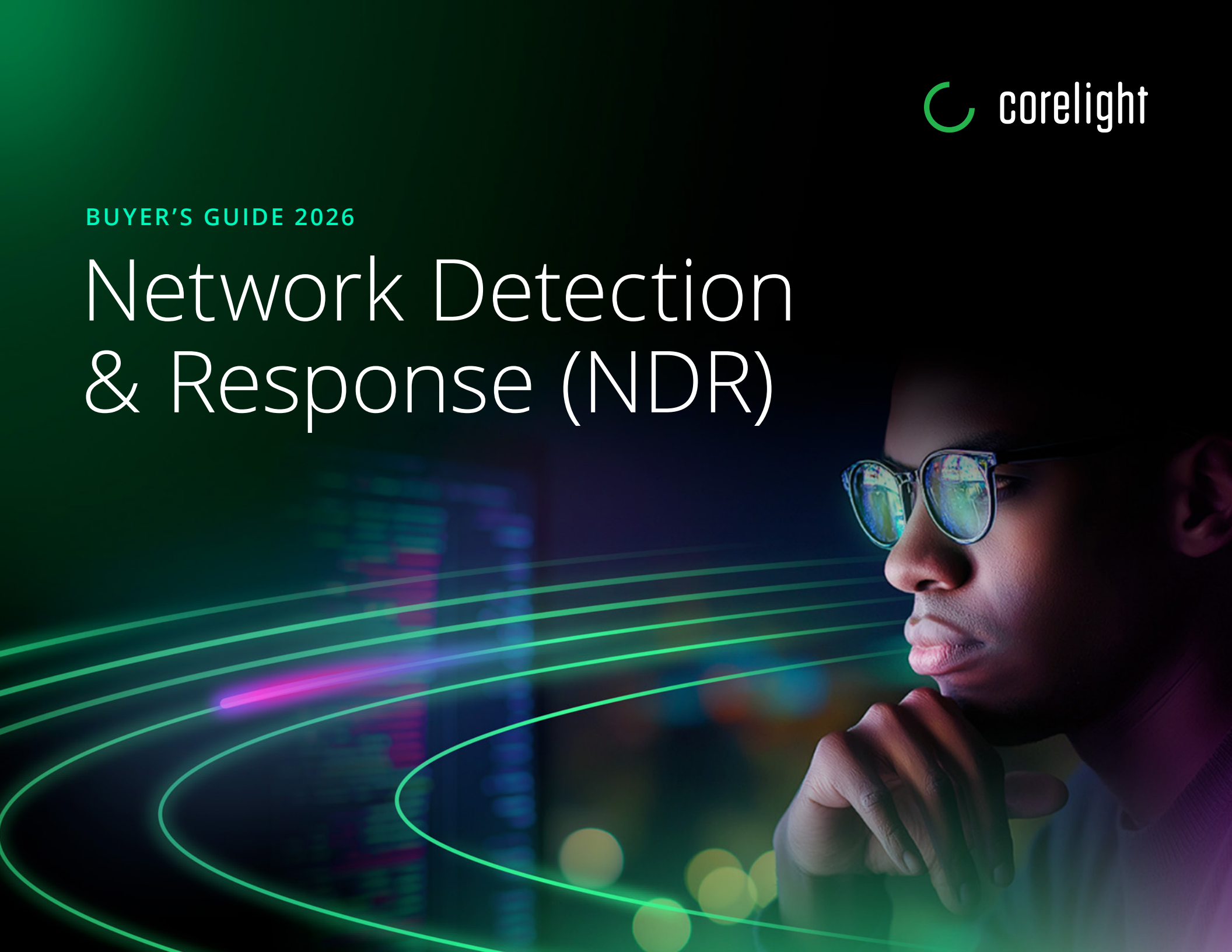
corelight

BUYER'S GUIDE 2026

Network Detection & Response (NDR)



The new imperative for network visibility

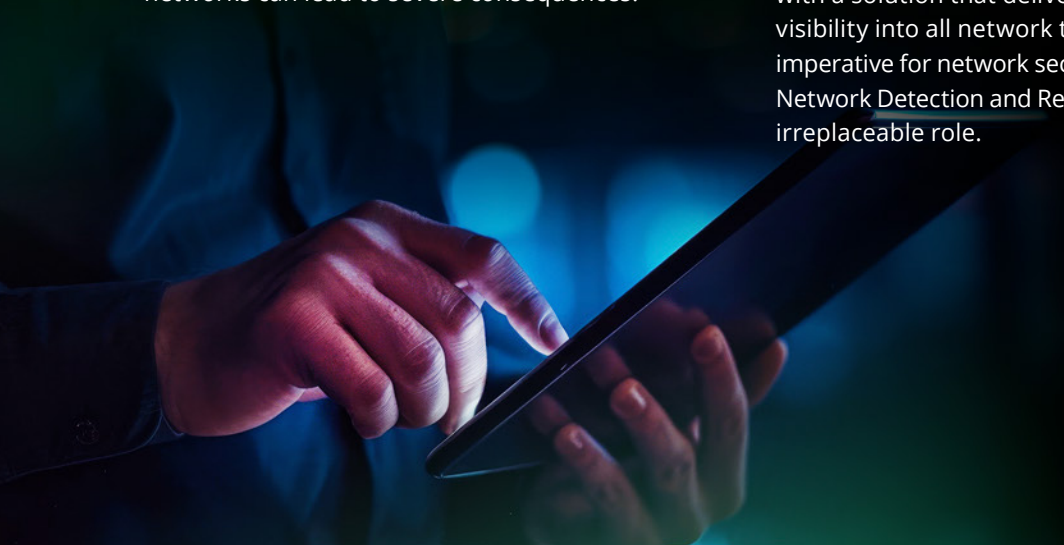
For years, cybersecurity strategy has relied on SIEM platforms and EDR agents. While valuable, this approach has critical gaps as cyberattacks evolve. A common mistake is believing network logs in a SIEM are enough for threat detection. However, logs from firewalls, DNS servers, or basic NetFlow often provide a false sense of security because they lack forensic depth. A firewall log shows a connection was allowed but not what happened inside it, while NetFlow cannot provide the application-layer context to distinguish a safe query from a malicious command.

The modern attack surface has expanded beyond the traditional perimeter, creating blind spots for logs and EDR. The rise of remote work, multi-cloud environments, and unmanaged devices—from IoT to critical ICS and OT systems—gives attackers more entry points. Many attacks now start at the edge on devices that cannot host an EDR agent and use protocols invisible to standard IT security tools. This is a significant challenge in critical infrastructure and manufacturing, where poor visibility into ICS/OT networks can lead to severe consequences.

Multi-cloud architectures also create new blind spots. Each cloud provider has proprietary logging, making a unified security view nearly impossible. Without telemetry that correlates activity across AWS, Azure, and GCP, security teams cannot see attackers moving laterally between cloud environments. In this landscape, a SIEM and EDR-based approach proves inadequate.

To defend against modern threats, security leaders must augment their security stack with a solution that delivers deep, widespread visibility into all network traffic. This is the new imperative for network security, and it is where Network Detection and Response (NDR) plays an irreplaceable role.

Without telemetry that can correlate activity across AWS, Azure, and GCP environments, security teams cannot see attackers moving laterally between cloud environments.

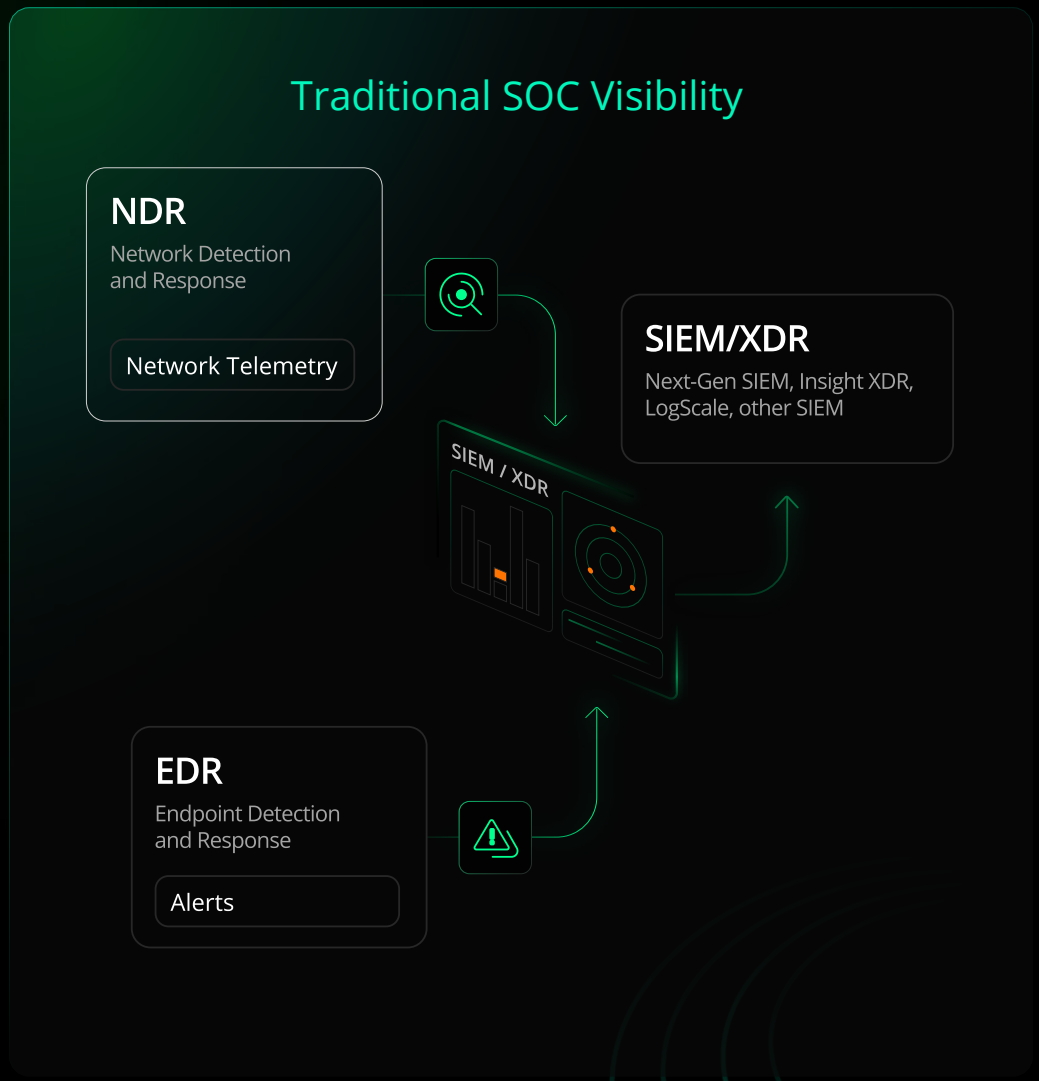


corelight

The modern network: pervasive, hybrid, and complex

Today's network is a borderless ecosystem of hybrid infrastructure, AI, multi-cloud infrastructure, and unmanaged devices. This expanded perimeter increases the attack surface and complicates visibility. Adversaries now use Gen AI to automate attacks, create convincing phishing, and deploy polymorphic malware that bypasses signature-based defenses. AI-driven attacks outpace traditional detection and response methods, and require new defense strategies.

In response, security operations must turn to a more resilient source of truth. Logs can be erased and endpoint agents disabled, but network traffic provides an immutable record of all activity. This principle is the foundation of the SOC Visibility Triad, which unites SIEM, Endpoint Detection and Response (EDR), and Network Detection and Response (NDR).



Comprehensive security depends on visibility from three distinct but complementary sources:

1. **SIEM/Log management:** Provides a historical record of events from applications and systems.
2. **Endpoint Detection and Response (EDR):** Offers deep visibility into process execution and activity on individual devices.
3. **Network Detection and Response (NDR):** Delivers a complete view of all interactions between devices, across all parts of the network.



EDR has no insight into unmanaged devices, and SIEM is blind to unlogged activity. NDR fills these critical voids, serving as the connective tissue that links disparate events into a coherent attack narrative. It detects lateral movement, agentless C2 communication, and reconnaissance scans that logs simply fail to capture.

NDR is irreplaceable for monitoring unmanaged devices and analyzing encrypted traffic. To effectively combat AI-powered threats, security teams must feed their defensive AI tools with high-quality network data. This reduces false positives and enables rapid, context-based response.

Choosing a modern NDR platform is a strategic shift in philosophy, not just a tactical purchase. It acknowledges that breaches are inevitable; true maturity lies in the ability to see and respond with precision. Beyond detection, NDR aids the entire lifecycle—including legal defensibility, compliance frameworks like GDPR and DORA, and forensics. An irrefutable record empowers confident decision-making in a crisis, potentially saving millions.

EDR has no insight into unmanaged devices, and SIEMs are blind to unlogged activity. NDR fills these critical gaps.

Defining Network Detection and Response (NDR): a strategic overview

An NDR solution provides continuous monitoring and analysis of network traffic to identify and respond to threats in real time. Using technologies like AI, machine learning, and behavioral analytics, these platforms detect known and unknown threats that evade traditional security across all environments. A key function of NDR is analyzing both north-south and, critically, east-west traffic, providing comprehensive visibility into all network activity.

For businesses seeking to enhance their cybersecurity posture, NDR offers several key benefits that directly address the challenges faced by modern security leaders:

- **Improved network visibility:** NDR delivers a unified view across on-premises, cloud, and hybrid environments covering north-south and east-west traffic.
- **Early threat detection:** By establishing a baseline of normal network activity, NDR quickly identifies anomalies indicating a threat. It uses a full spectrum of detection methods—from signatures to machine learning—and leverages threat intelligence to reduce triage efforts.
- **Rapid response:** NDR must provide swift response capabilities such as host containment and traffic blocking, along with automated and GenAI assisted workflows that integrate with other security tools.
- **Enhanced compliance:** NDR's continuous traffic monitoring, detailed visibility, and robust reporting help organizations demonstrate compliance with regulations like GDPR, NIS2, and HIPAA.
- **Efficient resource allocation:** High-fidelity alerts and contextual data allow security teams to focus on genuine threats, streamlining triage and investigation. For AI-driven SOCs, NDR data improves decision accuracy and accelerates response.
- **Flexible architecture integration:** Every SOC architecture is different, and NDR solutions are designed to integrate with and support a variety of deployment options, including air-gapped, SaaS and multi-hybrid cloud environments.

The NDR market is growing and innovating rapidly. Key trends like AI and machine learning are boosting detection accuracy, and the rise of cloud-native solutions offers seamless protection for complex infrastructures. Additionally, NDR's expansion into IoT and OT security addresses critical vulnerabilities in these connected ecosystems. Organizations must prioritize solutions with the scalability and flexibility to secure this evolving digital landscape.



corelight

A framework for evaluating modern NDR solutions

As the NDR market matures, a consensus on best-in-class capabilities has emerged. Security leaders must use a structured evaluation framework to find a platform that meets modern SOC demands. This framework rests on four pillars: the quality of forensic data, completeness of visibility, speed of response, and the platform's ability to drive SOC modernization and deliver a clear ROI.

Criteria I: Network data quality and forensic depth

The effectiveness of any response platform is limited by its underlying data. An alert without context is just noise; true response requires rich network data to reconstruct an attacker's actions. Therefore, the most critical criterion for evaluating an NDR solution is the quality and usability of the network data it generates.

Many security tools rely solely on shallow metadata like NetFlow or VPC Flow Logs. While useful for basic monitoring, this data is forensically insufficient. It provides a "5-tuple" summary but no insight into the payload activity where attacks unfold. It can show that servers communicated, but not if it was a benign query or a malicious command.

A modern NDR platform must transform raw traffic into high-fidelity, structured transaction logs and metadata, enriched with application-layer context at the point of collection to provide a complete narrative.time of collection, providing a complete narrative of network activity. And finally, a modern NDR platform must be ready for AI when you are—with data that is designed to power AI orchestration when you need it.

Key evaluation criteria:

- **Protocol coverage:** Does the solution parse and log transactions for a comprehensive range of protocols like HTTP, DNS, SMB, and Kerberos, beyond just common web traffic?
- **Data richness:** Does the data provide the precise context analysts need to quickly validate alerts, eliminating manual research and log fatigue?
- **Historical forensics:** Can the data provide an immutable, historical record of all network activity, allowing investigators to reconstruct the entire attack timeline?
- **Data structure:** Is the data structured and interlinked for easy querying, correlation, and threat hunting, and is it designed to integrate seamlessly into your existing SOC tools?
- **AI-ready data:** Is the data easily consumable by AI/ML detection models, GenAI workflows and AI agents?

Criteria II: Unified visibility and comprehensive threat detection

A modern NDR platform must provide complete, unified visibility across the entire hybrid enterprise. This requires monitoring not just north-south traffic but, more importantly, internal east-west traffic—where attackers spend most of their time during a breach. Visibility must extend seamlessly across on-premises, virtualized, and multi-cloud environments, presenting a single view of the attack surface.

Effective detection demands a sophisticated, multi-layered approach, as over-reliance on a single technique leads to gaps and false positives. A mature NDR solution combines multiple analytical methods for broad, high-fidelity coverage.

A critical distinction exists between vendors offering "closed-box" analytics and those providing transparent, extensible logic. Mature security teams need to understand why an alert fired and customize detections. A platform that obscures its logic ultimately hinders a sophisticated SOC.



Key evaluation criteria:

- ☐ **Traffic coverage:** Does the solution monitor both north-south and east-west traffic across on-premises, virtual, multi-cloud, and ICS/OT environments?
- ☐ **Detection methods:** Does the platform use a mix of signatures, behavioral analytics, and machine learning or does it rely solely on AI/ML? Does it map detections to the MITRE ATT&CK framework for maximum coverage?
- ☐ **Encrypted traffic analysis:** Can the solution analyze encrypted traffic for threats without requiring universal, performance-intensive decryption?
- ☐ **Explainability:** Is the detection logic transparent? Can your teams create or customize detection rules?
- ☐ **Integrated threat intelligence:** Does the platform integrate with trusted third-party threat intelligence that aligns with real-time network data?

Criteria III: Accelerating response and empowering analysts

Detecting a threat is just step one. The ultimate goal of an NDR platform is reducing mean time to respond (MTTR) and containing incidents before significant damage occurs. This requires a solution designed to actively accelerate the security analyst's workflow, not just generate alerts.

This means moving beyond siloed alerts to an integrated investigation experience. When an alert triggers, analysts need immediate, seamless access to the underlying forensic data. The platform should use modern technologies, including AI, to summarize events, provide context, and guide next steps—making deep insights accessible while protecting data privacy.

Finally, while rich metadata often suffices, deep forensics sometimes demand raw packets. A best-in-class NDR solution must provide intelligent packet capture (PCAP) linked directly to security events. This avoids the high costs of continuous full-packet capture while preserving a forensic-grade record of all network activity.

Key evaluation criteria:

- ☐ **Integrated data:** Does the platform link detections directly to rich, contextual network data in a unified interface?
- ☐ **AI-assisted workflows:** Does the solution use AI to generate plain-language summaries of alerts and network activity to assist with triage?
- ☐ **Access to raw data:** Does the platform provide access to raw data, including targeted packet captures, while minimizing storage costs?
- ☐ **Integrated response:** Does the platform offer native response actions or tight integration with tools like EDR or firewalls?



Criteria IV: Driving SOC modernization and enabling AI SOC

In an environment of constrained budgets and talent shortages, security leaders are pressured to maximize investment value and operational efficiency. A modern NDR platform must deliver a clear ROI by helping to modernize the Security Operations Center (SOC).

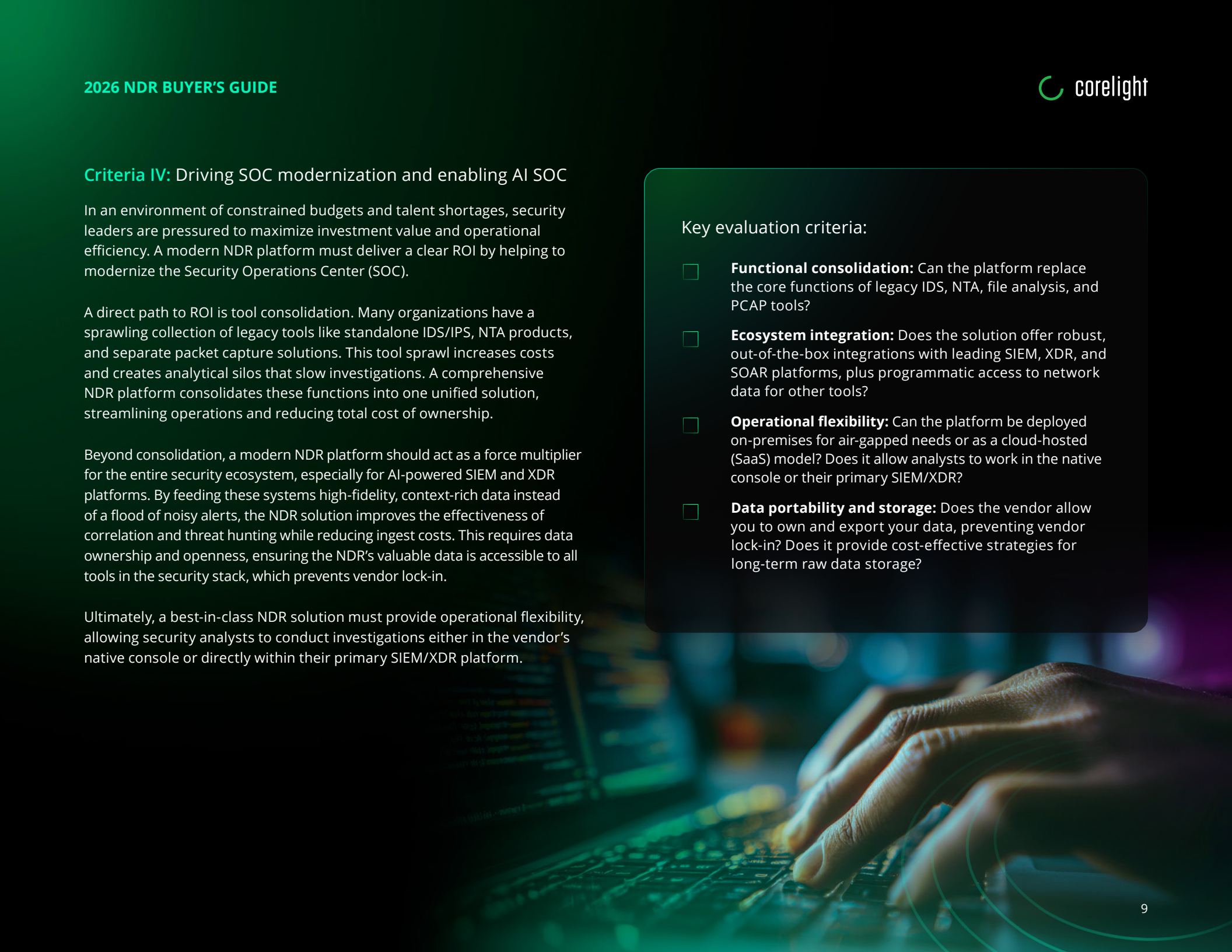
A direct path to ROI is tool consolidation. Many organizations have a sprawling collection of legacy tools like standalone IDS/IPS, NTA products, and separate packet capture solutions. This tool sprawl increases costs and creates analytical silos that slow investigations. A comprehensive NDR platform consolidates these functions into one unified solution, streamlining operations and reducing total cost of ownership.

Beyond consolidation, a modern NDR platform should act as a force multiplier for the entire security ecosystem, especially for AI-powered SIEM and XDR platforms. By feeding these systems high-fidelity, context-rich data instead of a flood of noisy alerts, the NDR solution improves the effectiveness of correlation and threat hunting while reducing ingest costs. This requires data ownership and openness, ensuring the NDR's valuable data is accessible to all tools in the security stack, which prevents vendor lock-in.

Ultimately, a best-in-class NDR solution must provide operational flexibility, allowing security analysts to conduct investigations either in the vendor's native console or directly within their primary SIEM/XDR platform.

Key evaluation criteria:

- ☐ **Functional consolidation:** Can the platform replace the core functions of legacy IDS, NTA, file analysis, and PCAP tools?
- ☐ **Ecosystem integration:** Does the solution offer robust, out-of-the-box integrations with leading SIEM, XDR, and SOAR platforms, plus programmatic access to network data for other tools?
- ☐ **Operational flexibility:** Can the platform be deployed on-premises for air-gapped needs or as a cloud-hosted (SaaS) model? Does it allow analysts to work in the native console or their primary SIEM/XDR?
- ☐ **Data portability and storage:** Does the vendor allow you to own and export your data, preventing vendor lock-in? Does it provide cost-effective strategies for long-term raw data storage?

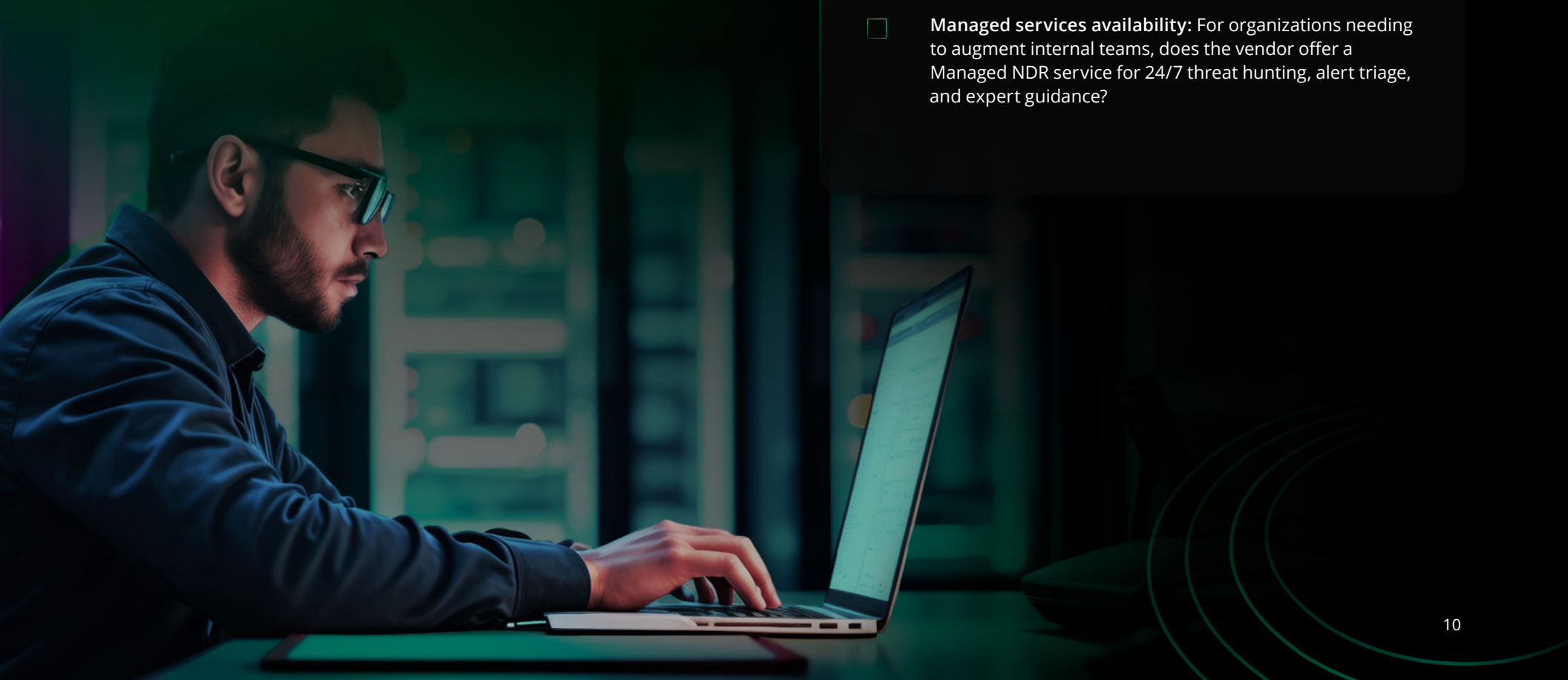


Criteria V: Enterprise-grade support and partnership

In an environment of increasing complexity and persistent talent shortages, adopting an NDR platform is more than just adding another product; the platform must deliver clear value. The quality of a vendor's support, professional services expertise, and managed offerings can be the deciding factor in shortening time-to-value. An enterprise-grade vendor must act as a true partner, invested in your operational success from deployment to daily operations. This requires looking beyond technical specifications to assess the vendor's commitment to customer success.

Key evaluation criteria:

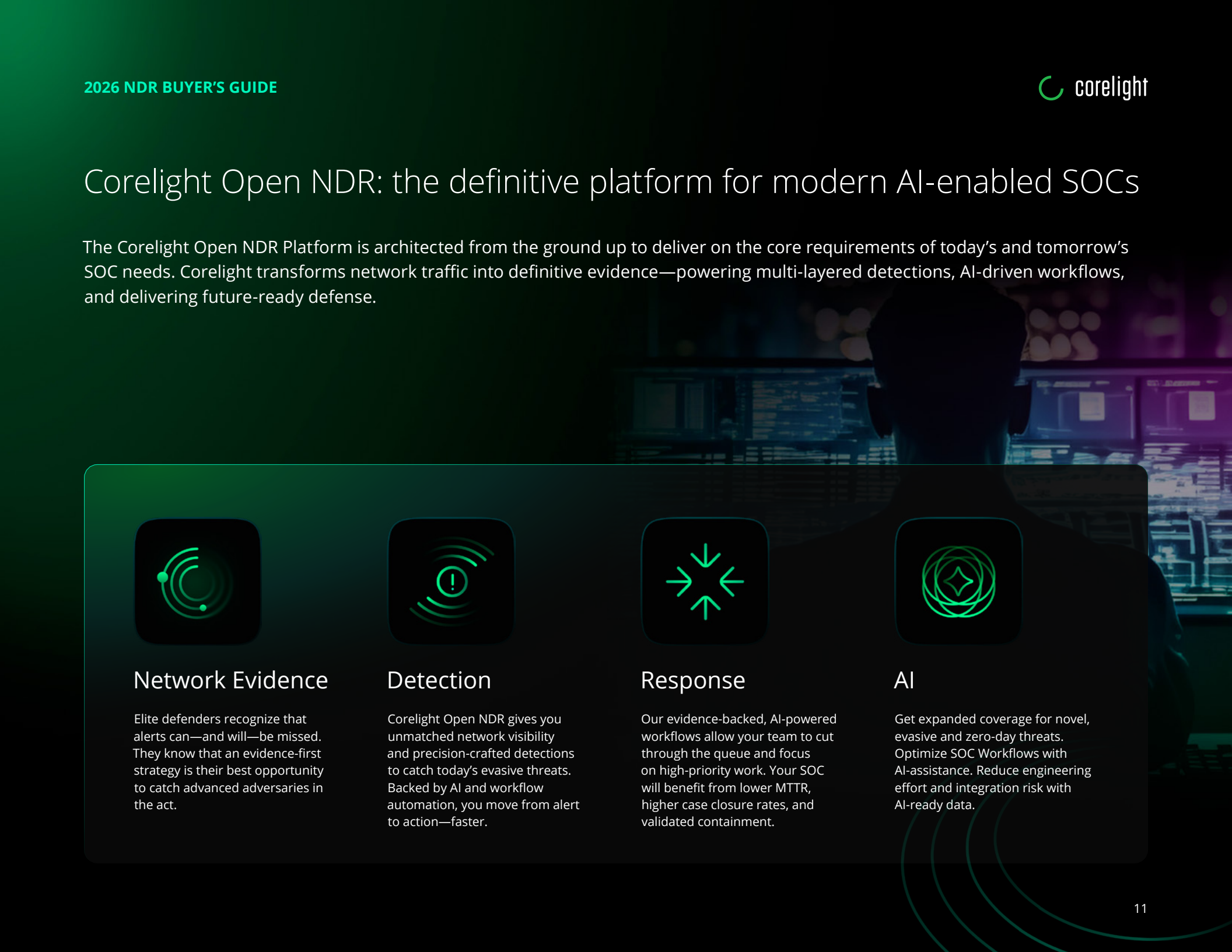
- ☐ **Proactive and responsive support:** Does the vendor provide proactive system health monitoring and demonstrate a track record of rapid, expert responses to customer issues?
- ☐ **Flexible service tiers:** Does the vendor offer a range of support options, from standard 24/7 help to dedicated resources like a Technical Account Manager (TAM) for strategic guidance?
- ☐ **Managed services availability:** For organizations needing to augment internal teams, does the vendor offer a Managed NDR service for 24/7 threat hunting, alert triage, and expert guidance?



corelight

Corelight Open NDR: the definitive platform for modern AI-enabled SOCs

The Corelight Open NDR Platform is architected from the ground up to deliver on the core requirements of today's and tomorrow's SOC needs. Corelight transforms network traffic into definitive evidence—powering multi-layered detections, AI-driven workflows, and delivering future-ready defense.



Network Evidence

Elite defenders recognize that alerts can—and will—be missed. They know that an evidence-first strategy is their best opportunity to catch advanced adversaries in the act.

Detection

Corelight Open NDR gives you unmatched network visibility and precision-crafted detections to catch today's evasive threats. Backed by AI and workflow automation, you move from alert to action—faster.

Response

Our evidence-backed, AI-powered workflows allow your team to cut through the queue and focus on high-priority work. Your SOC will benefit from lower MTTR, higher case closure rates, and validated containment.

AI

Get expanded coverage for novel, evasive and zero-day threats. Optimize SOC Workflows with AI-assistance. Reduce engineering effort and integration risk with AI-ready data.

corelight

Open NDR network evidence

At its core, the Corelight Platform is committed to providing the highest quality data possible. Corelight's network evidence is real-time, enriched data that helps security teams accelerate investigations and confidently respond to threats across any environment.

Corelight provides a single source of truth for network activity, transforming raw traffic into enriched, actionable logs using the open-source Zeek® framework. With over 10,000 deployments worldwide, Zeek open-source data is transparent, community vetted and trusted by elite defenders around the world. This high-fidelity evidence delivers the detail needed to reconstruct security events, validate alerts, and search historical data for incident response. Its open, machine-readable format powers the AI SOC ecosystem with comprehensive visibility, ensuring organizations can protect digital assets and meet audit requirements.

- **Protocol coverage:** Corelight provides full protocol semantics across hundreds of protocols, including JA3/JA4, TLS, DNS, HTTP, SMB, and Kerberos.
- **Data richness:** The evidence is a high-fidelity summary of network traffic, not just raw data. This real-time context validates alerts, reduces false positives, and enables confident threat hunting, eliminating the need to pivot to other tools.
- **Historical forensics:** The evidence is an immutable historical record for reconstructing attack timelines and meeting compliance. This data is more resilient to tampering than endpoint logs and is designed to support years of retention for threat hunting.
- **Data structure:** Built on the open-source Zeek framework, Corelight's evidence is delivered in a structured, AI-ready format, ensuring seamless integration with any SIEM, XDR, or data lake.

Customer case study

The difference between raw data and actionable evidence is critical. When a global game developer faced a $10 million ransom, their existing packet capture tools lacked the context to identify stolen assets. Corelight pinpointed the exfiltrated files, while SmartPCAP cut through the noise to isolate relevant packets. Armed with clarity, the team identified the breach's scope within hours and confidently rejected the ransom.



corelight

Open NDR visibility and multi-layered threat detection

Corelight delivers a comprehensive suite of network security analytics to help organizations identify over 100 adversarial TTPs across the MITRE ATT&CK® spectrum. The platform applies a multi-layered detection strategy—combining AI, behavioral analytics, signatures, and threat intelligence—to deliver risk-prioritized alerts.

- **Traffic coverage:** Corelight provides unified visibility by ingesting traffic from any source, including physical TAPs, virtual taps, native cloud mirroring (AWS, Azure, GCP), and flow data. This approach eliminates the visibility gaps and integration complexity that come from using disparate monitoring tools.
- **Detection methods:** Corelight's multi-layered detection leverages AI/ML models along with behavioral analytics, signatures, and threat intelligence to produce a high rate of deterministic detections and reduce false positives. It uses supervised and unsupervised ML models combined with best-in-class open-source engines (Zeek and Suricata) to detect over 100 adversarial TTPs.
- **Encrypted traffic analysis:** The platform addresses encrypted traffic visibility without complex decryption. It uses TLS fingerprinting (JA3/JA3S) to identify and track encrypted traffic. By analyzing protocols like SSH, SSL, and RDP, Corelight detects over 300 VPN types, SSH brute force attempts, and other hidden threats.
- **Explainability:** Every detection is supported by the underlying network evidence, showing analysts why an alert was generated. AI-powered explanations further clarify complex events in plain language. Because the platform is built on the open-source Zeek framework, teams can fully customize existing detections or create new ones to meet unique needs.

Customer case study

Global retailer Carrefour struggled with unified visibility across its extensive network of stores, headquarters, cloud, and partner connections, creating significant security blind spots. Reliance on limited firewall telemetry left critical areas without EDR coverage—such as store devices and partner networks—vulnerable to undetectable lateral movement. By deploying Corelight, Carrefour eliminated these blind spots, gaining high-quality network telemetry that integrated seamlessly into their SIEM and establishing a unified view of the entire attack surface. This comprehensive visibility empowered the security team to shift from reactive defense to proactive threat hunting, develop custom detections for early attacker activity, and ultimately boost the efficiency and effectiveness of their SOC.



corelight

Open NDR guided triage and integrated response

The Corelight Platform's AI-assisted workflows use Large Language Models (LLMs) to turn complex security alerts and network logs into plain-English summaries. These summaries explain why an alert was triggered, detail host behaviors, and offer guided triage steps. This Guided Triage capability reduces analyst cognitive load and makes forensic data accessible to all skill levels, elevating the entire SOC. The platform also includes suppression features to eliminate benign alerts, such as those from authorized red team exercises.

- **Integrated data:** Detections are shown in a visual timeline, letting analysts track attack progression. A single click pivots to correlated network logs, providing full context. The Unique Connection ID (UID) links all related logs (e.g., conn.log, http.log, dns.log) into a cohesive narrative, eliminating manual data stitching for faster investigations.
- **AI-assisted workflows:** Corelight integrates AI into workflows, making expert-level data accessible. AI generates plain-language summaries, context-aware explanations, and guided triage steps, ensuring no private data is shared or state preserved.
- **Access to raw data:** The Smart PCAP feature captures packets tied to suspicious traffic or alerts. Linked directly to detections, analysts can access full packets with one click. The Open NDR platform provides instant access to raw data, including logs and PCAP files, for deeper analysis.
- **Integrated response:** The Open NDR Platform enables swift responses with one-click actions to isolate hosts and enforce policies via integrations with EDR (e.g., CrowdStrike, Microsoft) and NGFW providers (e.g., Palo Alto Networks). These workflows reduce response times and mitigate threats effectively.

Customer case study

A critical malware alert at a financial services firm hit a common roadblock: the source IP was hidden behind a NAT barrier, making it hard to identify the compromised device. Corelight enabled the SOC team to overcome this by providing correlated evidence in a single interface. Pivoting from the HTTP-based alert to DNS requests and device logs, the team bypassed the NAT challenge in minutes. This streamlined workflow helped them pinpoint the infected machine and initiate remediation, turning a days-long investigation into swift action.

corelight

Open NDR SOC transformation and future-ready defense

Corelight provides a clear return on investment by modernizing the SOC through tool consolidation and delivering structured, context-rich network data. This data, based on open-source standards, is designed to integrate seamlessly with existing solutions, workflows, and AI toolsets.

- **Functional consolidation:** Corelight integrates IDS/IPS, NTA, file analysis, and full-packet capture into a single high-performance sensor. This approach reduces management overhead and hardware footprint while ensuring all data types are inherently correlated for superior investigative efficiency compared to siloed tools.
- **Ecosystem integration:** Corelight offers robust, out-of-the-box integrations with leading SIEM, XDR, and SOAR platforms. As the only Open NDR solution, it powers the SOC ecosystem with open, standards-based evidence and an MCP server built for AI orchestration.
- **Operational flexibility:** The platform supports all deployment models, from air-gapped to a full SaaS model with the Corelight Investigator console. It provides the same high-fidelity data and detection capabilities regardless of the deployment, allowing analysts to work in the native console or their existing SIEM/XDR.
- **Data portability and storage:** Corelight evidence is delivered in the non-proprietary Zeek format, ensuring you own your data and can export it anywhere. Unlike proprietary or "black box" data, Corelight data can be tuned, customized, stored and exported to meet your needs.
- **Cost efficiency:** Corelight controls SIEM ingest costs with data and log aggregation, SmartPCAP filters and SaaS solutions that allow you to store data outside your SIEM.



Customer case study

An investment firm's outdated, siloed toolset created an unsustainable trade-off between data retention and cost. Corelight solved this by consolidating disparate functions and shifting the strategy from "capture everything" to retaining the vital 5-10% of traffic as structured evidence. This pivot allowed the firm to extend retention from days to years on the same budget—cutting storage costs while securing the high-fidelity data necessary for a modern, AI-driven defense.

Extend retention from days to years on the same budget—cutting storage costs while securing the high-fidelity data

Open NDR customer success and managed NDR

Corelight's in-house cybersecurity experts assist customers from initial setup to ongoing strategic guidance, ensuring you maximize the value of your NDR investment and enhance your security posture.

- **Proactive and responsive support:** Corelight optimizes uptime with active system health monitoring. The Enterprise Support tier guarantees a one-hour response SLA for P1 issues, 24/7 availability, and next-business-day hardware replacement to ensure operational continuity.
- **Flexible service tiers:** Corelight offers flexible options, including a dedicated Technical Account Manager (TAM) in the Enterprise Support tier. TAMs act as strategic partners, providing ongoing guidance and targeted recommendations to help you optimize your investment.
- **Managed services availability:** To augment security teams, Corelight provides a 24/7 Managed NDR service. This offering acts as an extension of your SOC, delivering expert threat hunting, alert triage, and pre-configured playbooks for rapid response.

Customer case study

Seeking to create internal efficiencies and enhance their risk management, a government organization found that Corelight delivered more than just a product, but a true partnership that made a tangible difference to their SOC capabilities. The platform itself provided immediate value, delivering deep, actionable insights that integrated seamlessly with their existing SIEM. Just as importantly, Corelight's customer success team demonstrated exceptional knowledge, responsiveness, and proactivity at every stage, from initial concept to deployment and continuous maintenance, ensuring the solution's success.

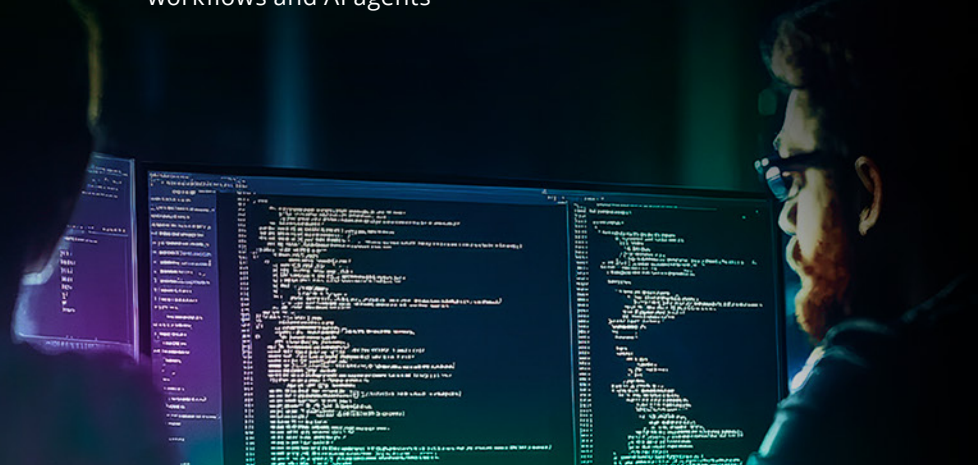


A buyer's checklist

To navigate the complex NDR market, security leaders need a clear framework for evaluation. The following checklist distills this guide's critical requirements into a practical tool for assessing any NDR vendor. This ensures your chosen solution provides the visibility, evidence, and control required to defend against modern threats.

Criteria I: Network data quality and forensic depth

- [ ] **High-fidelity data:** Transforms raw traffic and flow into structured, context-rich network data
- [ ] **Context enrichment:** Automatically identifies and enriches data with hostnames and service information, not just IP addresses
- [ ] **Comprehensive protocol coverage:** Parse9/13DNS, SMB, Kerberos, RDP, SSL/TLS)
- [ ] Delivers data in a structured, open, machine-readable format optimized for seamless integration with SIEMs, data lakes, and AI/ML pipelines
- [ ] Helps meet compliance requirements for different regulatory standards
- [ ] Data easily consumable by AI/ML detection models, GenAI workflows and AI agents



Criteria II: Unified visibility and comprehensive threat detection

- [ ] **Complete traffic coverage:** Provides consistent visibility across on-premises, virtual, multi-cloud, and IoT/OT environments from a single platform
- [ ] Comprehensive threat detection:
  - [ ] Maps all detections to the MITRE ATT&CK framework for clarity and consistency
  - [ ] **Anomaly detection:** Establishes a baseline of normal network activity to identify anomalous activity.
  - [ ] **AI models:** Utilizes AI models for detecting unknown threats
  - [ ] **Signature-based detection:** Utilizes high-performance signature engines to detect known threats
  - [ ] **Threat intelligence:** Natively ingests and operationalizes third-party threat intelligence feeds
- [ ] **Encrypted traffic analysis:** Detects threats within encrypted traffic without requiring costly and complex universal decryption
- [ ] **Explainable and extensible logic:** Provides explainable detections and enables security teams to customize or create their own rules

Criteria III: Accelerating response and empowering analysts

- **Intuitive, integrated interface:** Features a UI designed for efficient workflows, linking detections directly to the underlying data to eliminate context-switching
- **AI-assisted workflows:** Leverages AI to provide plain-language summaries of complex alerts and guided triage steps to accelerate investigation and empower junior analysts
- **Rapid time-to-value:** Allows for quick deployment and easy tuning, including simple suppression or allow-listing of authorized business activities
- **Integrated response actions:** Offers robust, out-of-the-box integrations with EDR, SOAR, and firewalls, enabling rapid, evidence-based response actions directly from the platform

Criteria IV: Driving SOC modernization and enabling AI SOC

- **Flexible deployment architecture:** Supports a full range of deployment models, including entirely on-premises/air-gapped, cloud-hosted (SaaS), and hybrid configurations without feature compromise. Offers centralized capabilities to manage configurations, updates, user roles, and access levels, as well as sensor health, across the enterprise
- **Scalable:** Ability to handle high-throughput networks exceeding 1Tbps traffic
- **Functional consolidation:** Replaces the core functions of multiple legacy tools (IDS, NTA, PCAP) in a single platform
- **Operational flexibility:** Enables analysts to perform investigations either using the platform's native console or seamlessly within their primary SIEM or XDR, accommodating the SOC's preferred workflow
- **Open and extensible ecosystem:** Is built on open standards to prevent vendor lock-in and offers robust integrations with the entire security stack (SIEM, SOAR, XDR, etc.)
- **Data portability and ownership:** Guarantees that customers own their data, delivering it in a non-proprietary format that can be easily and cost-effectively exported to any destination. Enables programmatic access to the data that other AI SOC agents can leverage through functionality like MCP server



up to 80%
Reduction in log volume

7:1
Log consolidation

up to 5x
Faster queries

corelight

Criteria V: Enterprise-grade support and partnership

- ☐ **Proactive and responsive support:** Offers proactive system health monitoring and a proven track record of rapid, expert-level responses with clear SLAs for critical issues
- ☐ **Flexible service tiers:** Provides a range of support options, from standard 24/7 assistance to dedicated resources like a Technical Account Manager (TAM) for ongoing strategic guidance
- ☐ **Managed services availability:** Offers an optional Managed NDR service to augment internal teams with 24/7 threat hunting, alert triage, and expert guidance

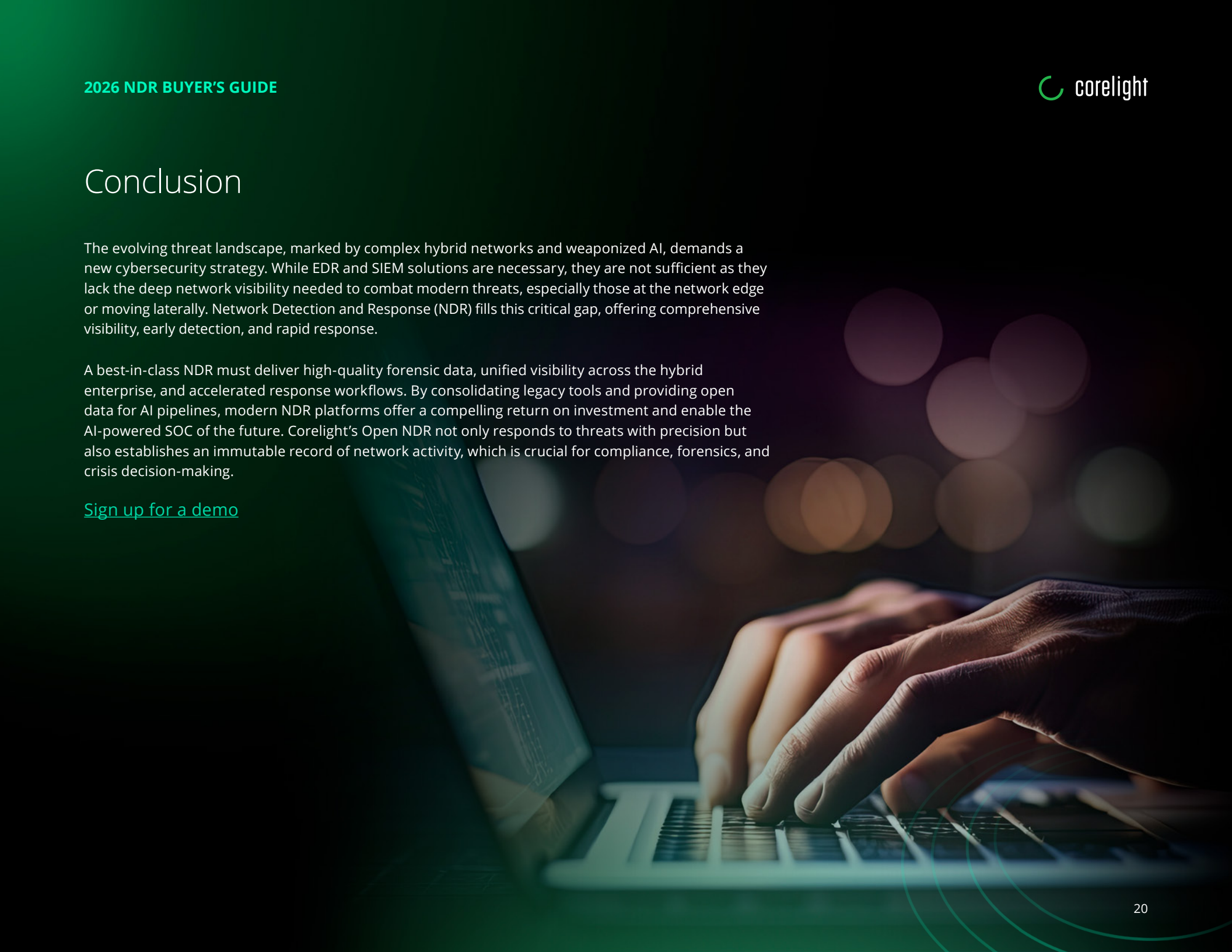


Conclusion

The evolving threat landscape, marked by complex hybrid networks and weaponized AI, demands a new cybersecurity strategy. While EDR and SIEM solutions are necessary, they are not sufficient as they lack the deep network visibility needed to combat modern threats, especially those at the network edge or moving laterally. Network Detection and Response (NDR) fills this critical gap, offering comprehensive visibility, early detection, and rapid response.

A best-in-class NDR must deliver high-quality forensic data, unified visibility across the hybrid enterprise, and accelerated response workflows. By consolidating legacy tools and providing open data for AI pipelines, modern NDR platforms offer a compelling return on investment and enable the AI-powered SOC of the future. Corelight's Open NDR not only responds to threats with precision but also establishes an immutable record of network activity, which is crucial for compliance, forensics, and crisis decision-making.

Sign up for a demo





Uncover hidden threats with network evidence:

Chat with us Request a demo

info@corelight.com | 888-547-9497

The Z and Design mark and the ZEEK mark are trademarks and/or registered trademarks of the International Computer Science Institute in the United States and certain other countries. The Licensed Marks are being used pursuant to a license agreement with the Institute.

All rights reserved. © Copyright 2026 Corelight, Inc.