SOLUTION BRIEF

SOPHOS

Stellar Cyber and Sophos

Unified Threat Detection and Response for Security Operations

Cyber threats are growing in complexity and volume, demanding a proactive and unified approach to security operations. The Stellar Cyber and Sophos integration empowers security teams with a seamless solution that combines Stellar Cyber's centralized security operations platform with Sophos' advanced endpoint protection and network firewall solutions. Together, they deliver detailed visibility, efficiency, and protection across the entire attack surface.

Key Challenges

Disjointed Tools and Data Silos: Manual correlation of data from disparate tools delays threat detection and response.

Growing Complexity in Security Operations: A fragmented approach to security increases operational overhead and risks missing critical threats.

Sophisticated and evolving threat landscape: Advanced Persistent Threats (APTs), ransomware, and phishing attacks are more sophisticated and harder to detect with isolated solutions.

Solution

The Stellar Cyber + Sophos integration delivers a unified approach to security operations by combining the strengths of both solutions:

- **Comprehensive Threat Visibility:** Sophos Endpoint and Sophos Firewall solutions feed rich telemetry into Stellar Cyber's platform, enabling a unified view of threats across endpoints and networks.
- **Advanced Threat Detection and Correlation:** Stellar Cyber's AI-driven Open XDR platform correlates threat data from Sophos technologies with other security tools, providing deep insights into attack patterns and enabling rapid response.
- **Proactive Threat Hunting and Intelligence:** Unparalleled threat intelligence from Sophos augments Stellar Cyber's capabilities, offering real-time insights into global trends to enhance threat detection and prevention.
- **Accelerated response:** The combined solution enables automated remediation actions, such as isolating endpoints or blocking malicious traffic, directly from the Stellar Cyber interface.

Benefits

- **Unified Security Operations:** A single, consolidated platform to manage threats across the entire attack surface.
- **Faster Detection and Response:** AI-driven automation reduces detection times and accelerates response to minimize attack impact.
- **Reduced Complexity:** Eliminate tool sprawl and simplify security operations with deeply integrated workflows.
- **Enhanced Threat Intelligence:** Access actionable, globally sourced insights from Sophos to stay ahead of evolving threats.
- **Scalable for All Organizations:** Tailored solutions for enterprises and MSSPs to meet the unique needs of their security operations.

Use Case Example: Detecting and Responding to Ransomware

1. Detection: Sophos Endpoint detects unusual file encryption behavior and sends an alert to Stellar Cyber's platform.

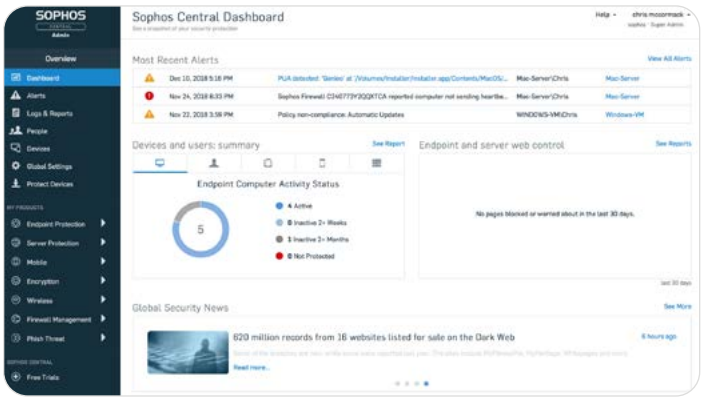
2. Correlation: Stellar Cyber correlates the endpoint alert with firewall logs and identifies lateral movement attempts within the network.

3. Response: Automated workflows isolate the affected endpoint, block malicious IP addresses, and alert the security team for further action.

4. Prevention: Threat intelligence from Sophos identifies the ransomware variant, enabling updates to defenses and proactive protection.

Why Choose Stellar Cyber + Sophos

By leveraging the power of Stellar Cyber's Open XDR platform and Sophos' cutting-edge protection technologies, organizations gain a holistic, efficient, and proactive approach to securing their environments. This integration simplifies security operations while delivering industry-leading protection against modern threats.



Get Started Today

Contact us to learn more about how the Stellar Cyber + Sophos solution can revolutionize your security operations.

- **Stellar Cyber: stellarcyber.ai**
- **Sophos:** sophos.com

About Stellar Cyber

Stellar Cyber provides a unified security operations platform, integrating data from all tools to automate and accelerate threat detection and response.

About Sophos

Sophos is a global leader in next-generation cybersecurity, delivering endpoint, firewall, and managed detection and response solutions.

Stellar Cyber's Automation-driven Security Operations Platform, including NG-SIEM and NDR and powered by Open XDR, delivers comprehensive, unified cybersecurity without complexity. It empowers lean security teams of any skill level to successfully secure their environments. As part of this unified platform, Stellar Cyber's Multi-Layer AI™ enables enterprises, MSSPs, and MSPs to reduce risk with early and precise threat identification and remediation while slashing costs, retaining investments in existing tools, and improving analyst productivity. This results in a 20X improvement in MTTD and an 8X improvement in MTTR. The company is based in Silicon Valley. For more information, visit https://stellarcyber.ai.