

SERVICE OVERVIEW

Network Detection & Response

Network security monitoring is complex. Managing it shouldn't be.

Hackers are consistently changing their tactics to bypass network security. With 24x7 SOC monitoring, these threats are identified and blocked.

NuSecure Network Detection and Response (NDR) is a 24x7 SOC monitoring service that allows customers to immediately visualize, identify and protect against advanced network threats. With this NDR service, there's no need to spend money on a SIEM, hire more security specialists, integrate more security devices or make additional capital expenditures. The NDR service monitors traffic inside your local area network (LAN) 24x7, where it blocks known threats and quickly discovers new ones that have bypassed your security defenses. Newly discovered indicators of compromises (IOCs) are then sent to Nuspire's Security Operations Centers (SOCs) for remediation.

Additionally, NDR stores your data for 400 days, aiding our team of security experts in continually searching your network data for threats, restoring your network to a secure state, and preserving your data for forensic investigations.



THREAT DETECTION

- Demonstrates cybersecurity compliance
- Provides threat detection for threats that bypass preventive security controls such as traditional Firewall or AV technologies
- Features 24x7 SOC monitoring, analysis, and customer alerting of security events
- Incident triage performed by security analysts and researchers



SOC SERVICES

- Identify indicators of compromise (IOCs)
- Reverse engineer malware to understand what it does
- Create countermeasures for threats
- Consult on containment and remediation
- Provides explicit instructions and works with you to fully remediate threats