confluera Industry’s first Autonomous Detection and Response Platform

UNDERSTANDING

The Current State of Security

In spite of aggregate spending exceeding $33 billion on network & infrastructure security, 77% enterprises are anticipating a critical infrastructure breach in near future.

85%+ breaches are a compromise of server enterprise infrastructure, since attackers are after the most critical data assets.

Sophisticated Attacks

Prevailing security solutions fail to address sophisticated attacks that use stealthy techniques to navigate around the infrastructure.

Disjointed Signals

Disparate cybersecurity point solutions generate contextually disconnected signals which do not reflect the attacker’s real intent.

Alert Deluge

Over 30% of security alerts are ignored due to fatigue while the remaining 70% lack actionable intelligence.

Big Hammer Responses

Containment first response strategies not only perturbs business continuity but also hinders actual remediation.

Autonomous Detection & Response

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.

34
DAYS
IQ HUB
ANTIVIRUS
FIREWALL
FILE INTEGRITY MONITOR
VULNERABILITY
AMAZON AWS
GOOGLE CLOUD
MICROSOFT AZURE
PACKAGES
WINDOWS
LINUX

Track Movement

The Confluera platform tracks all events within critical enterprise infrastructure to build real-time activity trails.

Rank Intent

Security signals from multiple sources are contextually fused with activity trails to rank malicious intent.

Eradicate Threat

Surgical responses are deployed automatically across affected entities to stop attack progression.

CONFLUERA

Benefits

Risk Reduction

Automatically tracks and stops modern cybersecurity attacks.

Cost Elimination

Eliminates SecOps productivity loss due to manual triaging.

Spend Leverage

Enhances the value of existing security investments by delivering integrative intelligence.

PLATFORM CAPABILITIES

- Online contextual graph processing vs. offline batch log analysis
- Causal attack sequencing vs. correlational guesswork
- Behavioral detection of MITRE ATT&CK tactics and techniques vs. malware signatures
- Infrastructure wide contextual attack understanding vs. siloed signals
- Graph contextualization of security alerts from other tools vs. noisy alerts
- Automated intent ranking vs. manual scoping of threats
- Autonomous surgical remediation vs. seldge hammer response

> "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 that can help us detect and thwart ongoing attacks. Confluera allows us to very easily deploy a unique solution that operationalizes our critical infrastructure security."

CohnReznick
ADVISORY · ASSURANCE · TAX

Richard Cannici *Head of Infrastructure and 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, we are able to accurately detect and respond to breaches in real-time without impacting our business."

SHOWA
AMERICAN SHOWA INC.

Sean Henry *Sr. MIS Manager*

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

About Confluera

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

Request a Demo

contact@confluera.com
+1 650-485-2826
+1 833-CONFLUERA

Confluera, Inc.
195 Page Mill Rd
Palo Alto, CA 94306

www.confluera.com