SOPHOS XDR | SOPHOS MDR

Solution Integrations

SOPHOS

Visibility Across All Key Attack Surfaces

SOPHOS
✓ Integrations included

- Ep Endpoint
- WP Workload
- Mob Mobile
- Cld Cloud
- Fw Firewall
- Em Email
- ZT ZTNA
- NDR Network

Endpoint
✓ Included

Microsoft, CROWDSTRIKE, SentinelOne, TREND MICRO, Symantec by Broadcom (beta), BlackBerry CYLANCE (beta)

+ Others with Sophos XDR sensor agent

Firewall

Barracuda, paloalto NETWORKS, FORTINET, CHECK POINT, CISCO Meraki, f5, Forcepoint, SONICWALL, WatchGuard

Network

DARKTRACE, THINKST CANARY, CISCO Umbrella, Skyhigh Security, Secutec, VECTRA (beta), zscaler

Email

Microsoft 365 ✓ Included

Google Workspace ✓ Included

mimecast

proofpoint.

Productivity
✓ Included

Microsoft 365

Google Workspace

Cloud

orca security

+ AWS, Azure, and GCP integrations with Sophos Cloud Optix product

aws

Identity

Microsoft ✓ Included

okta, auth0, CISCO DUO, CISCO ISE, ManageEngine

Backup and Recovery

Acronis, rubrik, veeam

Sophos Endpoint and Sophos Workload Protection solutions are included with Sophos XDR and MDR. Other Sophos integrations require an applicable subscription for the Sophos product.

Third-party Endpoint, Microsoft, and Google Workspace integrations are included with Sophos XDR and MDR subscriptions at no additional charge. Integration Packs for other non-Sophos solutions are available as add-on subscriptions for each integration category. Licensing is based on the total number of users and servers.

Updated December 20, 2024

Included Integrations

Sophos XDR

The only XDR platform that combines native endpoint, server, firewall, cloud, email, mobile, and third-party integrations.

Sophos Firewall

Monitor and filter network traffic to stop threats before they have a chance to cause harm. Xstream Protection subscription required.

Microsoft Security Suite

- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Microsoft Entra ID Protection
- Microsoft 365 Defender
- Microsoft Purview DLP
- Office 365 Management Activity

Sophos Endpoint

Endpoint Prevention and EDR that stop advanced threats and detect malicious behaviors—including attackers mimicking legitimate users.

Sophos Network Detection and Response

Continuously monitor activity inside your network to detect suspicious actions and lateral attacker movement.

Google Security Suite

- Google System Defined Rules
- Suspicious Activities
- Malware and Phishing
- User and Device Activity
- Alert Center
- Authentication
- Access Control
- Data Control

Sophos Cloud Optix

Stop cloud breaches and gain visibility across your critical cloud services, including AWS, Azure, and Google Cloud Platform.

Sophos Email

Protect your inbox from malware and benefit from advanced AI that stops targeted impersonation and phishing attacks.

Third-Party Endpoint Protection

Compatible with...

- Microsoft
- CrowdStrike
- SentinelOne
- Symantec (Broadcom)
- Trend Micro
- BlackBerry (Cylance)

+ Other solutions with the Sophos XDR sensor agent

Includes 90 days of data retention

Add-Ons

Firewall

Compatible with...

- Barracuda
- Check Point
- Cisco
- F5
- Forcepoint
- Fortinet
- Palo Alto Networks
- SonicWall
- WatchGuard

Identity

Compatible with...

- Auth0
- Cisco ISE
- Duo
- ManageEngine
- Okta

Microsoft integration included

Cloud

Compatible with...

- Orca Security

Integrations with AWS, Azure and GCP are available via the Sophos Cloud Optix product, sold separately

Network Security

Compatible with...

- Cisco Umbrella
- Darktrace
- Secutec
- Skyhigh Security
- Thinkst Canary
- Vectra
- Zscaler

Email

Compatible with...

- Mimecast
- Proofpoint

Microsoft 365 and Google Workspace integrations included

Backup and Recovery

Compatible with...

- Acronis
- Rubrik
- Veeam

Data retention

1-year retention add-on

Sophos Managed Risk

Powered by Tenable

Add-on service for Sophos MDR

Integration Packs and the Data Retention Pack are available for Sophos MDR and Sophos XDR. All Integration Packs are licensed based on the total number of Sophos MDR/XDR seats (users+servers).
Sophos Managed Risk is available as an add-on service for Sophos MDR only.

SOPHOS