# Kaseya®

## NOC Services Catalog

Whether you are just starting your MSP business, struggling to staff appropriately while expanding your business, or looking to provide round-the-clock coverage without breaking your business model, Kaseya NOC Services can help.

Designed to let you scale quickly, Kaseya NOC Services deliver the monitoring and management services you need to extend your existing in-house staff and meet your customers' demands. You can deploy Kaseya NOC Services 24x7 as a permanent 'virtual' member of your IT staff. NOC Services can absorb a large percentage of the alarms and requests coming at your team so that you can focus on strategic projects and growing your business.



## KASEYA NOC SERVICES OFFLOADS YOUR TEAM SO YOU CAN FOCUS ON GROWTH

Kaseya NOC Services' à la carte pricing model allows you to choose the services that matter for the endpoints you manage. Mix and match the services to suit your needs. For example, you may choose Server Management + Patch + Backup + Antivirus for production servers, but Patch + Antivirus for test and dev environments.

Grow faster and reduce IT operating costs with Kaseya NOC Services.

## Kaseya NOC Services at a Glance

Kaseya's à la carte pricing model allows you to choose any combination of the following services across your IT infrastructure.

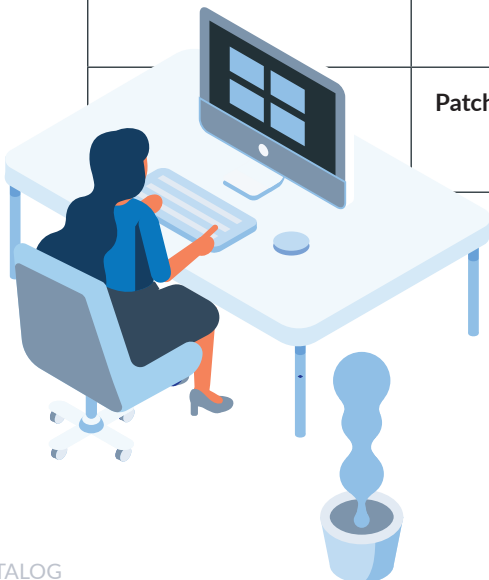| 24x7 ALERT MANAGEMENT | |
|---|---|
| Server Monitoring | Kaseya NOC Best Practice Monitor Sets<br>Triage and escalation of validated alerts<br>Rule-based notifications and escalations<br>Suggested remediations |
| Server Management | Kaseya NOC Best Practice Monitor Sets<br>Triage, escalation and remediation of validated alerts<br>Rule-based notifications and escalations<br>Offload routine IT tasks to free up time (See IT Task Management below)<br>Server Health Checks |
| Workstation Management | Kaseya NOC Best Practice Monitor Sets<br>Triage, escalation and remediation of validated alerts<br>Rule-based notifications and escalations<br>Offload routine IT tasks to free up time (See IT Task Management below) |
| SNMP Endpoint Monitoring | Up/down monitoring of SNMP endpoints<br>Rule-based notifications and escalations |
| **BACKUP** | |
| Backup Management | Monitor and remediate backup jobs/schedules<br>Report backup success/failure counts per defined objectives |
| **PATCH** | |
| Patch Management | Schedule and deploy patch cycles<br>Monitor and address failures<br>Report patch compliance scores |
| **ANTIVIRUS & ANTIMALWARE** | |
| Antivirus & Antimalware Management | Schedule and deploy security scans and update cycles<br>Monitor and address failures<br>Report security compliance scores |
| **TASK MANAGEMENT** | |
| IT Task Management | Assign IT tasks to the NOC Services team, choosing from a predefined list such as investigating performance issues, performing VM migrations, troubleshooting printer problems, etc. See the Server and Workstation Tasks in the detailed section below. |

# Kaseya NOC Services in Detail

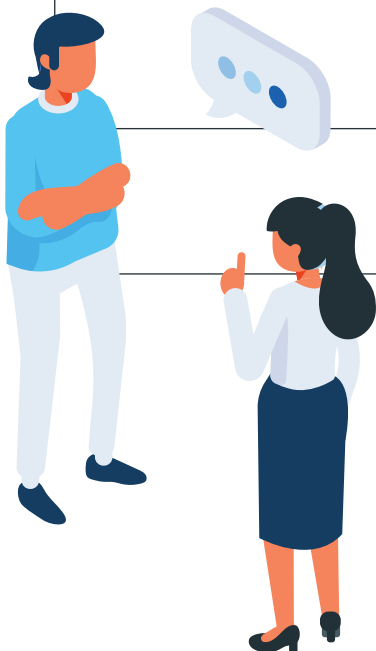| Service and SKU | Deliverables | Detailed Description |
|---|---|---|
| **Server Monitoring**<br><br>**SKU: NOC-MOSM** | **Monitoring Setup** | Set up monitoring parameters and thresholds on VSA. For example, define rules to generate an alert if CPU/Disk space parameters exceed the set threshold. We monitor Agent Status, Windows Services State, Performance Counters and Event Logs. |
| | **24/7 Alert Monitoring** | Confirm if the alert condition is persistent and needs action. Alerts are categorized as Critical, High or Normal. Escalate with resolution steps via agreed notification channels. Customer can choose to be notified via Phone/Email/SMS for different machines for different criteria. For example, phone notification for Critical alerts, email notification for High and Normal alerts. |
| **Server Management**<br><br>**SKU:<br>NOC-MASM-BASE** | **Includes all Server Monitoring deliverables plus the additional ones below** | |
| | **24/7 Alert Remediation** | Resolve the cause of the alert. For example, free up space when disk is out of space, bring a machine back up if it is down, restart services, etc. Escalate via agreed notification channels if NOC team cannot resolve the issue; include ticket history. |
| | **Scheduled / Ad Hoc Maintenance Activities** | Server reboots, services restarts, hardware and software audit reports. Exchange defragmentation. |
| | **Server Health Check** | Scheduled Server Analysis based on Microsoft BPA (Best Practices BPA Analyzer). Reports are shared with the customer |
| | **Reports and Trend Analysis** | Provide 5 Monthly Reports:<br>1. Ticket Volume Trending by Week<br>2. SLO Compliance Score by Severity<br>3. Alerts Handled by NOC vs Escalated to Customer (Count and Alert Types to see if escalations can be reduced)<br>4. Top Alerts generated<br>5. Top Alert generating machines |

| Service and SKU | Deliverables | Detailed Description |
|---|---|---|
| **Server Tasks**<br><br>**SKU:**<br>**NOC-MASM-TASK** | • AD User Account Administration<br>• Network Share Configuration<br>• Service Pack installation<br>• VM Migration<br>• VM Resource Upgrade<br>• AD Migration Assistance Replication Issues<br>• AD Replication Issues Troubleshooting<br>• Server Performance Troubleshooting<br>• Exchange Server Troubleshooting | Server tasks listed on the left can be assigned to Kaseya NOC Services.<br><br>2X (number of servers under management) tasks per month are included.<br><br>Additional server tasks are sold in bundles of 25 tasks.<br><br>The server should have a Kaseya agent on it. |
| **Workstation Management**<br><br>**SKU:**<br>**NOC-MAWKS-BASE** | **Monitoring Setup** | Set up monitoring parameters and thresholds on VSA. For example, define rules to generate an alert if CPU/Disk space threshold is breached. We monitor Hardware and Resource parameters. |
| | **24/7 Alert Remediation** | Resolve the cause of the alert. For example, free up space when disk is out of space. Notify customer of hardware issues. Escalate if NOC team cannot resolve the issue; include ticket history. |
| | **Alert Notifications** | Alerts are categorized as Critical, High or Normal.<br><br>Set up notification rules per customer requirements. Customer can choose to be notified via Phone/Email/SMS for different machines for different criteria. For example, phone notification for Critical alerts, email notification for High and Normal alerts.<br><br>An escalation tree can also be set up such that the secondary customer contact is notified if the primary doesn't respond. |
| | **Scheduled / Ad Hoc Maintenance Activities** | Temp file cleanup, disk analyze, hardware and software audit reports. |
| | **Reports and Trend Analysis** | Provide 5 Monthly Reports:<br>1. Ticket Volume Trending by Week<br>2. SLO Compliance Score by Severity<br>3. Alerts Handled by NOC vs Escalated to Customer (Count and Alert Types to see if escalations can be reduced)<br>4. Top Alerts generated<br>5. Top Alert generating machines |

| Service and SKU | Deliverables | Detailed Description |
|---|---|---|
| **Workstation Tasks**<br><br>**SKU:**<br>**NOC-MAWKS-TASK** | • Investigation and Remediation of Performance Issues<br>• Network Share Access Issues<br>• Troubleshoot Printer Problems (Driver installations/updates)<br>• User Login Administration/ Troubleshooting<br>• User Profile Migration<br>• Third-Party Software Installation/ Updates<br>• Windows 10 Updates | Workstation (e.g. desktop, laptop) tasks listed on the left can be assigned to NOC.<br><br>1X (number of workstations under management) tasks per month are included.<br><br>Additional tasks are sold in bundles of 25 tasks.<br><br>The workstation should have a Kaseya agent on it. |
| **SNMP Device Monitoring**<br><br>**SKU:**<br>**NOC-MOSNMP** | **24/7 Alert Monitoring** | Once the SNMP device is set up in VSA, Kaseya NOC Services will monitor for Critical Alerts/Failures. |
| | **Alert Notifications** | Set up notification rules per customer requirements. Customer can choose to be notified via Phone/Email/SMS for different devices.<br><br>An escalation tree can also be set up such that the secondary customer contact is notified if the primary doesn't respond. |
| **Patch Management**<br><br>**SKU:**<br>**NOC-PTCH** | **Configuration of NOC/Customized Patch Policies on VSA** | Set up Default NOC Patch Policy for all Security and Critical Updates OR set up a user-defined Patch Policy. |
| | **Patch Deployment** | Ensure patches are deployed during maintenance window. Perform pre/post checks. |
| | **Patch Failure Resolution** | Fix failed patches to ensure completion within maintenance window. |
| | **Patch Compliance Reporting** | Provide a Patch Score report at the end of each Patch cycle. |

| Service and SKU | Deliverables | Detailed Description |
| --- | --- | --- |
| **Backup Management**<br><br>**SKU: NOC-BKUP** | **Backup Management (Multi-vendor)** | Ensure backups are successfully completed as per user requirements. |
| | **Agent/Software Updates** | Update backup agent/software as required. |
| | **Backup Failure Resolution** | Fix backup failures. For example, ensure space is available at the destination and rerun the job. |
| | **Backup Compliance Reports** | Provide a monthly Backup Score report indicating how many machines have backups within SLAs. |
| **AV/AM Management**<br><br>**SKU:<br>NOC-AVAM** | **Antivirus Management (Multi-Vendor)** | |
| | **Installation / Definition Updates Failure Resolution** | Ensure definition updates are applied within 30 days of release. |
| | **Scan Failures** | Trap / fix scan failures. |
| | **Threat Resolution** | Isolate / clean up threats detected by AV. Notify the customer of actions taken. |
| | **AV/AM Compliance Reports** | Provide a monthly AV/AM Score report. |

# Onboarding

During NOC Services onboarding, customer participation is key to a successful engagement. We have structured the onboarding process to optimize the value we deliver to your company.

Listed below are the various tasks, ownership and timeline for the NOC onboarding process:

| Nr | Task | Ownership | Timeline |
|----|------|-----------|----------|
| 1. | Welcome Email /Introduction Call with NOC Service Delivery Manager(SDM) | NOC Services | Week 1 |
| 2. | Walkthrough of Onboarding Process with Timelines | NOC Services | Week 1 |
| 3. | Provide details of<br>• End-points to be enrolled for NOC Services<br>• Custom requirements/ Special Handling instructions if any<br>• Notification and Escalation Workflows | Partner | Week 1 |
| 4. | Deploy the VSA agents on the identified endpoints | Partner | Week 1 |
| 5. | Create the Kaseya NOC user ids on the VSA | Partner | Week 1 |
| 6. | Configure the VSA for NOC services | NOC Services | Week 2 |
| 7. | Install NOC agent on the Partner's VSA to monitor the on-premise VSA itself | NOC Services | Week 2 |
| 8. | Customize, Update Monitor Sets per Partner's needs | NOC Services | Week 2 & 3 |
| 9. | Test VSA configuration and Notification Workflow | NOC Services | Week 3 |
| 10 | Share details of Test run/ Fine tune if required | NOC Services | Week 4 |
| 11 | Green Signal for Go-Live | Partner | Week 4 |

# Terms and Conditions

Kaseya will use commercially reasonable efforts to provide the Services and to meet the Hours of Availability, Response Times and Service Levels based on available staffing; provided, however, that Customer acknowledges and agrees that not all issues can be resolved, a particular outcome cannot be guaranteed, Hours of Availability, Response Times and Service Levels may vary. The purchase and use of all Software and Services is subject to the Agreement as defined in http://www.kaseya.com/legal.aspx. Use of the Software or Services indicates Customer's acceptance of the Agreement. Capitalized terms not otherwise defined herein shall have the meaning set forth in the Agreement.

## ABOUT KASEYA

Kaseya® is the leading provider of complete IT infrastructure management solutions for managed service providers (MSPs) and internal IT organizations. Through its open platform and customer-centric approach, Kaseya delivers best in breed technologies that allow organizations to efficiently manage, secure, automate and backup IT. Kaseya IT Complete is the most comprehensive, integrated IT management platform comprised of industry leading solutions from Kaseya, Unitrends, Rapidfire Tools, Spanning Cloud Apps, IT Glue and ID Agent. The platform empowers businesses to: command all of IT centrally; easily manage remote and distributed environments; simplify backup and disaster recovery; safeguard against cybersecurity attacks; effectively manage compliance and network assets; streamline IT documentation; and automate across IT management functions. Headquartered in Dublin, Ireland, Kaseya is privately held with a presence in over 20 countries. To learn more, visit www.kaseya.com.

08102020