Sophos EDR and XDR

Intercept X Advanced with XDR, Intercept X Advanced with EDR, Intercept X Advanced for Server with XDR, Intercept X Advanced for Server with EDR

Intercept X 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. Sophos XDR extends visibility beyond the endpoint with rich data sources including endpoint, server, firewall and email.

Answer IT operations and threat hunting questions

Quickly get answers to business-critical questions. Both IT admins and cybersecurity professionals will see real value added when they are performing day-to-day IT operations and threat hunting tasks.

Start with the best protection

Intercept X stops breaches before they can start. Which means you get better protection and spend less time investigating incidents that should have been automatically stopped. You also have access to detailed threat intelligence giving you the necessary information to take rapid, informed actions.

Dive into the details and respond fast

When you have identified something that requires further investigation you can pivot from the Sophos Data Lake and deep dive to get rich details live, directly from the device in addition to up to 90 days of historic data. When an issue is confirmed remotely access the device and take any necessary actions such as uninstalling an application and rebooting.

Cross-product visibility

Sophos XDR goes beyond the endpoint and server, enabling Sophos Firewall, Sophos Email and other data sources* to send key data to the Sophos Data Lake, giving you an incredibly broad view of your organization's environment.

Get information even when a device is offline

The Sophos Data Lake, a key component of both XDR and EDR functionality is a cloud data repository. It enables the ability to store and access critical information from your endpoints, servers, firewall and email, as well as utilizing device information even when that device is offline.

Get started in seconds

Choose from a library of pre-written SQL queries to ask a wide variety of IT and security questions. If you prefer you can customize them or write your own. You can also refer to the Sophos community where queries are shared on a regular basis.

Highlights

- Answer business critical IT operations and threat hunting questions
- Designed for IT admins and security analysts
- Remotely take remedial actions on devices of interest
- Get a holistic view of your organizations' IT environment and drill into granular detail when needed
- Leverage endpoint, server, firewall, email and other data sources*
- Out-of-the-box, fully customizable SQL queries
- Available for Windows, macOS* and Linux

**Cloud Optix and Sophos Mobile coming soon*

**XDR capabilities coming to macOS soon*

SOPHOS

EDR and XDR use cases

	IT Operations	Threat hunting
EDR	➦Why is a machine running slowly? ➦Which devices have known vulnerabilities, unknown services or unauthorized browser extensions? ➦Are there programs running that should be removed?	➦What processes are trying to make a network connection on non-standard ports? ➦Show processes that have recently modified files or registry keys ➦List detected IoCs mapped to the MITRE ATT&CK framework
XDR	➦Identify unmanaged, guest and IoT devices ➦Why is the office network connection slow? Which application is causing it? ➦Look back 30 days for unusual activity on a missing or destroyed device	➦Extend investigations to 30 days without bringing a device back online ➦Use ATP and IPS detections from the firewall to investigate suspect hosts ➦Compare email header information, SHAs and other IoCs to identify traffic to a malicious domain

XDR customers have access to all EDR functionality and use cases

What's included?

	Endpoint Detection and Response (EDR)	Extended Detection and Response (XDR)
Cross-product data sources		✓
Cross-product querying		✓
Endpoint & server querying	✓	✓
Sophos Data Lake	✓	✓
Data lake retention period	7 days	30 days
On-disk data retention period	✓	✓
SQL query library	✓	✓
Intercept X protection capabilities	✓	✓

For further details on licensing please see the Intercept X and Intercept X for Server license guides.