DerScanner

LESS TIME FIXING, MORE TIME BUILDING

with DerScanner's AI Vulnerability Triage and Auto-fix

While AI tools like GitHub Copilot and ChatGPT boost developer productivity 10-50x faster than traditional methods, they also introduce significant security threats into codebases. Compounding this issue, traditional manual vulnerability triage and remediation processes are highly resource-intensive, requiring highly skilled security analysts to sift through false positives, prioritize issues, and implement fixes. This not only slows down development cycles but also increases the likelihood of critical vulnerabilities slipping into production as teams become overwhelmed by the sheer volume of potential threats.

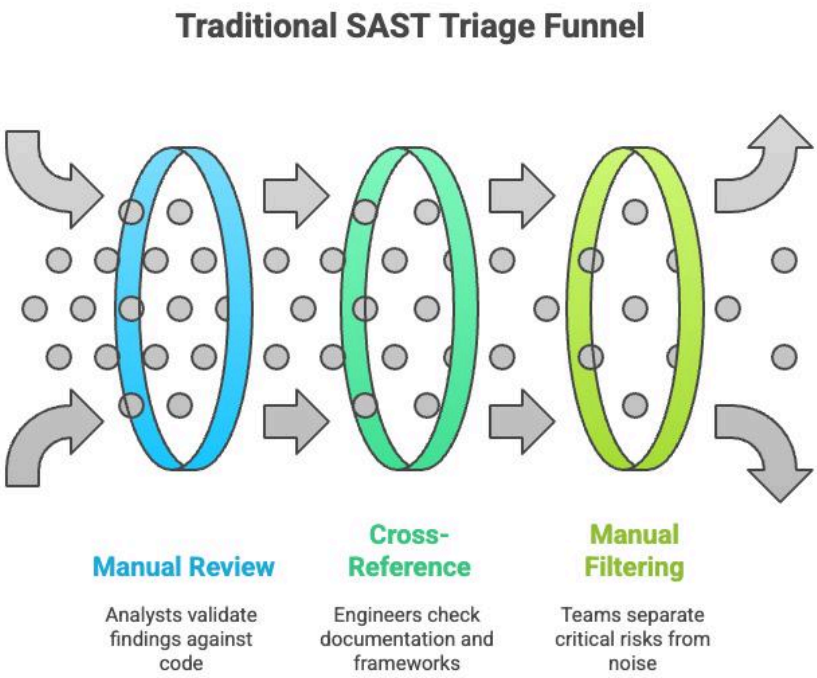
DerScanner redefines triage and remediation workflows with AI-powered DerTriage and DerCodeFix capabilities. By automating issue prioritization and streamlining fixes, DerScanner empowers both developers and security teams to **spend more time on building features rather than fixing issues**.

REINVENTING VULNERABILITY TRIAGE WORKFLOWS

DerTriage, the new AI-powered triage module within DerScanner, transforms how teams prioritize, analyze, and act on SAST findings. Built to complement fast-paced development environments, DerTriage brings context-aware reasoning and automation into the heart of vulnerability management—drastically reducing noise, manual effort, and time-to-fix.

What Traditional SAST Triage Process Used to Look Like

Historically, SAST triage has been manual and time-intensive.



1. Analysts reviewed every flagged SAST finding, validating it against code logic and business context.
2. Security engineers cross-referenced documentation, frameworks, and known false positives.
3. Teams manually filtered through hundreds of issues per scan to separate critical risks from noise.

This reactive, person-driven workflow was often disconnected from development velocity—leading to **bottlenecks, delayed remediations, and reduced trust in SAST output**.

What Resources Were Required?

Traditional triage demanded significant investments:

- **Time**. Weeks of accumulated review effort across projects.
- **Expertise.** Senior AppSec engineers or security-savvy developers familiar with frameworks, logic, and language-specific edge cases.
- **Communication cycles**. Repeated back-and-forth between security and development teams to interpret findings.

In fast-moving environments, this became unsustainable.

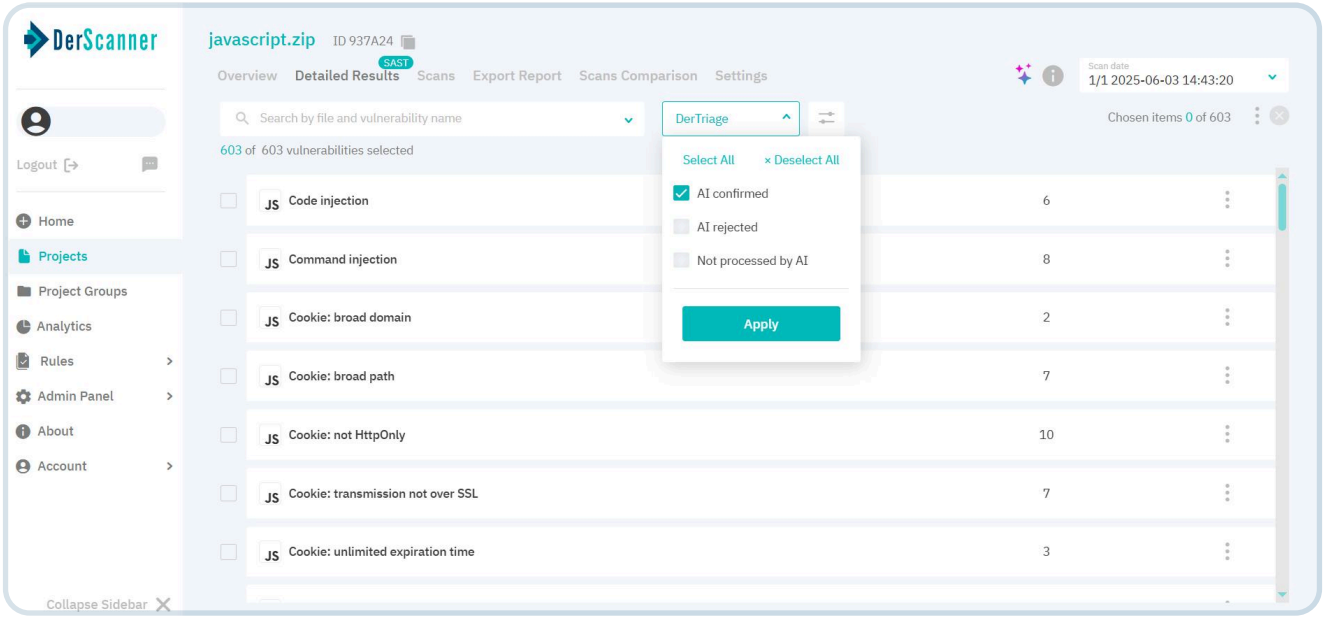
The Challenges of Manual Vulnerability Triage

Despite its criticality, manual triage is fraught with challenges:

- **High False Positive Rates**. Static analysis engines are powerful, but without context, they often flag non-exploitable patterns.
- **Security Bottlenecks**. As AI accelerates code output, triage speed cannot keep up—creating security debt.
- **Inconsistent Prioritization**. Human triage is subjective. Two analysts may classify the same issue differently.
- **Developer Friction**. Overreporting leads to fatigue, undermining trust in security tooling and slowing adoption.
- **Wasted Effort**. Teams repeatedly triage the same common patterns across projects, adding no new value.

How DerTriage Transforms Vulnerability Triage

DerTriage is not just another filter—it's an AI reasoning engine purpose-built for static analysis triage.



Eliminate 95% of False Positives

Advanced AI models analyze vulnerability context, code patterns, and exploitability factors to automatically classify findings as genuine threats or false positives with 95%+ accuracy.

Continuous Developer Eduction

Each triage verdict comes with a clear explanation. No black-box logic–just clear, human-readable justifications for every action.

Continuous Codebase Improvement

Trained on real-world examples and static analysis best practices, DerTriage improves with every release, adapting to evolving code trends and exploit patterns.

Seamless Integration

Trigger DerTriage alongside your standard DerScanner analysis–no pipeline changes required. Use in bulk or apply selectively to critical results.

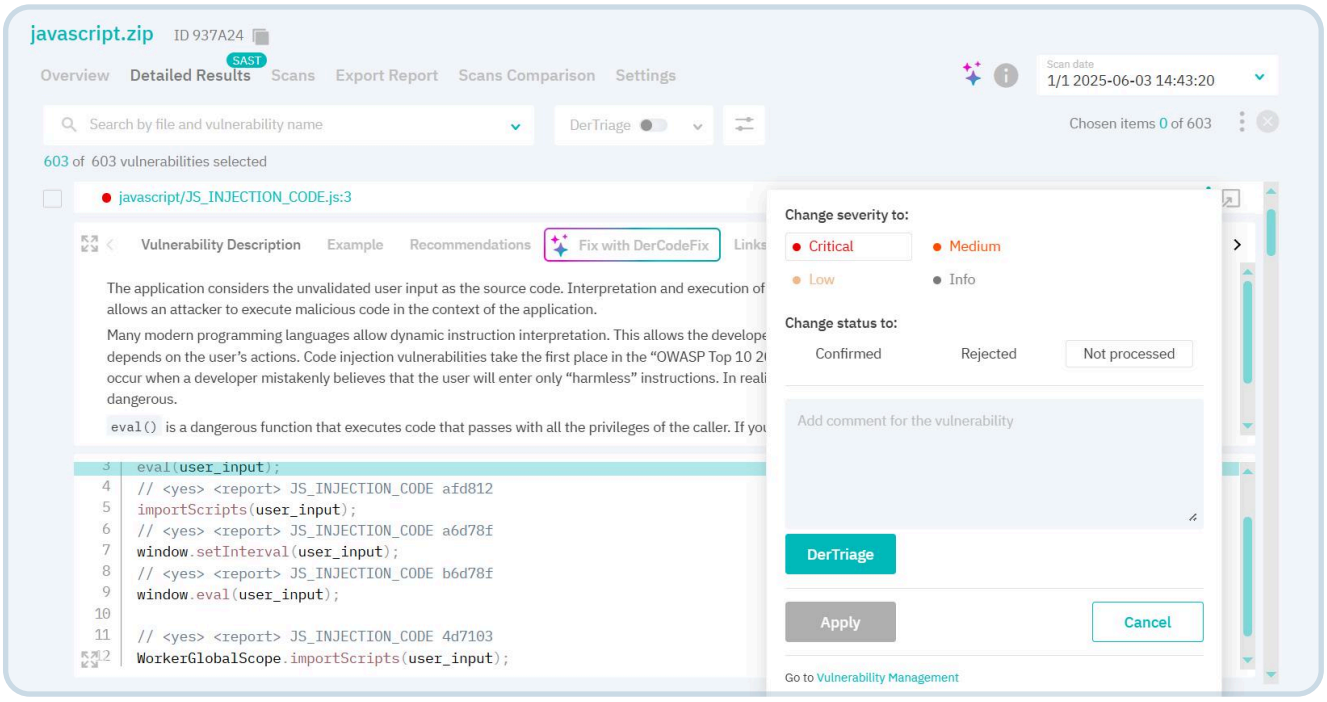
Benefits of DerTriage in DerScanner

Noise Reduction	Up to 90% fewer false positives in triaged results
Faster Time-to-Remediation	Cuts down triage time from hours to minutes per scan
Developer Trust	Clean, actionable findings improve developer buy-in and remediation rates
Scales with Code Volume	Triage AI matches the velocity of AI-generated and high-volume codebases
On-Prem, IP-Safe	All AI processing can be done offline with full control over code privacy

Designed for New Age Development Workflows

DerTriage was purpose-built for the demands of modern development teams:

- Stellar for CI pipelines and legacy projects alike.
- Integrates seamlessly with DerScanner's remediation engine (DerCodeFix) to suggest AI-generated fixes for confirmed vulnerabilities.
- Fully configurable—apply triage logic to all findings or only high-priority risks.
- Operates in air-gapped environments for maximum IP safety and compliance.



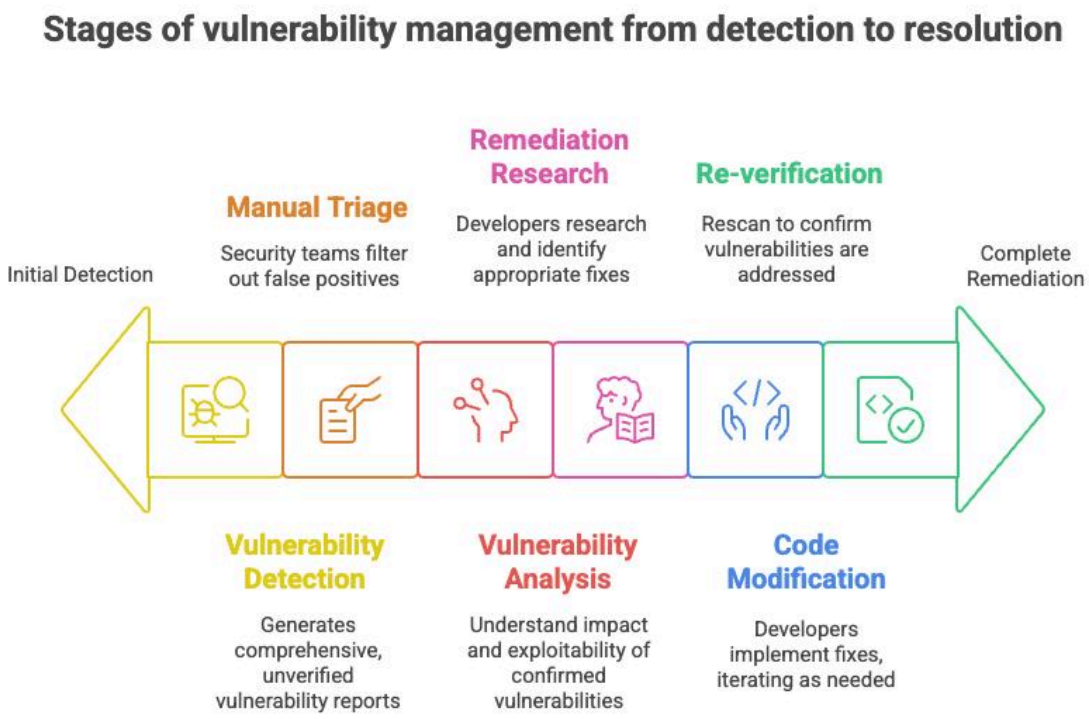
SPEEDING UP VULNERABILITY FIXING WITH DERCODEFIX AI

In the race to deliver software faster, development teams are writing more code than ever—often assisted by generative AI tools. While productivity soars, so does the risk: AI-generated code frequently contains hidden vulnerabilities. Traditional security workflows can't keep up.

Enable DerCodeFix AI—an AI-powered vulnerability remediation engine that revolutionizes how security and development teams handle static application security testing (SAST) results in DerScanner.

What Vulnerability Fixing Used to Look Like

Traditionally, SAST vulnerability management followed a labor-intensive, multi-stage process:



1. **Raw Vulnerability Detection:** Static analysis tools would scan codebases and generate comprehensive vulnerability reports

2. **Manual Triage:** Security teams would manually review each finding to determine if it represented a genuine security risk or was a false positive

3. **Vulnerability Analysis:** Security professionals would analyze confirmed vulnerabilities to understand their impact and exploitability

4. **Manual Remediation Research:** Developers would research appropriate fixes, consulting documentation and security best practices

5. **Code Modification:** Developers would manually implement fixes, often requiring multiple iterations

6. **Re-verification:** Teams would re-scan to confirm vulnerabilities were properly addressed

Resource Requirements That No Longer Scale

This traditional approach demanded extensive human resources:

- **Highly paid dedicated application security analysts** to perform vulnerability triage and classification
- **Senior developers with security expertise** to understand and implement fixes
- **Significant time investment**—often days or weeks per vulnerability depending on complexity
- **Specialized security knowledge** to distinguish between genuine threats and false positives
- **Continuous training** to stay up to date with evolving vulnerability patterns and remediation techniques

The Compounding Problems of Manual Vulnerability Fixing Processes

Manual vulnerability fixing creates cascading inefficiencies:

- **False Positive Fatigue:** SAST tools, while comprehensive, inevitably generate false positives. Security teams waste 40-60% of their time investigating non-threats, leading to alert fatigue and reduced attention to genuine vulnerabilities.
- **Knowledge Bottlenecks:** Vulnerability remediation requires specialized security expertise that's concentrated in a few senior team members, creating bottlenecks that slow down the entire development pipeline.
- **Inconsistent Remediation Quality:** Manual fixes vary in quality depending on developer experience and security knowledge, leading to incomplete fixes or the introduction of new vulnerabilities.
- **Scalability Crisis:** As codebases grow and development velocity increases, manual processes simply cannot keep pace. The vulnerability backlog grows exponentially while security debt accumulates.
- **Context Loss:** By the time vulnerabilities are identified and triaged, the original developer context is often lost, making remediation more difficult and time-consuming.

- **Technology Stack Expansion:** The number of programming languages, frameworks, and third-party libraries in use is constantly growing. Even experienced teams find themselves dealing with unfamiliar technologies, making it harder to assess and fix vulnerabilities correctly and efficiently.

- **Third-Party Code Maintenance:** In many cases, teams are responsible for maintaining legacy systems or third-party code they didn't write. Without deep understanding of the codebase, even identifying the impact of a vulnerability becomes a major challenge—let alone fixing it without breaking functionality.

DerCodeFix AI: Context-Aware Fixes Built for High-Speed Development

DerCodeFix AI fundamentally transforms vulnerability management by introducing new AI capabilities directly into the DerScanner platform. DerCodeFix AI intelligently analyzes detected vulnerabilities and generates context-aware, production-ready code fixes.

Generates Production-Ready Fixes: AI analyzes vulnerable code patterns and generates secure, contextually appropriate remediation that preserves functionality while eliminating security risks.

Maintains Code Quality: Fixes are generated with proper coding standards, maintaining readability and performance while addressing security concerns.

Provides Transparency: Every fix includes detailed explanations of what was changed and why, enabling developer learning and code review confidence.

Transformative Business Value

500% Faster Vulnerability Remediation with AI-Generated Fixes

75% Developer Acceptance Rate for DerCodeFix AI Remediation Suggestions

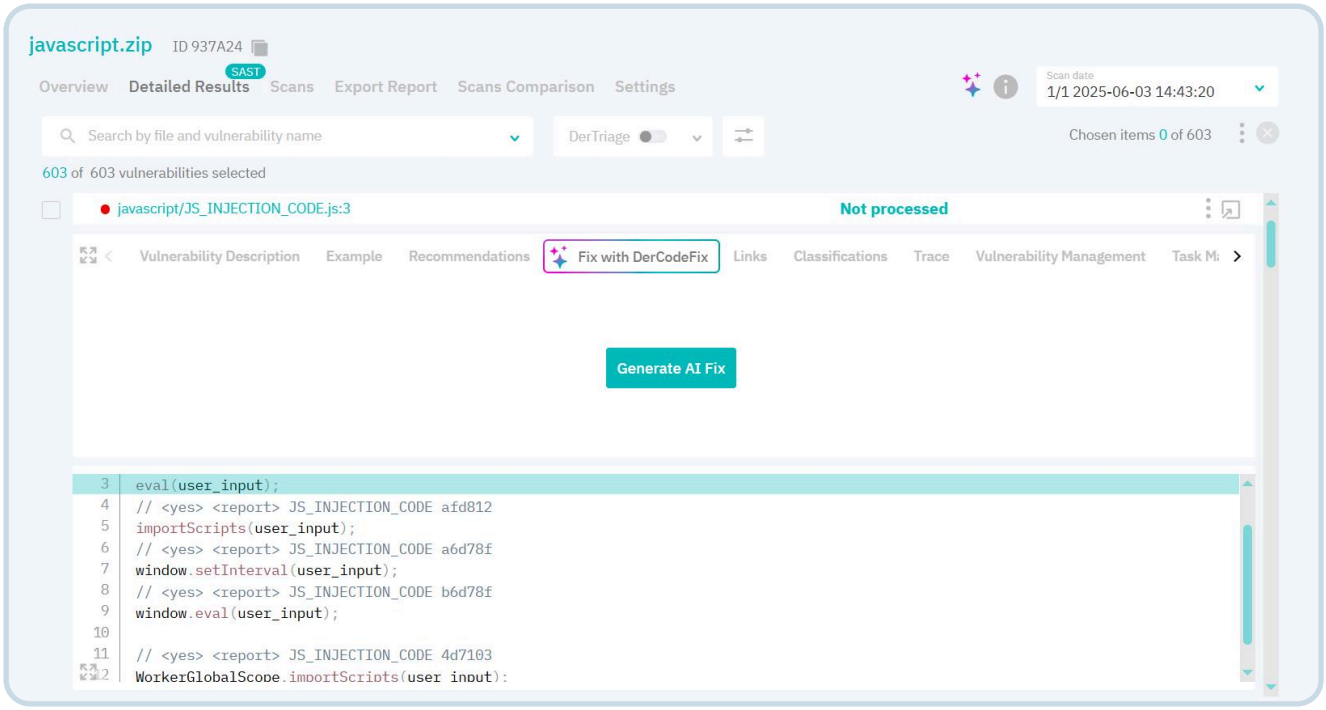
10x Boost in Team Productivity – Focus Shifts to Building More than Fixing

DerCodeFix AI: Smart and Actionable Remediation

Secure-by-default code fixes generated automatically, with human-readable diffs and justifications. Fix vulnerabilities at the speed of AI—without sacrificing security context.

How It Works

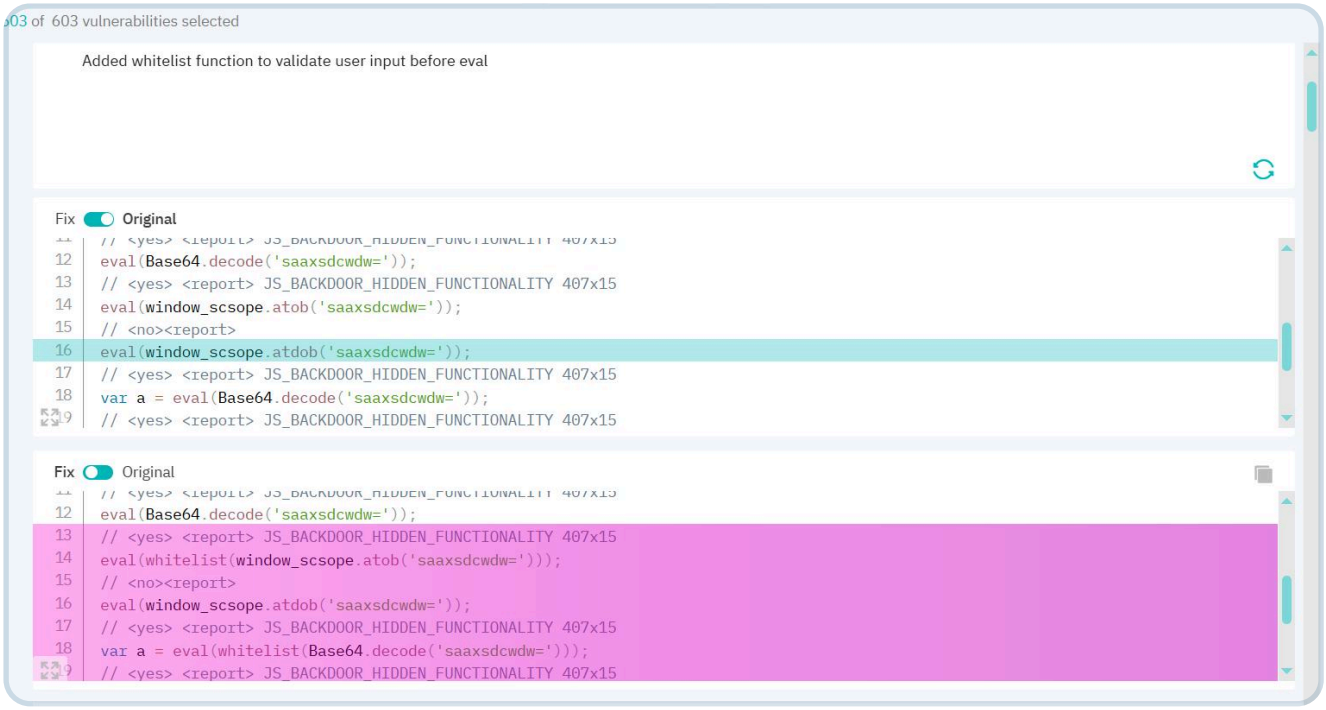
1. **Scan** your codebase with DerScanner (on-prem or cloud).



2. **Triage**: DerTriage AI evaluates each finding for true exploitability.

3. **Fix**: DerCodeFix AI generates secure remediation suggestions in place.

4. **Review**: Developers get full transparency—view the before/after code and fix rationale.



5. **Ship Securely**: Push secure, reviewed code with confidence.

Benefits of DerCodeFix AI in DerScanner

While cloud-based AI Auto-Fix tools present data residency and IP governance risks, DerCodeFix AI delivers:

Accelerated Fixes	• Cut time-to-remediation from hours to seconds • Faster time-to-market with security built-in rather than bolted-on • Real-time security matching the pace of modern development workflows
Developer Enablement	• No more back-and-forth between AppSec and Dev • Consistent remediation quality eliminating human error and knowledge gaps • Executive confidence in security posture despite accelerated development
Complete Data Control	• On-premises LLM deployment ensuring complete intellectual property protection • Air-gapped environments available for maximum security • Zero data sharing with external AI services, maintaining confidentiality

DERSCANNER BRINGS ON THE FUTURE OF AI-POWERED SECURE DEVELOPMENT

DerTriage and DerCodeFix AI represent the next evolution in application security—where AI-powered security keeps pace with AI-powered development. Organizations using DerScanner new AI capabilities report:

Security teams becoming strategic partners rather than development bottlenecks	Developers learning security best practices through AI-generated explanations	Zero compromise between development velocity and security posture

With DerScanner's advanced AI capabilities, development and security teams can finally shift their focus from tedious vulnerability management to driving innovation. By leveraging DerTriage and DerCodeFix, organizations achieve up to 500% faster remediation times, reduce false positives by up to 90%, and empower developers to maintain productivity without sacrificing security. These tools eliminate inefficiencies, enhance the quality of fixes, and provide actionable insights, enabling seamless integration into fast-paced development workflows. The result is a secure development cycle where tackling vulnerabilities no longer hinders progress but paves the way for faster, more confident software delivery.

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/