Cloud Security Threats Every Organization Must Know

Real-Time Protection Is Crucial to Stopping Breaches

750M+
cloud-native applications expected by 2025[1]

80%
of exposures found in cloud environments[2]

66%
increase in cloud attacks in the past year[3]

$5.17M
average cost of a public cloud data breach[4]

Organizations need a revolutionary approach that breaks the barriers between cloud security and security operations teams, enabling them to **detect, investigate** and **respond** to threats with the same agility that attackers use to exploit these divides.

The Cloud Security Divide

Attackers see one cloud attack surface
Security teams see and work in silos

Siloes create dangerous blind spots and leave organizations vulnerable to cloud attacks

Cloud Security
Lack real-time protection to stop cloud attacks

Security Operations
Limited cloud visibility for effective response

Real-Time Protection Is Crucial to Stopping Breaches

Key Challenges in Modern Cloud Security

Several fundamental challenges make cloud security particularly complex:

Dynamic environments
Cloud resources are ephemeral, making traditional security approaches obsolete.

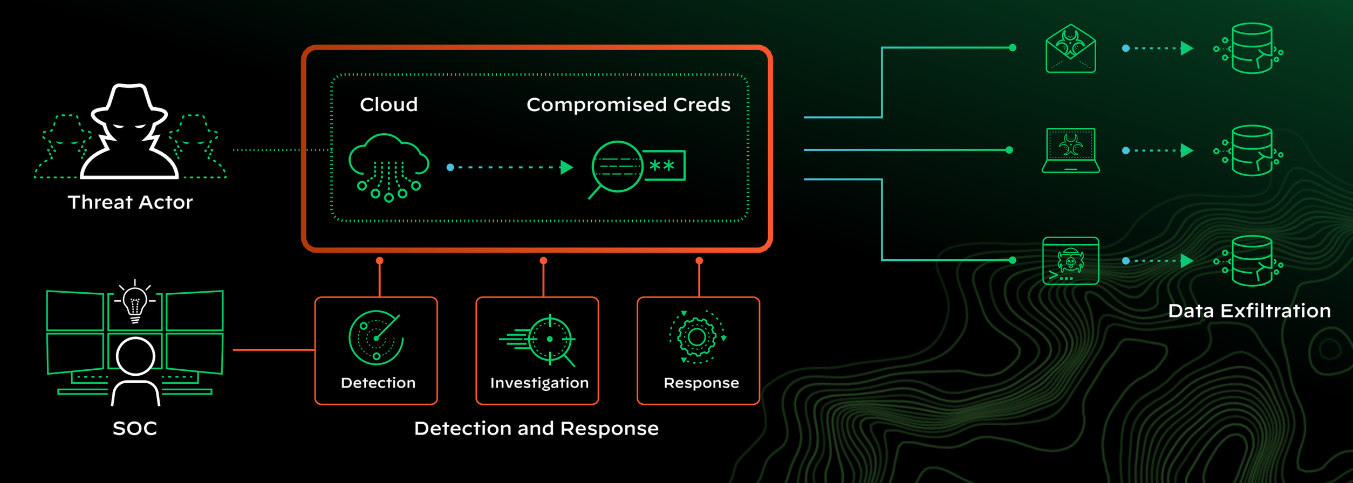
AI-powered threats
Adversaries are leveraging AI to automate attacks and evade detection, making traditional rule-based security obsolete for cloud protection.

Real-time visibility
Traditional tools detect threats after the damage is done. Cloud environments need instant visibility to alert and contain attacks.

Risk prioritization
Cloud environments generate thousands of alerts daily. Without runtime context, security teams can't effectively determine which threats require immediate action.

Security ownership
Fragmented responsibilities between DevOps, SecOps and IT teams create confusion and delays in security response, leading to dangerous gaps in cloud protection.

The Growing Cloud Threat Landscape



The cloud attack surface has evolved dramatically, with threat actors exploiting interconnected cloud infrastructure. A compromised credential or misconfiguration can now trigger widespread impact.

Cloud security cannot be an afterthought and organizations need a comprehensive strategy spanning code, cloud, and SOC.

Rapid detection and response capabilities are needed to stop threats before they escalate into business-disrupting breaches.

Major Attack Vectors

Unit 42 for Cybercrime Operations

Large-Scale Credential Harvesting

In a massive coordinated campaign, attackers targeted environment variable (.env) files across thousands of domains to harvest credentials, particularly focusing on cloud service platforms' API keys and hosted applications' OAuth tokens. The attack's unprecedented scale demonstrates how TAs are exploiting hardcoded credentials and misconfigurations to gain access to cloud environments.

111,000
domains targeted

90,000+
credentials harvested

7,000
cloud service platform credentials compromised

1,200+
organizations affected

Environmental Leak Techniques

The breakdown of the attack flow details how the TAs succeeded and highlights key locations and techniques SOC teams can use to detect similar operations in their environments.

1. Scan Resources

TA initiated the attack with a scan on their target domain, looking for exposed .env files. Cloud XDR agents can detect the collection operations and prevent them.

- Hardcoded credentials (CSP Config)
- Exposed .env files (CSP Config)
- Access to these files (XDR Agent)

2. Create Resources

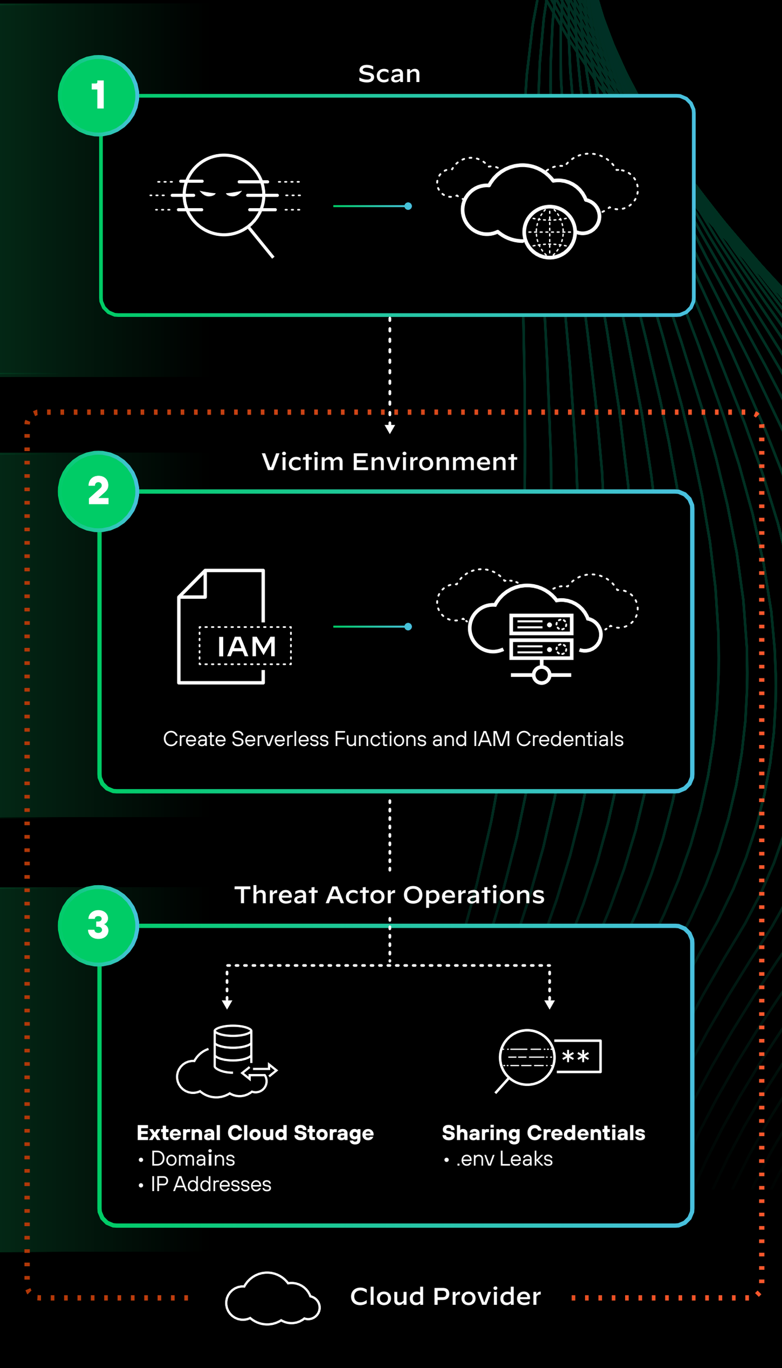
With the collected credentials, the TA pivoted and created new resources. Cloud Detection and Response (CDR) can assist organizations to detect these new IAM or serverless functions.

- Serverless function creation (CSP logging)
- IAM creation (CSP logging)

3. Exfiltrate Data

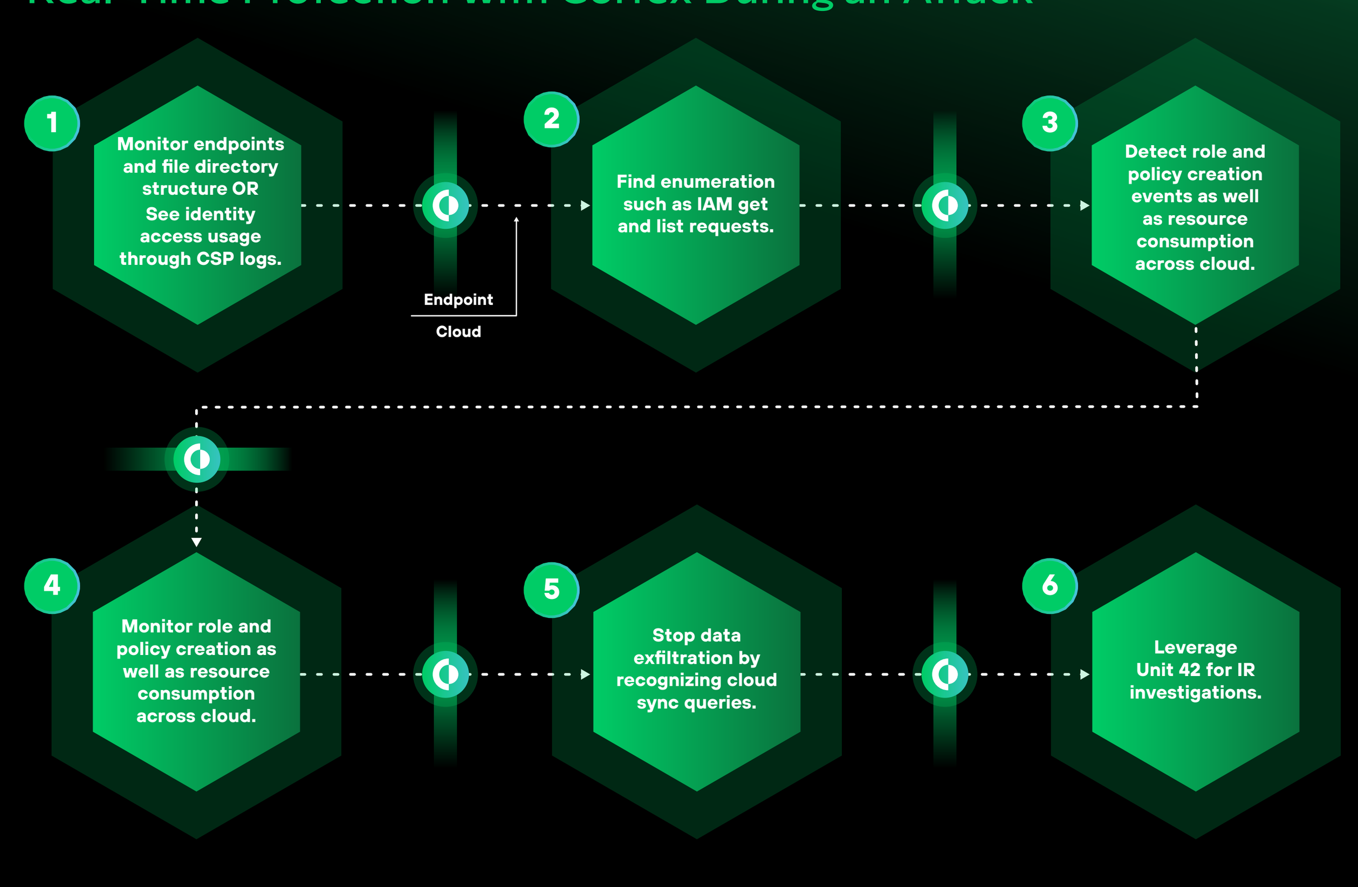
Finally, the TA exfiltrated the discovered cloud data. The detection of data movement operations provided by CDR allows SOC teams to respond accordingly.

- Data sync/move (CSP logging)



Break the Modern Attack Path in Real Time

Real-Time Protection with Cortex During an Attack



Cloud Detection and Response Benefits

Organizations need a unified approach to empower SecOps and cloud security teams to detect and respond at cloud speed. Cloud workloads can be replicated thousands of times, making it critical to detect vulnerabilities and misconfigurations quickly. CDR provides AI-powered prevention, real-time detection and automated response to help SecOps and cloud security teams stop incidents before they become breaches.

Our Approach to Cloud Detection and Response

CDR
Detect and respond to attacks

- Prevent attacks before they escalate
- Detect and prioritize threats with AI
- Speed investigation with analytics
- Automate end-to-end response to save time

Cortex CDR's stops attacks before they become breaches and secures cloud environments during their most vulnerable moments.

Cortex CDR delivers AI-driven security operations that unify cloud protection with your broader security strategy. Experience the power of AI and automation to simplify operations, stop threats at scale, and accelerate incident remediation.

100%
detection score in MITRE ATT&CK® Evaluations — no modifiers or delayed detections.

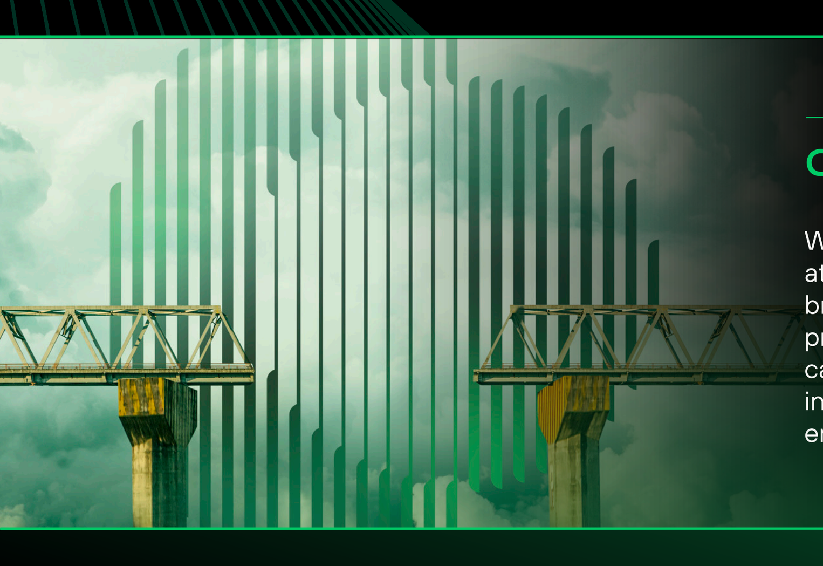
90%
reduction in mean time to respond (MTTR) — from days to minutes.

75%
reduction in analyst workload through AI-driven automation.

Cortex CDR Real-Time Protection

Cortex CDR delivers real-time protection across all cloud workloads and applications:

- **Containers and Kubernetes®:** Secure containers and Kubernetes applications from code to cloud.
- **Hosts and VMs:** Protect hosts and VMs with a defense-in-depth approach that starts with prevention.
- **Serverless functions:** Secure serverless functions across the full application lifecycle.
- **Cloud APIs:** Monitor and protect APIs for suspicious activity.



Closing the Cloud Security Gap

While SecOps and cloud security teams work in silos, attackers exploit the gaps between them. Cortex CDR bridges this divide by unifying teams with AI-powered protection, real-time detection and automated response capabilities. The result? Threats are stopped in minutes instead of days, and teams can finally protect cloud environments at the speed and scale of modern attacks.

Transform Your Cloud Security Today

Request a Demo

Learn More About Cortex CDR

[1] "IDC FutureScape: The Digital Business Era Has Arrived, Augmented by GenAI," IDC, November 29, 2023.
[2] 2023 Unit 42 Attack Surface Threat Report, Palo Alto Networks, September 14, 2023.
[3] 2024 Unit 42 Incident Response Report, Palo Alto Networks, February 20, 2024.
[4] Cost of a Data Breach Report 2024, IBM Security, July 30, 2024.

paloalto NETWORKS | CORTEX