paloalto NETWORKS | PRISMA® AIRS

Prisma AIRS

Deploy Bravely.

Campaign Playbook for Partners

Table of Contents

Introduction

Empowering Partner Success

This campaign playbook is your guide to a new, urgent, and lucrative market: AI security. As enterprises rapidly adopt AI, they face new, complex threats traditional cybersecurity can't handle. Our solution enables businesses to embrace AI innovation confidently, overcoming security fears and fragmented solutions.

Use this playbook to engage prospects and run joint marketing programs that reinforce the value of your services and Prisma AIRS and position it as the leading AI security platform. This campaign includes:

- Co-brandable digital campaigns on LaunchPad*
- Event Kits
- Customer presentation
- Outreach Sequence

* You can access LaunchPad via the Partner Campaigns page on the NextWave Partner Portal or directly from the LaunchPad Home Page. For login issues, please contact nextwave@paloaltonetworks.com.

Why Run this Campaign

This campaign is about solving critical customer challenges. The market is ripe with opportunities as businesses are in desperate need of a solution that can safely build and deploy AI.

Help your customers “Deploy Bravely” and secure their future in the age of AI.

By leading with Prisma AIRS, you can:

- Expand VM-Series. Position Prisma AIRS to VM-series customers. Upsell AI capabilities and at the sametime renew/expand their VM-Series.
- Capture Net New AI Workloads from existing PANW customers by introducing the API version of Prima AIRS.
- Capture Net New Logos by positioning Prisma AIRS as the beachhead solution to your customer’s footprint in a land and expand motion.

paloalto NETWORKS | PRISMA® AIRS

Solution Overview

Enterprises are adopting AI at speed. They are deploying AI apps and agents across the organization, often without the right security in place - creating new risks to manage. Patchwork of point solutions aren't up to the challenge of securing AI. Organizations need end-to-end security across the AI Lifecycle. With Prisma AIRS, customers can:

Discover their AI ecosystem.
Gain visibility and control over your AI infrastructure, platform and data.

Assess AI risk.
Detect vulnerabilities and risks early, ensuring AI models are safe before deployment.

Protect against threats.
Monitor behaviors in real time to detect anomalies and stop live threats.

Learn More

- Prisma AIRS Customer Presentation
- Prisma AIRS Golden Pitch Deck
- Prisma AIRS Golden Pitch Recording*
- Partner Portal

* Access The Learning Center by going directly to learn.paloaltonetworks.com in your desktop or mobile browser beginning. Visit The Learning Center: Partner Hub - FAQ for for details.

Solution Overview

Prisma AIRS™ is a groundbreaking AI security platform that serves as the cornerstone for robust AI protection. It's designed to secure the entire enterprise AI ecosystem — your applications, your agents, your models, and your data — at every step of the journey. The goal is simple: enable you to deploy AI bravely, without hesitation, and without compromise.

AI Model Security

Scans models for vulnerabilities like tampering, malicious scripts, and deserialization attacks.

AI Red Teaming

Automates penetration testing using an adaptive red team agent that stress-tests AI apps the way a real attacker would.

AI Posture Management

Surfaces risks from excessive permissions, sensitive data exposure, or misconfigurations before they're exploited.

AI Runtime Security

Stop prompt injection, malicious code, toxic content, data leaks, hallucinations, or resource overload in the moment they happen.

AI Agent Security

Protects no-code and low-code AI agents against entirely new threat classes like identity impersonation, memory manipulation, and tool misuse.

Solution Overview

What obstacles are customers faced with?

Compromised AI Deployments & Data Breaches: Without adequate security, AI applications and agents are vulnerable to attacks that can lead to unauthorized access, data breaches (including PII, PHI, and IP), compromised decision-making, and service disruptions (e.g., Model Denial of Service).

Hindered Innovation & Delayed AI Adoption: The fear of security risks, compliance failures, and the complexity of managing multiple point solutions can significantly slow down or even halt AI innovation and deployment initiatives, causing organizations to fall behind competitors.

Fear of Reputational Damage & Compliance Penalties: Security incidents involving AI can lead to severe reputational damage, loss of customer trust, and significant financial penalties due to non-compliance with evolving data privacy and AI security regulations.

Solution Overview

Prisma AIRS directly addresses the critical challenges faced by organizations in their AI journey, enabling them to achieve their goals of safe and confident AI deployment:

Addressing the Expanding Attack Surface: Through its comprehensive five-pillar approach, Prisma AIRS provides specialized protection against the new and evolving AI-specific threats.

Unified Platform & Eliminating Blind Spots: As a single, integrated platform, Prisma AIRS replaces the need for disparate point products.

Delivering Superior Protection Beyond Existing Tools: Prisma AIRS goes far beyond the limited capabilities of traditional NGFWs and native GenAI model guardrails. This empowers customers to confidently deploy complex AI initiatives without fear of advanced attacks or compliance gaps.

Key Differentiators

AI-Native Threat Defense
Specifically designed to counter unique AI threats such as prompt injection, model DDoS, data exfiltration, and malware output from models.

Proactive Red Teaming & Posture Management
Offers automated AI red teaming for pre-deployment vulnerability discovery and continuous posture management for ongoing risk visibility.

Seamless Portfolio Integration
Leverages and integrates with Palo Alto Networks' existing broad security platforms for unified operations and shared threat intelligence.

Cloud Agnostic
Customers can benefit from best-in-class, real-time security to help them protect all users, devices, and data in their network, regardless of location.

Learn more, review Prisma AIRS Positioning Guide

Target Audience

Primary Titles
CIOs

Secondary Titles
CISOs, AI Officers, AI/ML Leaders

Tertiary Titles
Cloud Architects, DevSecOps, AI Security Practitioners, App Builders, Compliance Officers, Digital Transformation Executives, Network Security Teams

Ideal Persona

"Classic"

NETWORK / SECURITY TEAM

*"Cares about **security**"*

CIO/CISO
Gloria

CLOUD SECURITY ENGINEER/ ARCHITECT
Tarak

"App Developers"

APP BUILDERS & APP Sec Teams

*"Cares about **performance**"*

CIO
Nandita

AppSec Lead
Owen

"AI COE"

NEW

AI TEAM

*"Cares about **experience**"*

CAIO
Eric

DATA SCIENTIST/ ARCHITECT
Tiffany

Leverage the Partner-led EBCs, NSDCs and CLARA engagements to align all stakeholders internally. All are critical for success.

Copy Blocks

Tagline: Deploy Bravely

Value Proposition: Prisma AIRS is the industry's most comprehensive AI security platform, providing full visibility and protection across five core layers of AI security. It is designed to give you a clear, consolidated view of your entire AI environment and proactively address risks.

Short (~25 words)

Prisma AIRS secures your entire AI ecosystem. It solves new AI threats, unifying fragmented security. Deploy AI bravely, confidently innovating with end-to-end protection.

Medium (~50 words)

Prisma AIRS is the comprehensive AI security platform, solving fragmented defenses and new AI threats. It protects your entire AI ecosystem across five pillars, enabling you to deploy AI bravely. Gain full visibility, proactive detection, and real-time protection to innovate with confidence.

Long (~150 words)

Enterprises face unprecedented AI threats and fragmented security. Traditional tools fail to protect against prompt injection, model tampering, and agent-specific attacks. Prisma AIRS is the unified, comprehensive platform that solves these challenges. It provides end-to-end security across five pillars: AI Model Security, AI Posture Management, AI Red Teaming, AI Runtime Security, and AI Agent Security. With best-in-class threat detection, adaptive red teaming, and unparalleled protection against 25+ prompt injection types, Prisma AIRS eliminates blind spots and ensures compliance. Deploy AI bravely, knowing your entire AI ecosystem is secure from development to runtime.

Campaign Toolkit

Your step-by-step digital campaign execution guide

We created this campaign toolkit to make it easy for you to promote Palo Alto Networks through the LaunchPad Platform or through your own marketing channels. Launch your digital campaign:

Option A (recommended)
Use LaunchPad* to send quick co-branded campaign emails to your own prospect/nurture lists and share co-branded social media posts across your channels.

- Access Prisma AIRS content offers in the LaunchPad Asset Library*.
- Start building your Prisma AIRS email campaigns* and social campaigns*.
- Create a co-branded Prisma AIRS microsite through LaunchPad for content syndication on your website. Use this link to execute the content syndication microsite*.

Option B
Use your organization's email/CRM platform or social channels. Customize the campaign graphics with your logo and personalize the email message.

- Campaign Email, Social Media, Landing Page copy and graphics

** Links to LaunchPad requires login to LaunchPad on the NextWave Partner Portal. To request your account, go here. If you have problems logging in, email nextwave@paloaltonetworks.com.* For immediate guidance, watch the video and download the Quick-Start guide.

Campaign Content Offers

Use LaunchPad to send co-branded email campaigns* and social campaigns* for the content offers below. Or leverage the email and social copy provided below to send through your own CRM platform.

A Simplified Guide to MCP Vulnerabilities

Download Report
Email, LP and Social Copy
LaunchPad

An LLM Security Guide for CIOs

Download Report
Email, LP and Social Copy
LaunchPad

Is Your GenAI Environment Secure?

Download Report
Email, LP and Social Copy
LaunchPad

Securing GenAI Report

Download Report
Email, LP and Social Copy
LaunchPad

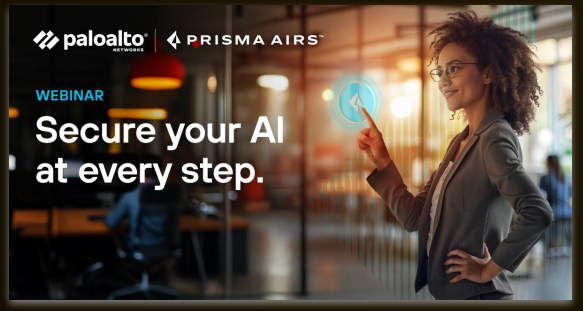
** Links to LaunchPad requires login to LaunchPad on the NextWave Partner Portal. To request your account, go here. If you have problems logging in, email nextwave@paloaltonetworks.com. For immediate guidance, watch the video and download the Quick-Start guide.*

Event Kits

AI Security Executive Roundtable

Run this program to engage **CXOs** with peer to peer discussions about AI Security and the need for a unified AI security platform that discovers, assesses, and protects how AI is both used and built across the enterprise. Includes Prisma AIRS Golden Pitch Deck and Recording.

EVENT KIT



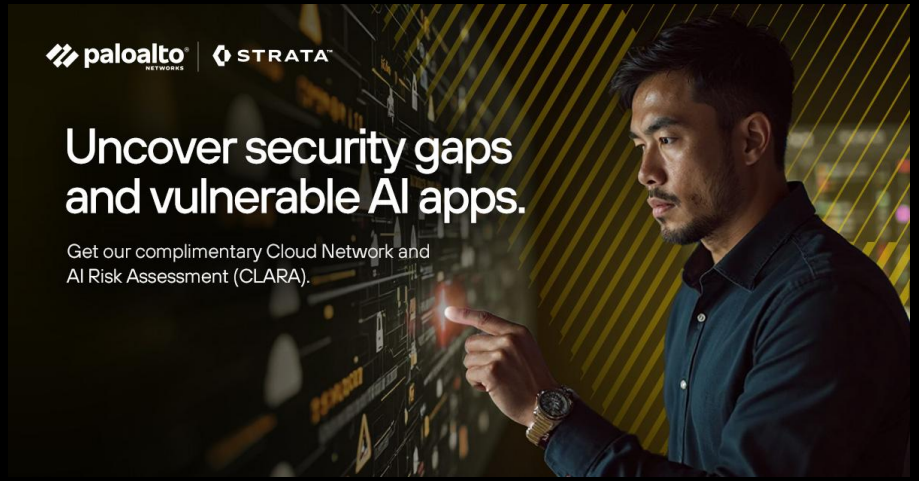
Prisma AIRS Event Kit

See Prisma AIRS in action.

Run this event to provide a high-level overview of Prisma AIRS. Introduce Prisma AIRS and demonstrate how our solution can help your customers secure their AI innovations.

EVENT KIT

CLOUD AND AI RISK ASSESSMENTS (CLARA)



CLARA is an expert-led, complimentary suite of three assessments providing actionable insights into your customers' cloud and AI risk. This powerful sales tool, the cloud version of our existing SLR (Security Lifecycle Review), helps engage customers and highlight critical security needs.

Why offer CLARA to your clients?

- Enhance customer engagement
- Increase win rate
- Higher deal value
- Accelerate sales cycle
- Expand opportunity to the cloud
- Capture new AI opportunities
- Validate firewall value
- Identify whitespace

LEARN MORE

CAMPAIGN KIT

Additional Resources

Marketing Resources

- Prisma AIRS Customer Presentation
- Outreach Sequence
- Prisma AIRS Interactive Demo & Campaign Kit
- Software Firewall Selector Tool & Campaign Kit
- Animated explainer video | MP4 Link
- Network Security Design for Cloud
- Partner-led EBC

Share with Customers

- PANW microsite highlighting common AI security risks that are mitigated by Prisma AIRS capabilities
- Webcast series with episodes released weekly
- Securing AI's Frontlines Whitepaper

Analyst Reports

- Gartner Market Guide for AI Trust, Risk and Security Management
  Report | Share with customers

Sales Enablement

- Prisma AIRS Golden Pitch Deck
- Prisma AIRS Golden Pitch Recording
- Prisma AIRS Partner Portal
- Prisma AIRS Positioning Guide

Training on The Learning Center*

- Sales: Prisma AIRS: The Comprehensive Platform for AI Security
- Technical: Prisma AIRS SONAR video

* Access The Learning Center by going directly to learn.paloaltonetworks.com in your desktop or mobile browser beginning. Visit The Learning Center: Partner Hub - FAQ for for details.