

SOLUTION BRIEF

Cyber resilience

Prepare and recover from cyber threats while maintaining business continuity

Quickly detect, block and recover from cyberattacks, minimizing downtime and data loss.

The problem: achieving cyber resilience with a rapidly changing attack surface

Security teams often face challenges in achieving cyber resilience because the attack surface has expanded due to interconnected digital ecosystems. Unlike traditional cybersecurity, which focuses on prevention, cyber resilience acknowledges that breaches are inevitable, but SOC teams often struggle to keep up with vulnerabilities and attacks.

Consider these key statistics:

- 67% of SOC teams cite [emerging threats](#) are the biggest source of pressure
- 68% of security incidents are caused by [known software vulnerabilities](#)
- Cybersecurity now exceeds 20% of the [average IT budget](#)

Despite growing investments, security leaders and their teams often feel like they are in a constant race to catch up with vulnerabilities and exploits.

The Contrast solution

Contrast Security strengthens cyber resilience by embedding security directly into the application layer, providing real-time visibility, intelligent threat detection and seamless integration into existing workflows.

Key capabilities include:

- Real-time application threat prevention:** Real-time blocking halts potential issues enabling proactive risk management and reducing exposure to attacks that compromise business continuity.
- Behavioral threat detection:** Provides actionable intelligence with contextual insights, helping SOC teams quickly understand attack vectors, mitigate risks, and respond effectively to evolving cyber threats.
- Seamless SOC tooling integration:** Seamless integration with your SIEM, XDR and CNAPP to deliver deep application visibility and control.

Keeping detection tools updated, maintaining threat intelligence and training personnel are ongoing challenges. The shift to cloud environments has further increased complexity, making it crucial for security teams to integrate intelligence and enforce security at the application layer.

Why it matters

Cyber resilience is critical for a Chief Information Security Officer (CISO) as it ensures an organization can anticipate, withstand, recover from and adapt to cyber threats. In an era of increasing cyberattacks, regulatory demands and evolving attack vectors, cyber resilience is not just about prevention but also about maintaining business continuity despite security incidents.

Cyber resilience is achieved by the security teams working on the front lines - detecting, responding to and mitigating threats. However, they face challenges such as the need for highly accurate, real-time threat intelligence. Effective cyber resilience requires automation and incident response capabilities to detect and contain attacks swiftly.

Transforming cyber resilience

Contrast strengthens an organization's security posture by reducing risk at the application level. It provides continuous insights into vulnerabilities and active threats, allowing proactive risk management to help CISOs make informed decisions about response strategies. For front line security teams, Contrast delivers measurable security improvements by equipping them with the tools and insights needed to stay ahead of emerging threats. By embedding security directly into applications, Contrast ensures continuous protection, reduces false alarms and enhances the ability to detect and mitigate risks in real time. This approach streamlines security operations, allowing teams to focus on high-priority threats without being overwhelmed by noise.

Proactive protection



Reduce application and business downtime by blocking malicious activity in real time, preventing threats from escalating into breaches or disruptions.

Streamlined SOC operations



Improve threat visibility and prioritization by seamlessly integrating application-layer defenses with existing SOC tools, eliminating silos and enhancing operational efficiency.

Improved incident response efficiency



Reduces Mean Time to Detect and Respond (MTTD/MTTR) by correlating security events across applications, improving threat containment capabilities.

Learn more

Ready to strengthen your organization's cyber resilience? Learn more about how Contrast Security can help protect applications and maintain business continuity against evolving threats.

BLOG

Bringing the application layer into cybersecurity monitoring and response

BLOG

Wake up, CISOs: You need an ADR flashlight to see into critical application blindspots

WHITEPAPER

The Case for Application Detection and Response (ADR)