Service description document: Prisma AIRA – AI Runtime Security (Managed SaaS)

Prisma AIRS – AI Runtime Security (Managed SaaS)

Service overview

Prisma AIRS is a cloud-delivered security platform designed to protect the full AI ecosystem across cloud environments. It secures AI applications, models, data and agents by combining real-time runtime protection, posture management and automated red teaming. The service helps prevent prompt injection, data leakage and malicious or unsafe AI outputs to enable trusted AI deployments.

The service is delivered as a subscription-based Software as a Service (SaaS) offering, with enterprise-grade security, availability and support provided by Palo Alto Networks, and optional managed support services available from the supplier.

What the service provides

Prisma AIRS is focused on protecting AI systems in use, not just traditional infrastructure. It provides visibility of AI assets, enforcement controls at runtime, and continuous assessment to identify and reduce security and compliance risk associated with AI models, applications and autonomous agents.

Prisma AIRS provides:

- Discovery and inventory of AI assets and services across cloud environments
- Runtime controls to detect and block AI-specific threats such as prompt injection
- Protections to prevent sensitive data leakage and preserve intellectual property
- Posture management to identify misconfigurations and risky AI exposure
- Automated red teaming to proactively test AI systems and reduce risk before exploitation
- Detection of hallucination and toxic or unsafe content patterns
- Controls to secure autonomous agents and agentic workflows
- Integration approaches suitable for security-as-code and automated workflows

The service can be adopted as a standalone AI security layer or used as an extension to existing Palo Alto Networks security services to support unified control and orchestration.

Service features

Prisma AIRS includes the following core features:

- AI asset discovery and inventory
- AI runtime firewall
- Autonomous AI red teaming
- Deep AI model scanning
- AI agent security
- AI posture management (AI-SPM)
- Enterprise data loss prevention (DLP)
- Hallucination and toxic content detection
- Security-as-code integration
- Model Context Protocol threat detection

Service benefits

Prisma AIRS helps organisations to:

- Accelerate safe AI adoption
- Eliminate AI blind spots through discovery and inventory
- Reduce risk proactively through continuous assessment and red teaming
- Protect against emerging and zero-day AI attacks
- Preserve intellectual property by preventing data leakage
- Support regulatory and governance compliance
- Maintain operational continuity through runtime threat prevention
- Improve trust in AI outputs through detection and enforcement controls
- Secure autonomous agents and agentic workflows
- Simplify oversight through unified management

Service scope and dependencies

Prisma AIRS can be deployed as a standalone service or as an extension to Prisma Access and Next-Generation Firewalls by adding specialised AI runtime protection. It integrates with Strata Cloud Manager for unified orchestration and uses Advanced WildFire threat intelligence to secure AI models, applications and agents against prompt injection and data leakage.

The service is delivered as a public cloud SaaS offering and requires internet connectivity. It relies on appropriate access to relevant AI applications, environments or integration points to enable discovery, policy enforcement and monitoring.

Customisation and configuration

Organisations can tailor the service to their requirements by configuring AI security controls and policies, including:

- AI security profiles that set detection and response actions (for example block, alert or mask)
- Custom topics to detect organisation-specific sensitive data and secrets
- Model groupings and policy application across different AI assets and services
- Integration patterns to support security-as-code workflows

Configuration and customisation can be performed through the web-based management interface and supported management APIs, with role-based access controls limiting policy changes to authorised administrators.

Access and user experience

Prisma AIRS is administered through Strata Cloud Manager, a web-based centralised interface used to configure controls, monitor security posture and review findings. The service aligns with WCAG 2.1 AA principles and includes accessibility considerations such as keyboard navigation support, screen reader labelling (ARIA) and appropriate colour contrast for alert visibility. A natural-language interface can support accessibility by enabling users to query security data using text-based commands rather than navigating dense menus.

Support and service management

The service includes vendor-backed support with defined response targets based on incident severity. Support is provided through online ticketing and can include phone and web chat options depending on the support level selected.

Support response targets include (by support tier):

- **Platinum:** S1 <15 minutes, S2 <30 minutes, S3 <2 hours, S4 <4 hours
- **Premium:** S1 <1 hour, S2 <2 hours, S3 <4 hours, S4 <8 hours
- **Standard (Mon–Fri 7am–6pm):** as per Premium response targets within standard hours

Technical account management is available as an optional add-on and may be delivered via professional services capability where required.

Availability and resilience

Prisma AIRS is delivered via a globally distributed cloud platform designed for resilience through redundancy, fault tolerance, dynamic routing and proactive monitoring. The service aims for high availability and includes service credit mechanisms where availability commitments are not met. Outages and service status updates are communicated via status portals and automated notifications (email, SMS and console) and supported by standard support channels.

Security and data protection

Security is embedded throughout the service design, including:

- Encryption protections for data in transit using modern cryptographic protocols
- Segmentation and firewall controls supporting secure service operation
- Continuous monitoring and threat detection using Precision AI, machine learning and Unit 42 intelligence
- Formal vulnerability management including scanning, prioritisation and patching cycles

- Regular penetration testing and independent verification through recognised audit frameworks

The service supports strong identity and access controls, using Zero Trust principles and least privilege access. Management interfaces and support channels are protected using MFA-enabled portals and access restrictions.

Customers can export relevant service data such as logs and reports using the management console. Supported export formats include CSV, JSON and PDF. At contract end, customers can retrieve data and transition to alternative solutions with vendor assistance if required.

Onboarding and offboarding

Onboarding is supported through documentation, training materials, step-by-step guidance and optional professional services. Documentation may be provided through online help, knowledge base content and video tutorials.

At contract end, services cease in line with contract arrangements. Customers can export data (including logs and reports) and complete transition or migration activities, with vendor assistance available where required. Any additional support beyond standard contract deliverables may be chargeable.

Commercial model

Prisma AIRS is provided on a subscription licensing model, typically priced per user or by the applicable service consumption basis for the AI security capability. Pricing includes access to the SaaS platform and vendor support aligned to the selected support level.

Optional enhancements, including premium support tiers, technical account management and professional services support, may be available at additional cost.

Out of scope

The following are not included unless explicitly agreed:

- Provision of underlying AI models or AI application development
- Hosting of customer applications or customer production platforms
- End-user support/helpdesk services
- Customer network connectivity services
- Custom software development beyond published service capabilities

business
secure, managed solutions for all.