Secrets Scanning

According to “The State of Secrets Sprawl, 2023” report, the number of hard-coded secrets detected in GitHub commits has increased by an average of 67% per year.

The risks of hard-coded secrets

Many of the high-profile data breaches that have occurred in recent years have been caused by seemingly simple mistakes that could have been avoided. Hard-coded secrets that are left exposed in configuration files or source code can allow attackers to steal data or gain access to your most sensitive systems.

Secrets scanning from Black Duck analyzes source code, infrastructure-as-code (IaC) templates, and other file types to detect hard-coded secrets so they can be removed before they put your business and customer data at risk.

Various types of secrets

Black Duck complements regular expression pattern matching with application context and language semantics to detect many types of secrets that can put your systems and data at risk if they end up in the wrong hands.

Types of secrets

- Passwords
- Access tokens
- SSH keys
- API keys
- Cloud provider secrets
- Generic secrets

File types

- Source code
- Configuration files
- Scripts
- IaC templates
- Text files

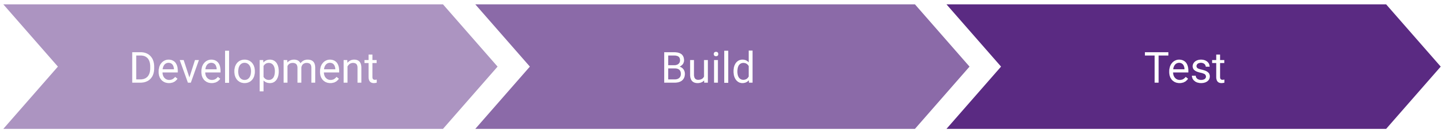
Secrets you know about, and some you don’t

Black Duck scans for more than 200 specific secrets patterns that are associated with popular technologies, such as AWS, Docker, and GitHub. This protects integrations with these systems from being exploited.

However, according to “The State of Secrets Sprawl, 2023” report, 67% of secrets detected in public repositories in 2022 were found using generic secrets scanning techniques. Generic scans identify text strings that resemble commonly used secrets without needing to define these patterns in advance. This is an effective complement to specific secrets detection, as these scans don’t require advanced knowledge of what you’re looking for and can help uncover vulnerabilities that would otherwise slip through the cracks. Black Duck combines specific secrets scans and generic secrets scans to ensure the best coverage for your applications.

Detecting hard-coded secrets throughout the SDLC

The best time to find and remove any vulnerability is early in the development process, before it's merged with other code or impacts other teams. Black Duck detects hard-coded secrets at several stages of the SDLC to make remediation as easy as possible and minimize the chance of secrets being pushed to public repositories or production environments.



Real-time IDE

- Code Sight™ IDE Plug-in

Static Analysis

- Polaris fAST Static
- Coverity® Static Analysis

Software Composition Analysis

- Black Duck® SCA
- Black Duck Binary Analysis

IAST

- Seeker® Interactive Analysis

- **Code Sight alerts developers to coding issues and hard-coded secrets in real time** so they can resolve issues before code is committed, without needing to switch tools.
- **Static application security testing (SAST) scans identify secrets hidden throughout your applications**, with the ability to trigger scans on commits or pull requests to prevent secrets from being merged into your main branch.
- **Software composition analysis (SCA) scans detect secrets in IaC templates** or source files that are packaged inside containers during the build phase of the pipeline.
- **Interactive application security testing (IAST) scans find vulnerabilities exposed during runtime,** such as secrets that are included in JavaScript code that's produced by a web server and sent to a mobile front end.

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.