# Service Description: Fortified Monitoring & Support

Version: 1.4
Date: 23/05/2025

## Service Overview

### What is Optec Fortified Network Monitoring and Support?

Optec Fortified Network Monitoring and Support is the provision of Fortinet focused network visibility and expert support as a service. It provides your organisation with a best of breed network monitoring solution, configured to your needs, and backed by a highly skilled team of engineers located in Optec's Network Operations Centre for a fixed monthly cost subscription model.

Optec's Fortified Network Monitoring and Support solution is designed for organisations who need network visibility and support but don't have the time, the in-house skills or the resources needed to deploy and manage it themselves. We provide a true end-to-end service and will take care of everything from the initial design of the solution, the installation and on-boarding, the on-going monitoring and maintenance and most importantly, we provide Fortinet certified engineers to keep your infrastructure operational.

Optec's Fortified Network Monitoring and Support solution includes all the features that you would expect from a modern infrastructure management platform including SNMP v3 and API based network monitoring with on-site probes to improve security and availability, but also provides service not usually seen in this industry space.

Optec's Monitoring and Support service offers your organisation several strategic benefits:

**Detailed Network Visibility** is at the heart Optec's solution. We know that your organisation relies on its infrastructure to function and so we provide full and detailed visibility into its operation. Our monitoring platform uses a variety of protocols and services to retrieve the monitoring metrics that matter to your organisation.

**Configuration Health Checks** carried out by Fortinet certified professionals and using both vendor and industry best practices to ensure that your Fortinet devices are configured in a secure and efficient manor to make sure that the network infrastructure of your business is operating optimally.

**Proactive Alerting and Response** to problems is a key factor in their timely mitigation and remediation. This means that when a key piece of your network infrastructure does start to experience a problem, this is flagged up to the Optec NOC for investigation and response, allowing us to deal with it before it impacts your business.

**Detailed Activity Monitoring** for all your managed devices means that we are constantly monitoring EVERY change made to them. If a breach does occur, changes made to the device by threat actors is one of the early indicators. Our activity monitoring means that a ticket will be automatically raised for any configuration change, and we will verify the authenticity of the change with you, meaning that any breach will be detected early in the process and stopped.

# Service Description: Fortified Monitoring & Support

Version: 1.4
Date: 23/05/2025

**Secure Customer Access** forms a key component of the solution. In addition to our experience as a network engineering company, Optec are also experienced in network security – we are proud to be Fortinet Expert partners. We understand the importance of network and infrastructure security and we have built our platform on best of breed remote access technology.

**PSIRT Advisory & CVE Monitoring and Remediation** ensures that your network infrastructure is always protected. Optec monitor all managed devices and operating system versions for common vulnerabilities and exposures. If we discover one that relates to you, we'll arrange and carry out an upgrade or apply a mitigation at your earliest convenience to ensure that your exposure is minimal.

**External Scanning** ensures that your external network perimeter, as presented to the outside world, is regularly scanned by us. This allows us to verify that the devices are secure and that any changes are picked up and verified by you.

## Key Components

The key components of Optec's Fortified Monitoring and Support Service are:

**Skilled Network Engineers**
The Optec Network Operations Centre is staffed by skilled and experience engineers with a wide range of industry certifications including Fortinet NSE4, NSE5, NSE6 and NSE7 and Cisco CCNA, CCNA Security, CCNA Wireless, CCNP and CCDP. You can rest assured that your critical infrastructure is being monitored and managed by a top tier technical team ready to respond to incidents as they arise.

**Extensible Monitoring Platform**
Optec utilise Zabbix as their chosen platform for infrastructure monitoring. Zabbix has the flexibility to monitor a diverse range of infrastructure devices including SNMP and API based monitoring for network devices, API integrations for several third-party platforms and fully extensible use of custom scripts to meet any requirement. Zabbix also allows for fully distributed monitoring, specialist OT based monitoring sensors, detailed reporting and much more.

Our NOC teams are all experienced Zabbix engineers, and their familiarity with the platform allows us to tailor a monitoring package to your unique environment.

**Software Vulnerability Monitoring**
As part of your on-boarding process, Optec will ensure that the make, model and software version of all of your network devices are entered into our CVE monitoring service. This ensures that, should a CVE be raised that affects your infrastructure, Optec will be aware and be in contact with you as a priority to ensure that updates or patches are applied, and your network is protected.

# Service Description: Fortified Monitoring & Support

Version: 1.4
Date: 23/05/2025

**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.

**Real Time Network Defence**
We understand that one of the most important factors in dealing with an incident is the speed of the response. Optec's Real Time Network Defence provides continuous monitoring of device level events and security logs collected from managed network infrastructure. Syslog data is securely captured and analysed in real time, with alerts and configuration changes automatically generating support tickets for investigation. This enables Optec to proactively identify security events, unauthorised changes, or abnormal behaviour and take timely action to protect the network environment.

# Service Description: Fortified Monitoring & Support

Version: 1.4
Date: 23/05/2025

## Right Sizing the Service

Optec offers a comprehensive consultancy and design stage for all prospective Fortified Monitoring and Support customers. Optec will discuss your operational and technical requirements with you, and we will design a solution that meets and exceeds the needs of your organisation.

Optec's Fortified Monitoring and Support solution is designed to accommodate the needs of all organisations, whether you are a smaller business on a single site, a large business with a multi-site enterprise network, a central or local government department, a SCADA based manufacturer or a cloud-based developer. All our solutions are designed to meet and exceed current government guidelines on service provider infrastructure and secure design.

### Modular Solution

Our modular packages are designed to meet the technology needs of modern businesses and provide our customers with configurable packages to enable you to pick the service level that best fits your business requirements. By choosing the packages that best fits your organisation, your Monitoring and Support solution will be deployed to provide the functionality you require.

Once you've chosen your packages, you can then choose which elements of the Fortified Network Monitoring and Support service you need. The elements that make up the service are listed in the table below.

| Service Element | Description | Optional? |
|---|---|---|
| Optec Service Desk | This is the heart of our service and the part that all other elements are built around. The service desk is made up of highly skilled and qualified network engineers dedicated to monitoring and maintaining your network infrastructure. | No |
| Monitoring and Reporting | This element covers adding your devices to our multi-tenanted NSM platform, installing monitoring probes if required, configuring monthly reporting, and setting up secure customer access. | Yes |
| Alerting | Optec will configure automatic alerting to both our internal NOC and to you if this is required. By default, we will use email as the chosen channel, but we can integrate with Teams or Slack. | Yes |
| Daily Backups | We will configure our Configuration Management platform to pull a full configuration backup of all supported devices every 24 hours if changes are detected. | Yes |

# Service Description: Fortified Monitoring & Support

Version: 1.4
Date: 23/05/2025

| Service Element | Description | Optional? |
|---|---|---|
| CVE Monitoring & Remediation | Optec utilise several CVE monitoring services as well as vendor PSIRT alerts to ensure that we are aware of new CVE alerts as they are announced. We will then work with you to apply the relevant update or mitigation as a priority. | Yes |
| Monitoring and Reporting | This element covers adding your devices to our multi-tenanted NSM platform, installing monitoring probes if required, configuring monthly reporting, and setting up secure customer access. | Yes |
| Vulnerability Scans | If vulnerability scanning is a compliance requirement or you would like to see your network perimeter as a potential threat actor does, then Optec can carry out regular vulnerability scans with a full report as the output. | Yes |
| Device Health Checks and Remediation | To ensure that your devices are configured securely and optimally, our NSE certified engineers will carry out a full configuration health check. We will provide you with a full report containing any suggested remediations and we will work with you to apply those remediations | Yes |
| Device Activity Monitoring | Optec configure your monitored devices to send all relevant information to our on-site probe for inspection and alerting if a change is detected. These tickets will be validated with you to ensure that all configuration activity is legitimate and approved. | Yes |

While the service is designed to be modular and can be tailored to meet specific technical or commercial requirements, Optec strongly recommends adopting the full set of service elements wherever possible. When all components of the Fortified Network Monitoring and Support service are in place, Optec is able to deliver end to end visibility, faster incident resolution, improved resilience, and stronger operational governance across the entire network estate. This integrated approach reduces risk, removes operational blind spots, and ensures the service operates as a cohesive, fully managed solution rather than a collection of individual capabilities.

# Service Description: Fortified Monitoring & Support

Version: 1.4
Date: 23/05/2025

## Support Hours

The final choice to make as part of the configuration 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 network 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 Monitoring and Support 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: Fortified Monitoring & Support

Version: 1.4
Date: 23/05/2025

## Onboarding

### Device Access

Once your Master Service Agreement has been signed, Optec engineers will initiate device onboarding by requesting supported device details via secure channels and providing you with device specific configuration scripts to apply to allow us to monitor and, where needed, manage your equipment. We will also request some details about members of your team who are authorised to work with us – these will be used to create individual secure access accounts.

### Lead Times

Standard lead time for an Optec Monitoring and Support deployment varies depending on the options chosen. If we are monitoring your FortiGates directly or across a VPN, the standard deployment time will be 1-2 days but if we are deploying probes to implement a full topology scan and implementation then deployment time is usually between 3-5 working days from time of order (depending on destination location).

### Probe Installation

Optec will work with you to identify an installation schedule for the probe(s) at your site(s) or a deployment of a virtual machine if this is your preferred option.

All physical probes will be sent to site and an Optec engineer will assist you with the installation, verifying remote access and confirming that the appliance is fully operational before setting you to a Live status.

The engineer will not be responsible for configuring non-Optec supplied equipment to enable the functionality of the probe. It will also not be the responsibility of the engineer to provide the relevant structured cabling and power to the appliances.

| Responsibility | Optec | You |
|---|---|---|
| **Hardware Probe**<br>Structured cabling, power and space: Ensure that the relevant structured cabling, required power, and installation space is in place for the Optec Monitoring and Support Probe installation to be completed successfully. | | X |
| **Hardware Probe**<br>Site access: You will provide convenient times when the engineers can gain access to the site within the contracted hours to perform the installation of the probe. | | X |
| **Virtual Probe**<br>The probe will be supplied as a virtual appliance. Ensure that the correct virtual resources and virtual network access is configured for the Optec Monitoring and Support Probe installation to be completed successfully. | | X |

# Service Description: Fortified Monitoring & Support

Version: 1.4
Date: 23/05/2025

## Monitoring & Support

Once your Optec Monitoring and Support 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: Fortified Monitoring & Support

Version: 1.4
Date: 23/05/2025

**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: Fortified Monitoring & Support

Version: 1.4
Date: 23/05/2025

**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: Fortified Monitoring & Support

Version: 1.4
Date: 23/05/2025

| 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: Fortified Monitoring & Support

Version: 1.4
Date: 23/05/2025

| Responsibility | Optec | You |
|---|---|---|
| **Support Team Process:** Remain familiarised with how to raise support tickets and the expected response times. | X | |
| **Contact list:** Provide and maintain an up-to-date contact list, including any changes in authorisation | X | |
| **SLA:** Adhere to the Request for services levels and associated SLA's | X | |
| **Assist:** 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.