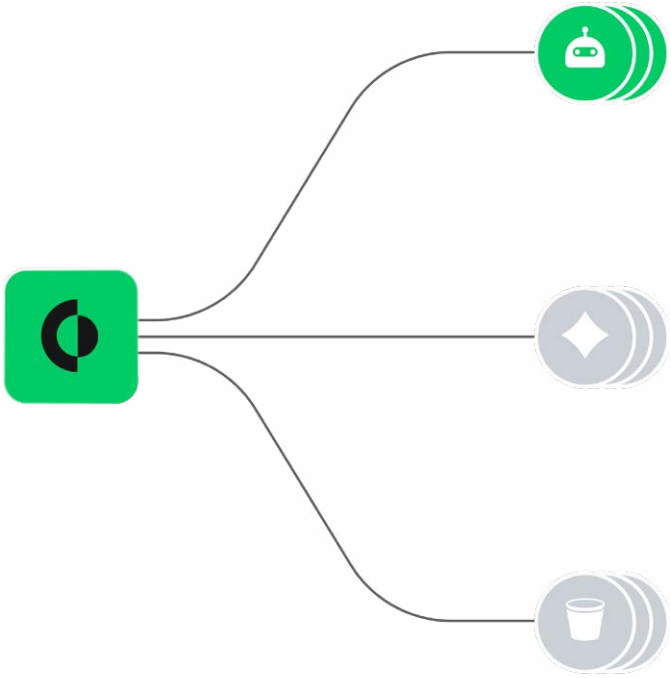
paloalto NETWORKS | CORTEX® CLOUD

Cortex Cloud AI-SPM

Artificial intelligence (AI) is permeating every aspect of modern IT and operations, and you can't afford to ignore the security ramifications. Learn how Cortex Cloud enables you to support innovation, manage risk, and maintain compliance across the increasingly complex AI landscape.



Industry Challenges

AI is at the top of everyone's agenda, and speed is the name of the game. Novel models and implementations are being released at breakneck speed, while organizations are racing to bring new applications to market. However, when AI implementations are poorly governed and lack necessary controls, they can become security time bombs due to risks such as:

- Sensitive data leakage from either insecure supply chains or overly-permissive access schemes
- Unfiltered and unpredictable model output that causes reputational or legal damage to the organizations deploying them
- Noncompliance with either new AI-centered standards and regulations or existing standards such as GDPR

These threats are expected to intensify as AI-powered applications become further embedded into core operations, and even more so as agentic systems that combine multiple models become increasingly popular. As such, security strategies must adapt to a radically different technology landscape to mitigate AI risk while not stifling innovation.

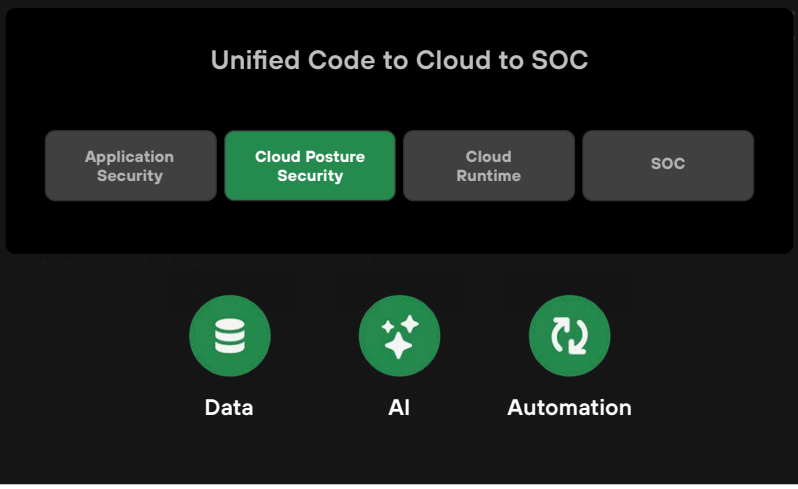
Solution Highlights

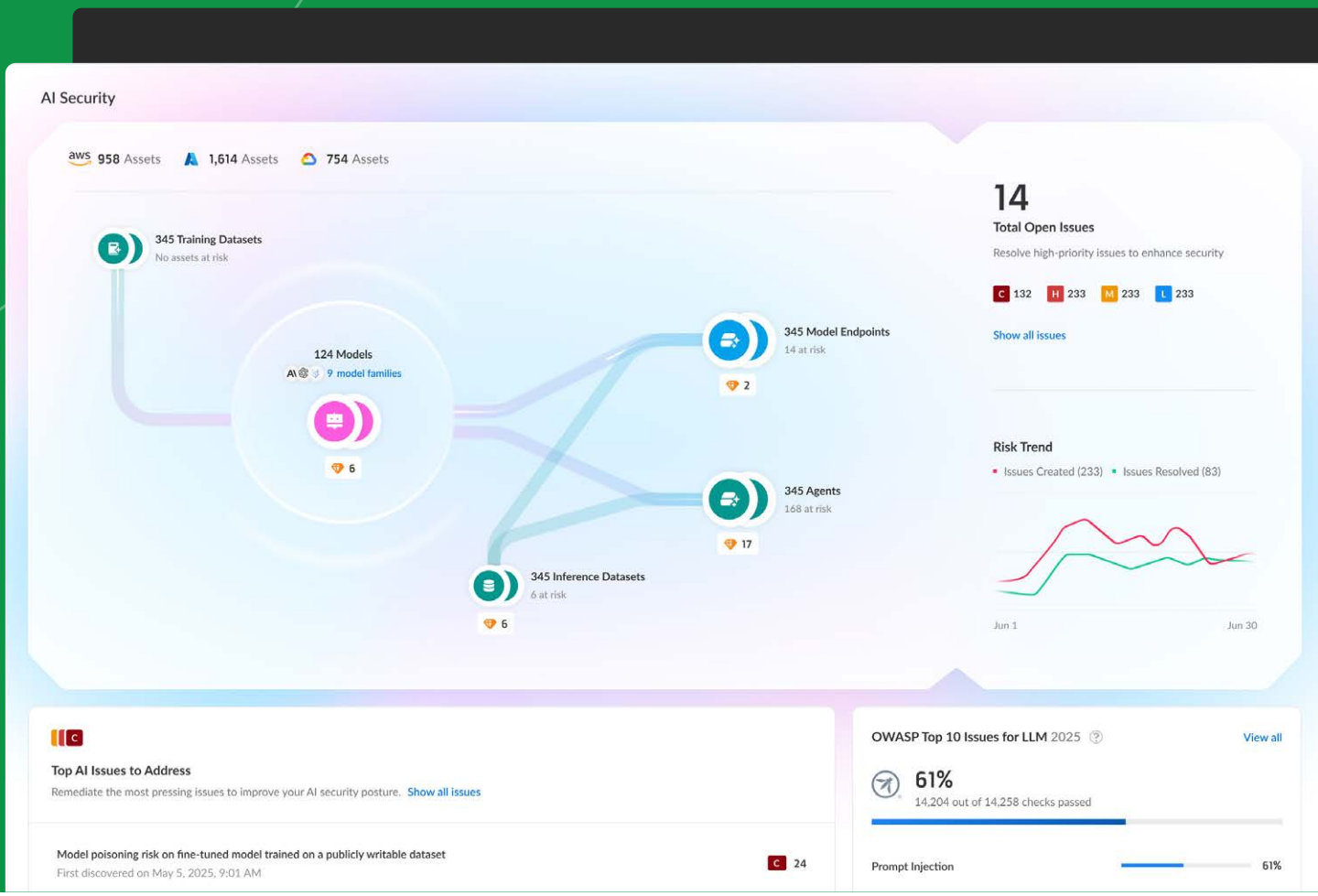
Cortex Cloud offers a complete solution to protect AI-powered applications. The platform provides visibility and risk management across the AI development life cycle – from model evaluation, through training and testing, to deployment in production. This includes unique detection, risk analysis, and response capabilities tailored to AI-specific risks, enabling security and development teams to:

- **See the entire organizational AI picture:** Gain full visibility into AI models, agents, data flows, and infrastructure across your cloud environment.
- **Govern and control:** Implement comprehensive guardrails and controls for AI models in development and production.
- **Tackle AI-specific risk:** Detect misconfigurations, manage permissions, and ensure that proper security measures are in place across the AI supply chain.
- **Monitor risk with end-to-end context:** Track and assess AI-specific risks in real time with full context of the cloud environment and a broader security posture.
- **Align with compliance standards:** Maintain compliance with emerging AI regulations and industry standards such as the OWASP Top 10 for LLMs.

Cortex Cloud is the only unified code to cloud to SOC solution.

Move beyond point solutions. See the full picture of AI in your cloud architecture, and prioritize remediation based on threats to sensitive data and business-critical production systems.





Capabilities Overview

Gaining Visibility into AI Models and Ecosystems

- **Model discovery and inventory:** See which AI models are deployed in your cloud environment – whether through APIs or cloud services such as Amazon Bedrock, or on virtual machines.
- **AI ecosystem insight:** Uncover key components of AI-powered systems – models, agents, endpoints, and the flow of data between them. Identify which data and compute resources are attached to each model.
- **Attack path analysis:** Prioritize risks and misconfigurations based on the threat to sensitive data and the overall context of your cloud environment. Use this knowledge to prioritize scarce remediation resources effectively.

AI visibility helps you answer:

→ Which AI models and/or LLMs are currently being used?

→ Have new models been introduced recently?

→ Which data stores and other cloud resources can AI models access?

Mitigating AI-Specific Risk

- **Detect model misconfigurations and permission issues:** Identify when deployed models are operating without needed guardrails. Understand effective access and the impact of permissions granted to the models' resources.
- **Comply with AI standards and regulations:** Map risks to relevant frameworks such as NIST-AI-600-1 and the OWASP Top 10 for LLM Applications. Receive recommendations for relevant mitigations and apply them by using remediation workflows.
- **Protect the entire supply chain:** Map the dependencies between data, models, and cloud resources to remediate risks such as poisoned datasets or unsanctioned models. Maintain the integrity of your AI bill of materials (AI BOM).

Identify AI-specific threats such as:

→ Unvetted AI models with poor reputations (e.g., on Hugging Face) that are used in development or production

→ Training datasets that are publicly writable, thereby risking data poisoning

→ Guardrails disabled for models in production

Securing the Data that Powers AI

- **Understand how data is used in embeddings and retrieval augmented generation (RAG):** Classify the sensitive data either ingested into vector databases or used in other RAG workflows.
- **Prevent data misconfigurations that put models at risk:** Monitor data before it becomes part of a "black box" model to prevent customer records or unwanted biases from finding their way into applications.
- **Prioritize AI risk based on data risk:** Understand where models are trained on sensitive data (e.g., customer PII) or where AI applications use sensitive data for inference.

Data-centric security allows you to answer questions such as:

→ Which models were trained on sensitive data like PII or PCI?

→ Which external-facing AI applications have access to internal data?

→ Have any vector embeddings been created using proprietary company data?

Better AI Security Through a Unified Platform

Partnering with Palo Alto Networks enables you to enjoy the advantages of our platform-first approach. Integrate your AI security policies into your broader cloud security strategies and benefit from powerful synergistic features across our world-leading suite of cloud security solutions.

Extend your AI security program with features such as:

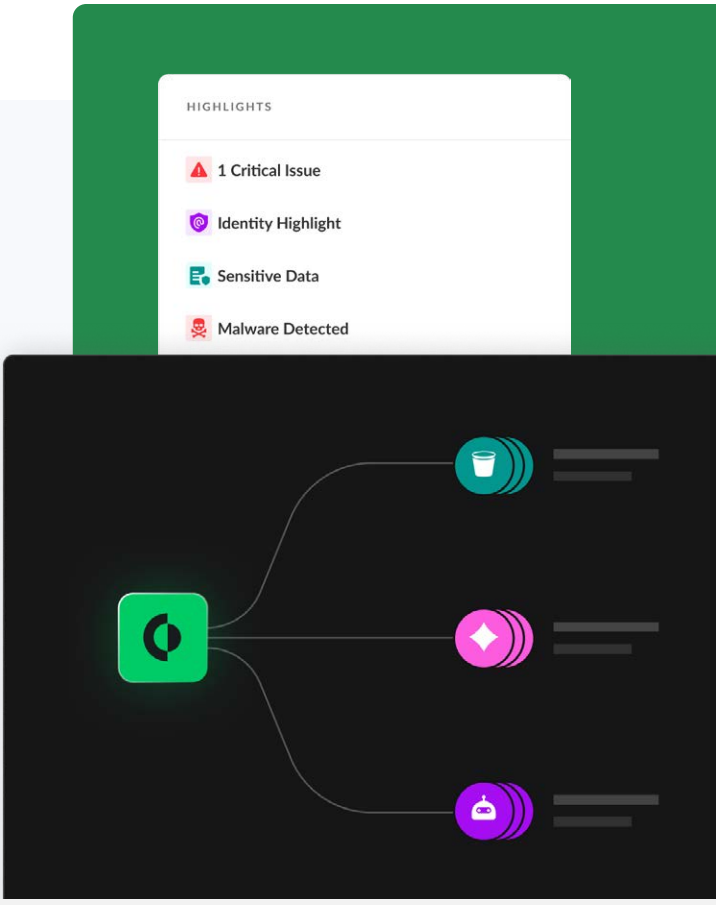
- **Cloud infrastructure entitlement management (CIEM):** See and manage human and nonhuman identities that can access AI resources and sensitive data. Prevent permissions and entitlement sprawl, such as those resulting from microservice environments, and rightsize permissions to AI models without sacrificing development velocity.

- **Data security posture management (DSPM):** Detect and classify sensitive data across cloud environments, including datasets used for AI training or inference. Detect combinations of misconfigurations that create high-priority attack paths.
- **Unified telemetry and data model:** See the full context of applications, workloads, physical infrastructure, and data – all in one place. Understand the way each component interacts with others and the impact of changes on your environment.
- **Graph-based analysis:** Visually examine your environment by using natural language search to quickly receive answers to complex security questions (e.g., Show me every virtual machine running in Google Cloud that is running an AI model and is open to the world).
- **No-code security automation:** Ensure that AI security incidents are handled promptly and according to policy with out-of-the-box templated playbooks featuring thousands of integrations. Create advanced, no-code automations to fix multiple issues simultaneously, increase efficiency, and eliminate risk.
- **Best-in-class detection and response:** Combine AI-based detection, anomaly detection, and behavioral signals to surface high-risk incidents in real time. Enable teams from Dev to SecOps to solve problems together on a single platform.
- **Easy onboarding and setup:** Get to value faster by accessing all your data in one centralized security lake with a common data model. Quickly onboard new data sources and capabilities without manual integration.

About Code to Cloud to SOC Security with Palo Alto Networks

Cortex Cloud, the next generation of Prisma Cloud, merges best-in-class CDR with industry-leading CNAPP for real-time cloud security. Harness the power of AI and automation to prioritize risks with runtime context, enable remediation at scale, and stop attacks as they occur. Bring together your cloud and SOC on the unified Cortex platform to transform end-to-end operations.

Experience the future of real-time cloud security at https://www.paloaltonetworks.com/cortex/cloud.



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

cortex cloud_ds_Cortex Cloud AI-SPM_2025