Service description document: Cloud-Delivered Security Services (CDSS) (Managed SaaS)

Cloud-Delivered Security Services (CDSS) (Managed SaaS)

Service overview

Cloud-Delivered Security Services (CDSS) are subscription-based, cloud-delivered security capabilities that extend protection against advanced threats across network environments. CDSS provides specialised services such as malware analysis, web security and DNS protection, sharing real-time threat intelligence to help deliver consistent prevention for HQ, branches and remote locations.

What is included:

- Subscription licensing for Palo Alto Networks Cloud-Delivered Security Services (CDSS)
- Cloud-delivered protection modules (selected per requirement), including: Advanced Threat Prevention, Advanced URL Filtering, Advanced WildFire, DNS Security, Enterprise DLP, IoT Security and SaaS Security
- Unified policy and operational management through a central management interface (for example Strata Cloud Management or Panorama, depending on the connected platform)
- Vendor support options (Standard, Premium or Platinum)
- Optional eir Business professional services for onboarding, policy configuration, integrations and optimisation (time and materials)

Service features

- Advanced Threat Prevention
- Advanced URL Filtering
- Advanced WildFire (automated sandboxing)
- DNS Security
- Enterprise Data Loss Prevention (DLP)
- IoT Security
- SaaS Security
- Artificial Intelligence for IT Operations (AIOps)
- Unified Management
- Real-time Reporting

Service benefits

- Eliminates known and zero-day exploits without impacting network performance
- Boosts productivity by blocking access to dangerous websites
- Secures operations against unknown malware using automated sandboxing
- Stops data exfiltration and neutralises botnet threats quickly
- Prevents accidental sensitive data leaks and protects organisational reputation
- Protects unmanaged devices to maintain operational uptime
- Helps control unauthorised application use and reduce shadow IT
- Predicts and prevents network disruptions before they impact users

- Streamlines security policy updates across locations from one console
- Improves decision-making with instant visibility into network threats

Service scope and dependencies

CDSS is designed as an add-on service that extends Palo Alto Networks platforms such as Next-Generation Firewalls (NGFW), Prisma Access (SASE) and VM-Series virtual firewalls. It integrates directly with these platforms to provide additional cloud-delivered security layers (for example URL filtering, DNS security and threat prevention) across supported network environments.

Customisation and configuration

Buyers can define and tailor security policies, controls and reporting to suit their requirements. Configuration is typically performed via the management interface and can include segmentation, access controls, policy tuning and integration with wider security and IT operations tooling. eir Business can provide optional professional services support (time and materials).

Access and user experience

CDSS is administered via a web-based management interface, including Strata Cloud Management and/or Panorama (depending on the underlying platform in use). This provides centralised configuration, monitoring and reporting.

API and integrations

APIs can be used to support configuration management, user provisioning, reporting/analytics, integrations and monitoring/alerting workflows (subject to product capabilities and role-based permissions). Vendor API documentation is available.

Support model

Support is delivered via vendor support plans (Standard, Premium or Platinum) and can be complemented by eir Business services if required.

Vendor response targets (by plan):

- **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 (UK time), aligned to Premium targets above

A Technical Account Manager is available as an additional service (typically delivered via professional services).

Onboarding and implementation

Buyers can start using CDSS through vendor documentation, step-by-step guides, support and training resources. Optional eir Business professional services can support onboarding, policy configuration and integrations (time and materials).

Service availability and resilience

The underlying cloud services are designed for resilience using global points of presence, redundancy, fault tolerance, dynamic routing and proactive monitoring. Outages and service status may be communicated through a status page/portal and automated notifications (for example email/SMS/console), alongside support channels.

Where applicable (depending on which CDSS-backed platform is used), availability commitments and service credits are defined in the relevant Palo Alto Networks service level agreements (for example Cloud NGFW for AWS, Cloud NGFW for Azure and Prisma SD-WAN).

Security and data protection

- Data-in-transit protections may include TLS (v1.2+), IPsec/TLS VPN gateways, and segmentation/firewall controls (depending on deployment and connected platform).
- Data-at-rest protections follow vendor platform controls, including encryption of physical media and vendor-defined controls where applicable.
- Security governance and operational processes align to the vendor's security framework and published trust resources.

Data export and reporting

Buyers can export logs, reports and relevant service outputs via management consoles and/or APIs. Typical export formats include CSV, JSON and PDF (where supported). Data import/export formats may include CSV, JSON and XML (where supported by the platform and integration approach).

Commercial model

- **Primary:** subscription licensing for CDSS modules/capabilities (term-based)
- **Options:** vendor support plan selection (Standard/Premium/Platinum)
- **Optional:** eir Business professional services (time and materials) for onboarding, policy design/tuning, integration and optimisation

End of contract

At contract end, services cease unless renewed. Buyers can export logs/reports and complete transition activities in line with operational requirements. Optional vendor and/or eir Business assistance can be provided for data retrieval, migration and transition support (additional cost).

Service constraints

- Internet connectivity is required for access to cloud-delivered capabilities, updates and support.

- CDSS is typically consumed as an extension to supported Palo Alto Networks platforms (for example NGFW, VM-Series and Prisma Access).
- Planned and emergency maintenance windows may apply in line with vendor service terms and platform-specific SLAs.


business
secure, managed solutions for all.