DATA SHEET

Stellar Cyber Sensors

Maximize Threat Detection and Telemetry Collection Across IT and OT Environments

To combat today's advanced cyber attacks, security teams must be confident that they have complete visibility across the entire attack surface. When security teams are unknowingly blind to portions of the attack surface due to the lack of coverage, attackers can and will exploit this weakness to carry out attacks.

Stellar Cyber Sensors help mitigate security risk by covering the entire environment across on-premises, cloud, virtual, and physical hosts. These sensors offer a simple way to deploy detection capability to the edge and collect all telemetry wherever required.

Stellar Cyber Sensors come in virtual and physical forms and can work in large and small environments, delivering 360° visibility. The detection capabilities at the edge leverage both heuristics (in the form of signatures and rules) and Machine Learning to provide comprehensive threat detection. This detection approach at the edge reduces Mean Time To Detect (MTTD) and collected data volumes.

Optimal Cost and Flexibility

Stellar Cyber bundles many sensors and its Open XDR Platform without extra costs. Additional sensors are available for purchase to increase coverage. Stellar Cyber sensors work with any network environment, physical, virtual, cloud, and core server operating systems.

Functionality Overview

The following list covers all functionality across all sensor packages. To map which sensor package includes which functionality, reference the next section - "Family of Sensors."

Intrusion Detection System (IDS)

Tens of thousands of signatures for known threat detection, updated daily from emerging threat research.

File Integrity Monitoring (FIM)

Deploy our Windows and Linux servers across their network with the ability to monitor specific sensitive files and folders to ensure an attacker has not moved or corrupted these critical files.

File Anti-Virus (AV)

Files are reconstructed over the wire and then analyzed with machine learning to detect if they are malicious.

Malware Sandbox

If reconstructed files over the wire are determined to be suspicious or unknown, they are detonated in a cloud Malware Sandbox to detect novel threats.

Deep Packet Inspection (DPI)

Discover and analyze tens of thousands of apps running across the network for threats and anomalies.

Traffic Metadata Capture

Reduce raw packets by several orders of magnitude while retaining beneficial flow and application metadata for analysis.

3rd Party Connectors

3rd party security and IT products are often not accessible from the internet due to firewalls, such as vulnerability scanners or self-hosted identity solutions like local Active Directory; run connectors to collect and respond through 3rd party products directly in the environment they reside.

Log Collection

Collect, filter, and normalize logs from security and IT products to stream for centralized analysis.

Server Log Collection

Collect customized system logs from any server for centralized analysis.

Local Response

Secure channel for orchestrating the incident response to local security tools like firewalls and active directory.

Data Normalization

Data from any source, Stellar Cyber or 3rd party products, is normalized into a standard data format for centralized analysis.

Data Buffering

Enables short-term data buffers when connectivity is lost.

Centralized Management

Provisioning, monitoring, and upgrading software.

Family of Sensors

Feature	Network Sensor	Security Sensor	Server Sensor
Deployment Methods	**Physical or Virtual**	**Physical or Virtual**	**Virtual**
Intrusion Detection System		✓	
File Anti-Virus		✓	
Malware Sandbox		✓	
Deep Packet Inspection	✓	✓	
Traffic Metadata Capture	✓	✓	✓
3rd Party Connectors	✓	✓	
Local Response	✓	✓	
Log Collection	✓	✓	✓
Server Log Collection			✓
File Integrity Monitoring			✓
Data Normalization	✓	✓	✓
Central Management	✓	✓	✓
Data Buffer	✓	✓	✓

Deployment

Virtual network and security sensors deploy as virtual machines, into all popular hypervisors or on any public cloud. Physical Network and Security Sensors mirror traffic from a switch or network tap. In either case, the configuration takes only a minute to set up.

Server Sensors deploy onto Windows- and Linux-based hosts, regardless of where that host lives - on-premises or in the cloud. Installers provide for both operating system groups, with management, happening directly from Stellar Cyber's user interface.

Stellar Cyber Security Sensors Virtual Specifications

The following table covers the necessary virtual machine specifications for running the Network and Security Sensors at various maximum throughputs.

Sensor Type	Maximum Throughput	Virtual Cores (Reserved)	Ram (GB) (Reserved)	SSD (GB) (Reserved)
Network Sensor	10Gbps	24	64	512
	1Gbps	12	32	128
	250Mbps	4	8	64
Security Sensor	10Gbps	24	64	512
	1Gbps	12	32	128
	500Mbps	8	16	128
	200Mbps	4	8	128

**Stated specifications support the corresponding maximum network traffic inspection throughput. Performance may vary depending on your environment, configuration, and other variables.*

Stellar Cyber Photon Hardware Sensor Specifications

The following Photon Hardware devices are the physical options for Network and Security Sensors at different rated throughputs.

	PHOTON-160	PHOTON-250	PHOTON-400
Network Capture Throughput (All Features Enabled)	Up to 500 Mbps	Up to 1 Gbps	Up to 10 Gbps
Network Interfaces	6 x RJ45 (1Gbps)	4 x GbE RJ45 Intel® SoC Integrated MAC 2 x GbE RJ45 Intel® i350 2 x GbE SFP Intel® i350	6 x GbE RJ45 2 x 10G SFP+
Storage	238 GB	512 GB	480 GB
External Connector	3 X USB 3.0, 3 X USB 2.0, HDMI and Serial Console (COM) ports	2 x USB 2.0	3 x USB 2.0
Size	7.32" x 4.98" x 2.60"	9.10" x 7.87" x 1.73"	17.08" x 1.68" x 28.13"
Weight	3.025 lbs	2.65 lbs	38.9 lbs
Power	DC 12Volts (AC 100~240V @50~60 Hz external)	AC 100~240V @50~60 Hz 60W	AC 100~240V @50~60 Hz 550W

**Stellar Cyber has the discretion to modify external connectors, size, weight, and power of any model noted above to accommodate enhancements that do not impact 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.**