Comparing Clear NDR® Community to Clear NDR® Enterprise

By Éric Leblond, Peter Manev

White Paper

WP-COMMUNITY-ENTERPRISE-092025-1

STAMUS® NETWORKS

Many Clear NDR® Community (formerly SELKS) users are pleased with its capabilities. If you are one of those users, you may be wondering if there is any value in upgrading to the Clear NDR Enterprise, the commercial product offering from Stamus® Networks. In this white paper we will explain the differences among the systems and help the reader make an informed decision.

BACKGROUND

Before we explore the distinctions between these two solutions, we first need to establish some baseline understandings.

Developed as an open core solution, it is available in two tiers: the open source "Community" edition (formerly SELKS) and the flagship "Enterprise" edition (formerly Stamus Security Platform).

Clear NDR Community

Developed by Stamus Networks, Clear NDR Community is a turnkey Suricata-based IDS/IPS/NSM ecosystem with its own graphic rule manager and basic network threat hunting capabilities. Clear NDR Community is a Linux-based live distribution built from 6 key open-source components – Suricata, Fluentd, OpenSearch, Evebox, Arkime, and Scirius (the Suricata Management and Suricata Hunting user interface from Stamus Networks).

Clear NDR Community is a contribution made by Stamus Networks to the open-source community. It is freely available and is released under the GNU GPLv3 license.

The source files, README, issues tracker and wiki may be found on GitHub: https://github.com/StamusNetworks/Clear NDR Community

Information on each individual component may be found at the sites listed to the right:

- **Suricata IDPS** - http://suricata-ids.org/
- **Scirius** -https://github.com/StamusNetworks/scirius
- **OpenSearch**- https://opensearch.org/
- **Fluentd**- https://www.fluentd.org/
- **EveBox** - https://evebox.org/
- **Arkime** - https://arkime.com/

CLEAR NDR ENTERPRISE

The Clear NDR Enterprise is a commercial enterprise-scale solution developed and supported by Stamus Networks. Clear NDR Enterprise is an advanced network detection and response system that exposes serious and imminent threats to critical assets and empower rapid response.

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).

To learn more about Clear NDR Enterprise, visit the Stamus Networks website here: https://www.stamus-networks.com/

KEY DISTINCTIONS

While Clear NDR Enterprise is built using many of the same components as Clear NDR Community, it is in fact, much more complete and enterprise class systems. There are seven major dimensions to consider when comparing Clear NDR Community to Clear NDR Enterprise:

- Enterprise Scale and Integration
- Organization-Specific Context
- Threat Detection and Hunting
- Network Security Monitoring
- Event Noise Reduction
- Total Cost of Ownership
- Enterprise Support

This paper looks more closely at each of these.

ENTERPRISE SCALE AND INTEGRATION

Scale is one of the most obvious differences between the Clear NDR Community and Clear NDR Enterprise. In the simplest terms, Clear NDR Community includes only a single instance of Suricata and is only capable of managing one sensor. In Clear NDR Community, the Suricata rules management and threat hunting interface are directly coupled with the sensor.

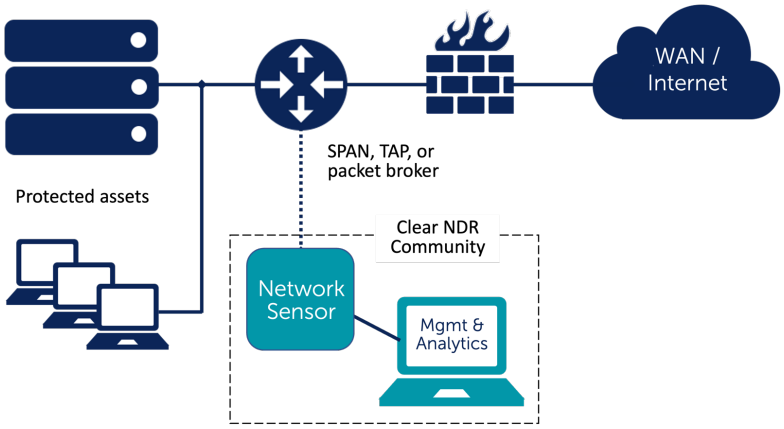


Figure 1. Clear NDR Community - a single instance of Suricata with the management system integrated into the sensor.

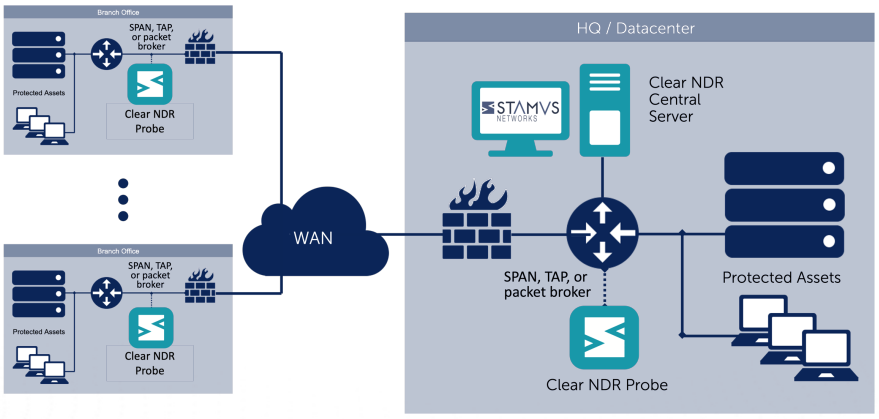


Figure 2. Clear NDR Enterprise – independent probe management and threat hunting systems may access multiple probes in multiple branch offices or network segments.

With Clear NDR Enterprise, the management and threat hunting systems are independent of the sensors, providing the operator with a consolidated management and threat hunting view into the event data from many Suricata sensors or Stamus Network Probes from a single pane of glass.

In addition, Clear NDR Enterprise supports multiple tenants, allowing each probe or sensor to have its own organizational context applied to its alerts and hierarchical management layers. This multi-tenancy capability allows you to oversee probes deployed in multiple networks and multiple organizations from a single threat hunting and management console.

While Clear NDR Community may be installed on a range of hardware options, including virtual machines, installing, tuning, and optimizing your implementation will require some trial and error. Alternatively, with Clear NDR Enterprise, you have the option to purchase the software integrated on one of the optimized Stamus Network Appliances, which are tested and rated for a given performance level – for example, up to 100 Gbps in a single probe.

Here are several key scalability and integration features available in Clear NDR Enterprise, but not in Clear NDR Community:

Clear NDR Enterprise feature not available with Clear NDR Community	Impact
Management of multiple sensors/probes	Allows you to deploy probes/sensors in multiple network segments and locations, giving you greater visibility into your organization's threat posture from a single pane of glass.
Aggregated event data from multiple sensors/probes	Gives you a centralized view of the security posture for your entire network.
Integration with Splunk, XSOAR, SentinelOne SIEM, Crowdstrike Falcon	If you already use a SIEM for centralized log management, you'll want to include the enriched event data from Clear NDR
Multiple organization-specific network definitions	Allows you to define different contextual environments for different networks or organizational subsets.
Multi-tenant operation	Manage multiple distinct organizations from a single pane of glass.
Available on tested, verified and high-performance turnkey appliance	You can deploy with confidence, knowing that your system will not drop packets or miss events due to performance issues.
Online or offline (Air-gapped) software maintenance	Simple installation of software updates does not require an Internet connection.
Integration with LDAP and Active Directory	You can stay compliant with your security policies by integrating Clear NDR into your existing access control systems.
Backup and restoration of configurations	Ensures you can quickly restore your security monitoring functions in the event of a disaster.

ORGANIZATION-SPECIFIC CONTEXT

When viewed through the Clear NDR Community user interface (UI), your organization's network segments, and devices – such as endpoints and hosts – are displayed simply as IP addresses. If you manage a large network, you will likely need to switch to a different system to look up the IP address in order to associate it with your network asset. This takes time and can disrupt your concentration during an intense threat hunting session.

With Clear NDR Enterprise, the event and log data is enriched - in real-time - with context that is unique to your organization. You can easily import your organization's network definitions, so those network names will appear alongside the IP addresses.

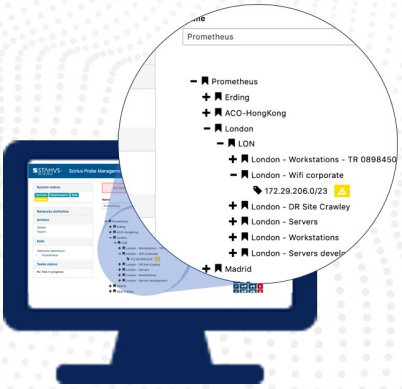


Figure 3. Clear NDR Enterprise network definition screen allows user to apply organizational context to the system.

In addition, Clear NDR Enterprise queries your internal domain name server to associate fully-qualified internal domain names (FQDNs) with those IP addresses, bringing even more organizational context to events and investigations without having to leave the tool. Armed with this context you can use those familiar names to develop filters and hunting strategies, allowing you to quickly assess the target or source or host associated with suspicious activity on the network.

Here is a summary view of the organizational-specific context features available in Clear NDR Enterprise but not in Clear NDR Community:

Clear NDR Enterprise feature not available with Clear NDR Community	Impact
Internal IP addresses are identified with internal network names	Easily recognize your organization's assets and networks while threat hunting and incident investigation. Filter on events based on this organizational context. Aids in rapid detection of lateral threats and policy violations.
Internal hosts are identified as fully qualified domain names (FQDN)	
Custom organization-specific threat detection rules	Define custom threat detection rules using the language of your organization's network and assets.

THREAT DETECTION AND HUNTING

The cornerstone of a security practice is effective threat detection and the ability to quickly assess the risk and severity of the indicators of compromise that your systems detect.

Because it includes a Suricata engine, Clear NDR Community is capable of using some of the most sophisticated threat intelligence on the market, including signatures/rules from commercial feeds such as Proofpoint ETPro and others and indicator of compromise (IoC) threat intelligence feeds. This provides Clear NDR Community users with excellent foundation of network-based threat detection, albeit on a single network segment.

In addition, Clear NDR Community includes basic cyber threat hunting capabilities, giving you the opportunity to begin a threat hunting session based on, for example, signatures that triggered events, IP addresses and domains.

However, Clear NDR Enterprise delivers significantly more capability for detection, metadata collection and management, and threat hunting.

Clear NDR Enterprise delivers next-generation threat detection capabilities that go beyond traditional signature-based approaches. This advanced edition combines artificial intelligence, machine learning, and behavioral analytics to detect sophisticated, unknown threats while providing high-confidence automated threat determinations. It's engineered for organizations facing advanced persistent threats and those seeking to implement autonomous security operations with minimal analyst intervention.

Detection Approach: Multi-layered intelligent detection combining traditional and modern techniques

- AI and Machine Learning: Behavioral analysis that learns normal network patterns and identifies deviations that may indicate threats
- Statistical Algorithms: Mathematical models that detect anomalies in network traffic patterns and user behaviors
- Other Heuristics: Rule-based logic that identifies suspicious activities based on threat intelligence and behavioral indicators

Event Detection Coverage: Comprehensive threat landscape visibility

- Suspicious Events: Advanced threat indicators like Command & Control (C2) beacon detection for persistent threats
- Sightings: Behavioral anomalies at both host and user levels that may indicate compromise or insider threats
- Declarations of Compromise® (DoC): High-confidence automated alerts that definitively identify active threats with minimal false positives
- Declarations of Policy Violations® (DoPV): Organization-specific policy enforcement with automated detection of compliance violations
- Rich Structured Network Metadata: Detailed network intelligence optimized for AI-driven analysis in autonomous Security Operations Centers

Key Differences

Community focuses on detecting known threats using established signatures and indicators, making it effective against previously identified attacks.

Enterprise adds unknown threat detection capabilities through behavioral analysis and machine learning, enabling it to identify novel attacks, insider threats, and sophisticated adversaries that evade signature-based detection. The Enterprise version also provides higher-confidence alerts and supports automated SOC operations through its AI-optimized metadata.

Clear NDR Enterprise enriches the detection with context derived through both network traffic analysis and organization-specific network information. In addition, Clear NDR Enterprise offers you the ability to create your own custom detection policies built around your organization's unique needs. These important features give you the ability to not only detect north-south intrusions, but also lateral threat movement and policy violations, such as disabled virus detection and unauthorized SSL certificate or proxy deployments.

And your ability to proactively hunt for threats is significantly improved with Clear NDR Enterprise compared to Clear NDR Community. This is due to its extensive data enrichment, classification-assisted workflow, advanced search and filtering capabilities, and mapping indicators of compromise to the stages along the cyber kill chain. These features allow you to quickly assess your threat posture from a number of angles and begin your threat hunting from the appropriate starting point.

Here is a summary view of the threat detection and hunting features available in Clear NDR Enterprise but not in Clear NDR Community:

Clear NDR Enterprise feature not available with Clear NDR Community	Impact
Over 40+ additional metadata fields derived from network traffic analysis and organizational context are used to enrich the alert data in real-time.	The improved detection and more-effective threat hunting saves you time and reduces your exposure.
Turnkey integration and automation of ETPro threat intelligence ruleset	Arms you with the industry's most effective commercial threat intelligence that is automatically updated as new rules become available (typically 10-50+ each day)
Detection of lateral threat movement, security policy violations, use of homoglyphs in phishing attacks	More complete coverage of various methods of attack and various stages of the cyber kill chain.
Advanced detection algorithms mapped to cyber kill chain	You can quickly assess the criticality of a given alert and begin your investigation by focusing on indicators that matter most.
Advanced filtering based on Boolean combinations of events and metadata	Allows you to rapidly pivot your investigation as you uncover additional insights. You may save commonly-used filters and/or take advantage of 30+ predefined filters developed by the Stamus Networks threat intelligence team.
Classification-assisted workflow	By tagging events that match a given filter criteria, you are able to suppress informational alerts and identify others as relevant and worthy of further inspection. This lets you focus on what matters most, saving you time and allowing for less skilled team members to make more effective contributions.

NETWORK SECURITY MONITORING

Both threat detection and proactive threat hunting benefit from the visibility and context provided by network security monitoring (NSM), also known as network traffic analysis. Without details such as usernames, user agents, network segments, network flow data and fully qualified domain names, many threats will go undetected and even your most sophisticated analyst will have difficulty separating important indicators of compromise from simple informational alerts.

While a Clear NDR Community system will collect some of this raw data for a single network sensor, you will need to also deploy a standalone network traffic analysis solution if you hope to gain visibility into that host-oriented data. In addition, you will need to feed logs from both systems into a SIEM or SOAR in order to correlate the context with the alerts.

With Clear NDR Enterprise, all the NSM metadata context is correlated -- in real time -- with events and is available to you in a single web interface (and via API) for all of your network probes/sensors. And you may create filters that incorporate many of the metadata fields to investigate, for example, all alerts associated with a given hostname and attack target type. Deploying Clear NDR Enterprise eliminates your need to run a separate NSM, reducing your costs and your management overhead.

Here are several examples of the network traffic analysis features available in Clear NDR Enterprise, but not in Clear NDR Community:

Clear NDR Enterprise feature not available with Clear NDR Community	Impact
Protocol-independent hostname Split (FQDN, TLD, domain, subdomain)	Form of event data enrichment facilitates easier and more flexible thread detection by allowing for use of advanced Boolean combinations and criteria, ultimately saving time and expense during hunt and detection
Host Insights™ using user agents, services, host name, TLS agents and username	Cyber situational perspective provides invaluable fingerprinting of end points for not only data threat detection but also compliance and anomaly profiling.
Geolocation, AS number, AS Organization information for IP	Saves your team time and cost during hunt and incident investigation
Metadata integration with SIEM, SOAR, and data lakes	Streamlines reduces the volume of transactions and expense associated with hunting and investigation.

For a complete list of NSM-based metadata attributes, please contact Stamus Networks.

THREAT DETECTION AND EVENT NOISE REDUCTION

NDR solutions have evolved significantly to address two critical challenges in modern cybersecurity: comprehensive threat detection and event noise management. While traditional signature-based detection remains effective against known threats, today's sophisticated adversaries increasingly rely on zero-day exploits, living-off-the-land techniques, and advanced persistent threat (APT) methodologies that can evade conventional security measures.

Simultaneously, security teams face overwhelming alert volumes that lead to analyst fatigue and missed critical incidents.

The Community edition provides essential network security monitoring through proven detection methods, while the Enterprise edition leverages artificial intelligence and behavioral analytics to identify unknown threats while dramatically reducing noise through high-confidence automated determinations.

Clear NDR Community - Basic Detection with Standard Alerting

Clear NDR Community provides foundational network security monitoring through proven, traditional detection methods. This edition focuses on identifying known threats using established threat intelligence and signature-based detection techniques, generating standard security alerts that require analyst review and investigation. It's designed for organizations seeking reliable baseline security coverage with straightforward deployment and maintenance requirements.

Threat Detection Capabilities: Traditional signature-based detection

- Signatures: Relies on known attack patterns and predefined rules to identify established threats
- IoC (Indicators of Compromise) Matching: Identifies threats based on previously cataloged malicious artifacts like IP addresses, domain names, file hashes, and URLs

Event Types and Noise Management: Standard alerting approach requiring manual analysis

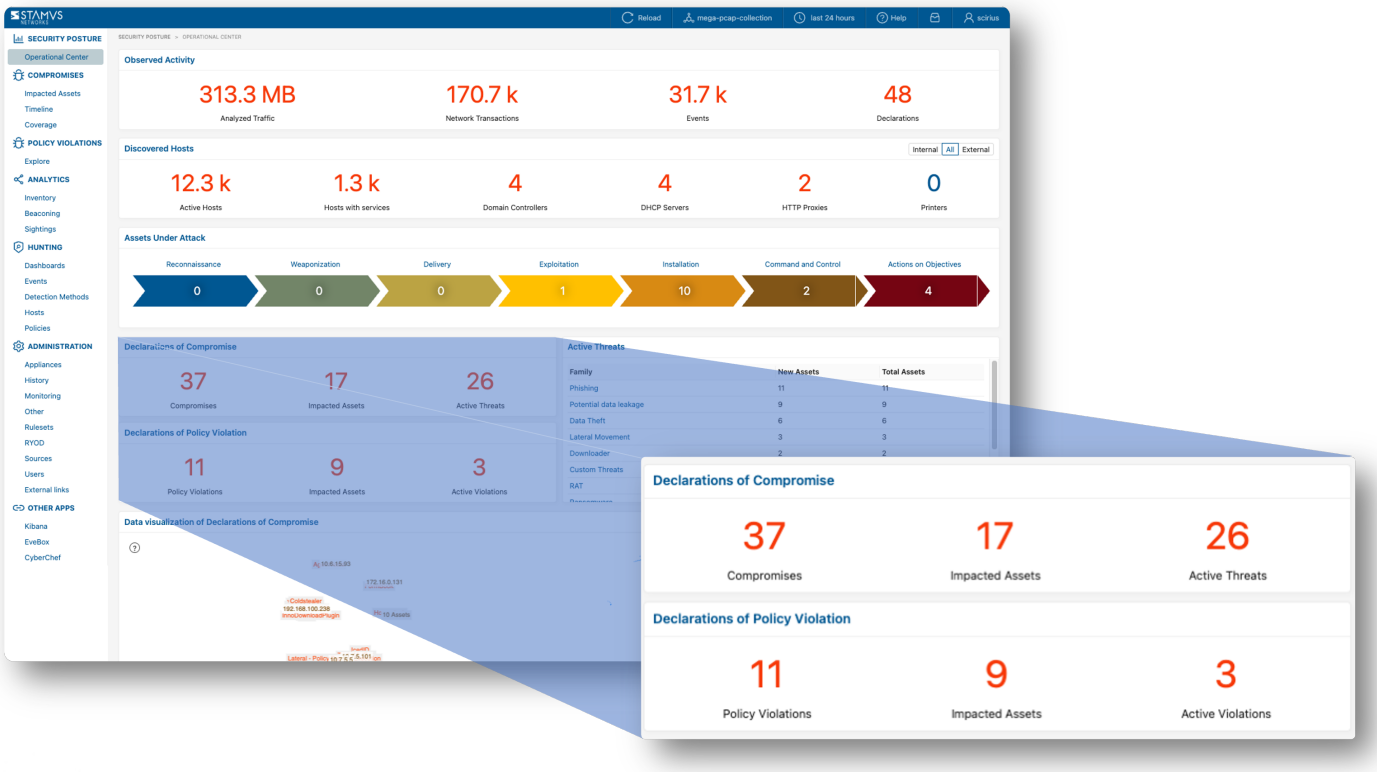
- IDS Alerts: Standard intrusion detection system notifications for known threats that require analyst investigation to determine legitimacy
- Network Protocol Transactions: Monitors and logs network communications across various protocols, generating events for suspicious activities
- Flow Records: Captures high-level network traffic metadata (source, destination, ports, protocols) with basic anomaly detection

Clear NDR Enterprise - Advanced Detection & Intelligent Noise Reduction

Clear NDR Enterprise delivers next-generation threat detection that go beyond traditional signature-based approaches while dramatically reducing alert fatigue through intelligent event classification and automated threat determinations. This advanced edition combines artificial intelligence, machine learning, and behavioral analytics to detect sophisticated, unknown threats while providing high-confidence automated decisions that minimize analyst workload.

Clear NDR Enterprise feature not available with Clear NDR Community	Impact
AI and Machine Learning	Behavioral analysis that learns normal network patterns and identifies deviations indicating both known and unknown threats
Statistical Algorithms	Mathematical models that detect subtle anomalies in network traffic patterns and user behaviors that signature-based systems miss
Other Heuristics	Advanced rule-based logic that identifies complex attack patterns and suspicious activities based on threat intelligence and behavioral indicators
Suspicious Events	Advanced threat indicators like Command & Control (C2) beacon detection and lateral movement patterns, classified by confidence level to prioritize analyst attention
Sightings	Behavioral anomalies at both host and user levels that may indicate compromise or insider threats, correlated across multiple data sources to reduce false positives
Declarations of Compromise®	Ultra-high-confidence automated events that definitively identify active incidents with statistical confidence levels exceeding 95%, eliminating the need for initial analyst investigation and enabling immediate response actions
Declarations of Policy Violations®	High-confidence automated detection of organization-specific policy violations and compliance failures, providing definitive determinations rather than requiring manual policy interpretation
Rich Structured Network Metadata	Detailed network intelligence optimized for AI-driven analysis that enables correlation and context-aware alerting, dramatically reducing event noise through intelligent aggregation and prioritization

Enterprise adds comprehensive unknown threat detection capabilities through behavioral analysis and machine learning while implementing intelligent noise reduction through automated high-confidence determinations. The Declarations of Compromise® and Declarations of Policy Violations® features provide definitive threat and policy violation determinations, enabling security teams to focus on confirmed incidents rather than investigating numerous uncertain alerts.



TOTAL COST OF OWNERSHIP

As we mentioned earlier, Clear NDR Community is freely available and is released under the GNU GPLv3 license. Free, open-source software can be a cost-effective alternative at the beginning of a new installation. But in order to understand the true costs of a project, it is important to factor in both the direct and the indirect costs associated with owning and operating the solution.

Here are several items to evaluate when evaluating the cost of an open source Clear NDR Community solution versus the commercial Clear NDR Enterprise platforms:

Upfront licensing fees for the software – obviously, Clear NDR Community has the edge here. Afterall, it's free.

Installation and onboarding - while Clear NDR Community is a turnkey ISO image or container instance intended to install quickly and easily on a bare metal server, installing, tuning, and optimizing your implementation will require some time and expertise - both of which have real costs for your organization. As a Stamus Networks customer of Clear NDR Enterprise, you will enjoy complimentary support during the installation and onboarding process. And the burden of the expertise falls on the Stamus Networks support team.

Technical support and maintenance - As a Clear NDR Community user, you are ultimately responsible for supporting your organization's technical needs with respect to the Clear NDR Community installation. Yes, there are numerous online resources and a very active community, nurtured in large part by the Stamus staff, available to assist you in your efforts. As a Stamus Networks customer of Clear NDR Enterprise, you will enjoy complimentary technical support, patches and feature enhancements throughout the term of your license. Once again, the burden of the expertise falls on the Stamus Networks support team.

Filling in the missing capability gaps - since Clear NDR Community is not as full-featured as the commercial Clear NDR Enterprise alternatives, you may wish to augment Clear NDR Community capabilities with standalone network traffic analysis (NTA) and SIEM or SOAR system to fill the gaps. Even if you obtain open-source versions of these functions, there are significant indirect costs associated with integration, maintenance, and support that you must consider. Clear NDR Enterprise not only fills capability gaps, but it eliminates the need for time-consuming integrations while reducing the operating expense of SIEM and SOAR deployments.

ENTERPRISE SUPPORT

Most enterprises want their staff focused on leveraging the capabilities of a best-in-class solution rather than spending their valuable time to build and support one.

As an open source solution, Clear NDR Community asks that you assume most of the responsibility for installing, troubleshooting, maintaining and supporting the system in your environment. For those who are equipped and funded to do so, this can be quite rewarding. For others, it can cause a substantial distraction from their primary task of protecting the organization's network.

With Clear NDR Enterprise , you get the full support of Stamus Networks throughout the lifecycle of your deployment. Beginning with system onboarding and throughout the lifetime. This includes tuning and enablement, training, troubleshooting, new feature upgrades, patches and threat intelligence updates. Each Stamus Networks customer is given access to a dedicated channel on our online support system and access to a team of technicians.

Here is a summary view of the support available with Clear NDR Enterprise but not in Clear NDR Community:

Clear NDR Enterprise Support Not Available with Clear NDR Community	Impact
Onboarding	Reduces the time to impact. You will be up and productive within a few days with your organizational specific context in place.
Technical support	When you have questions, Stamus Networks technical experts are available to help.
Ongoing software maintenance	You'll know you have access to the most current version and the latest available features.

For more information on the enterprise support, please request a copy of the Stamus Networks support agreement.

SUMMARY

The table on the following page summarizes the similarities and differences between Clear NDR Community and the Clear NDR Enterprise.

	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

LEARN MORE

If you need a powerful investigative toolset to support your security operations and threat hunting teams, Clear NDR Enterprise provides the rich network data collection, high-fidelity incident detection and a proactive threat hunting user interface that allows you to pivot from detection right to investigation by providing packet-level visibility and integrated data enrichments to help investigate threats in real time.

There are numerous factors to review when evaluating and considering the upgrade from Clear NDR Community to Clear NDR Enterprise. If you would like to have a detailed conversation to discuss, please contact us via email at contact@stamus-networks.com or complete the form on our website.

ABOUT THE AUTHORS

Éric Leblond

Chief Technology Officer

Éric is an active member of the security and open-source communities. He is a Netfilter Core Team member working mainly on communications between kernel and userland. He works on the development of Suricata, the open source IDS/IPS since 2009 and he is currently one of the Suricata core developers.

Peter Manev

Chief Strategy Officer

Peter has 15 years of experience in the IT industry, including enterprise-level IT security practice. He is an adamant admirer and explorer of innovative open-source security software. He is the Lead QA on the development of Suricata, the open-source IDS/IPS.

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

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

Copyright © 2025