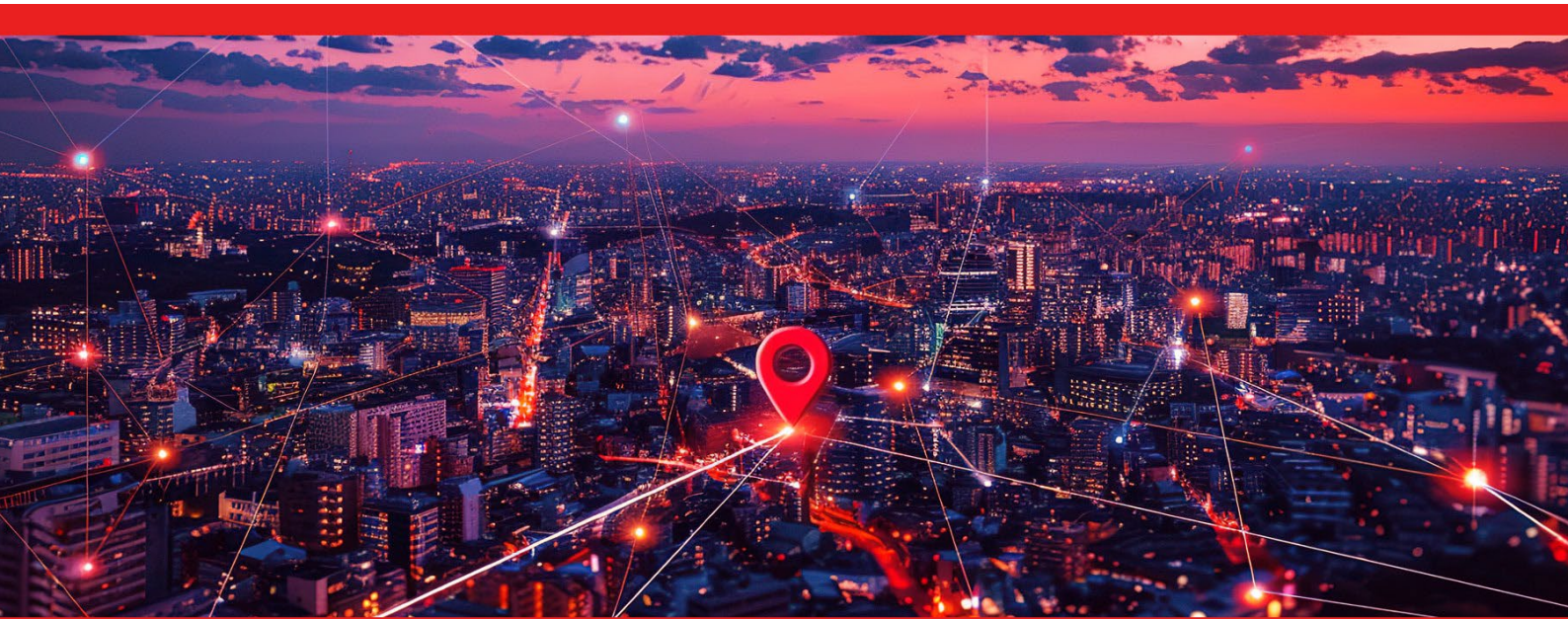


Koris365 Network & Security Monitor

Service Description



Copyright

The information contained in this document is the property of Koris365, a trading name of Koris365 UK Limited. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means; electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Koris365. Legal action will be taken against any infringement.

Confidentiality

All information contained in this document is provided as Commercial-in-Confidence. It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without Koris365's prior permission in writing. These obligations shall not apply to information which is published or becomes known legitimately and independently of either party.

Contents

1 Executive Summary.....	4
1.1 Service Scope Summary	4
2 Service Onboarding & Mobilisation	5
2.1 Onboarding Requirements & Activities.....	5
2.2 Key Operational & Transition Risks	6
2.3 Onboarding & Mobilisation Success Criteria	6
3 Monitoring & Alert Management	7
3.1 Alert Management.....	7
4 Service Reporting	8
4.1 Monitoring Coverage Report.....	8
5 Technical Deliverables.....	9
6 Out of Scope.....	11
7 Service Level Agreement (SLA).....	12
7.1 Hours of Service	12
7.2 Alert Response	12
7.3 Service Level Measurement.....	12
8 Offboarding	13
8.1 Offboarding Activities.....	13
8.2 Customer Responsibilities	13
8.3 Data Retention & Deletion	13

1 Executive Summary

Koris365 Network & Security Monitor provides proactive, automated monitoring and alerting across supported network and security infrastructure.

The service monitors agreed devices, interfaces, services, and applicable performance thresholds across switching, WAN, wireless, firewall, and Identity Management technologies. Monitoring coverage will vary by technology and deployment model and will be agreed during onboarding based on the information available from the supported platform.

Where Network & Security Resolve is also purchased, applicable alerts may be escalated into Resolve for incident investigation and service restoration. Without Resolve, the customer remains responsible for acting on notifications and arranging any required remediation.

1.1 Service Scope Summary

Service Scope	Status	Relevant Service	Relevant Service Purpose
24/7 Automated Monitoring & Alerting	Included	Monitor	Detection
Health, Availability & Performance Monitoring	Included	Monitor	Detection
Alert Generation & Notification	Included	Monitor	Detection
Monitoring Threshold Management	Included	Monitor	Detection
Incident Investigation & Service Restoration	Not included	Resolve	Restoration
Service Requests & Changes	Not included	Operate	Administration
Patching & Software/Firmware Updates	Not included	Patch	Maintenance

2 Service Onboarding & Mobilisation

Onboarding prepares Koris365 to deliver Network & Security Monitor by confirming the devices and services to be monitored, establishing the required connectivity and permissions, configuring monitoring thresholds and alerting, and validating that monitoring is operating as expected.

A controlled onboarding process will be completed before the service enters Business-as-Usual operation.

2.1 Onboarding Requirements & Activities

The following requirements must be in place for Koris365 to provide the service:

- The devices, services and interfaces to be monitored have been identified and accurately documented.
- Required service accounts, credentials and monitoring permissions are provided.
- Connectivity between the customer environment and the Koris365 monitoring platform is available.
- Required routing and firewall changes are implemented to permit monitoring traffic.
- Customer technical contacts and escalation contacts are identified.
- Alert recipients and notification requirements are agreed.
- Supported devices can provide the required monitoring information.

Following order acceptance, a Project Manager will coordinate onboarding, confirm service readiness and manage the transition to go-live.

Phase	Key Activities
Initiation & Scope Confirmation	Confirm monitored assets, services, interfaces, customer contacts, alert recipients, and onboarding requirements.
Connectivity & Access	Establish and validate required service accounts, permissions, routing, firewall rules and connectivity to the Koris365 monitoring platform.
Monitoring Deployment & Validation	Configure monitored assets, apply monitoring templates and thresholds, validate polling and alert generation, and fine-tune the configuration where required.
Operational Handover & Hypercare	Confirm alert notification routes, validate service operation, address onboarding issues, and formally transition into Business-as-Usual monitoring.

2.2 Key Operational & Transition Risks

Koris365 uses structured discovery, knowledge transfer, access validation and process testing to reduce operational risk during service onboarding.

Risk	Impact	Mitigation
Incomplete or inaccurate asset information	Devices, interfaces or services may not be monitored as intended.	Validate monitoring scope and documentation during onboarding.
Delayed or incomplete monitoring access	Monitoring deployment or data collection may be delayed.	Identify and validate service accounts and permissions before go-live.
Connectivity, routing or firewall restrictions	The monitoring platform may be unable to poll supported assets.	Validate monitoring connectivity and required network rules during onboarding.
Unsupported monitoring protocols or telemetry	Required health or performance information may not be available.	Confirm monitoring capability for supported assets during discovery.
Incorrect thresholds or alert configuration	Excessive, missed or inappropriate alerts may be generated.	Validate and tune monitoring thresholds during deployment and Hypercare.
Incomplete customer contact information	Alert notifications may not reach the appropriate recipient.	Confirm alert recipients and escalation contacts before go-live.

2.3 Onboarding & Mobilisation Success Criteria

Onboarding and mobilisation will be considered successful when:

- The monitoring scope and supported assets have been validated.
- Required monitoring access, service accounts and permissions have been provided and tested.
- Connectivity between the supported environment and the Koris365 monitoring platform has been validated.
- Required devices, services and interfaces have been configured for monitoring.
- Monitoring thresholds and alerting have been tested and validated.
- Alert recipients and notification routes have been confirmed.
- Where Resolve is also purchased, applicable alert escalation into Resolve has been confirmed.
- The service has been formally handed over into Business-as-Usual operation.

3 Monitoring & Alert Management

Koris365 Network & Security Monitor provides automated monitoring and alerting for supported network and security infrastructure. The service monitors agreed devices, interfaces, services, and performance conditions to identify availability, health, and performance issues.

3.1 Alert Management

When a monitored condition meets an agreed alert threshold, the monitoring platform automatically generates an alert.

Koris365 will:

- Receive and record applicable monitoring alerts.
- Automatically generate a ticket where configured.
- Notify agreed customer contacts where applicable.
- Where Network & Security Resolve is also purchased, route applicable alerts into Resolve for investigation and service restoration.

4 Service Reporting

Koris365 provides service reporting to give customers visibility of the infrastructure configured within Network & Security Monitor. The Monitoring Coverage Report is provided every six months.

4.1 Monitoring Coverage Report

The Monitoring Coverage Report provides a summary of the assets configured within the monitoring service and may include:

- Device name and type.
- Site or location.
- Monitoring status.
- Monitored interfaces or services, where applicable.
- Assets added to or removed from monitoring during the reporting period.

The report provides customers with visibility of the monitored estate and supports validation that the monitoring scope remains aligned with the supported environment.

5 Technical Deliverables

The following tables define the key monitoring activities undertaken under Network & Security Monitor:

Switch	Included
Monitoring	Monitoring and notification for: • Device up/down, reload, interface down, packet loss, backup failure where backup monitoring is configured, environmental conditions (PSUs, fans, sensors) • CPU, memory, and disk utilisation • Interface utilisation • Switchport utilisation • Stack failures
Threshold Management	Ongoing maintenance and tuning of applicable monitoring thresholds

WAN	Included
Monitoring	Monitoring and notification for: • Device up/down, reload, interface down, packet loss, backup failure where backup monitoring is configured, environmental conditions (PSUs, fans, sensors) • CPU, memory, and disk utilisation • Interface utilisation
Threshold Management	Ongoing maintenance and tuning of applicable monitoring thresholds

Wi-Fi	Included
Monitoring	Monitoring and notification for: • Device up/down, reload, interface down, packet loss, backup failure where backup monitoring is configured, environmental conditions (PSUs, fans, sensors) • CPU, memory, and disk utilisation • Interface utilisation • AP registration • Number of client associations
Threshold Management	Ongoing maintenance and tuning of applicable monitoring thresholds

Firewall	Included
Monitoring	Monitoring and notification for: • Device up/down, reload, interface down, packet loss, backup failure where backup monitoring is configured, environmental conditions (PSUs, fans, sensors) • CPU, memory, and disk utilisation • Interface utilisation • L2L VPN status
Threshold Management	Ongoing maintenance and tuning of applicable monitoring thresholds

Identity Management	Included
Monitoring	Monitoring and notification for agreed supported Identity Management and NAC components, subject to the monitoring capabilities available within the solution. Coverage may include appliance health, service availability, node status, resource utilisation, interfaces, and other vendor-exposed health information.
Threshold Management	Ongoing maintenance and tuning of applicable monitoring thresholds

6 Out of Scope

The following items are considered out of scope. This list is provided for guidance and is not exhaustive.

- Monitoring of devices, services, or technologies that have not been agreed and onboarded as part of the service.
- Incident investigation and service restoration are not included. Where Network & Security Resolve is purchased, applicable alerts may be escalated into Resolve in accordance with its contracted service hours and SLAs. Otherwise, the customer is responsible for investigating and resolving notified issues.
- Routine administration, Service Requests, and configuration changes are not included. Where Network & Security Operate is purchased, applicable activities will be delivered under that service; otherwise, they remain the customer's responsibility or may be separately authorised as chargeable professional services.
- Patching, firmware/software updates, and vulnerability remediation are not included. Where Network & Security Patch is purchased, applicable remediation will be delivered under that service; otherwise, it remains the customer's responsibility or may be separately authorised as chargeable professional services.
- Configuration backup and recovery are not included. Where backup status is monitored, Monitor provides detection and notification of backup failures only.
- Security monitoring, SIEM, threat investigation, and SOC services are not included.
- Monitoring is dependent on available connectivity, credentials, protocols, and telemetry. Connectivity failures, polling intervals, or other technical limitations may prevent or delay detection of some events.
- Site attendance, audits, surveys, training, and project work are not included but can be purchased separately outside the scope of this service.

7 Service Level Agreement (SLA)

7.1 Hours of Service

Service	Monday to Friday 08:00 - 18:00	Monday to Friday 18:00 - 08:00	Weekends	Bank holidays
Automated Monitoring & Alerting	Included	Included	Included	Included

Working hours are aligned to UK local time, using Greenwich Mean Time (GMT) or British Summer Time (BST), as applicable.

7.2 Alert Response

Network & Security Monitor provides automated detection, alerting, ticket logging, and notification only.

Where Network & Security Resolve is purchased, applicable monitoring alerts may be routed into Resolve for investigation and service restoration. Response and restoration will then be provided in accordance with the customer's contracted Resolve service hours and SLAs.

Where Resolve is not purchased, the customer is responsible for investigating and resolving notified issues.

7.3 Service Level Measurement

As Network & Security Monitor is primarily an automated service, incident response and restoration SLAs do not apply to Monitor itself.

8 Offboarding

Upon termination or expiration of Network & Security Monitor, Koris365 will facilitate an orderly transition of the service. Following completion of offboarding, Koris365 will have no ongoing responsibility for monitoring, alert generation, or notification under Monitor. Any other contracted Koris365 services will remain unaffected.

8.1 Offboarding Activities

The following activities may be performed as part of the offboarding process:

- Provision of current monitoring documentation maintained under the service agreement.
- Transfer of customer-owned credentials or service account information held by Koris365, where applicable.
- Removal of monitored assets from the Koris365 monitoring platform.
- Removal of Koris365 access that is no longer required for any remaining contracted services.
- Reasonable transition assistance with the customer's internal IT team or designated replacement provider for a period of up to five working days following service termination.
- Delivery of a final summary of the monitoring scope and any known outstanding monitoring issues.

Any transition support, project work, documentation updates, data migration assistance, or knowledge transfer activities that Koris365, acting reasonably, determines to be outside the agreed scope, or unreasonable in nature, complexity, or volume, will be provided on a time-and-materials basis and charged at Koris365's prevailing professional services rates.

8.2 Customer Responsibilities

The customer is responsible for:

- Appointing an authorised contact for transition coordination.
- Ensuring receipt and secure storage of any transferred credentials or documentation.
- Providing any information required to support transition to a replacement monitoring service.
- Confirming completion of the offboarding process within the agreed transition period.
- Changing passwords and disabling accounts as necessary for security purposes.

8.3 Data Retention & Deletion

Customer data will be retained and deleted in accordance with applicable legislation and Koris365 retention policies.

Requests for the latest Customer Data backup must be received within 10 days of service termination or expiry. If no request is received, the data may be deleted.