exeon

Rethinking Threat Detection & Response

An Evaluation Guide for BFSI Security & IT Leaders

exeon.com

Why 2026 Is a Defining Moment for BFSI Cyber-Defense

Banking, financial services, and insurance (BFSI) organizations are operating in an environment where visibility is shrinking while attack sophistication is accelerating.

- Over 90–95% of network traffic is now encrypted, limiting traditional inspection methods
- Financial institutions remain among the top 3 most targeted industries globally
- AI-assisted attacks (automated phishing, adaptive malware, polymorphic C2) are now mainstream
- Regulations such as Digital Operational Resilience Act (DORA) and NIS2 Directive are now actively enforced, not just planned

Security Operations Centers (SOCs) are under pressure:

- Persistent talent shortages (≈65–75% of SOCs report gaps)
- High alert volumes with 30–50% still classified as low-value noise
- Increased pressure for real-time reporting and auditability

The result:
More complexity, less clarity, stricter accountability.

BFSI leaders are re-evaluating the role of:

- Network Detection & Response (NDR)
- SIEM and next-gen data platforms
- Detection engineering and automation

Modern NDR has emerged as a critical control layer to restore visibility, reduce dwell time, and support regulatory compliance, without adding operational burden.

What to Look for in a Modern Threat Detection & Response Platform

These are the five lenses seasoned decision-makers use when short-listing NDR, SIEM or Intrusion Detection System (IDS) vendors.

Each angle reflects lessons learned across European and global banks that replaced first-generation tools with new, ML-driven platforms.

01 **Holistic Visibility in Encrypted & Hybrid Environments**

02 **Architecture Simplicity & Cost Efficiency**

03 **SOC Productivity & Detection Quality**

04 **Compliance & Audit Readiness by Design**

05 **Measurable Business Impact & ROI**

01 Holistic Visibility in Encrypted & Hybrid Environments

Traditional Intrusion Detection Systems (IDS) approaches relying on packet inspection are no longer sufficient.

As a result, attackers exploit the blind spots between cloud and on-premises, and between managed and unmanaged devices (like IoT/OT), to move laterally and exfiltrate data undetected.

Modern platforms must:

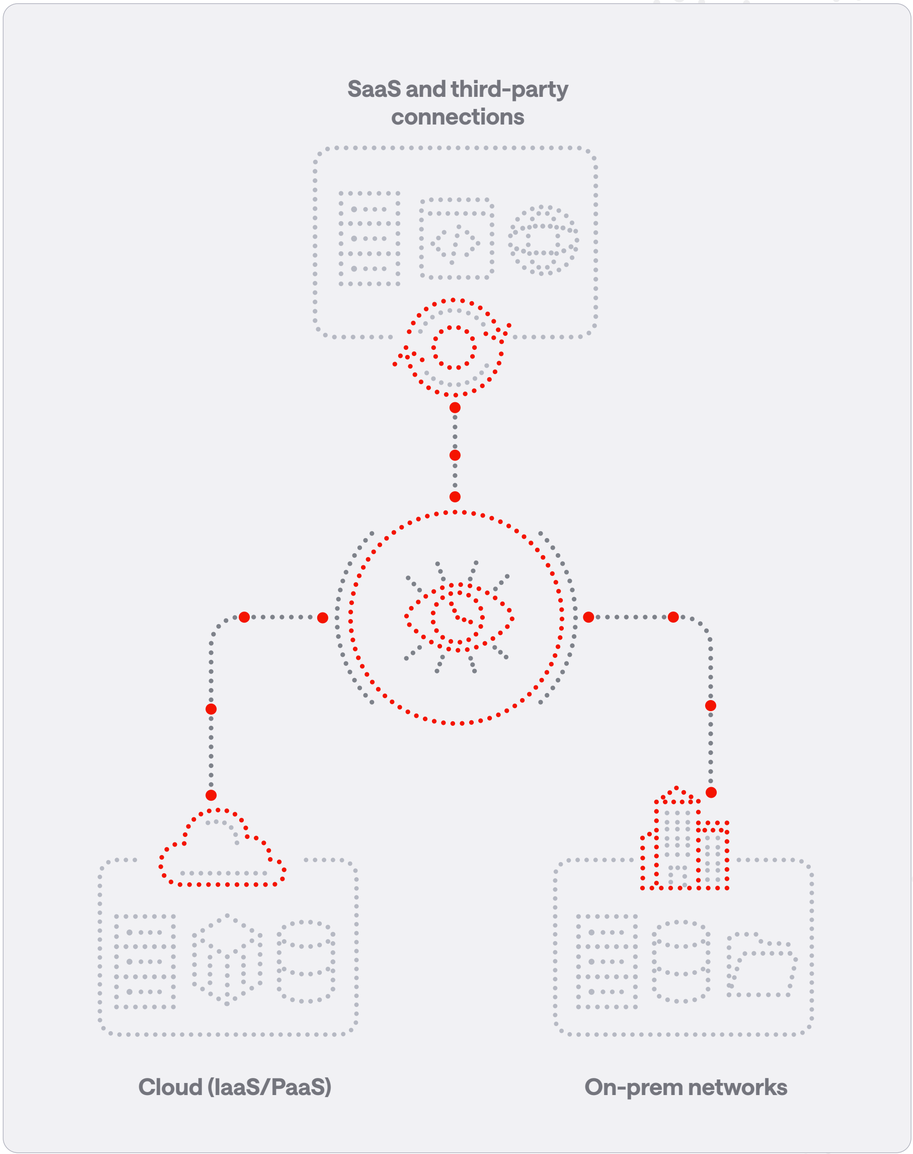
Provide visibility across:

- On-prem networks
- Cloud (IaaS/PaaS)
- SaaS and third-party connections

Analyze:

- Network flows
- DNS
- Identity-linked activity
- East-West traffic* patterns

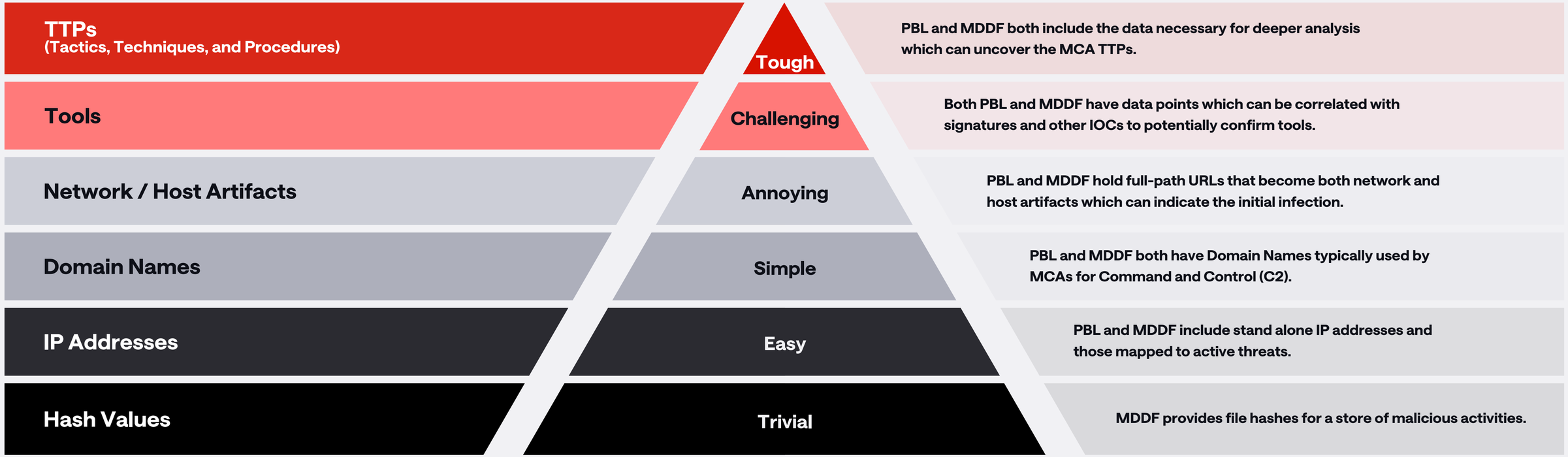
*East–West traffic refers to the movement of data between systems within the same internal network, often representing lateral communication that attackers can exploit after gaining initial access.



The Pyramid of Pain
Prioritizing What Truly Disrupts Attackers

Shift focus from transient IOCs to enduring TTPs.

IOC Based Detection: Catches known bad artifacts (like specific IPs or file hashes).
TTP Based Detection: Catches the attacker's behavior, making it far harder to evade.



What to look for in a modern NDR, SIEM or Intrusion Detection System (IDS)

Behavioral analytics (ML + Statistical Models)

Detection of TTPs (not just static IOCs)

As well as the coverage of:

Lateral movement

Covert Channels

Data Exfiltration

AI-Driven Attack Patterns

Achieving holistic security in encrypted and hybrid environments requires moving beyond isolated tools.

While behavioral analytics and TTP detection are critical capabilities,
the ultimate goal is a unified defense where NDR, SIEM, and EDR work as a cohesive system.

02 Architecture Simplicity & Cost Efficiency

Complex, sensor-heavy architectures have proven difficult to scale in modern BFSI environments, particularly as networks extend across branches, data centers, and cloud. Over time, the operational overhead and hidden costs of managing distributed sensors can outweigh their initial value. Modern NDR should therefore be designed with simplicity and efficiency in mind.

Key capabilities to look for include:

1 Adopt a Sensor-Light or Sensor-Free Architecture

The platform should minimize or eliminate the need for additional hardware or distributed appliances, reducing deployment complexity and ongoing maintenance effort across the environment.

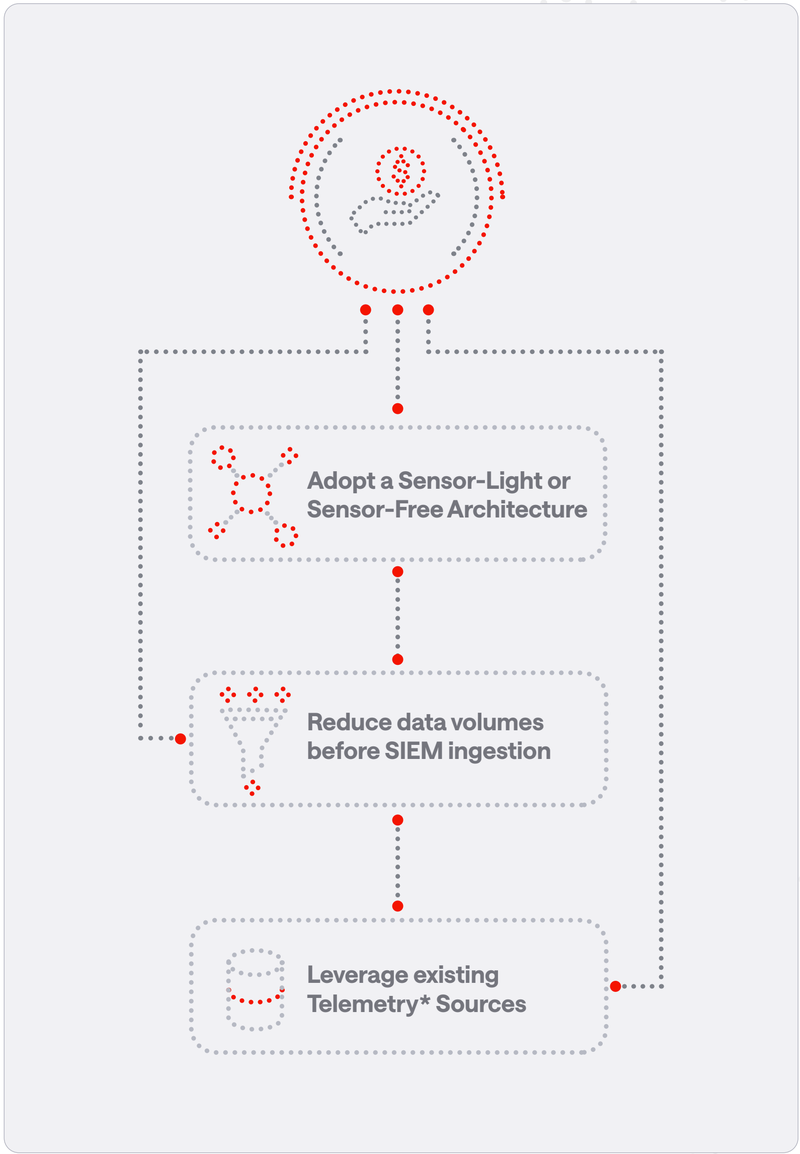
2 Reduce data volumes before SIEM ingestion

By aggregating, enriching, and compressing telemetry upstream, modern NDR platforms can significantly lower the volume of data sent downstream, often by a factor of 10× to 100×, with a direct impact on storage costs and licensing models.

3 Leverage existing Telemetry* Sources

Rather than introducing new data collection layers, the solution should make full use of already available data, such as NetFlow, firewall and proxy logs, DNS activity, and cloud-native metadata, accelerating deployment while avoiding duplication.

*Telemetry is the continuous collection and transmission of data from systems, networks, and devices to monitor activity, detect threats, and support analysis.



Vendor Evaluation

Look beyond feature lists and assess the broader architectural and financial implications.

Question 1:

What infrastructure is required across branches, data centers, and cloud environments?

Question 2:

What is the true three-year total cost of ownership, including storage, computer, and ongoing maintenance?

Key takeaway:

The most effective solutions are those that reduce architectural complexity while delivering scalable visibility, resulting in a more predictable and defensible cost structure over time.

03 SOC Productivity & Detection Quality

The goal is not more alerts — It's better decisions, faster.

Key capabilities to look for include:

1 Operational risk-based prioritization that reflects real-world impact

Alerts should be dynamically scored and contextualized based on factors such as asset criticality, behavioral severity, and attack progression. This ensures that analysts focus first on what matters most to the business, rather than working through undifferentiated queues.

2 Explainable detections ("White-Box" Analytics)

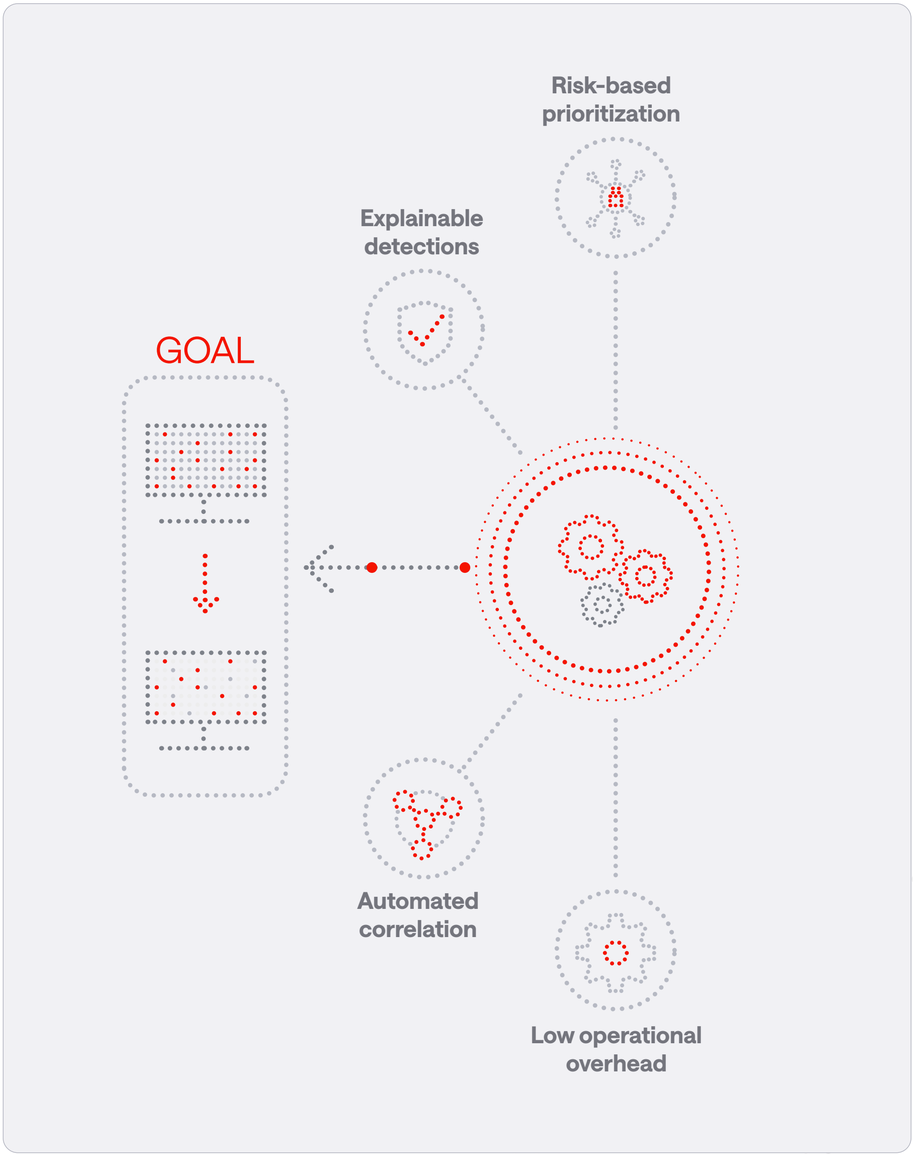
Analysts should be able to understand why an alert was generated, what data points contributed to it, and how it fits into a broader attack pattern. Transparent detection logic builds trust, accelerates triage, and enables teams to fine-tune rules without relying on external support.

3 Automated correlation across the attack lifecycle

Rather than presenting isolated events, the platform should connect signals across multiple stages of an attack, such as initial access, lateral movement, and data exfiltration, all into a coherent narrative. This reduces investigation time and helps teams quickly assess scope and impact.

4 Low operational overhead and minimal tuning requirements

In resource-constrained SOCs, platforms must deliver value out of the box. Look for solutions that require limited manual rule adjustments, support adaptive learning, and provide built-in mechanisms for reducing recurring noise (e.g., whitelisting, baselining).



Vendor Evaluation

When evaluating vendors, prioritize measurable outcomes over feature claims – ideally validated during a pilot phase.

40–70%

Reduction in false positives

Clear decrease in low-value alerts and improved signal-to-noise ratio.

Faster cycles

Minutes instead of hours spent on investigation

Analysts can move from alert to actionable insight without complex queries or tool switching.

High usability

Across analyst levels

Both junior and senior analysts can quickly understand and act on detections.

30-60 days

Stable performance after initial tuning

Limited manual effort required to reach and maintain a high-quality detection baseline.

The key question:

Does the platform consistently reduce noise,
while accelerating response in day-to-day SOC operations?

04 Compliance & Audit Readiness by Design

In 2026 and beyond, compliance is no longer a periodic exercise, it is a continuous operational requirement. Detection platforms must therefore not only identify threats, but also provide clear, audit-ready evidence at any point in time.

Key capabilities to look for include:

1 Support for sovereign and on-premise deployments

Given strict data residency requirements in BFSI, the platform should offer flexible deployment options that ensure sensitive data remains within national or regional boundaries (e.g., EU or Switzerland).

2 Long-term data retention with accessible historical context

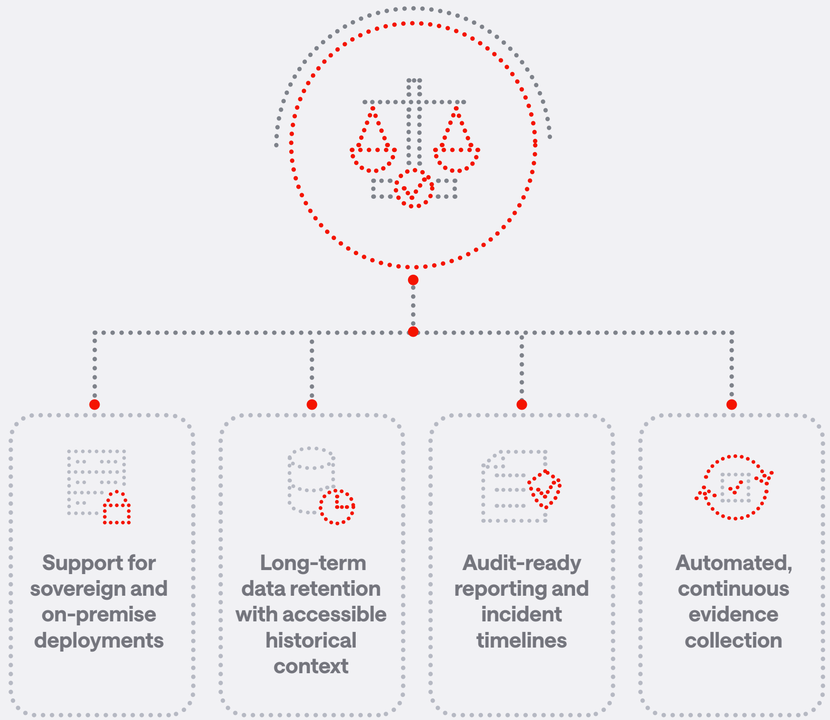
The platform should support retention of relevant telemetry (typically 12 months or more), allowing teams to investigate incidents and demonstrate compliance without relying on fragmented data sources.

3 Audit-ready reporting and incident timelines

Security events should be automatically structured into clear timelines, including affected systems, attack progression, and response actions. This eliminates the need for manual reconstruction when responding to auditors or regulators.

4 Automated, continuous evidence collection

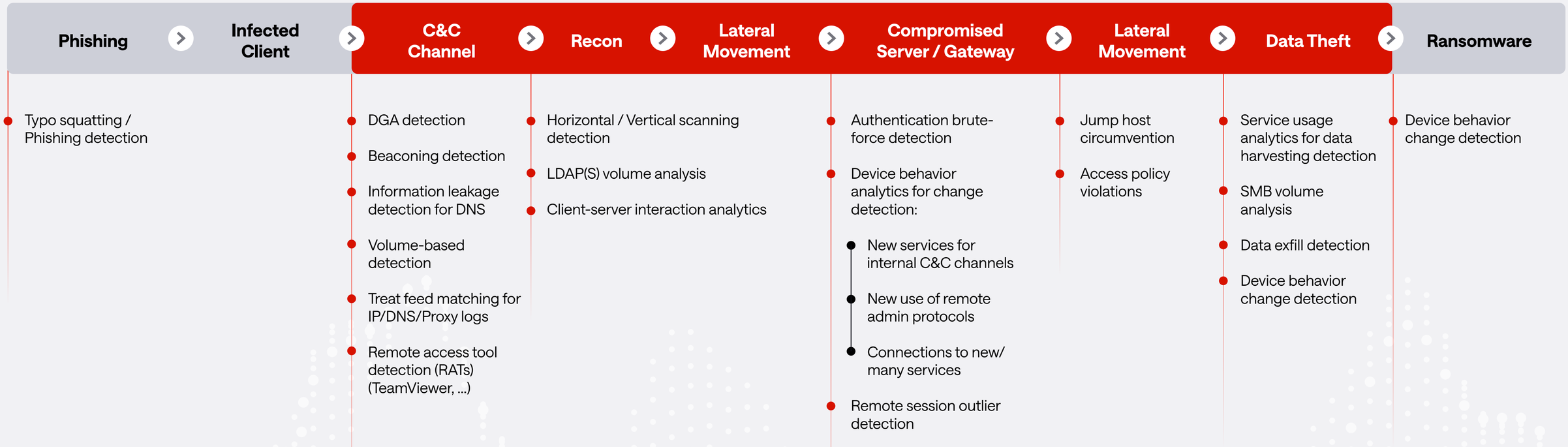
The platform must automatically gather and preserve proof of control effectiveness (e.g., access logs, configuration states, incident timelines) in real time. This creates a continuous, immutable audit trail, turning compliance from a point-in-time effort into an always-on state.



Native mapping to regulatory frameworks & security standards

Detections should be automatically aligned with frameworks such as **MITRE ATT&CK**, as well as regulatory requirements like **Digital Operational Resilience Act and NIS2 Directive**.

This enables faster reporting, consistent classification of incidents, and reduced manual effort during audits.



Vendor Evaluation

Focus on how easily the platform
translates detection into compliance outcomes.

Dashboard access

Access to dashboards and options to export audit-aligned and incident evidence.

Data control

Data hosting and processing sovereignty as well as strict privacy.

Alert mapping

Clear mapping of alerts to regulatory controls and known frameworks.

Effortless reporting

Ability to support regulatory reporting timelines without manual effort.

The key question:

Does the platform turn security operations
into continuous, audit-ready compliance by default?

05 Measurable Business Impact & Return On Investment

Cybersecurity investments in BFSI must be justified not only technically, but also in terms of tangible business impact. Detection platforms are increasingly expected to demonstrate how they reduce risk, control cost, and improve operational efficiency.

Key capabilities to look for include:

1 Reduction of breach risk and potential financial impact

By improving visibility and detection speed, the platform should contribute to lowering the likelihood and impact of incidents, particularly those affecting critical systems such as payments or core banking.

2 Lower SIEM and data management costs

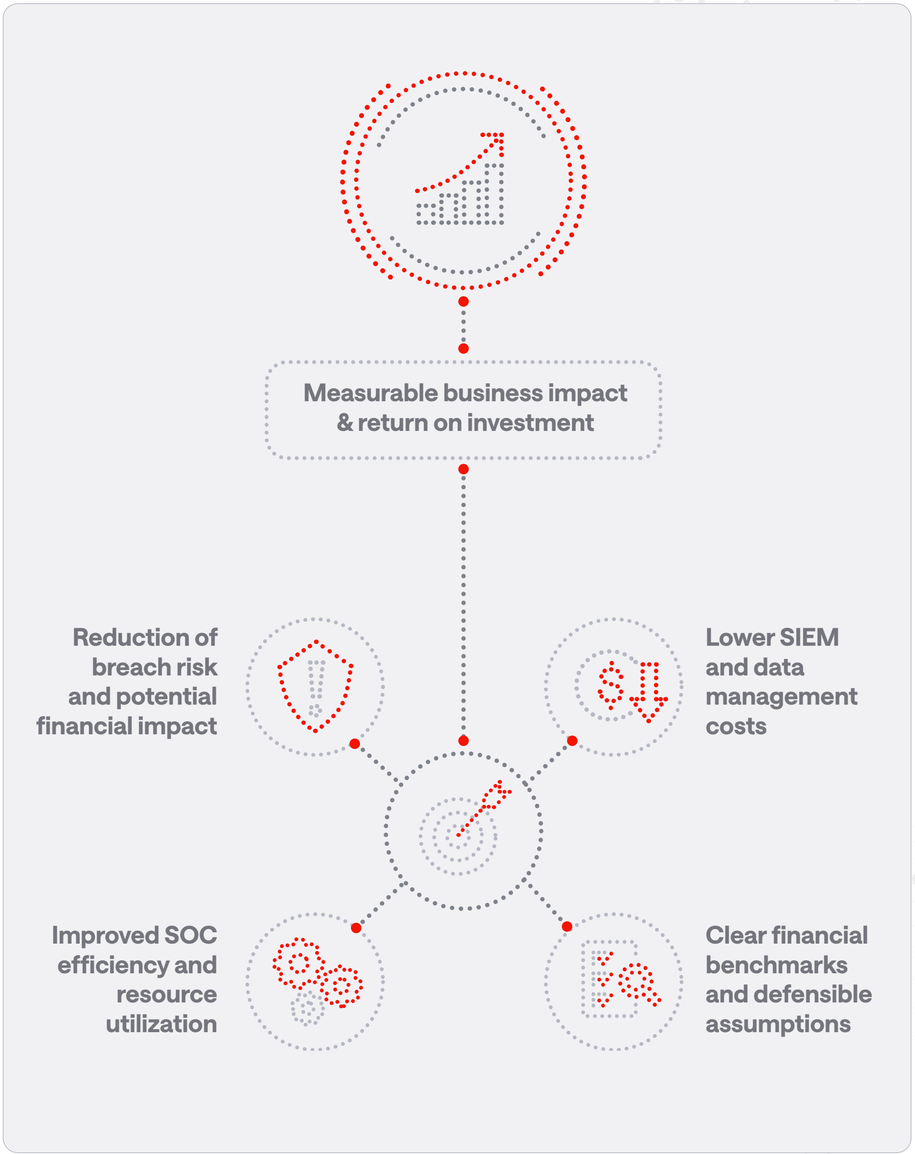
Through upstream data reduction and smarter processing, modern NDR solutions can significantly decrease SIEM ingestion volumes and long-term storage requirements, addressing one of the largest cost drivers in security operations.

3 Improved SOC efficiency and resource utilization

By reducing alert noise and accelerating investigations, the platform should enable existing teams to handle more incidents without proportional increases in headcount.

4 Clear financial benchmarks and defensible assumptions

Given the multi-million € exposure of breaches in the BFSI sector, the business case should connect security improvements directly to avoided costs and operational savings.



Vendor Evaluation

Prioritize those that can substantiate their claims with real data.

Transparent ROI

Transparent ROI models tailored to your environment.

Benchmark data

Benchmark data from comparable BFSI organizations.

Proven efficiency

Documented customer outcomes and cost savings.

The key question:

Can the platform deliver a quantifiable return that stands up to board-level scrutiny, balancing risk reduction with measurable cost efficiency?

A Narrative Checklist
Questions to Ask Every Vendor

Use these during vendor Demos & PoCs:

Visibility & Detection

Can you detect lateral movement in encrypted environments without decryption?

How do you identify unknown threats vs known IoCs?

Deployment & Architecture

Can we deploy using existing data sources (flows, logs)?

What infrastructure is required across hybrid environments?

Detection Quality

What is the alert-to-incident ratio after 30–60 days?

How much manual tuning is required?

Compliance

How does the platform support DORA/NIS2 reporting?

Can we generate audit-aligned incident timelines and correlations easily?

Cost & ROI

How much SIEM ingest/storage reduction can we expect?

What is the 3-year TCO vs current setup?

Next Steps
For Your Evaluation Journey

1 Start with a High-Impact Pilot

- Focus on critical zones: Payments, SWIFT, Core Banking
- Define success criteria: Encrypted threat detection False-positive reduction

2 Measure Data & Cost Impact

- Compare SIEM ingestion before/after
- Quantify storage and processing savings

3 Align with Compliance Objectives

- Map findings to DORA/NIS2 requirements
- Translate technical results into audit value

4 Scale Fast

Successful pilots typically scale to production within 6–10 weeks, with:

- Reduced infrastructure footprint
- Lower operational cost
- Improved detection outcomes

Why BFSI Leaders Ultimately Choose Exeon

Across European BFSI institutions, three themes stand out:

Sensor-Free Visibility

- Uses existing data:
  Flows, DNS, firewall logs
- Covers encrypted and segmented environments

Explainable AI

- Transparent ML models
- Reduced alert fatigue
- Full data sovereignty (EU/CH)

Proven ROI

- Up to 100× data reduction
- Lower SIEM costs
- Faster audit reporting

Use this framework to evaluate any vendor — **including Exeon**.

See how **Exeon can help you gain visibility,**
detect **real threats**, and **strengthen** your **cyber resilience**.

BOOK A DEMO


exeon
Gartner
ATTESTA
ISO 27001
CERTIFIED
CYBERSECURITY™
MADE IN EUROPE