2022

Factsheet

exeon
Smart Cyber Security.

ExeonTrace

01

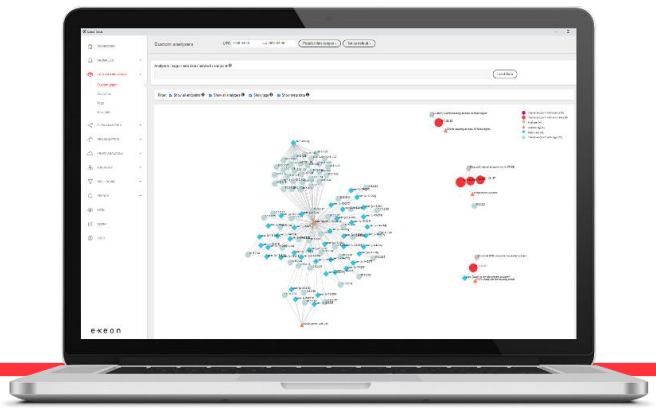
Smart Network Detection and Response

The ExeonTrace Network Detection & Response (NDR) platform is the smart way to strengthen cybersecurity. Powerful AI 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.

02

Why ExeonTrace

- **Rapid Deployment:** Ready in hours. No sensors or agents required
- **Total Visibility:** Unified view of distributed networks, endpoints & applications
- **Vigorous Detection:** Powerful AI and proven algorithms
- **Future-Proof:** Ready for increasing traffic and encryption
- **Effective Response:** Quick assessment, investigation & hunting
- **Clever Data Handling:** Minimal storage needs with full data control



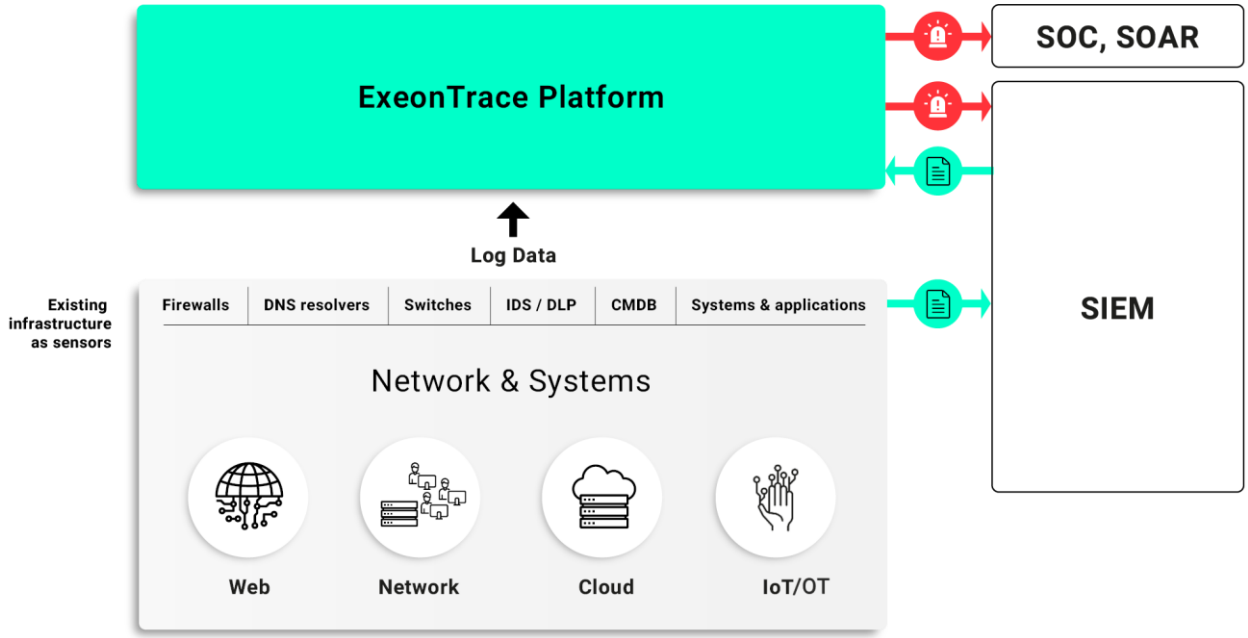
Customers who rely on ExeonTrace, i.a.:

PostFinance · 3 Banken IT · SWISS · HAAG-STREIT DIAGNOSTICS · PLANZER · solothurner spitäler soH · V-ZUG · WIN GD · UNIVERSITÄT BERN

03

How ExeonTrace works

ExeonTrace analyzes security-related log data from the network and systems. As a software-only solution, ExeonTrace uses existing enterprise infrastructure (i.e. firewalls, switches, etc.) as data sensors and does not require additional Hardware-Appliances or sensors.

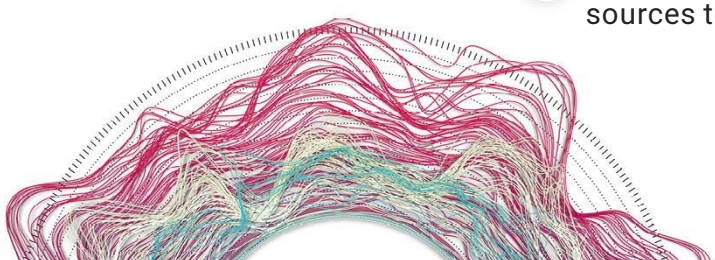


04

Comprehensive 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.

- Identification of hidden data leaks like browser plug-ins or data collecting software
- Finding unusual services in your network
- Exposure of undesired/malicious calls to internal services
- Discovering misconfigured devices
- Unauthorized and outdated devices: Clustering of machine-to-machine (M2M) devices for outlier detection (internal shadow IT)
- Internal Shadow IT: Correlation with CMDB information
- External Shadow IT: Detection of unauthorized cloud services or uploads.
- Correlate network data with other log data sources to cover custom use cases



05

Detection – the Alarm System for your Network

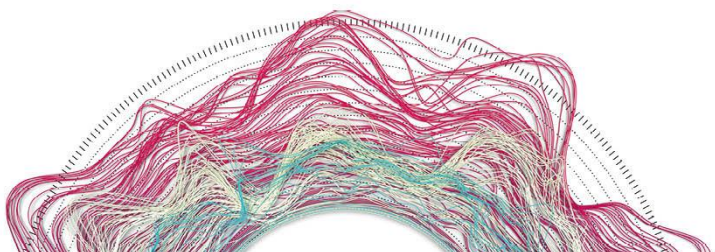
Immediate detection of cyber threats such as advanced persistent threats (APTs), ransomware, supply chain attacks, or data leaks from exposed, insecure systems. Powerful detection, even for threats that span multiple data sources.

- Detecting attackers' hidden HTTP(S)-based command and control channels
- Detecting lateral movements, e.g. the spreading of ransomware and other intrusions in your enterprise network.
- Detecting malware using Domain Generation Algorithms (DGAs)
- Detecting horizontal and vertical scanning within your network
- Detecting covert DNS channel: Hidden data leakage via Domain Name System (DNS)
- Detecting security policy violations
- Blacklist Matching: Correlation with external intelligence

06

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
- Save crucial time in security operations and reduce your team workload
- Intuitive graphical representation of security incidents for effective investigation of the network
- Algorithm-driven threat scoring for efficient incident prioritization
- Rapid queries results (seconds instead of minutes for TB of log data)
- Correlation of data from various data sources to quickly get the full picture



07

ExeonTrace Subscription

Protect your company's IT network with ExeonTrace. Our subscription includes the software license and a support package for setup, training and support from our engineers. The pricing depends on the chosen analysis packages and the number of active internal IP addresses.

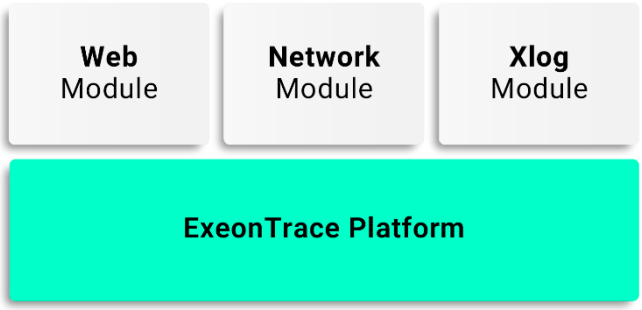
Please contact us for more information or a live demonstration of ExeonTrace.

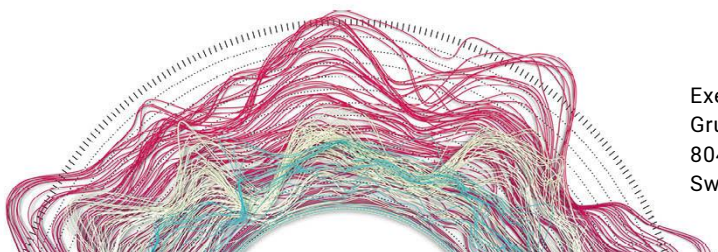
contact@exeon.com

Web Module: **Covering web activities of internal devices**
For proxy logs of SSL/TLS-intercepting Secure Web Gateways

Network Module: **Covering internal & external network traffic**
For NetFlow, IPFIX, Corelight & DNS

Xlog Module: **Cross-data threat detection**
For correlation and analysis of additional security relevant log data, such as general event logs (system and application logs, active directory logs), configuration management database (CMDB) information, security application logs (events created by your EDR, IDS, anti-virus software etc.) or cloud application logs





Exeon Analytics AG
Grubenstrasse 12
8045 Zürich
Switzerland

contact@exeon.com