Sophos XDR

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

Intercept X is the industry's only XDR solution that synchronizes native endpoint, server, firewall, email, cloud and O365 security. Get a holistic view of your organization's environment with the richest data set and deep analysis for threat detection, investigation and response for both dedicated SOC teams and IT admins.

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.

Know where to focus

Hone in on the important issues with a prioritized list of suspicious detections and vulnerable configurations that includes key information for further investigation. Choose from a library of pre-written templates to ask a wide variety of IT ops and threat hunting questions or create your own.

Minimize investigation and response time

AI-guided investigations enable you to quickly understand the scope and cause of an incident and minimize time to respond. Access devices for real-time state and up to 90 days of historic data or 30 days historic data in the data lake.

Cross-product visibility

Get maximum visibility of your organization with native integration of Intercept X, Intercept X for Server, Sophos Firewall, Sophos Email, Sophos Mobile, Cloud Optix and Microsoft Office 365 data.

Multi-platform, multi-OS support

Inspect your environment whether in the cloud, on-premises or virtual across Windows, macOS, Linux, Amazon Web Services, Microsoft Azure, Google Cloud Platform, and Oracle Cloud Infrastructure deployments.

Highlights

- Answer business critical IT operations and threat hunting questions
- Leverage a prioritized list of detections and AI-guided investigations
- Remotely take remedial actions on devices of interest
- Get a holistic view of your organizations' IT environment and drill into granular detail when needed
- Native endpoint, server, firewall, email, cloud, mobile and O365 integrations
- Access a library of pre-written, customizable template use cases

SOPHOS

Use cases

IT Operations

- 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?
- 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
- Locate mobile devices that are unpatched or have out of date software

Threat hunting

- 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
- 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
- Identify users with multiple failed authentication attempts

What's included?

	Extended Detection and Response (XDR)
Cross-product data sources	✓
Cross-product detection, investigation & response	✓
Prioritized detections list & AI-guided investigations	✓
Sophos Data Lake	✓
Data lake retention period	30 days
Real-time state information	✓
On-disk data retention period	Up to 90 days
Threat hunting & IT ops template library	✓
Intercept X protection capabilities	✓

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

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

© Copyright 2022. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

22-01-06 DS-NA (MP)

SOPHOS

Authorized Distributor :

SecureOne
Optimize with SECURITY

HQ Office (KL)
SecureOne Distribution Sdn Bhd (828358 - X)
No.7, Jalan 109E, Desa Business Park,
Taman Desa, Jalan Kelang Lama,
58100 Kuala Lumpur, Malaysia.

Tel: +6(03) 7984 6086 Fax: +6(03) 7984 6032
Email: sales@secureone.com.my

Northern Office
SecureOne Distribution (Northern) Sdn Bhd (977172 - H)
1A-2-02 @ One Precint (1160),
Lengkok Mayang Pasir,
11950 Bayan Baru, Penang, Malaysia.

Tel: +6(04) 619 2692 Fax: +6(04) 619 2699
Email: northern@secureone.com.my

www.secureone.com.my