SOLUTION BRIEF

Evolution in application security

The need for a new application security model

The velocity of modern software development, driven by AI-powered code generation, has exposed the inherent limitations of traditional application security tools. These legacy toolsets force a trade-off: either sift through the noise of scanners (DAST/SAST) to find theoretical vulnerabilities, or attempt to block attacks by analyzing perimeter network traffic and endpoint data, which lack application-level context. This creates a dangerous gap. AppSec teams are left managing a growing backlog, while production systems are attacked by exploits invisible to their existing security stack.

Application layer attacks present a mandate for security teams to re-evaluate what data they should bring into their existing SIEM and SOAR tools. The goal is not to replace these investments, but to enhance them with a fundamentally superior data stream built for the complexity of today's application landscape.

The different approaches

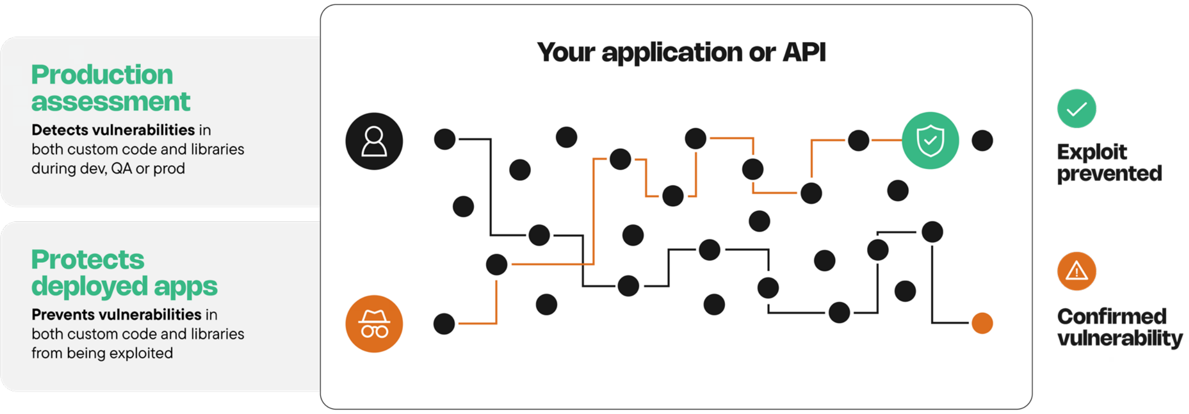
The critical difference between legacy and modern AppSec platforms lies in how they acquire and analyze security data.

Legacy architecture: outside-in analysis

This approach uses separate, siloed tools for different problems. SAST and DAST scanners are used to simulate attacks and analyze code. They are white-box and black-box by nature, respectively, and both infer the existence of a vulnerability. This lack of runtime context leads to high false-positive rates. For production protection, this architecture relies on separate tools like Web Application Firewalls (WAFs) that are completely disconnected from vulnerability data. These perimeter defenses use static signatures to identify threats, an approach that is ineffective at distinguishing a harmless probe from a genuine attack and leaves applications exposed to novel or zero-day exploits.

Modern architecture: instrumentation-based intelligence

This approach puts a sensor directly into the application's runtime environment (e.g., JVM, .NET CLR, Node.js), without making any changes to an application or API's source code . By monitoring an application at runtime, this single, lightweight agent pinpoints actual exploitable lines of code. It uses this deep runtime context to simultaneously detect and block active attacks—including novel and zero-day threats—while also providing developers with the exact remediation guidance to fix the root cause permanently. Instead of inferring risk with disconnected tools, this "inside-out" architecture directly observes both the vulnerability and the attack, providing a single, correlated source of truth from a single platform.



Production assessment

Detects vulnerabilities in both custom code and libraries during dev, QA or prod

Protects deployed apps

Prevents vulnerabilities in both custom code and libraries from being exploited

Legacy toolsets vs. runtime security

A modern platform provides a new, critical data stream that is impossible to generate with legacy tools. This data feeds directly into your existing SIEM tools, providing a new view into application-layer attacks. The table below breaks down the difference in the data generated by each approach.

Evaluation criteria	Legacy toolkits	Contrast runtime security platform
Core technology	A collection of disconnected tools: static "white-box" analysis (SAST), dynamic "black-box" scanning (DAST) and signature-based perimeter detection (WAF).	Deep security instrumentation that provides direct observability of runtime execution from a single agent.
Vulnerability detection	Generates high rates of false positives due to a lack of real-world runtime context.	Confirms vulnerabilities by tracking real data from entry point to a sensitive function, virtually eliminating false positives.
SCA context	Identifies the presence of a vulnerable library in a manifest file.	Identifies a vulnerable library and confirms whether it is actually being called by the application at runtime.
Attack context and prioritization	Vulnerability data is disconnected from attack data, forcing prioritization based on theoretical scores.	Correlates active attack data with known vulnerabilities, allowing teams to prioritize remediation based on real-world risk.
Real-time attack blocking	Testing tools (SAST/DAST) offer no protection. Relies on separate, signature-based tools (WAF) that are ineffective against novel zero-day attacks.	Precise in-application blocking of malicious activity, including zero-day exploits, without relying on signatures.
Response and remediation data	Provides either the line of code (SAST) or the URL (DAST), but findings often lack proof of exploitability, requiring manual validation.	Delivers the exact line of code, full stack trace, and complete HTTP request for verified vulnerabilities, enabling rapid remediation.

The superiority of the modern, unified platform stems from its ability to not only collect vast amounts of runtime telemetry but also to contextualize it. This is where a true architectural advantage emerges, moving beyond simple data collection to active intelligence.

From raw data to actionable intelligence: the Contrast Graph

A SIEM is only as good as the data it ingests. While it provides visibility into network, cloud, and endpoint activity, it has a critical blind spot: the application layer. The Contrast Graph is the source of truth that fills this gap.

The rich telemetry gathered by our sensors feeds the Contrast Graph, an intelligent engine that contextualizes application security data before it is sent to your SIEM. Instead of flooding your security operations with low-context alerts, the Graph delivers high-fidelity intelligence by:

- **Mapping attack surfaces:** The Graph continuously models the complex architecture of your applications, including all APIs, services, libraries, and infrastructure connections.
- **Correlating signals:** This model links observed vulnerabilities directly to active attack probes, allowing you to prioritize remediation based on real-world risk.
- **Enabling dynamic prioritization:** Advanced analysis calculates risk scores based on exploitability, asset criticality and active threat intelligence to ensure your teams focus on what truly matters.

A strategic upgrade for modern application security

Adopting an instrumentation-based architecture is more than a tool replacement—it is a strategic decision to eliminate operational friction, accelerate development and gain a true, unified view of application risk. By giving security teams real-time visibility into production attacks and vulnerabilities, and using that intelligence to provide developers with trusted, actionable findings, the Contrast platform creates a sustainable and effective operating model for modern application security.

Learn more

Contrast Security is the world's leader in Runtime Application Security, embedding code analysis and attack prevention directly into software. Contrast's patented security instrumentation enables powerful Application Security Testing and Application Detection and Response, allowing developers, AppSec teams and SecOps teams to better protect and defend their applications against the ever-evolving threat landscape.

contrastsecurity.com

6800 Koll Center Parkway
Ste 235
Pleasanton, CA 94566
Phone: 888.371.1333