paloalto NETWORKS | CORTEX CLOUD

TD SYNNEX Public Sector | DLT

Fix thousands of alerts with 1 action.

A playbook for scaling cloud posture security

Cloud security is under pressure.

In 2024, organizations saw a 388% increase in cloud alerts—a spike driven by rapid adoption of cloud services and the growing complexity of multicloud environments. Security teams are left sorting through thousands of alerts with limited time and resources. Addressing every issue manually isn't realistic, and ignoring them isn't an option.

This cheatsheet offers a practical way forward, with steps to help you reduce alert noise, focus on what matters most, and scale your remediation efforts.

The increase in cloud alerts organizations experienced in 2024.[1]

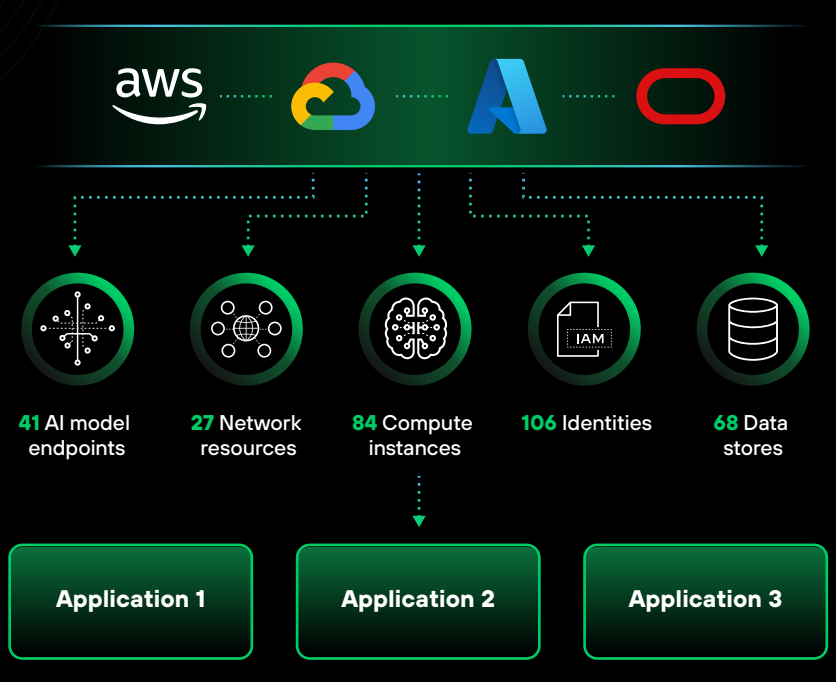
Gain visibility

The cloud is complex, with unknown blind spots that leave your organization open to risk. The first step in reducing that risk is to understand what cloud services are actively running and how they relate.

Agentlessly connect your cloud environment.

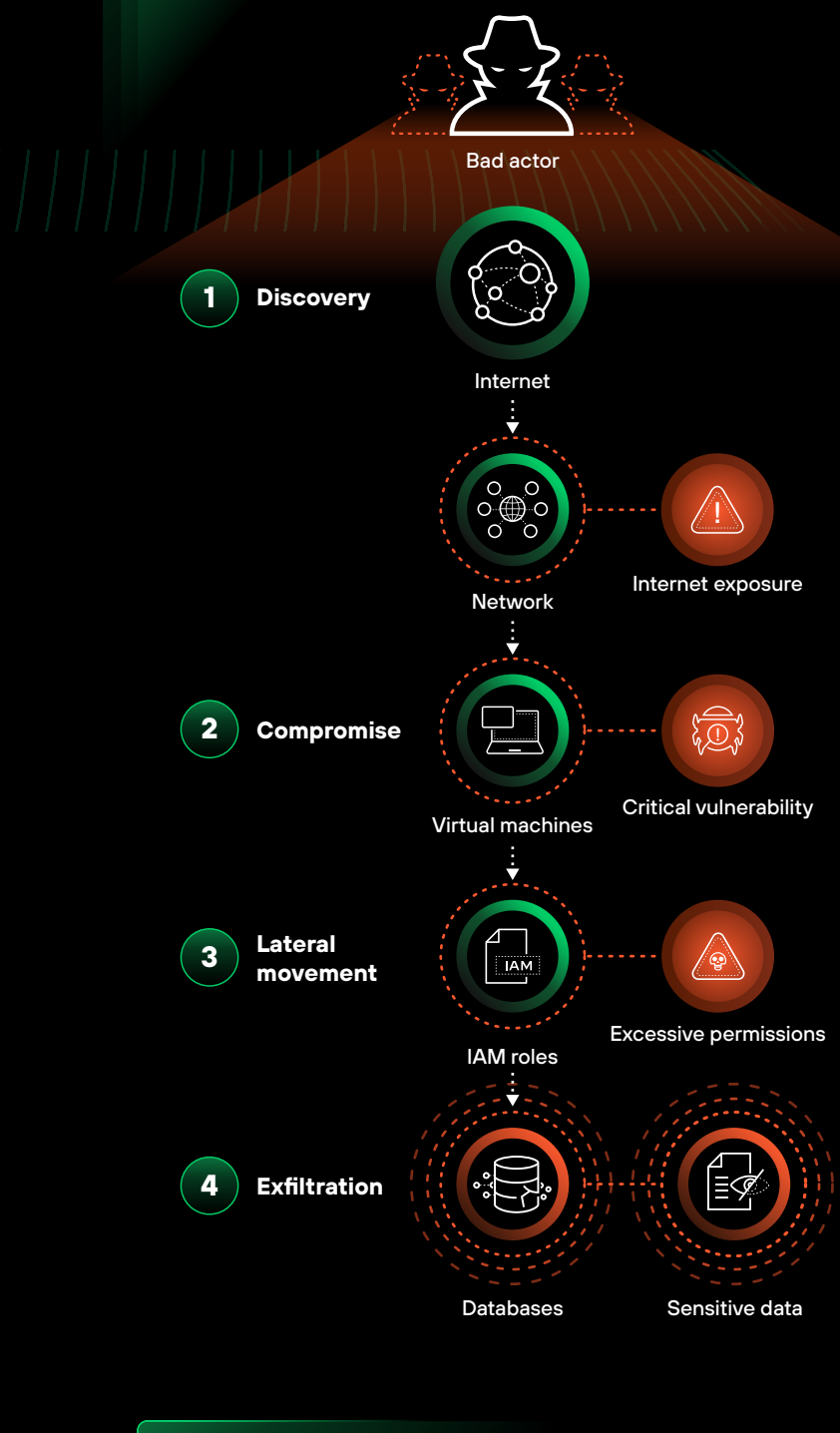
See an inventory of your complete cloud stack.

Gain visibility into all the applications in your cloud inventory.



Focus on critical issues

Not all cloud risks are equally important. Prioritize the ones with the greatest potential for harm using context-based risk analysis and correlation.

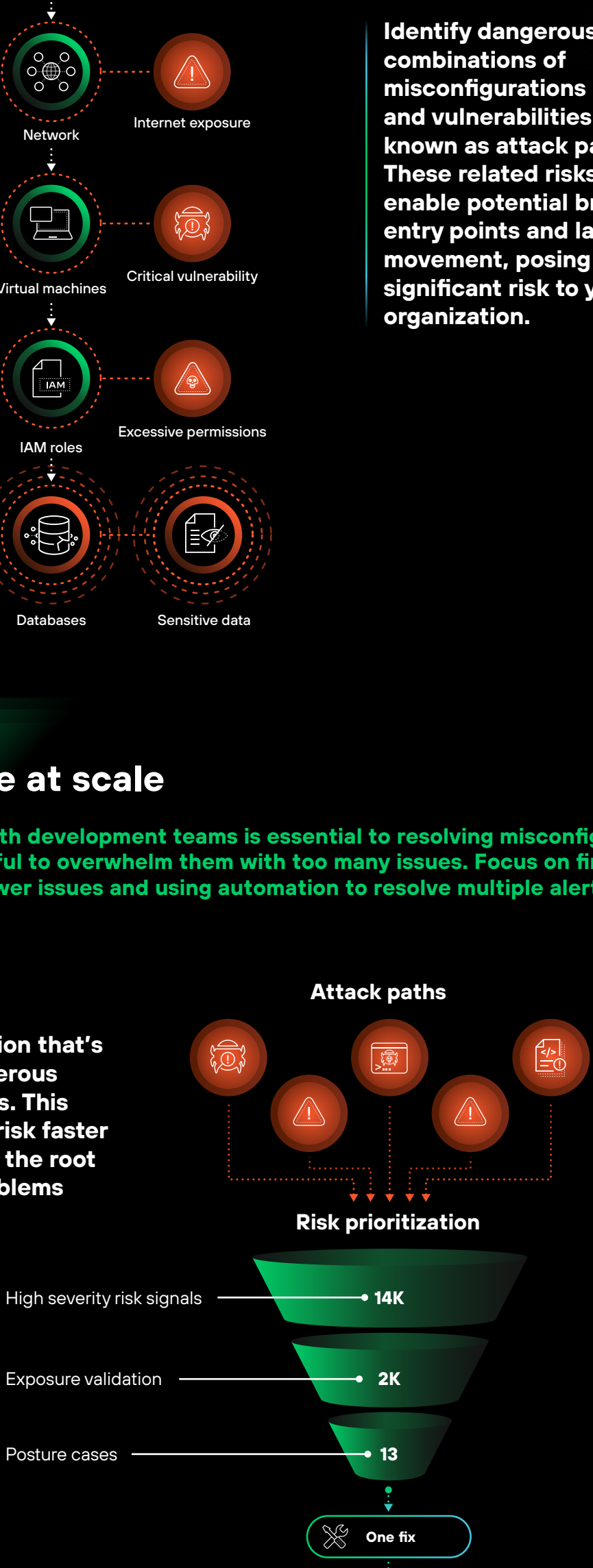


Identify dangerous combinations of misconfigurations and vulnerabilities known as attack paths. These related risks enable potential breach entry points and lateral movement, posing a significant risk to your organization.

Remediate at scale

Collaborating with development teams is essential to resolving misconfigurations, but it's not helpful to overwhelm them with too many issues. Focus on finding ways to send fewer issues and using automation to resolve multiple alerts with a single action.

Address any misconfiguration that's linked to numerous security issues. This helps reduce risk faster by addressing the root of several problems at once.



Leverage playbooks to automate remediation workflows and accelerate responses.

Want to learn more?

Check out the 5 critical requirements to elevate your cloud posture.

Read the guide

[1] Palo Alto Networks Unit 42 Cloud Threat Report article "Cloud Threats on the Rise: Alert Trends Show Intensified Attacker Focus on IAM Exfiltration" published March 2025

paloalto NETWORKS | CORTEX CLOUD | TD SYNNEX Public Sector | DLT