EXTRAHOP SENSORS

Analytics at the Speed of the Digital Enterprise

The ExtraHop sensor performs stream processing on network traffic, providing security and IT teams with complete visibility, instant threat detection, and intelligent response capabilities at scale. Physical and virtual appliances are available for both SaaS and Self-Managed deployments for flexible, powerful Network Detection and Response (NDR) in hybrid and multi-cloud environments at any scale.

UNMATCHED SCALABILITY

A single ExtraHop sensor can analyze behavior for up to 100,000 endpoints up to a sustained 100 Gbps, equivalent to more than 1 PB of analysis each day, while still guaranteeing at least 90 days of lookback.

VALUABLE DETAILS

The ExtraHop real-time stream processor extracts over 5,000 L2-L7 metrics from network traffic, providing rich data for our cloud-scale ML security detections, enabling 95% faster threat detection and 84% faster incident response.

THE ONLY NDR WITH TLS 1.3 / PFS DECRYPTION

ExtraHop is the only NDR product that can decrypt TLS 1.3 with perfect forward secrecy in real time for analysis, enabling covert detection of the stealthiest threats.

IMMEDIATE VALUE FOR ALL TEAMS

ExtraHop sensors are available as physical or virtual appliances for both SaaS and Self-Managed deployments, including hybrid environments and in the cloud in AWS, Azure, and Google Cloud. Reveal(x) 360 is available as a pure SaaS service in AWS.

SaaS SENSORS

Reveal(x) 360 SaaS for AWS	1Gbps
Premium (Sensor only)	Yes
Ultra (Sensor + Continuous PCAP)	Yes
Record Lookback	90 days

PHYSICAL SENSORS

SPECIFICATIONS	EDA 10200	EDA 9200	EDA 8200
TRAFFIC ANALYTICS			
Throughput	100 Gbps	50 Gbps	25 Gbps
NETWORK	ExtraHop appliances can receive data via RPCAP, ERSPAN, VXLAN, or physical ports.		25 Gbps
Management ports	2 x 1 GbE copper + 2 x 10 GbE fiber	2 x 1 GbE copper + 2 x 10 GbE fiber	4 x 1 GbE copper
High Speed Monitoring Connectivity Options	2 x 100 GbE/40 GbE MPO fiber (base) 4 x 100 GbE/40 GbE MPO fiber (option) 4 x 25 GbE/10 GbE LC fiber (option) 4 x customer-supplied DAC	4 x 25 GbE/10 GbE LC fiber 4 x customer-supplied SFP28 DAC	2 x 25GbE/10GbE LC fiber 2 x customer-supplied SFP28 DAC
CHASSIS			
Datastore	18 TB (RAID 10)	7.2 TB (RAID 10)	7.2 TB (RAID 10)
Packet capture (optional)	480 GB	480 GB	480 GB
Power supply	2 x 1100 W	2 x 750 W	2 x 750W
Rack Unit	2U	2U	1U
Height	8.68 cm (3.42 in.)	8.68 cm (3.42 in.)	4.28 cm (1.68 in.)
Width	43.4 cm (17.09 in.)	43.4 cm (17.09 in.)	43.4 cm (17.08 in.)
Depth	71.6 cm (28.17 in)	71.6 cm (28.17 in)	73.4 cm (29.61 in.)
Weight	26.3 kg (57.98 lb)	26.3 kg (57.98 lb)	21.9 kg (48.28 lbs)
ENVIRONMENT DETAILS			
Heat dissipation	4100 BTU/hr maximum	2891 BTU/hr maximum	
Operating temperature	10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment		
Storage temperature	–40°C to 65°C (–40°F to 149°F)		
Operating relative humidity	10% to 80% RH with 29 °C (84.2° F) max. dew point		
Operating vibration	0.26 Grms at 5 Hz to 350 Hz (all three axes)		
Operating altitude	3,048 m (10,000 ft)	-15.2m to 3,048 m (-50 ft to 10,000 ft)	3,048 m (10,000 ft)
Operating shock	Six consecutively executed shock pulses in the positive and negative x, y, and z axes of 6 G for up to 11 ms		
Operating system	The operating system is a security-hardened embedded Linux with a networking microkernel developed specifically for high-speed packet processing via the ExtraHop real-time stream processor		
Remote management	iDRAC8 remote management controller		

PHYSICAL SENSORS

SPECIFICATIONS	EDA 6200	EDA 4200	EDA 1200
TRAFFIC ANALYTICS			
Throughput	10 Gbps	5 Gbps	1 Gbps
NETWORK	ExtraHop appliances can receive data via RPCAP, ERSPAN, VXLAN, or physical ports .		
Management ports	4 x 1 GbE copper	4 x 1 GbE copper	1000BASE-T
High Speed Monitoring Connectivity Options	2 x 10GbE LC fiber 2 x customer-supplied SFP+ DAC	2 x 10GbE LC fiber 2 x customer-supplied SFP+ DAC	1x1 GbE
CHASSIS			
Datastore	1.2 TB (RAID 10 optional)	Included 240gb SSD	88 GB
Packet capture (optional)	480 GB	480 GB	140 GB
Power supply	2 x 750W	2 x 495W	1x100W
Rack Unit	1U	1U	See physical dimensions below
Height	4.28 cm (1.68 in.)	4.28 cm (1.68 in.)	5.9 cm (2.3 in.)
Width	43.4 cm (17.08 in.)	43.4 cm (17.08 in.)	19.3 cm (7.5 in.)
Depth	73.4 cm (29.61 in.)	73.4 cm (29.61 in.)	20.0 cm (7.9 in.)
Weight	21.9 kg (48.28 lbs)	21.9 kg (48.28 lbs)	1.9 kg (4.2 lbs)
ENVIRONMENT DETAILS			
Heat dissipation	2891 BTU/hr maximum		
Operating temperature	10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment		0 °C to 40 °C
Storage temperature	-40 °C to 65 °C (-40 °F to 149 °F)		-20 °C to +70 °C (4 °F to 158 °F)
Operating relative humidity	10% to 80% RH with 29°C (84.2°F) max. dew point		
Operating vibration	0.26 G rms at 5 Hz to 350 Hz (all operation orientations)		
Operating altitude	3,048 m (10,000 ft)		
Operating shock	Six consecutively executed shock pulses in the positive and negative x, y, and z axes of 6 G for up to 11 ms		
Operating system	The operating system is a security-hardened embedded Linux with a networking microkernel developed specifically for high-speed packet processing via the ExtraHop real-time stream processor		
Remote management	iDRAC8 remote management controller		N/A

VIRTUAL & CLOUD SENSORS

SPECIFICATIONS	EDA 8200V	EDA 6100V	EDA 1100V
TRAFFIC ANALYTICS			
Throughput	up to 25 Gbps	up to 10 Gbps*	up to 1 Gbps
NETWORK REQUIREMENTS			
Monitoring options	ExtraHop appliances can receive data via RPCAP, ERSPAN, VXLAN, and port mirroring. RPCAP, ERSPAN, and VXLAN have a maximum throughput of 1 Gbps per management virtual interface.		
Management virtual interface	1 or more	1 or more	1 or more
Capture virtual interfaces	3	3	1
Firewall requirements	TCP port 443 inbound to appliance for administration purposes UDP port 53 outbound to Internet for registration purposes, unless managed by an ExtraHop Command Appliance (ECA)		
RESOURCE REQUIREMENTS	ExtraHop requires thick provisioning on all virtual appliances. CPUs require hyperthreading, VT-x technology and 64-bit architecture.		
vCPUs	32	16	4
Memory	96 GB	64 GB	8 GB
Disk	2 TB	1TB	46 GB
Packet capture (optional)	1 GB – 500 GB	1 GB – 500 GB	1 GB – 500 GB
VIRTUAL & CLOUD ENVIRONMENTS			
ESX	—	√	√
KVM	—	—	√
AWS	√	√	√
Azure	—	√	√
GCP	—	—	√
Operating system	The operating system is a security-hardened embedded Linux with a networking microkernel developed specifically for high-speed packet processing via the ExtraHop real-time stream processor.		

*ExtraHop was the sole tenant on the server during performance testing. The server under test used two Intel Xeon processors E5-2695 v2, 96GB DDR3 RAM, and 1 TB of storage, and was running VMware ESX v5.1. Data was sent from physical port mirrors to two dedicated 10GbE physical interfaces. Performance may vary by server and network configuration.

ABOUT EXTRAHOP NETWORKS

ExtraHop is on a mission to arm security teams to confront active threats and stop breaches. Our Reveal(x) 360 platform, powered by cloud-scale AI, covertly decrypts and analyzes all cloud and network traffic in real time to eliminate blind spots and detect threats that other tools miss. Sophisticated machine learning models are applied to petabytes of telemetry collected continuously, helping ExtraHop customers to identify suspicious behavior and secure over 15 million IT assets, 2 million POS systems, and 50 million patient records. ExtraHop is a market share leader in network detection and response with 30 recent industry awards including Forbes AI 50, Cybercrime Ransomware 25, and SC Media Security Innovator.

info@extrahop.com
www.extrahop.com