



Service description document: Prisma Access – Cloud-Delivered Secure Access Service (iSaaS)

Service overview

Prisma Access is a cloud-based security service that enables organisations to securely access applications and data from any location. It delivers a consistent security posture for users, devices and applications by enforcing Zero Trust access controls and cloud-delivered security services, regardless of where users are working.

The service provides advanced protection capabilities including threat prevention, secure web access, data loss prevention and encrypted connectivity, helping organisations protect against modern cyber threats while supporting remote and hybrid working models.

When purchasing Prisma Access through eir Business, buyers receive:

- Access to the Palo Alto Networks Prisma Access cloud platform
- The relevant Prisma Access service entitlements required to enable the service
- Ongoing platform updates and enhancements delivered by Palo Alto Networks
- Access to vendor-defined service levels and availability commitments
- Additional support and service coordination provided by eir Business

Service capabilities

Prisma Access provides the following core capabilities as part of the service:

- Zero Trust Network Access to applications and services
- Cloud-delivered firewall and secure web gateway functionality
- Cloud Access Security Broker (CASB) controls for SaaS applications
- Enterprise data loss prevention
- Advanced threat prevention and inspection
- Internet of Things (IoT) security visibility
- Remote browser isolation for unmanaged devices
- Autonomous digital experience management
- Global scalability and resilience through distributed cloud points of presence

These capabilities are delivered from the cloud and managed through a centralised web-based management interface.

Service benefits

Key benefits of the service include:

- Improved overall security posture
- Consistent security enforcement regardless of user location
- Reduced risk of initial compromise (“patient zero”)
- Improved visibility and control of shadow IT
- Prevention of data leakage
- Faster detection and response to security incidents
- Future-proofed security architecture
- Enhanced visibility of blind spots across users and applications
- Secure access for unmanaged or third-party devices
- Improved end-user experience

Integration and extensions

Prisma Access can be used as a standalone service or as an extension to other Palo Alto Networks services.

Where required, the service integrates with:

- Next-Generation Firewalls (NGFW)
- Prisma SD-WAN for unified networking
- Prisma Browser for unmanaged device security
- Cortex XSOAR for automated response
- Supported third-party SIEM platforms and ServiceNow

This allows organisations to extend existing security investments into a cloud-delivered secure access model.

Service delivery model

Prisma Access is delivered as a public cloud service.

The underlying cloud infrastructure, platform operation and core service availability are provided by Palo Alto Networks.

eir Business acts as the reseller and provides additional support, service coordination and escalation management.

Availability and resilience

The service is designed for high availability and resilience through:

- A globally distributed cloud architecture
- Redundant points of presence
- Fault-tolerant design
- Dynamic routing and traffic optimisation
- Proactive monitoring

The service aims for 99.99% availability.

Support and service management

Support for Prisma Access is delivered through defined support tiers, which may include:

- Email and online ticketing support
- Phone support
- Web-based support channels
- Optional onsite support

Vendor support response times are available across Standard, Premium and Platinum tiers, with defined response targets for critical, high, medium and low severity incidents.

eir Business provides additional service coordination, support management and escalation to Palo Alto Networks where required. A Technical Account Manager is available at additional cost through professional services.

Security and data handling

Prisma Access is designed and operated in line with recognised security standards and best practices.

Key principles include:

- Customer data remains under customer ownership and control
- Secure encrypted communications between users and the service

- Controlled access to management interfaces
- Logging, monitoring and audit capabilities
- Secure handling of customer data throughout the service lifecycle

Data export and reporting capabilities are available through the management interface in common open formats such as CSV, JSON and PDF.

Service constraints and requirements

To use the service, buyers require:

- Supported end-user devices and operating systems
- Internet connectivity

The service depends on network connectivity to the cloud platform and planned maintenance windows may apply.

End of contract and data portability

At the end of the contract:

- Services are terminated or renewed as agreed
- Customers can export logs, reports and relevant data
- Data migration and transition assistance may be provided
- Vendor assistance is available where required

Commercial model

Prisma Access is priced using a licence-based model, with pricing determined by the required service entitlements and service tier.

Pricing includes:

- The Prisma Access service entitlements
- Access to the cloud platform
- Vendor-defined service levels and availability commitments

Additional support levels, professional services and a Technical Account Manager are available at additional cost.

