NDR - What it is, why it matters, and how to deploy it safely

Gridinsoft Help Center

What it is

Network Detection and Response (NDR) watches live network traffic to spot and investigate suspicious behavior in real time. Instead of relying on signatures, it analyzes patterns and anomalies to catch threats moving across your environment. For a deeper look, see our NDR explainer.

Why it matters

Attackers can slip past endpoints or use unmanaged devices. NDR sees what crosses the wire - lateral movement, data exfiltration, C2 beacons - so you can detect, contain, and respond even when malware hides.

How it works - quick tour

- Deep visibility: inspects north-south and east-west traffic on key taps or SPANs
- Behavior and ML: baselines normal activity and flags anomalies
- Threat intel correlation: matches domains, IPs, and protocols against feeds
- Response hooks: enriches alerts and can trigger blocks or quarantines

Where it fits

- Complements EDR/XDR on endpoints and SIEM for log correlation
- Covers IoT, OT, and shadow IT that you cannot install agents on
- Ideal for finding lateral movement and quiet data leaks

Quick setup tips

- Monitor core choke points and critical VLANs first
- Feed alerts to your SIEM and unify triage workflows
- Tune early noise - whitelist known services and back-ups
- Enable automatic enrichment and test block lists before auto-response
- Pair with deception assets to increase signal quality