

Service Definition: Managed Security Services (Lot 3)

Category: Security Services & Cloud Support

Primary Vendors: Palo Alto Networks, Fortinet.

1. Service Overview

We provide comprehensive 24/7 managed security support for private, public, and hybrid cloud environments. Our service focuses on the lifecycle management of Palo Alto Networks (Next-Generation Firewalls, Prisma SASE) and Fortinet (FortiGate, Security Fabric) ecosystems. We act as a specialized technical partner, ensuring your security posture is resilient, compliant, and optimized against evolving cyber threats.

2. Service Features

- **Managed Firewall Service:** 24/7 proactive monitoring and administration of Palo Alto and Fortinet estates.
- **Threat Hunting & Prevention:** Advanced AI-driven threat detection using Cortex XDR or FortiGuard.
- **Zero Trust Implementation:** Design and enforcement of Zero Trust Network Access (ZTNA) and micro-segmentation.
- **Security Policy Optimization:** Continuous auditing and hardening of firewall rules to reduce the attack surface.
- **Vulnerability Management:** Regular scanning and patching of security infrastructure to prevent exploitation.
- **Secure Connectivity:** Management of high-availability SD-WAN, IPSec VPN, and GlobalProtect/FortiClient remote access.
- **Incident Management:** Rapid response to security alerts with defined SLA-based mitigation.
- **Compliance Reporting:** Automated reporting aligned with NCSC, Cyber Essentials Plus, and ISO27001 standards.
- **Change Management:** Secure, ITIL-aligned processing of all firewall configuration changes.
- **Log Management & Analytics:** Centralized logging and analysis using Panorama or FortiAnalyzer.

3. Service Benefits

- **Enhanced Protection:** Leverages market-leading threat intelligence to stop advanced malware and lateral movement.
- **Reduced Business Risk:** Minimizes downtime and data breach potential through proactive 24/7 monitoring.
- **Cost Predictability:** Fixed-price managed service removes the need for expensive in-house 24/7 security teams.
- **Regulatory Compliance:** Ensures your cloud network meets strict security and data protection standards.
- **Operational Efficiency:** Centralized management of complex multi-vendor security environments via a single partner.
- **Expert Technical Assurance:** Direct access to certified Palo Alto and Fortinet engineers for complex troubleshooting.
- **Accelerated Deployment:** Faster rollout of security policies using automated "Infrastructure as Code" (IaC) templates.

- **Improved Visibility:** Deep granular insights into network traffic, application usage, and user behaviour.
- **Scalable Security:** Easily extend security policies from local data centres to multi-cloud environments.
- **Business Continuity:** High-availability designs ensure security services remain resilient during infrastructure failures.

4. Onboarding and Implementation

Our 15-day onboarding process ensures a smooth transition to managed support:

- **Security Audit:** We perform a Best Practice Assessment (BPA) to identify current gaps in your configuration.
- **Connectivity Setup:** Establishment of secure, encrypted links for our management of your Panorama or FortiManager controllers.
- **Baseline Documentation:** Creation of a detailed "as-is" configuration state and risk register.
- **SLA Activation:** Final handover and commencement of 24/7 proactive monitoring and incident response.

5. Offboarding and Exit Strategy

We ensure zero vendor lock-in through a structured exit process:

- **Documentation Export:** Provision of all firewall configurations, policy sets, and topology diagrams in PDF/ODF.
- **Credential Decommissioning:** Secure revocation of our management access and purging of administrative accounts.
- **Final Knowledge Transfer:** Detailed briefing for your internal team or new provider to ensure service continuity.

6. Service Constraints

- **Physical Hardware:** Buyers must provide or separately procure physical firewall appliances (Lot 3 is support-only).
- **Vendor Licensing:** Active support subscriptions (e.g., FortiCare, PAN-DB) must be maintained by the buyer.
- **Remote-First:** Standard management is provided remotely; on-site attendance is subject to additional agreement.