Cortex Cloud Runtime Security

Stop Sophisticated Cloud Attacks in Real Time

Prevent threats from compromising your cloud environment with containment actions that stop malicious processes, workload attacks, web-based exploits, and API abuse. Cortex® Cloud Runtime Security extends industry-best cloud runtime protection with enterprise-wide visibility and response in a single source of truth for full context and workflow sharing across cloud security and the SOC. Transform how you protect your cloud ecosystem and ensure business continuity in an increasingly dynamic threat landscape.

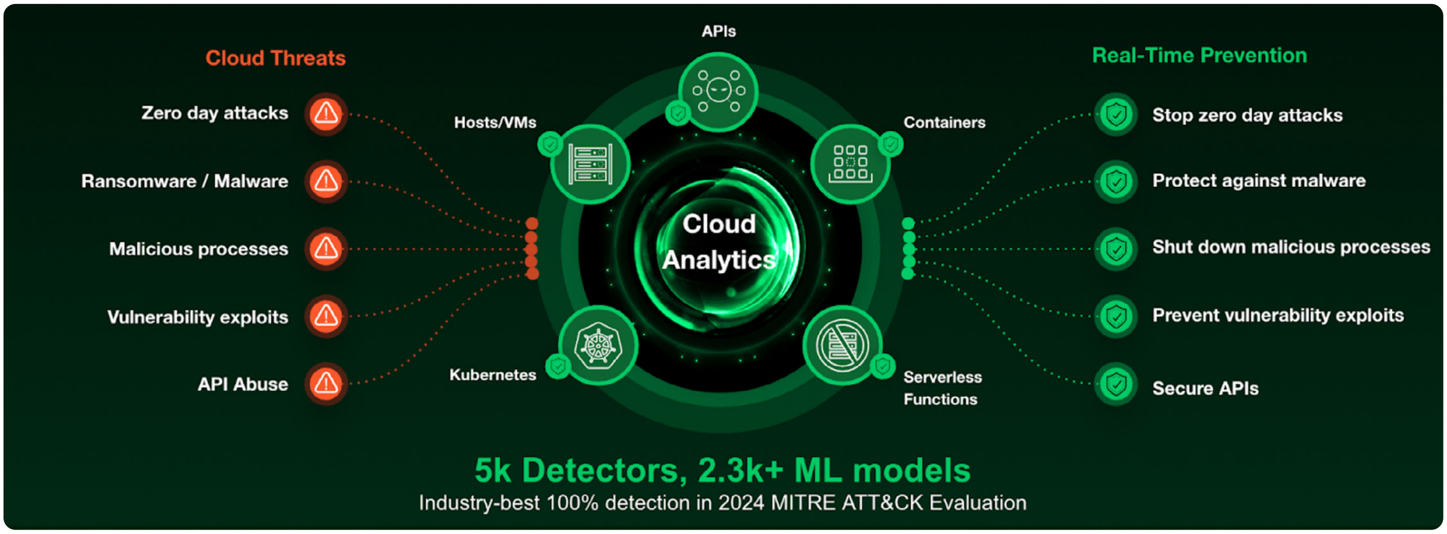


Figure 1: Cortex Cloud Runtime Security provides real-time protection against myriad threats

Complex, Rapidly Changing Threats Stretch Cloud Security Teams

Cloud security now spans infrastructure, identities, custom and open-source code, and vast amounts of cloud-generated data. The rapid adoption of AI-driven services has further expanded the attack surface, while decentralized access to cloud resources enables developers to deploy at unprecedented speed—often bypassing traditional security controls. These shifts fuel innovation but create security gaps that attackers exploit.

With over 750 million cloud-native applications supported by 38 million developers, attacks on cloud environments have surged, increasing by 66% in the past year.[1] Security exposures in the cloud now account for 80% of all risks,[2] and nearly half of them shift monthly,[3] making defense a moving target.

As attacks grow more frequent and architectures, more dynamic, security teams need a centralized solution to protect, detect, and respond to threats in real time, with unmatched visibility and protection.

Cortex Cloud Runtime Security

Stop cloud attacks in real time, before they escalate into breaches, with industry-leading runtime protection that includes:

Runtime Defense

Protect cloud environments at scale with both predictive and threat-driven active security. Cortex Cloud leverages advanced machine learning models to detect and block attacks on running workloads, minimizing risk without disrupting performance.

Host (VM) Security

Secure virtual machines across public and private cloud environments with real-time threat prevention, automated policy enforcement, and deep visibility into workload activity. Cortex Cloud protects VMs against malware, unauthorized access, and advanced exploitation techniques.

[1] *Unit 42 Incident Response Report*, Palo Alto Networks, February 20, 2024.
[2] *Unit 42 Attack Surface Threat Report*, Palo Alto Networks, September 14, 2023.
[3] *Incident Response 2024 Report*, Palo Alto Networks, February 20, 2024.

Container Security

Defend Kubernetes and containerized applications with full-lifecycle protection. Cortex Cloud continuously scans images and applies runtime defense to detect anomalous behavior, securing both managed and unmanaged environments.

Serverless Security

Secure serverless workloads by identifying misconfigurations, detecting code vulnerabilities, and preventing malicious activity in ephemeral environments. Cortex Cloud enables security teams to apply consistent controls without slowing down development.

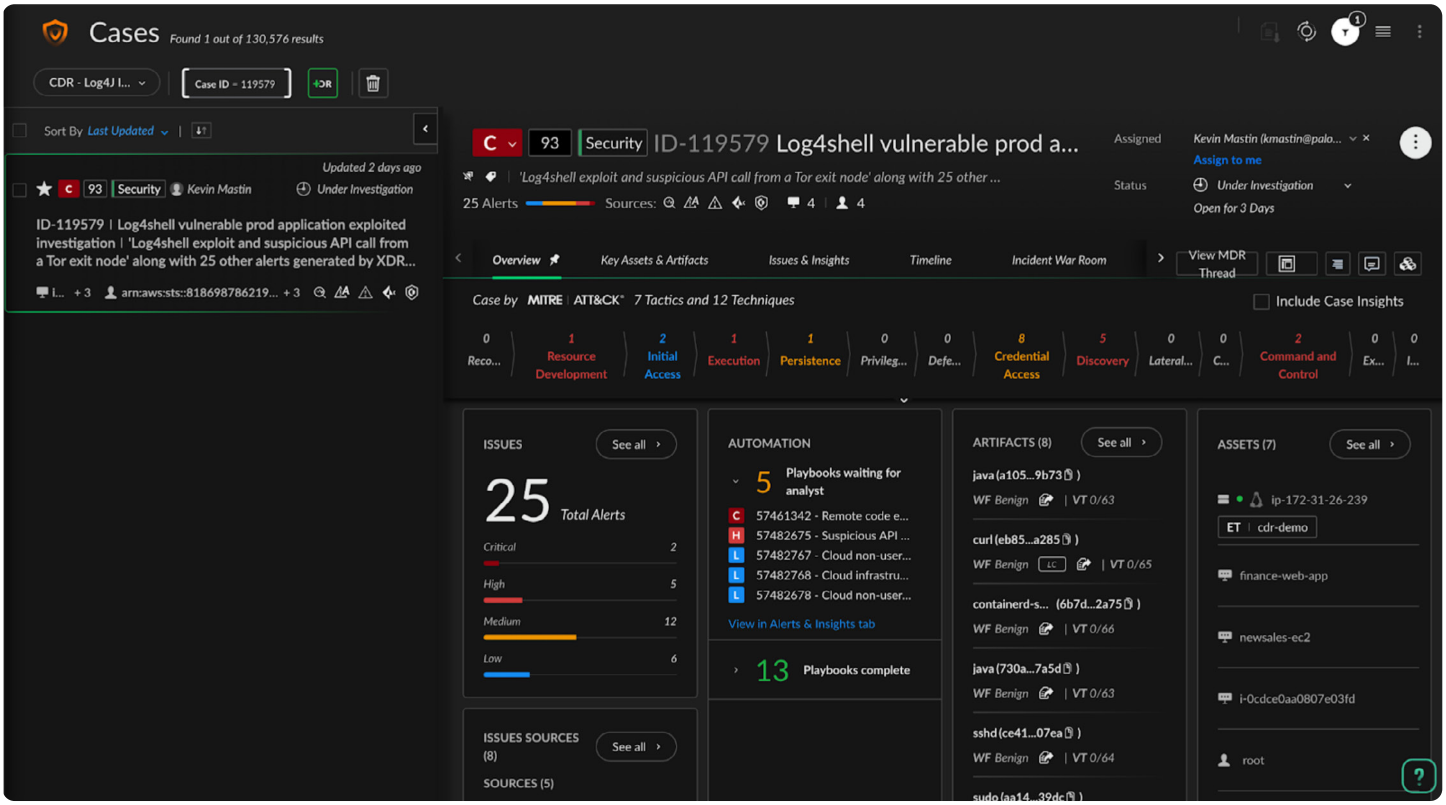
Web Application and API Security (WAAS)

Protect web applications and APIs against sophisticated attacks, including SQL injection, cross-site scripting, and API abuse. Cortex Cloud delivers adaptive security tailored to ensure microservices and APIs remain resilient against emerging threats.

Cloud Detection and Response (CDR)

Detect, investigate, and respond to cloud-native threats in real time with deep visibility into workloads, identities, and network activity. Cortex CDR bridges cloud security and SecOps, integrating runtime telemetry, cloud control plane insights, and AI-driven analytics to detect threats with unmatched accuracy.

Automated correlation turns fragmented alerts into high-fidelity incidents, accelerating investigations and reducing response time. With over 1,000 prebuilt playbooks and automated remediation, security teams can contain threats at their source—before they escalate.



Cases Found 1 out of 130,576 results

CDR - Log4J I... | Case ID = 119579

Sort By Last Updated

Updated 2 days ago

C 93 Security Kevin Mastin Under Investigation

ID-119579 | Log4shell vulnerable prod application exploited investigation | 'Log4shell exploit and suspicious API call from a Tor exit node' along with 25 other alerts generated by XDR...

arn:aws:sts::818698786219... +3

C 93 Security ID-119579 Log4shell vulnerable prod a...

'Log4shell exploit and suspicious API call from a Tor exit node' along with 25 other ...

25 Alerts Sources: 4 4

Assigned: Kevin Mastin (kmastin@palo...

Assign to me

Status: Under Investigation

Open for 3 Days

Case by MITRE ATT&CK® 7 Tactics and 12 Techniques

☐ Include Case Insights

0	1	2	1	1	0	0	8	5	0	0	2	0	0
Reco...	Resource Development	Initial Access	Execution	Persistence	Privileg...	Defe...	Credential Access	Discovery	Lateral...	C...	Command and Control	Ex...	I...

ISSUES

25 Total Alerts

Critical	2
High	5
Medium	12
Low	6

AUTOMATION

5 Playbooks waiting for analyst

- C 57461342 - Remote code e...
- H 57482675 - Suspicious API ...
- L 57482767 - Cloud non-user...
- L 57482768 - Cloud infrastru...
- L 57482678 - Cloud non-user...

View in Alerts & Insights tab

13 Playbooks complete

ARTIFACTS (8)

java (a105...9b73)	WF Benign | VT 0/63
curl (eb85...a285)	WF Benign | VT 0/65
containerd-s... (6b7d...2a75)	WF Benign | VT 0/66
java (730a...7a5d)	WF Benign | VT 0/63
sshd (ce41...07ea)	WF Benign | VT 0/64
sudo (aa14...39dc)	

ASSETS (7)

- ip-172-31-26-239 ET cdr-demo
- finance-web-app
- newsales-ec2
- i-0cdce0aa0807e03fd
- root

ISSUES SOURCES (8)

SOURCES (5)

Figure 2: Cortex Cloud uses AI and analytics to automatically aggregate disparate alerts into highly prioritized cases

Stay Ahead of Cloud Attacks with Proactive Runtime Security

Cloud attacks move fast, targeting vulnerabilities across workloads, containers, and APIs. Security teams need more than visibility—they need the ability to detect, block, and respond.

Cortex Cloud Runtime Security delivers proactive defense with AI-driven runtime protection, real-time threat detection, and automated response. Unifying cloud security with SOC operations, Cortex Cloud enables teams to stay ahead of attackers, reduce risk, and secure cloud environments at scale.

See how Cortex Cloud Runtime Security transforms cloud protection.

SEE CORTEX CLOUD IN ACTION

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com