exeon

Exeon.NDR

Modern network defense for a hybrid, encrypted, and evolving threat landscape

Hybrid, distributed, and increasingly encrypted networks create blind spots that traditional security tools can't see into. At the same time, attackers move laterally and faster across IT, OT, and cloud environments.

Exeon.NDR delivers sensorless, metadata-driven network visibility to detect hidden and unknown threats early, reduce noise, and strengthen SOC resilience.

What you gain with Exeon.NDR

Full network visibility, no blind spots

See **all assets and communication paths** across IT, OT, cloud, and hybrid environments – even when traffic is encrypted.

Early detection of advanced threats

Identify lateral movement, APTs, and unknown attacks using **AI-driven behavior analytics and expert rules**.

Less noise, better SOC efficiency

Reduce noise with correlated, **high-fidelity alerts and intuitive** network visualizations that **speed up investigation** and response.

Lower Total Cost of Ownership (TCO)

No sensors or agents to maintain, combined with **strong data reduction that lowers SIEM ingestion and storage costs.**

Fast deployment & integration

No sensor or agent installation required. Built-in detection rules and open APIs enable quick SIEM, SOAR, and SOC integration.

Compliance, data sovereignty & privacy

Supports NIS2/DORA with fast visibility and reporting. **On-prem** deployments and metadata-based analysis ensure **data privacy.**

Trusted by

PostFinance · SWISS · cargolux · LGT · Schweizerische Eidgenossenschaft, Confédération suisse, Confederazione Svizzera, Confederaziun svizra · BonnNetz, Ein Unternehmen der Stadtwerke Bonn

Why act now

Shrinking visibility

90%+ of enterprise network traffic is encrypted, limiting visibility.

Source: Microsoft Digital Defense Report 2024

Faster attacks & SOC overload

Average ransomware dwell time is **~24 hours**, leaving little time to detect and respond.

Source: Secureworks

Unmanaged assets

Over **90%** of successful ransomware attacks originate from unmanaged assets.

Source: Microsoft Digital Defense Report 2024

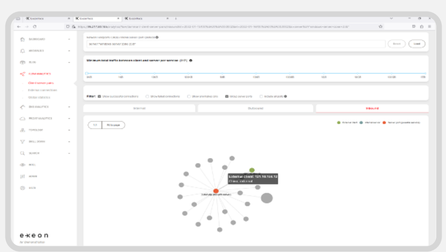
Rising regulatory pressure

DORA/NIS2 require demonstrable, continuous network monitoring and incident reporting.

Source: EU Digital Operational Resilience Act (DORA); EU Network and Information Security Directive (NIS2)

How Exeon.NDR works

Log collection



- Collect logs instantly thanks to sensor/agent-free, metadata-based traffic analytics

- Deploy in days, not months
- No sensors or agents required

Log processing

- Reduce log data thanks to smart data handling
- Communication map for effective correlation

- Normalizes and enriches network metadata
- Full IT/OT/Cloud discovery

Threat detection

- Identify hidden threats with the help of multiple detection layers (AI, static expert rules, ...)

- AI + expert rules = accuracy
- Catch zero-days & APTs fast

Visualization & response

- High-fidelity alerts for faster, high confidence response
- Intuitive GUI and powerful REST-API

- Actionable alerts, not noise
- Seamless SIEM / SOAR integration

Interested in seeing Exeon.NDR in action?

Exeon Analytics AG

exeon.ai

+41 44 500 77 21

contact@exeon.com

CYBERSECURITY MADE IN EUROPE

Gartner Peer Insights