CODESentry®
CODESECURE

Binary Composition Analysis (BCA)

Identify Vulnerable Open-Source Software (OSS) in Third-Party Components | Create SBOMs

Risk in the Software Supply Chain

Building secure software requires development teams to follow good security practices. Most software today includes externally developed code, including open-source components and commercial binaries. In addition, teams are also being tasked with delivering an SBOM to their customers.

Software Bill of Materials (SBOM) without Source Code

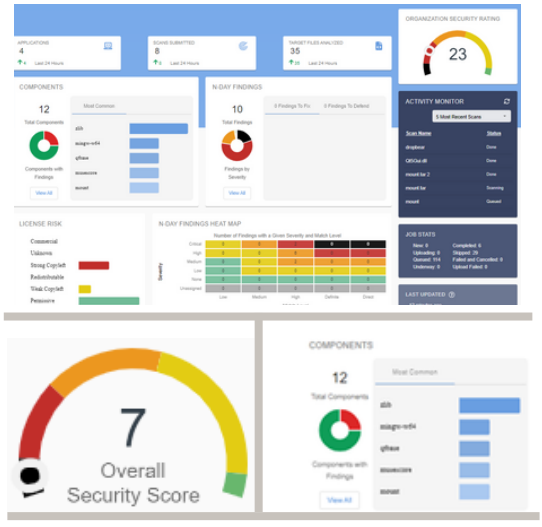
CodeSentry is a Binary Composition Analysis solution that identifies open-source components and shared library dependencies in binaries, including firmware, containers, and mobile or desktop applications. The resulting component inventory is reported through an SBOM, which is also mapped to VulnDB, the industry's most complete database of software vulnerabilities. The resulting application intelligence and vulnerability visibility mitigates risk, improves software security, and strengthens enterprise security postures by defending your products against software supply chain attacks.

Component Inventory and License Information

Knowing what components are in your scanned software helps identify vulnerabilities. In addition, checking license information ensures compliance and reduces the risk that software is released and/or consumed with unlicensed components.

- **SBOM Generation, Annotation, and Output:** CodeSentry scans binaries to auto-generate a detailed SBOM and display it in an intuitive interface – easy for non-technical users. The Annotation feature allows users to edit SBOM components and associated vulnerabilities, and supports an open-source license approval workflow. Flexible SBOM output formats include PDF, HTML, CSV, SPDX, JSON, and CycloneDX.
- **Inventory and Vulnerability Search:** CodeSentry search finds components and vulnerabilities across the inventory of scanned files and identifies vulnerable components, thereby saving time when vulnerabilities are declared and remediation actions are required. The inventory of scans can be filtered to show the latest updates to vulnerability, remediation, and exploit information to easily determine what actions should be take to mitigate security risks.

Example UI Elements



codesecure.com
Email: sales@CodeSecure.com

- **API-First Approach & Integration:** An advanced GraphQL interface facilitates sophisticated integration with external systems including ticketing and vulnerability tracking systems.
- **Audit Logging**: CodeSentry logs API activities, user logins and exports via UI and APIs to ensure proper usage and allow identification of potentially improper or malicious activity.
- **Deployment Flexibility:** CodeSentry can be deployed on-premises, including in air gapped environments. For organizations that wish to maintain lower overhead, it is also available as a single-tenant SaaS deployment.
- **Purchasing Flexibility:** CodeSentry is available in three editions: SBOM Edition, Security Edition, and Advanced Security Edition, which provide distinct capability bundles.
- **Live N-Day Updates:** CodeSentry continuously updates the database of known components and vulnerabilities, and syncs existing scans with the latest vulnerabilities, remediation, and exploit information.

The CodeSentry Difference

Binary SCAs unique capabilities are not available in Source-based SCA solutions.

- **No requirement for source code.** Source code is rarely available for third-party components, and is not always available to security teams, even for in-house applications. Binary SCA can produce an accurate SBOM without access to source code.
- **Views code "as deployed".** Source SCA only sees components "as built". CodeSentry analyzes the binary that executes. This allows it to identify any components or vulnerabilities introduced during compilation and packaging code for release. Source SCA also often lists components that are not in the final build image, generating false positives. CodeSentry can accurately tell whether a component is present in the final product or not.
- **2nd, 3rd, and 4th party coverage.** Direct vendors may use their own third parties for software development. CodeSentry solves this problem by analyzing the final binary "as deployed". It identifies open source no matter where it entered the software supply chain.
- **Shift Left and Shift Right.** Binary SCA allows organizations to identify vulnerable open source when they evaluate third-party code, well before they incorporate it into their products. The security of delivered software is enhanced by using Binary SCA as a final check to scan binaries before deployment or releasing them to customers.
- **N-day and Zero-day Vulnerability detection and security scoring.** CodeSentry identifies reused components and continuously tracks any vulnerabilities throughout the software lifecycle, supported by daily updates. Detecting critical, N-day, and Zero-day vulnerabilities as well as misconfiguration of security features in compilers early and precisely is key to reducing the cybersecurity risk and impact.

VulnDB Vulnerability Database

Most approaches to SCA leverage NIST's National Vulnerability Database (NVD) and augment those vulnerabilities with a small number of publicly disclosed vulnerabilities published by open-source projects. But by some estimates, NVD is missing over 90,000 publicly disclosed vulnerabilities and can delay publishing new vulnerabilities for up to 4 weeks – a time during which attackers can exploit them.

CodeSentry leverages VulnDB to provide data on open-source security. VulnDB provides the most comprehensive and timely vulnerability intelligence available, and provides actionable information about the latest security vulnerabilities. As of 2023, VulnDB contains over 330,000 vulnerabilities, with over 20,000 new vulnerabilities added this year.Yet only two-thirds of these are published in the NVD. This leaves thousands of organizations relying on NVD unable to defend against the risk posed by these vulnerabilities.

System Specifications	Description
Client	Any modern desktop web browser GraphQL API
Deployment	On-premises, FIPS Compatible SaaS (supports GovCloud)
Software Bill of Materials (SBOM) Output	CycloneDX, SPDX, JSON, CSV, PDF, HTML
Compiled Languages	
C/C++	Executables, objects, libraries (.exe, .obj, .dll, .o, .so, .a, <no extension>) Linux Kernel / Kernel Module Other ELF file types
C#	.exe / .dll
Java	java class files, .jar
Go	.exe / .dll / .o / .so / <no extension>
Interpreted Languages	
JavaScript	Manifest, .npm, .js
Python	Manifest, .python, .py
CPU Architectures	
Supported	Intel, PowerPC, Sparc, ARM32/64, MIPS, AVR32
Desktop / Server Operating Systems	
Windows, Linux, macOS	Libraries, executables, kernel modules, applications
Linux Package Manager	RPM, Debian
RTOS	VxWorks, QNX, INTEGRITY, Linux
Container / File Systems	
Docker	tar.gz, overlay2, aufs
File System	ext2, ext3, ext4, iso, squashfs, cramfs, Android Sparse Disk Image, romfs, JFFS2, ubifs, yaffs2, vmdk
Embedded	VxWorks, QNX, Squashfs, Cramfs
Mobile Platforms	
Android	apk, Dex, Odex, Android Sparse (disk image)
iOS	ipa
Archive Formats	
File Types	7z, chm, lzip, rzip, lzma, tar, cpio, lzop, upx, Ar, gzip, xar, bzip2, zip, lrzip, rar, arj, xz, pkg, dmg, msi, msu, cab, rpm, deb, apk (alpine linux)
Firmware	
Aris, Juniper, Kosmos, Cisco	SREC, bFLT, base64, Intel Hex, uBoot, wim