CONTRAST SECURITY

SOLUTION BRIEF

The Contrast Graph

A digital twin of application-layer security

Real-time application security data model that continuously maps, updates and correlates security insights across applications, APIs and infrastructure.

Protecting business-critical applications is a top priority for any business. However, organizations are frequently managing their application security in isolated tools which offer only fragmented and static views of risk. Their only model is a lengthy list of theoretical problems without the necessary context to understand how these issues truly impact the broader enterprise.

The "no-context problem list" approach often leads to an overwhelming number of false positives, pushing security teams into a reactive posture and hindering effective collaboration between development, security and operations. Furthermore, these traditional tools often lack crucial real-time production context, leaving organizations with significant security blind spots and incomplete coverage. The key to success is moving beyond simply identifying vulnerabilities to understanding which issues are truly exploitable and require immediate attention, enabling efficient prioritization and rapid response to evolving threats.

Unifying application security with the Contrast Graph

Imagine having a real-time, comprehensive security model that could answer any security question about your entire application layer — down to the most detailed technical, architectural and business-level insights. This is the reality of the Contrast Graph. Solving traditional challenges. The real-time, unified security model is created from a wide variety of telemetry directly measured from running code by Contrast's threat sensors. The telemetry automatically creates a single graph-based model that spans development, production, security and business context — enabling operations, development and security teams to detect incidents and issues quickly, accurately understand the real risk and respond quickly.

Revolutionizing application security workflows

- **Deep vulnerability insight for rapid incident response:** Quickly understand the cause and impact of any attack with the enriched data from the Contrast Graph. This includes architectural, threat and business context directly measured from production environments, enabling teams to decide on an efficient and effective response.
- **Confidently manage real vulnerabilities:** Each vulnerability is proven exploitable at runtime, mapped to entry points and data flows, and scored based on real-world exploitability and business impact. The Contrast Graph shows exactly how an attacker could exploit an issue.
- **Context-rich application security training:** The Contrast Graph enables developers to get instant full-context feedback they can trust, rather than waiting for scans only to learn many are false positives. This reduces the number of vulnerabilities being created and cuts the cost of finding and fixing vulnerabilities downstream.

How the Contrast Graph works

The Contrast Graph is a digital twin of application layer security constructed by observing applications and APIs while they run.

Integrated threat sensors

Lightweight sensors installed on application and API servers, automatically observing security behavior. These sensors collect data to build the Contrast Graph, using open telemetry and scalable methods for near-zero performance impact.

Streaming data architecture

Sensor data flows through a modern streaming data architecture where it is analyzed, updated and merged into the Contrast Graph. This highly scalable approach seamlessly supports millions of applications and APIs in real-time.

Sophisticated graph model

Sophisticated graph model allows modeling of complex enterprise architecture, correlation of vulnerabilities and attacks, dynamic contextual risk scoring, and much more. Includes apps, APIs, attack surface, runtime behavior, defenses, vulnerabilities, attacks, connections, infrastructure and ownership.

Dynamic risk scoring

The Contrast Graph automatically calculates risk scores using production context — scores are enriched with asset criticality, exploitability, threat intelligence, business value, and even active attacks — to ensure focus is on what truly matters.

The missing link that provides a holistic view of the application and API ecosystem

While organizations may have visibility into their network, cloud, containers and other infrastructure, the critical activity at the application layer often remains invisible. The Contrast Graph emerges as the missing link, providing understanding across these complex layers. By tagging everything in the Contrast Graph with identifiers, it serves as a bridge that enables correlation between application and infrastructure layers for a truly holistic view of security risks.

The Contrast Graph is the foundation for AI-powered workflows across the Contrast runtime security platform. By maintaining a continuously updated, real-world model of application behavior, the Graph enables advanced capabilities like Contrast AI SmartFix, which generates precise, AI-crafted remediation pull requests complete with test cases. Contrast MCP Server enables agentic workflows to pull data from other tools and gain insight across development, security and operations.

Together, Contrast AI SmartFix and Contrast MCP Server, transforms the Contrast Graph from a data model into an intelligent engine for proactive, scalable security. The future of application security isn't about running more scans; it's about empowering DevSecOps teams with the information they need to work together and efficiently defend their enterprise.

Learn more

contrastsecurity.com

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