
Improving Enterprise Level Visibility Using NDR: Your Complete Guide to Network Security

There was an average major security breach in 95% of organizations in 2023, at an average price of \$4.45 million. In today's rapidly evolving threat landscape, complete visibility of the network is required for businesses. As enterprises increase their digital footprints, monitoring and securing complex network infrastructures become more and more important. With the emergence of sophisticated hackers and regular ransom attacks, organizations must implement the strongest [network security solutions](#).

Evolution of Network Security Visibility

Traditional vs. Modern Approaches

The modern network monitoring tools are not enough to counter sophisticated cyber-attacks. They often rely on simple metrics and lack the capability to detect subtle yet dangerous anomalies. Deep visibility in modern enterprises is powered by advanced [network traffic analysis](#) and real-time network insights.

This is where [NDR solutions](#) really shine, offering unprecedented visibility in network security. NDR leverages advanced technologies, such as machine learning enabling organizations to detect, respond to, and prevent threats with precision.

Enterprise-level network visibility covers all aspects of network activity, including east-west traffic, which happens between devices or between data centers and can include encrypted traffic where malicious activity is hidden, and cloud interactions. Organizations must look for abnormal access patterns, such as sudden spikes in data transfer between servers or erratic behavior at one endpoint, encrypted or in hybrid environments. Without this visibility, critical threats go undetected, and enterprises are left vulnerable to attacks.

Why Deep Visibility Matters

Network security visibility has become the cornerstone of modern cybersecurity strategies. Here's why:

Faster Threat Detection

NDR solutions allow for the detection of threats much faster than traditional security measures. This is because it minimizes the amount of time a threat can exist without being detected, thereby minimizing the damage caused.

Proactive Threat Hunting

[Proactive threat hunting](#) capabilities can help enterprises detect potential threats earlier, which

will keep them ahead of the curve when it comes to evolving security risks and minimize exposure.

Machine Learning-Powered Insights

Through machine learning-based anomaly detection, suspicious activity is identified in a timely manner to prevent it from becoming a significant security incident.

Breach Impact Reduction

An all-inclusive view of network activity enhances the detection of threats so that organizations can [respond quickly to breaches](#) and limit financial and reputational damage.

Understanding the Threat Landscape

The threats that modern enterprises face include:

Advanced Persistent Threats (APTs)

Advanced Persistent Threats, also known as APTs, are sophisticated threat actors who maintain long-term access to networks with the intent to steal sensitive data or disrupt operations. Detection and mitigation require a high level of visibility and continuous network monitoring. Studies have shown that APTs were responsible for 23% of major data breaches in 2023.

Ransomware

[Ransomware attacks](#) have increased in complexity from simple encryption schemes to data theft and extortion. Over the past year, there was a reported 300% surge in the kinds of ransomware network infrastructures reported by organizations. This requires organizations to build strong network monitoring capabilities and response.

Mobile Device Threats

With the new trend of remote work comes the increasing need for securing mobile devices. Studies show that 60% of breaches today originate from mobile devices, meaning that mobile security must be part of network visibility plans. Solutions that ensure usability must be embraced by enterprises in order to have these mobile devices provide visibility without compromising usability.

Key Components of Enterprise Network Visibility

Deep Packet Inspection and Analysis

Modern NDR-based solutions rely on DPI as a method to inspect data packets at a granular level. This allows teams to:

- **Detect anomalies in real time:** Identify unusual behaviors potentially indicating malicious activity.

-
- **Monitor multiple forms of networks in parallel:** Ensure visibility across on-premise, cloud, and hybrid networks.
 - **Identify data exfiltration:** [Detect and block unauthorized data transfers](#) before this causes damage.
 - **Anomaly detection in encrypted traffic:** Gain insights into encrypted data without compromising privacy.
 - **Profile normal network behavior:** Establish baselines to quickly identify deviations indicative of threats.

Cloud Network Monitoring

With 94% of enterprises using cloud services, a recent report claims that cloud network monitoring has become essential. NDR solutions provide:

- **Visibility into hybrid environments:** Monitor activity across on-premises and cloud platforms seamlessly.
- **Advanced threat detection:** Identify risks in cloud applications and services.
- **Real-time monitoring:** Analyze connections from mobile devices to cloud resources.
- **Comprehensive controls:** Implement unified security policies across diverse environments.
- **Microservices visibility:** Monitor containers and microservices effectively in dynamic cloud environments.

Incident Response Automation

Automation is revolutionizing incident response in enterprise security. Key benefits include:

- **Speeded Response Times:** Automated responses show a 62% reduction in meantime to respond (MTTR).
- **Proactive Threat Management:** Automated playbooks manage routine tasks and allow teams to be proactive in threat hunting.
- **Increased Accuracy:** Automation reduces human error, thus making the incident response more reliable.
- **Integration Capacity:** Integration with SOAR platforms streamlines response efforts on multiple tools and systems.
- **Better Threat Intelligence:** Real-time feeds improve the accuracy of threat detection and response.

Implementing Data Loss Prevention (DLP)

Data Loss Prevention (DLP) has become a cornerstone of network data security. Modern DLP solutions integrated with NDR platforms help organizations:

- **Identify and protect critical data:** Understand what data most at risk is and ensure its protection.
- **Prevent breaches:** Proactively block unauthorized data transfers.
- **Monitor sensitive data movement:** Gain insights into how and where data travels within the network.
- **Address phishing and ransomware threats:** [Prevent exfiltration](#) and extortion attempts.
- **Ensure compliance:** Meet regulatory requirements with confidence.

Recommended Reading

If you want to know about the best practices to prevent data breaches, then read our blog

[Read More](#)

The Importance of Actionable Network Visibility

Improving enterprise-level visibility is a necessity in today's threat landscape. Network Detection and Response offers:

Enhanced Security Posture

Comprehensive tools to defend against advanced threats.

Proactive Threat Management

The ability to address risks before they escalate.

Data Protection

Safeguarding sensitive information and critical assets.

If your Organization isn't Leveraging NDR, It's Time to Act.
Strengthen your security posture today to stay ahead of evolving threats.

[Talk to an expert](#)

The Role of Machine Learning in Achieving Enterprise Network Visibility

Machine learning is revolutionizing enterprise network visibility by providing powerful tools for predictive and proactive security measures. Here's an expanded look at its role:

Capabilities Description 1. Predictive Threat Detection

[Machine learning](#)

algorithms analyze historical data and recognize patterns that indicate potential threats, allowing organizations to act before issues escalate. 2. Behavioral Analysis ML models create baselines for normal network behavior, enabling real-time detection of deviations that might signal malicious activity. 3. Automated Anomaly Detection Machine learning simplifies anomaly detection, flagging issues that might be missed by manual monitoring and reducing false positives significantly. 4. Pattern Recognition ML tools excel at identifying complex patterns across massive datasets, helping detect even the most sophisticated threats. 5. Integration with

Incident Response Machine learning aids in automating incident response processes, reducing response times and freeing security teams to focus on higher-priority tasks.

Common Challenges and Solutions

Security Solution Integration

Challenges

- Managing diverse security controls.
- Monitoring multiple network types.
- Addressing complex threat actors and network segments.

Solution

Adopt unified NDR platforms that integrate seamlessly with existing tools, offering comprehensive visibility and streamlined workflows.

Scalability and Performance

Challenges

- Managing increasing network complexity.
- Maintaining performance as networks expand.

Solution

- Use distributed monitoring architectures.
- Leverage cloud-based security services.
- Deploy edge computing for localized data processing.
- Optimize traffic analysis to ensure speed and efficiency.

Future Trends in Network Visibility

As technology evolves, network visibility strategies must also transform. Here are the trends shaping its future:

• 1. Integration with Zero Trust Architecture

Zero Trust principles will be adopted in a wide approach to ensure that no one user or device is automatically trusted. This will naturally call for continuous monitoring as well as authentication, ensuring network security visibility.

• 2. Quantum-Resistant Encryption

Encryption methods must be based on the quantum computing scenario and should align with quantum-resistant decryption methods.

• 3. Extended Detection and Response (XDR)

[XDR solutions](#) that collect data from endpoints, networks, and servers are imperative to provide complete visibility along with streamlining the process of threat response.

• 4. 5G Network Security Needs

Ultrafast low-latency 5G networks will bring along new vulnerabilities and requires an advanced solution for protecting oneself against threats meant for such networks.

Frequently Ask Questions

How does NDR differ from traditional network monitoring?

NDR incorporates advanced features like machine learning, deep packet inspection, and automated threat responses, making it significantly more effective at detecting and mitigating sophisticated attacks.

What role does machine learning play in network visibility?

Machine learning enhances anomaly detection, predicts potential risks, and automates responses, ensuring comprehensive and proactive security.

How can enterprises measure the ROI of implementing NDR solutions?

ROI can be measured by reduced response times, fewer successful breaches, improved detection accuracy, and decreased manual security workload.