paloalto NETWORKS | CORTEX CLOUD

Cloud Detection and Response Buyer's Guide

What to Know, What to Ask, and What to Insist On

Table of Contents

What's the right way to secure your cloud?

With 80% of all medium, high, and critical exposures found in the cloud,[1] SOC teams must adapt their strategies to secure dynamic, distributed environments where traditional tools fall short.

Cloud detection and response (CDR) is emerging as a critical capability in cloud security, offering the visibility and agility needed to address gaps left by legacy tools. Unlike traditional approaches, CDR provides continuous monitoring, real-time threat detection, and automated response tailored to the cloud's ephemeral nature.

In this buyer's guide, we outline key considerations and features to help you move from evaluation to implementation with confidence.

[1] *Unit 42 Attack Surface Threat Report 2023*, Palo Alto Networks, September 2023.

What cybersecurity leaders want. And need.

91%

report that the number of point tools they use creates blind spots, affecting their ability to prioritize risk and prevent threats.

94%

have expressed the need for a centralized security solution that spans all cloud accounts and services.

Source: Palo Alto Networks, *The State of Cloud-Native Security Report 2024.*

MUST-HAVES

The top 5 capabilities to look for.

To provide true protection, cloud detection and response should span the entire attack cycle.

1| Runtime protection

2| Real-time detection

3| Advanced investigation

4| Integrated automation

5| Remediation at scale

1 Runtime protection

✓ Protect cloud applications during execution by detecting and blocking threats like malware, ransomware, fileless attacks, cryptominers, and exploits.

✓ Use behavioral analysis to identify anomalies in application behavior and stop attacks in real time.

✓ Ensure coverage across all environments, including containers, virtual machines, and serverless applications.

2 Real-time detection

✓ Continuously monitor cloud environments to detect threats as they happen, ensuring no activity goes unnoticed.

✓ Prioritize low-latency detection to identify attacks that unfold within hours—rather than days—and enable immediate action.

✓ Correlate events across workloads, identities, APIs, and data flows to provide full visibility into attack vectors.

3 Advanced investigation

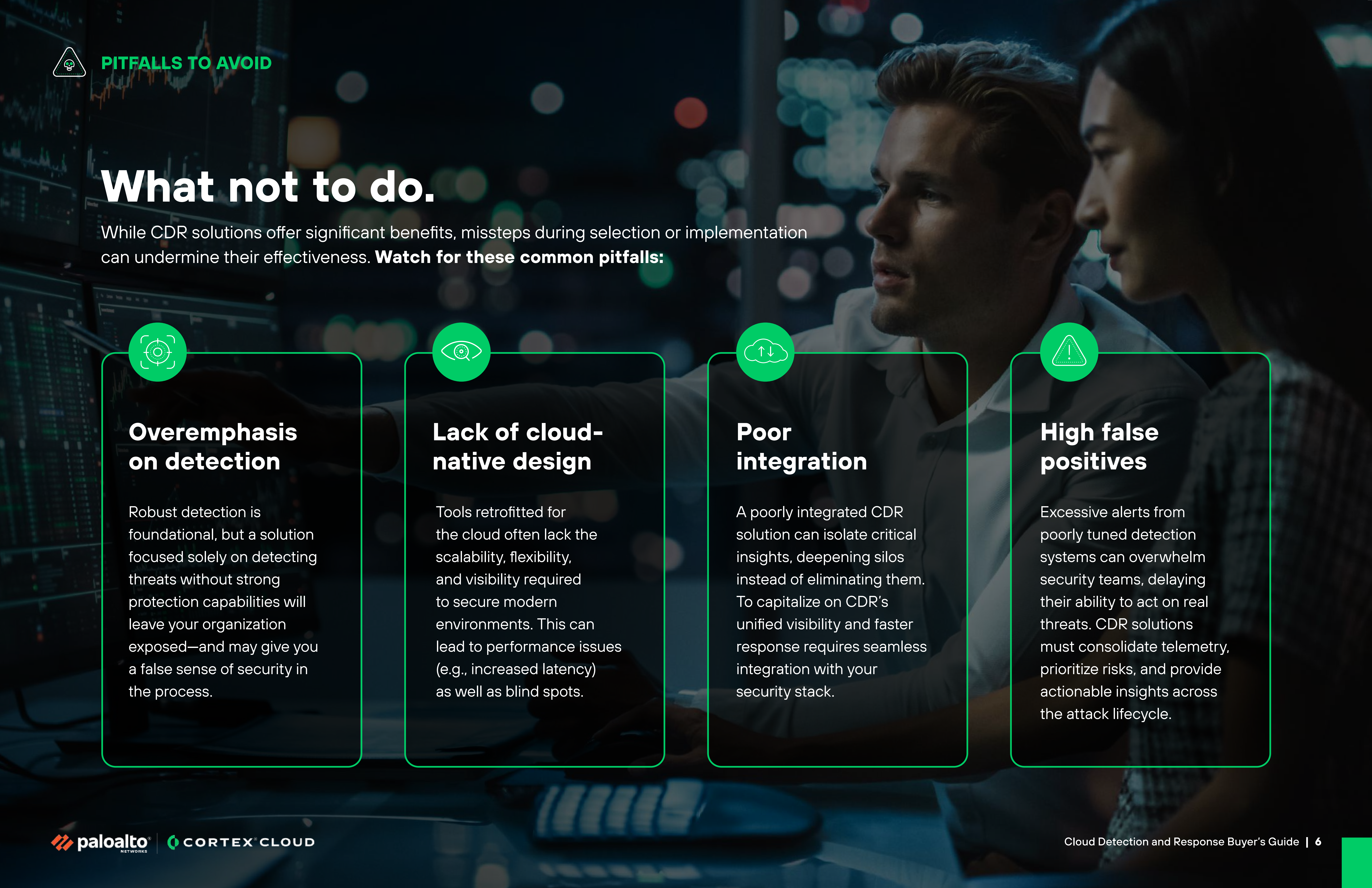
- ✓ Provide deep visibility into attack stages by contextualizing data from multiple cloud sources, such as identities, networks, data resources, and workloads.
- ✓ Detect and analyze advanced threats—including lateral movement, privilege escalation, and data exfiltration—by correlating activity across environments.
- ✓ Automatically prioritize critical alerts, allowing security teams to focus on the most urgent threats and streamline investigations.

4 Integrated automation

- ✓ Automate detection, contextualization, and prioritization, using AI to reduce reliance on manual workflows and streamline incident response.
- ✓ Identify root causes quickly, enabling faster mitigation and significantly lowering mean time to respond (MTTR).
- ✓ Integrate automation into key aspects of incident response to enhance efficiency and scalability, reducing reliance on ad-hoc playbooks.

5 Remediation at scale

- ✓ Remediate risks by deploying fixes across cloud infrastructure, applications, and endpoints in a coordinated way.
- ✓ Automate containment and response to prevent attack spread and quickly mitigate risk.
- ✓ Address root causes to resolve multiple related vulnerabilities simultaneously, preventing recurring issues.



What not to do.

While CDR solutions offer significant benefits, missteps during selection or implementation can undermine their effectiveness. **Watch for these common pitfalls:**

Overemphasis on detection

Robust detection is foundational, but a solution focused solely on detecting threats without strong protection capabilities will leave your organization exposed—and may give you a false sense of security in the process.

Lack of cloud-native design

Tools retrofitted for the cloud often lack the scalability, flexibility, and visibility required to secure modern environments. This can lead to performance issues (e.g., increased latency) as well as blind spots.

Poor integration

A poorly integrated CDR solution can isolate critical insights, deepening silos instead of eliminating them. To capitalize on CDR's unified visibility and faster response requires seamless integration with your security stack.

High false positives

Excessive alerts from poorly tuned detection systems can overwhelm security teams, delaying their ability to act on real threats. CDR solutions must consolidate telemetry, prioritize risks, and provide actionable insights across the attack lifecycle.

QUESTIONS TO ASK

A guide for the conversation with your vendor.

DATA, VISIBILITY, AND TEAM UNIFICATION

- Does the solution provide real-time visibility across multicloud environments, including hybrid setups?
- What integrations are available with existing security tools—including SIEM, SOAR, and CNAPP solutions—as well as DevOps pipelines?
- Is telemetry shared and correlated between cloud security and SecOps teams to support unified investigations?
- Does the solution provide real-time visibility and monitoring for ephemeral assets—e.g., containers and serverless functions—and does it address their short lifespans?

PREVENTION AND DETECTION

- Can the tool detect both known and unknown threats in real time?
- How does the solution's runtime protection extend beyond workload security to detect and contain active threats across the broader cloud environment?
- Does the solution reduce alert noise and ensure that critical threats are prioritized for security teams? Can the vendor provide metrics demonstrating this capability?
- What false positive rate does the solution achieve?
- How does the solution scale to support large, dynamic cloud environments with significant telemetry volume?

QUESTIONS TO ASK

ADVANCED INVESTIGATION

- Does the solution provide real-time correlation of data from different sources—e.g., workloads, identities, networks, and APIs—to provide full context of incidents?
- Can the solution map events across the attack lifecycle to support threat hunting and root cause analysis?
- Does the solution provide prebuilt queries or dashboards to accelerate investigations?

COMPLIANCE

- Does the solution handle compliance monitoring and reporting for frameworks such as GDPR, HIPAA, and PCI DSS?
- Can the solution generate detailed audit trails for incident handling and policy enforcement to support compliance efforts?

RESPONSE AND AUTOMATION

- Does the solution support automated remediation workflows that are customizable to an organization's needs?
- Can the solution orchestrate response actions across multicloud, hybrid, and on-premises environments?
- Does the solution use AI and machine learning to continuously improve detection, response precision, and adaptability?
- Can you define granular policies to automate response actions based on specific triggers or conditions?

> “As cybersecurity threats evolve, organizations must adapt by seeking better visibility into their code-to-cloud environment, identifying ways to accelerate remediation, strengthening organizational collaboration, and streamlining processes to counter risks effectively.”
>
> **Hillary Baron,** Senior Technical Director of Research, Cloud Security Alliance

96% of organizations express apprehension about public cloud security.

55% identify securing multicloud environments as a challenge.

69% depend on three or more separate solutions to manage cloud security.

Source: *2024 Cloud Security Report*, Cybersecurity Insiders.

> "Unified cloud security is essential in the face of increasing cloud adoption and sophisticated cyber threats. By providing centralized management and integrating advanced threat detection capabilities, unified security solutions enhance an organization's ability to protect its digital assets."

Rene Millman, "What are the benefits of unified cloud security?," CLOUDPro., September 2, 2024.

Make sure your solution includes the following capabilities.

Data, visibility, and team unification

□ Provides real-time visibility into cloud ecosystems by continuously monitoring dynamic activity across workloads, identities, APIs, and data flows (in contrast to point-in-time scans).

□ Identifies cloud-specific threats, including misconfigurations and insecure APIs.

□ Enables secure coding practices by integrating security into the CI/CD pipeline, ensuring DevOps teams can address vulnerabilities earlier.

□ Leverages a unified dataplane that consolidates and correlates information from across the cloud environment to provide full risk context.

Prevention and detection

□ Monitors cloud infrastructure (compute, storage) and applications for suspicious activity and vulnerabilities.

□ Identifies cloud-based threats from third-party sources, including malware and unauthorized access attempts.

□ Detects unusual network activity, including data exfiltration and lateral movement.

□ Tracks and alerts on security events, including failed login attempts and privilege escalation.

□ Implements anomaly detection using user behavior analytics and machine learning.

□ Detects unauthorized API calls and suspicious authentication attempts.

□ Uses threat intelligence to proactively hunt for threat actor tactics, techniques, and procedures in the cloud environment.

Advanced investigation

□ Correlates cloud activity and threat intelligence using SIEM systems.

□ Integrates external threat intelligence feeds directly for enriched analysis.

□ Escalates cloud security incidents according to predefined workflows, ensuring consistent and timely response.

Response and automation

□ Offers automated playbooks for handling cloud-specific security incidents, e.g., compromised instances or data breaches.

□ Enables automated responses, including IP blocking, workload isolation, and containment of compromised resources.

□ Uses cloud-native automation tools (e.g., AWS Lambda, Azure Automation) for rapid containment.

□ Automates ticket creation, incident reporting, and notifications to streamline response workflows.

□ Uses machine learning and AI to detect emerging threats.

Integration and ecosystem compatibility

□ Natively integrates with SIEM, SOAR, XDR, and CNAPP solutions to ensure a seamless security ecosystem.

□ Supports APIs for custom integrations, enabling data sharing and enhanced flexibility.

□ Provides compatibility with DevOps pipelines and CI/CD tools to embed security into development workflows.

Compliance

□ Monitors and audits access to sensitive data, including personally identifiable information and financial records.

□ Tracks compliance with industry standards and regulations, e.g., GDPR, HIPAA, and PCI DSS.

□ Maintains detailed audit trails of user actions and system changes for transparency and accountability.

□ Records cloud security incidents and their resolutions to support compliance audits and continuous improvement.

Cortex® CDR Redefines Cloud Detection and Response

The complexity of the modern attack surface requires moving beyond isolated tools to an integrated platform that empowers teams to prevent, detect, and respond to threats with precision and speed. It's time for a new approach to security: one that breaks down the barriers between AppSec, CloudSec, and SecOps.

Cortex CDR delivers an AI-driven, automation-first approach to securing cloud environments by unifying real-time detection, investigation, and response across cloud workloads, identities, APIs, and networks. Built to break down silos between cloud security and security operations, it enables teams to detect faster, investigate smarter, and respond with precision—reducing risk and operational overhead.

1 | **Proactive defense**
Block threats before they materialize

2 | **Context-rich investigation and prioritization**
Turn fragmented alerts into highly prioritized threats

3 | **Accelerated response**
Reduce mean time to resolution (MTTR) by 90%

4 | **Future-proof automation**
Leverage AI that continuously learns from incidents

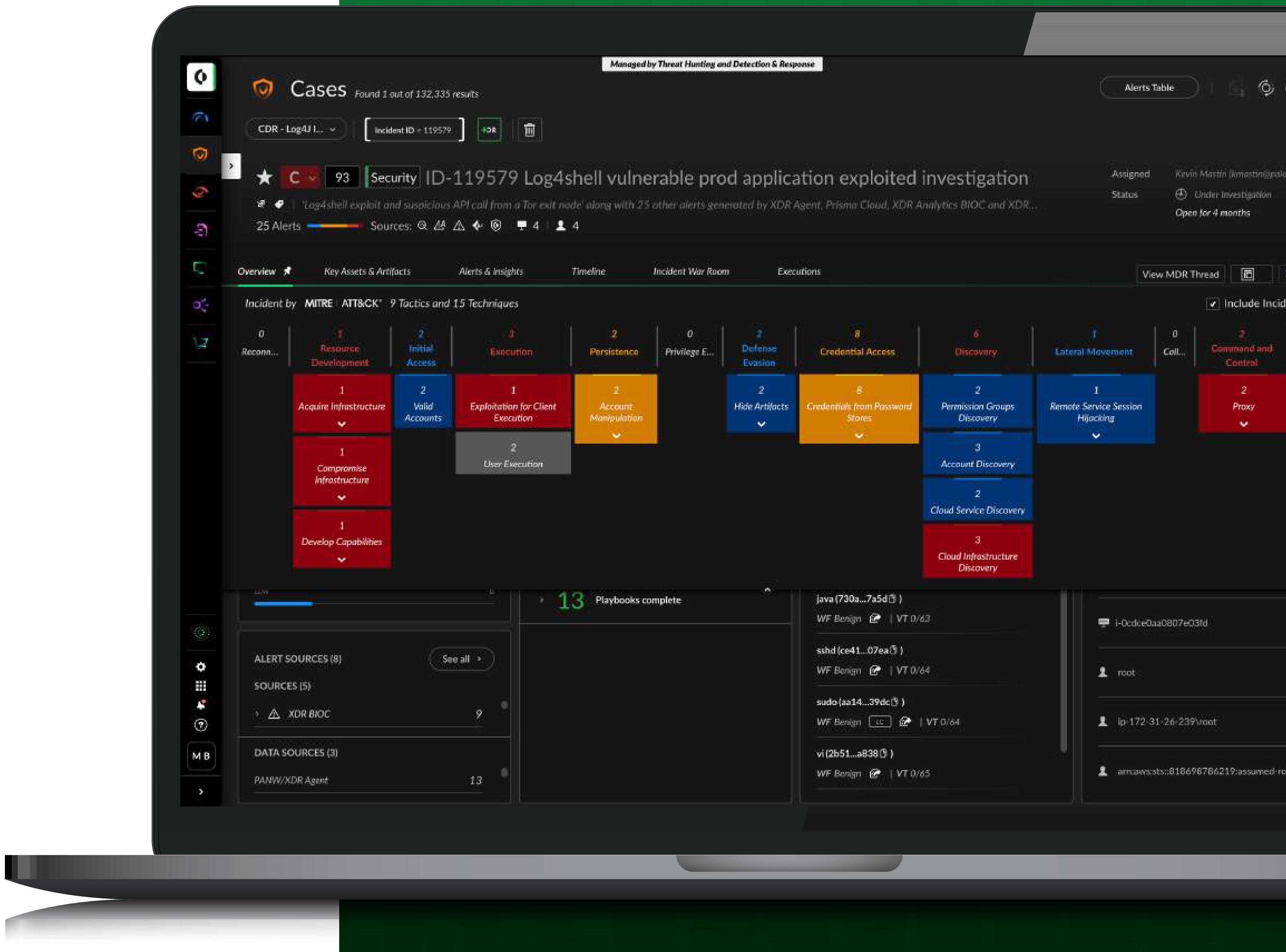
5 | **Analyst productivity**
Decrease analyst workload by 75%

1

Proactive Defense

Cortex CDR stops attacks before they escalate by combining real-time protection with elite threat intelligence and AI-powered detection. Unlike solutions that rely on periodic scanning, Cortex monitors continuously for behavioral anomalies, unauthorized API activity, and cloud-native threats across workloads, containers, and serverless functions. Its MITRE ATT&CK®-mapped detections provide security teams with deeper insights into attack tactics, techniques, and procedures, allowing for earlier and more effective intervention.

- **100% technique-level detection** in MITRE ATT&CK evaluations with no configuration changes
- **Runtime protection** for VMs, Kubernetes, containers, and serverless environments
- **Automated containment actions** to stop threats before they impact business operations



Managed by Threat Hunting and Detection & Response

Cases Found 1 out of 132,335 results

C 93 Security 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 Agent, Prisma Cloud, XDR Analytics BIOC and XDR...

25 Alerts Sources: 4 4

Assigned: Kevin Mastin (kmastin@palo
Status: Under Investigation
Open for 4 months

Incident by MITRE ATT&CK® 9 Tactics and 15 Techniques

0 Reconn...	1 Resource Development	2 Initial Access	3 Execution	2 Persistence	0 Privilege E...	2 Defense Evasion	8 Credential Access	6 Discovery	1 Lateral Movement	0 Coll...	2 Command and Control
	1 Acquire Infrastructure	2 Valid Accounts	1 Exploitation for Client Execution	2 Account Manipulation		2 Hide Artifacts	8 Credentials from Password Stores	2 Permission Groups Discovery	1 Remote Service Session Hijacking		2 Proxy
	1 Compromise Infrastructure		2 User Execution					3 Account Discovery			
	1 Develop Capabilities							2 Cloud Service Discovery			
								3 Cloud Infrastructure Discovery			

13 Playbooks complete

ALERT SOURCES (8) See all
SOURCES (5)
XDR BIOC 9
DATA SOURCES (3)
PANW/XDR Agent 13

java (730a...7a5d)
WF Benign | VT 0/63
sshd (ce41...07ea)
WF Benign | VT 0/64
sudo (aa14...39dc)
WF Benign LC | VT 0/64
vi (2b51...a838)
WF Benign | VT 0/65

i-0cdce0aa0807e03fd
root
ip-172-31-26-239\root
arn:aws:sts::818698786219:assumed-ro

90%

reduction in mean time to respond (MTTR) by consolidating data into actionable insights

2 Context-Rich Investigation and Prioritization

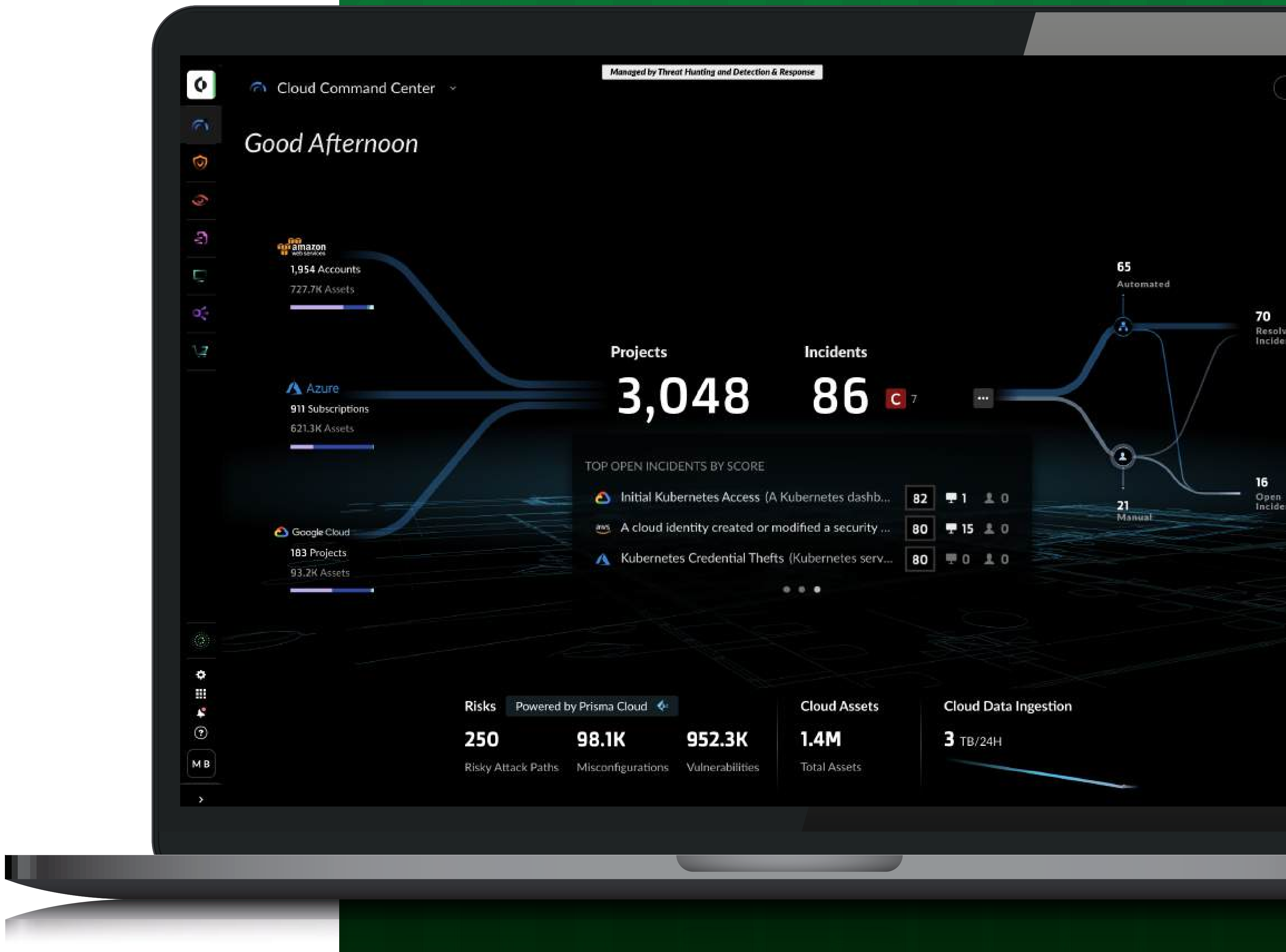
Security teams face an overwhelming volume of alerts and fragmented data across multiple security solutions. Cortex CDR automates correlation across cloud telemetry, mapping events into a single, high-fidelity threat narrative that provides full attack context. AI-driven SmartGrouping consolidates multiple alerts into prioritized incidents, while SmartScoring ranks threats based on risk severity and asset criticality—eliminating guesswork.

- **Integrated cloud and SOC context** to surface critical threats instantly
- **Automatic correlation across cloud control, data, and management planes** for a unified investigation

3 Accelerated Response

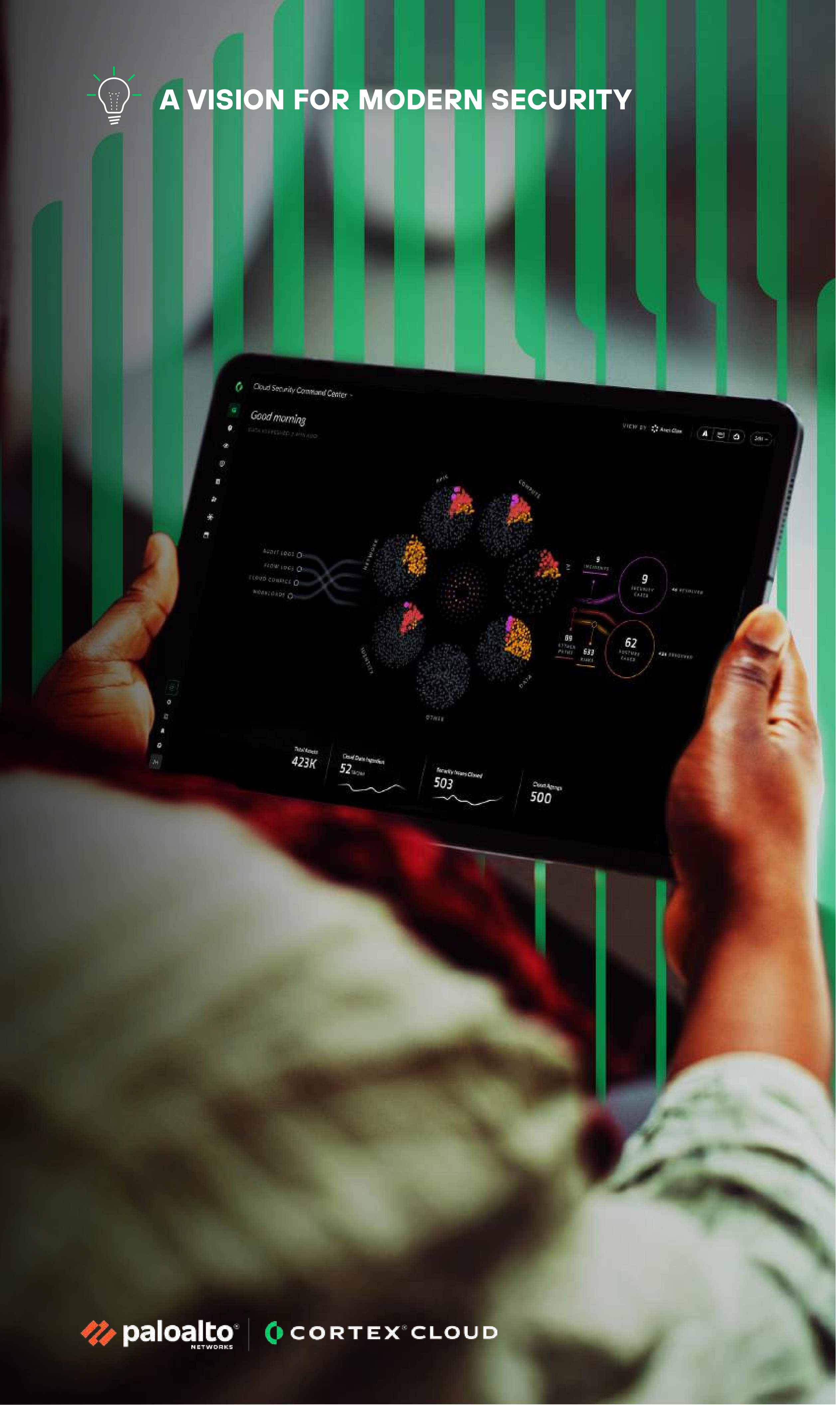
Cortex CDR reduces response times from days to minutes by automating containment, remediation, and mitigation workflows. Prebuilt playbooks and automated enforcement empower security teams to act immediately on validated threats—without manual intervention. Whether isolating a compromised workload, blocking a malicious IP, or terminating an unauthorized API session, Cortex CDR ensures that response actions are precise, timely, and scalable.

- **AI-driven automation executes response actions instantly** based on predefined security policies
- **1,000+ automation capabilities and integrations** with SIEM, SOAR, and CNAPP solutions
- **Cross-cloud response orchestration** for multicloud, hybrid, and on-premises environments



TOP OPEN INCIDENTS BY SCORE

Initial Kubernetes Access (A Kubernetes dashb...	82	1	0
A cloud identity created or modified a security ...	80	15	0
Kubernetes Credential Thefts (Kubernetes serv...	80	0	0



4

Future-Proof Automation

Cloud threats evolve at machine speed, and so must security operations. Cortex CDR integrates self-learning AI models that continuously adapt to new attack techniques, suggest new playbooks, and improve detection accuracy over time. The solution provides end-to-end automation that goes beyond static rule-based responses, enabling dynamic, risk-based security enforcement.

- **AI learns from previous threats to** optimize detection and response workflows
- **Automated threat hunting** reduces reliance on manual investigations
- **Context-aware remediation suggestions** empower security teams with guided actions

5 Analyst Productivity

With AI-driven prioritization and automation, Cortex CDR alleviates alert fatigue and allows security teams to focus on what matters. By streamlining investigation workflows, reducing false positives, and automating low-level tasks, analysts can spend more time on proactive threat hunting and high-value security initiatives.

- **One unified interface** for cloud detection, investigation, and response
- **Seamless collaboration between CloudSec and SecOps** to eliminate data silos

75%

reduction analyst workload

through AI-powered case consolidation

Cloud Defense Without Limits

Cortex CDR leads the industry with a unified, AI-enabled solutions for preventing, blocking, detecting, and responding to threats.

The solution bridges the gap between cloud security and security operations, enabling teams to detect, investigate, and respond to threats in real time—without being overwhelmed by noise.

AI-driven correlation and automation replace fragmented workflows, reducing risk while increasing speed and precision.

Instead of reacting to incidents after the fact, security teams gain the capability to neutralize threats before they escalate—at cloud scale and speed.

What makes Cortex different?

- A single agent for cloud and endpoint.
- One data lake for centralized data collection, analysis, and correlation.
- The first to achieve 100% technique-level detection coverage with no delays or configuration changes in MITRE ATT&CK evaluations.
- Consistently recognized as a leader by Forrester, Gartner, and others.

Ready to see Cortex CDR in action?

SCHEDULE A DEMO TODAY

3000 Tannery Way
Santa Clara, CA 95054

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