RED VECTOR

CONTEXT+

YOUR SECURITY STACK SEES ALERTS CONTEXT+ TELLS YOU WHICH ONES MATTER.

CONTEXT+ adds contextual intelligence to your existing SIEM, DLP, and IAM platforms, making those Systems significantly smarter. No rip-and-replace. No new agents. Just the context your stack is missing.

The gap in your stack is not detection. It is context. Your SIEM, DLP, and IAM platforms generate thousands of alerts daily, but they lack the organizational awareness needed to determine which activity truly represents risk. Without understanding changes in role, access patterns, environment, or intent, analysts are left to chase noise while the signals of real risk remain hidden. The result is a Detection Paradox: organizations are simultaneously overwhelmed by alerts and blind to the threats that matter most.

WHAT IT DOES

CONTEXT+ answers the question your security stack cannot: Is this alert meaningful for this specific individual or agent? It builds continuous contextual baselines for every entity in your environment, enriching your existing tools with the organizational and human context they are missing. Analysts stop triaging raw alerts and start responding to prioritized, narrative-ready risk signals.

WHY IT'S DIFFERENT

- **Contextual Signal Fusion**. Correlates HR lifecycle events, identity changes, access patterns, and nontechnical signals into a unified contextual risk baseline for every entity.
- **Continuous Risk Evaluation**. Delivers real-time contextual risk signals directly to your SIEM, DLP, and IAM platforms as they operate.
- **API-native Integration.** Connects to your existing stack in days, not months.
- **No Endpoint Agents.** Leverages telemetry your tools already generate. Nothing new to deploy or manage.
- **Human and AI Agent Signals.** Supports any entity type requiring contextual evaluation, including autonomous AI agents operating across your environment.
- **Outcome-driven Implementation.** A structured Bootcamp engagement delivers validated risk findings and a prioritized deployment roadmap in 30 days.

WHO IS THIS FOR

- **CISOs** seeking better insider risk visibility across their existing stack
- **Insider Risk Programs** struggling with signal overload and analyst fatigue
- **DLP Leaders** trying to separate real incidents from noise
- **Security Teams** investigating anomalies without adequate organizational context

PROOF POINT

"CONTEXT+ was easy to implement because it worked as a non-disruptive overlay on top of our existing security stack. We didn't have to install new agents or replace any tools. We quickly had contextual baselines feeding across our security stack, and our false positives dropped by more than 70%. Just as important, Security, HR, and Legal finally had a shared way to understand and discuss risk. CONTEXT+ gave us a common, explainable risk signal that all three teams could trust. As we've grown, the platform has scaled with us as we add new signals, models, and integrations."

National Security Research Laboratory

False Positive Reduction	Returned to Active Defense
60-80%	$57K Per Analyst Per Year
Reduction in Insider Risk Incidents	**Existing Stack Value Unlocked**
50%	$500K

See CONTEXT+ Operating in Your Environment

The Red Vector Bootcamp applies CONTEXT+ to your operational environment in 30 days. Your team receives a validated risk exposure report, a data-backed business case, and a prioritized mission action plan delivered directly to your CISO.

BEGIN YOUR ENGAGEMENT
redvector.ai
info@redvector.ai

info@redvector.ai | redvector.ai

RED VECTOR