SOLUTION BRIEF

Runtime protection for software providers and application developers

Balance rapid innovation without compromising security

Technology organizations that create, manage and distribute software solutions, range from enterprise software providers to specialized application developers. Their solutions support business operations, data management, cybersecurity and digital transformation initiatives for organizations from boutique retailers to Fortune 50 global enterprises. Today's SaaS-based solutions enable scalable deployment, continuous updates and remote access, offering rapid deployment, flexibility and efficiency for customers.

Yet, technology organizations must prioritize rapid innovation and excellent user experience without compromising on security to maintain competitive advantage. Many are leaning more heavily on AI and open source to innovate faster, but this leaves a lot of open questions around the security of the underlying code.

Statistics: The pace of application delivery in the AI era

- Up to 30% of code is AI-generated
- 86% of codebases had open source software vulnerabilities
- 76% of apps had security flaws
- Only 5 days for attackers to exploit vulnerabilities
- Up to 63 days for software companies to patch a vulnerability

The problem: Drowning in alerts, but blind to real threats

As technology companies accelerate software development using DevOps and CI/CD pipelines, the pace and complexity of modern application delivery are outpacing the capabilities of traditional application security methods. These legacy approaches, often reliant on periodic scans and manual processes, cannot match the continuous and automated nature of modern development cycles. Additionally, the rise of AI-generated code—while enhancing productivity—is introducing new and unforeseen vulnerabilities at a scale and speed never seen before.

Without runtime application security solutions, organizations risk exposing critical systems to exploitation. To stay secure, security practices must evolve alongside development methodologies and emerging technologies like AI, accounting for these primary challenges:

- **Inadequate runtime protection,** which leaves applications exposed to zero-days and known vulnerabilities.
- **AI-generated insecure code** (trained on potentially vulnerable human-written code) proliferation.
- **False positives** that can overwhelm security teams and developers.
- **Point-in-time testing** (SAST, DAST) which misses critical runtime context.
- **Limitations of penetration testing** which offers only a "point-in-time" assessment.
- **Delayed feedback** in the dev cycle, leading to bottlenecks.

Bottom line: Application security can no longer be bolted on after deployment; it must be built in and run continuously.

Why runtime application security for technology organizations?

Crowd-sourced intelligence

Leveraging aggregated telemetry across thousands of real-world running applications, enhanced with AI to detect patterns that might indicate emerging zero-day threats.

Block attacks against vulnerable AI-generated code

Runtime application security provides context-aware detection, which is essential when AI might write thousands of lines of insecure code in minutes, and zero-day vulnerabilities might spread faster than manual teams can respond.

Detect vulnerabilities at runtime in pre-production and in production

Traditional AppSec methods focus on finding vulnerabilities before deployment, but runtime security can detect and prevent exploits against vulnerabilities in production, including zero-day vulnerabilities.

Visibility into actual attack behavior

Runtime application security operates within the live application, offering real-time visibility into actual attack behavior, which enables smarter vulnerability prioritization and immediate compensating controls.

Essential safety net

When a vulnerability is identified, deploying a patch can take time, especially in complex systems with strict release schedules or regulatory constraints. Runtime application security can apply compensating controls even before a permanent fix is deployed.

Protect against zero-day attacks

A zero-day attack is an exploit that targets a previously unknown software vulnerability before a fix is available. Runtime application security can block these attacks by monitoring application behavior in real time.

Continuous protection throughout the SDLC

Runtime application security provides continuous security observability, embedding security into applications to protect them from threats during all stages of their lifecycle, including development, testing and production.

Scalable protection

Runtime application security can scale to protect entire application stacks, including APIs and third-party applications, ensuring comprehensive protection across the entire software ecosystem.

The Contrast advantage: Securing software in development and production environments

Benefit	Value
Detect and quickly block attacks	Monitors application behavior and data flow identifying suspicious patterns and anomalies and when an attack is detected, leveraging agentic AI to block the attack and alert security teams with context and actionable information.
Zero-day resilience	Instruments applications from within, rather than relying on signature-based detection, enabling the detection and response to both known and unknown threats, including zero-day exploits, through behavioral analysis within the application runtime.
Automated remediation guidance	Delivers precise, actionable security insights, accelerating response times and ensuring that vulnerabilities are fixed before they impact critical services. Dynamic risk scoring brings a smarter way to prioritize based on what's actually at risk in production.
Reduce MTTR and strengthen security posture	Provides a unified platform that eliminates the guesswork that plagues traditional tools, enabling accurate, automated prioritization and remediation allowing teams to filter out noise, enabling a focus on the most critical risks to data and application integrity.

Why Contrast is different

Together, Contrast AST and ADR create a feedback loop between development, security and operations. AppSec teams can prioritize fixes based on exploitability data from AST, while SOC teams gain high-fidelity alerts enriched with code-level context.

CONTRAST APPLICATION DETECTION AND RESPONSE (ADR)

Protect applications and APIs from exploits and zero days.

Detect attacks on applications and APIs so security operations teams can respond before exploits occur.

CONTRAST APPLICATION SECURITY TESTING (AST)

Monitor code as it runs.
Identify vulnerabilities instantly.

Prioritize and address risks with faster application and API vulnerability detection and fewer false positives.

CONTRAST ONE

Defend your applications and APIs with Contrast One.

Managed application and API security powered by the people who built it.

Ready to see the Contrast runtime security platform in action?

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