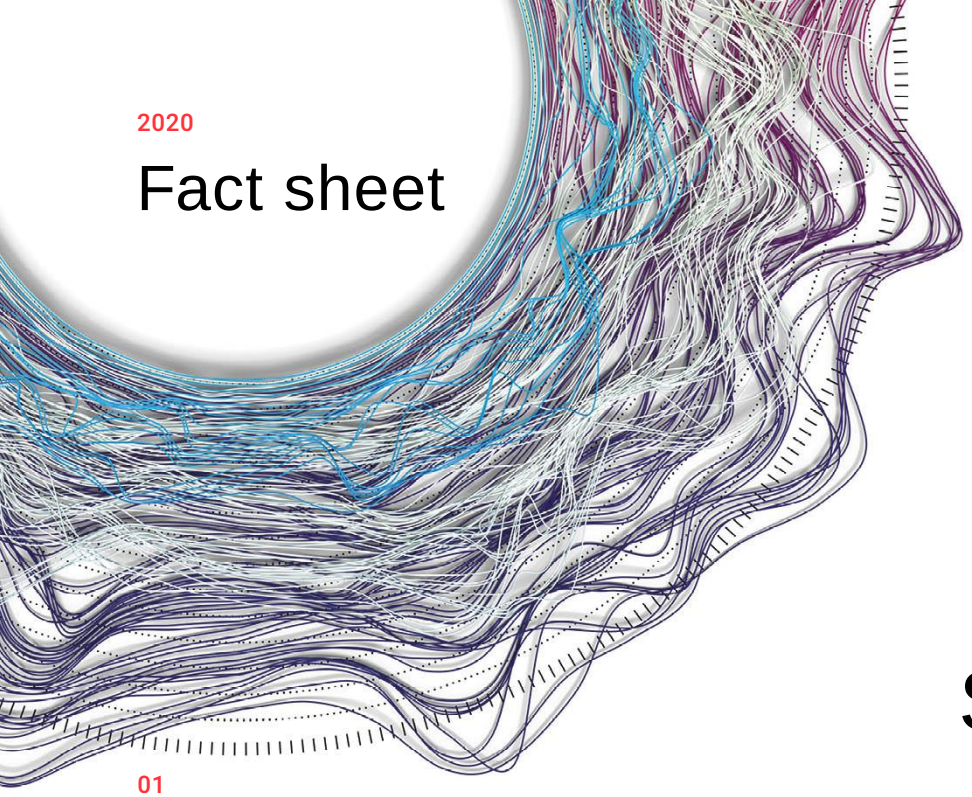
2020

Fact sheet

exeon

Detecting Hidden
Cyber Threats.



ExeonTrace Subscription

01

Visibility into data leaving your organization

Cyber attackers and malicious insiders regularly circumvent IT protection measures and breach highly sensitive data.

Such breaches often happen in plain sight, hidden in millions of regular activities caused by daily business operations and remain undetected over several months. Exeon is specialized in detecting hidden data breaches and advanced cyber attacks. We find the so-called needle in the haystack with our ExeonTrace analysis and visualization software.

02

Why ExeonTrace

Best-in-class algorithms for network traffic analysis
A high detection rate and few false positives are the basis for your cyber security.

No dedicated hardware required, easy and light-weight to set up
ExeonTrace does not need dedicated hardware sensors. It analyzes log data exported by your existing IT infrastructure, making the ExeonTrace software appliance operational from day one.

You remain in control of your data
ExeonTrace can be operated completely offline.
You decide if ExeonTrace is set up on-site or in your trusted cloud.

Integration into your existing environment
ExeonTrace collects log data itself or analyzes existing log stored in Splunk or Elasticsearch.

03

ExeonTrace Subscription

Would you like to use ExeonTrace to protect your organization? Our annual subscription includes the software license and a support package for setup, training and support through 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.

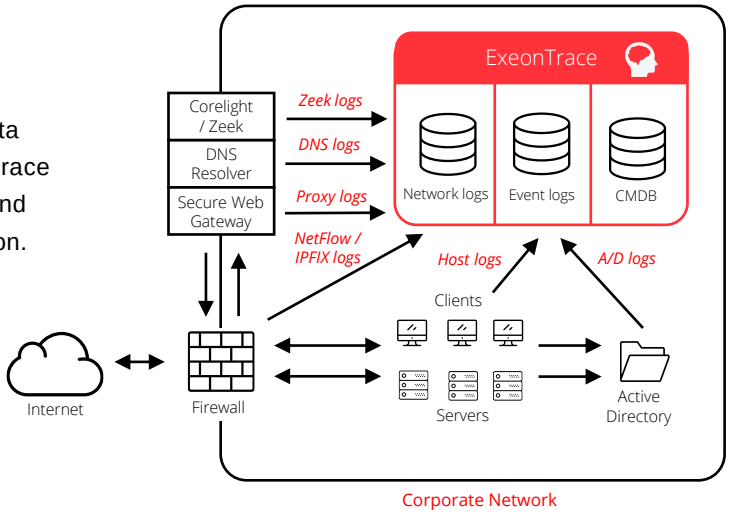
04

How ExeonTrace works

ExeonTrace effectively identifies gaps in IT security perimeters and detects anomalies in millions of IT data points (log data). Contrary to other solutions, ExeonTrace can analyze and correlate various log data sources and thus represents a holistic solution for your organization.

ExeonTrace integrates:

- Network traffic logs (Proxy, NetFlow/IPFIX, Corelight and DNS data)
- Event logs (Host logs, Active Directory logs)
- Configuration management database (CMDB)



05

Packages

ExeonTrace offers two analysis packages. The packages can be selected independently or jointly. Package one analyzes proxy log data and package two analyzes flow and DNS log data.

Package 1
Proxy/secure web gateway analysis

Analysis of the **web activities** of your internal devices.

✓ **APT attack detection**
- Detecting hidden HTTP(S)-based command and control channels
- Detecting malware using Domain Generation Algorithms (DGAs)

✓ Detection of **hidden data leaks** such as browser plugins or software collecting data

✓ **External shadow IT:** Detection of unauthorized cloud services and uploads

✓ **Unauthorized and outdated devices:** Clustering of machine-to-machine (M2M) devices for outlier detection

✓ Identification of **unauthenticated proxy access**

✓ Correlation with selected **threat feeds** (blacklists)

Requirements: Proxy logs recorded by an SSL/TLS-intercepting secure web gateway.

Package 2
Flow and DNS analysis

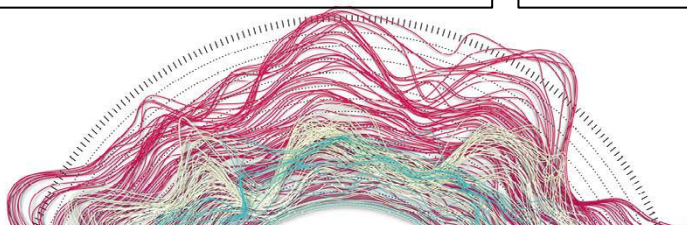
Analysis of your **internal & external** network traffic.

✓ **APT attack detection**
- Detecting lateral movement: Expansion of malicious software in your network
- Detecting horizontal and vertical scanning inside your corporate network
- Detecting malware using Domain Generation Algorithms (DGAs)
- Detecting covert DNS channel: Hidden data leakage via Domain Name System (DNS)

✓ **Network visibility**
- Discovery of unusual services in your network
- Discovery of undesired/malicious access to internal services
- Identification of misconfigured devices
- Understand communication of critical networks

✓ Correlation with selected **threat feeds** (blacklists) and **CMDB information** (internal shadow IT)

Requirements: Firewalls/switches capable of exporting NetFlow v5/v9/IPFIX log data or Corelight sensors. DNS logs recorded by our network sensor or your DNS resolvers.



exeon.ch

Exeon Analytics AG
Grubenstrasse 12
8045 Zurich
Switzerland

info@exeon.ch