Product Brief

Clear NDR®

Uncover and respond autonomously to hidden threats and unauthorized activity lurking in your network

Clear NDR is an open and transparent Network Detection and Response that delivers:

- Clear Visibility - Monitor activities across your entire attack surface
- Clear Detection - Multi-layer, transparent detections you can understand
- Clear Evidence - Everything you need to quickly resolve the incident
- Clear Response - The confidence you need to automate your response

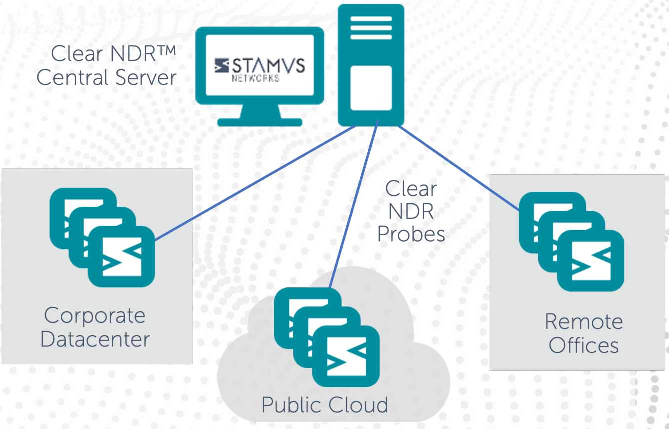
Clear NDR™ empowers defenders with the deep network insights needed to build a more efficient and secure AI-powered autonomous security operations center (SOC).

Clear NDR Probes

Clear NDR Probes inspect and analyze all network traffic to perform real-time threat detection, enrich the resulting events with extensive metadata, and capture network protocol transactions. The probe delivers all this data to the Clear NDR Central Server for additional analytics, processing and another layer of threat detection.

Clear NDR Central Server

Clear NDR Central Server provides the centralized management of the probes, third party threat intelligence and rulesets, consolidated event storage and a central integration point. It includes an additional layer of machine learning and algorithmic threat detection, along with automated event triage – enabled by tagging and classification. Finally, the Clear NDR Central Server provides a powerful threat hunting and incident investigation user interface an integrates seamlessly with the entire AI-powered security operations tech stack.



Clear NDR supports all combinations of physical, virtual, and cloud installations

Clear NDR is focused on solving five primary challenges facing security teams today:

- Detection of and response to attacks that evade other controls
- Lack of confidence in automated response
- Lack of visibility into the modern hybrid attack surface in AI-based security operations
- Missing explainable event context and evidence
- Alert fatigue

Unlike other solutions, Clear NDR uses a tapestry of transparent threat detection and response technologies – including AI, machine learning, advanced heuristics, signatures, and IoC matching – in a highly customizable system – supported by extensive metadata and evidence – that delivers detection you can trust with results you can explain.

Developed as an open core solution, it is available in two tiers: the open source “Community” edition and the flagship “Enterprise” edition

	Basic capabilities offered by Clear NDR® - *Community*	**Additional** capabilities in Clear NDR® - *Enterprise*
Primary Use Cases	• Single site IDS/IPS replacement • Single site open source NDR • Suricata education and threat research	• Multi-site hybrid enterprise attack surface (cloud, branch office, data center, etc) • Enabler of the AI-powered Autonomous SOC • Enterprise network detection and response • Regulatory or directive compliance
Best Fit Organizations	• Small organizations • Students • Threat researchers	• Medium-to-extra large Enterprises with a dedicated security operations team • Highly-targeted entities, including critical infrastructure • Managed security service providers (MSSP or MDR)
Detection mechanisms	• Signatures • IoC matching	• AI and Machine learning • Statistical algorithms • Other heuristics
Event types	• IDS Alerts • Network protocol transactions • Flow records	• Suspicious events – such as C2 beacons, host outliers, SMB insights • Sightings – host and user anomalies • Declarations of Compromise™ (DoC) – ultra high-confidence threat events • Declarations of Policy Violations™ (DoPV) – high-confidence events triggered by organization-specific policy violations • Rich source of structured network metadata - ideal for use in AI models for the autonomous SOC
Evidentiary artifacts	• Network protocol transactions • Flow records • Conditional PCAP • File extraction	• Incident timeline • Cyber kill chain mapping • Optional conditional logging • File extraction
Event workflow and triage	• Manual	• Users are presented high-fidelity threat incidents (DoC) and policy violation (DoPV) events, and incident investigation is aided by an attack timeline, detailed evidence collection and review, and reporting • Experienced users may tag events as “Informational” or “Relevant” and are automatically classified by the system for easy prioritization by less experienced users
Response Automations	• Not included • Can be built using API calls into the event data.	• Triggered based on high-fidelity detection events – DoC and DoPV • Simple notifications such as email or messaging • Sophisticated responses, including policy changes, quarantine actions, or playbook initiations in third party systems such as XDR, EDR, SOAR, IR, or Firewall systems
Other Integrations	• Third party threat intelligence and rulesets • API-based query and control • User interface contextual deep linking into other systems • Model context protocol (MCP) with basic endpoints	• Pre-built integrations into various third-party systems to support the response automations described above • These include XDR, EDR, SOAR, IR, Firewall, DDI, and more • Straightforward integrations into other systems via API, Webhook, custom deep-linking, and email • Model context protocol (MCP) endpoints provide access to advanced network intelligence for DoC, DoPV, Host Insights, and more
Host attributes	• May be collected via periodic queries into database and correlated using third party analytics	• Hosts are auto-classified into device types (roles), such as domain controllers, printers, proxy servers, etc • Host Insights – collects and maintains 60+ attributes for every host seen on the network (up to millions) • Attack surface inventory - identifies all hosts seen communicating on the network
Organizational context	• Usernames are extracted and presented	• Associates host names, usernames, and organization-specific network names for rapid assessment and identification during triage and incident response
Support	• Support is through the open-source user community • Issues and feature requests reported via GitHub	• Enterprise-class onboarding, training, and technical support • Dedicated customer success manager • Quarterly business reviews • Issues and feature requests logged and tracked though ticketing system

ABOUT STAMUS NETWORKS

Stamus Networks believes that cyber defense is bigger than any single person, platform, company, or technology. That’s why we leverage the power of community to deliver the next generation of open and transparent network defense. Trusted by security teams at the world’s most targeted organizations, our flagship offering – Clear NDR® – empowers cyber defenders to uncover and stop serious threats and unauthorized network activity before they harm their organizations. Clear NDR helps defenders see more clearly and act more confidently through detection they can trust with results they can explain.

STAMVS NETWORKS

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

✉ contact@stamus-networks.com
www.stamus-networks.com