Confluera XDR FOR CLOUD INFRASTRUCTURE

confluera

Today, every cyber security vendor "correlates" all kinds of data to hopefully give defenders the upper hand. But correlation leads to a number of, at best, misleading and, at worst, wrong conclusions. Faced with a growing attack surface and ever-improving hacker methods, correlation can't keep up. Today, alert fatigue, false positives and false negatives remain the norm.

Legacy tools provide SOC teams with a series of disorganized snapshots instead of a concise, streaming narrative. Attacks today are a sequence of many, seemingly unrelated, steps along the cyber kill chain. Individual detections are probabilistic weak signals--often proving unactionable. Security teams suffer from digital exhaust as thousands of alerts are sent to their SIEM dashboard. Understaffed, security teams are unable to triage each alert, succumbing to the belief that most of the alerts received are actually false-positives. Unless attack signals are deterministically combined as a sequence, today's sophisticated attacks cannot be detected, let alone blocked. Instead, vendors relying solely on correlation force SOCs to miss attacks in a sea of alerts. Despite this reality, the entire cyber security industry echoes the virtues of correlation.

Except Confluera.

"With the number of data breaches in the headlines on a daily basis, and customer-sensitive data appearing on the dark web, we at CohnReznick are focused on state-of-the-art technologies to help us detect and thwart ongoing attacks. Confluera XDR allows us to very easily deploy a unique solution that operationalizes our critical infrastructure security."

Richard Cannici

Head of Infrastructure & Security

"As a global company, we are always concerned about protecting our core applications and data against ever-increasing cyberattacks. None of the solutions in the market could detect breaches in real-time, and more importantly, remove them surgically. With Confluera XDR, we are able to accurately detect and respond to breaches in real-time without impacting our business."

Sean Henry

Sr. MIS Manager

HOW DOES CONFLUERA WORK?

Confluera XDR protects core infrastructure running critical applications as data center attack surfaces grow and become more ephemeral. How?

Gather Telemetry

Confluera XDR gathers telemetry through enrichment and contextual mapping of security results from sources including firewalls, multi cloud, file integrity monitoring, HIDs and more. In addition, Confluera sensors deployed on the guest operating system of enterprise assets capture granular telemetry that describes causal relationships of activity sequences between system events within and across hosts. Sensors are also capable of invoking response steps initiated by the central hub to respond to the attacks in progress.

Stitch Everything

Like a DVR for your data center, Confluera XDR autonomously records ALL events, stitching together non-security and security events through causal attack sequencing versus correlational guesswork. Like a time-lapse movie, Confluera shows highlights in detail using the full catalog of events--not snippets--to understand what happened, when and how so security can track suspicious activity. Unlike other technologies that look back to analyze events, Confluera distils attack information in real time. Confluera tags and traces attack indicators to autonomously stitch related events together across the entire infrastructure to detect attacks with virtually no false positives.

PLATFORM SUPPORT

LINUX

- RHEL 7 & 8
- CentOS 7
- Amazon Linux 1 & 2
- Ubuntu 16.04 & 18.04 LTS

WINDOWS

- Win Server 2019
- Win Server 2016
- Win Server 2012

CUSTOMERS USE CONFLUERA FOR:

- SOC automation
- Storyboarding
- Enable digital transformation
- Incident response automation
- Threat hunting
- Privileged Activity Monitoring and Tracking

Build Attack Narratives

Confluera XDR autonomously analyzes attacks by extracting execution-based threat signals, Confluera graphically streams attack events, enabling SOC teams to convert data into automated attack visibility for threat hunting and situational awareness—not a manual jigsaw puzzle. While recording events and sequences, Confluera applies dynamic risk scores against attack data in detail and at scale. The detection engine leverages:

- **MITRE-based detection engine:** Behavioral detections on ALL PHASES of kill chain using the MITRE ATT&CK framework based on Host Process, File and Network activities. Confluera records each and every session across all users—good or bad—to generate rules based on the MITRE framework to identify malicious patterns.
- **AI/ML based detection:** Machine learning based anomaly detection complements Confluera's causality-based approach to profile process, network, file and user behavior. This helps identify anomalies, zero days and behavioral deviations.

Continuous Attack Interception

While recording events and sequences, Confluera XDR applies dynamic risk scores against attack data in detail and at scale. Confluera XDR then deterministically identifies complex, multi-stage attacks to block attackers at every step with virtually no false positives.

THE CONFLUERA IMPACT

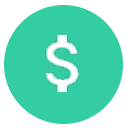
Confluera introduces the industry's first XDR platform delivering real-time visibility and autonomous response.

Improved productivity

Kiss alerts goodbye. Force multiply any-sized SOC with precision and automation driven by comprehensive attack narratives.

Leave no stone unturned

Eliminate blind spots to see more attacks across your full spectrum of attack surfaces.



Lower total cost of ownership

Shift from tactical alert management to strategic risk management while consolidating security spend.

About Confluera

Confluera delivers autonomous infrastructure-wide cyber kill chain tracking and response by leveraging 'Continuous Attack GraphTM' to deterministically stop and remediate cyberthreats in real-time.

Request a Demo

contact@confluera.com

1-833-CONFLUERA

195 Page Mill Rd
Palo Alto, CA 94306

www.confluera.com