

Stellar Cyber Open XDR Appliance

Turn-key Appliance for On-Premises Security Operations

While many organizations choose to use the Stellar Cyber Open XDR Platform from the cloud, known as the Software-as-a-Service offering, situations that require an on-premises deployment of Stellar Cyber exist. In those cases, we offer a turn-key hardware appliance built for performance and scale.

The Stellar Cyber Open XDR On-Premises Appliance enables organizations to:

- **Automatically collect**, reduce, and enrich data to facilitate comprehensive threat detection.
- **Correlate and respond** to incidents across the attack surface - from endpoints to the cloud and anywhere between.
- **Use a multi-tenancy architecture** for large organizations with segmented environments and managed security service providers with multiple customers.
- **Support clustering** for scalability and high availability.

How It Works

The appliance ingests data from sensors, agents, or log forwarders on the network and physical and virtual servers. The sensors or agents transform raw data into Interflow™ records, sent to a centralized data processor that reduces, enriches, correlates, and indexes stored data in the data lake. Once received, big data analytics executes, including machine learning on the dataset to identify high-fidelity threats. The appliances conveniently package all functionalities in a single platform while allowing flexible deployment of additional sensors and agents 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. The appliance runs on 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. This architecture enables pervasive collection and data processing, enabling effective threat detection, alert correlation, and incident response.

Appliance Specifications

Name	Model-6000
Form Factor	1 Rack Unit
Daily Data Ingestion Limit	300 GB per day
Raw Data Storage	30 Days
Security Event Storage	365 Days
Multi-Tenancy*	50 Tenants
Automated Threat Hunting (ATH) Rules*	1,000
Reports*	100
Records/Second*	3,000
CPU	Dual high-end Intel server-class processors
Copper Network Interface	4 x 10/100/1000BASE-T
SFT+ Network Interface	4 x 10Gbe/1Gbe SFP+
Storage for Data Ingestion	16 TB
External Connector	2 x USB 3.0, 1 x USB 2.0
Size	18.98" x 31.8" x 1.69"
Weight	48.3 lbs.
Power	AC 100V-240V @50-60Hz, 750W Dual PSUs

* Based on average utilization, Multi-tenant sizing, ATH rules, reports, and records/second scaling metrics. Contact Stellar Cyber to establish guidelines for specific deployments.

Stellar Cyber can modify external connectors, size, weight, and power to accommodate enhancements without impacting performance.

Stellar Cyber delivers comprehensive, unified security without complexity, empowering lean security teams of any skill to successfully secure their environments. With Stellar Cyber, organizations reduce risk with early and precise identification and remediation of threats while slashing costs, retaining investments in existing tools, and improving analyst productivity, delivering an 8X improvement in MTTD and a 20X improvement in MTTR. The company is based in Silicon Valley. For more information, visit stellarcyber.ai.