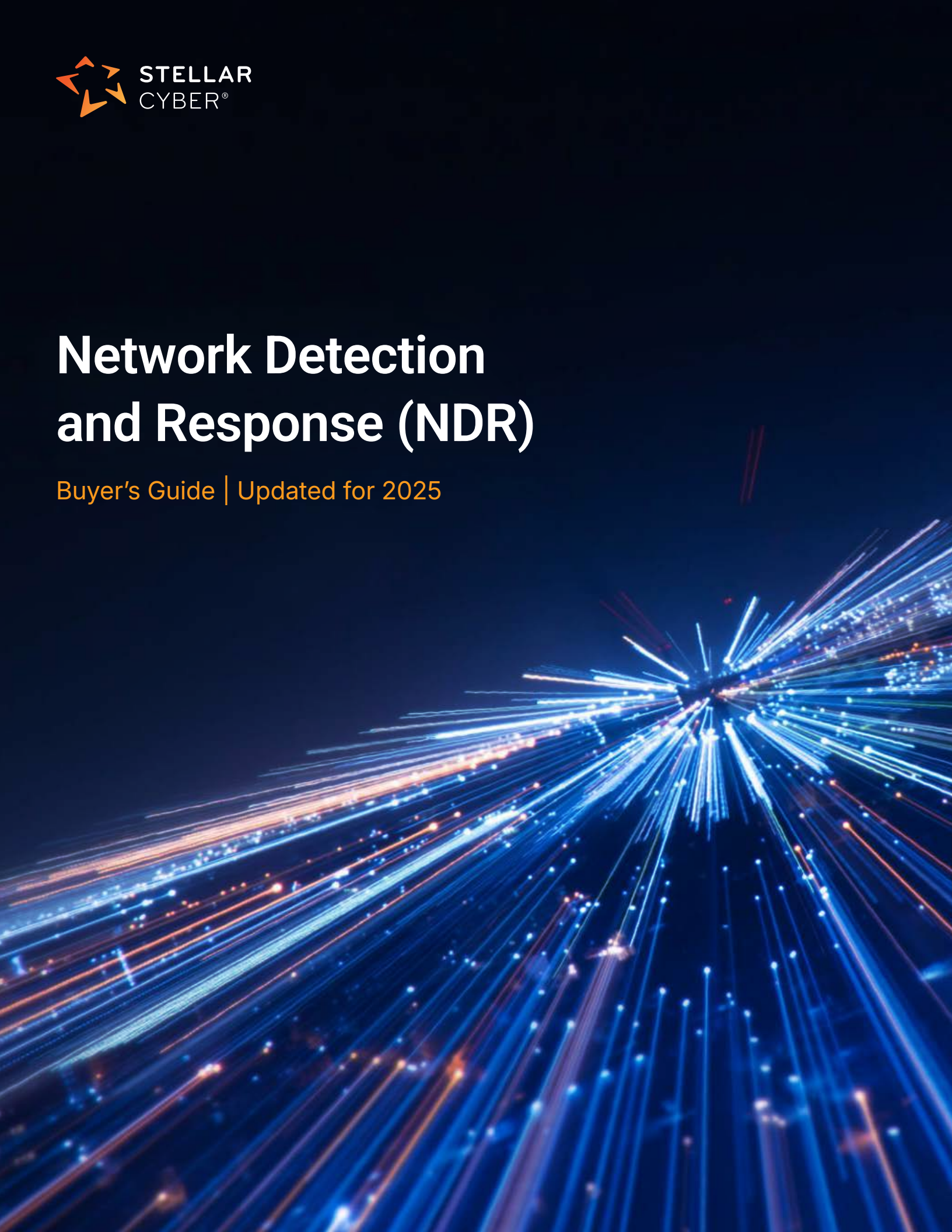
STELLAR CYBER®

Network Detection and Response (NDR)

Buyer's Guide | Updated for 2025



The Evolution of NDR

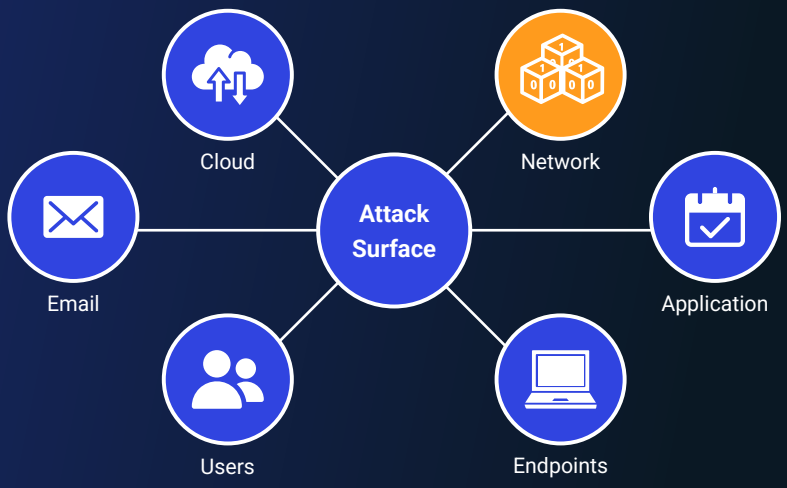
Network Detection and Response (NDR) evolved from traditional network security and network traffic analysis (NTA). Perimeter firewalls and intrusion prevention systems (IPS) once stood as the primary defenses. Adversaries now move laterally across hybrid environments and exploit cloud, SaaS, and unmanaged devices. Modern NDR meets this challenge by monitoring traffic everywhere—IT and OT networks, data centers, cloud, and remote sites—to detect threats early and guide an effective response.

Rather than bolt together point tools, leading NDR platforms consolidate capabilities formerly delivered by NTA, IDS, UEBA, and TIP. They normalize telemetry, enrich it with context, and correlate activity across users, hosts, apps, and industrial systems to expose real attacks quickly.

Why You Need NDR

Endpoints and logs alone miss too much. Network traffic doesn't lie. NDR completes the data picture alongside EDR for endpoint telemetry and SIEM for logs by observing everything that moves on the wire—including unmanaged devices, IoT/OT assets, and SaaS traffic. NDR becomes the single source of truth and enables real-time response.

As organizations adopt Zero Trust and segment networks, NDR's "trust but verify" model validates enforcement and quickly flags policy gaps or malicious lateral movement across IT and OT segments.



Modern NDR Architecture

An effective NDR platform ingests data from sensors (physical, virtual, and cloud), network devices, firewalls, and IDS/IPS, as well as metadata sources such as NetFlow/IPFIX. It monitors north–south and east–west traffic across on-prem, cloud, and industrial networks. The platform streams telemetry into a scalable data lake and applies multi-layer AI for high-fidelity detections.

AI is More Than Generative AI
Modern NDR platforms require multi-layer AI to deliver accurate detections and actionable insights.

- Machine Learning (ML) establishes baselines, detects anomalies, and identifies known threats through both signature-based and model-driven methods.
- Generative AI (GenAI) accelerates investigations by summarizing evidence, explaining findings in plain language, and recommending next steps.

By combining ML and GenAI, organizations cut through alert noise, boost analyst productivity, and dramatically reduce the time to detect and respond.

Response Matters
NDR must trigger action. Effective platforms integrate with firewalls, EDR, NAC, and identity systems to block traffic, contain endpoints, suspend risky accounts, or orchestrate playbooks—automatically or with analyst approval.

NDR Buyer's Checklist

Prioritize these core capabilities when evaluating solutions:	
Gather activity from raw packets and traffic flows (e.g., IPFIX/NetFlow) in real time or near real time.	Employ both Machine Learning + Generative AI to detect unknowns and accelerate investigation with explanations and guidance.
Monitor and analyze both north–south and east–west traffic across IT and OT environments.	Aggregate alerts into coherent incidents that correlate evidence from network, endpoint, cloud, and identity systems.
Enrich metadata at ingestion and during analysis to add user, device, asset, and application context.	Provide automated and manual responses (e.g., block traffic, quarantine endpoints, revoke access) through native integrations.
Model normal traffic and highlight suspicious deviations with behavioral analytics.	Offer flexible form factors (appliances, VMs, containers, cloud sensors) to cover data center, campus, remote, and cloud networks.

Disqualify solutions that:	
Require a prerequisite SIEM or firewall to function.	Focus only on IoT/OT analytics without covering the broader enterprise use cases.
Rely primarily on log analysis or full-PCAP forensics instead of real-time detection.	Lack market-proven NDR capabilities or cannot integrate with your existing security stack.

Recommendations for Buyers

1. Select an NDR platform that integrates seamlessly with your current and future network and security tools across IT and OT.
2. Ensure the platform combines ML-driven analytics with GenAI assistance to speed detection, triage, and investigation.
3. Validate automated response options and analyst-guided workflows that reduce dwell time without adding headcount.
4. Confirm visibility beyond logs by deploying sensors to key network segments (campus, data center, cloud, remote, and OT).

Stellar Cyber® Delivers NDR+

The Stellar Cyber open and unifying platform includes native NDR. It correlates network telemetry with data from endpoints, cloud, and identity systems to give security teams complete visibility across IT and OT. Out of the box, Stellar Cyber provides:

- Distributed sensors that collect packet and flow telemetry in any environment (physical, virtual, cloud, and industrial).
- An ML-IDS engine for known attack detection and behavioral analytics for unknowns.
- Integrated AV/Sandbox analysis for zero-day malware and suspicious objects.
- Advanced processing for normalization and context creation (assets, users, apps, locations).
- A centralized data lake to store contextualized telemetry at scale.
- A Threat Intelligence Platform (TIP) to fuse third-party feeds into detections.
- Multi-Layer AI™ that detects, and correlates across sources, explains findings, and guides response.
- Automatic triage and automated response through integrations with firewalls, EDR, NAC, and SOAR.
- Stellar Cyber Interflow™: Solving the NDR Data Problem
- Interflow is the normalized, enriched, and actionable data model that powers Stellar Cyber NDR. It extracts deep telemetry from packets, enriches it automatically, and unifies data so IT and OT tools speak the same language. This approach reduces data volume while increasing analytic value.
- Stop manual enrichment—Interflow automatically contextualizes telemetry.
- Correlate events easily—common data elements enable cross-source correlation.
- Reduce volume—PCAP-to-Interflow reduction can be orders of magnitude.
- Improve interpretation—clean, structured data shortens analyst ramp-up.

Take the First Step

Protect your network from compromise and deliver continuous security outcomes wherever assets and data live. With Stellar Cyber NDR, part of the Open XDR Platform, you gain the visibility and response you need without adding resources.

Visit www.stellarcyber.ai to start your journey.

By shining a bright light on the darkest corners of security operations, Stellar Cyber empowers organizations to see incoming attacks, know how to fight them, and act decisively – protecting what matters most. Stellar Cyber's award-winning open security operations platform includes NG SIEM, NDR, Open XDR, and Multi-Layer AI™ under one license. With almost 1/3 of the top 250 MSSPs and over 14,000 customers worldwide, Stellar Cyber is one of the most trusted leaders in security operations. Learn more at https://stellarcyber.ai/.