

Complete Application Security Testing Solution to Eliminate Known And Unknown Code Threats Across SDLC

The digital transformation has made application development 10x more agile

Frequent code changes and a fast pace cause security to be deprioritized in the rush to meet deadlines. Agile methods, emphasizing rapid development, often place security considerations on the back burner rather than being integrated into the initial design. Integration of third-party components can introduce vulnerabilities if not properly vetted and updated.

Due to deadlines, developers are taking shortcuts and overfilling the source code with

Hardcoded Secrets

Such as passwords, encryption and, API keys

Backdoors

Hidden entry points left for debugging can be exploited by attackers

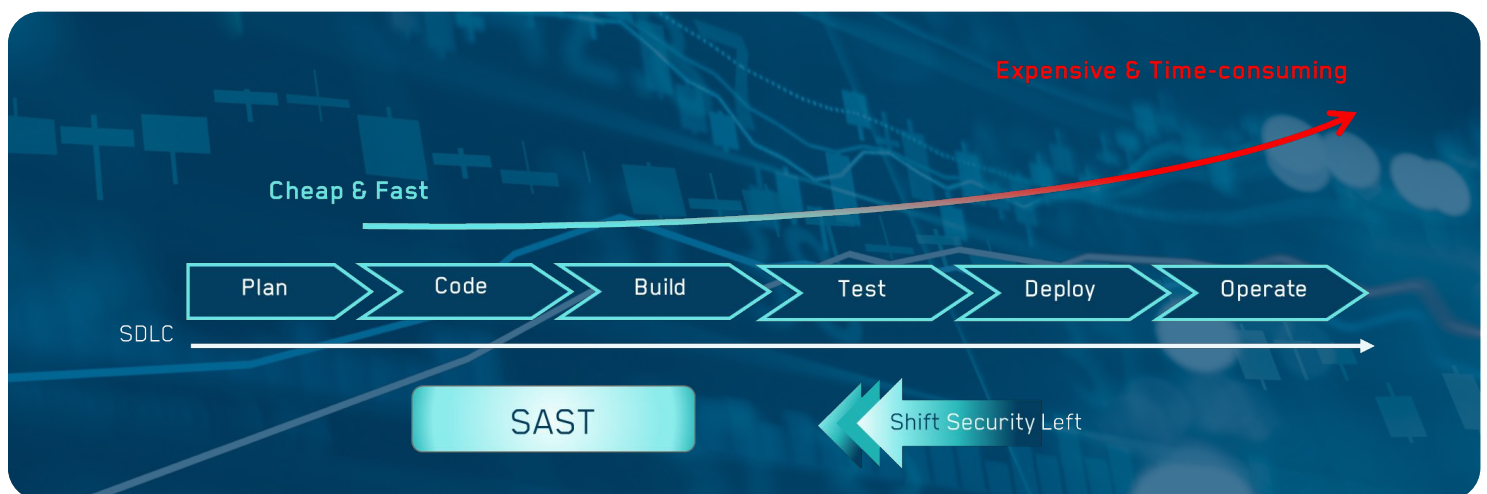
Insufficient Input Validation

May lead to SQL injection, cross-site scripting (XSS), and buffer overflows

Unverified open-source or third-party components

Downloaded from the Internet may bring malicious code

Discovering vulnerabilities at a later stages in the development process significantly increases the cost and time of fixing them



Start with Early Detection of Known Vulnerabilities

Shift security left with DerScanner by implementing Static Analysis (SAST) early in the development pipeline. Scan the application's source code to identify patterns that match known vulnerabilities.

A Single Solution for 43 Popular Languages

DerScanner perfectly deals with polyglot applications streamlining security analysis across 43 programming languages.



Integrate Security Checking in your Software Development Lifecycle

Integrate DerScanner with key developer tools to conduct early source code checks in the pipeline, making security a seamless aspect of the development process. Such integration reduces friction between developers and security teams, promoting satisfaction on both sides. It not only helps meet release deadlines but also ensures the release of safer applications.



Unveil the Unseen, Secure the Undiscovered

Opt for binary scanning with DerScanner to reveal hidden vulnerabilities and ensure robust security, especially when source code access is limited or unavailable.

Legacy Applications

Assess and mitigate vulnerabilities where source code might be lost, outdated, or poorly documented

Compliance and Audit

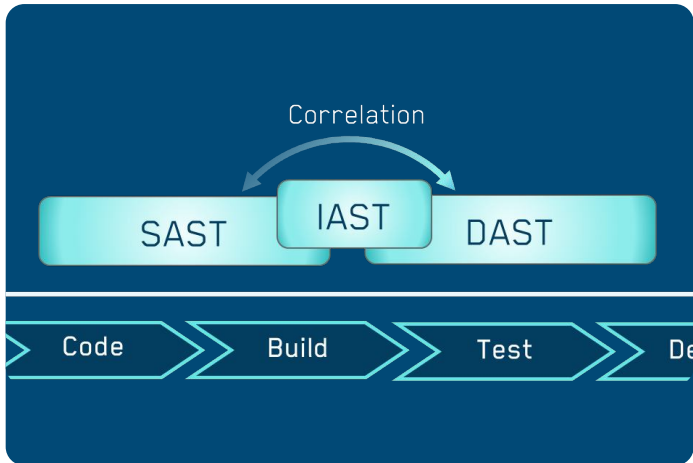
Ensure the compiled application complies with security regulations in compliance strict industries

Identify Exotic Vulnerabilities

Discover harmful vulnerabilities that might not be detectable through source code analysis



Test Web Applications from an External Perspective



Dynamic Analysis (DAST) in **DerScanner** operates like an external attacker, similar to penetration testing, to uncover vulnerabilities that might be exploited once the application is live. IAST (Interactive Application Security Testing) unifies the efforts of DAST and enhances SAST findings by cross-checking and correlating vulnerabilities detected by both methods. As a black-box testing method, DAST does not require access to the source code, making it ideal for testing web applications.

Pass Compliance Assessment with Ease

According to your industry, various regulatory standards require security testing of operational applications. Get a vulnerability report to ensure your code is compliant with the dedicated frameworks.



Ensure Confidence in Open-source Components with Software Composition Analysis

You can't restrict developers from using third-party components. But you still can prevent the open-source driven and supply chain risks with Software Composition Analysis in DerScanner.



open source

Visibility into Open-source

Gain visibility into open-source components and dependencies to detect known vulnerabilities before they become exploitable.

Supply Chain Risk Prevention

Prevent threats targeting supply chain including typosquatting, starjacking, and MavenGate attacks.

License Compliance

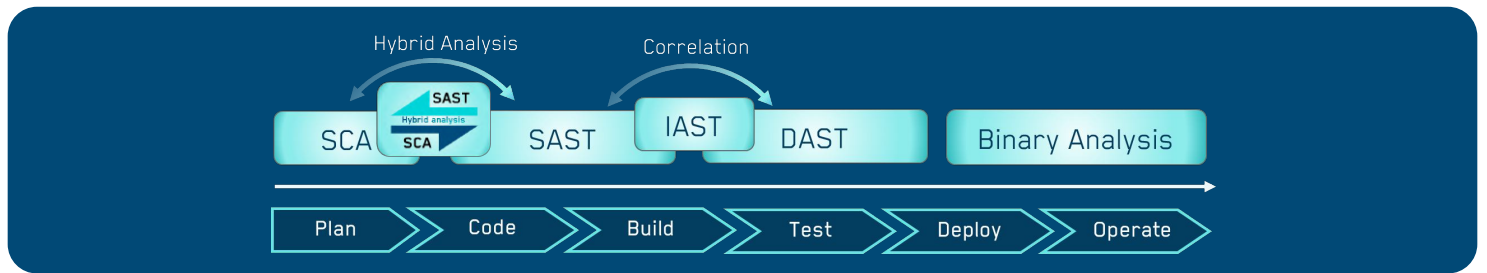
Ensure that the open-source licenses of used components are compatible with the project's licensing terms to avoid legal issues.

Package Healthy Scoring

Choose packages with high health scores to avoid projects with a history of vulnerabilities or poor security practices.

Remediate Known and Unknown Code Threats across SDLC

Protect any application from both known and unknown vulnerabilities and integrate security checks in your SDLC to sync development and security efforts.



Why Customers Choose DerScanner

Single AppSec Platform

- Natively integrated major application security technologies
- Detects correlation for the full context of what issues matter the most

Low False Positives

- Proprietary AI-driven Confi AI engine to set the threshold of alerts that suits your priorities best

Industry Recognized

- Recognized by **FORRESTER** among notable SAST and SCA vendors.
- CWE certified by **MITRE**
- Highly rated by customers on G2



Security Friendly Reports

- Reports are written in simple language that a security professional with no development experience can understand

Best for Security Audits

- Even if the source code is not available, check running web and mobile apps or legacy apps with a combination of binary SAST and DAST

Traditional Technical Support

- No bots. Only classical people-powered support
- Messenger chat support for Enterprise customer

About DerSecur

DerSecur, established in 2011, is at the forefront of application security. Its team of 70 experts has developed DerScanner, a versatile application security solution that supports 43 programming languages and provides static, dynamic and software composition analysis. DerSecur is committed to furthering cybersecurity research and development, ensuring a more secure digital future.

<https://derscanner.com/> company@dersecur.com

