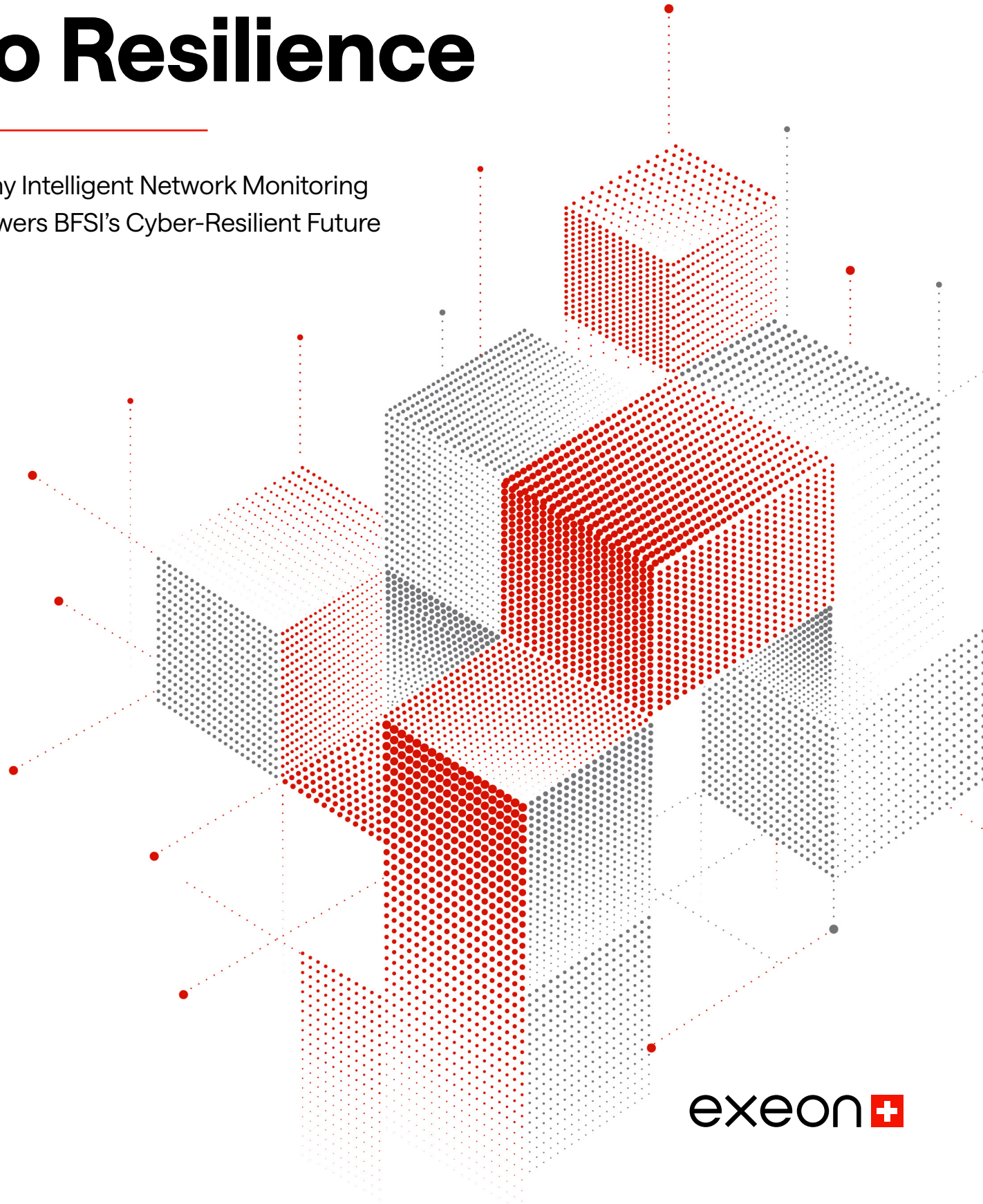
2026–2027 Industry Stat Report for CISOs, Heads of SOC, CIOs & Compliance Leaders

From Data Overload to Resilience

Why Intelligent Network Monitoring Powers BFSI's Cyber-Resilient Future

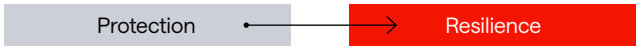


exeon

Executive Introduction

BFSI Research Report

As the BFSI sector accelerates toward hyper-connected, cloud-first ecosystems, cybersecurity is undergoing a fundamental shift – from protection to resilience.



Financial institutions actions

Financial institutions must now:

- Secure hybrid IT/OT and multi-cloud environments
- Comply with evolving regulations like DORA and NIS2
- Navigate geopolitical instability and data sovereignty requirements
- Maintain operational continuity despite inevitable breaches

2026–2027 represents a strategic inflection point

Security leaders are no longer measured by prevention alone, but by their ability to sustain business operations under attack.

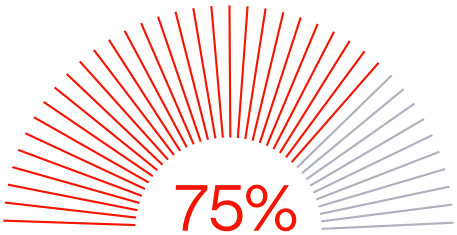
Let’s dive deeper

This report consolidates the latest data and strategic insights to guide decision-making across security, IT, and compliance functions.

1. Visibility Blind Spots and Operational Complexity

Most interesting for: CISO / Head of SOC
Also relevant for: CIO

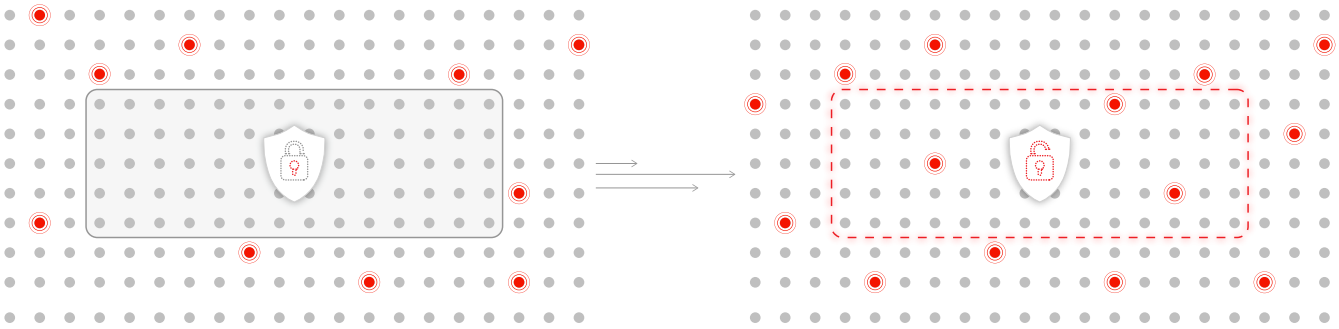
Modern BFSI environments have become too distributed and opaque for traditional monitoring approaches.



of BFSI firms experienced compliance issues tied to unmanaged assets or shadow IT (KPMG, 2024)

Key Statistics and Trends

68%	of organizations report critical visibility gaps across hybrid cloud environments (IBM Security, 2024).
75%	of BFSI firms experienced compliance issues tied to unmanaged assets or shadow IT (KPMG, 2024).
80%+	of network traffic is now encrypted, yet less than half is effectively inspected (Zscaler, 2025).
60%+	of connected OT/IoT devices in financial environments run outdated or unsupported software (SANS, 2024).
60%+	increase in API-related attacks year-over-year in financial services (Salt Security, 2025).



Strategic Implications

The attack surface is no longer perimeter-bound – it spans cloud workloads, APIs, partner ecosystems, and OT systems.

Visibility must become continuous, unified, and intelligence-driven.

Action points

Adopt AI-driven network detection solutions that:

1 Map all assets (IT + OT + cloud)

2 Monitor encrypted traffic behaviorally

3 Provide real-time API and east–west traffic visibility

2. Evolving Threats and the Inevitability of Breaches

Most interesting for: CISO / Head of SOC
Also relevant for: CIO

Attackers are faster, more adaptive, and increasingly AI-enabled.

Ransomware impacts over 70% of financial institutions annually

Key Statistics and Trends

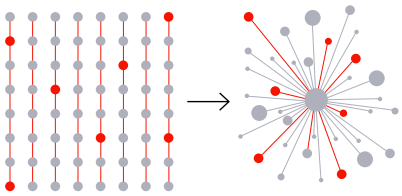
62%	of malware in 2025 is polymorphic or previously unseen (CrowdStrike, 2025).
70%+	of financial institutions are impacted by ransomware annually (Sophos, 2025).
~80	days remains the average breach dwell time in financial services (IBM, 2024).
83%	of organizations experienced more than one breach in 2024–2025 (IBM, 2025)

Half of CISOs will rebrand cybersecurity programs by 2028

Gartner Insight Integration

By 2028, half of CISOs will rebrand cybersecurity programs as cyber resilience programs.

Security strategies will shift toward minimizing impact rather than preventing all breaches.



Move from static protection to context-aware, behavioral security

Strategic Implications

Breaches are inevitable – operational disruption is not.

Organizations must move beyond static defenses toward behavioral, context-aware detection and response.

Action points

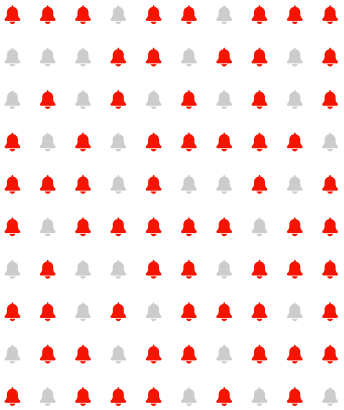
1 Implement behavioral analytics and anomaly detection

2 Establish continuous threat hunting

3 Focus incident response on containment and business continuity

3. SOC Efficiency and the Talent Constraint Reality

Most interesting for: Head of SOC / CIO
Also relevant for: CISO



65%

Up to 65% of alerts are false positives (Palo Alto Networks, 2025)

Security teams are overwhelmed – not just by threats, but by operational inefficiency.

Key Statistics and Trends

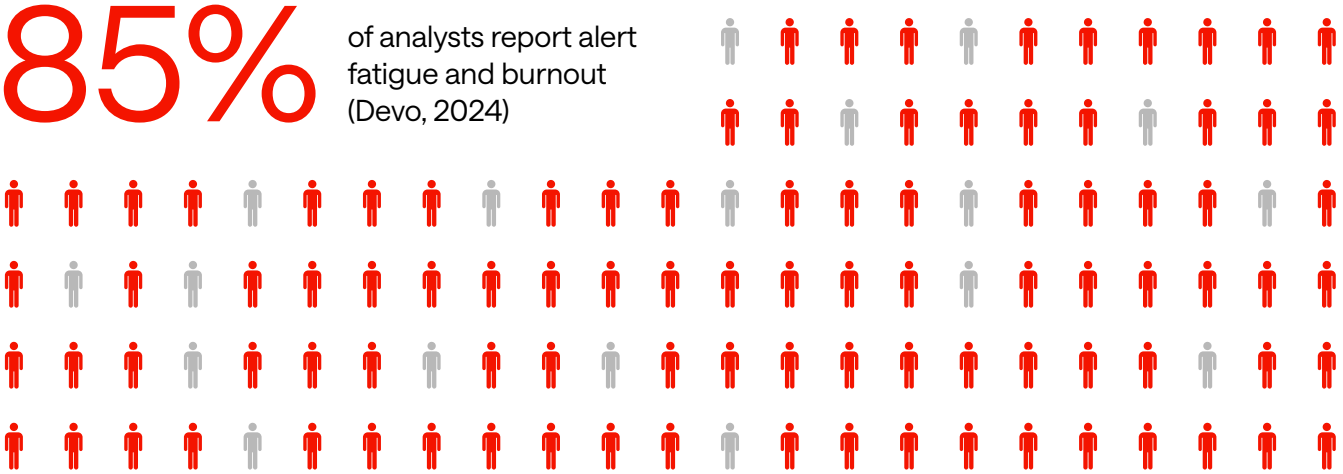
85% of analysts report alert fatigue and burnout (Devo, 2024).

65% of alerts are false positives (Palo Alto Networks, 2025).

40-50 security tools are used on average by enterprises, with limited integration (IBM, 2024).

4+ million professionals are needed to close the global cybersecurity workforce gap (ISC2, 2024).

85% of analysts report alert fatigue and burnout (Devo, 2024)



Gartner Insight Integration

By 2028, 40% of cybersecurity leaders will streamline resilience efforts to focus only on critical business services.

Strategic Implications

The future SOC is smaller, more automated, and focused on business-critical risks.

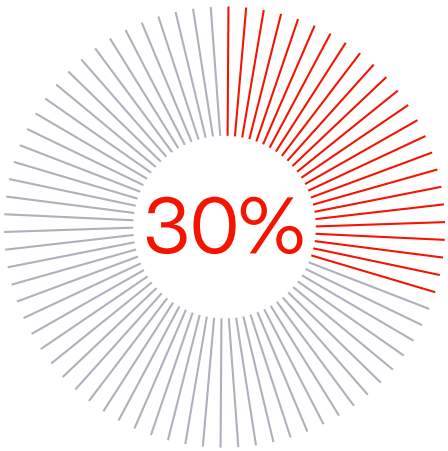
Action points

1 Consolidate tools into unified platforms (XDR/NDR+, I thin teAutomate Tier-1 triage using SOAR

2 Prioritize alerts based on business impact

4. Regulation, Sovereignty, and Geopolitical Pressure

Most interesting for: Compliance / CIO
Also relevant for: CISO



30% of organizations will require sovereign cloud security controls

Cybersecurity is increasingly shaped by geopolitics and digital sovereignty.

Key Statistics and Trends

30% of organizations will require sovereign cloud security controls by 2027 (Gartner).

DORA and NIS2 enforce:

01 24–72 hour incident reporting

02 Third-party risk accountability

03 Mandatory resilience testing

70% of financial institutions consider geopolitical risk a top cybersecurity driver (World Economic Forum, 2025).

Expanded Geopolitical Context

Cybersecurity is now a strategic and political issue – not just a technical one.

Rising geopolitical tensions are driving:

- Data localization requirements
- Restrictions on cross-border data transfers
- Increased scrutiny of third-party providers

Strategic Implications

Organizations must:

- Ensure control over where data and security operations reside
- Continuously monitor third-party and supply-chain risks
- Align with regional regulatory frameworks

Action points

Adopt sovereign-aware architectures with:

1 Region-specific data processing

2 Transparent control over logs and telemetry

3 Integrated third-party risk monitoring

5. The Transformation of the CISO Role

Most interesting for: CISO
Also relevant for: CIO / Risk

New roles of CISOs

- Cyber risk management
- Strategic business integration
- Regulatory Changes and Compliance
- Crisis management
- Incident Response
- Decision-making processes
- Zero Trust Architecture

From Protection Leader to Resilience Executive. Leadership expectations are shifting.

Key Trends

Minimum Viable Security: Focus on reducing impact and ensuring continuity rather than achieving perfect protection.
Cyber Resilience as Core Mandate: Align cybersecurity with uptime, recovery, and operational resilience.
Value Creation: Support revenue-generating initiatives and enable digital transformation.

“CISOs are no longer expected to prevent all breaches – they are expected to ensure the business continues operating despite them.”

Gartner Insight

By 2028, 50% of CISOs will be responsible for disaster recovery in addition to incident response.

Strategic Implications

The CISO becomes:

1 A resilience-focused business leader

2 A cross-functional executive

3 A driver of trust and competitive advantage

From Data Overload to Resilience
2026–2027 Industry Stat Report

How Network Detection & Security Monitoring Has Evolved

What Is the Network Today?

The perimeter has dissolved.

Remote employees, branch offices, cloud workloads, SaaS applications, and operationaltechnology (OT) environments now interact through zero-trust connections rather than a fixed castle-and-moat.

Visibility into these distributed pathways is crucial because attacks increasingly traverse VPNs, SD-WANs, APIs, and east–west cloud traffic long before reaching a traditional gateway.

What has changed

- The network is no longer location-based, but identity- and access-driven
- Traffic flows are predominantly east–west, not north–south
- Critical assets span IT, cloud, SaaS, and OT environments

New considerations

Data sovereignty requirements demand visibility into where data is processed and monitored

Geopolitical fragmentation increases the need for regionally controlled infrastructure.
Third-party and API ecosystems expand the effective network beyond organizational boundaries.

Implication:

Security teams must achieve **full-path visibility across all environments**, including encrypted and lateral traffic, while maintaining control aligned with regulatory and sovereignty requirements.

What is SIEM Today?

Modern SIEMs have evolved far beyond log management.

They ingest OT and IT telemetry, cloud APIs, identity logs, and business-process data into a centralized platform that supports both compliance and real-time detection.

Tightly coupled automation and SOAR orchestration replace noisy rule stacks with riskweighted, contextualized storylines, giving analysts clarity instead of alert fatigue.

What has changed

- SIEM is now a data and analytics platform, not just a log repository
- Detection is enriched with behavioral analytics and threat intelligence
- Automation reduces manual triage and accelerates response

New considerations

Resilience metrics (response time, containment, recovery) are becoming as important as detection.
Regulatory alignment (DORA, NIS2) requires auditable, end-to-end visibility and reporting.
Data control and sovereignty require clarity over where SIEM data is stored and processed.

Implication:

SIEM must serve as the **central nervous system of cyber resilience**, combining detection, compliance, and operational intelligence in a unified platform.

What to Look for in a Solution?

(“NDR+” Reality)

Analyst categories can be confusing: IDS, NDR, NDV, SIEM, SOAR — all continue to evolve, overlap, and consolidate.

The emerging consensus is: “NDR is dead, long live NDR+.”

Solution

This reflects a shift toward integrated platforms that combine:

- Network visibility
- Advanced analytics
- Automated response
- Operational context

Core capabilities to prioritize

- **Full-path visibility** across on-prem, cloud, SaaS, and OT environments
- **Encrypted traffic** analysis without breaking performance or compliance
- **Behavior-based detection** for unknown and evolving threats
- **Built-in correlation and case management** to reduce tool fragmentation
- **Automated response** and playbook execution to improve SOC efficiency

New considerations

Resilience-first design: solutions must support containment and recovery, not just detection.
Sovereignty-aware architecture: control over data location, processing, and access.
Business-context prioritization: focus on protecting critical services, not all assets equally.
Intelligent specialization over consolidation: instead of forcing all capabilities into a single platform, organizations are increasingly deploying expert systems (e.g., NDR, UEBA) that operate upstream of SIEM to:

- Filter and enrich high-volume telemetry
- Detect specific threat classes with higher accuracy
- Reduce noise and data ingestion costs
- Forward only high-fidelity, context-rich alerts into SIEM/SOAR

Implication:

The future is not about centralizing everything into one tool, but about building a lean, layered architecture – where specialized detection systems enhance signal quality and seamlessly integrate with existing SIEM, SOAR, and endpoint solutions to deliver efficient, scalable, and resilient security operations.

Conclusion: From Detection to Resilience

Cybersecurity in banking, financial services and insurance organizations is no longer about stopping every attack – it is about ensuring operational continuity despite them.

Advanced analytics solutions and automated threat detection strategies are essential to reduce cost, risk, and noise.

For CISOs & Heads of SOC

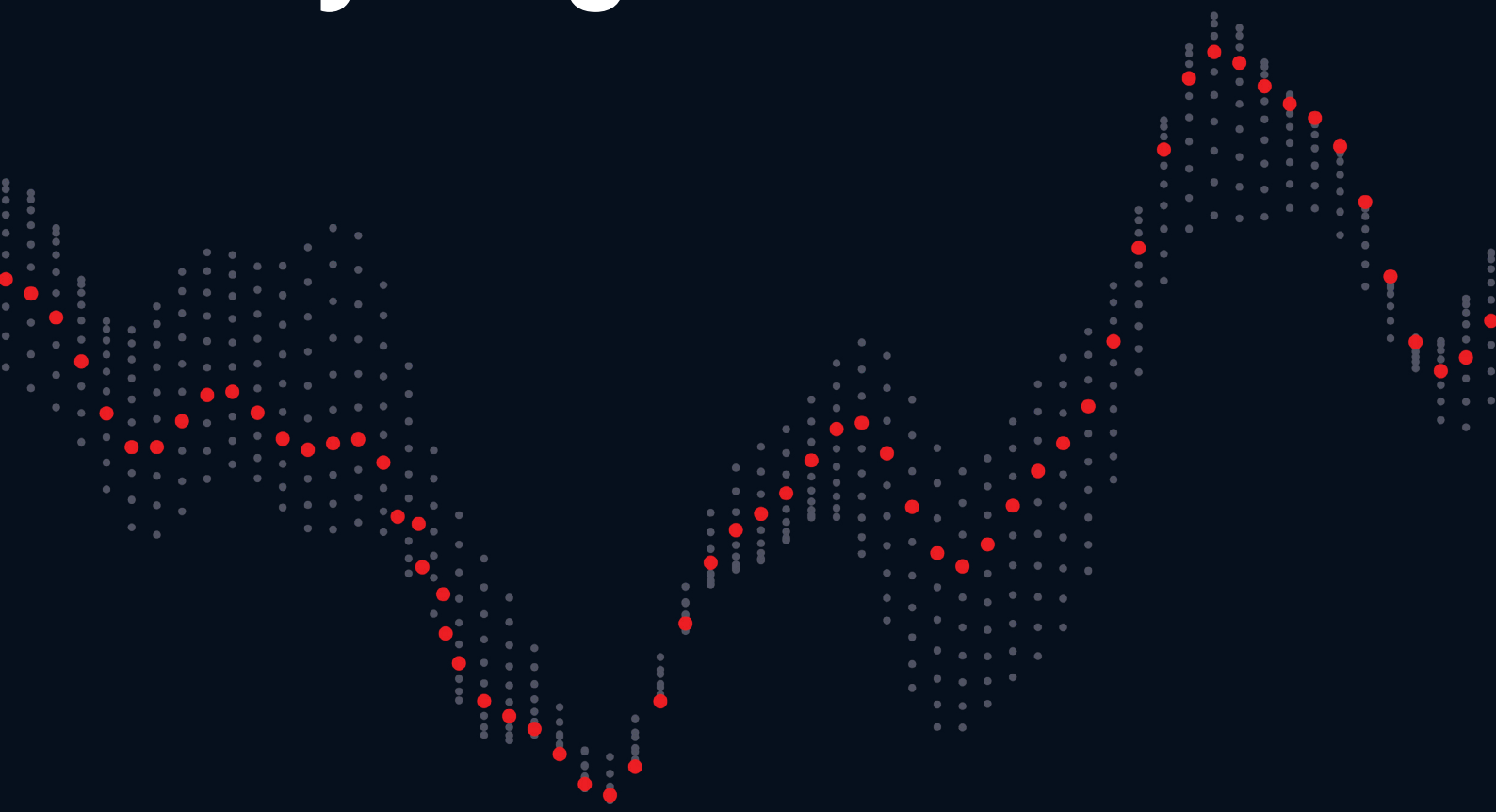
- Achieve faster detection and response with reduced analyst burnout by adopting AIdriven platforms that correlate signals across the full environment and surface highconfidence alerts
- Reduce noise and improve efficiency through behavior-based, deductive threat detection that prioritizes real threats over raw alerts
- Strengthen resilience by focusing on containment, impact minimization, and continuity of critical services
- Increase SOC effectiveness with intuitive dashboards, automated triage, and streamlined workflows that enable teams to act decisively with limited resources

For CIOs & Compliance Leaders

- Gain complete, real-time asset visibility across IT, cloud, and OT environments to reduce blind spots and improve control
- Achieve efficient regulatory alignment (e.g., DORA, NIS2) by leveraging existing tools and mapping them to measurable security outcomes
- Improve ROI by enabling comprehensive monitoring – including encrypted traffic – without adding unnecessary tool complexity
- Strengthen governance and audit readiness through centralized logging, reporting, and seamless integration into existing ecosystems (SIEM, SOAR, APIs)
- Ensure long-term compliance and control with sovereignty-aware architectures and transparent data handling practices

Final Thought

Clarity enables resilience. **Resilience** enables trust. **And in BFSI, trust is everything.**



Sources

01. **IBM Cost of a Data Breach Report**
(2024–2025)

02. **Gartner Cyber Resilience & CISO Role Evolution**
(2024–2025)

03. **CrowdStrike Global Threat Report**
(2025)

04. **Sophos State of Ransomware**
(2025)

05. **Zscaler ThreatLabz Report**
(2025)

06. **KPMG Cybersecurity in Financial Services**
(2024)

07. **SANS Institute OT/IoT Security Reports**
(2024)

08. **Salt Security API Security Report**
(2025)

09. **Devo Security Operations Report**
(2024)

10. **Palo Alto Networks Unit 42 Threat Report**
(2025)

11. **ISC2 Cybersecurity Workforce Study**
(2024)

12. **World Economic Forum Global Cybersecurity Outlook**
(2025)


exeon