aa teknoloji

Black Duck

Automated Security Analysis Across the Software Lifecycle

Black Duck is an application security solution that automates security controls in software development. It assesses source code through static testing (SAST), running applications through dynamic (DAST) and interactive (IAST) testing, and open source and third-party components through software composition analysis (SCA). It can be used on its own or integrated into existing DevSecOps processes.

Modern Security Challenges

In software projects, source code, running applications and third-party components each carry different security risks. When security controls are not built into development processes, vulnerabilities are found late and become more costly to fix. A growing number of findings also makes it harder for teams to prioritize critical risks.

Who can benefit?

- Software teams that want to identify security vulnerabilities
- DevSecOps teams that want to integrate security testing into CI/CD pipelines
- Security teams that want to prioritize and track security findings
- Organizations that want to build software security into their development processes

Core Principles

Security
Identifying software vulnerabilities and risky dependencies

Automation
Integrating security analysis into CI/CD pipelines

Prioritization
Focusing on critical security findings

Continuity
Supporting security throughout the software lifecycle

Technical Specifications

Analysis Coverage
- Static application security testing (SAST)
- Dynamic application security testing (DAST)
- Software composition analysis (SCA)
- Interactive application security testing (IAST)

Detection Capabilities
- Detection of known component vulnerabilities
- Analysis of open source license risks
- Assessment of software components by security risk
- Impact analysis of vulnerabilities in source code

Integrations
- Source code management platforms such as GitLab and GitHub
- CI/CD automation tools such as Jenkins and GitLab CI/CD
- Integration with IDEs and developer tools
- SIEM/SOAR integration

Compliance and Reporting
- Tracking of open source license obligations
- Creating and managing a software bill of materials (SBOM)
- Central tracking of security findings
- Risk and license compliance reporting

How Does Black Duck Work?

Black Duck analyzes source code, running applications and software components to help identify vulnerabilities and license risks. By combining SAST, DAST, IAST and SCA, it brings security controls into the software development lifecycle and helps teams prioritize critical findings.

Workflow

1. Software Analysis
- Source code, running applications and software components are analyzed.
- SAST, DAST, IAST and SCA checks are applied.
- Security vulnerabilities and risky dependencies are identified.
- License compliance risks are assessed.

2. Evaluating Security Findings
- Detected vulnerabilities are reviewed centrally.
- Findings are prioritized by severity and risk level.
- Critical security risks are identified.
- Findings that require remediation are assigned to the relevant teams.

3. Remediation and Process Integration
- Developers receive guidance on how to fix security findings.
- Security checks are integrated into CI/CD pipelines.
- Pipelines or releases can be blocked automatically when critical findings are detected.
- Follow-up scans track the status of fixes.

Why AA Teknoloji?

AA Teknoloji handles Black Duck installation, integration with your existing CI/CD and source code management infrastructure, and product training for your teams. After deployment, we provide 24/7 technical support in Turkish.

Advantages

Comprehensive Security Analysis
Helps identify vulnerabilities and license risks by analyzing source code, running applications and software components.

Early Vulnerability Detection
Helps identify vulnerabilities during development and testing, reducing remediation costs.

Risk-Based Prioritization
Evaluates security findings by severity, so teams can focus on critical risks.

DevSecOps Integration
Supports integrating security controls into CI/CD pipelines and applying them throughout the software development lifecycle.

aa teknoloji

AA Teknoloji is a technology company and an Anadolu Ajansı affiliate, providing media technologies, cybersecurity, and open-source solutions. It delivers SOC services, penetration testing, SIEM/EDR, threat intelligence, and media infrastructure solutions together with deployment, integration, and 24/7 local technical support.

For more information, visit aateknoloji.tr or follow @aateknoloji on LinkedIn.