Intercept X

Intercept X Advanced, Intercept X Advanced with EDR, Intercept X Advanced with XDR, Intercept X Advanced with MTR

Sophos Intercept X is the world's best endpoint protection. It stops the latest cybersecurity threats with a combination of deep learning AI, anti-ransomware capabilities, exploit prevention and other techniques.

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 widest range of threats.

Stop Unknown Threats

Deep learning AI in Intercept X excels at detecting and blocking malware even when it hasn't been seen before. It does this 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. Files that have been encrypted will be rolled back to a safe state, minimizing any impact to business productivity.

Prevent Exploits

Anti-exploit technology stops the exploit techniques that attackers rely on to compromise devices, steal credentials and distribute malware. By stopping the techniques used throughout the attack chain Intercept X keeps your organization secure against file-less attacks and zero-day exploits.

Layered Defenses

In addition to powerful modern functionality, Intercept X also utilizes proven traditional techniques. Example features include application lockdown, web control, data loss prevention and signature-based malware detection. This combination of modern and traditional techniques reduces the attack surface, and provides the best defense in depth.

Synchronized Security

Sophos solutions work better together. For example, Intercept X and Sophos Firewall will share data to automatically isolate compromised devices while cleanup is performed, then return network access when the threat is neutralized. All without the need for admin intervention.

Highlights

- Stops never seen before threats with deep learning AI
- Blocks ransomware and rolls back affected files to a safe state
- Prevents the exploit techniques used throughout the attack chain
- Answers critical IT operations and threat hunting questions with EDR
- Provides 24/7/365 security delivered as a fully managed service
- See and leverage firewall, email and other data sources* with XDR
- Easy to deploy, configure and maintain even in remote working environments

**Cloud Optix and Sophos Mobile coming soon*

SOPHOS

Endpoint Detection and Response (EDR)

Designed for IT admins and cybersecurity specialists, Sophos EDR answers critical IT operations and threat hunting questions. For example, identify devices with performance issues or suspicious processes trying to connect on non-standard ports, then remotely access the device to take remedial actions.

Managed Threat Response (MTR)

24/7/365 threat hunting detection and response service that's delivered by a team of Sophos experts. Sophos analysts respond to potential threats, look for indicators of compromise and provide detailed analysis on events including what happened, where, when, how and why.

Extended Detection and Response (XDR)

Go beyond endpoints and servers, pulling in firewall, email and other data sources*. You get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail. For example, understand office network issues and what application is causing them.

Straightforward Management

Intercept X is managed via Sophos Central, the cloud-management platform for all Sophos solutions. It's a single pane of glass for all of your devices and products, making it easy to deploy, configure and manage your environment even in remote working setups.

Technical Specifications

Intercept X supports Windows and macOS deployments. For the latest information please read the Windows system requirements and Mac datasheet.

Sophos Cloud Optix and Sophos Mobile XDR integration coming soon

Licensing Overview

Features	Intercept X Advanced	Intercept X Advanced with EDR	Intercept X Advanced with XDR	Intercept X Advanced with MTR Standard	Intercept X Advanced with MTR Advanced
Foundational protection (inc. app control, behavioral detection, and more)	✓	✓	✓	✓	✓
Next-gen protection (inc. deep learning, anti-ransomware, file-less attack protection, and more)	✓	✓	✓	✓	✓
EDR (Endpoint detection and response)		✓	✓	✓	✓
XDR (Extended detection and response)			✓		See note*
Managed Threat Response (MTR – 24/7/365 threat hunting and response service)				✓	✓
MTR Advanced (Leadless hunting, dedicated contact and more)					✓

***Note:** The MTR team will have the ability to leverage XDR data and functionality for MTR Advanced customers. However, MTR customers will be limited to EDR functionality in their Sophos Central console, unless they purchase an XDR license.

Thailand : E-Rong Consultants Co.,Ltd. I Tel : 02-664-6588 I E-mail : sales@e-rong.co.th

www.e-rong.co.th
E-mail : sales@e-rong.co.th
Line official ID:@e-rongconsultants

E-Rong Consultants Co., Ltd.
THINK OF TECHNOLOGY THINK OF E-RONG