Snyk maintains the leading database in the industry

**Dedicated security experts**
Snyk operates a dedicated subject matter expert security research team built of security veterans

**Comprehensive coverage**
Coverage goes far and beyond CVEs and includes many additional non-CVE vulnerabilities

**Curated, enriched & actionable content**
The content regarding each vulnerability is enriched to support analysis and triaging

**Powering the ecosystem**
Snyk database was validated by industry leaders as their preferred security solution

**Team of security experts**
Snyk’s security database is managed by a team of experts researchers and analysts ensuring the database maintains a high level of accuracy with a low false-positive rate.

- All items in the database are analyzed and tested.
- CVSS score and vector assigned to 100% of vulnerabilities
- Hand curated content and summaries, including code snippets where applicable
- The team also invests in proprietary research to discover new vulnerabilities.

The team is headed by Snyk’s co-founder, Danny Grander, a veteran security researcher. Previously, Danny built cyber solutions for government agencies, led vulnerabilities research and managed research and development teams. Danny is a competitor and frequent winner of CTF at DefCon, CCC CTF, Google CTF.

**Comprehensive security coverage**

- **Beyond CVE/NVD** - Snyk’s database goes far beyond CVE vulnerabilities (which consist only 60% of the database) and includes many additional non-CVE vulnerabilities that are derived from several sources
- **Best coverage in the market** - Snyk regularly wins head to head comparisons to other vendors and finds many more vulnerabilities not detected by others
- **First to know & publish** - Snyk exposes many vulnerabilities before they are added to public databases. On Average, Snyk publishes vulnerabilities 92 days sooner than NPM Audit

40% of Snyk’s database is proprietary

280% better database coverage compared to other vendors

72% of the vulns in NPM Audit were already found in Snyk's database
Snyk maintains the leading database in the industry

1. **Enriched data from over 10 vulnerability databases**: such as CVE, NVD and more. Data derived from these resources is analysed, tested and enriched, before being included in Snyk’s database.

2. **Dedicated proprietary research for new vulnerabilities**: Snyk’s dedicated security team is focused on uncovering severe vulnerabilities in key components. A recent disclosure by our team is **Zip-Slip**

3. **Threat Intelligence systems**: listens for vulnerabilities mentioned in release notes, commits, JIRA issues and forums, but not reported to vulnerability DBs or CVE. Previously surfaced vulnerabilities from this source include **Apache Airflow** and **marked**.

4. **Community relationship**: Snyk collaborates with the community and operates bug bounties for new disclosures. This activity results in hundreds of community disclosures, such as **fze-server**.

5. **Collaboration with Academia**: The team partners with PhD academia labs such as Berkeley, Virginia Tech and Waterloo, to exchange tools, methods and data. Findings are then exclusively disclosed by Snyk.

### Curated, enriched and actionable content

#### Hand curated content and enriched metadata:
The team enriches the data describing each vulnerability with hand-curated content and summaries, including code snippets were applicable. All items in the database are analyzed and tested for their accuracy (version ranges, vulnerable method, etc). CVSS score and vector assigned to 100% of vulnerabilities.

#### Remediation with Precision Patches
In 20% of vulnerability instances, upgrading a vulnerable package is too disruptive or is not possible in the application context (i.e. for some transitive dependencies). In many such cases, Snyk uniquely extends the remediation coverage by offering its precision patches. These patches are developed and rigorously tested in collaboration with the package owner, by **backporting the original fix to all applicable historical versions**, including the **minimal changes required in order to fix** the vulnerability without introducing breaking changes.

#### Triage support:

**Vulnerable functions called in runtime**
For issue prioritization, Snyk is able to alert when a vulnerable function is actually being called during the runtime of the application. Out of all the functions in a vulnerable open source package, Snyk identifies the specific functions within the package that are truly vulnerable. Snyk analyses the application behavior during runtime and indicates for each vulnerability whether the exploitable function is actually being used.

**Exploitability**
When a vulnerability becomes public, sometimes a proof of concept of how the vulnerability can be exploited is published as well. Published exploit code serves as a good indicator of exploitability because it enables attackers to easily weaponize a vulnerability. The availability of a remedy also influences the exploitability metric. This information is analyzed and calculated into the CVSS score (temporal score) of each vulnerability, as well as displayed in the vulnerability content.
Snyk maintains the leading database in the industry

Powering security across the ecosystem

“We didn’t trust the security coverage provided by the previous solution was comprehensive enough, which later comparing to Snyk was indeed clear”

Leif Dreizler
Segment, Security Engineering

Tech giants and security industry leaders are choosing to adopt Snyk’s database to enhance their existing scanning capabilities:

- Powering Google Chrome
- Powering Microsoft Sonar
- Powering NodeSource N|Solid and Certified Modules
- Powering Anchore Enterprise

Top-tier players are choosing to be protected by Snyk, validating the quality of the coverage Snyk provides:

1. Based on comparison of scan results of Snyk versus Whitesource and NPM Audit. The scanned projects are: NodeGoat, Spring-boot, thimble.mozilla.org, angular, generator-jhipster

2. Zip Slip is a widespread critical archive extraction vulnerability, typically resulting in remote command execution. It was discovered and responsibly disclosed by the Snyk Security team. It affects thousands of OSS projects, and vendors, including ones from HP, Amazon, Apache, Pivotal, Microsoft, Hive, Hadoop, Pivotal Spring, LinkedIn, Twitter, Alibaba, Eclipse, Jenkins, OWASP, SonarQube, and many more.


4. See here Virginia Tech study with Snyk.