Sophos Endpoint

Prevent Breaches, Ransomware, and Data Loss

Sophos Intercept X delivers unparalleled protection against advanced attacks. It employs an extensive suite of sophisticated technologies to stop the broadest range of threats before they impact your systems. Powerful EDR and XDR tools enable your organization to hunt for, investigate, and respond to suspicious activity and indicators of attack.

Prevention-First Approach

Intercept X takes a comprehensive approach to endpoint protection without relying on one security technique. Web, application, and peripheral controls reduce your attack surface and block common attack vectors. AI, behavioral analysis, anti-ransomware, anti-exploitation, and other state-of-the-art technologies stop threats before they escalate. This means resource-stretched IT teams have fewer incidents to investigate and resolve.

Context-Sensitive Defenses

These additional dynamic defenses represent industry-first initiatives. They provide automated protection that adapts to the context of an attack. This removes the attacker's ability to operate, disrupting and containing the attack while buying valuable time to respond.

Easy to Set Up and Manage

Sophos Central is a cloud-based management platform for managing all of your Sophos products. Our recommended protection technologies are enabled by default, ensuring you immediately have the strongest protection settings with no tuning required. Granular control is also available. The Account Health Check identifies security posture drift and high-risk misconfigurations, enabling administrators to remediate issues with one click.

Synchronized Security

Intercept X shares status and health information with Sophos Firewall, Sophos ZTNA, and other products to provide additional visibility into threats and application usage. Synchronized Security will automatically isolate compromised devices while cleanup is performed and then return network access once the threat is neutralized — all without administrator intervention.

Highlights

- Stops never-before-seen threats with deep learning AI
- Blocks ransomware and rolls back affected files to a safe state
- Prevents the exploit techniques and malicious behaviors used throughout the attack chain
- Automatically adapts defenses to changing attacker behavior
- Reduces the attack surface with app, device, and web control
- Identifies security posture drift and high-risk misconfigurations with one-click remediation
- Supports threat hunting and IT ops security hygiene with EDR/XDR
- Provides 24/7/365 security delivered as a fully managed service
- Easy to deploy, configure, and maintain, even in remote work environments

SOPHOS

Block Ransomware

Intercept X includes CryptoGuard, an advanced anti-ransomware technology that stops new variants or never-before-seen ransomware. CryptoGuard inspects the contents of files to detect encryption and ransomware running on your network. Files encrypted by ransomware will be automatically rolled back to a safe state, irrespective of size or file type, minimizing the impact on business productivity.

Extended Detection and Response (XDR)

Powerful EDR/XDR functionality enables you to hunt for, investigate, and respond to suspicious activity across Sophos and third-party security controls. Threat hunt across the Sophos Data Lake or pivot to a device for real-time data and up to 90 days of historical data. Get a holistic view of your organization's environment enriched with Sophos X-Ops threat intelligence for threat detection, investigation, and response designed for dedicated SOC teams and IT admins.

Prevent Exploits

Anti-exploitation technology stops the techniques that attackers rely on to compromise devices, steal credentials, and distribute malware. Sophos deploys novel on-device anti-exploitation approaches at scale for all applications. Straight out of the box, Intercept X builds on the basic protection available in Microsoft Windows, adding no fewer than 60 proprietary, pre-configured, and tuned exploit mitigations. Intercept X protects against fileless attacks and zero-day exploits by stopping the techniques used throughout the attack chain.

Managed Detection and Response (MDR)

Sophos MDR is a fully managed threat hunting, detection, and incident response service that integrates with Sophos and third-party security controls, providing a dedicated 24/7 security team to detect and neutralize the most sophisticated and complex threats.

Licensing Overview

Features	Intercept X Advanced	Intercept X Advanced with XDR	Intercept X Advanced with MDR Complete
Next-Gen Threat Protection Web protection, deep learning anti-malware	✓	✓	✓
Malicious Activity Blocking and Context-Sensitive Defenses Anti-ransomware protection, anti-exploitation technology, Adaptive Attack Protection	✓	✓	✓
Threat Exposure Reduction Web control, peripheral control, application control, DLP, Account Health Check	✓	✓	✓
Detection and Response (EDR/XDR) Suspicious activity detection, threat hunting, investigation tools, response actions		✓	✓
Managed Detection and Response Fully managed 24/7 threat hunting, detection, and incident response			✓

Try it now for free

Register for a free 30-day evaluation at sophos.com/intercept-x

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

23-09-07 DS-EN (DD)

SOPHOS