DATASHEET

Network Detection and Response (NDR)

Get holistic situational awareness of your network to act on cyberattacks immediately.



Detect so you can respond

Protect your network by eliminating blind spots

Open Systems NDR combines IDS and IPS to find compromised systems quickly, and enables efficient analysis and response. The service provides a holistic view of which hosts behave suspiciously in a monitored network by combining the threat intelligence from different sources and assigning a threat score to each of them.

Contrary to conventional detection systems, NDR is built around and focuses on the security of end users rather than on individual events.

The key to managing network breaches is detecting them rapidly. NDR closes the gap between traditional detection and security monitoring and more complex SIEM/SOC solutions.

It complements EDR and XDR by providing visibility into network activity involving systems that cannot run endpoint agents, such as some servers, IoT and OT devices.

What the NDR service delivers

1. Intrusion Detection System (IDS) with signature-based inspection.
2. Intrusion Prevention System (IPS) with anomaly-based inspection and traffic throttling or blocking:
   - Certificate validation checks
   - File filtering
3. Threat intelligence:
   - Multiple sources of threat intelligence signatures
   - Additional feeds including extended Indicators of Compromise (IoCs) of targeted attacks on Common Vulnerabilities and Exposures (CVE); Command and Control (C&C); and JA4 network fingerprints
4. Global event collection and correlation.
5. Machine-learning scoring of security events for host-level threat prioritization.
6. Notification of high threat score.
7. Proactive event investigation and categorization (available only with Mission Control tier).
8. Exclusion lists for events and hosts.
9. Global dashboard.
10. Drilldown from global overview to event details.
11. Host view including context information.
12. Packet capture utility.
13. Inspection of encrypted HTTPS traffic in combination with Secure Web Gateway.

A combination of anomaly and signature inspection methods are used to analyze network traffic and detect network threats, making it possible to respond to suspected intrusions quickly, even automatically. Due to multilayer event processing by a central correlation unit, the generated alerts have maximum relevance in the security context.

Proactive investigation of high-threat events is available with the Mission Control tier.
Open Systems analysts either resolve false positives or escalate suspicious devices to customers for further investigation.

Components

NDR consists of four main components: sensors, threat scores, correlator and the dashboard and Security Center in the Mission Control Portal.



Main components of NDR.

1.

Sensors

Monitor the network, match traffic against their signature base, and generate events upon a match.

2.

Correlator

Analyzes and enriches events from multiple sensors to improve detection accuracy and threat prioritization.

3.

Threat Scores

Indicate whether an infection and/or malicious or unwarranted behavior is likely. A threat score is assigned to each monitored host.

4.

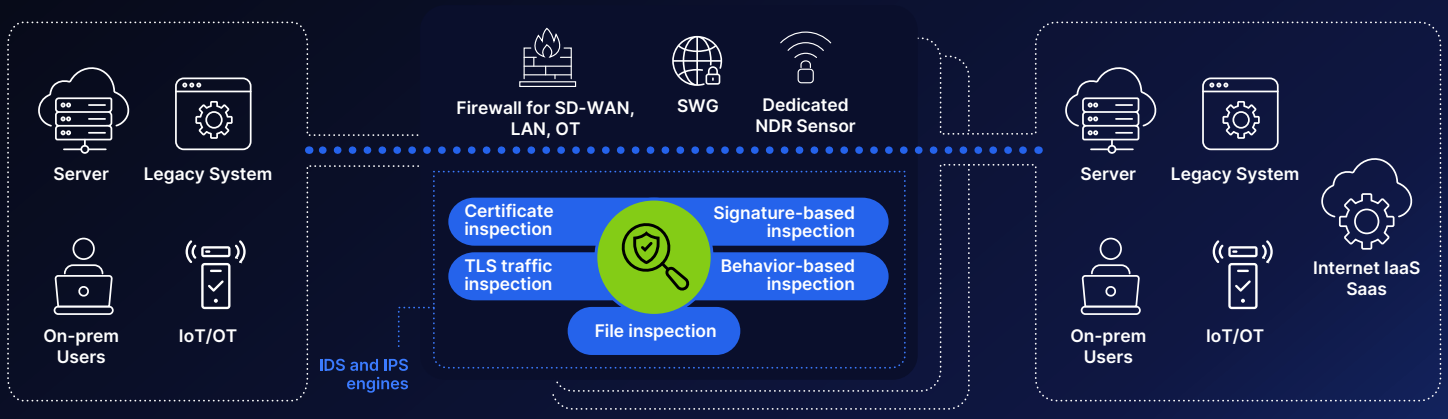
Dashboard and Security Center

Provide a real-time overview of the global threat scores, enabling detailed analysis at the host and event level.

If Secure Web Gateway is part of your subscription, the Web Traffic Tap allows you to monitor even encrypted web traffic.

Sensors

IDS and IPS systems are seamlessly unified on the sensors that can be SD-WAN Firewalls, LAN Firewalls, OT Firewalls, Secure Web Gateways and/or dedicated NDR sensors to provide true global aggregation and correlation of network traffic, even encrypted.



Different types of NDR Sensors.

The traffic is analyzed through packet and behavior inspection as well as more granular aspects like certificate attributes and files, providing lots of information and context to better investigate and block potential suspicious events.

Malware Inspection and Automated Containment

Files transferred over unencrypted network traffic can be extracted and inspected for known malware. By combining network-based file analysis with threat intelligence and malware detection capabilities, suspicious or malicious files can be identified before they spread within the environment.

If malware is detected, Open Systems automatically raises an alert. Relevant context is provided for further investigation. To limit the risk of lateral movement and further compromise, the affected host can be configured to be automatically isolated through the firewall.

Key benefits

- Faster identification of malware before it can spread across the environment
- Reduced investigation effort through validated alerts and enriched threat context
- Faster containment of infected hosts to limit lateral movement
- Lower operational risk through automated response workflows
- Better protection of business applications and sensitive data

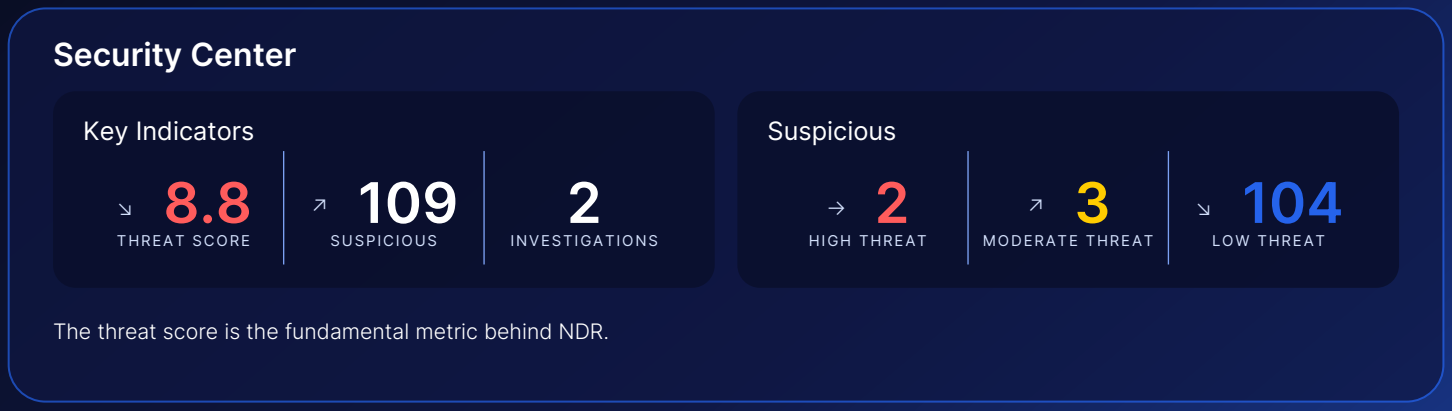


Correlator

The Correlator brings together and processes security events from all NDR sensors. It evaluates incoming signals using detection logic, machine learning, and analyst-defined filters, and raises NDR alerts when activity requires further investigation.

Threat Score

The threat score is the fundamental concept and metric behind detection and response. It consists of a single metric between 0 and 10, and provides an indicator of the likeliness of an infection and/or malicious or unwarranted behavior. A threat score is assigned to each monitored host. Machine learning is used to score detected security events, which contribute to the threat score and level tracked for each monitored IP.



The threat score is the fundamental metric behind NDR.

The host threat score is determined by the most critically scored event for that host. Focusing on hosts rather than single events makes it possible to get better leverage of contextual information about the host, including historical behavior or related events. The inherent prioritization of hosts based on threat scores allows every company – no matter how much security personnel is available – to focus on analyzing the hosts with the highest threat scores first.

Factors that increase or decrease the threat score:

1.

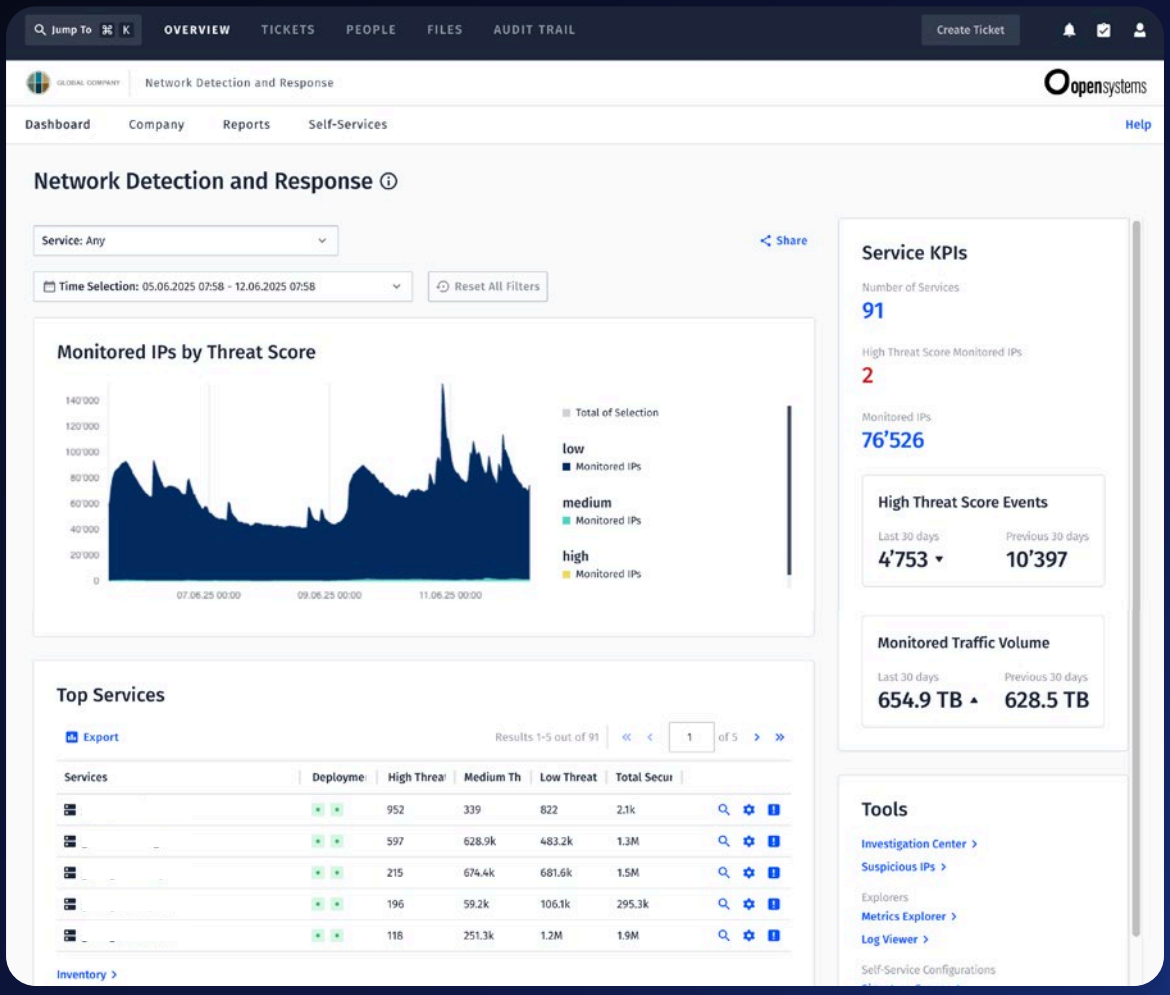
Categorizing a host or events will directly update the threat score of a host. The system assumes that after a categorization the host is tracked internally, and past events no longer attribute to the most current threat score. Categorizing events or hosts also increases or decreases the impact on future threat scores depending on the selected category.

2.

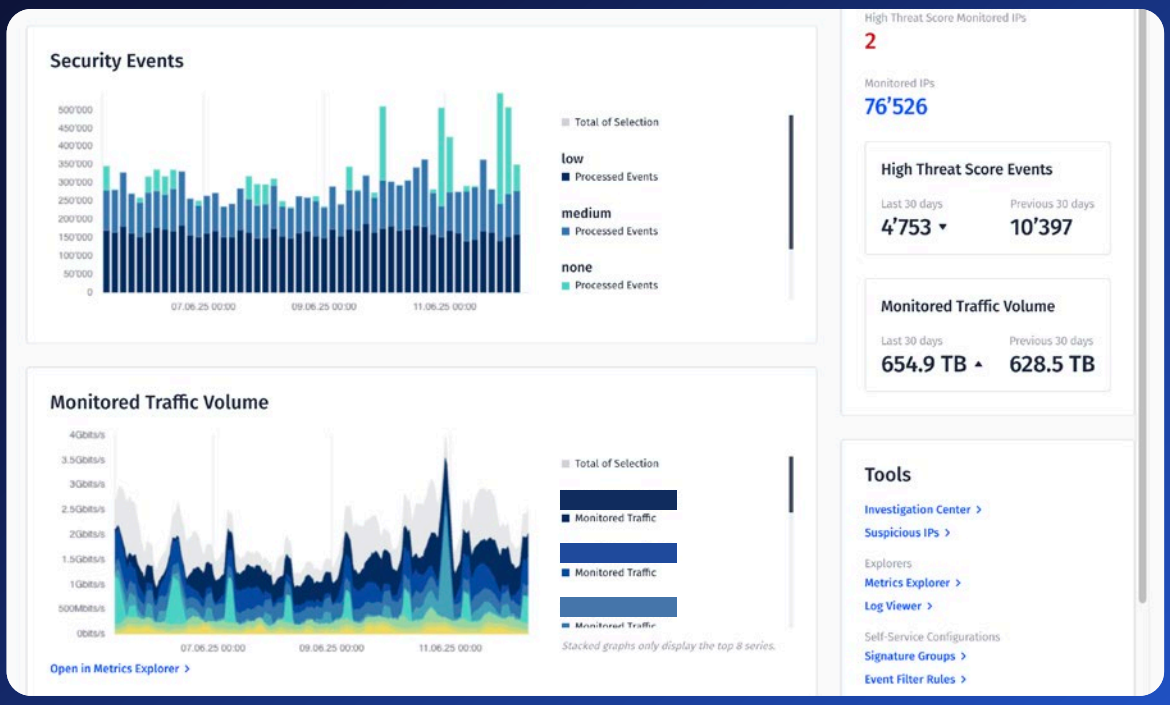
Creating exclusion list entries and filter rules will directly influence the threat score of future events and originating hosts. For example, if an event filter with action “log” is created, corresponding events will no longer trigger a high threat score.

Dashboard

The NDR Dashboard shows the monitored IPs with threat scores in the high, moderate, and low threat levels.



Network Detection and Response dashboard.



Network Detection and Response dashboard.

The metrics can be used as an indicator of the threat observed for a specific location or the company as a whole.

Security Center

The Security Center features key statistics for the sensors, and an overview of all suspicious hosts monitored by the sensor.

A monitored host can have four different threat levels:



High:
The host triggered events which are highly indicative of an infection and/ or malicious behavior.
It should be closely monitored and the root cause for triggering these events analyzed.



Moderate:
The host triggered events which lead to a moderate threat score and hence should be prioritized over hosts with a low threat score. You may choose to investigate such hosts internally depending on your security policy.



Low:
The events that were triggered by this host lead to a low threat score and have low security relevance. These events are usually not related to infections but may still indicate noteworthy behavior of hosts.
A typical example are policy violations.



None:
No events were triggered for the monitored host. The threat score is zero.

Investigation Center

The Investigation Center can be thought of as a company-internal “to do” list for hosts that are marked for investigation. It allows you to track the most pressing threat indicators and helps specify tasks outside of Open Systems ticket handling.

How NDR works

1.
Collect

Define which network traffic and hosts are monitored. NDR sensors inspect the selected traffic and generate security events when relevant activity is detected.

2.
Detect

Define what NDR looks for in monitored traffic, including Indicators of Compromise (IoCs), IDS signatures, and other detection criteria. This determines which network activity is identified for further analysis.

3.
Respond

Detected events are centrally processed, evaluated, and surfaced as NDR alerts when further investigation is required. Investigation outcomes feed back into detection rules and machine learning, helping reduce false positives and improve detection quality over time.

Same detection. More value at each tier.

The alert stream does not change. AIOps adds AI-assisted understanding; Mission Control adds analyst-led validation and escalation on top.



Service Delivery

Edge Platform

- IPv6 compatible.
- Log file distribution via Logs API.

Services run on an Edge Platform whose location is flexible:

Customer Premises Equipment (CPE)

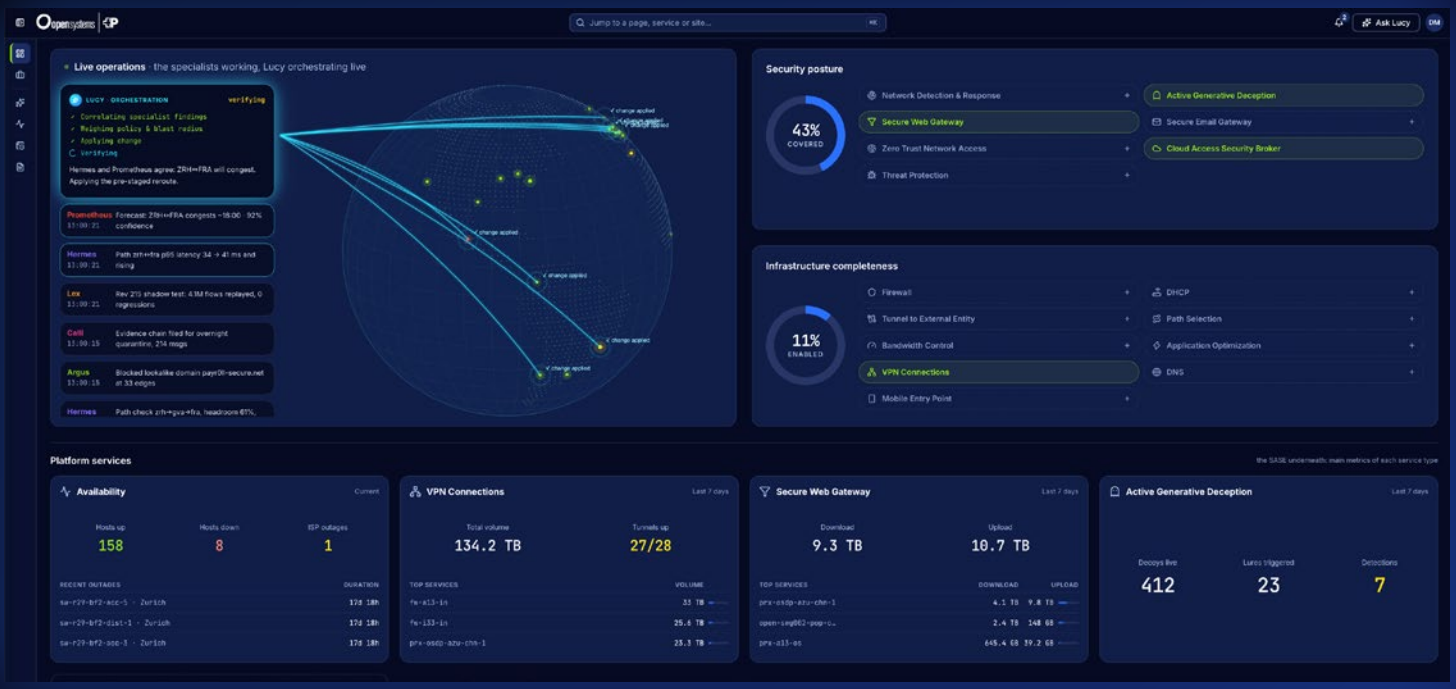
- Services run on premises or at a data center, on extendable, industrial strength hardware for reliable 24×7 operations. A hardened operating system minimizes the attack surface by enabling only essential tools and services, helping improve system stability and security.
- Multi-release boot configuration: The device is capable of booting different releases, which facilitates an effective fallback and rapid recovery if required.

Virtual Customer Premises Equipment (vCPE)

Open Systems services can be provided from the cloud. Public clouds such as Microsoft Azure, Amazon Web Services and Google Cloud Platform are supported as well as private clouds.

Cloud Platform

Built-in security, elastic scalability, and deployment flexibility support operational resilience and data sovereignty requirements, while a global high-performance network delivers reliable service wherever users are located.



Mission Control Portal

The Mission Control Portal provides real-time visibility into network, security, and service operations across the Open Systems platform. Through a unified interface, users can access monitoring, reporting, investigation, configuration, and operational workflows.

The portal combines operational transparency with AI-assisted insights and automation capabilities, enabling teams to investigate events, analyze service health, and accelerate operational tasks. Where available, Lucy provides conversational access to operational information, guided investigations, and workflow assistance.

1. Strong user authentication with audit trail
2. Full audit log
3. Real-time monitoring and reporting
4. Operational dashboards and key performance indicators
5. Event investigation and troubleshooting tools
6. Access to relevant configurations and system information
7. Ticketing and collaboration workflows
8. Delegated administration
9. Self-service and debugging tools
10. AI-assisted insights and workflow support through Lucy

Open Systems is certified for ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018.

HIPAA Compliance Verified by VanRein Compliance 2026

Approved for public use. Open Systems reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Note: Due to the licensing and export restrictions of our technology suppliers, we are not permitted to provide services in certain sanctioned countries. The specific countries affected depend on each supplier's compliance requirements. We therefore refer to the respective suppliers' license terms, which may also apply to end users.

©2026 MS, November 2026