

# Real-Time Cloud Security

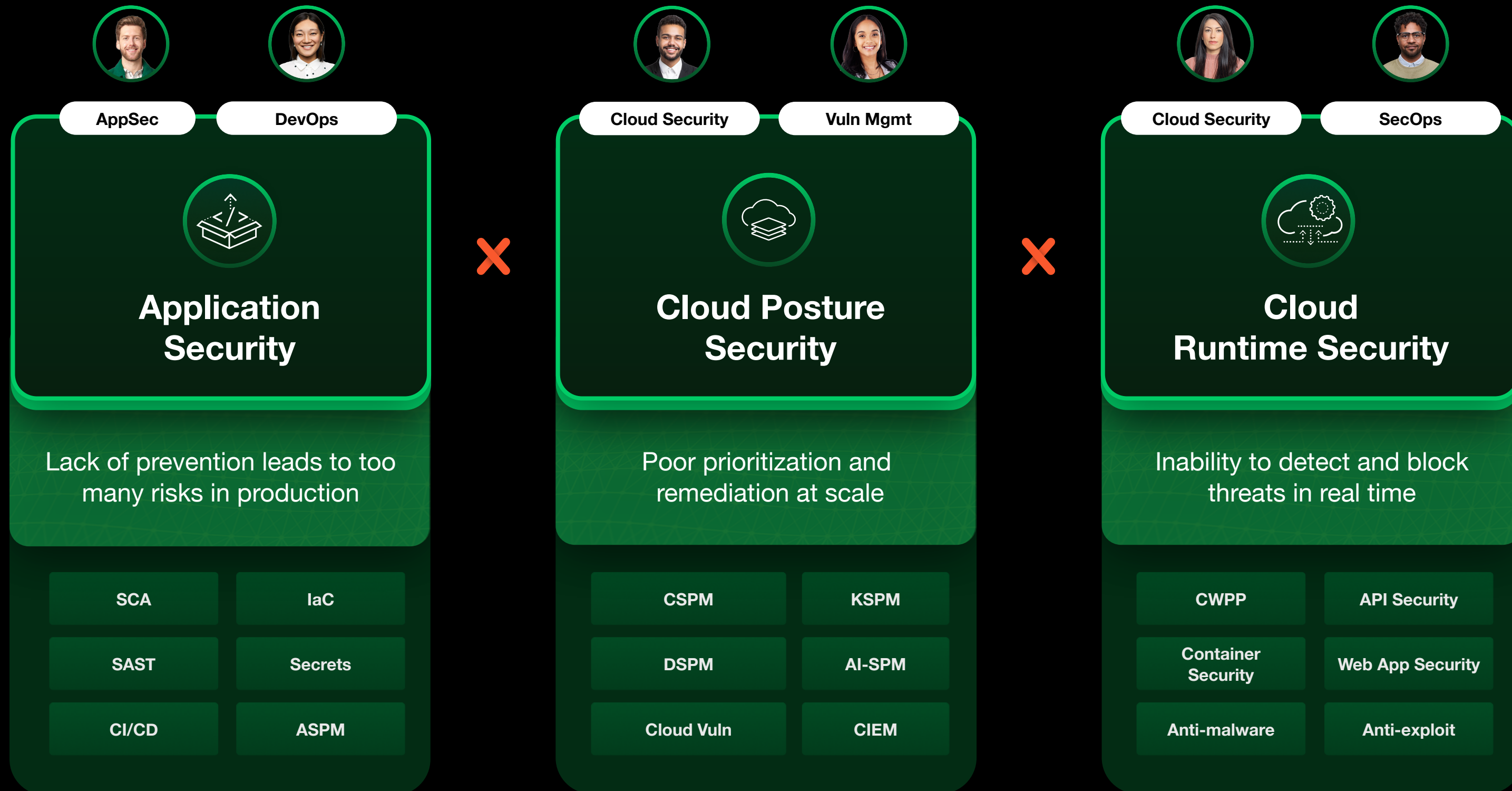
The industry's first AI & automation driven  
platform spanning code to cloud to SOC

---

Zsolt Vilhelm | Solutions Consultant

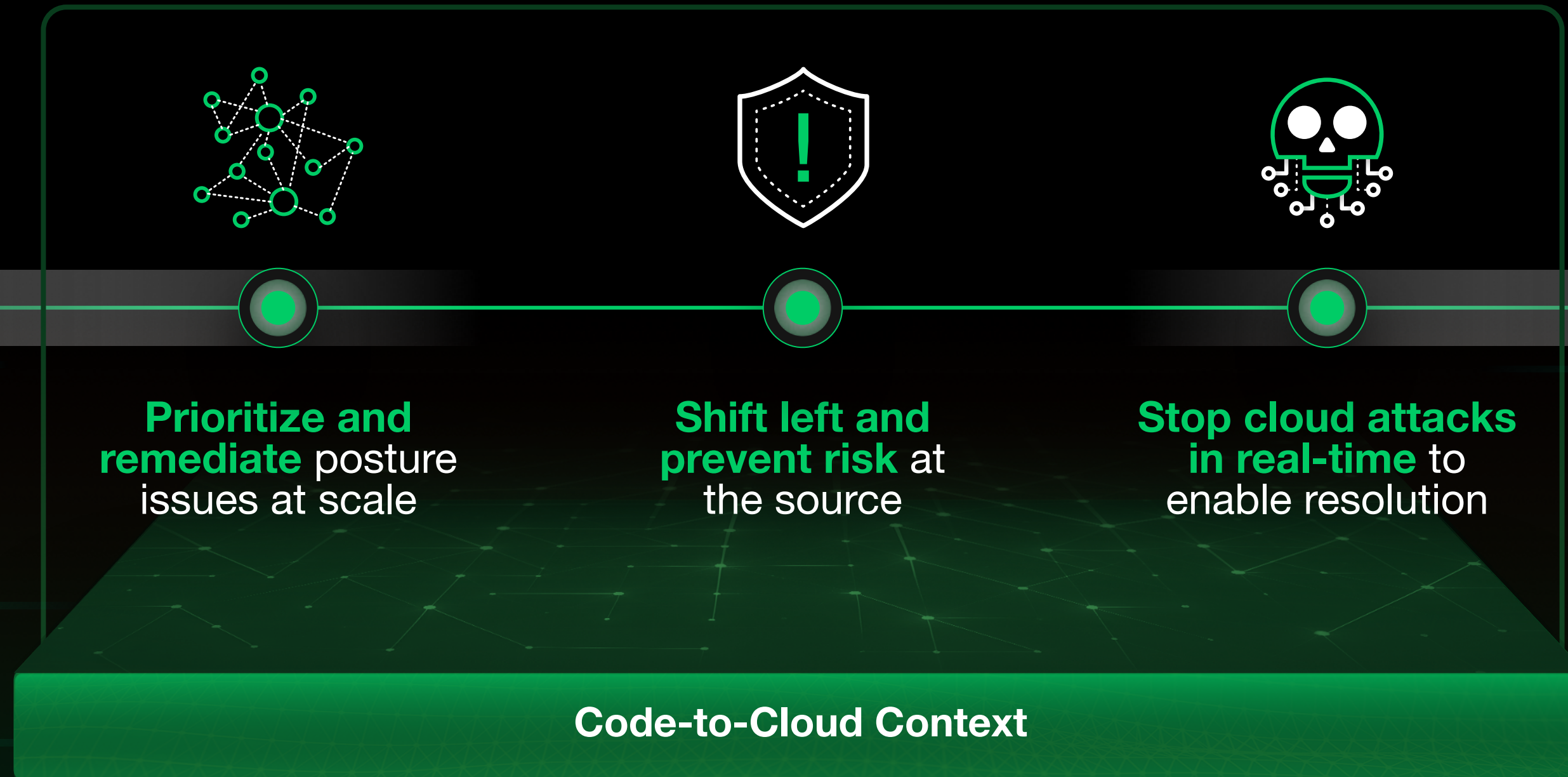
# The Industry Is Building Cloud Security in Silos

Creating massive complexity and gaps in protection



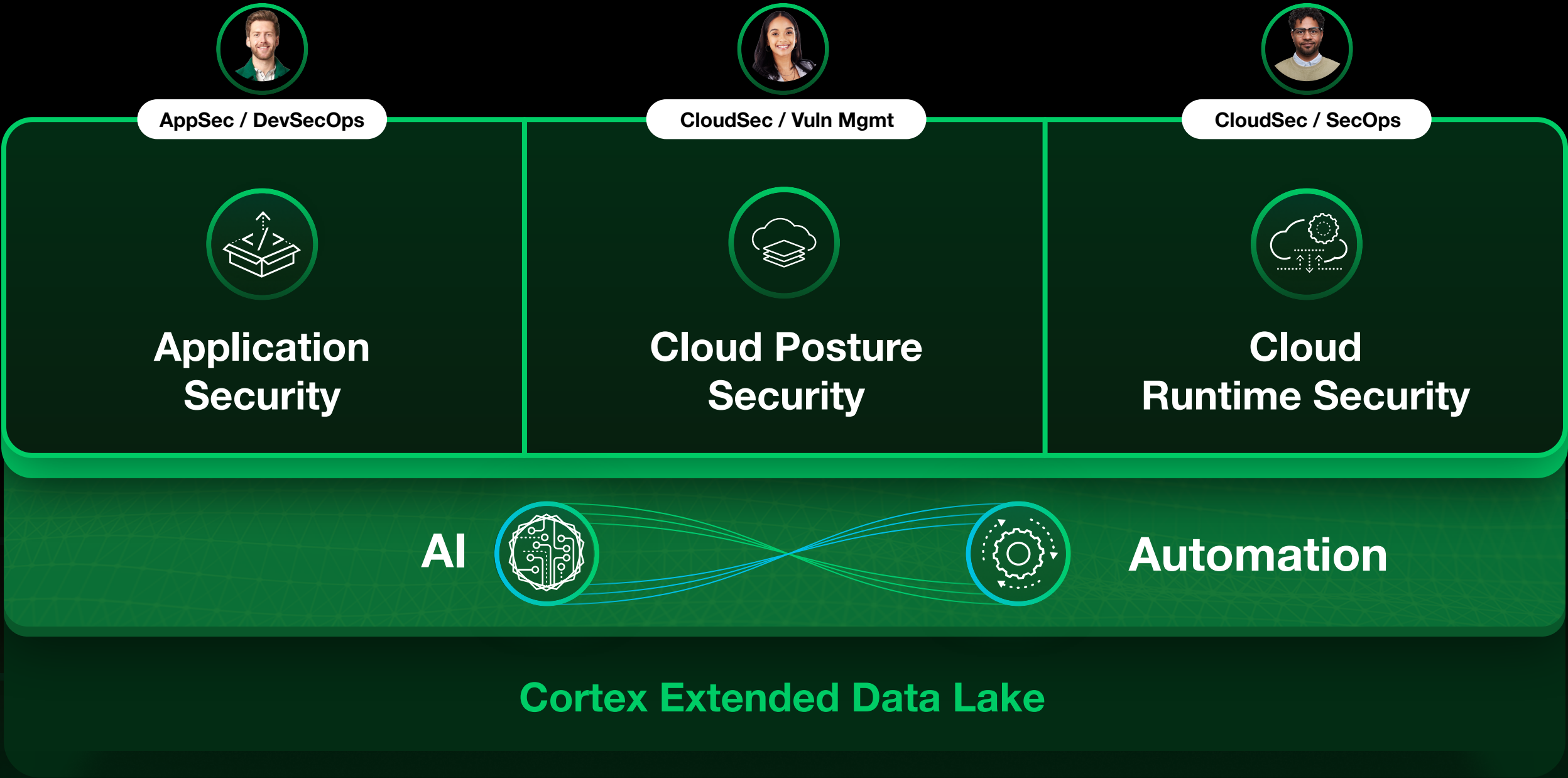


# What's Needed for Effective Cloud Security



# Introducing Cortex Cloud

The industry's leading CNAPP merged with best-in-class CDR for real-time cloud security



CODE



SUPPLY  
CHAIN



AI MODELS



CONFIGS



IDENTITY



CLOUD LOGS



WORKLOADS



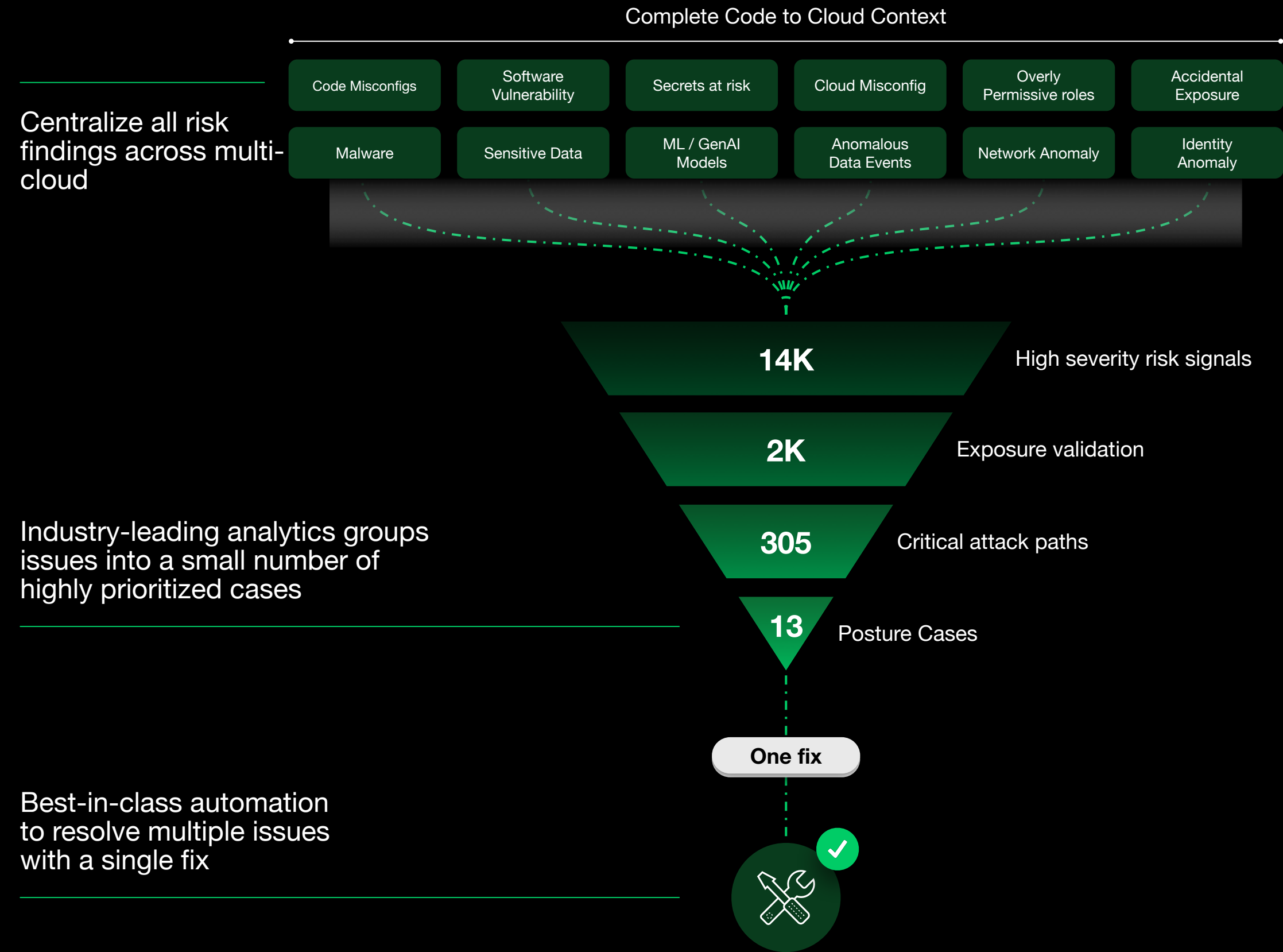
CVES



SENSITIVE  
DATA



NETWORK



Prioritize  
& Remediate  
Posture Issues



# AI-Powered Security Posture Assessment and Prioritization

Cases deliver  
**cloud remediation at scale**

Always take the right  
action **with best fix guidance**

Take **one action** to:

Resolve **28 issues** and secure **29 assets**

The screenshot displays the Cortex XDR console interface for a security case. The top navigation bar includes tabs for 'Cases', 'Findings Table', and 'Issues Table'. The main content area is divided into several sections:

- Case Overview:** Shows the case ID 'ID-4969911', title 'Fix AWS IAM Role 'az-admin-hr' to resolve 28 issues related to privilege escalation', and a status of 'In Progress'. It also indicates '28 Issues' and '29 Assets'.
- Issues (28):** A section showing the total number of issues and a breakdown by severity: Critical (5), High (11), Medium (10), and Low (2).
- Automation:** A section showing the number of actions, recommendations, and completed playbooks.
- Assets (29):** A list of assets associated with the case, including 'az-admin-hr' (IAM Role), 'web-server-prod-01' (EC2 Instance), 'db-master-01' (EC2 Instance), 'app-instance-staging-02' (EC2 Instance), 'worker-node-03' (EC2 Instance), 'load-balancer-01' (EC2 Instance), 'api-gateway-prod-03' (EC2 Instance), 'etl-processing-node-01' (EC2 Instance), and 'dev-app-instance-01' (EC2 Instance).

Red lines highlight the 'Issues (28)' and 'Assets (29)' sections, indicating the scope of the remediation effort.



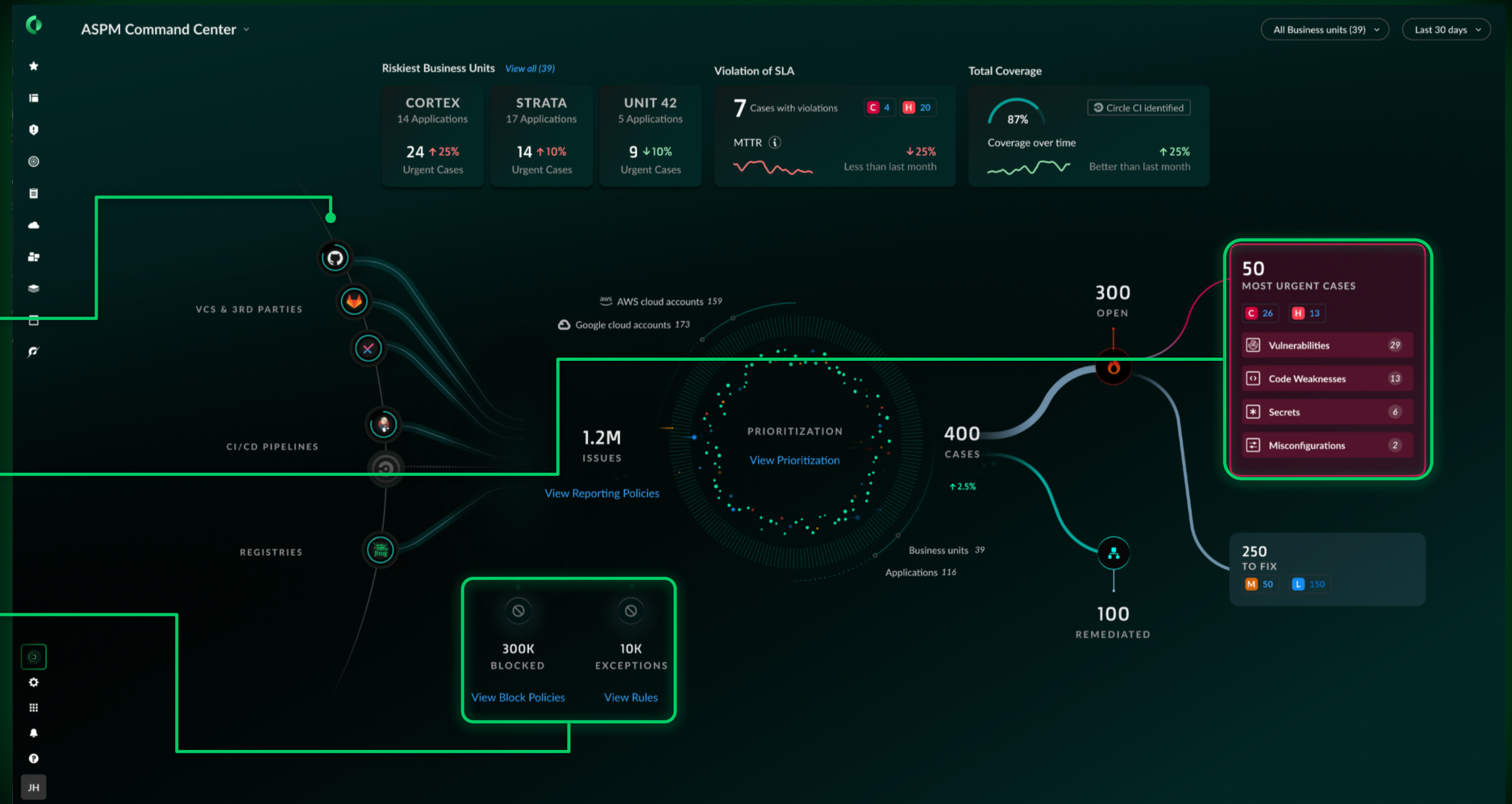
# Prevent insecure code and fix it before production

Comprehensive risk prioritization based on **code, runtime and application** context

**Centralize visibility**  
integrate native AppSec tools and third-party scanners

**Quickly identify**  
critical application risk

Easily learn how to **prevent** future risk from being introduced



# Stop Cloud Attacks in real time with Cloud Runtime Security

## Prevent sophisticated attacks on workloads and APIs

Shut down behavioral threats, vulnerability exploits, malicious processes, and, zero-day attacks

## Accelerate detection and response

See the full attack timeline with Security Cases and pinpoint the root cause

## Easy to deploy and operate

Deploys in minutes to gain real-time visibility and protection across your multi-cloud environment in eBPF or Kernel mode.

### Best-in-class Protection

100% Detection Score

MITRE | ATT&CK®

10k Detectors  
2.6k+ ML models



Kubernetes



Containers



APIs



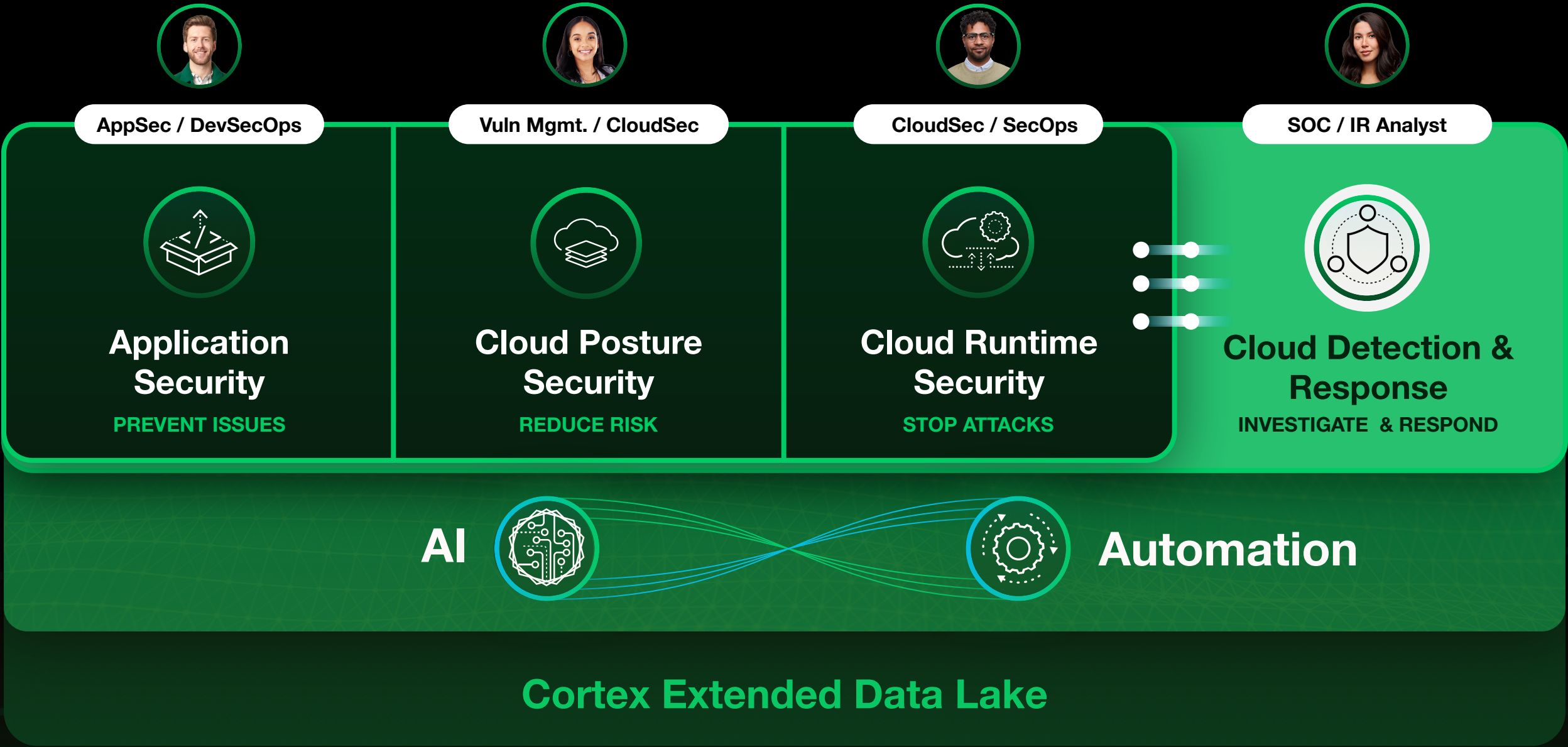
Serverless



Hosts / VMs



Extending the Industry's Leading CNAPP to the SOC  
For real-time Cloud Detection & Response

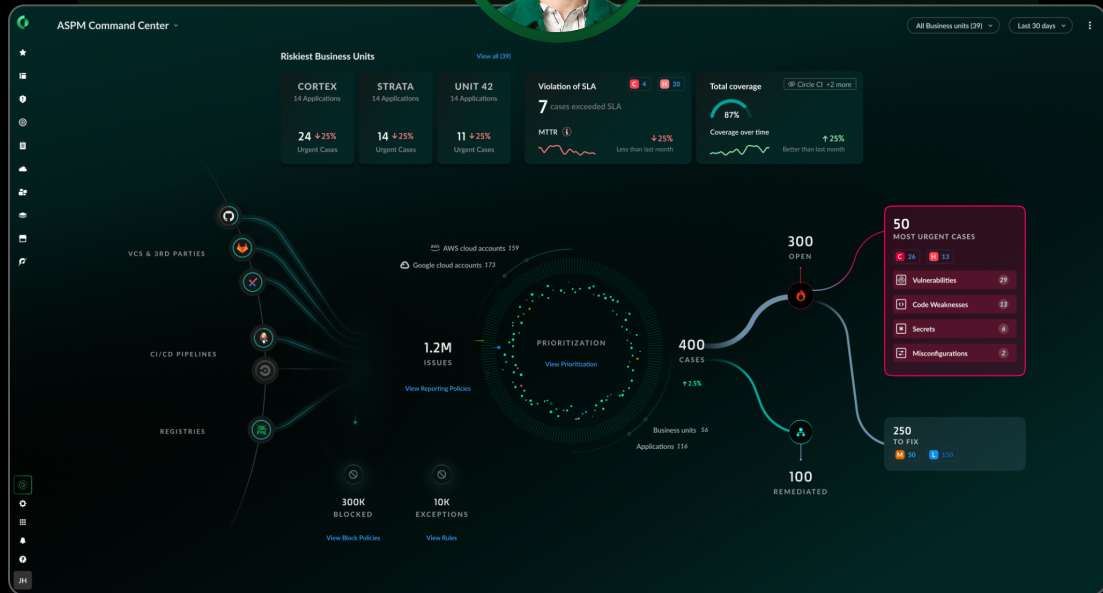


# Purpose Built User Experiences for Each Team

Optimized dashboards and workflows with granular role-based access control (RBAC)

AppSec

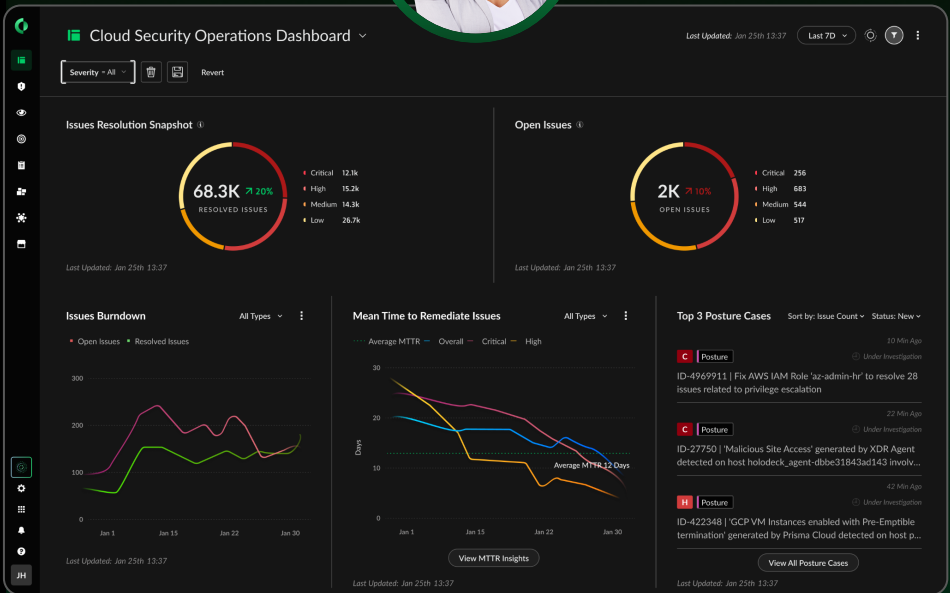
DevSecOps



Application Security

CloudSec

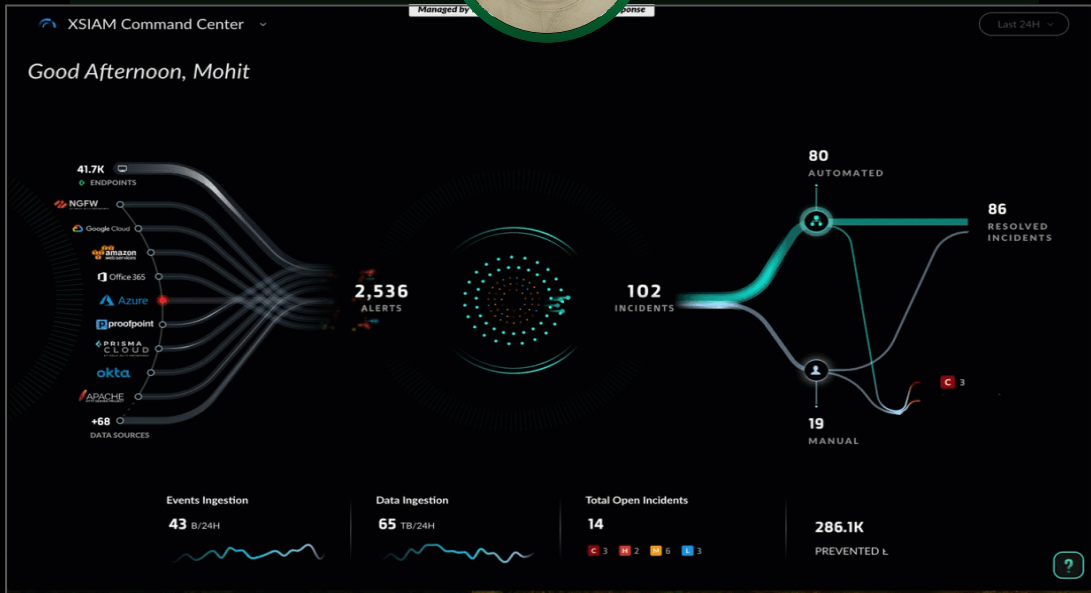
Vuln Mgmt



Cloud Security

SOC Analyst

IR Analyst



Security Operations



# Start Anywhere, Expand to Anything

Adopt best-in-class capabilities independently or as part of a single platform



## Application Security

PREVENT ISSUES



## Cloud Posture Security

REDUCE RISK



## Cloud Runtime Security

STOP ATTACKS

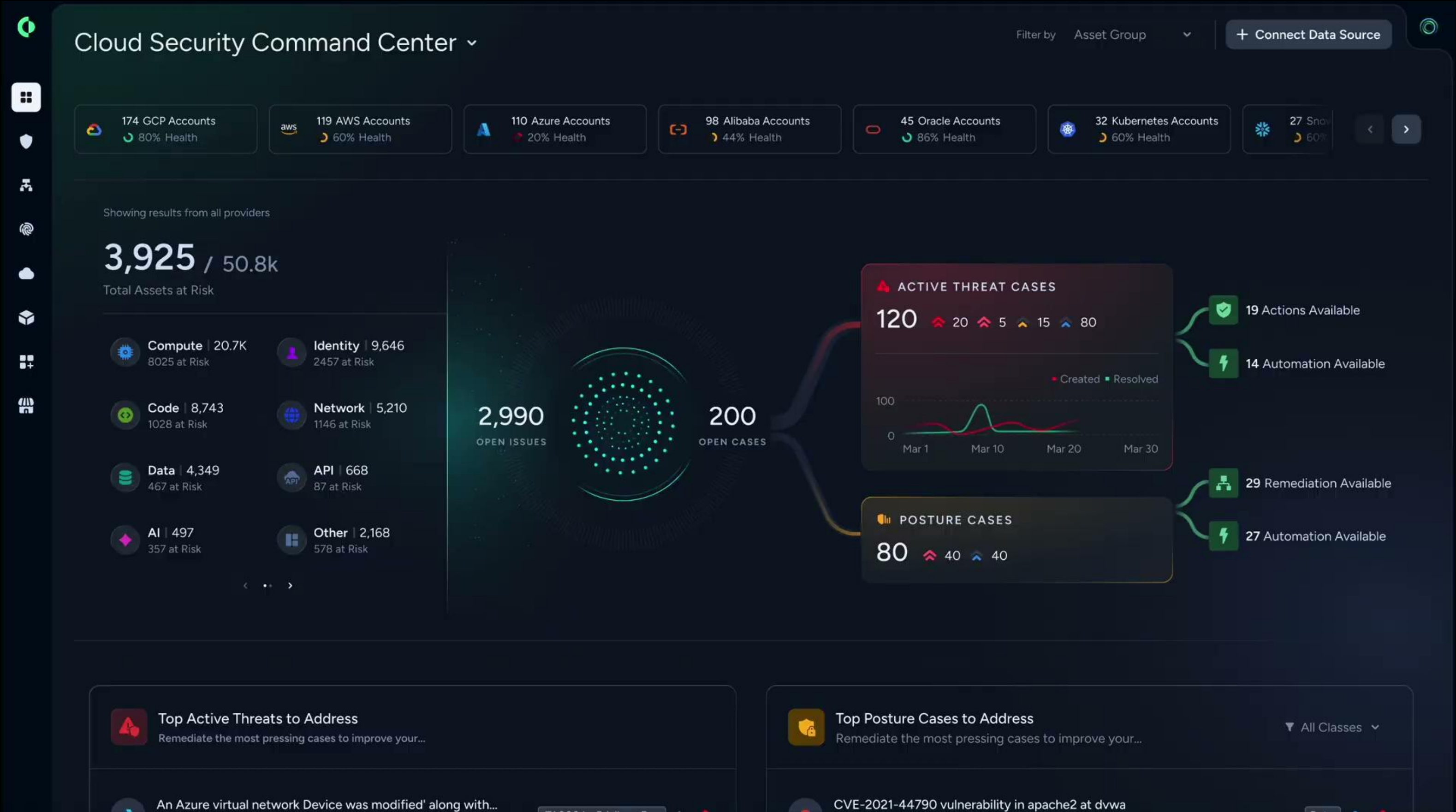


## Cloud Detection and Response

INVESTIGATE &  
RESPOND

Deploy as a standalone cloud security solution or as a SOC extension on top of XSIAM

# Cortex Cloud 2.0 Preview Video



# Thank You

---

[paloaltonetworks.com](https://paloaltonetworks.com)

# ALT SLIDES