WHITE PAPER

Turn your MSP into a Profitable MSSP with Stellar Cyber

Powered by the Stellar Cyber Open XDR Platform

STELLAR CYBER®

Cybersecurity has evolved over the past 30 years, moving from perimeter defenses (firewalls) to more holistic approaches that incorporate security for email, endpoints, applications, servers, and cloud. With this evolution have come a huge array of discrete tools that provide protection in each area, so now a typical MSSP has dozens of individual tools to manage. The challenge is that each tool has its own data format and its own console, so analysts must move from one console to another and manually correlate alerts among them to discover today's complex cyberattacks. As new tools emerge, MSSPs must find more expensive, scarce analysts to run these tools' consoles, adding complexity and cost to the whole cyber defense effort.

XDR is a response to this challenge. By unifying most or all security tools under a single interface with a single data lake, XDR makes it easier to spot complex attacks and enables analysts to respond more quickly. XDR also reduces the number of analysts required to run the cybersecurity system, thereby reducing costs.

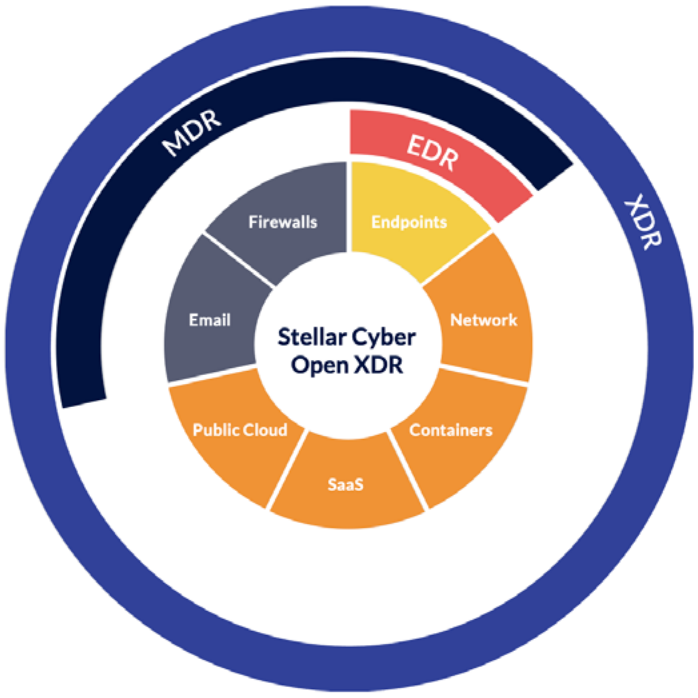
This paper explains how Stellar Cyber's Open XDR platform helps MSPs become MSSPs with the fastest, least expensive, and most comprehensive XDR solution.

Executive Summary

Cybersecurity is top-of-mind for most IT managers, but many mid-sized enterprises can't afford to deploy a full-fledged security operations platform on their own. Rather, they are turning to Managed Security Service Providers (MSSPs). Managed Service Providers want to become MSSPs to get into the high-demand managed security business, but like mid-sized enterprises, they lack the resources to do this using traditional, stand-alone security tools. Each tool has its own license fee, its own console, and its own data format, which makes creating a suite of such tools expensive and complex.

Today's cyberattacks target multiple vectors (user logins, servers, firewalls, etc.), but when analysts are forced to manually interpret and correlate data from many different consoles, it is difficult to detect and respond to attacks in a timely manner. Many organizations only discover cyberthreats after they have been in the network for weeks or months.

MDR, EDR and XDR Services and Attack Surface Coverage
360° Visibility



XDR is a promising solution to these challenges. It unifies multiple security tools under a single interface, making threat signals easier to spot and interpret. Stellar Cyber's Open XDR solution goes beyond other XDR products to deliver 8X faster Mean Time to Detect and 20X faster Mean Time to Respond. It unifies all the data from multiple tools, automatically correlates that data, displays a prioritized list of actual cybersecurity incidents for immediate action by analysts, and responds to many threats automatically through the appropriate network systems.

This paper discusses the challenges for MSPs wanting to become MSSPs and shows how Stellar Cyber's Open XDR platform addresses them, providing the fastest route to creating a fully functional Security Operations Center.

Why MSPs are Becoming MSSPs

Many MSPs are looking to offer MSSP services. Cybersecurity is in the news daily, and attacks are occurring every minute of every day. Every organization wonders if it will be next. By evolving from an MSP to an MSSP, a provider can broaden its customer base, increase revenue, and, most importantly, improve margins.

Stellar Cyber's Open XDR platform is the fastest and most cost-effective way to transform from an MSP to an MSSP.

Barriers to Becoming an MSSP

MSPs have been told for the last several years that if you cannot afford to build a SOC, you should outsource the MSSP services to a larger partner or manufacturer that does. Most of the manufacturers are understaffed and provide little more than lists of alerts to respond to for your customers. We talk to hundreds of MSP partners that are frustrated with their current providers. It has been very expensive to purchase a SIEM and SOAR, and to staff a 24x7 operation. At Stellar Cyber, we believe the exact opposite is true: you should not trust your customers with a third party that does not have the history or relationship with your customer that you do.

Defense in Depth has caused almost every customer to purchase a different mix of security technologies. Supporting a diverse set of technologies can be extremely costly and challenging. Many MSP and MSSP partners have standardized on a set of products their customers must purchase to get their MDR service which can lead to vendor lock-in. In today's market, that's not realistic – you are reducing your addressable market with that strategy. Customers won't readily abandon their existing investments just to purchase an MDR service.

Most MSPs find it nearly impossible to attract and hire analysts to man their SIEM, SOC, or other security tool. What many MSP partners also do not realize is that providing managed security services requires them to offer a full suite of tools, including NDR, MDR, EDR, SIEM, UEBA and TIP. Leveraging machine learning and automation in the Stellar Cyber Platform, you can provide all these services with one-third of the staff required for traditional SOC tools.

To compete in an increasingly crowded marketplace, the MSP must build a differentiated MDR service, yet the output from most SIEMs is inconsistent and generates a lot of false positives. MSSPs need a "wow" factor to succeed, and Stellar Cyber provides high-fidelity, actionable alerts that are correlated into incidents automatically. We don't stop there. The platform also includes response capabilities directly from the alert. No more logging into your customer's VPN and looking up their firewall credentials – your team will be able to not only respond manually, but to develop playbooks to respond automatically to routine threats.

Finally, to retain customers, an MSSP must prove its unique value, which is normally done through reporting. In traditional SOCs, cross-enterprise reporting is difficult because each siloed tool produces its own data formats and its own reports. By normalizing the data as we ingest it, we create a standardized record of all alerts. This data can be built into any report your customer will need with no limitations.

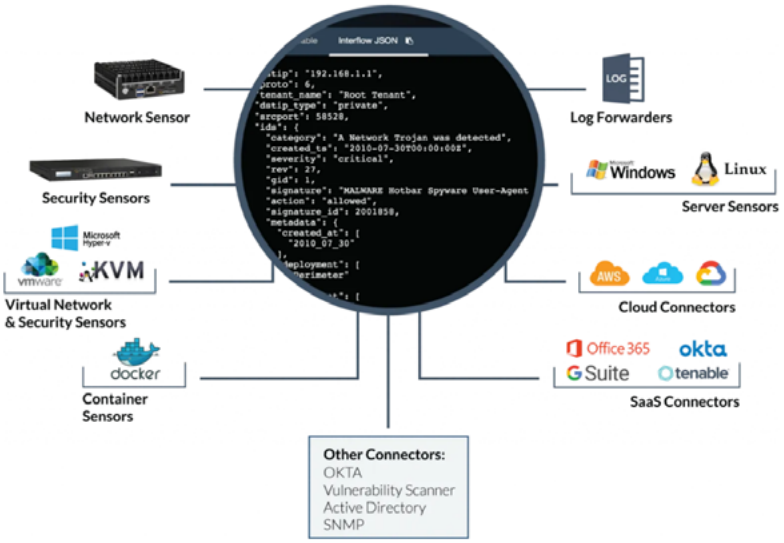
Auditors really like not having to review multiple spreadsheets.

Stellar Cyber's solution

Stellar Cyber's Open XDR platform was designed from the ground up to address these challenges by solving five key security needs: Visibility, Automated Detection, Automated Response, Comprehensive Reporting, and Cost.

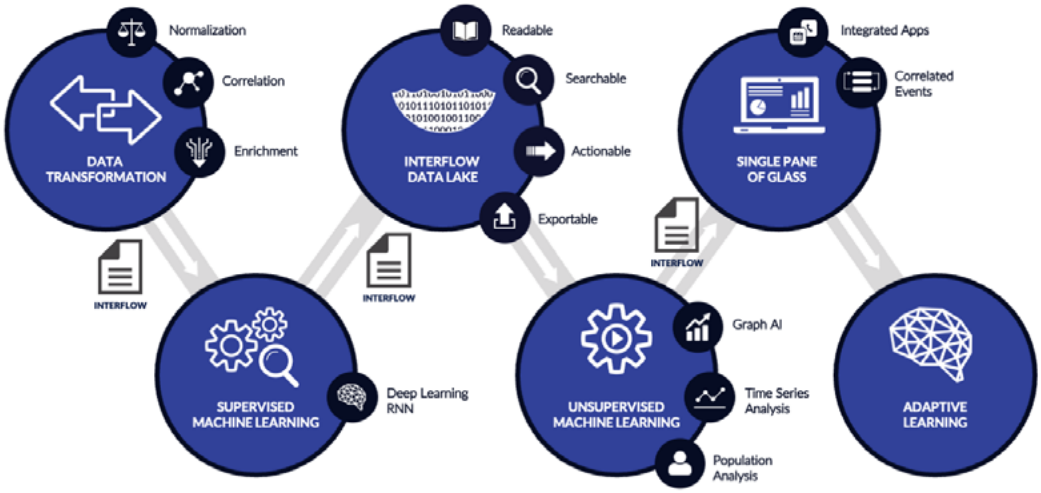
- **Visibility** – In addition to its internal capabilities (NG-SIEM, NDR, UEBA and TIP), the platform has been built with multi-level multi-tenancy from the ground up. It integrates data from other popular security tools with the goal of presenting a comprehensive picture of any organization's security posture. Collecting log data from as many sources as possible is critical to piecing together today's multi-vector attacks. Stellar Cyber does this through a family of sensors, parsers, and APIs. We have hundreds of parsers to ingest data from local devices on your customers' networks – all you need to do is configure them to send them to the correct port on the sensor.

Stellar Cyber Virtual and Physical Environments Ensuring 360-degree Visibility



- **Automated Detection** – Siloed security tools often produce logs in their own data formats, which makes analysis and reporting very difficult. The Stellar Cyber platform ingests data from all security tools and automatically normalizes that data into a standard JSON format stored in its data lake. It then automatically correlates that data to reveal complex, multi-vector attacks. Finally, it uses machine learning to automatically analyze that data against a dynamic set of rules that become more intelligent as the platform is used:
  1. Supervised Machine Learning allows you to train a detection to look for something specific like a brute-force successful login.
  2. Unsupervised Machine Learning significantly reduces the amount of time spent by analysts building custom notifications for specific customers. These models learn the normal behaviors of each tenant and the users in it – when they typically log in, which machine does the user normally logs into, where they normally log in from, and what applications we normally see them using. This allows us to detect even the most sophisticated attacks, even if they are moving low and slow within the environment.

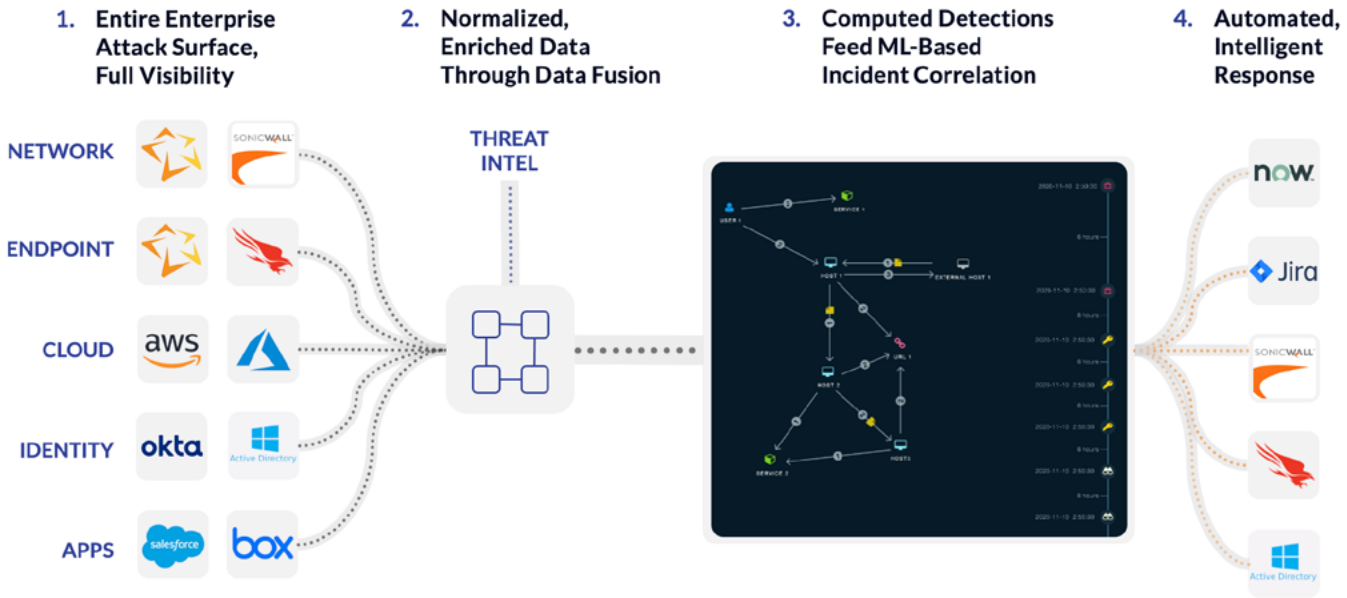
Stellar Cyber's advanced AI Engine Ensures Analysts See Context In all Security Data



3. Finally, we leverage Graph Machine Learning (GraphML) to correlate alerts into contextual, prioritized incidents. The platform scores them based on their severity and ranks them in order of severity. This helps analysts quickly focus on the things that matter the most. Stellar Cyber is the only platform currently leveraging this type of machine learning in our platform.

- **Automated Response** – The platform includes fully integrated response capabilities. First, you can take a manual response directly from the alert in our platform – setting a block rule on a firewall, for example. Normally, an analyst would need to log into their VPN and look up the credentials for the firewall to finally set the rule. In Stellar Cyber, we create an encrypted connection between the Data Processor and the Sensor on the customer's site. This allows you to send a block request from the Data Processor to the Sensor, which sends it to the firewall locally. This is significantly faster, and seconds count when there is a serious incident.

Stellar Cybers Open XDR Platform Normalizes, Enriches and Processes Data Driving Automated Incident Correlation, And Response Capability



Finally, anything we can do manually in the platform can be automated in the form of Playbooks. Anything we can detect on the platform or any detection you can dream up can be run on the data. Rules can run on your overall environment, on groups of tenants, or on individual tenants.

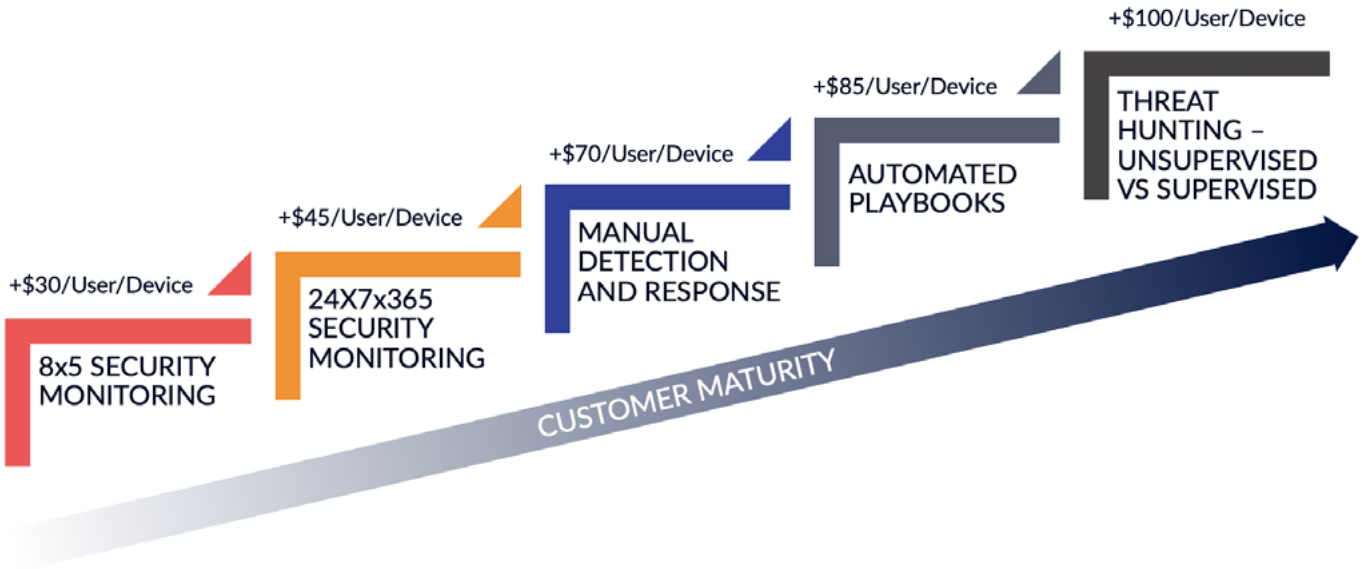
- **Reporting** – Because it normalizes all the data it ingests, the Stellar Cyber platform allows you to create any report you want within our platform. Auditors really like our platform because once we normalize the data, we can consolidate multiple spreadsheets of compliance controls into a single report.
- **Cost** – The Stellar Cyber platform is sold under a single license. It includes an NG-SIEM, NDR, UEBA, and TIP functions plus a family of four different sensors for servers, logs, networks, and security, all at a cost that's typically lower than the license for a SIEM alone.

Making the Transformation

Stellar Cyber has created a high-speed onramp to becoming an MSSP called our Jumpstart Program. We have a three-step process:

- **Step 1** – Deployment & Training – The Stellar Cyber platform can be deployed in less than an hour. Thanks to our single-console interface, most analysts can be trained on it within an hour or two. There are two simple virtual enablement courses for architects and analysts.
- **Step 2** – Onboarding Customers – The platform has built-in multi-tenant capabilities and customer templates. Once the first customer is added, you can use templates to further speed the onboarding process for successive customers. We also provide transition assistance to get your first couple of customers onto the Stellar Cyber Platform.
- **Step 3** – Matching customer services with customer maturity – less mature customers will not need the advanced features of the platform. The subscription cost per asset

Phased Approach to Building a Full SOC Service
MSP to MSSP Program: Staging the Transformation



includes all the features in the platform whether you are using them or not; there are no surprise upcharges for the advanced features in the platform. As you add more complex services, the additional amount you charge will go straight to your bottom line and more of your customers will purchase security from you.

Where to Begin?

To facilitate your business transformation from MSP to MSSP, Stellar Cyber offers its Jumpstart program, which assists you through the steps outlined above. To get started, go to https://stellarcyber.ai/partners/become-a-mssp-partner/ and click Apply Now.