HUGHES®
An EchoStar Company

NETWORK DETECTION AND RESPONSE— FINDING HIDDEN THREATS

INTRODUCTION

Our interconnected world

Networks form the cornerstone in today's interconnected world, making them a primary focus for cyber attackers seeking to disrupt business operations.

Cyberattacks are growing, not just in number, but also in sophistication. This, coupled with evolving IT landscapes and a continuous rise in network activity, can create conditions where threat actors remain unnoticed.

In today's digital environment, every company—regardless of its size—is susceptible to being the target of an attack, jeopardizing its operations, brand, reputation and revenue streams—which are all potentially at risk of a breach.

A survey by Statista revealed that over 45% of IT security professionals claim that one to five successful cyberattacks against their organization's global network happened within the past 12 months. Nearly 12% experienced more than ten successful cyberattacks.

The goal of a cyberattack is often to breach the corporate network perimeter and infiltrate internal systems in an attempt to gain unauthorized access. Once inside, attackers steal, modify or delete data, compromise endpoints and spread malware, viruses, Trojan horses and other elements in an attempt to control the network and protocols, as well as exploit vulnerabilities within the network.

The resulting harm to both a company and its customers can be swift and substantial. The speed with which an organization responds is crucial, and yet most small and mid-sized companies aren't equipped to handle such incidents. The financial and business consequences can be insurmountable. No organization is 100% secure.

The good news — Cybercriminals can't hide in a network

Network Detection and Response (NDR) offers a holistic perspective on all enterprise devices, entities and network traffic, continuously monitoring and analyzing real-time traffic flow across the network. Meaning you are able to get a wider view of your network than before.

NDR tools provide context-rich visibility, not only at the entry and exit points, but also for lateral movements across the network—strengthening network monitoring, detection and prediction capabilities across cloud-native or hybrid-cloud network environments. With a shift toward cloud-based environments comes increased vulnerability, necessitating increased vigilance and protection.

NDR has the ability to protect any device that is connected to the network. With the rising prevalence of Internet of Things (IoT) and other connected devices, the risk of cyber threats grows, potentially putting millions of individuals at risk of being hacked or having personal data compromised.

Endpoint Detection and Response (EDR) solutions are effective, but they do not cover IoT devices that cannot run the EDR software (think of devices that connect to the internet but do not have screens or the ability to run windows). This means that cybercriminals can potentially bypass your security solutions to carry out attacks on IoT devices, underscoring the importance of NDR to catch these kinds of attacks.

The number of IoT cyberattacks worldwide amounted to over 112 million in 2022—a figure that has increased significantly from around 32 million detected cases in 2018, according to research by Statista.

Why you need complete network visibility

Networks are growing in both size and complexity with an unprecedented volume of data. This increased complexity creates a greater number and variety of connections susceptible to cyberattacks.

Cyber attackers actively seek out security vulnerabilities in networks, devices, data, users and applications. Common network security threats include malicious software (malware), phishing schemes, Distributed Denial of Service (DDoS) and encryption of data that leads to ransomware extortion, to name a few.

Small and mid-sized businesses who cannot afford significant investments in cybersecurity technologies, face the highest vulnerability.

Signs of a security breach

Cybersecurity failures often stem from lack of adequate controls. A threat actor just needs to get lucky once. Common signs of a security breach include:

- Irregular network or app traffic
- Unexpected network activity such as strange login attempts or downloads from remote or unfamiliar websites
- Slow network performance and abnormal resource usage
- Inability to login and access servers, email accounts or applications
- Unusual file modifications, encrypted files or the appearance of new directories
- New subdomains or unfamiliar types of Domain Name System (DNS) records that you did not create
- Browser security alerts while loading your web pages
- Unfamiliar code present in your applications
- Unusual amounts of outgoing email spam
- Unexpected service disruptions and server restarts
- Suspicious bank and credit card transactions
- Blacklisting of your server IP address

IoT devices are especially vulnerable

The number of IoT connections grew globally by 18% in 2022 to 14.3 billion active IoT endpoints, and is expected to grow another 16% to 16.7 billion according to the latest 2023 report by IoT Analytics.

As the use of IoT devices increases, so does the potential for cyber threats. IoT devices are especially vulnerable because they often lack a unified set of security standards, which can leave room for hackers to exploit those vulnerabilities.

The primary risks associated with the use of IoT devices revolve around security and privacy. These devices frequently gather and transmit data, potentially enabling the tracking of users' locations, habits and even shopping preferences. This poses a significant privacy challenge, particularly for individuals that are heavily dependent on such devices.

Other risks include weak or non-existent authentication mechanisms, lack of encryption, default settings and unsecure communications that could allow threat actors to gain access to sensitive information such as passwords or credit card numbers.

Every business is at risk

Cybersecurity continues to be a primary concern for boards of directors, leading to increased oversight and scrutiny. According to Gartner, in the past five years, the percentage of boards that consider cybersecurity a business risk has risen from 58% to 88%. By 2025, 40% of all boards of directors will have a dedicated cybersecurity committee overseen by a qualified board member.

The financial consequences of a cyberattack impact every corner of the business—including network downtime, service disruption, breach investigation, legal actions, reputation damage control, loss of productivity and the effort spent to improve security measures. According to Statista, the average cost of a data breach in the United States amounted to $9.44 million in 2022, up from $9.05 million in the previous year.

Beyond the financial impact, an attack can also have a devastating and long-term effect on the trust between an organization and its customers, as well as a material impact on sales and reputation.

What is Network Detection and Response?

Network Detection and Response (NDR) is a security tool that monitors an enterprise's network traffic and helps to eliminate network blind spots and detect potential threats before they occur.

It does this by continuously monitoring and analyzing a small sampling of network traffic patterns using advanced technologies such as behavioral analytics, Artificial Intelligence (AI) and Machine Learning (ML), to generate a baseline of normal network traffic behavior.

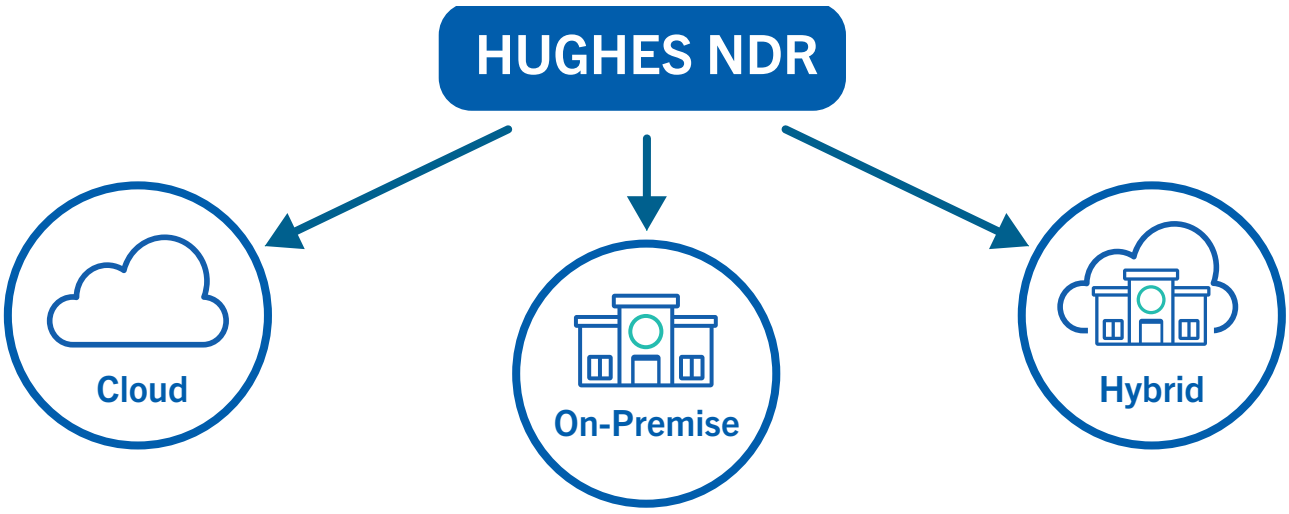
NDR applies AI and ML to detect any deviation from the baseline network traffic pattern and alert security teams of suspicious patterns and the potential threat to their network environment.

NDR is completely agnostic to the network size, scale and architecture, keeping all networks—whether legacy, public cloud, private cloud or hybrid—secured and optimized, while uncovering any vulnerabilities, blind spots or gaps. Some of the other benefits include autonomous discovery of major cloud assets and services, detection of network threats and anomalies/attacks down to the specific server, asset and service.

An intelligent NDR offers a virtual cyber analyst that provides human-like analysis, continuously monitoring networks and alerting security teams of malicious IPs, suspicious behaviors and unusual ports.

Security alerts with context-rich insights are automatically sent to security teams, giving them a full picture of network activity including a clear attack story, reports and extensive network-based querying. Organizations have the ability to observe active users on their network, their device interactions, network access locations and the type of data shared. This visibility empowers security teams to not just identify threats, but also pinpoint their origins, potential spread and which users have been compromised.

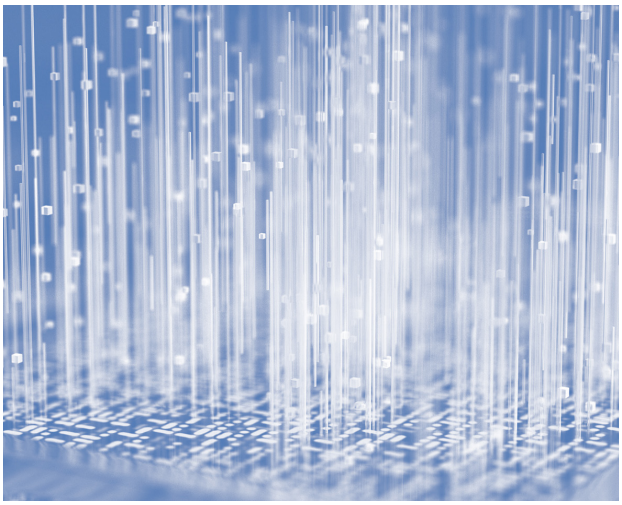
One of the most important benefits of NDR is its ability to monitor IoT devices, which are especially vulnerable in healthcare, retail, industrial and any industry that uses devices without screens or endpoints. With NDR, anything connected to the network can be monitored.



What happens when NDR finds a threat

When NDR discovers a threat, it immediately sends notifications to a Security Operations Center (SOC) and quarantines that area of the network to prevent the threat from spreading. For example, NDR can respond by updating firewall rules to block traffic from a suspicious IP address or device.

Notifications sent to security personnel at a SOC provide context-rich insights and recommendations, enabling them to take quick action depending on the severity of the event, before sensitive assets are reached.



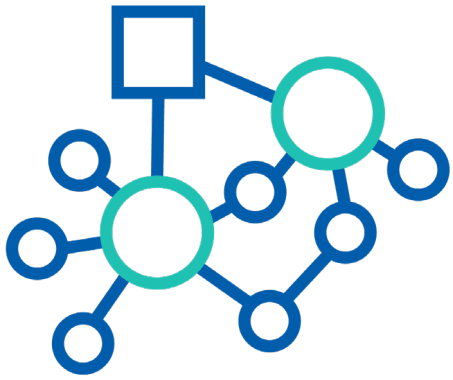
What to look for in Network Detection and Response solutions

Key capabilities to look for in a Network Detection and Response tool:

- Uses AI to infer 100% network visibility from a small sampling of network traffic to predict threats with minimal resource demand
- Is scalable, agnostic and generic to any network size or client architecture, providing full coverage with no gaps and without compromising any section of the network
- Provides security teams with granular, unhindered network visibility across legacy, cloud-native and hybrid environments
- Provides visibility to multiple cloud environments
- Works across all architecture types to create an integrated environment with total coverage to match any organization's needs
- Monitors IoT devices connected to the network
- Does not require installing an appliance or an agent to devices
- Is intuitive, easy-to-use, simple and fast to install
- Does not require costly hardware to deploy

Piecing it all together

Network Detection and Response is only one piece of the security puzzle. A layered approach to cybersecurity, with a variety of security controls that bolster and support each other when one of them fails, is crucial.



NDR can work together with Managed Detection and Response (MDR) or Endpoint Detection and Response (EDR), and they can act as a safety net for one another, catching anything that might have fallen through the cracks.

Other key security controls such as Multi-Factor Authentication (MFA), Zero Trust Architecture, well-maintained backups and a strong Incident Response Plan function both independently and collectively to prevent cybersecurity breaches.

Together, these solutions integrate data from multiple sources, providing a more comprehensive view of security across the entire organization. This helps to reduce the number of false positives and negatives, leading to faster and more accurate detection and response and enables security teams to detect and respond to threats that may have gone undetected using other methods.

Cybersecurity technologies and services

MDR is a service that provides a business with a team of experts who are part of a remote SOC, who use advanced tools to actively monitor the network. The team monitors cloud environments, network traffic and endpoints; identifies potential security threats; and takes action to mitigate those risks, with the goal of detecting and responding to threats swiftly, before they can cause harm.

A Managed Security Service Provider (MSSP) equipped with a 24/7 SOC can implement MDR service to small- and medium-sized businesses who may not be able to staff their own cyber professionals or who struggle to keep up with network monitoring activities.

- EDR is a core component of MDR that is focused specifically on endpoint devices. Endpoint devices on a network include all the servers, desktops, laptops, smartphones, cameras, scanners and other devices. EDR uses advanced analytics and ML to detect and respond to threats in real-time, providing in-depth visibility into endpoint activities and threats that may evade traditional antivirus solutions. EDR still requires manual intervention (typically from a SOC) to investigate and remediate threats.
- MFA is an identity verification method that requires users to provide at least one or two authentication factors in addition to a password to gain access to a website, application or network. Some examples of MFA include a verification code sent via SMS message, a one-time password sent via email, facial or voice recognition and answers to personal security questions.
- Zero Trust is a strategic approach to cybersecurity that assumes a network's security is always at risk and secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction. Under a Zero Trust model, users are consistently authorized and authenticated based on their identities and roles, plus other context such as time and date, historical usage patterns and device posture, regardless of their location or working environment.
- Well-maintained backups ensure that all data in an organization is protected, and the right data is backed up at the right time. An effective data backup plan is essential for businesses of any size or industry, in order to avoid data loss catastrophes, and guarantee ongoing business operations.
- An Incident Response Plan helps organizations effectively respond before, during and after a confirmed or suspected security incident with the appropriate actions. It is a formally approved written document outlining the procedures and tools a security team can use to identify, eliminate and recover from cybersecurity threats. A strong Incident Response Plan helps to minimize damage caused by threats, including data loss, abuse of resources and loss of customer trust.

Prioritize network detection now

While there are many different approaches to network security, every enterprise—regardless of size, shape, structure or industry—should implement proactive measures to stay ahead of cybersecurity challenges.

CISOs, CIOs and other technology leaders should prioritize Network Detection and Response as a complementary capability to other detection tools, focusing on low false positive rates and detection of anomalies that other tools do not cover.

As a global leader in Managed Network Services, Hughes has a wealth of deep expertise and a wide range of highly skilled professionals who can augment your existing IT and security staff by providing not only knowledge, but also valuable resources, capabilities and cutting-edge technologies to improve your security operations and enable your team to stay on top of emerging threats.

For more information on Hughes Network Detection and Response solutions, visit www.hughes.com/NDR.

HUGHES®
An EchoStar Company

www.hughes.com

11717 Exploration Lane
Germantown, MD 20876 USA