Solution Brief

STAMUS NETWORKS

The Transparent Advantage: Why Clear NDR Ends the "Trust the Algorithm" Trade-off

Most NDR systems force security teams to "trust the algorithm." Whether your organization is outgrowing legacy tools or evaluating its first platform, Clear NDR is the most accurate and transparent network detection and response system available. It delivers precision threat declarations with complete evidence and explainability, enabling your SOC to automate response with confidence, satisfy auditors with proof, and maintain total data sovereignty.

Unlike black-box anomaly-based systems that force SOC teams to "trust the algorithm" or legacy tools drowning them in false positives, Clear NDR combines the transparency of open-source Suricata with sophisticated multi-layered detection. The result is a platform that delivers both certainty and accuracy. Security teams get detections they can understand, evidence they can trust, and the confidence to respond automatically—all while maintaining complete control over their security data.

The Clarity Your SOC Has Been Missing

- **Precision Threat Declarations:** Move beyond alert noise with multi-layered detection (signatures, ML, heuristics, and behavioral analysis) that delivers precision findings—not just "interesting" anomalies.
- **Complete Explainability:** Eliminate the "black box" with full visibility into detection logic and algorithms. Your team deserves to understand the "why" behind every alert to respond with total confidence.
- **Forensic Evidence Packages:** Every detection is bundled with the underlying protocol metadata and PCAP evidence required for immediate verification, forensic investigation, and audit proof.

- **Total Data Sovereignty & Compliance:** Maintain absolute control with a platform built for air-gapped and on-premises environments. Our architecture ensures sensitive telemetry stays within your jurisdiction, helping you seamlessly satisfy DORA, NIS2, and GDPR requirements.
- **Intelligence for the AI-Powered SOC:** Empower your AI strategy with rich, structured network context. Using the Model Context Protocol (MCP), you can query network intelligence via your choice of LLM - even local models - for autonomous hunting and natural language triage.
- **Economic Efficiency:** Stop paying the "host tax," and stop paying for log storage you don't need. Our flat-rate licensing with unlimited host coverage provides the economic predictability legacy NDR vendors can't match. And with optional conditional logging and conditional PCAP capabilities, you only retain the evidence you need.

What Precision Detection Looks Like

Decision Factor	Clear NDR®	Typical Black Box Anomaly-Based NDR
Alert Confidence	Actionable declarations you can trust. Each Declaration of Compromise signals a verified, high-risk threat, not a statistical guess, enabling immediate response.	Probability scores (60-90% confidence) that still require analyst judgment and validation.
Detection Transparency	Understand why an alert exists. Analysts can review detection logic and algorithms, enabling confident decisions and repeatable processes.	"Anomaly detected" with no visibility into how or why it was flagged.
Data Sovereignty	Deploy anywhere without losing capability. On-prem, private cloud, public cloud, or fully air-gapped — with full detection fidelity intact.	SaaS-dependent architectures limit capability in restricted or regulated environments.
AI-powered SOC	AI that operates on facts, not guesses. Clear NDR provides structured, evidence-rich network context via direct integration to AI SIEM and via MCP for reliable automation and autonomous hunting.	AI decisions are based on opaque scores and limited contextual data.
Evidence Package	Immediate proof, no swivel-chair investigation. Every declaration includes logs, flows, session data, extensive Host Insights™, and PCAP for instant validation and response.	High-level anomaly summaries require analysts to gather evidence across tools.

Decision Factor	Clear NDR®	Typical Black Box Anomaly-Based NDR
Daily Analyst Workflow	Focus on real threats, not noise. Analysts investigate a small number of high-confidence incidents and spend the rest of their time hunting and improving defenses.	Analysts spend their day triaging dozens or hundreds of alerts to find a few real issues.
Background Events	Signal without distraction. Thousands of detection events are preserved as evidence but only surfaced when they support a confirmed threat.	All anomalies are surfaced as alerts, regardless of severity or relevance.
False Positive Rate	Minimal rework and alert fatigue. Declarations of Compromise consistently maintain a false positive rate below 1%. 15–40% false positives create investigation churn and erode trust.	15–40% false positives create investigation churn and erode trust.
Threat Hunting	Start from certainty, not suspicion. Guided hunting workflows let teams pivot quickly through precision historical data without re-triaging alerts	Limited context forces teams to revisit old alerts or reconstruct incomplete timelines.
Forensic Investigation	Faster root cause analysis. Complete timelines expose attacker movement and patient zero without manual correlation.	Investigations rely on stitching together logs from multiple platforms.
Agent-less Coverage	Full visibility where agents can't run. Infrastructure, IoT, OT, and unmanaged systems are continuously monitored with the same precision approach.	Coverage gaps or additional products required for non-endpoint assets.
Pricing Model	Predictable economics at scale. Line-rate pricing eliminates host-based penalties and surprise renewals.	Host-based pricing punishes growth and introduces cost volatility.

Precision Doesn't Matter If You're Blind to 40-60% of Your Infrastructure

The Problem: Your EDR/XDR stack provides excellent endpoint visibility. But attackers know they can move laterally through network infrastructure, exploit IoT devices, and pivot through OT systems completely undetected by agent-based tools.

The Solution: Clear NDR fills this gap with the same precision approach: high-confidence declarations of compromise when infrastructure is attacked, with thousands of detection events preserved as evidence—not presented as daily alerts.

Transparency Isn't a Feature – It's What Enables Confident Automation

Most NDR platforms talk about automation, but automation without transparency forces SOC teams into an impossible tradeoff: move fast and risk false positives, or slow down and manually validate every alert.

Clear NDR removes that tradeoff.

Because every detection is explainable, evidence-backed, and reproducible, transparency becomes an operational advantage, not a technical detail. Analysts don't just see that something was flagged; they understand why, can validate it immediately, and can defend the decision to stakeholders, auditors, and regulators.

This is what allows SOC teams to automate with confidence. Playbooks can trigger without hesitation. AI agents can assist in Tier-2 and Tier-3 workflows without introducing blind risk. And teams can train analysts on real attacker behavior instead of vendor-defined abstractions.

In practice, transparency enables:

- Confident automated response without second-guessing alerts
- Faster incident validation using built-in evidence, not external tools
- Audit-ready detections that clearly document how and why threats were identified
- Safer AI-driven hunting, grounded in structured, trustworthy network intelligence

Transparency isn't about exposing algorithms for curiosity's sake. It's about knowing exactly when you can trust a detection and act on it.

Clear NDR: The Strategic Choice

Every SOC team reaches an inflection point. Legacy tools create blind spots. Black-box platforms create doubt. Homegrown solutions strain teams as environments scale.

Clear NDR meets teams where they are and gives them a path forward without forcing tradeoffs between confidence, coverage, and control.

If you are currently using...	The Clear NDR® Advantage
Legacy IDS/IPS	Advance to behavioral and multi-layered detection without sacrificing the deterministic, evidence-based certainty your team depends on.
"Black Box" AI NDR	Replace opaque probability scores with evidence-backed Declarations of Compromise your SOC can trust, validate, and automate against.
Homegrown Suricata	Preserve your expertise while eliminating alert overload and maintenance fatigue with an enterprise-grade platform that scales your knowledge, not your workload.

Intelligence for the AI-Powered SOC

AI doesn't fail in the SOC because models aren't powerful enough, it fails because the data feeding them is incomplete, opaque, or untrusted. Clear NDR changes that.

By preserving and structuring high-confidence network intelligence, Clear NDR provides the foundation AI systems need to operate safely and effectively. Using the Model Context Protocol (MCP), Clear NDR can supply your choice of LLM — including local, air-gapped models — with evidence-rich context grounded in real network behavior.

The result is AI that works the way security teams expect it to:

- Ask natural-language questions like "Show me lateral movement in the finance subnet"
- Automate complex hunting and triage tasks without blind trust
- Generate explainable findings backed by packet-level evidence
- Maintain complete data sovereignty, even in restricted environments

This isn't AI layered on top of alerts, it's AI operating on transparent, verifiable intelligence, the kind SOC teams can trust.

Clarity Enables Action

Modern SOCs don't suffer from a lack of alerts, they suffer from a lack of clarity. When detections can't be explained, validated, or defended, teams slow down, automation stalls, and risk quietly accumulates. Clear NDR was built to change that dynamic.

By delivering high-confidence Declarations of Compromise and Declarations of Policy Violations backed by complete evidence and total transparency, Clear NDR gives security teams something rare: the ability to move faster without increasing risk. Analysts can trust what they see, automation can operate safely, and AI can assist without guesswork.

This is what precision detection looks like and why Clear NDR is becoming the foundation for modern, confident security operations.

Ready to Transform Your SOC?

Ready to see how Clear NDR can **transform your SOC operations**? Stop trusting the algorithm and start automating with confidence. Request a **personalized demonstration today** to see Clear NDR's precision detection and complete evidence in action, or dive in immediately with a **30-day no-obligation evaluation** to experience the clarity your security team has been missing.

Contact Stamus Networks for a consultation and live demonstration to determine if Clear NDR is a good fit for your organization: contact@stamus-networks.com

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.

STAMUS NETWORKS

229 rue Saint-Honoré
75001 Paris
France

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

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

