

# Service Description:

# Managed Fortinet Secure SD-WAN

Version: 2.0

Date: 08/09/2025

## Service Overview

### What is Optec Managed Fortinet Secure SD-WAN?

Optec Managed Fortinet Secure SD-WAN is the provision of Fortinet focused wide area network optimisation, visibility and expert support delivered as a managed service. It provides your organisation with a secure, resilient and application aware SD-WAN solution, configured to your requirements, and supported by a highly skilled team of engineers under a fixed monthly subscription model.

Optec's Managed Fortinet Secure SD-WAN service is designed for organisations that require improved connectivity performance, resilience and security across distributed sites but do not have the time, in house skills or resources required to design, deploy and operate an SD-WAN solution themselves. Optec delivers a true end to end service, taking responsibility for the initial engagement, design, build and deployment of the SD-WAN solution, followed by ongoing monitoring, management and support delivered by Fortinet certified engineers to keep your network operational.

Optec's Managed Fortinet Secure SD-WAN service includes all the capabilities expected from a modern SD-WAN platform, including application aware routing, secure overlay networking and centralised policy control across multiple connectivity types. In addition, the service provides operational assurance and governance capabilities that are not typically delivered as part of standard SD-WAN offerings.

Optec's Managed Fortinet Secure SD-WAN service offers your organisation several strategic benefits:

**Application Aware Traffic Steering** ensures that business critical applications are prioritised and routed across the most appropriate connectivity paths based on real time performance metrics. This improves user experience.

**Resilient and Optimised Connectivity** is achieved through the intelligent use of multiple access circuits, including MPLS, broadband and cellular. Automatic failover and dynamic path selection reduce the risk of outages and improve service availability without reliance on single connectivity types.

**Proactive Monitoring and Response** is central to the service. SD-WAN devices, links and performance metrics are continuously monitored, with issues automatically flagged to the Optec NOC for investigation and response. This enables problems to be addressed before they impact business operations.

**Configuration and Change Monitoring** ensures that all changes made to managed SD-WAN devices are tracked and validated. Any configuration change automatically raises a ticket for investigation, allowing Optec to verify legitimacy and identify unauthorised or unexpected activity at an early stage.

# Service Description:

## Managed Fortinet Secure SD-WAN

Version: 2.0

Date: 08/09/2025

**Secure Customer Access** forms a core part of the service. Leveraging Optec's expertise as a Fortinet Expert partner, the platform is built using secure remote access technologies that maintain strict customer separation while enabling controlled visibility and delegated access where required.

**PSIRT Advisory and CVE Monitoring and Remediation** ensures that all managed SD-WAN devices remain protected against known vulnerabilities. Optec actively monitors vendor advisories and exposure data and will coordinate upgrades or mitigations to minimise risk to your environment.

### Key Components

Optec's Managed Fortinet Secure SD-WAN service is delivered through a combination of platform capability, secure architecture and operational processes designed to provide performance, resilience and ongoing assurance across your wide area network.

#### Fortinet Secure SD-WAN Platform

The service is built on Fortinet SD-WAN capable devices, providing centralised control, policy driven traffic steering and integrated security services. SD-WAN policies are configured to align with application performance requirements, resilience objectives and security best practices, ensuring consistent behaviour across all customer sites.

#### Application and Link Performance Monitoring

Optec continuously monitors SD-WAN devices and underlying connectivity to provide visibility into link availability, latency, jitter and packet loss. Application performance metrics are used to validate SD-WAN policy effectiveness and to support proactive identification of degradation before it impacts users or services.

#### Secure Onsite Telemetry and Connectivity

Where required, secure onsite telemetry is used to collect monitoring data and operational metrics from customer environments. This approach improves visibility and security while maintaining strict separation between customer environments and Optec's managed service platform.

#### Proactive Alerting and Incident Management

Automated alerting ensures that SD-WAN related events, performance issues and outages are immediately flagged to Optec's Network Operations Centre. Incidents are logged, investigated and managed in line with agreed support levels, with remediation actions tracked through Optec's service desk.

#### Configuration and Change Control

All managed SD-WAN devices are subject to continuous configuration monitoring. Any change to device configuration or SD-WAN policy automatically generates a service ticket, enabling validation, auditability and rapid detection of unauthorised or unexpected changes.

# Service Description:

## Managed Fortinet Secure SD-WAN

Version: 2.0

Date: 08/09/2025

### **Vulnerability Scanning**

Once we obtain your explicit permission, Optec will configure our vulnerability scanning service to scan your external IP addresses on a regular, scheduled basis. We will include the results of these reports in your monthly service reports to ensure that you have an accurate and up to date view of your perimeter security posture. This service can be extended to scan and report on your internal infrastructure as well if this one of your requirements.

### **Configuration Management & Backup**

As part of your Monitoring and Support service, Optec will ensure that the configurations of your network devices are all monitored and continuously backed up if changes are detected. We will maintain a full repository of previous configurations to allow you to roll back to a known working state should this be required.

### **Proactive Incident Response**

Optec's Managed Network Service is delivered by a Fortinet certified Managed Services team that provides continuous, proactive monitoring and operational support for your network infrastructure. Incidents identified through Optec monitoring systems or reported by your teams are assessed, prioritised, and resolved in accordance with ITIL v4 aligned incident management processes. Optec engineers take ownership of incidents end to end, working to restore normal service operation as quickly as possible while providing clear and timely communication throughout.

### **Controlled Change Delivery**

In addition to incident response, the service includes the implementation of customer requested changes to the managed network environment. Changes are delivered using ITIL v4 aligned change management processes to ensure that configuration updates, security policy changes, and network modifications are implemented in a controlled and auditable manner. Where urgent action is required to restore service or reduce risk, emergency changes are applied in line with defined controls and reviewed retrospectively to maintain governance.

### **Security Advisory and Vulnerability Management**

Optec actively monitors Fortinet PSIRT advisories and common vulnerabilities and exposures that may affect managed SD-WAN devices. Where relevant issues are identified, Optec will coordinate upgrades, configuration changes or mitigations to reduce exposure and maintain security posture.

### **Reporting and Service Governance**

The service includes regular reporting covering availability, performance, incidents and changes. Service reviews provide visibility into trends, risks and improvement opportunities, ensuring that the SD-WAN solution continues to align with business requirements over time.

# Service Description:

## Managed Fortinet Secure SD-WAN

Version: 2.0

Date: 08/09/2025

### Bespoke Service Design and Build

Optec's Managed Fortinet Secure SD-WAN service includes a professional services component delivered by Optec's Fortinet Expert engineers and managed by experienced technical project managers. This ensures each SD-WAN solution is designed, deployed and transitioned into service in a controlled and predictable manner.

Optec's technical project managers provide full end to end project coordination, managing scope, timelines and dependencies while acting as the primary point of contact throughout delivery. This ensures clear communication, effective governance and minimal disruption to business operations.

Optec's Fortinet certified engineers design and deploy secure, resilient SD-WAN solutions aligned to application requirements, connectivity constraints and industry best practices. Device configuration, SD-WAN policy implementation and monitoring integration are completed as part of the deployment activity.

Once deployment is complete, the solution is validated and transitioned seamlessly into Optec's managed monitoring and support platform, ensuring continuity of responsibility across the full service lifecycle.

| Service Element | Description                                                                                                                                                                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Engage          | <ul style="list-style-type: none"> <li>Discovery workshops to understand business, application and connectivity requirements</li> <li>Review of existing network, circuits and site topology</li> <li>Definition of success criteria and deployment scope</li> </ul>                         |
| Design          | <ul style="list-style-type: none"> <li>High and low level SD-WAN design</li> <li>Link utilisation and resilience strategy</li> <li>Security and segmentation design aligned to organisational requirements</li> <li>Validation of design against Fortinet and Optec best practice</li> </ul> |
| Build           | <ul style="list-style-type: none"> <li>Device configuration and SD-WAN policy implementation</li> <li>Integration of monitoring, logging and alerting</li> <li>Pre deployment testing and validation</li> <li>Documentation of final configuration</li> </ul>                                |
| Deploy          | <ul style="list-style-type: none"> <li>Coordinated rollout of SD-WAN devices and policies</li> <li>Migration support and cutover planning</li> <li>Post deployment validation</li> <li>Handover into managed service operations</li> </ul>                                                   |

# Service Description:

## Managed Fortinet Secure SD-WAN

Version: 2.0

Date: 08/09/2025

### Support Hours

The final choice to make as part of your managed SD-WAN service is your desired support hours. Optec offer two choices, our Standard Support Hours which are 08:30 to 17:30 Monday to Friday (excluding UK bank holidays) or 24/7 which will cover your infrastructure continually throughout the year.

### Standard Support

Optec's standard support provides you with the service elements that you've chosen from the list above for all your devices from Monday to Friday between the hours of 08:30 and 17:30 excluding UK Bank Holidays. The SLA for all your devices under standard support will begin at the start of the support period.

### Example

If you log a ticket via the portal at 9pm on a Wednesday evening the clock on the SLA will start at 08:30 on Thursday morning.

### 24/7 Support

If your organisation requires round the clock coverage for your SD-WAN infrastructure and you chose to opt for 24/7 support, then that means your SLAs will begin immediately after raising tickets via the portal or via telephone.

Please be aware that our 24/7 support service will ONLY cover P1 (Critical) and P2 (High) incidents outside of our standard support hours.

### Examples

If you log a ticket at 2am on a Sunday morning for a P2 incident, then the SLA will start at this point, and this will be actioned immediately until resolution.

If you log a ticket at 2am on a Sunday morning for a P3 incident, then the clock on the SLA will start at 08:30 on Monday morning this will be actioned at that point.

As part of this process the Managed SD-WAN data capture form will be provided, and its completion is your responsibility. It is not the responsibility of Optec to ensure that the configuration you choose is suitable for your internal infrastructure. However, as part of your consultation, Optec can assist you in designing a configuration that is most suitable for your environment.

# Service Description:

## Managed Fortinet Secure SD-WAN

Version: 2.0

Date: 08/09/2025

### Onboarding and Transition into Managed Service

#### Device Configuration and Access

Once the Master Service Agreement and project scope are agreed, Optec's project team will initiate onboarding as part of the Professional Services section of your engagement. Optec engineers will configure SD-WAN capable devices, apply the required SD-WAN, security and monitoring configurations, and establish secure managed access in line with agreed security requirements. Details of authorised customer contacts will be requested to enable secure access, communication and change validation during both deployment and ongoing support.

#### Transition to Managed Service

Upon completion of the build, deployment and validation activities, devices are transitioned internally into Optec's managed monitoring and support platform. This internal transition ensures continuity between project delivery and operational support, with no customer led handover activities required. From this point, the service enters Live status and is fully supported under the agreed monitoring and support service level.

#### Roles and Responsibilities

The table below outlines the division of responsibilities between Optec and your organisation during onboarding and transition into the managed service.

| Responsibility                                                    | Optec | You |
|-------------------------------------------------------------------|-------|-----|
| SD-WAN device configuration and policy implementation             | X     |     |
| Integration with monitoring, logging and alerting platforms       | X     |     |
| Secure managed access configuration                               | X     |     |
| Provision of site connectivity and circuits                       |       | X   |
| Provision of power, rack space and physical access where required |       | X   |
| Provision and maintenance of authorised contact list              |       | X   |
| Validation of deployment and acceptance into live service         | X     | X   |

# Service Description:

# Managed Fortinet Secure SD-WAN

Version: 2.0

Date: 08/09/2025

## Monitoring & Support

Once your Optec Managed SD-WAN solution is up and running and the onboarding process has been completed, Optec will continue to monitor the availability and health of your infrastructure 24x7x365 to maintain its operation. The parameters of the ongoing management of the service and the appropriate roles and responsibilities are outlined in the areas below.

### Managed Infrastructure

Optec's monitoring service will automatically raise tickets if an issue is detected, or a threshold breached within your environment. Optec will manage these technical support incidents and keep you and your team informed throughout the process. You will be able to monitor these tickets and interact with the Optec support teams via the Supportal however, we will need you to provide at least one account with access to the management dashboard.

There are a lot of reports within the management dashboard that can provide you with insight into you network behaviours and performance.

### Change Management

As part of the managed service, you have the option to raise a change request. Where you require specific changes to be made to the configuration of your managed infrastructure, Optec will be responsible for writing, reviewing and implementing the change.

### Change Control Process

Optec's Change Management team are responsible for requests relating to any product and service configuration changes you wish to be made. The team specialise in configuration and follow strict processes in ensuring that the changes are authorised. The Change Management team are also responsible for Optec's Change Advisory Board (CAB), which discusses and approves changes raised internally.

### Raising a Request for Change (RFC)

Optec provides two ways for your approved contacts to raise, track and update standard support tickets; through the Optec Support portal and by telephone. For security and audit reasons, you are required to make all requests for change through the customer portal and only portal users with the correct privileges can request a change.

You will only see your services listed so please select the service relating to the request for change. In the event that the customer portal is unavailable, please contact Optec by telephone, where an emergency procedure will be in place to log change requests on your behalf. Request for changes will not be accepted through this number at any other time.

# Service Description:

# Managed Fortinet Secure SD-WAN

Version: 2.0

Date: 08/09/2025

## Number of Change Requests

You can raise up to five change requests per managed device in each calendar month and Optec reserve the right to charge you for any change requests that are made in excess of this amount. A single change request can be classified as a global change that impacts all sites through a change to a configuration template, or a change to a single device. for example, if you require 3 different changes to 3 different devices, this will result in three change requests.

Details of which adds, moves and changes are covered by your Optec Monitoring and Support solution can be found in the Adds, Moves and Changes document which makes up part of your onboarding pack.

An Emergency Change Request can be actioned by contacting Service Operations once an urgent change ticket has been raised via Supportal. Further information can be obtained through your Account Manager.

## Change of Service

In the event that your requirements change, and you need to enable new service, a change of service type, additional users or a change in service features, they must be requested via your Account Manager and may be subject to prevailing fees.

## Planned Changes, Emergency Maintenance and Patching

Optec will contact you about any planned maintenance. However, in order to ensure the continued operation of the service, it is necessary that rules relating to traffic routing are maintained and it may be necessary for Optec to do this without notification to you. Similarly, for security reasons, e.g., in the event of an attack.

## Notification

In the event of any planned maintenance, Optec will notify your nominated contacts through two primary channels, Supportal and by email notification. An email is sent to the nominated contact and details are announced through the notifications in Supportal. The notification will contain the date and time of the maintenance, the reason, the service affected and the likely impact to you. Optec will aim to provide at least seven days' notice of any planned maintenance work where an outage is expected or a reduction in the resiliency of infrastructure, wherever possible.

## Emergency Maintenance & Outages

Optec will provide as much notice as possible and we will seek to ensure minimal disruption. Wherever possible, changes will be made at periods of low service utilisation.

In some extreme cases, Optec may require an emergency outage to rectify a problem. In such cases, Optec will work with you to agree a mutually convenient time, but you agree that in such cases the problem cannot be rectified until the outage has taken place. These details can be maintained within Supportal.

# Service Description:

## Managed Fortinet Secure SD-WAN

Version: 2.0

Date: 08/09/2025

### Patching

Apply all critical patch updates as required. Where non-critical patches are released, Optec can apply these at your request. In the event of a firmware upgrade, Optec will work with you to identify a suitable time to perform the patch whilst minimising the impact to your business (further details regarding upgrades are available in our PSIRT Advisory & CVE Monitoring guidance document).

### Maintenance Window

The Major Incident process will be invoked during the maintenance window where a rollback or issue mitigation process does not exist, or should the planned work extend beyond the allocated time.

### Monitoring

#### Monitoring

Optec will actively monitor the status of your infrastructure 24x7x365. This will allow us to quickly understand when a device goes offline allowing us to create a support ticket and begin investigating the issue. Because there may be elements of your infrastructure that are out of Optec's control, you must notify our support desk should you be performing any maintenance that could cause any of the monitored devices or services to lose connectivity.

### Service Levels

The Service Level determines the parameters by which the Management element of the service is accountable.

#### Fix levels and response times

Not only will support tickets be raised as part of a break/fix or monitoring alert, but it is also possible for you to raise tickets through our support desk. It is possible for you to either contact our support desk by phone, email or via Supportal.

Our support desk is available between 8am and 6pm and will offer you support at any time. If a ticket is raised by either means, Optec will follow the below response times:

| Priority | Service Level Response | Description                                                                  |
|----------|------------------------|------------------------------------------------------------------------------|
| P1       | Within 30 minutes      | Total service is unavailable                                                 |
| P2       | Within 2 hours         | Partial service, an element of the total service has failed                  |
| P3       | Within 4 hours         | Impaired service, no element has totally failed but there is a quality issue |

# Service Description:

## Managed Fortinet Secure SD-WAN

Version: 2.0

Date: 08/09/2025

| Priority | Service Level Response | Description                                                                                     |
|----------|------------------------|-------------------------------------------------------------------------------------------------|
| P4       | Within 1 business day  | The service is unaffected. Request for product related technical advice or configuration change |
| P5       | Within 2 business days | Change request or general information and feature questions related to the Service              |

As part of the Optec Monitoring and Support Service, Optec will manage any alerts raised in line with the priorities mentioned above. By doing this you can trust that any equipment that goes offline will be captured, triage performed, escalation to vendor when required, and we will work with you to install a replacement device if this is necessary.

The circumstances where a fix service level is deemed to be met are:

- When the service has been fixed within the standard and expected response time
- Where you receive a telephone call (within the service level response time) resulting in a fix over the telephone
- Where you receive a telephone call and you defer the visit of an engineer to a specific time, the fix time is measured from the time you specify
- When a part which can be fitted by you arrives on site
- Where it is subsequently discovered that the issue giving rise to the telephone call falls outside the Services agreed to be provided by Optec
- When the equipment has been returned to an acceptable operational status or an item of loan equipment has been supplied
- Where the fault relates to an excepted Service

# Service Description:

## Managed Fortinet Secure SD-WAN

Version: 2.0

Date: 08/09/2025

| Responsibility                                                                                                        | Optec | You |
|-----------------------------------------------------------------------------------------------------------------------|-------|-----|
| <b>Support Team Process:</b> Remain familiarised with how to raise support tickets and the expected response times.   | X     |     |
| <b>Contact list:</b> Provide and maintain an up-to-date contact list, including any changes in authorisation          | X     |     |
| <b>SLA:</b> Adhere to the Request for services levels and associated SLA's                                            | X     |     |
| <b>Assist:</b> When requested, provide accurate information, or implement corrective actions to assist the resolution | X     |     |

In the event of a Service outage, you are responsible for complying as quickly as possible with any requests from Optec for help with diagnostics. Any delay in resolving the fault due to you not being available or not complying with Optec's requests may impact the validity of any Service Levels.

### Escalating a ticket

In the event that you need to escalate a ticket, Optec is ready and available to help you quickly bring your issue to closure. Within each level of the escalation path the person you speak with is responsible for evaluating your situation, facilitating the resolution plan and acting as your sponsor. The benefits of the escalation procedure are:

- A dedicated member of staff owning your escalation
- A focus on service recovery
- Improved communication
- Consistent process

An escalation may be initiated when, after working through our standard support processes and with our teams, you are not satisfied with the level or timeliness of the service you have received. Additionally, an escalation should be initiated when there is tangible impact to your production environment, or there is high risk to your business operations.

Once an escalation has been raised Optec will assign an Escalation Manager who will deal with your escalation and collaborate with you to develop a communication plan. A technical plan of action may be needed to ensure resolution of a technical issue. Your Escalation Manager works as your advocate internally and will become a virtual member of your own problem resolution team. Should you feel dissatisfied with the escalation process, please contact your Account Manager directly.

If you feel that Optec has failed to deliver any of the above stated service levels, Optec agrees that you shall be entitled to receive, in lieu of all other remedies available to you, Service Credits as set forth in this section against the fees owing to Optec under the Agreement.