SOPHOS
Cybersecurity made simple.

Intercept X Advanced with EDR

Intelligent Endpoint Detection and Response

Sophos Intercept X Advanced with EDR integrates intelligent endpoint detection and response (EDR) with the industry's top-rated malware detection, top-rated exploit protection, and other unmatched endpoint protection features.

Highlights

- EDR combined with the strongest endpoint protection
- Deep Learning Malware Analysis
- On-demand curated threat intelligence from SophosLabs
- Machine learning detection and prioritization of suspicious events*
- Guided investigations make EDR approachable yet powerful
- Respond to incidents with a single click

EDR Starts with the Strongest Protection

To stop breaches before they start, prevention is crucial. Intercept X consolidates unmatched protection and endpoint detection and response into a single solution. This means that most threats are stopped before they can ever cause damage, and Intercept X Advanced with EDR provides additional cybersecurity assurance with the ability to detect, investigate, and respond to potential security threats.

The inclusion of EDR into a consistently top-rated endpoint protection suite enables Intercept X to significantly lighten the EDR workload. The more threats that are prevented, the less noise that is created for security teams to investigate. This means teams can optimize key resources enabling them to focus on the business of IT rather than chasing false positives and an overwhelming volume of alerts.

Add Expertise, Not Headcount

Intercept X Advanced with EDR replicates the tasks normally performed by skilled analysts, so organizations can add expertise without having to add staff. Unlike other EDR solutions which rely on highly skilled human analysts to ask questions and interpret data, Intercept X Advanced with EDR is powered by machine learning and enhanced with curated SophosLabs threat intelligence.

Security expertise*: Intercept X Advanced with EDR puts security expertise into the hands of IT by automatically detecting and prioritizing potential threats. Using machine learning, suspicious events are identified and elevated as the most important and in need of immediate attention. Analysts can quickly see where to focus their attention and understand which machines may be impacted.

Malware expertise: Most organization rely on malware experts that specialize in reverse engineering to analyze suspicious files. Not only is this approach time consuming and difficult to achieve, but it assumes a level of cybersecurity sophistication which most organizations don't possess. Intercept X Advanced with EDR offers a better approach by leveraging Deep Learning Malware Analysis which automatically analyzes malware in extreme detail, breaking down file attributes and code and comparing them to millions of other files. Analysts can easily see which attributes and code segments are similar to "known-good" and "known bad" files so they can determine if a file should be blocked or allowed.

Threat intelligence expertise: When Intercept X Advanced with EDR elevates a potentially suspicious file, IT administrators can gather more information by accessing on-demand threat intelligence curated by SophosLabs which receives and processes approximately 400,000 previously unseen malware samples each day. This, and other threat intelligence is collected, aggregated, and summarized for easy analysis. This means that teams that do not have dedicated threat intelligence analysts, or access to expensive and hard to understand threat feeds, can benefit from one of the top cybersecurity research and data science teams in the world.

Guided Incident Response

Intercept X Advanced with EDR allows administrators to answer the tough questions about security incidents by providing visibility into the scope of an attack, how it started, what was impacted, and how to respond. Security teams of all skill levels can quickly understand their security posture thanks to guided investigations which offer suggested next steps, clear visual attack representations, and built-in expertise.

When an investigation is concluded, analysts can respond with a click of a button. Rapid response options include the ability to isolate endpoints for immediate remediation, clean and block files, and create forensic snapshots.

Intelligent EDR Use Cases

Intelligent endpoint detection and response means that security teams have the visibility and expertise they need to answer the tough questions that are asked as part of an incident response effort.

Answer the tough questions about an incident:

- Understand the scope and impact of security incidents
- Detect attacks that may have gone unnoticed
- Search for indicators of compromise across the network
- Prioritize events for further investigation
- Analyze files to determine if they are a threat or potentially unwanted
- Confidently report on your organization's security posture at any given moment

Beyond EDR

To stop the widest range of threats, Intercept X Advanced with EDR employs a comprehensive defense-in-depth approach to endpoint protection rather than simply relying on one primary security technique. This is the "the power of the plus" – a combination of leading foundational and modern techniques. Intercept X Advanced with EDR integrates the industry's top-rated malware detection, top-rated exploit protection, and intelligent endpoint detection and response (EDR).

Modern techniques include deep learning malware detection, exploit prevention, and anti-ransomware specific features. Foundational techniques include antivirus, behavior analysis, malicious traffic detection, data loss prevention, and more.

Intercept X Advanced with EDR combines endpoint detection and response capabilities with the modern features in Intercept X and the foundational techniques in Sophos Central Endpoint Protection. This is delivered as a single solution, in a single agent.

	Sophos Intercept X Advanced with EDR	Sophos Intercept X Advanced	Sophos Intercept X	Sophos Endpoint Protection
Foundational techniques	✓	✓		✓
Deep learning	✓	✓	✓	
Anti-exploit	✓	✓	✓	
CryptoGuard anti-ransomware	✓	✓	✓	
Endpoint detection and response (EDR)	✓			

Try it now for free

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

* Available early 2019

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

18-10-02 DS-NA (3098-DD)

SOPHOS