Stellar Cyber Overview

Stellar Cyber Empodera las Operaciones de Seguridad

- Equipo Global, con una base de clientes y partners
- Alrededor de ~10,000 clientes globalmente
- Alianzas con tecnologías líderes en el mercado

ORACLE · CROWDSTRIKE · CHECK POINT · deepinstinct · f5 · Microsoft · corelight · SentinelOne · SWIMLANE · Gigamon · Siemplify · SONICWALL · Malwarebytes · paloalto NETWORKS · netskope · proofpoint · tenable · Extreme networks · D3 · Hitachi Solutions · BlackBerry CYLANCE · EGNYTE · HDN Handreamnet · vmware · Barracuda · FORTINET · mimecast

Enfoque abierto garantizando inversiones

Gartner

Stellar Cyber se destaca en proyectos XDR

OMDIA
Brought to you by Informa Tech

Stellar Cyber mejora la eficacia, la eficiencia y la productividad del SOC

ESG
Enterprise Strategy Group

Stellar Cyber es seleccionada como una de las 20 mejores plataformas de análisis de seguridad

FORRESTER®

Stellar Cyber ofrece protección generalizada con su plataforma XDR

451 Research®

Las 10 Empresas de Seguridad más Calientes de XDR que debes seguir

THE CHANNEL CO. CRN

Solución de XDR más innovador 2023

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2023

Ganador de Cloud Security 2022

TMC Cloud Computing EXCELLENCE AWARD 2022

Premio Baby Black Unicorn 2022

BABY BLACK UNICORN AWARDS 2022 FINALIST

Editor's Choice XDR 2022

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2022

Mejor solución de Ciberseguridad 2022

Líder de Mercado Nube Futuriom 40 2022

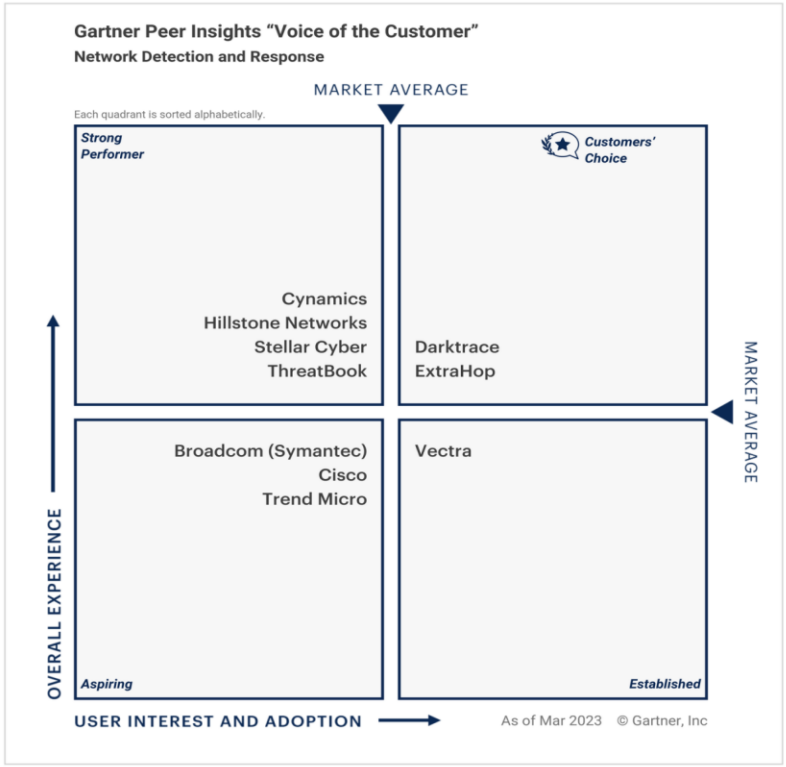
2022 FUTURIOM 40 STELLAR CLOUD MARKET LEADER

STELLAR CYBER®

Stellar Cyber Empodera las Operaciones de Seguridad

Gartner

Figure 1. Voice of the Customer for Network Detection and Response



Source: Gartner (May 2023)

Network Detection and Response Peer Reviews and Ratings

In addition to the synthesis provided by the "Voice of the Customer," you can read individual reviews and ratings on Gartner Peer Insights by clicking here.

Gartner

Table 1: Representative Vendors Offering XDR

(Enlarged table in Appendix)

Vendor	Product Name
CrowdStrike	Falcon Insight XDR
Cisco	XDR
Fortinet	FortiXDR
Trellix	XDR
Microsoft	365 Defender
Palo Alto Networks	Cortex XDR
SentinelOne	Singularity
Stellar Cyber	Open XDR
Sophos	XDR
Trend Micro	Trend Vision One

STELLAR CYBER®

Unique Capabilities of Stellar Cyber NDR

1

All Data Types
Raw packets,
NGFW/IDS Logs,
Netflow/IPFix

2

Various Data Sources
Physical or virtual
switches,
containers, servers
IaaS (Azure, AWS)

3

Rich Traffic Content
DPI/4,000+ identified apps
User-defined applications
L2-L7 metadata,

4

Big Data Reduction
Packet duplication,
(user-definable) data filtering
data compression

5

Handle Encrypted Traffic
Behavioral analysis,
certificate inspection
CN/SNI, JA3

6

Broad Data Enrichment
IP/URL reputation, IP
geolocation,
IP to hostname, IP to
username,

7

Flexible Data Retention
Configurable hot storage
external cold storage
for compliance

8

Wide Data Availability
Data buffering,
data replica, HA,
disaster recovery

9

Case Driven Detection
Supervised & unsupervised learning,
Deep learning, signature-based detection/IDS in one device

10

Different Type of Correlation
Auto CVE correlation among
IDS events and device vulnerability
Auto-correlation of alerts

11

Fast Response
Drop traffic, disable users,
contain endpoints, trigger
vulnerability scan, invoke script,
call APIs, alerting, reporting

12

Flexible Deployment
Physical or virtual appliance,
SaaS
distributed sensors
ML is part of the local deployment

STELLAR CYBER®

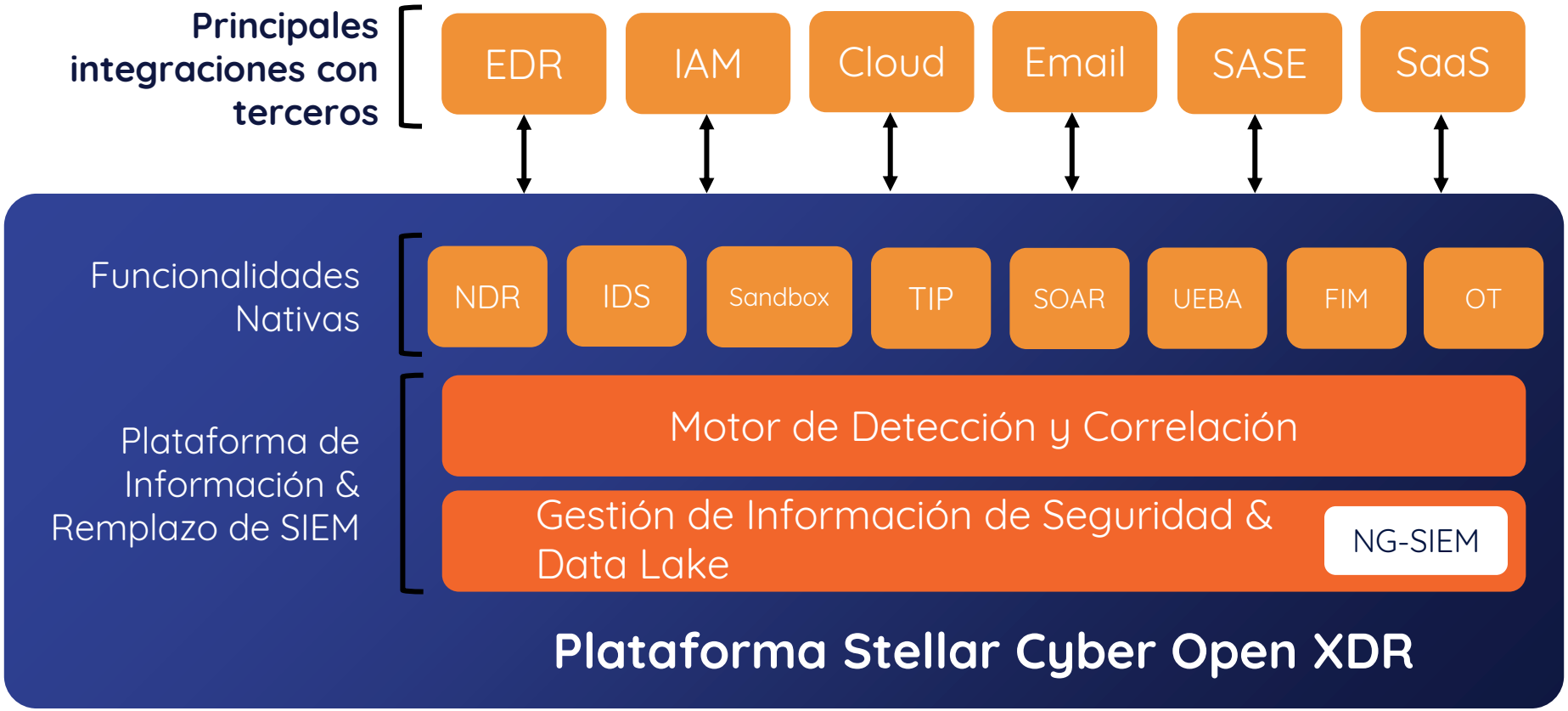
Plataforma Stellar Cyber Open XDR Principios

Simplificada

Automatizada

Abierta

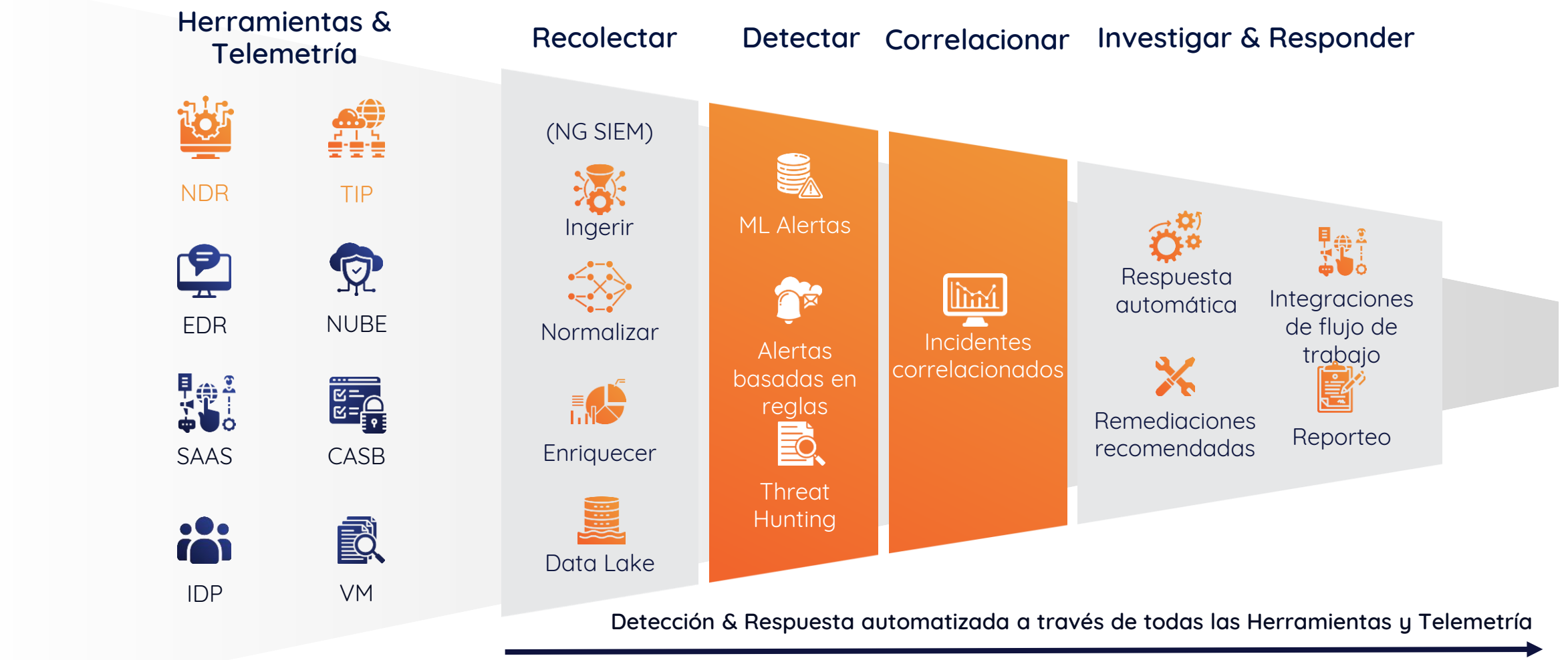
Unificada



STELLAR CYBER®

Una Plataforma y Una Licencia para Operaciones de Seguridad

Componentes Nativos en la Plataforma de Stellar Cyber's Open XDR



STELLAR CYBER®

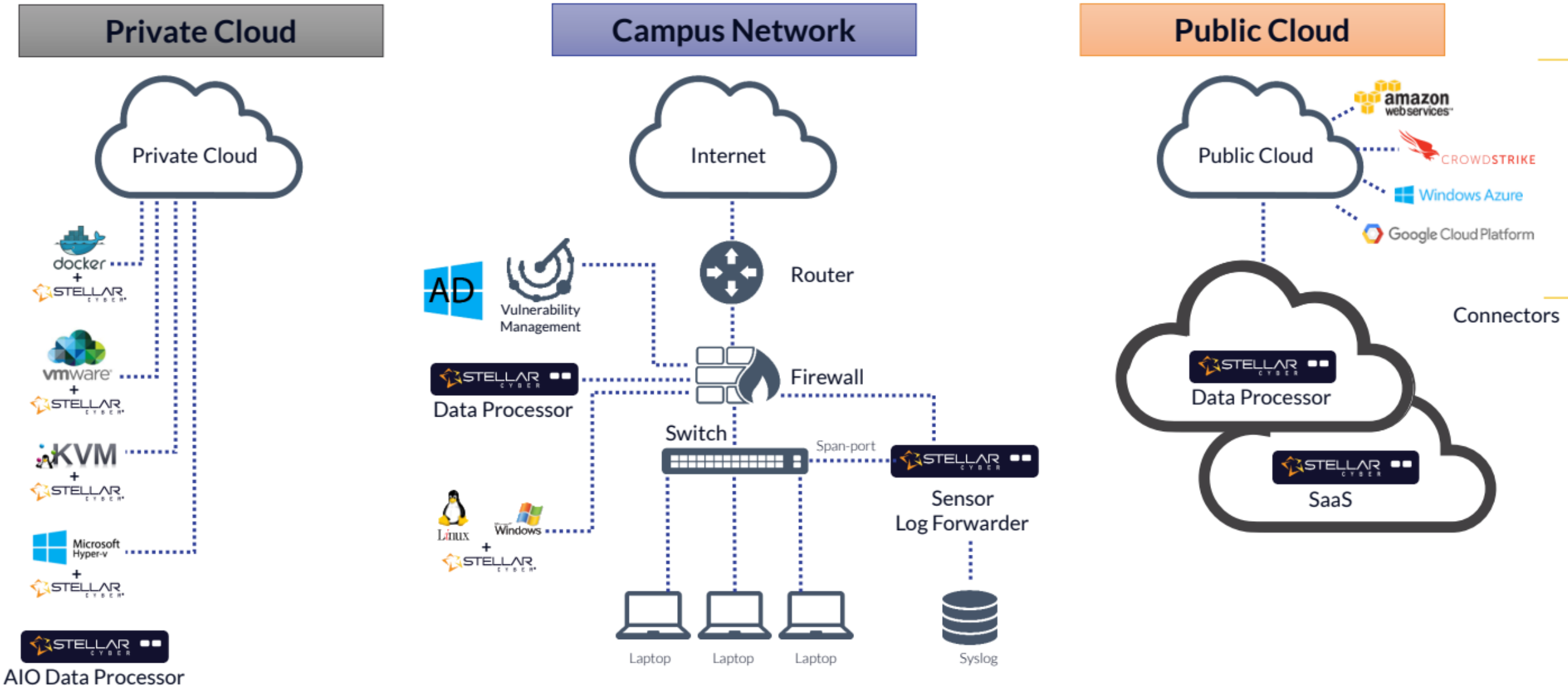
BENEFICIOS DE OPEN XDR POR FUNCIÓN

SIMPLIFICA LA COMPLEJIDAD DE LAS OPERACIONES DE SEGURIDAD

- TTV en 4 semanas
- 75% menos actividades de seguimiento y configuración
- MTTD -10 mins
- MTTR -15 mins

- 20% menos presupuesto para personal de monitoreo
- 80% menos personal para mantenimiento de plataforma
- Reducción de nivel de exposición de hasta un 75%

- MTTR -15 mins
- Evitar ataques avanzados al tener acciones de respuesta automatizadas
- Mejor calidad de sueño y de vida


Private Cloud
Campus Network
Public Cloud
Private Cloud
docker
+
STELLAR CYBER
vmware
+
STELLAR CYBER
KVM
+
STELLAR CYBER
Microsoft Hyper-v
+
STELLAR CYBER
STELLAR CYBER
AIO Data Processor
Internet
AD
Vulnerability Management
Router
STELLAR CYBER
Data Processor
Firewall
Switch
Span-port
STELLAR CYBER
Sensor
Log Forwarder
Linux
Windows
+
STELLAR CYBER
Laptop
Laptop
Laptop
Syslog
Public Cloud
amazon web services
CROWDSTRIKE
Windows Azure
Google Cloud Platform
Connectors
STELLAR CYBER
Data Processor
STELLAR CYBER
SaaS

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	✓	✓	✓

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

FEATURES & CAPABILITIES	STELLAR CYBER	ALIEN VAULT	exabeam	DARKTRACE	IBM Radar	LogRhythm	Microsoft Sentinel	securonix	splunk>
Native Multi-layer Multi-tenancy									
Unified Platform (NG-SIEM, NDR, SOAR, UEBA, TI)									
All Capabilities Included in Single License									
Services to Help Security Team at No Additional Charge									
Sensors for Remote Data Collection and Edge Detections									
Easy Setup									
Flexible Deployments									
Correlation									
Full Attack Surface Coverage									
Out-of-the-Box Integrations									

STELLAR CYBER®

¡GRACIAS!

agiraldo@stellarcyber.ai

www.stellarcyber.ai >>