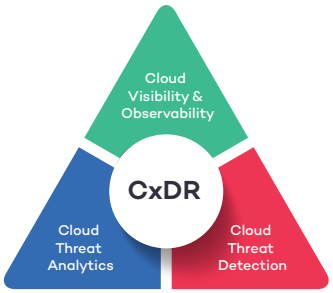
Confluera eXtended Detection and Response (CxDR)

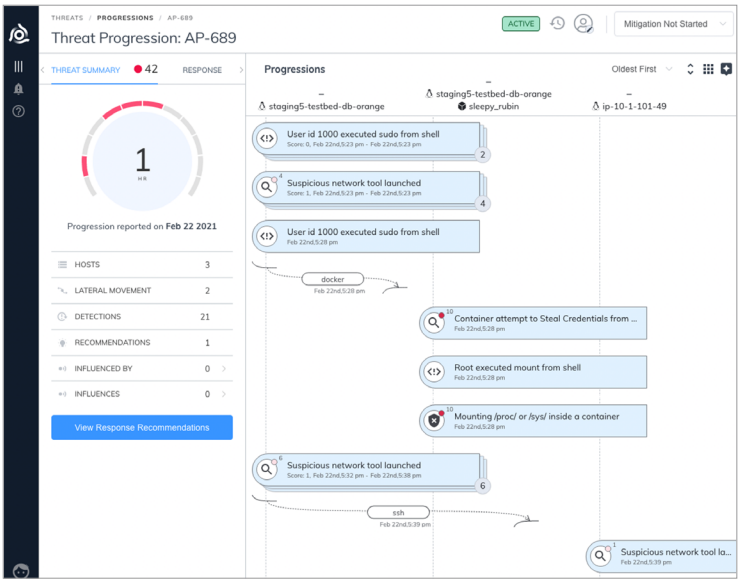
Despite the recent innovations in various detection and response capabilities, SOC and IT analysts continue to play catchup. With the time to detect and contain a breach averaging 280 days, security analysts are facing an uphill battle against attackers who have spent months exploring, navigating, and compromising the organization's network and assets from the inside. While new solutions have resulted in more security signals, the accompanying increase in false positives have limited any tangible ROIs. In fact, modern attacks take advantage of the resource-constrained security team by masquerading as benign activities and employing special tactics in an attempt to slip under the radar. The security tasks get even more challenging with the accelerated adoption of cloud services. The very nature of the cloud limits analyst visibility of the cloud inner workings as well as malicious activities. These challenges all amount to a need for a new category of solutions to address the challenges of modern cyber threats.



Confluera CxDR solution brings together the best security capabilities from the otherwise silo-ed category of solutions; threat detection, threat analytics, and cloud security. The layered solution includes Confluera's proven signal analytics from multiple sources such as APIs, third party intelligence, and Confluera's patented real-time threat storyboarding capability. Confluera CxDR reduces the industry average time to detect and mitigate advanced attacks from months down to hours while also reducing the need for analysts with highly specialized cybersecurity expertise.

Reduction in Detection and Response Time

Powered by Confluera's patented Continuous Attack Graph technology, Real-time Threat Storyboarding enables security teams to respond to modern cyberattacks in real-time as the attack is occurring. The storyboard displays the entire attack progression including how it started and what is currently happening with the level of accuracy and clarity that had only been available from a post-breach manual forensics exercise. Organizations now have the forewarning to stop the attack in-progress before it can result in a breach.



> *"With rapid detection and response built on cloud-native architecture, Confluera gives us confidence that we can mitigate cyberattacks before they can do any harm."*

Cloud-native Threat Protection

Confluera CxDR represents the next-generation detection and response solution with game changing continuous and real-time attack visibility designed specifically to address the threats and challenges in the cloud. Modern attacks on cloud native environments exploit attack surfaces that are unique to the cloud such as server misconfigurations, control plane vulnerabilities, container registry dependencies, API privilege escalations, etc. Confluera combines native signals gathered from Confluera workload sensors, Cloud Infrastructure signals and other Cloud security tools to create a real-time activity graph of each workload's activities, the lateral movements between them and the riskiness of each activity. This deep visibility allows accurate attack storyboarding of advanced cloud attacks and precise remediation actions, even when workloads are ephemeral and are being spun up or down at Cloud scale.

Lower False Positives

Today, SOC analysts are compelled to investigate each and every alert, many of which are false positives. The lack of context or 'big picture' results in inconclusive investigations with malicious activities often overlooked. And given the sheer number of alerts generated, it is not surprising that 44% of alerts are often completely ignored. Confluera CxDR stitches together the entire cyberattack sequence of events in real-time. The resulting alerts provide details at the attack progression level illustrating the sequence of steps that makes up the attack since the very beginning of the attack. Tailoring the investigation away from individual alert-level to attack progression-level greatly reduces the 'noise' and increases the capacity and efficiency of the security team.

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

INTEGRATIONS

- Public Cloud Logs
- Threat Intel Feeds
- CWPPs
- Shift Left tools
- Firewalls
- EDRs
- SIEMs
- SOARs
- Messaging and Ticketing
- Vulnerability Managers

PLATFORM SUPPORT

LINUX

- RHEL 7 & 8
- CentOS 6, 7 & 8
- Amazon Linux 1 & 2
- Ubuntu 16,18 & 20 LTS
- Oracle Linux 7 & 8

WINDOWS

- Win Server 2019
- Win Server 2016
- Win Server 2012 R2

Confluera CxDR Features and Capabilities

Workload Threat Detection

Protect server workloads and unique attack surface with comprehensive coverage across all MITRE ATT&CK tactics, including reconnaissance,discovery, and lateral movement. Confluera CxDR continuously gathers OS, network, and application events and applies a combination of behavioral detections and ML-powered anomaly detections to provide superior protection.

Run-time Container Security

Protect container workloads including container escapes, unsecured credentials and lateral movements between containers. Confluera CxDR stitches the full context of the container, host, network activities and detections into real-time storyboards, enabling rapid yet comprehensive analysis.

Multi-Source Threat Integration

Confluera CxDR integrates detections and telemetry from threat intelligence feeds and other security tools into its threat storyboards, enabling high confidence threat detection and speeding up investigations.

Incident Response Automation

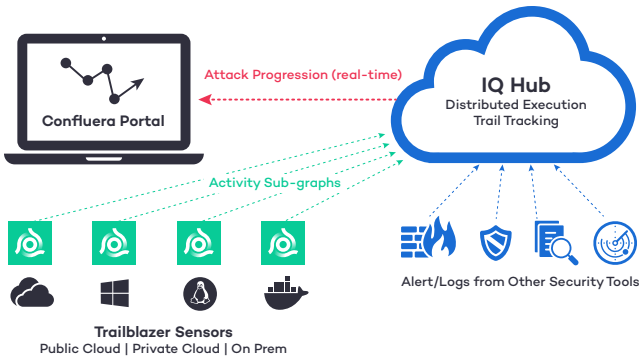
Take actions before the attack results in a breach. Confluera CxDR threat response allows you to mitigate attack progressions in their tracks and clean up all live entities, ingress, and egress points to prevent future attacks. Automatically generates remediation recommendations based on the hosts, applications, processes, users, and network connections greatly simplifies attack response.

Threat Hunting

Confluera CxDR assesses the full impact of the attack progression in context with other events. Security analysts only need to point to a thread to retrieve and unravel the details of the attack. Confluera's petabyte-scale OLAP platform optimized for real-time hunting provides all relevant workload events for investigation within seconds.

Observability and Security Insights

Confluera CxDR distills rich event telemetry into actionable insights and security KPIs that span a wide range of use cases, including runtime executables, file activities, user behavior, lateral movements, privileged activity, north-south network activity and manipulation of mission-critical assets. Confluera's workload-centric UEBA baselines user and application activity, automatically identifying compromised accounts or exploited applications.



Getting started is easy. Activate your account on the Confluera SaaS platform and deploy sensors on workloads

About Confluera Confluera is the leading provider of next-generation Cloud eXtended Detection and Response (CxDR) solutions. Recognized by Forbes as one of the Top 20 Cybersecurity Startups to Watch in 2021, Confluera's storyboard technology automates cyber attack analysis making security teams more efficient. The solution has unprecedented visibility of attacks in the cloud and modern application architectures, reveals threats in real-time, and will shut down advanced multistage attacks. To learn more about Confluera's award-winning solution, visit www.confluera.com.