BUYER'S GUIDE

NETWORK DETECTION AND RESPONSE (NDR)

NDR detects suspicious events that other network security tools are missing

STELLAR CYBER®

WHAT IS NDR?

NDR evolved out of Network Security

Today's network detection and response (NDR) has a long history, evolving out of network security and network traffic analysis (NTA). The historical definition of network security is to use a perimeter firewall and Intrusion Prevention Systems to screen traffic coming into the network, but as IT and security technology have evolved, the definition is much broader now due to modern attacks leveraging more complex approaches.

Today, network security is everything a company does to ensure the security of its networks, and everything connected to them. This includes the network, the cloud (or clouds), endpoints, servers, IoT, users and applications. Network security products seek to use physical and virtual preventive measures to protect the network and its assets from unauthorized access, modification, destruction and misuse.

These security products typically target certain aspects of the network:

- **User Entity and Behavior Analytics (UEBA):** monitor user and / or entity activity, baseline normal behavior, and alert on activities that deviate from normal activity.
- **Intrusion Prevention / Detection Systems (IPS / IDS):** monitor for and block known attacks in the allowed traffic that gets past the firewall.
- **PCAP Devices:** capture the raw packets traveling over a computer network and store them for forensic analysis and / or attack replays.
- **Network Traffic Analysis (NTA):** collect traffic metadata from all available sources, internal and external, and analyze for anomalies, risk, and threats.
- **Firewalls:** prevent unauthorized accessing the network by allowing or denying traffic.
- **Sandbox and Anti-Virus / Malware software:** protect network, endpoints and servers from becoming infected with damaging software that can corrupt files, export sensitive data, or perform other malicious activities.
- **Application Security:** look for and block vulnerabilities in the application software.
- **Cloud Security:** protect resources and applications in the cloud.

There are a lot of products that fall under the umbrella of network security, and managing those holistically to detect and respond to risk and threats on the network is challenging. That's where NDR comes in. **NDR as a technology category seeks to first consolidate NTA, IDS, UEBA and TIP into a single superset platform for both detection and response, and second go way beyond NTA ever did, acting as the brains behind all the other network security products through Machine Learning and auto-correlation.**

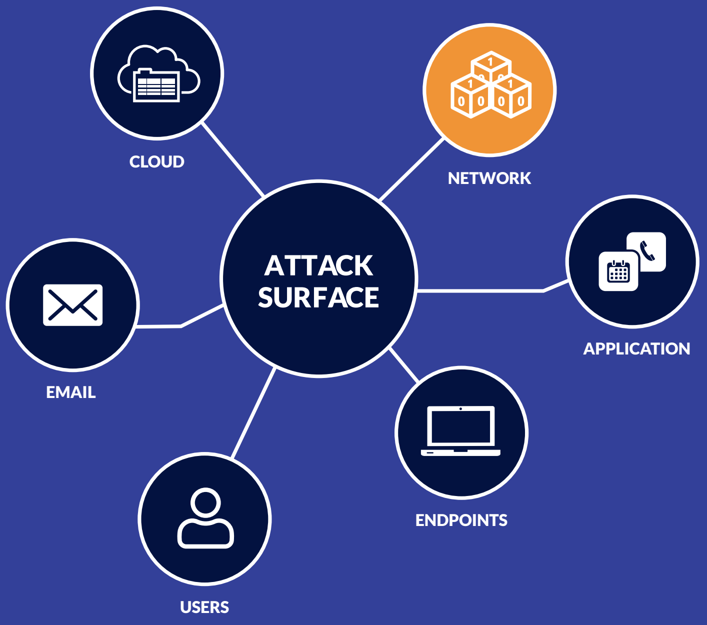
NDR today has been proposed by Gartner as a core capability for security operations to ensure you have the visibility you need to uncover modern attacks quickly. NDR is a perfect complement to SIEM or NG-SIEM to get visibility beyond logs.

WHY YOU NEED NDR

NDR ensures full visibility and verifies Zero Trust

Analyzing endpoint data and security tool logs is not enough to thwart today's attacks. **If there is one important thing to know about the network traffic, it's that it doesn't lie.** That's why NDR completes an organization's data journey to XDR alongside EDR for endpoint data and SIEM for security tool logs. Specifically, NDR sees what the endpoints and other logs don't see (the entire network; devices, SaaS applications, user behavior), acts as a quality ground truth data set, and enables real time response.

As Zero Trust continues to get adopted, the network will undergo different segmentations improving security fundamentals. As with any complex system, a trust but verify approach must be taken and NDR perfectly complements Zero Trust as its verification counterpart. **NDR enables organizations to adopt Zero Trust with confidence and verify its enforcement.**



MODERN NDR ARCHITECTURE

An adaptive approach to complete attack surface coverage

NDR solutions use non-signature-based techniques (for example, machine learning or other analytical techniques) alongside quality signature-based techniques (for example threat intelligence fused in-line for alerts) to detect suspicious traffic or activities. NDR can ingest data from dedicated sensors, firewalls, IPS / IDS, metadata (NetFlow), or any other network data source. **A flexible deployment architecture allows both north / south traffic and east / west traffic to be monitored in addition to traffic in all physical and virtual environments.** All data is sent to a centralized scalable data lake with a powerful AI Engine to detect suspicious traffic patterns and abnormal behaviors to raise high-fidelity alerts. Depending on particular solutions, the AI engine from the best NDR vendors may have advanced auto-correlation capabilities that group related alerts from many other security tools like EDR or logs to have a more efficient and accurate view of alerts.

Response is the critical counterpart to detections to enable a performant network-based approach to security operations and is fundamental to NDR. Automatic responses such as sending commands to a firewall to drop suspicious traffic or to an EDR tool to quarantine an affected endpoint, or manual responses such as providing threat hunting or incident investigation tools are common elements of NDR.

NDR BUYERS CHECKLIST

Use the table below to compile a short list of vendors.

The capabilities listed below are what enables a solution to deliver on:

- The modern definition of NDR – A platform that is a superset of capabilities that acts as the brains for all network security products
- Full visibility and Zero Trust verification – Ability to be able to consume all network security data
- Adaptive architecture – Flexible and pervasive deployment models

CAPABILITY	DESCRIPTION
360º data collection from any network source	• Extract metadata at ingestion by dedicated network sensors from both virtual and physical infrastructure • Collect firewall traffic logs, IDS events, NetFlow and cloud flow logs • Assemble files from traffic
Data normalization and context creation	• Normalize the data to a common human-readable and searchable format • Enrich the data with context including Threat intelligence, and Geolocation, asset information, and user information • Correlate the data among security tools such as IDS events with rich network metadata from network sensors
High-fidelity detection with AI and automated grouping of alerts	• A full suite of pre-configured network detections via machine learning: unsupervised, supervised or Graph ML • User and entity behavior analysis through machine learning or advanced analytics • Automatic correlation of related alerts from different security tools into high-level incidents
Automated response	• Manual and automatic threat hunting • Automatic response playbooks • Broad integration with many other tools to take quick response actions such as disabling users on AD or blocking traffic on a firewall
Tightly integrated suite of additional tools	• ML-IDS for known attack detection, Sandbox for zero-day malware analysis • Asset management for comprehensive and automatic inventory of assets • Compliance reporting

RECOMMENDATIONS FOR BUYERS

To improve security and the detection of suspicious network traffic and abnormal user behaviors, security and risk management leaders should:

- Implement a solution that delivers on NDR as a superset platform to avoid having to manage a complicated network security stack and ensure top performance
- Implement a solution that marries both AI-based detections tools alongside the signature based for comprehensive detection of both known and unknown attacks from network traffic
- Decide early in the evaluation process whether the solutions under assessment have adequate automated response or manual response capabilities integrated directly with other security products – seamless integration is critical for reducing dwell time

STELLAR CYBER DELIVERS COMPREHENSIVE NDR+

Stellar Cyber's Open XDR includes NDR and correlates network data with all your data—delivering NDR+

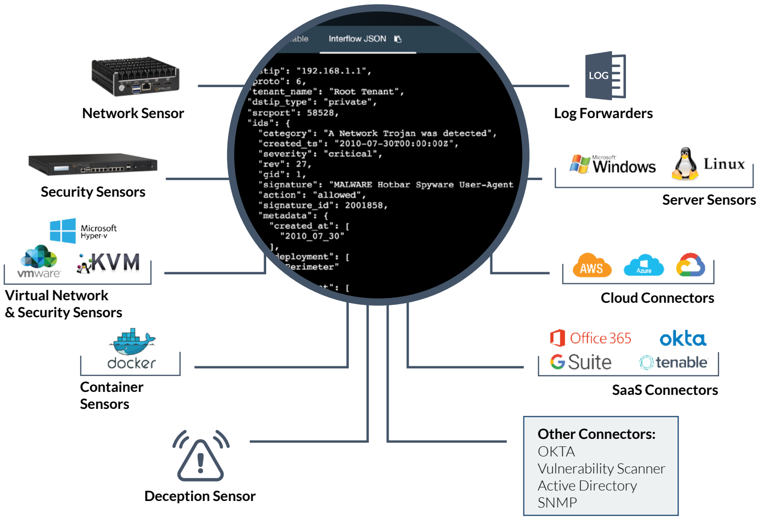
Go beyond logs and get full visibility into all aspects of your network, regardless of where your network is. Stellar Cyber's Open XDR Platform has an industry-leading NDR capability built-in. It has a family of sensors distributed to collect network telemetry, an ML-IDS engine for known attacks, an AV/Sandbox for zero-day malware analysis, an advanced processor engine for data normalization and context creation, a centralized data lake store contextualized network telemetry, a Threat Intelligence Platform (TIP) for TI feeds, a powerful AI engine for detection and correlation, and automatic response through various integrations. All these features work out of the box. Get up and running with NDR in days and see threats that were previously hidden.

- Analyze raw network packet traffic and extract metadata in real time with a powerful Deep Packet Inspection (DPI) engine through dedicated network sensors or traffic logs from existing firewalls or traffic flows (NetFlow).
- Monitor and analyze north / south traffic (as it crosses the perimeter), as well as east / west traffic (as it moves laterally throughout the network).
- Model normal network traffic and user behaviors, and highlight suspicious traffic or user behaviors that fall outside the normal range.
- Use behavioral techniques (non-signature-based detection) such as machine learning or advanced analytics that detect network anomalies.
- Provide automatic or manual response capabilities to react to the detection of suspicious network traffic or user behaviors.
- Use advanced machine learning such as Deep Learning for evasive attacks like DGA and DNS tunneling.

STELLAR CYBER SOLVES THE NDR DATA PROBLEM

Stellar Cyber's Interflow – Normalized, enriched, actionable data

The industry has been challenged to solve the Goldilocks dilemma of cybersecurity by capturing network packets, files and logs in an effort to output a dataset that is richer than NetFlow (too little), significantly lighter weight than PCAP (too big) and fused with context (just right) such as host name, user information, Threat Intelligence and geolocation, etc.



```
stip": "192.168.1.1",
proto": 6,
"tenant_name": "Root Tenant",
"dstip_type": "private",
"srcport": 58528,
"ids": {
  "category": "A Network Trojan was detected",
  "created_ts": "2010-07-30T00:00:00Z",
  "severity": "critical",
  "rev": 27,
  "gid": 1,
  "signature": "MALWARE Hotbar Spyware User-Agent
  "action": "allowed",
  "signature_id": 2001858,
  "metadata": {
    "created_at": [
      "2010_07_30"
  ],
  deployment": [
  Perimeter"

  t": [
```

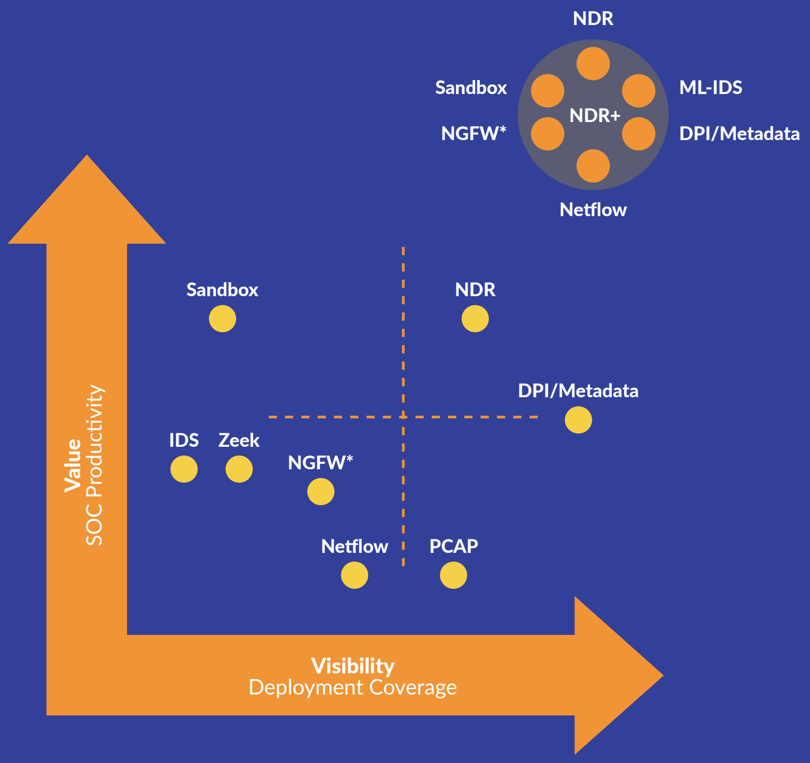
Other Connectors:
OKTA
Vulnerability Scanner
Active Directory
SNMP

Interflow is an integral part of the Stellar Cyber Open XDR platform – a data extraction engine with a powerful DPI functionality that extracts telemetry from packets and a fusion engine that automatically makes your telemetry more valuable. It is a normalized, enriched data model that allows IT and security tools to talk the same language so you can detect and respond to every threat. Interflow solves network security problems with a model that was purpose-built for network security. Stellar Cyber's rich set of sensors literally collects all telemetry from anything, anywhere.

With Interflow, your security team can:

1. Stop doing manual data munging – With Interflow, context is automatically created
2. Reduce data volume – PCAP-to-Interflow data reduction can be up to two orders of magnitude
3. Correlate across seemingly unrelated events – Standard key values make correlation easy
4. Highly interpretable – Reduce analyst training time with easy-to-understand data.

STELLAR CYBER'S INTERFLOW DELIVERS VALUE & VISIBILITY



PCAP:	Too much data to store and too hard to analyze
Netflow:	Not enough data to be useful while limited by switches / routers
IDS:	Not scalable; too noisy and too expensive
NGFW*:	Not enough data and limited scale
Sandbox:	File based malware only and very expensive
DPI/ Metadata:	Good balance of fidelity and cost; easy to deploy
NDR/NTA:	Often noisy and expensive

GARTNER MARKET GUIDE: FOR NETWORK DETECTION & RESPONSE: JUNE 2020

Only Stellar Cyber delivers on all twelve NDR criteria

	CRITERIA	DETAIL	STELLAR CYBER
1	**Data Type**	Raw packets, NGFW/IDS Logs, NetFlow / IPFix	✓
2	**Data Source**	Physical or virtual switches, containers, servers, IaaS (Azure, AWS, Google Cloud, Platform, Oracle Cloud Infrastructure)	✓
3	**Traffic Content**	Powerful DPI with 3000+ identified applications 10,000+ L2-L7 metadata, files from traffic flow	✓
4	**Data Reduction**	Meta data extracting, data filtering, data compression, packet de-duplication	✓
5	**Encrypted Traffic**	Behavioral analysis, certificate inspection, JA3	✓
6	**Data Enrichment**	Threat intelligence, IP geolocation, IP to host name, IP to username, IP address types	✓
7	**Data Retention**	Configurable hot storage and external cold storage for compliance	✓
8	**Data Availability**	Data buffering, data replica, HA, disaster recovery	✓
9	**Detection**	Supervised & unsupervised learning, deep and adaptive learning, IDS with ML, Sandbox, UEBA	✓
10	**Correlation**	Auto-correlation among IDS events, vulnerability, EDR, Sandbox and suspicious events detected from ML	✓
11	**Response**	Drop traffic, disable users, contain endpoints, trigger vulnerability scan, invoke scripts, call APIs, alerting, reporting	✓
12	**Deployment**	Physical or virtual appliance, servers, IaaS in IaaS (AWS, Azure, GCP, OCI) all-in-one or distributed	✓

REQUEST A DEMO NOW!

stellarcyber.ai

Stellar Cyber's Open XDR platform delivers Everything Detection and Response by ingesting data from all tools, automatically correlating alerts into incidents across the entire attack surface, delivering fewer and higher-fidelity incidents, and responding to threats automatically through AI and machine learning. Our XDR Kill Chain™, fully compatible with the MITRE ATT&CK framework, is designed to characterize every aspect of modern attacks while remaining intuitive to understand. This reduces enterprise risk through early and precise identification and remediation of all attack activities while slashing costs, retaining investments in existing tools and accelerating analyst productivity. Typically, our platform delivers a 20X improvement in MTTD and an 8X improvement in MTTR. NDR is one of the natively supported tools of Open XDR platform. The company is based in Silicon Valley.

www.stellarcyber.ai | sales@stellarcyber.ai