NETWITNESS

Guide

RFI Evaluation Checklist for Security & Risk Leaders

The Enterprise NDR Evaluation Checklist for CISOs

Table of Contents

Chapter	Page No.
Evaluating Network Detection and Response (NDR) Platforms	3
How to Use This Document	3
Evaluation Scope	3
Intended Audience	4
Instructions to Vendor	4
NDR Architecture	4
Packet Capture & Metadata Processing	4
TLS & Encrypted Traffic Visibility	5
Detection Logic & Content Framework	5
Investigation & Threat Hunting Workflow	5
Integration & Automation	5
Scalability & High Availability	6
Platform Security Controls	6
Proof of Value (PoV) Execution	6
Licensing & Commercial Transparency	6

Evaluating Network Detection and Response (NDR) Platforms

Security and risk management leaders evaluating Network Detection and Response (NDR) platforms typically face two operational requirements:

1. Obtaining reliable visibility into network activity across on-premises, cloud, and hybrid environments
2. Validating security alerts through verifiable evidence during investigation and response

Multiple technologies in the market are positioned as NDR solutions. However, implementation approaches vary significantly in areas such as traffic acquisition, data retention, detection methodology, and investigation workflow.

As a result, organizations must determine whether a proposed platform supports operational security outcomes, not only detection capabilities.

This checklist documents required capabilities that organizations should evaluate before selecting an NDR solution suitable for enterprise security operations.

How to Use This Document

This fillable worksheet is intended to help business and technical decision-makers evaluate vendor capabilities in a consistent and auditable manner.

The checklist allows organizations to:

- Compare vendor capabilities across standardized technical criteria
- Validate functionality during demonstrations or proof-of-value exercises
- Record responses for procurement and architecture review
- Identify operational gaps prior to deployment

Vendors should provide detailed responses in the designated fields and include supporting documentation where applicable.

Evaluation Scope

The checklist is organized into the following capability areas:

- Platform Architecture & Deployment
- Network Visibility & Data Collection
- Encrypted Traffic Analysis
- Detection Logic & Threat Intelligence
- Investigation & Threat Hunting Workflow
- Integration & Automation
- Scalability & Availability
- Platform Security & Access Control
- Proof of Value & Operational Validation
- Licensing & Commercial Transparency

Each section contains structured questions designed to confirm technical capability, operational usability, and long-term viability of the platform.

Intended Audience

This document is designed for use by:

- Chief Information Security Officers (CISOs)
- Security Architecture Teams
- Security Operations Centers (SOC)
- Incident Response Teams
- Procurement and Vendor Management

Instructions to Vendor

Vendors are requested to:

- Provide clear, technical responses
- Avoid marketing language
- Include configuration or architectural details where applicable
- Reference documentation, guides, or validated deployments
- Indicate limitations where functionality is not available

Incomplete or non-technical responses may require follow-up clarification during evaluation.

NDR Architecture

Requirement / Question	Vendor Response	Supporting Documentation / References
Describe the deployment of Decoders for full packet capture (PCAP), including throughput limits per instance.		
Explain the role and configuration of Concentrators for metadata indexing and query performance.		
Detail Broker configuration for federated search across multiple sites.		
Describe Respond module integration for case management and workflow.		
Provide reference architecture for physical, virtual, and cloud deployments.		

Packet Capture & Metadata Processing

Requirement / Question	Vendor Response	Supporting Documentation / References
Confirm full packet capture capabilities and sustained ingestion throughput.		
List supported protocol parsers and metadata extraction coverage.		
Explain the session reconstruction workflow from metadata to packet retrieval.		
Define packet vs metadata retention model and storage architecture.		
Provide performance benchmarks in environments exceeding 10 TB/day.		

TLS & Encrypted Traffic Visibility

Requirement / Question	Vendor Response	Supporting Documentation / References
Explain TLS handshake inspection and certificate metadata extraction.		
Confirm JA3/JA4 fingerprinting support and operational use cases.		
Describe detection of encrypted command-and-control traffic without decryption.		
Clarify technical limitations in encrypted payload visibility.		

Detection Logic & Content Framework

Requirement / Question	Vendor Response	Supporting Documentation / References
Describe App Rules and ESA Rule implementation.		
Explain threat intelligence integration mechanisms.		
Provide MITRE ATT&CK mapping for built-in detection content.		
Describe detection update cadence and content lifecycle management.		
Explain false positive tuning and suppression mechanisms.		

Investigation & Threat Hunting Workflow

Requirement / Question	Vendor Response	Supporting Documentation / References
Describe pivot workflow: Alert → Metadata → Packets.		
Explain session reconstruction and file extraction process.		
Provide query performance benchmarks at scale.		
Describe cross-site investigation using Broker.		
Detail Respond module case management workflow.		

Integration & Automation

Requirement / Question	Vendor Response	Supporting Documentation / References
Detail SIEM integration capabilities.		
Explain SOAR integration and automation triggers.		
List supported APIs and export formats (REST, Syslog, STIX/TAXII).		
Describe integration with EDR and third-party telemetry.		

Scalability & High Availability

Requirement / Question	Vendor Response	Supporting Documentation / References
Explain the horizontal scaling model for Decoders and Concentrators.		
Describe high availability configurations.		
Provide multi-site deployment reference architecture.		
Clarify storage scaling model for packet retention.		

Platform Security Controls

Requirement / Question	Vendor Response	Supporting Documentation / References
Describe role-based access control (RBAC) configuration.		
Explain encryption standards for data at rest and in transit.		
Detail audit logging and administrative controls.		
Describe multi-tenancy configuration (if applicable).		

Proof of Value (PoV) Execution

Requirement / Question	Vendor Response	Supporting Documentation / References
Describe structured PoV deployment model.		
Explain validation methodology for detection effectiveness.		
Provide metrics for alert fidelity and investigation time reduction.		
Describe the integration testing approach during PoV.		

Licensing & Commercial Transparency

Requirement / Question	Vendor Response	Supporting Documentation / References
Clarify licensing model (throughput-based, component-based, subscription).		
Define storage cost implications for packet retention.		
Detail support tiers and SLAs.		
Provide 3–5 year Total Cost of Ownership estimate.		

Conclusion

Selecting an enterprise NDR platform is a long-term operational decision that directly impacts detection confidence, investigation speed, and incident response effectiveness. Security leaders must therefore validate not only detection claims, but also architectural soundness, evidence availability, scalability, and integration readiness within the existing security ecosystem.

A structured RFI evaluation helps organizations move beyond feature comparison toward measurable security outcomes. By documenting technical responses, validating workflows during proof-of-value exercises, and assessing total operational impact, teams can reduce deployment risk and ensure alignment with enterprise security objectives.

This checklist is intended to support informed decision-making, strengthen vendor accountability, and enable security teams to adopt an NDR capability that improves real-world investigative readiness.

Contact Information

Email for customer Service
support@netwitness.com

Website
www.netwitness.com

Follow us for regular updates