WHITEPAPER

Runtime security for small and midsize businesses (SMB)

Overcoming the application blindspot and resource constraints through runtime visibility and control

Businesses under 1000 employees were breached 4 times more often than large organizations and faced double the breach risk from vulnerability exploits, according to the 2025 Verizon Data Breach Investigations Report. This disproportionate targeting occurs precisely when security teams often manage broad responsibilities with carefully allocated resources, making effective defense challenging. For these businesses, a successful breach isn't just an operational setback; it can trigger crippling financial penalties, legal liabilities and a loss of customer trust that threatens their very existence.

A primary reason for this breach risk lies in the "application blindspot." While firewalls monitor networks and endpoint detection watches processes, the complex interactions within running applications and APIs often remain opaque to traditional security tools. Attackers exploit this visibility gap to target business logic and internal flaws. This lack of runtime insight allows threats to dwell undetected, leading to potentially severe consequences like data theft, operational disruption and erosion of customer trust — impacts that can derail a growing company and, in some cases, prove unrecoverable. Addressing this blindspot is a critical security imperative, especially when the financial and operational stakes are so high.

Alert fatigue, context gaps and blindspots: The reality for security teams

Security functions within midsize businesses face a unique convergence of challenges when securing applications:

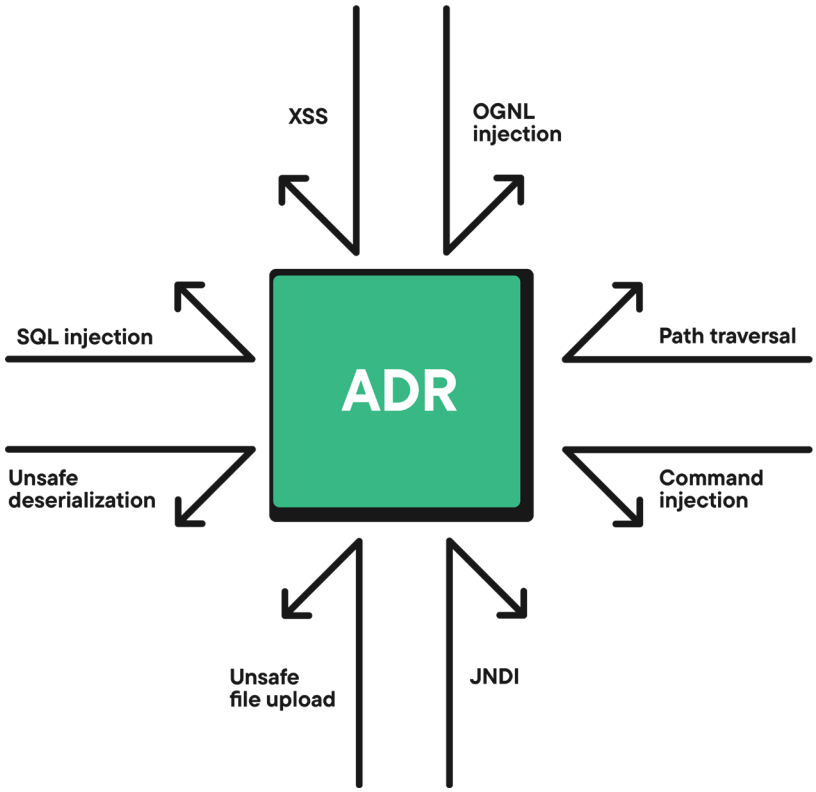
- **The application blindspot:** Traditional tools provide essential perimeter and endpoint visibility but lack deep insight into application runtime behavior. This leaves security teams unable to see attacks specifically targeting application logic or exploiting vulnerabilities from within.
- **Noise vs. context:** Security teams are frequently overwhelmed by high volumes of noisy alerts, particularly from WAFs and scanners. Crucially, these alerts often lack the necessary application context, making it difficult and time-consuming to validate real threats versus false positives.
- **The skills gap:** Finding and retaining personnel with specialized application security expertise is a major hurdle for businesses. This leaves IT/security teams without the deep knowledge needed to effectively interpret complex application alerts or investigate potential exploits.
- **Delayed threat response:** The combination of the blindspot, alert noise, lack of context and skills gap inevitably leads to slower detection and response times for application-layer threats, increasing attacker dwell time and overall risk.
- **Expanding application attack surface:** Rapid development cycles fueled by AI, API sprawl, microservices and cloud adoption constantly expand the potential avenues for attack, stretching already thin security resources.
- **Disproportionate breach impact:** The financial and operational fallout from an application breach can disproportionately harm a growing business's trajectory and customer trust.

The limits of perimeter and endpoint security for application threats

While necessary, the tools commonly monitored by security teams provide an incomplete picture:

- **Web Application Firewalls (WAFs):** Operate at the perimeter, inspecting HTTP/S traffic. They lack insight into internal application logic and struggle with encrypted traffic, custom application flaws and zero days, often generating significant noise that security personnel must sift through.
- **Endpoint Detection and Response (EDR):** Focuses on OS-level processes. These tools cannot see the specific code execution or data flow within the application process where exploits often originate.
- **Vulnerability scanners (e.g., Static/Dynamic Application Security Testing (SAST/DAST)):** Identify potential weaknesses, often pre-production or periodically. Their findings frequently lack runtime context regarding actual exploitability in production, contributing to alert volume without clear prioritization for the security function.

These tools leave security teams guessing when faced with inevitable application incidents, forcing time-consuming manual correlation and often requiring slow, inefficient handoffs to security partners and development teams for investigation.



Contrast ADR: Gaining security insight from within the application

Contrast Application Detection and Response (ADR) provides visibility and control where lean security teams need it most: directly within running applications and APIs. By instrumenting applications in runtime, ADR observes actual code execution and data flow, eliminating the guesswork required with external tools. This integrated approach allows ADR to deliver accurate alerts, precise context for faster triage and response and reliable threat blocking – significantly reducing noise and the need for expert expertise.

Key benefits for security teams include:

Effective application and API protection

- **Comprehensive threat blocking:** Defend against known attacks (like SQLi, RCE), zero days and entire vulnerability classes in real time, providing robust protection as the application landscape grows.
- **Enhance existing security stack:** Feed high-fidelity application context into existing workflows — whether using internal tools like a Security Information and Event Management (SIEM), or partner platforms — for better overall detection.

Empower security teams

- **Actionable intelligence, less noise:** Receive accurate, context-rich alerts based on verified runtime activity, cutting through WAF/scanner noise and enabling security personnel to focus on real threats.
- **Bridge the skills gap:** Empower existing teams with guided runbooks and clear context to confidently handle application alerts and apply compensating controls without deep AppSec expertise.

Accelerate threat response

- **Faster detection and containment:** Eliminate the application blindspot to detect attacks faster and enable rapid containment before damage escalates.
- **Streamline remediation:** Provide external security teams or development teams with precise, actionable details (including code location and exploit context) to remove friction and accelerate permanent fixes.

ADR acts as a critical last line of defense when other tools miss the threat, helping to prevent breaches that could incur devastating regulatory fines, legal costs, and reputational damage from which an SMB may not recover. It's not just better alerts; it's protection against existential threats.

Integrating runtime security into the existing workflow

Contrast Security's platform utilizes threat sensors inside each application. This provides continuous, real-time monitoring, detection and protection purpose-built for the complexities of modern application architectures. Contrast ADR integrates seamlessly with the tools security teams already use — such as SIEMs or IT ticketing systems — ensuring actionable intelligence flows into existing workflows and enhances current security investments.

The path forward: Application Detection and Response for all businesses

For an SMB, operating with an application security blindspot isn't just a risk; it's an invitation for potentially catastrophic consequences. Relying solely on traditional monitoring tools leaves critical applications vulnerable, and the financial and legal fallout of a breach can be insurmountable. Contrast ADR empowers lean security teams — whether internal or outsourced — to overcome resource limitations and the AppSec skills gap. By providing unparalleled runtime visibility, actionable context, and real-time protection from within the application, Contrast ADR acts as essential 'insurance' against these threats. It enables teams to defend their application and API, significantly reduce the risk of business-ending incidents, and focus confidently on innovation and scaling, knowing they have a robust protection where most breaches start.

contrastsecurity.com

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