DATA SHEET

Stellar Cyber Sensors

Maximize Detection and Telemetry Collection Across Every Environment

To combat today's advanced cyber attacks, security teams need to 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 telemetry coverage, attackers can, and will, exploit this weakness to carry out attacks.

Stellar Cyber Sensors help you mitigate the security risk by enabling you to cover your entire environment across on-premises, cloud, virtual hosts, and physical hosts. These sensors offer a simple way for you to deploy detection capability to the edge and collect all forms of telemetry wherever the coverage is required.

Stellar Cyber's Sensors come in multiple form factors, virtual, physical, or containers, and can work in large and small environments, ultimately delivering the most cost-effective 360° coverage. The detection capabilities at the edge leverage both heuristics (in the form of signatures and rules) and Machine Learning. Getting this multi-modal detection approach to the edge reduces Mean Time To Detect (MTTD) and reduces overall collected data volumes.

Optimal Cost and Flexibility

Stellar Cyber bundles many sensors and its Open XDR Platform, so you don't need to worry about getting up and running in terms of extra costs. Additional sensors can be purchased to increase coverage. Stellar Cyber's sensors work with any network environment, physical, virtual, or cloud, and all core server operating systems to ensure maximum deployment flexibility. Finally, the broad family of sensors allows you to deploy only the capability you need.

Functionality Overview

The following list covers all functionality across all sensor packages. For a mapping of 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 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 tens of thousands of apps running across your network to be analyzed for threats and anomalies.

Traffic Metadata Capture

Raw packets are reduced by several orders of magnitude while retaining useful flow and application metadata for analysis.

cont'd >

STELLAR CYBER®

Log Collection

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

Server Log Collection

Collect customized sets of system logs from any server for centralized analysis.

Local Response

Secure channel for orchestrating 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.

Centralized Management

Provisioning, monitoring, and upgrading software.

Data Buffering

Short-term data buffer for when connectivity is lost.

FAMILY OF SENSORS

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

Deployment

Virtual Network and Security Sensors are deployed as virtual machines, into all popular hypervisors or on any public cloud. Physical Network and Security Sensors are run by mirroring traffic off of a switch or network tap. In either case, the configuration takes only a minute to set up.

Server and Container Sensors are deployed onto hosts, both Windows and Linux based, regardless of where that host lives—on-premises or in the cloud. Easy installers are provided 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. The feature comparisons of a sensor configured as a Network Sensor vs. a Security Sensor are shown in the matrix earlier in this document. In summary, for network capture, Network Sensors only perform DPI and metadata collection, whereas a Security Sensor performs DPI, metadata collection, and at least one of IDS, File AV, or Malware Sandbox.

	PHOTON-100	PHOTON-150	PHOTON-250	PHOTON-300	PHOTON-400
					
Network Capture Throughput (DPI Only)	Up to 200 Mbps	Up to 500 Mbps	Up to 5 Gbps	Up to 10 Gbps	Up to 10 Gbps
Network Capture Throughput (All Features Enabled)	Up to 200 Mbps	Up to 500 Mbps	Up to 1 Gbps	Up to 1 Gbps	Up to 10 Gbps
Network Interfaces	4 x RJ45 (100Mbps / 1Gbps)	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+	6 x GbE RJ45 2 x 10G SFP+
Storage for Data Buffering	64 GB	256 GB	512 GB	480 GB	480 GB
External Connector	1 x USB 3.0, HDMI	4 x USB 3.0, HDMI	2 x USB 2.0	3 x USB 2.0	3 x USB 2.0
Size	4.53” x 4.23” x 1.54”	7.32” x 4.98” x 2.60”	9.10” x 7.87” x 1.73”	17.08” x 1.68” x 28.13”	17.08” x 1.68” x 28.13”
Weight	1.1 lbs	2.87 lbs	2.65 lbs	38.9 lbs	38.9 lbs
Power	DC 12Volts (AC 100~240V @50~60 Hz external)	DC 12Volts (AC 100~240V @50~60 Hz external)	AC 100~240V @50~60 Hz 60W	AC 100~240V @50~60 Hz 550W	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 have no impact on performance.*

Stellar Cyber Open XDR delivers **world-class, comprehensive, unified security without complexity**, empowering security teams of any size and skill to deliver continuous security. 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 a **20X improvement in MTTD and an 8X improvement in MTTR**.