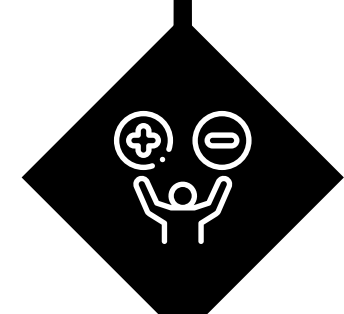


5 Signs It's Time to Upgrade Your NDR Solution

Don't let outdated network detection leave you exposed



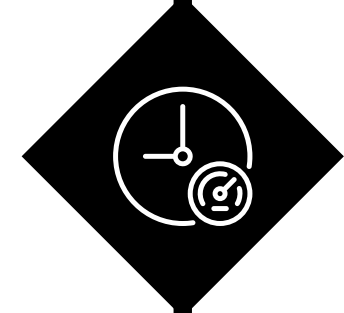
1. False Positive Overload

Your security team spends more time chasing ghosts than real threats. When alert fatigue sets in, you're not just wasting time, you're training your team to ignore warnings that matter.



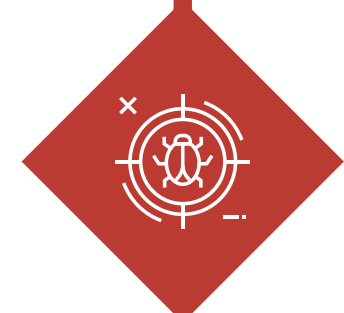
2. Blind Spots in Cloud & Hybrid

Your legacy NDR was built for yesterday's network. If you can't see what's happening in AWS, Azure or your hybrid infrastructure, you're flying blind where most attacks happen today.



3. Response Time Measured in Hours

When your current solution takes too long to detect threats, attackers have already moved laterally, exfiltrated data, and covered their tracks. Speed kills their plans, not yours.



4. No AI-Powered Threat Hunting

Manual threat hunting is like searching for a needle in a haystack, blindfolded. Without machine learning that actually learns your environment, you're missing sophisticated threats designed to blend in.



5. Limited Forensic Capabilities

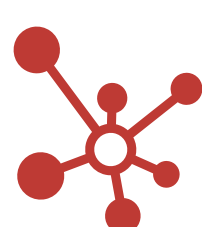
When a breach happens (not if), you need full packet capture and detailed forensics. If your current NDR can't reconstruct the complete attack timeline, compliance audits will be brutal.

Stop Playing Defense with Outdated Tools

NetWitness NDR delivers real-time visibility, AI-powered detection, and comprehensive forensics across your entire infrastructure. See why industry leaders trust us to stop threats others miss.

[Learn more about NetWitness NDR](#)

Powered by



NETWITNESS