exeon
Smart Cyber Security.

ExeonTrace for corporate networks
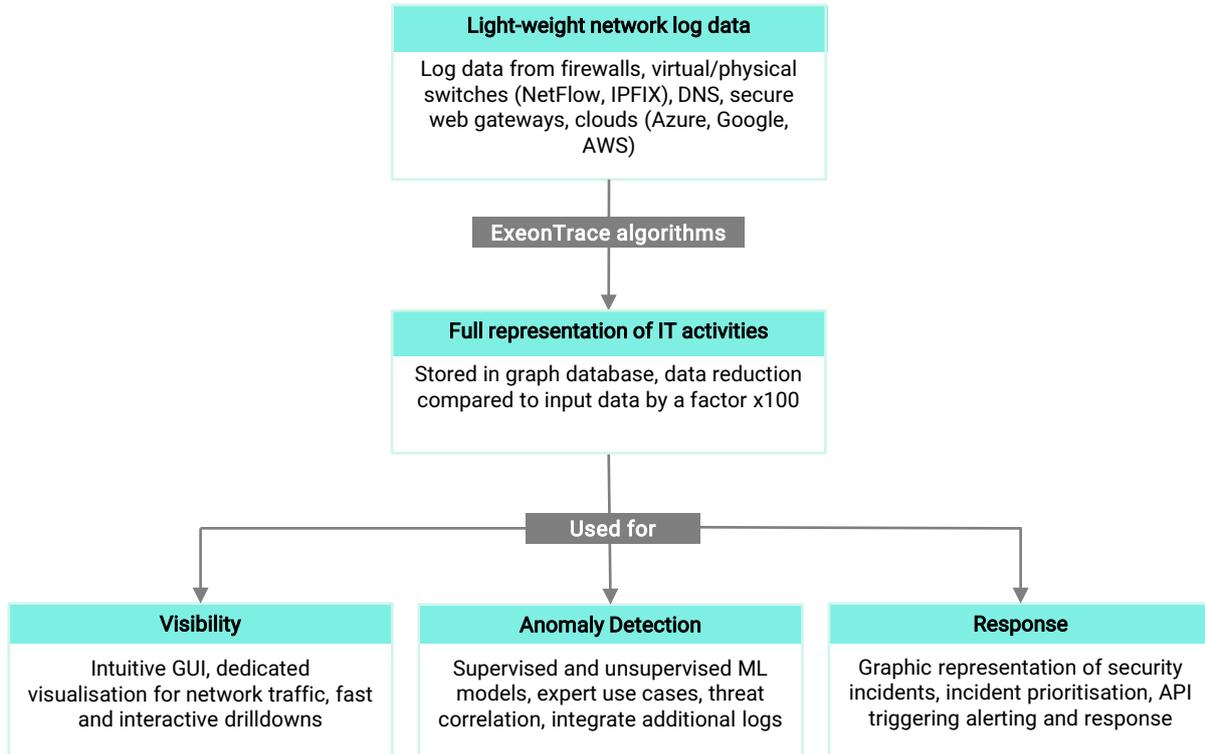
Smart Network Detection & Response

The ExeonTrace Network Detection & Response (NDR) platform is the smart way to strengthen cybersecurity. Powerful ML and proven algorithms provide complete visibility across the entire network, automatically detecting suspicious behavior and helping the respective security team to efficiently assess and combat cyber threats before damage is done.

Why ExeonTrace?

- ✓ ExeonTrace was developed to monitor distributed networks as it does not require any additional hardware sensors and relies on log data analysis

- ✓ ExeonTrace is specialised in protecting cloud, on-premise or hybrid network environments

- ✓ ExeonTrace offers holistic visibility into IT/IoT/OT network communications to identify and respond to cyber threats quickly and effectively

- ✓ ExeonTrace leverages and augments the existing cybersecurity infrastructure (firewalls, SIEM etc.) and completely runs within your network or cloud (full data control)

- ✓ ExeonTrace can be virtually deployed, is compatible with leading network device vendors and easily integrable into the existing cybersecurity infrastructure

- ✓ Exeon is a Swiss vendor, based on more than a decade of academic research at a leading European technical university (ETH Zurich)

PostFinance   3 Banken IT   SWISS   HAAG-STREIT DIAGNOSTICS

PLANZER   solothurner spitäler soH   WIN GD   Universität St.Gallen

How ExeonTrace works

Light-weight network log data
Log data from firewalls, virtual/physical switches (NetFlow, IPFIX), DNS, secure web gateways, clouds (Azure, Google, AWS)

ExeonTrace algorithms

↓

Full representation of IT activities
Stored in graph database, data reduction compared to input data by a factor x100

Used for

Visibility	Anomaly Detection	Response
Intuitive GUI, dedicated visualisation for network traffic, fast and interactive drilldowns	Supervised and unsupervised ML models, expert use cases, threat correlation, integrate additional logs	Graphic representation of security incidents, incident prioritisation, API triggering alerting and response

Visibility – Network data flows easily understood

✓ With unique and intuitive visualizations, large and complex networks can be instantly monitored and easily understood. Data breaches are detected early, and the IT security is strengthened without disrupting ongoing, critical business processes.

Detection – The alarm system for your network

✓ Immediate detection of cyber threats such as advanced persistent threats (APTs), ransomware, supply chain attacks, or data leaks from exposed, insecure systems. Powerful detection, even for threats that span multiple data sources.

Response – Efficient investigation of security incidents

✓ Security alerts can be handled faster and better by immediately displaying all relevant information. Our algorithms minimize false alarms and automatically prioritize incidents by threat level. Security teams save crucial time in security operations and reduce workload.