OMNIDATA

Effective April 22, 2025. These Service Descriptions supersede and replace all prior versions.

# Schedule of Services

### Schedule of Services - Management Levels

### Overview

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a new Order including those Services. The following outlines the service levels available: ALERTS, RESPOND, RESPOND PROACTIVE, RESPOND PROACTIVE PREMIUM, and SECURE/ADD-ON. Each level includes specific features designed to meet varying needs for monitoring, security, protection, and support.

---

### Service Levels and Descriptions

### ALERTS

The **ALERTS** service level provides basic monitoring and notification services to ensure Clients are informed of critical system events.

- Device Monitoring: Provider will monitor Client's devices to detect operational issues, performance degradation, or potential failures.
- Alerting to Customer: Provider will notify Client of detected issues via email, client portal, or other agreed-upon methods.
- Customer Portal: Access to a secure online portal for viewing alerts, service tickets, and basic system status.
- Secure Pay Invoices Online: Clients can securely pay invoices through the customer portal.
- Online Training in Customer Portal: Access to basic training materials within the portal to assist with system usage and best practices.
- Traffic Insights: Provides visibility into network traffic patterns to identify unusual activity or bottlenecks.
- Top N Conversations: Reports on the most significant network conversations (e.g., top talkers) to aid in network management.

**RESPOND**

The **RESPOND** service level builds on **ALERTS** by adding remote service capabilities and additional security features.

- All ALERTS Features: Includes all features listed under the **ALERTS** service level.
- Remote Service: Provider will perform remote remediation services to address detected issues, such as configuration adjustments or software updates.
- Vulnerability Assessment: Periodic assessments to identify potential vulnerabilities in Client's systems or network.
- Self Assessments in Customer Portal: Tools within the portal for Clients to conduct basic security self-assessments.
- Access to Device Documentation: Clients have access to documentation for managed devices, including configurations and logs.

**RESPOND PROACTIVE**

The **RESPOND PROACTIVE** service level enhances **RESPOND** with proactive issue resolution and additional protective measures.

- All RESPOND Features: Includes all features listed under the **RESPOND** service level.
- Omni to Notify Customer and Automatically Correct Issue: Provider will proactively resolve certain issues without requiring Client approval, based on predefined criteria.
- Backups (Servers) – Base Includes 1TB Storage: Provider will perform server backups with up to 1TB of storage, as specified in the Order.
- Patch Management (Servers): Regular application of Microsoft patches and other critical updates to servers.
- Automatic Switch Config Backups: Automated backups of network switch configurations to ensure quick recovery in case of failure.
- Automatic Firewall Config Backups: Automated backups of firewall configurations to support rapid restoration.
- Security Updates to Firmware for Managed Devices: Regular firmware updates for managed devices to address security vulnerabilities.

**RESPOND PROACTIVE PREMIUM**

The **RESPOND PROACTIVE PREMIUM** service level offers comprehensive support, including on-site services and advanced security monitoring.

- All RESPOND PROACTIVE Features: Includes all features listed under the **RESPOND PROACTIVE** service level.
- OnSite Service: Provider will deliver on-site support during normal business hours for issues that cannot be resolved remotely, as specified in the Order. Additional on-site support is billed at Provider's then-prevailing hourly rate.
- Endpoint Detection and Response (EDR): Advanced monitoring and response capabilities to detect and mitigate threats at the endpoint level.
- Security Operations Center (SOC): 24/7 monitoring by a dedicated SOC to identify and respond to security incidents.
- Zero Trust 24/7/365 Security Operations Center: Implementation of a zero-trust security model with continuous monitoring and verification.
- Security Incident Event Management (SIEM): Deployment of SIEM probes to monitor critical network devices (e.g., domain controllers, firewalls, switches, routers) and, where required for compliance, all Windows devices.
- Dark Web Monitoring: Monitoring of dark web sources to detect compromised credentials or sensitive Client data.

**SECURE/ADD-ON**

The **SECURE/ADD-ON** service level provides optional, advanced security and support features that can be added to any of the above service levels.

- Block Time or Open PO for Services: Clients can pre-purchase blocks of service hours or maintain an open purchase order for additional services not covered in the Order.
- Services Included: Specific add-on services will be detailed in the Order, which may include:
    - Advanced Security Features: Such as enhanced malware protection, ransomware rollback, or client-side DNS filtering.
    - Customized Support: Tailored services like security awareness training, phishing simulations, or multi-factor authentication configuration.
    - Compliance Support: Assistance with meeting regulatory requirements through SIEM, log management, or other tools.

---

Contract Details

- Omni to Notify Customer / Customer to Determine if Omni Should Respond: For ALERTS and RESPOND levels, Provider will notify Client of issues, and Client will decide whether Provider should take action.

- Omni to Notify Customer and Automatically Correct Issue: For RESPOND PROACTIVE and higher, Provider may automatically resolve issues based on predefined protocols.
- Remote Service: Available in RESPOND and higher levels, includes remote troubleshooting and remediation.
- OnSite Service: Available in RESPOND PROACTIVE PREMIUM, with additional on-site support available at an hourly rate.
- Block Time or Open PO Needed for Services: For SECURE/ADD-ON or non-covered services, Clients must have pre-arranged payment terms.
- Services Included: All services are subject to the terms specified in the Order.

---

Additional Notes

- Third-Party Services: Certain features (e.g., SIEM, EDR, backups) may be provided through third-party vendors. Client agrees to be bound by applicable third-party terms of use or end-user licensing agreements, which are subject to change without notice.
- Limitations: Services such as hardware replacements, major upgrades, or new installations are not included in the Service Fee unless specified in the Order.
- Changes to Services: These descriptions are subject to change at any time without notice.

Below are the definitions for the terms

- Device Monitoring: Continuous observation of Client's devices to detect operational issues, performance degradation, or potential failures.
- Alerting to Customer: Notification sent to the Client via email, client portal, or other agreed methods when issues are detected on monitored devices.
- Customer Portal: A secure online platform where Clients can view alerts, service tickets, system status, pay invoices, and access training materials.
- Secure Pay Invoices Online: A feature within the customer portal allowing Clients to securely pay invoices electronically.
- Online Training in Customer Portal: Access to educational materials within the customer portal to help Clients understand system usage and best practices.
- Traffic Insights: Visibility into network traffic patterns to identify unusual activity, bottlenecks, or performance issues.
- Top N Conversations: Reports highlighting the most significant network conversations (e.g., top talkers) to assist with network management and optimization.

- Vulnerability Assessment: Periodic evaluation of Client's systems or network to identify potential security vulnerabilities.
- Self Assessments in Customer Portal: Tools within the customer portal that allow Clients to conduct basic security self-assessments independently.
- Endpoint Detection and Response (EDR): Advanced security monitoring and response system that detects and mitigates threats at the endpoint (e.g., laptops, desktops) level.
- SOC (Security Operations Center): A 24/7 team dedicated to monitoring, detecting, and responding to security incidents on Client's network.
- Zero Trust 24/7/365 Security Operations Center: A SOC implementing a zero-trust security model, requiring continuous verification of all users and devices, operating around the clock.
- SEIM (Security Incident Event Management): Deployment of monitoring probes to track and analyze security events across critical network devices (e.g., domain controllers, firewalls) and, if required for compliance, all Windows devices.
- Access to Device Documentation: Availability of documentation for managed devices, including configurations, logs, and other relevant information.
- Dark Web Monitoring: Surveillance of dark web sources to detect compromised Client credentials or sensitive data being traded or exposed.
- Security Updates to Firmware for Managed Devices: Regular updates to the firmware of managed devices to patch security vulnerabilities and ensure optimal performance.
- Backups (Servers) – Base Includes 1TB Storage: Server data backups performed by the Provider, with a base storage capacity of 1TB, as specified in the Order.
- Patch Management (Servers): Routine application of Microsoft patches and other critical updates to servers to maintain security and functionality.
- Automatic Switch Config Backups: Automated backups of network switch configurations to enable quick recovery in case of failure.
- Automatic Firewall Config Backups: Automated backups of firewall configurations to support rapid restoration if needed.
- Omni to Notify Customer / Customer to Determine if Omni Should Respond: The Provider notifies the Client of detected issues, and the Client decides whether the Provider should take action (applies to ALERTS and RESPOND levels).
- Omni to Notify Customer Automatically Correct: The Provider notifies the Client and automatically resolves certain issues based on predefined criteria (applies to RESPOND PROACTIVE and higher levels).
- Remote Service: Remote troubleshooting and remediation services performed by the Provider to address detected issues.

- OnSite Service: In-person support provided by the Provider at the Client's location during normal business hours for issues that cannot be resolved remotely, available in RESPOND PROACTIVE PREMIUM (additional on-site support billed at an hourly rate).
- Block Time or Open PO Needed for Services: Pre-purchased service hours (block time) or an open purchase order required for additional services not covered in the Order, typically for SECURE/ADD-ON features.
- Services Included: Specific services outlined in the Order, which may include advanced security, customized support, or compliance assistance, depending on the service level.