FOR IMMEDIATE RELEASE

Cyber Attacks at the Application Layer Surge 31%

Contrast Security Application Detection and Response Report details the need for immediate protection of apps and APIs

MENLO PARK, Calif., February 18, 2025 – Contrast Security's latest Application Detection and Response (ADR) Report reveals a sharp rise in attacks bypassing perimeter defenses, underscoring the need for stronger application layer security. In January 2025, Contrast ADR blocked an increasing number of attacks, preventing major breaches.

Contrast Security also reports attackers are increasing in sophistication and are now more easily bypassing perimeter defenses, such as Web Application Firewalls (WAFs). The attackers are also able to craft attacks that evade other defenses, including Endpoint Detection and Response tools.

The research shows that many of the alerts reported by traditional security methods create too much noise for Security Operations Centers, preventing them from focusing on real, impactful attacks. The more sophisticated attackers are leveraging the application layer blind spot and increasingly focusing their attacks there.

"Software runs our lives and the application layer in which it operates has long been under protected. With the advent of AI attacks, criminals can now too easily launch millions of application and API attacks in a short period of time," said Rami Elkhatib, Board Member of Contrast Security and General Partner of Acero Capital. "Organizations need to either augment or shift away from legacy software security tools to more modern technologies like instrumentation for real time visibility, and defenses like Application Detection and Response."

Key Findings:

- **Attacks Evading Defenses Up 31%** – Per application, attacks rose from **45 in December to 59 in January.**
- **Top Threats:** Cross-site scripting (XSS), untrusted deserialization, SQL injection, and method tampering (HTTP verb tampering).
- **Security Noise vs. Real Threats:** Of **500M function calls**, only **59 were true attacks** — emphasizing the need for precision over volume.

For more insights on this topic, join us on February 24 at Rami Elkhatib's keynote presentation: Cybersecurity, the Attackers and the VC Backers, at Web Summit Qatar 2025, 23 – 26 February

Bottom Line:
Attackers launch persistent, automated campaigns on exposed apps. Contrast ADR detects and blocks real exploits in real time.

Supporting links:

Application Detection and Response: https://www.contrastsecurity.com/press/contrast-security-introduces-application-detection-and-response-adr-to-identify-and-block-attacks-and-zero-days-on-applications-in-production

Application Vulnerability Monitoring: https://www.contrastsecurity.com/press-contrast-security-launches-new-capabilities-of-application-detection-and-response-to-catch-vulnerabilities-in-production-before-attack

Media Contact:
Rami Elkhatib
rami@acerovc.com
+1-650-863-1781

Acero Capital (https://www.linkedin.com/company/acero-capital/) is actively pursuing investments in enterprise software including cybersecurity, enterprise AI, next-gen analytics and cloud infrastructure. The unifying themes across our investments are (a) a relentless search for new approaches to large and established markets, (b) management teams with exceptional foresight and resourcefulness and, (c) an emphasis on capital-efficient business models that can turn capital efficiency into competitive advantage.

At Acero Capital, we pride ourselves on recognizing and backing the ‘Unconventional Wisdom’ - the prescience to go against the herd and champion a new approach.