

Sophos Endpoint

Prevent Breaches, Ransomware, and Data Loss



Sophos Intercept X is the industry's most sophisticated endpoint security solution, offering multiple layers of security for unparalleled protection against advanced attacks. It employs a comprehensive defense-in-depth approach that stops the broadest range of threats before they impact systems. Powerful EDR/XDR tools enable IT and security teams to hunt, investigate, and respond to threats.

Use Cases

1 | PREVENTION-FIRST APPROACH

Desired Outcome: Stop more threats upfront to minimize risk and reduce investigation and response workload.

Solution: Intercept X takes a comprehensive approach to protecting all endpoints and does not rely on any single security technique. Web, application, and peripheral controls reduce the attack surface and block common attack vectors. AI, behavioral analysis, anti-ransomware, anti-exploitation, and other state-of-the-art technologies stop threats fast before they escalate.

2 | STREAMLINED MANAGEMENT

Desired Outcome: Focus on threat prevention, detection, and response instead of administration.

Solution: Sophos Central is a cloud-based management console where customers manage all Sophos products and hunt for and investigate threats. Strong default policy settings ensure customers immediately have the recommended protection settings without additional training or tuning. The Account Health Check within Sophos Central helps identify and address security issues.

3 | CONTEXT-SENSITIVE DEFENSES

Desired Outcome: Defenses that automatically adapt as an attack evolves.

Solution: When Intercept X detects a hands-on-keyboard attack, it automatically activates extra defenses on the endpoint with a "shields up" approach to stop the attack from proceeding. Adaptive Attack Protection blocks suspicious activities like downloads of remote admin tools, giving your team valuable time to respond.

4 | DETECTION AND RESPONSE

Desired Outcome: Detect and respond to threats that can't be addressed through protection alone.

Solution: Powerful EDR/XDR functionality enables customers to hunt, investigate, and respond to suspicious activity across Sophos and third-party security controls. Examples include data exfiltration and silent adversaries who don't use malicious code. Customers without the resources to manage security in-house can engage Sophos MDR for 24/7 threat detection and response delivered by an elite team of experts.

Gartner®

A Leader in the Magic Quadrant for Endpoint Protection Platforms for 13 consecutive reports

SE Labs

Industry-leading protection results in independent third-party testing



Best Endpoint Security in the CRN Tech Innovators Awards (July 2023)

Learn more and try Sophos Intercept X:
sophos.com/endpoint