Banking-Erfolgsgeschichte

# Von Transparenz zu schneller Reaktion: Exeon.NDR bei PostFinance

## Über das Unternehmen

**PostFinance**

Gegründet 1906 · Bern, Schweiz · Retail-Banking

PostFinance ist eines der führenden Retail-Finanzinstitute der Schweiz. Gegründet im Jahr 1906, ist PostFinance die Finanzdienstleistungseinheit der Schweizerischen Post. Als Marktführer mit 1,4 Milliarden Zahlungstransaktionen pro Jahr sorgt das Unternehmen täglich für einen reibungslosen Zahlungs- und Liquiditätsfluss.

PostFinance wird von der FINMA beaufsichtigt und muss regulatorische Anforderungen an die Betriebsresilienz, die Überwachung der Cybersicherheit sowie das Incident-Response-Management erfüllen. Dies umfasst die Einhaltung der ICT-Risikomanagement- und Auslagerungsrichtlinien der FINMA sowie der relevanten Datenschutzverpflichtungen gemäss DSGVO.

## Ausgangslage

- Weitreichende Anforderungen der Eidgenössischen Finanzmarktaufsicht (FINMA)
- Best-of-Breed-Ansatz mit zahlreichen Schnittstellen zu bestehenden Sicherheitssystemen
- Vollständige Netzwerkverkehrsspiegelung war keine Option
- Umfassende Evaluation führender NDR-Anbieter
- Ziel war eine vollständige Transparenz über die hochvirtualisierte IT-Infrastruktur

## Herausforderungen

### HERAUSFORDERUNG 01

**Definition eines Architekturansatzes nach dem Best-of-Breed-Prinzip**

Über sämtliche sicherheitsrelevanten Bereiche hinweg - einschliesslich Bedrohungserkennung, Threat Hunting, Schwachstellenmanagement und weiterer sicherheitsrelevanter Funktionen.

### HERAUSFORDERUNG 02

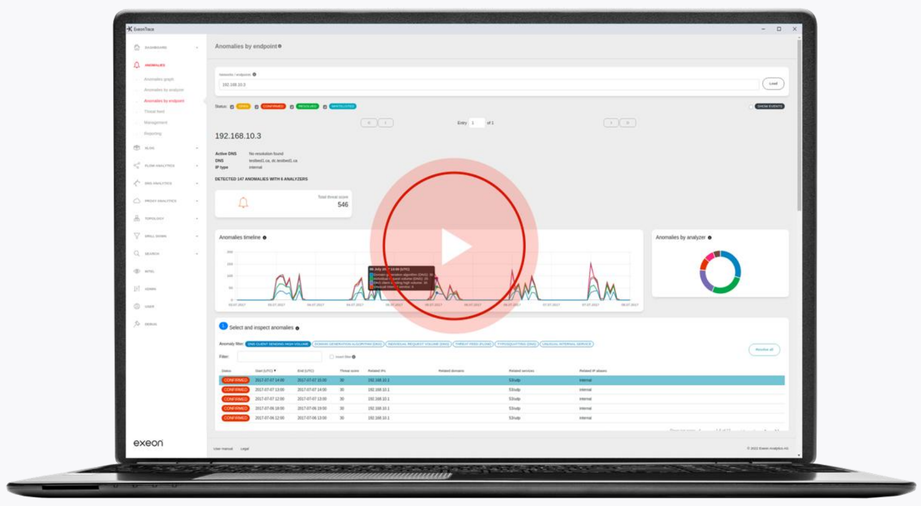
**Die vollständige Spiegelung des Netzwerkverkehrs als Option ausschliessen**

Dadurch entstanden hohe Anforderungen an die Integration der Network Detection & Response (NDR)-Lösung in bestehende Sicherheitssystemen.

### HERAUSFORDERUNG 03

**Umfassende Evaluation führender NDR-Anbieter**

Bewertung führender Network Detection & Response-Lösungen im Hinblick auf die Monitoring- und Integrationsanforderungen von PostFinance.




**Demo-Video ansehen — Kontinentweites ATM-Monitoring**

> PostFinance hat sich für Exeon.NDR entschieden, weil es eine offene und zukunftssichere Architektur bietet. Da keine Hardware-Sensoren benötigt werden und die Datenflüsse kontrollierbar sind, mussten wir keine wesentlichen Änderungen an unserer bestehenden Infrastruktur vornehmen. Wir sind zudem von der Zusammenarbeit mit dem kompetenten und technisch hervorragenden Exeon-Team überzeugt.
>
> — **Leiter IT-Sicherheit**, PostFinance

## Ergebnisse

Exeon.NDR erzielte im Red-Team-Proof-of-Concept die stärkste Erkennungsleitung für die definierten Use Cases.

**Zu den getesteten Use Cases gehörten:**

- Lateral movements
- Domain Generation Algorithms (DGA)
- Versteckte DNS-Kanäle
- Command & Control-Kanäle
- Threat-Hunting-Use-Cases

**Integration & Support:**

- Mehrjährige Lizenzierung und laufender Support zur Integration von Exeon.NDR in die Cybersicherheitsarchitektur von PostFinance
- Die Lösung ist nahtlos in die Kernsysteme von PostFinance integriert
- Die Implementierung deckt mehrere PostFinance-Standorte ab

## Mehrwert durch Exeon

1. **Hochintegrierte NDR-Lösung** für die umfassende Absicherung der PostFinance-Kernsysteme.
2. **Einfache Navigation durch historische Logdaten** für vollständige Transparenz direkt in der Exeon.NDR-Oberfläche - ermöglicht durch eine Graphdatenbank mit reduziertem Speicherbedarf
3. **Vollständige Transparenz über die hochvirtualisierte IT-Infrastruktur** von PostFinance.
4. **Kontinuierliche Echtzeitüberwachung** kritischer Systeme wie Geldautomaten.
5. **Laufender Support** bei der Integration von Exeon.NDR in bestehende Technologie-Stacks und Sicherheitsarchitekturen.
6. **Automatische Berichterstellung und Dokumentation** zur Einhaltung regulatorischer Anforderungen.

**Andere Finanzinstitute, die Exeon.NDR vertrauen**

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

LGT

3 Banken IT

## Kontakt


UNTERNEHMEN
**Exeon Analytics AG**

WEBSITE
**exeon.com**

EMAIL
**contact@exeon.com**

TELEFON
**+41 44 500 77 21**


Demo buchen