SOPHOS
Cybersecurity evolved.

virtue TECHNOLOGIES

Intercept X Advanced with EDR

Endpoint Detection and Response built for threat hunting and IT operations
Sophos Intercept X Advanced with EDR consolidates powerful endpoint detection and response (EDR) with unmatched endpoint protection. Hunt threats to detect active adversaries, or leverage for IT operations to maintain IT security hygiene. When an issue is found remotely, respond with precision.

Highlights

- EDR combined with the strongest endpoint protection
- Designed for security analysts and IT administrators
- Proactively maintain IT hygiene and hunt threats before damage occurs
- Ask any question about what has happened in the past, and what is happening now
- Out-of-the-box, fully customizable SQL queries
- Up to 90 days fast access to current and historical on-disk data
- Remotely respond with precision using a command line tool
- Detect, investigate, and prioritize incidents with the aid of machine learning
- Speed up investigations and reduce attacker dwell time
- Available for Windows, MacOS*, and Linux

EDR starts with the strongest protection

To stop breaches before they start, prevention is crucial. Intercept X consolidates the world's best endpoint protection and EDR into a single solution. This means that most threats are stopped before they can ever cause damage. 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. As more threats are prevented, less noise is created, which prevents analysts from wasting time chasing false positives and an overwhelming volume of alerts.

Add expertise, not headcount

Automatically detect, prioritize, and investigate threats using artificial intelligence: Intercept X Advanced with EDR leverages machine learning to automatically detect and prioritize potential threats. If a potentially malicious file is discovered, users can leverage deep learning malware analysis to automatically analyze malware in extreme detail, breaking down file attributes and code and comparing them to millions of other files.

Out-of-the-box queries designed for practitioners, by practitioners: Security analysts and IT administrators can start using Sophos EDR on day one thanks to out-of-the box SQL queries categorized by use case. Queries can easily be edited for custom searches, built from scratch, or sourced from our community.

Answer the tough questions by replicating the roles of hard-to-find analysts: Intercept X Advanced with EDR replicates the tasks normally performed by skilled analysts, so organizations can add expertise without having to add staff.

Built for threat hunting and IT operations

Sophos Intercept X Advanced is the first EDR solution designed for IT administrators and security analysts. It allows you to ask any question about what has happened in the past, and what is happening now on your endpoints. Hunt threats to detect active adversaries, or leverage for IT operations to maintain IT security hygiene. When an issue is found remotely, respond with precision. This is achieved by leveraging two key features: Live Discover and Live Response.

**Coming soon*

Live Discover: Ask any question to stay ahead Live Discover gives security analysts and IT admins the ability to ask, and answer, almost any question they can think of across their endpoints and servers. Quickly discover IT operations issues to maintain IT hygiene and ask detailed questions to hunt down suspicious activity. Live Discover uses powerful, out-of-the-box, fully-customizable SQL queries that can quickly search up to 90 days of current and historical on-disk data. Example use cases include:

IT operations

- Why is a machine running slowly? Is it pending a reboot?
- Which devices have known vulnerabilities, unknown services, or unauthorized browser extensions?
- Are there programs running that should be removed?
- Is remote sharing enabled? Are unencrypted SSH keys on the device? Are guest accounts enabled?
- Does the device have a copy of a particular file?

Threat hunting

- What processes are trying to make a network connection on non-standard ports?
- List detected IoCs mapped to the MITRE ATT&CK framework
- Show processes that have recently modified files or registry keys
- Search details about PowerShell executions
- Identify processes disguised as services.exe

Live Response: Remotely respond with precision When issues are discovered, Live Response provides users command line access to endpoints and servers across their organization's estate. Remotely access devices to perform further investigation or remediate any issues. Administers can reboot devices, terminate active processes, run scripts, edit configuration file, install/uninstall software, run forensic tools, and more.

Managed detection and response

The Sophos Managed Threat Response (MTR) service provides 24/7 threat hunting, detection, and response delivered by a team of Sophos experts as a fully managed service. While other managed detection and response (MDR) services simply notify you of attacks or suspicious events, with Sophos MTR, your organization is backed by an elite team of threat hunters and response experts who take targeted actions on your behalf to neutralize even the most sophisticated threats. Customers who choose to leverage Sophos MTR also receive Intercept X Advanced with EDR.

	Sophos Intercept X Advanced with EDR	Sophos Intercept X Advanced	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

virtue TECHNOLOGIES

Call: 01695 731 233
Email: sales@virtuetechnologies.co.uk

20-05-12 DS-NA (MP)

SOPHOS