vehere

WHITEPAPER

Navigating Network Security: Understanding the need for Network Detection & Response beyond Firewalls

What is Network Detection & Response?

During the early 2010s, Network Detection and Response (NDR) technology surfaced as a means to detect and mitigate evasive network threats that could not be blocked by conventional prevention methods reliant on known attack patterns or signatures. NDR, previously known as network traffic analysis (NTA), leverages machine learning and behavioral analytics to monitor network traffic, establishing a baseline of activity. Subsequently, it identifies irregular activities linked to targeted attacks, insider abuse, and risky behavior.

Network Detection and Response (NDR) tools utilize behavioral analytics on network traffic data to identify irregular system behaviors. These solutions consistently evaluate either the raw network packets or traffic metadata within internal (east-west) and external (north-south) networks. NDR systems are typically a blend of hardware and software components serving as sensors, alongside a management and orchestration console available either as on-premise software or via a Software as a Service (SaaS) model.

Enterprises depend on NDR for the identification and containment of post-breach activities, such as ransomware, insider threats, or lateral movements within their networks. NDR works in tandem with other technologies that primarily generate alerts based on predefined rules and signatures, enhancing security by constructing heuristic models of typical network behavior and identifying any deviations from these norms.

Some of the most important benefits of the NDR solution include-

- Early detection of network security issues
- Improved visibility
- Enhanced analytics
- Reduced mean time to detection (MTTD) and mean time to resolution (MTTR)
- Enhanced threat intelligence
- Maintaining regulatory compliance

What is Firewall?

A firewall is a network security system, either hardware or software-based, that monitors inbound and outbound network traffic and determines whether to allow or block specific traffic based on a pre-defined set of security rules.

Firewalls have served as the first layer of defense in network security for more than 25 years. They create a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks.

Significance of a firewall include-

- Monitoring network traffic
- Stops virus attacks
- Aids in prevention of hacking activities
- Stops spyware
- Helps promoting privacy

Comparative study between Network Detection & Response and Firewall

Point of difference	Firewall	Network Detection and Response (NDR)
Purpose	Enforces access control policies and control network traffic.	Detects and responds to security threats within the network.
Functionality	Filters and controls traffic based on predefined rules and policies.	Analyzes network traffic in real-time, identifies anomalies, and provides incident detection and response capabilities.
Real-time Monitoring	Provides real-time traffic control by blocking or allowing packets based on rules.	Monitors network traffic continuously in real-time and identifies security threats as they occur.
Protection Focus	Focuses on preventing unauthorized access and known threats.	Focuses on detecting unknown, emerging, and advanced threats, including insider threats.
Use Cases	Protects the network by controlling inbound and outbound traffic.	Identifies and responds to security incidents, advanced threats, and abnormal network behaviours.
Incident Response	Limited incident response capabilities, mainly focused on blocking malicious traffic.	Provides advanced threat detection and facilitates comprehensive incident response, including isolation and mitigation of threats.
Log Retention	May retain logs for compliance and auditing purposes.	Retains extensive network traffic and event logs for forensic analysis and investigations.
Visibility	Provides visibility into allowed or blocked traffic based on rules.	Offers deep visibility into network behaviour, facilitating threat detection, and forensic analysis.
Deployment Location	Typically deployed at network perimeter or between network segments.	Deployed at various points in the network infrastructure, including gateways, switches, and routers.
Proactive vs. Reactive	Proactively prevents security incidents in real-time.	Proactively detects threats in real-time and supports reactive incident response for known and unknown threats.

Customization	Rule-based customization to define allowed and denied traffic.	Requires advanced configuration and tuning to establish a baseline of normal network behaviour and detect anomalies.
Data Sources	Analyzes packet headers, port numbers, IP addresses, and protocols.	Analyzes network traffic payloads, behaviour, and flow data for anomaly detection.
Integration with SIEM	Often integrated with SIEM solutions for centralized log management.	Frequently integrated with SIEM for comprehensive threat correlation, analysis, and incident response.

Why is NDR essential?

Firewalls can only detect traffic travelling north and south, not east and west. Furthermore, firewalls lack a large enough data lake to conduct additional behaviour analysis. Firewalls are similar to security guards. When unknown threat actors circumvent the gateway security control, the firewall becomes practically useless. A further obstacle is that AI-enabled malware can quickly comprehend the environment in which it operates. This enables it to avoid detection and removal by taking evasive steps. So, to counter these challenges, organizations should implement an NDR solution so that they can benefit from a layered approach to security.

Vehere Network Detection and Response (NDR)

Vehere NDR detects abnormal system behaviors by leveraging behavioral analytics/AI-ML. It detects and contains post-breach activity such as ransomware, APTs, insider threats or lateral movements. Some of the key features of this technology are:

- 100% visibility with lossless packet capture
- Analytics based on DPI with L2-L7 metadata
- Monitoring both E-W and N-S traffics
- Historical metadata and content
- Behavior-based Protocol Detection

It is a core component of Vehere AI Network Security, a 5-in-1 unified platform that acts as a “Second Line of Defense” to protect your corporate network from the most advanced cyberthreats. Apart from NDR, it includes Network Forensics, Next-gen Sandboxing, Proactive Threat Hunting and Intrusion Detection System.

About Vehere

Vehere is a new-age Cybersecurity software company specializing in AI Cyber Network Intelligence. For more than a decade, Vehere has been supporting counter-terrorism analysts in Defense & Intelligence communities. Vehere is now trusted by cyber-analysts in Fortune 500 companies, including Telecom, Financial institutions, and Smart Cities to protect their critical infrastructure against real-time cyberattacks.

Vehere preserves fundamental principles of privacy and civil liberties. We proactively defend your cyberspace by cross-leveraging our expertise between national security and enterprise security.

Vehere InVehere Vehere