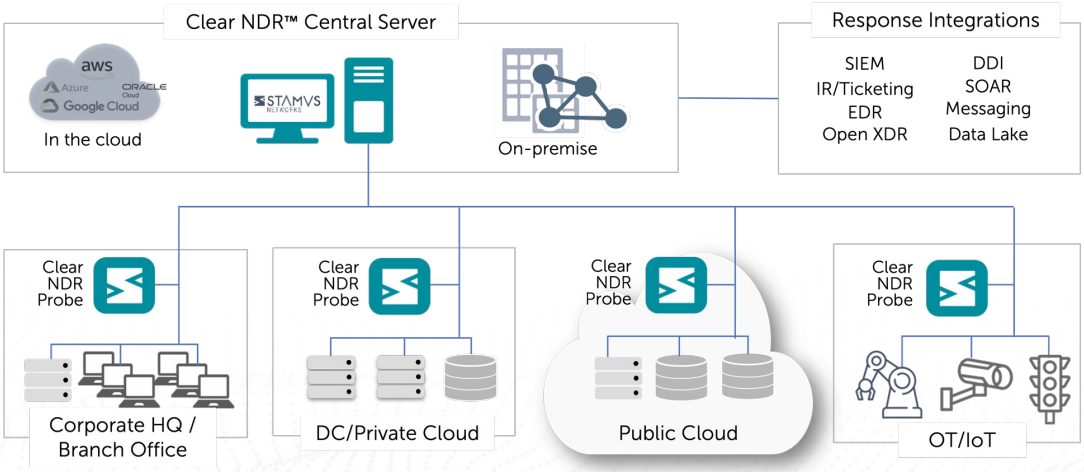
Product Brief

Clear NDR™ Probe AMI for Amazon Web Services®

Extending network visibility and threat detection into your public cloud workflows

Clear NDR™ (formerly Stamus Security Platform) is an open network detection and response solution that delivers actionable network visibility and threat detection. Clear NDR consists of two components: Clear NDR™ Probe and Clear NDR™ Central Server. Each plays a critical role in scaling the system. Clear NDR Central Server and Clear NDR Probes can be deployed in private cloud, public cloud, on-premise, or hybrid environments. Together they provide complete network-based threat detection and response across the enterprise hybrid attack surface.



Clear NDR Probe

Clear NDR Probes inspect and analyze all network traffic using deep packet inspection 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.

The Clear NDR Probe software may be deployed in public cloud (IaaS), private cloud, data center, on premise, or in hybrid environments, providing complete visibility into an enterprise IT and OT activity.

Clear NDR Probe in Amazon Web Services (AWS)

When deployed in Amazon Web Services (AWS) environments, the Clear NDR Probe provides first party visibility into traffic moving in and out of and among IaaS workflows. This real-time analysis empowers you to:

- **Detect Threats Early:** Identify malicious activity hidden within legitimate traffic patterns.
- **Gain Deep Visibility:** Uncover suspicious lateral movements and anomalous behavior within your cloud environment.
- **Accelerate Incident Response:** Reduce dwell time and streamline threat mitigation with rich context and actionable insights.

Leveraging the efficiency and scalability of Amazon Web Services (AWS), the Clear NDR Probe is deployed as a pre-built Amazon Machine Image (AMI). This AMI encapsulates the Clear NDR Probe software along with its necessary configurations. Deployment is very straightforward: simply launch the AMI within your AWS environment, configure security groups to allow traffic from your workloads, and integrate the probe with your VPC. This streamlined process gets you up and running quickly, providing deep visibility into your cloud traffic for enhanced security.

Directing Traffic to the Probe

The Clear NDR Probe analyzes east-west traffic flowing among your cloud workloads. To achieve this, you'll need to configure traffic mirroring within your AWS environment. Here is the standard method for setting up automated traffic mirroring to the Clear NDR Probe:

- **Network Source:** An EC2 or ENI can be a network source. These can use tags with a Lambda function automatically send selected traffic to a Traffic Mirror Target using a traffic mirror filter.

- **Traffic Mirror Target:** This can be the capture ENI of the Clear NDR Probe or an AWS network load balancer that points to the probe's ENI.

- **Traffic Mirror Filter:** Allows you to strategically define what traffic is sent to the Clear NDR Probe for analysis.

Stamus recommends consulting the AWS documentation for detailed instructions on configuring traffic mirroring using each of these methods. This ensures proper integration with your existing AWS infrastructure.

Technical Requirements for the AWS Instance of the Probe

The Clear NDR Probe has minimal resource requirements and scales to meet your workload needs. The probes must be created with 2 network interfaces. One for packet monitoring and the second for administration, control, and sending telemetry to the Clear NDR Central Server.

For detailed specifications, please refer to the the table below

Monitored Bandwidth	Instance type	vCPU	Memory	Disk size (root)	Disk size (logs)
Up to 10Gbps	c5.12xlarge c5.18xlarge	48 72	96 GB 144 GB	gp3, 100 GB	gp3, 2000 GB
Up to 1Gbps	t3.2xlarge c5.4xlarge	8 16	32 GB 32 GB	gp3, 70 GB	gp3, 500 GB
Up to 100Mbps	t3.medium	2	4 GB	gp3, 50 GB	st1, 200 GB

Learn More

- Download the Clear NDR datasheet for a detailed overview
- Visit the Stamus Networks website to explore the Clear NDR
- Contact Stamus Networks directly for a demonstration or security consultation

STAMUS NETWORKS

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

5 Avenue Ingres
75016 Paris
France

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

