

DATA SHEET

Stellar Cyber Open-XDR Appliances

Turn-key appliances for SOC teams and security analysts

Pervasively collect, reduce, enrich and correlate data

Detect and respond to events from anything and anywhere—cloud, endpoint, network and users

Multi-tenancy architecture for large organizations with multiple departments as well as managed services providers

Support clustering for scalability and high availability

How it works

The appliance works by ingesting data from sensors, agents or log forwarders on the network, physical and virtual servers, or containers. The sensors or agents transform raw data into Interflow™ records which are sent to a centralized data processor that reduces, enriches, correlates and indexes stored data in a data lake. Once this data is received, big data runs analytics including machine learning on the dataset to identify high fidelity breach events.

The appliances conveniently package all functionalities in a single platform while allowing additional sensors, agents and containers to be flexibly deployed anywhere to collect data.

Built for performance and scale

The appliance delivers steady data ingestion and processing performance due to its custom hardware and software design surpassing any off-the-shelf commodity x86 server platform. It's built upon a high-speed I/O bus architecture with solid state disk drives, large amounts of memory, packet accelerated network interface cards and dual high-end processors. Pervasively collect, reduce, enrich and correlate data.



TWO MODELS TO CHOOSE FROM

Hardware Specifications

	MODEL-3000	MODEL-6000
Form Factor	1 rack unit	1 rack unit
Daily Data Ingestion Limit	200 Giga Bytes per day	300 Giga Bytes per day
Raw Data Storage	30 days	30 days
Security Events Storage	365 days	365 days
Multi-Tenancy*	30 tenants	50 tenants
Automated Threat Hunting (ATH) Rules*	600	1,000
Reports*	60	100
Records/Second*	6k	9k
CPU	Dual high-end Intel server class processors	Dual high-end Intel server class processors
Copper Network Interface	4 x 10/100/1000BASE-T	4 x 10/100/1000BASE-T
SFP+ Network Interface	4 x 10Gbe/1Gbe SFP+	4 x 10Gbe/1Gbe SFP+
Storage for Data Ingestion	8 TB	16 TB
External Connector	2 x USB 3.0, 1 x Mini USB	2 x USB 3.0, 1 x Mini USB
Size	17.24" X 1.73" x 12.64"	17.24" X 1.73" x 12.64"
Weight	39.6 lbs	39.6 lbs
Power	AC 100V~240V @47~63Hz, 850W Dual PSUs	AC 100V~240V @47~63Hz, 850W Dual PSUs

*Multi-tenant sizing, ATH rules, Reports and Records/second scaling metrics are based on average utilization, contact Stellar Cyber to establish guidelines for specific deployments.

Stellar Cyber has the discretion to modify external connectors, size, weight and power of any models noted above to accommodate enhancements which have no impact on performance.