Sophos Intercept X

Next-Gen Endpoint Protection that defends against unknown malware, exploits and ransomware

Highlights

- Block ransomware and rolls back affected files to a safe state
- Prevents the exploit techniques used throughout the attack chain
- Stops never seen before threats with deep learning AI
- Provides 24/7 security

Introduction

Sophos Intercept X employs a comprehensive, defense in depth approach to endpoint protection, rather than relying on one primary security technique. This layered approach combines modern and traditional techniques to stop the latest cybersecurity threats. The combination of deep learning AI, anti-ransomware capabilities, exploit prevention and other techniques have built Sophos Intercept X to be one of the best endpoint detection and response solutions in the market.

Stop unknown threats

Deep learning AI excels at detecting and blocking malware by scrutinizing file attributes from hundreds of millions of samples to identify threats without the need for a signature.

Block Ransomware

Intercept X includes advanced anti-ransomware capabilities that detect and block the malicious encryption processes used in ransomware attacks.

Prevent Exploits

Anti-exploit technology stops the exploit techniques that attackers rely on to compromise devices, steal credentials and distribute malware, thus protect business against file-less attacks and zero-day exploits.

Layered Defenses

Intercept X utilizes a combination of modern and traditional techniques such as application lockdown, web control, data loss prevention and signature-based malware detection to reduce the attack surface, and provide the best defense in depth.

Optional: Extended Detection and Response (XDR)

Sophos XDR gives organizations the tools to quickly answer critical threat hunting and IT operations questions. It goes beyond traditional Endpoint Detection and Response (EDR) by integrating network, email, and cloud in addition to endpoint and server. For example, identify suspicious processes trying to connect on non-standard ports, then remotely access the device to take remedial actions or understand office network issues and which application is causing them.

Sophos Intercept X

LGA as a Managed Security Services Provider (MSSP)

As a Managed Security Services Provider (MSSP), LGA owns our very own Security Operations Centre (SOC) which runs 24/7 by our well experienced security engineers. Leveraging on the technological capabilities of Sophos Intercept X, not only do we help you in the solution setup and implementation, on top of that, we also provide you with robust 24 by 7 security monitoring, as well as timely alerting and responses to threats for your piece of mind.

FEATURES

Alert analysis	Upon detecting the alert from LGA's SIEM dashboard, LGA SOC will examine the characteristics and context of the events and incidents before reaching out to you. This can effectively minimise false positive rates and allow your IT team to focus on their core business tasks.
Email notification	Upon detection and identification of urgent threats, LGA SOC will reach out to your IT team on a 24/7 basis, to prevent any delay of response to the threats.
Threat analysis reports	Threat analysis reports will be provided for critical confirmed security events and recommendations will be provided.
Security events log	Critical security events log will be archived for 12 months for audit and compliance purposes.
8 by 5 Support	LGA will be your local point of contact to assist you on any service-related inquiries and technical issues. Tickets will be created for any service-related inquiries and technical issues can be logged on a 8/5 basis via email or telephone.

ABOUT LGA

In business for the last 25 years, LGA is one of the top B2B Services-Based Operators (SBO). LGA's Headquarters is in Singapore with a regional presence, as a System Integrator for Connectivity, CyberSecurity & Compute solutions, serving 2000 Enterprise, SME, regional and MNC customers. Our backbone is across multiple data centres, with our security and network operations team operating 24x7x365.

LGA is ISO/IEC 27001 certified and our key services include Mission-Critical Telco Diverse Circuits, Business Broadband, Cybersecurity SOCaaS, DDoS, WAF, Prevention of Confidential Data Loss security offering, Cloud Solution Provider for AWS, Azure, Co-Location, Mobile IoT and Edge Computing.

Contact Us

LGA Telecom Pte Ltd

22 Sin Ming Lane
#04-72 Midview City
Singapore 573969

Tel: (65) 6892 2308
Email: sales@lgatelecom.net
Website: www.lgatelecom.net