Stream.Security

Security Born in the Cloud. Raised by SecOps.

The industry's only real-time detection and response solution purpose-built for the cloud

Cloud-native environments are continuously evolving, with shifting assets, configurations, and identities constantly redefining the threat landscape. Adversaries exploit this dynamic nature using cloud-native TTPs—modifying configurations, escalating privileges, and expanding their foothold—all while evading traditional security tools.

Where Existing Solutions Fall Short

Traditional security tools rely on raw cloud logs and fail to grasp the complexity of cloud-native attacks. They cannot assess the impact of events or connect anomalies to cloud-native TTPs, resulting in critical blind spots. This leaves security teams struggling to address cloud threats effectively and meet strict MTTR requirements.

Pinpoint threats by understanding the past, present, and future of your cloud infrastructure.

Stream brings real-time cloud context to SecOps teams, complementing SIEM, SOAR, and XDR solutions to help teams proactively prepare, detect, investigate, and respond to cloud threats.
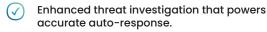
With Stream, your security team will benefit from:

✓ Real-time cloud visibility that reduces MTTR to under 5 minutes.

✓ Significant cost savings in time wasted on false positives.

✓ Enhanced threat investigation that powers accurate auto-response.

✓ Minimized downtime and cost of damage in incident response.

Cloud Detection and Response (CDR)

CDR models cloud activities to empower security operations teams to prepare, detect, investigate, and respond to threats across the complex cloud attack surface.

Goodbye Raw Logs; Hello *CloudTwin*®

Stream Security's CloudTwin technology models configurations, networks, identities, and behaviors in real time, delivering actionable cloud context to accelerate response.

How does it work?

Prepare
Leverage real-time attack surface intelligence to prioritize alerts by critical assets, their attack paths, and associated vulnerabilities.

Detect
Precisely identify critical threats by correlating activities with expected behavior, TTPs, and IOCs while minimizing false positives through deep cloud context.

Investigate
Automate triage and investigation by instantly revealing the full attack storyline, correlating TTPs, IOCs, and cloud-native operations.

Respond
Respond with surgical accuracy by pinpointing the least intrusive action to break the kill chain. Choose to automate critical responses, implement them manually, or integrate seamlessly with your SOAR.

Hear from our customers:

shield.

75%
Reduction in investigation time

RingCentral

77%
Reduction in false positives

Hi Bob

4x
Faster response to threats

PayU GPO · CATO NETWORKS · TiVo · RingCentral · SONY · shield. · Bancolombia · kaltura

Book a meeting

Stream.Security was named a 2024 Gartner Cool Vendor for the moderm SOC.
Learn more >

Stream.Security

aws PARTNER Security Software Competency · SOC 2 TYPE 2 · CSA cloud security alliance® · 2023 CYBERSECURITY · WINNER CYBER SECURITY EXCELLENCE AWARDS · GLOBAL INFOSEC AWARDS WINNERS 2024 · 2024 LinkedIn TOP STARTUPS Israel · Gartner COOL VENDOR 2024