# LINKSHADOW®
# INTELLIGENT NDR


## OVERVIEW

### LINKSHADOW, INTELLIGENT NDR.

LinkShadow®, The Intelligent NDR Platform, was developed to provide unparalleled monitoring, detection, and response to the most sophisticated cyber threats and incidents. LinkShadow® empowers organizations to defend against advanced cyber-attacks, zero-day malware, and ransomware through a comprehensive analysis of the network, systems, and applications traffic and utilizes the various organizations' security solutions through out-of-the-box connectors that ensure responding to different incidents over these solutions.

## HIGHLIGHTS

- Get a global view of the latest attacks on your organization based on threat feeds from existing security assets with AttackScape Viewer
- Geo-intelligence based topological view helps you monitor suspicious inbound/outbound traffic with TrafficSense and Attack Visualizer
- Detect anomalies through behavioral analytics performed on correlated logs, packet and 3rd party tool detection using advanced machine learning algorithms with ThreatScore Quadrant
- Visual trend analytics on user behavior including authentication patterns, application usage habits, etc. with Identity Intelligence
- Automatically discover all devices across your entire network, providing insight into device type and OS, plus validation of whether devices are managed or unmanaged, and whether endpoint security is installed with Asset AutoDiscovery
- Single-pane-of-glass view on the effectiveness of your existing security systems through log correlation: firewall, sandbox, IPS and endpoint security with BlockCount Ratio
- Agentless application and endpoint behavioral analytics enabling deep learning about your users with User Investigator
- Get a detailed view of an anomalous entity in your network and the connections it makes with other entities in the network with Entity Inspector
- Automated Response on anomaly triggered using Response Module

# NDR Specifications

| | LS 500 | LS 1000 | LS 3000 | LS 6000 | LS 10000 | LS 20000 | LS 40000 | LS 100000 |
|---|---|---|---|---|---|---|---|---|
| **Network Throughput** | Upto 500 Mbps | Upto 1 Gbps | Upto 3 Gbps | Upto 6 Gbps | Upto 10 Gbps | Upto 20 Gbps | Upto 40 Gbps | Upto 100 Gbps |
| **Network Interface** | 4 x 1 GbE Copper<br>2 x 1 GbE Mgmt Port | 4 x 1 GbE Copper<br>2 x 10 GbE Fiber(optional)<br>2 x 1 GbE Mgmt Port | 2 x 10 GbE Copper<br>2 x 10/25 GbE Fiber<br>2 x 1 GbE Mgmt Port | 2 x 10 GbE Copper<br>2 x 10/25 GbE Fiber<br>2 x 1 GbE Mgmt Port | 2 x 10 GbE Copper<br>2 x 10/25 GbE Fiber<br>2 x 1 GbE Mgmt Port | 2 x 10 GbE Copper<br>2 x 10/25 GbE Fiber<br>2 x 1 GbE Mgmt Port | 2 x 100 GbE Fiber<br>2 x 10/25 GbE Fiber<br>2 x 1 GbE Mgmt Port | 2 x 100 GbE Fiber<br>2 x 10/25 GbE Fiber<br>2 x 1 GbE Mgmt Port |
| **Form Factor** | 1U | 1U | 1U | 1U | 1U | 1U | 1U | 1U |
| **Power Supplies** | 700 W, 200 — 240 VAC, hot swap redundant | | 1100W, 100—240 VAC, hot swap with full redundant | | | | | |
| **Fans** | Up to 4 fans | | Up to 4 sets (dual fan module) hot plug fans | | | | | |
| **Dimensions** | • Height – 42.8 mm (1.68 inches)<br>• Width – 482.0 mm (18.97 inches)<br>• Depth – 585.3 mm (23.04 inches) without bezel<br>• Depth — 598.9 mm (23.57 inches) with bezel | | • Height – 42.8 mm (1.68 inches)<br>• Width – 482 mm (18.97 inches)<br>• Depth – 822.88 mm (32.39 inches) with bezel<br>• Depth – 809.04 mm (31.85 inches) without bezel | | | | | |
| **Bezel** | Security bezel or Optional Filter bezel | | Optional LCD bezel or security bezell | | | | | |
| **Heat Dissipation** | 2625 BTU/hr | | 4100 BTU/hr | | | | | |
| **Cooling Options** | Air Cooling | | | | | | | |
| ***GPU (optional)** | NA | | Peak FP32: 4.5 TFLOPS, Peak FP16: 18 TFLOPS, 16 GB Memory, 200 GB/s Bandwidth | | | | | |

**GPU is a prerequisite for enabling the **ShadowGPT functionality.***

# NDR Sensor Appliance Specifications

| Feature | Technical Specifications |
|---|---|
| **Appliance** | **LS 500-S** |
| **Network Interface** | 2x1 GbE Mgmt Interface 4x1 GbE Copper |
| **Network Throughput** | Upto 500 Mbps |
| **Power Supplies** | 700 W Titanium 240 V DC, cabled |
| **Form Factor** | 1U Rack Server |
| **Fans** | Up to four cabled fans |
| **Cooling Options** | Air Cooling |
| **Dimension** | • Height: 42.8 mm (1.68 inches)<br>• Width: 482 mm (18.97 inches)<br>• Depth: - 598.64 mm (23.56 inches) with bezel<br>- 585 mm (23.03 inches) without bezel |
| **Bezel** | Optional bezel or security bezel |
| **Heat Dissipation** | 2625 BTU/hr |

# LinkShadow VM Appliance Resource Requirements and Performance

| Resource Type | | | | |
|---|---|---|---|---|
| **Appliance** | **LSSR500-V** | **LS 1000-V** | **LS 3000-V** | **LS 5000-V** |
| **Network Throughput** | Upto 500 Mbps | Upto 1 Gbps | Upto 3 Gbps | Upto 5 Gbps |
| **Drive** | Min 500 GB - Data<br>Min 500 GB - PCAP | Min 1 TB - Data<br>Min 1 TB - PCAP | Min 3 TB - Data<br>Min 3 TB - PCAP | Min 5 TB - Data<br>Min 5 TB - PCAP |
| **Interface** (1) | 1 Management Port (2)<br>1 Monitoring Port (3) | 1 Management Port (2)<br>1 Monitoring Port (3) | 1 Management Port (2)<br>1 Monitoring Port (3) | 1 Management Port (2)<br>1 Monitoring Port (3) |
| **CPU** (4) | 12 vCPU, Intel Broadwell and above | 24 vCPU, Intel Broadwell and above | 40 vCPU, Intel Broadwell and above | 40 vCPU, Intel Broadwell and above |
| **Memory** | 24 GB minimum Required | 64 GB minimum Required | 128 GB minimum Required | 192 GB minimum Required |
| **Hypervisors** | VMware ESXi 6.7 or Higher, and Hyper-V | | | |
| **Supported Cloud Platforms** | AWS, Azure, GCP, OCI | | | |
| **VMware Virtual Switch Type** | VMware Virtual Standard Switch (VSS) or VMware Distributed Switch (VDS a.k.a. dvSwitch) | | | |

(1) Interface – Linkshadow uses VMXNET3 driver for capture and management ports.

(2) Management Port – One network port is required for management. The interface must be accessible on port 443.

(3) Monitoring Port – The throughput of network port is recommended based on the LinkShadow Model (Total Throughput) for the physical mirror port. The physical port mirror interface must be connected to the port mirror destination on the switch.

(4) CPU requirements- CPU must be server grade CPU, and vCPU should support instruction set AVX512. (This requires Hypervisor host to run on Intel Broadwell processor or above).

# NDR Virtual Sensor Appliance Specifications

| Resource Type | |
|---|---|
| **Appliance** | **LSSR500-V-S** |
| **Network Throughput** | Upto 500 Mbps |
| **Drive** | Min 500 GB - Data |
| **Interface** [1] | 1 Management Port[2]<br>1 Monitoring Port[3] |
| **CPU** [4] | 12 vCPU, Intel Broadwell and above |
| **Memory** | 24 GB minimum required |
| **Hypervisors** | VMware ESXi 6.7 or Higher, and Hyper-V |
| **Supported Cloud Platforms** | AWS, Azure, GCP, OCI |
| **VMware Virtual Switch Type** | VMware Virtual Standard Switch (VSS) or VMware Distributed Switch (VDS a.k.a. dvSwitch) |

# LINKSHADOW® TECHNOLOGIES

## Shadow 360
Obtain in-depth view of all activities before and after an anomaly

## AI-Powered Engine
Manages end-to-end from data collection to detection and visualization

## AML Anomaly Detection
Detect anomalies through advanced machine learning algorithms applied on enriched network & user data

## BlockCount Ratio
Validate the effectiveness of existing security solutions and their ROI

## Management Dashboard
Overview of organizations' security posture providing high-level security KPIs & KRIs to CXOs

## LiveShadow
Compilation of all critical security findings in real-time


## Asset AutoDiscovery
Automatically discover & track assets across the entire network and monitor activity trends

## ThreatScore Quadrant
Learn, score and prioritize assets & users for action, based on risk scores

## Identity Intelligence
Get visual trend analytics on user behavior including authentication patterns, application usage habits etc.