GRAMMATECH

# CodeSentry
## Binary Software Composition Analysis

CODESentry™

## Securing the Modern Software Stack

Third-party software use is a reality today. In fact, at least 90% of corporations use third party software, and 95% of proprietary or custom software applications they create contain third party components. A recent study found that at least 42% of applications contain one or more components with a known, high risk security vulnerability[1]. Software reuse provides productivity improvements that organizations rely on, but do so at significant risk.

[1]*Source: "Technical Insight for Software Composition Analysis," Gartner | November 2019*

### Vulnerability Detection

CodeSentry identifies reused components and continuously tracks any vulnerabilities throughout the software lifecycle. Detecting critical, N-day vulnerabilities early and precisely is key to reducing the cybersecurity risk and impact.

### Audit / Compliance

Requirements for inventory or financial audits apply to what is in your software as well – not just your physical assets. Audit prompts may range from internal financial needs to external validation requirements. Tracking third party software manually with spreadsheets or email is invariably error prone. CodeSentry keeps your applications audit ready without rework or guesswork. Our SBOMs can be stored alongside the applications they describe, providing [more] reliable audit information and third party licensing records.

### Software Bill of Materials

Software reuse represents a risk assessment blind spot for many organizations. Many organizations do not have the capability to independently measure this exposure. GrammaTech CodeSentry allows security professionals to quickly and easily measure and manage the risk associated with third-party software. Given the final executable or library it detects actual component reuse, creates a detailed software bill of materials (SBOM), and lists known vulnerabilities in the detected components including any dependencies. CodeSentry's deep binary analysis can detect components from open source projects, commercial-off-the-shelf products, and custom vendor code: these include components for networking, GUIs, and authentication.

### Modern Software Stacks

Most applications have a complex set of dependencies. The tip of the iceberg is usually custom code, often referred to as first party code. This often depends on vendor libraries, also known as second party code, and/or commercial libraries, known as third party code. This is combined with open source software, as well as API dependencies for functionality like mapping software or general information look-up. Understanding security as it relates to this complex stack of components is important.

# Binary SCA vs Source SCA

Binary Software Component Analysis (SCA) is more reliable than traditional source based SCA.

- It analyzes the actual code that will run, not the build environment. This significantly reduces false positives due to superfluous code in the build environment as well as components that are excluded due to build configurations.
- In many cases, source is simply not available.
- Even if source is available, setting up a build environment is far from trivial.

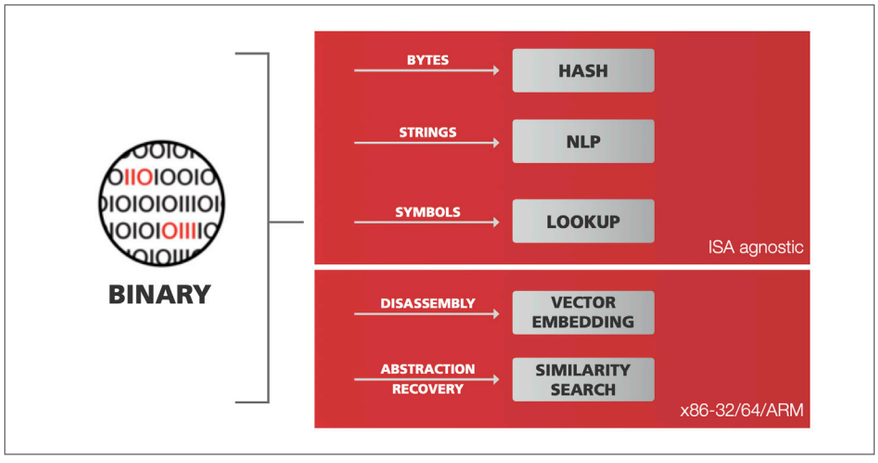
## Recent Vulnerability Examples

**Ripple20** is a set of 19 vulnerabilities in the Treck TCP/IP stack with four vulnerabilities rated critical with CVSS scores over 9 and combine to enable remote code execution. These vulnerabilities impact devices from a wide variety of vendors, including HP, Schneider Electric, Intel, Rockwell Automation, Caterpillar, Baxter and many more across medical, industrial, transportation, oil & gas and other industries.

**Urgent/11** is a set of vulnerabilities in the IPNet stack originally developed by Interpeak AB. Six of these vulnerabilities are critical and enable Remote Code Execution. It impacts real-time operating systems from ENEA, Green Hills, Microsoft, Mentor and Wind River, impacting possibly billions of devices in medical, industrial, automotive, aerospace and defense industries.

The famous **Heartbleed Bug** reported as CVE-2014-0160 is a serious vulnerability in the OpenSSL cryptographic software library. While many systems have been patched, there are still vulnerable systems out in the wild. The impact of the Heartbleed bug is significant as it can easily be used to leak confidential information over unprotected network connections.

## Component Detection Algorithms




CodeSentry uses several algorithms to detect components in applications with increasing level of recall and sophistication.

- Strings are input into natural language processing.
- If symbols are available in the application, they are matched to the symbols in the component.
- A technology called ‘embedding’ is used to map component disassembly to multi-dimensional vectors and compare them to vectors derived from the components.
- Logic recovery calculates code features and matches them with machine learning to detect similarities between CodeSentry’s database of known components.

# CodeSentry Features

**Ease of use**
An easy to use application upload interface accepts native binaries, zip files, or other archives. Binaries do not require debug information and can be of a number of different instruction set architectures (ISAs). CodeSentry supports multiple output formats and the information can easily be understood by IT professionals. Programming experience is not required.

**Identification**
Diverse component matching algorithms identify the components present in native binaries. Identifies components, including versions, to generate a Software Bill Of Material (SBOM). Links component versions to CVE-IDs (Common Vulnerability Enumeration) and and CVSS (Common Vulnerability Scoring System) scores, both based on the National Vulnerability Database (NVD).

**Management**
Tracking and annotation for identified vulnerabilities allows a security researcher to change the CVSS score for a particular vulnerability to indicate whether the vulnerability is applicable to the application or can be ignored.

**Remediation**
Notifications indicate cases where a vulnerability can be resolved by upgrading a component to a newer version.

**Multiple Deployment Options**
CodeSentry is available as an on-prem solution for those businesses that are unable to send their intellectual property off-site. A scalable Software-as-a-Service option is also available when on-premise deployment is not a hard requirement. This solution offers hardware-less deployment and easy scalability.

## Semantic Signatures Using Deep Binary Analysis

CodeSentry is backed by GrammaTech's expertise and research acumen in cybersecurity and code analysis. Deep analysis of the binary code, including the logic inside the binaries, is used to calculate multi-dimensional semantic signatures. These signatures are used in the component matching algorithms and improve the precision and recall of component recognition, for fewer missed vulnerabilities and high confidence that the vulnerabilities that are reported are accurate.

## Software Re-Use Risk Management

Many organizations have a blind spot in assessing risk due to software re-use in internal and customer facing applications. They do not have the capability to independently measure this exposure. GrammaTech CodeSentry allows security professionals to quickly and easily measure and manage the risk associated with third-party software. With deep binary analysis of the final executable or library it detects component re-use in software applications, creates a detailed software bill of materials (SBOM) and lists known vulnerabilities in the detected components including any dependencies. CodeSentry can detect components from open source, custom code from vendors as well as commercial-off-the-shelf components such as network components, GUI components or authentication layers.

## CodeSentry

**Deep scalable analysis** without the need for source code is less error prone then conventional SCA tools and facilitates efficient enterprise-wide adoption that is both efficient and less error prone than conventional SCA tools.

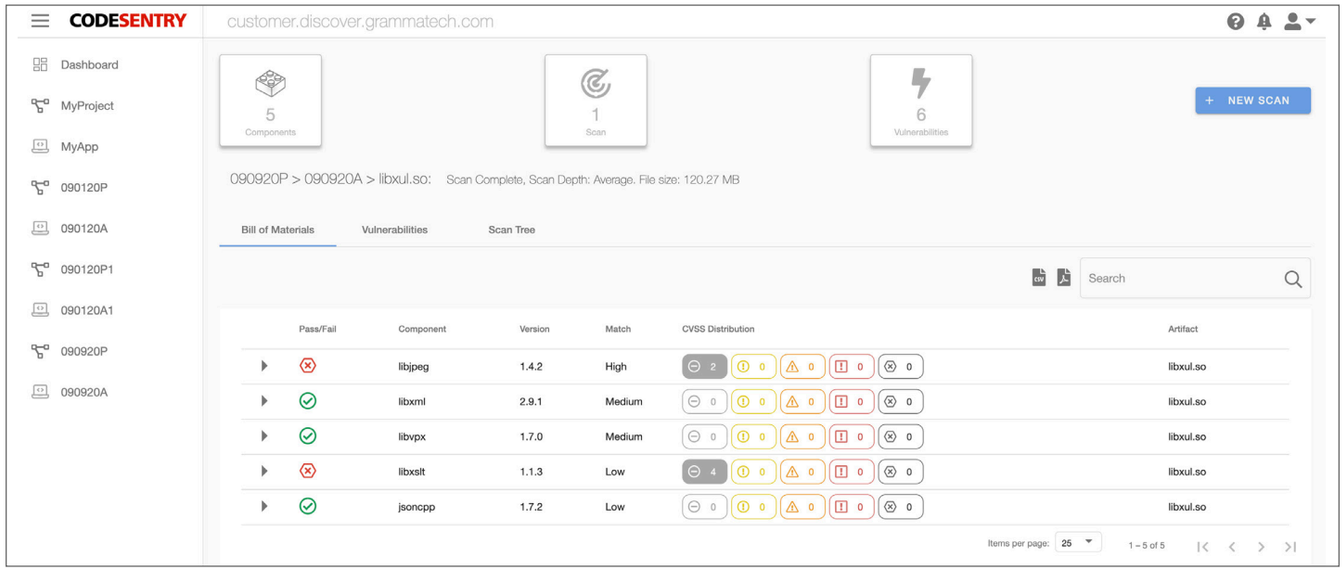
**High precision and recall**; fewer false positives; fewer missed vulnerabilities. This reduces risk and saves time spent chasing inaccurate warnings.

**Multiple component matching algorithms** provide speed and accuracy for component detection and are resilient to Instruction Set Architecture (ISA) and compiler differences. The algorithms compare semantic signatures that utilize specific information about components such as the contents of strings that can also incorporate abstractions of the high level logic contained in functions.

**Detection of third-party components**, either open source, or COTS.

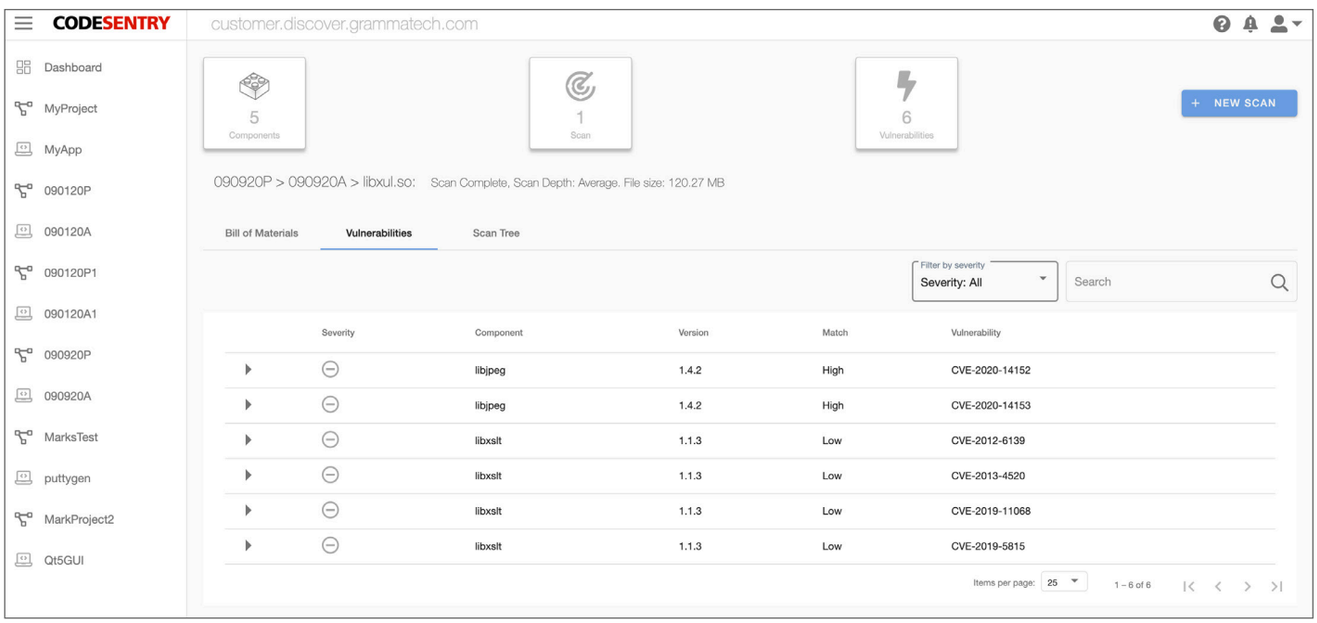
# CodeSentry Capabilities

- User uploads a set of artifacts to be scanned.




## Bill of Materials

- Bill of Materials lists the components identified by the analysis engine.
- Indicators show number and severity of vulnerabilities associated with each component.




## List of Vulnerabilities

- List of vulnerabilities associated with the identified components.
- Details of each vulnerability, including link to CVE report.

# System Requirements

**Server**

- Linux based system with 32 Gb of memory and Kubernetes

**Client**

- Any modern web browser (desktop or mobile)

**Deployment**

- On-premise
- Software-as-a-Service (future)

**Bill of Materials Output**

- CSV
- PDF

**Languages**

- C
- C++
- Objective-C

**Object Format**

- ELF
- PE
- Mach-O

**Compression / Archive / Installation Formats**

- Zip (zip)
- 7-Zip (.7z)
- Tar (.tar)
- Bzip2 (.bz2)
- Gzip (.gz)

**Binary Formats**

- Linux: executables, objects (.o), archives (.a), libraries (.so)
- Windows: executable (.exe), objects (.obj), libraries (.dll)
- Mac: executable (.exe), objects (.obj), libraries (.dll)

**Target Operating Systems**

- Windows
- Linux
- MacOS

**Future Support**

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

## Contact

**U.S. Sales:** 888-695-2668
**International Sales:** +1-607-273-7340
**Email:** sales@grammatech.com

**Corporate Headquarters:**
6903 Rockledge Drive, Suite 820
Bethesda, MD 20817

**Research & Development Center:**
531 Esty Street
Ithaca, NY 14850