SOPHOS

Sophos Cloud Optix FAQs

Sophos Cloud Optix agentless, SaaS-based service combines deep security expertise with the power of artificial intelligence. It delivers cloud security monitoring, analytics, and compliance automation with one simple-to-use interface in a process-efficient way.

This FAQ document provides a comprehensive overview of Sophos Cloud Optix:

- Product overview
- Setup and management
- Data
- Contracting
- 30-day free trial

Product Overview

What is Sophos Cloud Optix?
Sophos Cloud Optix is a cloud security posture management solution that protects organizations from the next generation of public cloud cyberattacks and compliance penalties.

The agentless SaaS solution provides security, operations, development, and compliance teams with a focused console, automatically identifying potential security gaps before they are exploited, and active threats within public cloud environments.

Protecting Kubernetes clusters, Amazon Web Services, Microsoft Azure, Google Cloud Platform, and Infrastructure-as-Code environments, Cloud Optix augments data obtained via native cloud provider APIs and log information with artificial intelligence, analyzing these environments to identify a range of threats.

What key components of cyber risk are addressed by Cloud Optix?
The threats addressed by Cloud Optix include resource misconfigurations, abnormal login behavior suggesting stolen credentials, over-privileged user and service roles, suspicious API calls, abnormal network traffic suggesting potential data exfiltration, and cloud spend anomalies. Cloud Optix has the potential to significantly reduce the likelihood of unauthorized cloud account access, data breaches, cryptojacking, and regulatory compliance failures.

What are the mechanics and output of Cloud Optix, including characteristics such as expected impact, efficacy, and accuracy?

The Ponemon Institute's 2018 Cost of a Data Breach Study: Global Overview revealed the estimated average cost of a security breach at $3.86 million, with a 27.9% likelihood of a recurring breach in the following two years. Sophos Cloud Optix utilizes industry-accepted standards to harden public cloud environments against cyberattacks.

Certified by the Center for Internet Security (CIS) in both level 1 and 2 benchmark profiles for AWS, Azure, and Google Cloud Platform, Cloud Optix continually assesses public cloud and Kubernetes environments based on best practices for secure configuration. Cloud Optix detects cloud resource misconfigurations and security vulnerabilities in near-real time, and continually monitors architecture changes to stay ahead of attacks. It hardens security posture with guardrails to prevent and automatically remediate accidental or malicious changes in resource configuration. This gives organizations potential to significantly reduce the likelihood of breaches in the first year and beyond when maintained by the security team.

Accuracy of Cloud Optix findings is ensured by accessing cloud environment information via the cloud provider APIs and through environment log data. The service collects information from connected cloud environments using two communication channels: infrastructure metadata is collected periodically using a "pull" channel, and log information is collected in near-real time using a "push" channel.

Infrastructure metadata includes inventory information about cloud resources, such as instances/VMs, storage buckets, and security groups, and their associated security states. Log information includes, for example, AWS CloudTrail and VPC/network flow logs.

Security monitoring scans for compliance failures and misconfigurations can be scheduled to meet the needs of individual organizations and teams. This includes REST API-driven scans during build pipeline processes with DevOps, and both on-demand and scheduled scans of live infrastructure. These can be set as intervals (every 30 minutes, or every one, two, six, 12, or 24 hours). Alternatively, scans can be scheduled to only run during specific time of the day. Network flow log data and activity log data for AI-based anomaly detection is sent to the Cloud Optix service in near-real time.

What are the common use cases Sophos Cloud Optix enables?

Increase visibility

- Get real-time inventory of assets deployed across multiple clouds and accounts
- Network topology visually displays application architecture and traffic flows
- Actionable insights with contextual security alerts leads to faster and more accurate incident response
- Continuously monitor multi-cloud infrastructure and resources to detect threats and remediate

Continuous compliance

- Continuously ensure cloud infrastructure adheres to company security best practices
- Out-of-the-box policies continuously assess and report on cloud infrastructure, with contextual information that allows the organization to take appropriate action. Policies include CIS (Center of Internet of Security), PCI, HIPAA, SOC2, GDPR, FedRamp, and others
- Instantly benchmark the compliance policy framework against the actual implementation with customizable dashboards and exportable reports

Add security to DevOps practices

- Establish guardrails to prevent, detect, and remediate accidental or malicious changes in network configuration, network traffic, resource configuration, and user behavior or activities
- Integration with third-party security tools, such as SIEM and DevOps tools for CI/CD results in simplified security operations
- Orchestrate compliance processes using third-party integrations with tools like Jira and ServiceNow to manage compliance-related workflows

What third-party integrations does Sophos Cloud Optix support?

- **Jira issue tracking system** – Create Jira tickets for new Sophos Cloud Optix alerts. This is a two-way integration whereby an existing Jira ticket for the same type of issue is updated if present before a new one is created
- **Slack team collaboration tool** – Push new Sophos Cloud Optix alerts into a specific slack channel for instant notification
- **ServiceNow IT workflow management system** – Create ServiceNow tickets for new Sophos Cloud Optix alerts. This is a two-way integration whereby an existing ServiceNow ticket for the same type of issue is updated if present before a new one is created
- **Splunk SIEM** – Send all new Sophos Cloud Optix alerts and/or dashboard access logs for your company into Splunk
- **Pager Duty incident response solution** – Push new Sophos Cloud Optix alerts into Pager Duty
- **AWS GuardDuty threat detection service** – Aggregate AWS GuardDuty alerts into the Sophos Cloud Optix dashboard regardless of region. When turned on, other enabled integrations (e.g. Jira, Slack, ServiceNow) to automatically work for GuardDuty alerts as well

Are security and compliance policies provided with the solution, or do I to create these?

Sophos provides the following policies by default and plans to add additional policies over time (policy availability varies for each cloud platform):

- CIS Benchmarks
- FedRamp
- FFIEC
- HIPAA
- PCI DSS
- SOC2
- GDPR

Setup and Management

How long does initial setup take?
The Sophos Cloud Optix solution requires no agents, so the initial setup consists of connecting the Sophos Cloud Optix SaaS management console to your public cloud accounts. This is done using provided scripts which take only a few moments to run. These scripts set up read-only access by default and once run, useable information showing inventory and topology should start showing in the console within 10 minutes.

Are there any prerequisites required before connecting Sophos Cloud Optix to a cloud provider account?
To onboard a cloud environment, Sophos Cloud Optix requires that the provided scripts be run to create a read-only connection. The exact permissions needed vary by cloud provider but generally admin-level permissions are needed so that the scripts can properly execute.

How do I access the Cloud Optix management console?
Sophos Cloud Optix can be purchased directly through Sophos or via AWS Marketplace. The option chosen will determine the URL used to access the Cloud Optix console.

- If purchased through Sophos, Cloud Optix accounts can be managed via the Sophos Central console at https://central.sophos.com/manage/login
- If purchased via AWS Marketplace, Cloud Optix accounts can be managed via the dedicated console at https://optix.sophos.com.

Is there an API?
Yes, Sophos Cloud Optix provides access via a secure REST API, which can be used to add IPs to the whitelist, get alert information, and to gather details on outgoing traffic.

What permissions are needed by the solution?
By default, read-only access is configured by the installation scripts, which then allow Sophos Cloud Optix to query a cloud environment to assess inventory, security, and compliance posture, and to receive event and flow logs for analysis. The optional remediation mode for AWS environments requires additional permissions, which are contained within the script provided. Please review the onboarding scripts for exact details.

Data

What information is stored by Sophos Cloud Optix?
To enable you to log into the Sophos Cloud Optix console, Sophos collects and stores your email address in a database using industry-standard AES 256 encryption. You can choose to sign up using Google single sign-on authentication or create a password for Sophos Cloud Optix. If you create a password to log into Sophos Cloud Optix, it is hashed using bcrypt. If you use Google single sign-on authentication, Google may send information to Sophos such as your name, email address, and profile picture associated with your Google account.

Note: Customers can improve the security of their Sophos Cloud Optix account by enabling multi-factor authentication (MFA) using Google Authenticator.

To use the service, you need to connect one or more cloud environments to Sophos Cloud Optix (e.g. Amazon Web Services account, Microsoft Azure subscription, Google Cloud Platform project). By connecting a cloud environment, you explicitly authorize Sophos to access information via APIs and to collect log data. Data is transferred from the customer's cloud environment to Sophos Cloud Optix in two ways. Infrastructure metadata is 'pulled' from the environment by using the cloud platform's APIs (for example, using AWS SDK). Network flow logs and usage logs are 'pushed' by a serverless function (e.g. AWS Lambda) in the customer's cloud environment, to Cloud Optix log collectors. In both cases, the data transfer uses TLS encryption. Full details of the data collection channels can be found in the Sophos Cloud Optix online help.

Infrastructure metadata includes inventory information about your cloud resources, such as instances/VMs, storage buckets, and security groups, and their associated security states. Log information includes, for example, AWS CloudTrail and VPC/network flow logs. These logs may include information about an IAM user who accessed and/or made changes to the infrastructure (e.g. IAM user "JDoe" created a new VM instance). In addition, these logs may include information about which IP address is communicating with another IP address, on which port, using which protocol (E.g. 1.1.1.1 to 2.2.2.2 on port 80 via tcp). All infrastructure metadata and log information collected by the service is stored using industry-standard AES 256 encryption. You can remove a cloud environment from your Sophos Cloud Optix account at any time. All associated infrastructure metadata and log information will be deleted automatically.

Sophos Cloud Optix also offers optional third-party integrations, for example Slack, Jira, ServiceNow, PagerDuty, and Splunk. Credentials that you provide in order to use these integrations are stored using AES 256 encryption.

Contracting

Does an authorized Sophos reseller or distributor need to do anything new or sign a new agreement to resell/distribute Sophos Cloud Optix?
Managed Service Providers must accept the MSP Connect 2019 agreement to resell Cloud Optix.

Apart from this, a reseller is able to resell, and a distributor is able to distribute, the Sophos Cloud Optix service as part of the normal Sophos GA portfolio, and under the existing reseller/distributor agreement terms.

Does the existing Sophos End User License Agreement ("EULA") apply to Sophos Cloud Optix?
No, the Sophos Cloud Optix service is governed by a Sophos Cloud Services Agreement ("CSA"), which is available at https://www.sophos.com/en-us/legal.aspx along with the EULA.

30-Day Free Trial

Are free trials available for Sophos Cloud Optix?
Yes, customers and partners can sign up for a free no-obligation trial via Sophos.com.

Where can customers and partners sign up for a free trial?
Visit Sophos.com/cloud-optix and click on any free trial link in this area to sign up for a free trial. There will also be a link to sign up for a free trial of Sophos Cloud Optix in the Free Trials area of Sophos Central.

How long does a Cloud Optix free trial last?
Free trials of Sophos Cloud Optix are 30 days. A banner in the Cloud Optix console will count down the number of days remaining.

Are all features available during a free trial?
Yes. The free trial allows customers and partners to try out the full capabilities of Sophos Cloud Optix.

Do customers need to add their own environments to their free trial account?
Yes. To try out the Sophos Cloud Optix product, the customer will need to onboard their own Amazon Web Services (AWS) accounts, Microsoft Azure subscriptions, or Google Cloud Platform (GCP) projects. If the customer or partner would prefer to see Cloud Optix in action without onboarding their own environments, they can use the public demo available via Sophos.com.

Are there any Terms and Conditions for free trials?
Yes. Terms and Conditions regarding trials/evaluations are included in the Sophos Cloud Services Agreement that the customer will need to agree to when signing up for a trial.

What happens at the end of the free trial?
To continue using Sophos Cloud Optix after a 30-day free trial, customers must purchase a subscription. After 30 days, if the customer has not purchased a subscription, features may be deactivated and the customer's data will be deleted from the service.

For more information visit sophos.com/cloud-optix.

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

2020-05-11 FAQ (PC)