



Service description document: VM-Series NGFW (Managed SaaS)

VM-Series NGFW

Service overview

VM-Series Next-Generation Firewall is a virtualised firewall service that provides consistent threat prevention and policy enforcement across public and private cloud environments. It uses machine learning to identify applications, control user activity, and block known and unknown threats, helping secure virtualised workloads and data with consistent security policies.

What the service provides

Buyers purchase a subscription licence to use VM-Series NGFW in their chosen cloud or virtual environment, plus access to vendor software updates and (where selected) vendor support services. Optional additional services (such as Technical Account Manager support and professional services) can be added.

Service features

- Application-based policy enforcement (App-ID)
- User identification and control (User-ID)
- Advanced Threat Prevention (ATP)
- Zero Trust segmentation and micro segmentation
- Machine learning powered WildFire sandboxing
- Advanced URL filtering
- Enterprise data loss prevention (DLP)
- Automated scaling and provisioning
- GlobalProtect for secure remote access

- Centralised management via Panorama or Strata Cloud Manager

Service benefits

- Consistent security posture across hybrid environments
- Instant threat prevention for known and unknown risks
- Improved operational efficiency through automation
- Faster time-to-protection for new workloads
- Lower total cost of ownership through cloud-native scale
- Reduced risk of lateral movement with segmentation
- Automated compliance and governance support
- Cloud-native agility for scaling up or down
- Fewer blind spots across virtualised estates
- Secure migration to cloud environments

Service scope and dependencies

VM-Series NGFW extends next-generation firewall capabilities to virtualised and cloud environments. It integrates with Cloud-Delivered Security Services (where licensed) including Advanced WildFire, DLP, and IoT Security, and is managed via Panorama or Strata Cloud Manager. It can also extend security to remote users through GlobalProtect.

Constraints and dependencies

- Internet connectivity is required.
- Deployment relies on appropriate integration and data ingestion with the target environment.

System requirements

- Supported devices / environments
- Operating system requirements for the chosen deployment model
- Internet connectivity

Customisation and configuration

Administrators can define and tailor security policies, access controls, and network segmentation, and integrate the service with relevant ecosystem tooling and workflows.

Access and user experience

VM-Series NGFW is managed through the Strata Cloud Management console (web-based) for centralised configuration and monitoring (and/or via Panorama, depending on deployment choices).

The platform has been tested with assistive technologies and supports keyboard-only navigation and screen readers through ARIA labelling and accessibility-focused design practices (details available via vendor accessibility reporting on request).

Support and service management

Support channels

Support is provided via online ticketing, with options for phone and web chat support depending on the support package selected.

Support response targets (by severity)

- **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):** response targets align with Premium

A Technical Account Manager is available at additional cost and is typically delivered as part of professional services.

Availability and resilience

The service is designed for resilience using global points of presence, redundancy, fault tolerance, dynamic routing, and proactive monitoring. Target availability is **99.99%**, supported by a service credit mechanism where applicable.

Service status and outage communications are provided via a status page/portal and automated notifications (for example email/SMS/console alerts), alongside standard support channels.

Security and data protection

Security controls include segmentation, encryption, and protective monitoring aligned to recognised cloud security principles.

Vulnerability management follows a proactive lifecycle (identify, assess, prioritise, mitigate, remediate, monitor), supported by continuous scanning and third-party penetration testing. Threat intelligence is sourced from Unit 42, global partners, and relevant agencies. Critical patches are prioritised and typically deployed within 24–48 hours for urgent threats, with standard updates following a regular cycle.

Protective monitoring uses continuous telemetry analysis and automated response playbooks to identify and contain threats quickly, with logging and audit support for compliance.

Onboarding and offboarding

Onboarding typically includes documentation, support, training options, and (if required) professional services with step-by-step guidance.

Offboarding / end of contract

At contract end, services cease unless renewed. Buyers can extract/export relevant data (such as logs and reports) and complete transition activities with vendor assistance where required. Data export is available via the management interface in formats including CSV, JSON, and PDF

Commercial model

VM-Series NGFW is provided as a subscription licensing model (term-based), giving the buyer the right to use the virtual firewall software in supported environments. Buyers can select the appropriate support tier (Standard, Premium, Platinum). Additional services (including Technical Account Manager support and professional services for onboarding, configuration, and change activity) are available at extra cost.

As your partner, eir business can provide procurement, licensing management, onboarding support, and optional professional services to implement and operationalise the solution in your environment. These services can be called off on a time and materials basis using our rate card.

