BLACK DUCK®

COVERITY
STATIC ANALYSIS

Key advantages

High performance. Fast incremental scans identify issues in new or changed code, with no loss of fidelity compared to full scans. This makes it easy to run frequent scans on commits or pull requests without slowing developer velocity.

Enterprise scale. Coverity scans many of the largest applications in the world, including those with thousands of developers and tens of millions of lines of code.

Extensibility. Custom checkers can be easily created to add support for proprietary frameworks or unsupported languages.

Deployment flexibility. Coverity runs where you need it, on-premises or in your private cloud environment. This gives you the best static analysis scans while keeping all your data inside your network.

THE MOST COMPREHENSIVE STATIC ANALYSIS

Coverity® Static Analysis provides the most accurate and scalable static analysis on the market, empowering developers and security teams to deliver secure, high-quality applications at scale. By building an in-depth model of each application, then combining it with insights into all dependencies, compilers, and support for more than 20 programming languages and 200 frameworks, Coverity can uncover complex issues that span multiple files and libraries across some of the largest applications in the world.

FAST SCANS EARLY IN THE DEVELOPMENT LIFE CYCLE

Coverity scans can be performed throughout the early stages of the SDLC to uncover security and quality issues when they're least disruptive and easiest to resolve.

Run in real time in the IDE

Developers are notified of vulnerabilities and code quality issues as they code, preventing issues from being checked in to the code repository.

Trigger on pull requests

Incremental scans identify issues in any new or changed code, with integrations into popular source code management systems.

Automate in CI/CD pipelines

Full application scans identify security or quality issues that haven't yet been resolved, with the ability to break the build if policy violations exist.

THE MOST ACCURATE RESULTS

Coverity generates highly accurate scan results that reduce the burden on developers, letting them focus on resolving actual defects without wasting their time triaging false positives.

- **An in-depth model of each application** gives key insights into how it runs, including all dependencies and compilers as well as dataflow and control flow paths.
- **A deep understanding of more than 20 programming languages and 200 frameworks** provides the context to help distinguish between false positives and real issues.
- **Contextual insights** are applied to initial scan results to validate each result and assess the likelihood of it ever being exploited.
- **Configurable security and quality checkers** are tuned for high accuracy by default but can be adjusted to align with the business or application's risk profile.

EXTENSIVE COVERAGE OF SECURITY AND INDUSTRY STANDARDS

Coverity provides best-in-class identification of code quality issues and the most comprehensive coverage of security, safety, and industry standards, including

- **Security:** OWASP Top 10, SANS CWE Top 25, PCI DSS
- **Safety:** MISRA®, CERT C/C++, CERT Java, DISA STIG, ISO 26262, ISO 23434, ISO/IEC TS 17961, AUTOSAR®, and Hyundai Secure Coding Standards

Reports can be downloaded as PDFs, making it easy for auditors to maintain detailed compliance records for each standard. Trend reports provide additional insights, showing severity levels over time as well as how individual developers and project teams are progressing in clearing their prioritized issues.

Additionally, the Coverity Qualification Kit (Q-Kit) ensures that Coverity is configured properly for safety-critical projects to comply with industry safety standards, such as ISO 26262 and DO-330.

KEY FEATURES

- **Easy onboarding.** The Point and Scan desktop application enables users to onboard applications simply by pointing to their source code. For development teams that prefer a command-line interface (CLI), Coverity's CLI feature provides similar functionality.
- **Streamlined integrations with developer workflows.** The Black Duck Bridge provides a simple, predictable approach to integrate any Black Duck application security testing solution, including Coverity, into popular CI/CD tools via the CLI.
- **Real-time identification of defects.** The Code Sight™ IDE Plug-in gives developers accurate static analysis insights as they code. Each issue includes descriptions, categories, severity, CWE data, defect location, and detailed remediation guidance right within the IDE.
- **Actionable remediation guidance.** Detailed suggestions and context-specific eLearning help developers understand how to fix issues quickly, without having to become security experts.
- **Detailed reporting.** Dashboards display prebuilt reports based on industry-recognized lists, issue types, and technical risk indicators, helping your developers prioritize and focus on the issues that matter most to your organization. Filters make it easy to group issues by CWE, standards taxonomy, priority list, risk indicator, path, and individual developer.

For a detailed list of supported technologies, please see the Coverity Languages and Framework webpage.

ABOUT BLACK DUCK

Black Duck® meets the board-level risks of modern software with True Scale Application Security, ensuring uncompromised trust in software for the regulated, AI-powered world. Only Black Duck solutions free organizations from tradeoffs between speed, accuracy, and compliance at scale while eliminating security, regulatory, and licensing risks. Whether in the cloud or on premises, Black Duck is the only choice for securing mission-critical software everywhere code happens. With Black Duck, security leaders can make smarter decisions and unleash business innovation with confidence. Learn more at www.blackduck.com.