RED VECTOR

DATA SHEET

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. It answers the question your stack cannot: **is this alert meaningful for this specific individual or agent?** No rip-and-replace. No new agents. Just the context your stack is missing.

THREE FAILURE MODES IN YOUR STACK

THE NOISE TRAP

Thousands of alerts, most meaningless, burying real risk in noise.

THE BLINDNESS TRAP

Authorized actions, gradual drift, and autonomous entities operating undetected.

THE SEAM FAILURE

Risk signals span systems but no tool sees across them.

The gap in your stack is not detection. **It is context.**

FEATURES

Contextual Baselines

Continuous contextual baselines for every entity in your environment.

Alert Enrichment

Adds the organizational and human context your existing tools are missing.

Prioritized Risk Signals

Analysts respond to narrative-ready signals, not raw alerts.

Real-time Delivery

Contextual risk signals feed your SIEM, DLP, and IAM as they operate.

Human + AI Coverage

Supports any entity type, including autonomous AI agents.

Shared Risk Language

One explainable signal Security, HR, and Legal can all trust.

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.
- **API-native Integration.** Connects to your existing stack in days, not months.
- **Human and AI Agent Signals.** Contextual evaluation for any entity type, including autonomous AI agents across your environment.
- **Continuous Risk Evaluation.** Real-time contextual risk signals delivered directly to your SIEM, DLP, and IAM platforms as they operate.
- **No Endpoint Agents.** Leverages telemetry your tools already generate. Nothing new to deploy or manage.
- **Outcome-driven Implementation.** A structured Bootcamp engagement delivers validated risk findings and a prioritized deployment roadmap in 30 days.

PROOF POINT

"CONTEXT+ worked as a non-disruptive overlay on our existing stack: no new agents, no replaced tools. False positives dropped by more than 70%."

National Security Research Laboratory

BY THE NUMBERS

70% — **False Positive Reduction**

$57K — **Returned to Active Defense** PER ANALYST PER YEAR

50% — **Reduction in Insider Risk Incidents**

$500K — **Existing Stack Value Unlocked**

WHO IS THIS FOR

- **CISOs** seeking better insider risk visibility across their existing stack
- **Insider Risk Programs**: signal overload and analyst fatigue
- **DLP Leaders**: separating real incidents from noise
- **Security Teams**: anomalies without organizational context

BEGIN YOUR ENGAGEMENT

The Red Vector Bootcamp applies CONTEXT+ in 30 days: validated risk report, business case, and action plan for your CISO.

Start with a Bootcamp

redvector.ai · info@redvector.ai