From Visibility to Action: Exeon.NDR Enhances PostFinance Security

Banking success story

PostFinance's business context

PostFinance is one of Switzerland's leading retail financial institutions. Founded in 1906, it is the financial services unit of the Swiss Post.

As a market leader with **1.4 billion payment transactions** a year, it ensures a seamless flow of liquidity daily.

As a licensed bank, PostFinance is subject to supervision by the FINMA and must comply with regulatory requirements related to operational resilience, cybersecurity monitoring, and incident response. This includes adherence to FINMA guidelines on ICT risk management and outsourcing, as well as data protection obligations under the GDPR where applicable.

Initial situation

1. Far-reaching requirements of the Swiss Financial Market Supervisory Authority (FINMA)
2. Best-of-breed approach with various interfaces to surrounding systems
3. Mirroring the whole network traffic was not an option
4. Broad evaluation of leading suppliers
5. Seeking complete visibility into the highly virtualized IT infrastructure

The challenges

1. Define an architectural approach that follows a best-of-breed strategy across all security-relevant segments, including threat detection, threat hunting, vulnerability management, and others.
2. Exclude full network traffic mirroring as an option, thereby establishing high integration requirements for the Network Detection & Response (NDR) solution with surrounding security systems.
3. Conduct a broad evaluation of the leading Network Detection & Response providers.

Testimonial

"PostFinance has chosen Exeon.NDR because of its open and future-proof architecture. Not needing any hardware sensors and being able to control data flows, we didn't have to make any significant changes to our existing infrastructure.

We are also convinced by the cooperation with the competent and technically outstanding Exeon team."

— Head IT Security, PostFinance

PostFinance

exeon

The solution

Exeon.NDR was the most successful in detecting the tested use cases in the Red Team Proof of Concept.

- Tested use cases included:
  - Lateral movements
  - Domain Generation Algorithms (DGA)
  - Hidden DNS channels
  - Command & Control channels
  - Various threat hunting use cases

- Integration and support:
  - Multi-year licensing and support to integrate Exeon.NDR into PostFinance's cybersecurity architecture.
  - The solution is deeply integrated into PostFinance's core systems.
  - Multiple PostFinance locations are covered by the implementation.

Exeon.NDR's Benefits

Highly integrated Network Detection & Response supporting the multi-faceted protection of PostFinance core systems.

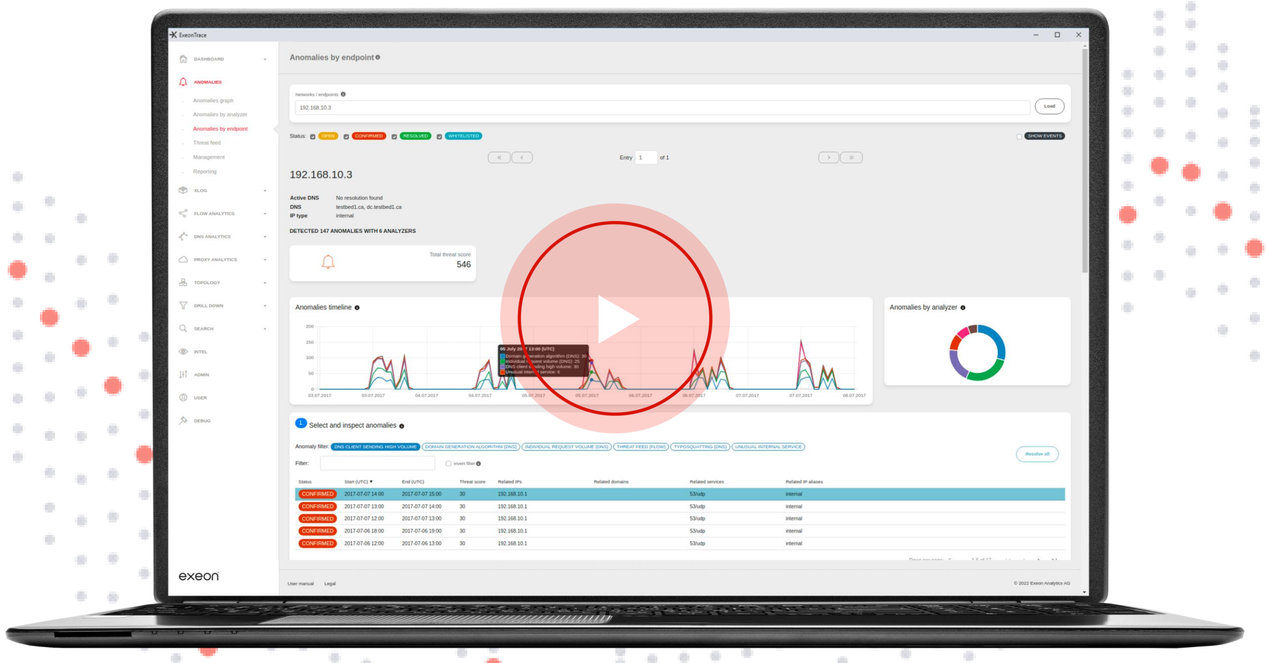
Easy navigation through the historic log data for complete visibility directly in the Exeon.NDR interface – achieved through a graph database that reduces the required storage.

Complete visibility into the highly virtualized IT infrastructure of PostFinance.

Continuous, real-time monitoring of industry-specific assets, such as ATMs.

Ongoing support in integrating Exeon.NDR in the customer's wider technological stack and security architecture.

Automatic reporting and documentation are generated for compliance with the various regulations.



Monitoring ATM machines - continent-wide demo video

Watch how extended logs in Exeon.NDR are used to create completely new use cases and solve even complex requirements very simply.

Watch demo

Gartner Peer Insights™

★★★★★

Learn more

exeon.ai