Confluera XDR FOR CLOUD WORKLOADS

Modern cyber attacks result from many, seemingly unrelated, steps attackers execute along the cyber kill chain. While EDRs have evolved to detect and respond to cyber attacks on user endpoints, the current practice of bolting on such user endpoint solutions on server workloads puts the enterprise data and applications at risk—leaving your mission critical hybrid cloud susceptible to attack. Even basic investigations with endpoint tools require analysts to examine heaps of disjointed alerts that eventually end up in SIEMs. What investigators really need is a concise and complete narrative across all the steps the attacker took during a multi-stage attack campaign.

Confluera XDR delivers a purpose-built cloud workload detection and response solution with the unique ability to deterministically track threats progressing across multiple workloads, and holistically integrate security signals to provide the complete context, in real-time. With Confluera, security teams can intercept threats as they are happening instead of investigating alerts after the fact.

HOW DOES CONFLUERA XDR WORK?

The Confluera XDR protects Cloud Workloads running critical applications as your data center attack surfaces grow and the workloads become more ephemeral.

USE CASES

- Workload monitoring, detection, and response
- Automated incident investigation
- Response orchestration and automation
- Context-enabled threat hunting
- Privileged activity monitoring
- Operational Insights

CONFLUERA IMPACT

- Protect workloads from known and unknown attacks
- Visualize the cyber kill chain in real-time
- Respond to attacks before they turn into breaches
- Reduce threat hunting time from hours to minutes
- Force multiply any-sized SOC team

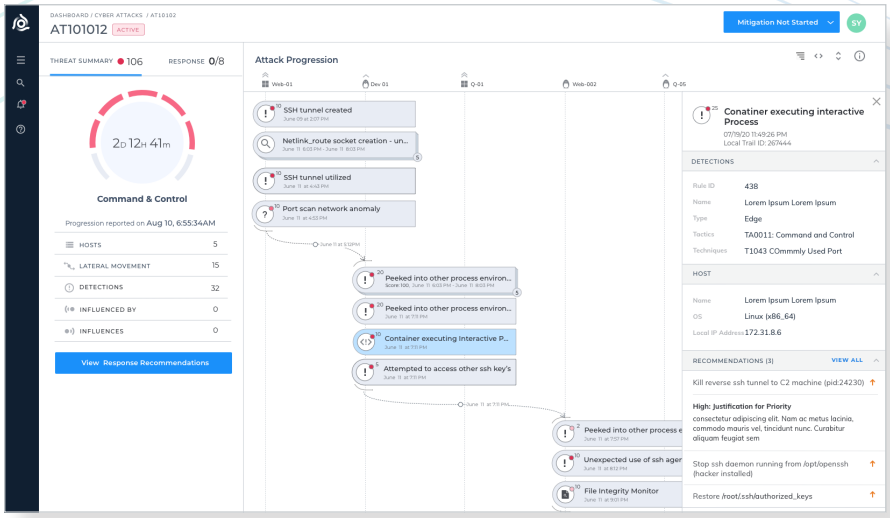
> "With the number of data breaches in the headlines on a daily basis, and customer-sensitive data appearing on the dark web, we at CohnReznick are focused on state-of-the-art technologies to help us detect and thwart ongoing attacks. Confluera XDR allows us to very easily deploy a unique solution that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

Infrastructure-wide Event Sequencing

Confluera sensors capture granular telemetry from enterprise workload and create causal relationships of events within a system and across hosts. The Confluera IQ Hub (available in cloud or on-prem) autonomously stitches all events across the infrastructure. Unlike other technologies that look back to analyze events, the event stitching enables Confluera to look at the telemetry as a set of activities (benign or suspicious), progressing through the environment. This is what allows security teams to trace and track the execution steps of an attack campaign, including lateral movements across hosts.

Behavioral and Anomaly Detections

Confluera's threat detection engine, purpose-built for workloads, continuously analyzes the infrastructure-wide event graphs to detect indicators of compromise on workloads based on the MITRE ATT&CK framework. The engine relies on a set of rule-based behavioral detection techniques, and ML-based detection capabilities for identifying anomalies related to process executions, file/network operations, and user actions. As the detection engine identifies malicious behaviors, Confluera automatically maps the event sequences, surfacing the all preceding steps of an ongoing attack campaign.



Security Ecosystem Integration

Confluera takes in security results from a multitude of 3rd party security tools and threat intelligence feeds to contextually stitch them into the infrastructure-wide activity progressions. As a result, even weak signals, which would otherwise be overlooked, can now be analyzed in context of the overall attack narrative. Confluera's integrations span industry leading products across EDR, Firewall, Vulnerability Managers, Public Cloud Logs, etc.

Risk Scoring and Threat Ranking

While detecting malicious behaviors, the Confluera IQ Hub dynamically applies a predefined risk score to all individual detections (native or third-party), which are automatically aggregated over the activity sequence, combining the individual risks into a threat score for the entire sequence. This overall threat score, along with other heuristics such as the use of specific tactics and techniques, is then used to rank and prioritize the threats automatically, so that security teams can mitigate them in the order of their severity.

Attack Narratives and Threat Interception

As the Confluera XDR autonomously builds the attack narratives, it also identifies the series of actions that are necessary to thwart the campaign's progress. The Confluera sensors are capable of invoking such response actions initiated at the portal via IQ Hub. The response actions are highly surgical in the sense that they are typically executed at process, file, network levels as opposed to complete isolation of a compromised host.

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

Request a Demo contact@confluera.com / 1-833-CONFLUERA

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

INTEGRATIONS

- Threat Intel Feeds
- Firewalls
- EDRs
- Public Cloud Services
- Open Source Agents
- File Integrity Monitors
- Vulnerability Managers

"As a global company, we are always concerned about protecting our core applications and data against ever-increasing cyber attacks. 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