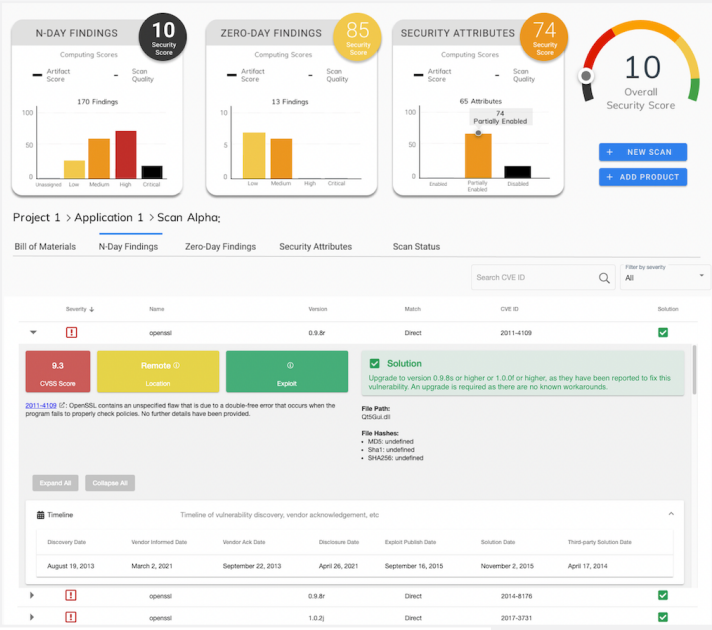
Executive Risk Dashboard –
Quick at-a-glance views into open source components, vulnerabilities and application security scoring

Software Bill of Materials (SBOM) –
Automate detailed SBOM generation to identify open source components and license information in third-party software

N-Day and Zero-Day Vulnerability Reports –
Detect hidden vulnerabilities in open source components and provide remediation guidance

CodeSentry
Software Supply Chain Security Platform

CodeSentry delivers unprecedented visibility into the software supply chain for applications being developed and/or consumed without needing access to source code. By performing binary software composition analysis on applications, CodeSentry identifies open source components in third-party software, detects N-Day and Zero-Day vulnerabilities and generates a detailed software bill of materials (SBOM) and vulnerability reports. Resulting application intelligence and vulnerability visibility mitigates risk, improves software security and strengthens enterprise security posture to defend against software supply chain attacks.



CodeSentry Executive Risk Dashboard View

Improving Software Supply Chain Security

Commercial Software Security

Application security should be foundational, yet enterprise organizations often just trust vendors when deploying commercial-off-the-shelf (COTS) software. By scanning application binaries, CodeSentry enables organizations to make informed risk-based decisions to choose more secure software and proactively prevent cyber threats.

Software Security Assurance

When applying a DevSecOps approach to software development, security is built-in to the software development life cycle (SDLC). As a final check before deploying in-house software or releasing commercial software to market, CodeSentry scans the binary to produce an SBOM and identifies vulnerabilities that must be fixed to ensure delivery of secure software.

Who Uses CodeSentry

Information Security

Proactively prevent cyber threats against business-critical applications and protect sensitive data ensuring software meets security standard

Procurement

Better manage vendor risk and only approve software purchases based upon security analysis and verification of the application

Risk and Compliance

Audit software and gain visibility into risk to efficiently monitor and measure the risk and ensure regulatory compliance

Software Development

Ensure secure and compliant software by managing open source components in custom and third-party code, mitigating licensing issues and remediating vulnerabilities throughout the SDLC

CodeSentry Features

Component Matching Identification
Multiple algorithms and machine learning are used to identify components with increasing levels of recall and sophistication

Vulnerability Detection & Security Scoring
Scan for N-day and Zero-day vulnerabilities in open source components, rank according to criticality, check for security attributes and produce a security score

License Information
Checking license information ensures compliance and reduces risk that software is released and/or consumed with unlicensed components

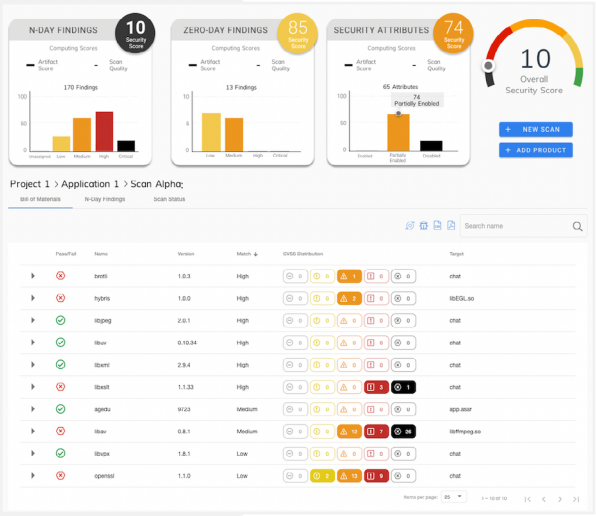
API-First Approach & Integration
An advanced GraphQL interface allows sophisticated integration with external systems including ticketing and vulnerability tracking systems

SBOM Generation & Output
Easy to use interface for scanning binaries to auto generate a detailed SBOM. Flexible SBOM formats include PDF, CSV, JSON and CycloneDX

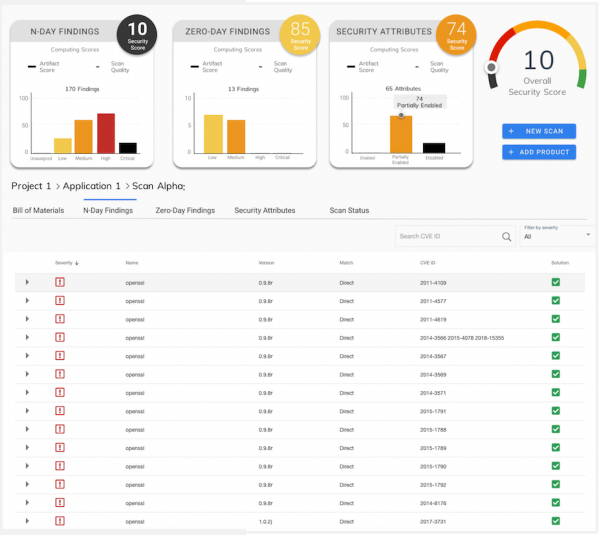
Vulnerability Intelligence & Reporting
Integration with Risk Based Security's VulnDB provides the most comprehensive vulnerability intelligence to prioritize remediation

Audit Logging
Logs API activities, user logins and exports via UI and API to ensure proper usage and identify potentially improper or malicious activity

Flexible Deployment Options
Customers can choose to CodeSentry as a SaaS solution or deploy it on-premises when unable to send intellectual property off-site



SBOM Dashboard View



Vulnerability Report View

Business Drivers

Software Supply Chain Attacks on the Rise
Recent Osterman Research report found 100% of commonly used applications contained vulnerable open source components. These results highlight a broken software supply chain and a vulnerable application layer that is increasingly being targeted by cyber attackers.

Presidential Executive Order Cybersecurity Mandates
Improving software supply chain security is one of the top initiatives of the recent cybersecurity executive order. Software vendors working with the U.S. Government will soon be required to provide SBOMs

SBOM Compliance Requirements Governing bodies are now starting to require SBOMs. As an example, the FDA is requiring medical device manufactures to produce SBOMs as go-to-market prerequisite.

For more information, visit www.grammatech.com

To request a CodeSentry demo, contact:
U.S Sales: 888-695-2668
International Sales: +1-607-273-7340

Email: sales@grammatech.com

System Requirements and Specifications

Server (on premise deployment)
- Linux based system with 32 Gb of memory and Kubernetes
- 1TB of storage space

Client
- GraphQL API
- Any modern desktop web browser

Deployment
- On-premises
- Software-as-a-Service

Software Bill of Materials (SBOM) Output
- CycloneDX
- CSV
- PDF
- JSON

Languages
- C
- C++
- Objective-C Object

Format
- ELF
- PE
- Mach-O

Vulnerabilities and Checks Performed
- N-Day Vulnerabilities (CVE)
- Zero-Day Vulnerabilities (CWE)
- Security Attributes (Stack Cookies, etc. etc.)

Compression / Archive / Installation Formats
- Zip (zip)
- Tar (.tar)
- Bzip2 (.bz2, .bzip2, .tbz2, .tbz)
- Gzip (.gz, .gzip, .tgz, .tpz)
- Portable Archive Exchange - PAX (.pax)
- RPM Package Manager (.rpm)
- LZMA / LZMA2 (.xz)
- CPIO (.cpio)
- -Xar (.xar)
- 7zip (.7z)
- VSIX (.vsix)
- JAR (.jar)

Binary Formats
- Linux: executables, objects (.o), static libraries (.a, .ar), libraries (.so), Debian package (.deb)
- Windows: executable (.exe), objects (.obj), libraries (.dll), installer (.msi), update (.msu), cabinet (.cab)
- Mac: executables, installer (.pkg, .dmg), libraries (.dylib)
- Embedded: PPC, ARM, Renesas, Embedded Linux

Target Operating Systems
- Windows
- Linux

Future Support
- Containers
- Disk images / file systems
- Installer images
- Directories