

What's New in Sophos XDR and EDR 4.0

Intercept X and
Intercept X for Server



SOPHOS
Cybersecurity evolved.

This release brings powerful cross-product insight with Extended Detection and Response (XDR), the ability to query offline devices with the Sophos Data Lake and some of the top requested Endpoint Detection and Response (EDR) features.

Sophos XDR - Extended Detection and Response

Go beyond the endpoint and server by integrating important network data to build up an in-depth picture of potential threats across your estate. In this first release of XDR, detailed intelligence from Sophos Firewall and Sophos Email is available in addition to endpoint and server data, with more products being added over time. As standard 30 days of cloud data storage is included, ideal for investigations and tracking back an issue to its root cause. Sophos XDR capabilities are a paid for upgrade.

Use cases include:

- ▶ **Understand your entire environment**
See contextual information from your endpoints, servers and firewall in one place, making it easy to see the complete picture and take action. You can quickly compare indicators of compromise from multiple data sources to understand a suspected attack, drilling down for granular detail and taking any necessary actions.
- ▶ **Hunt down network threats**
Use detailed network information to identify threats. For example, use ATP and IPS detections to investigate suspect hosts and activity. Use blocked malicious traffic events to understand a wider attack campaign
- ▶ **Identify unmanaged devices**
Firewall data enables admins to pinpoint unmanaged, guest and IoT devices across their organization's environment

[See more XDR and EDR use cases.](#)

Offline Access via the Sophos Data Lake

A key component of both XDR and EDR, the Sophos Data Lake stores critical data from Intercept X, Intercept X for Server, Sophos Firewall and Sophos Email and enables access to that data even when devices are offline. For example, look back 30 days for unusual activity on a device that has been destroyed or taken without authorization. It's an important part of cybersecurity visibility giving organizations the ability to see their entire environment and quickly drill down to granular detail in areas of interest. Data retention periods are 7 days (EDR) and 30 days (XDR). This is in addition to the current 90 days of retention available on the device.

Cross-product querying

Quickly move between data sources to answer critical questions. For example, use firewall data to identify suspicious activity, then seamlessly switch to investigating the suspect endpoint to confirm the issue and take any required actions.

Scheduled Queries

Have critical information waiting for you. Schedule queries to run overnight so key data is there when you are ready to go. Note that initially scheduled queries are available for data lake queries only, device data will follow soon.

Enhanced Usability

Work even faster with enhancements to workflow and pivoting that help users get key information and take action even more quickly.

Coming Soon

Sophos Mobile and Cloud Optix will soon be sending data into the Sophos Data Lake giving XDR users access to rich mobile and cloud environment data.

EDR vs XDR – what's included?

Feature	Endpoint Detection and Response (EDR)	Extended Detection and Response (XDR)
Cross-product data sources e.g. Firewall, Email		✓
Cross-product querying		✓
Sophos Data Lake	✓	✓
Sophos Data Lake retention period	7 days	30 days
On-disk data retention period	90 days	90 days
Scheduled queries	✓	✓
Live Discover (SQL querying for threat hunting and IT operations)	✓	✓
Live Response (remote terminal access)	✓	✓