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 an AI-powered, next-generation cloud infrastructure security platform. It delivers continuous security monitoring, compliance, analytics, and remediation across multiple public cloud accounts and multiple public cloud platforms.

How does the solution work?
Sophos Cloud Optix is an agentless SaaS solution that integrates with customer cloud infrastructure accounts using the native cloud provider APIs, logs, and cloud services. Information from these sources are used to provide the customer with a detailed inventory of all assets in the cloud account and provide an intuitive topological view of the environment's architecture and traffic flows.

This information is also matched against both out-of-the-box and customer-created policies to provide ongoing security and compliance assessments, which then result in configurable alerts and auditor-ready reports. The solution also features integrations with third-party operations and security team tools such as JIRA and Splunk. This allows for proactive scanning of developer-provided Infrastructure as code templates, sourced from locations such as Github, Terraform, and Bitbucket.

What specific challenges does Sophos Cloud Optix address?

- **Perimeter-based security tools and policies alone are inadequate**
  Public cloud environments have eliminated the traditional perimeter in some cases and created multiple perimeters in others.

- **DevOps practices break traditional security processes**
  Agile development requires production changes on a daily basis, and a small security oversight can leave sensitive data exposed, resulting in ransomware and data breaches.

- **Cybersecurity attacks have become highly sophisticated**
  Hackers are using intelligent bots to attack, affecting companies of all shapes and sizes.

- **Cloud security is a shared responsibility**
  The cloud providers are responsible for security "*of* the cloud," i.e. the infrastructure. But companies are responsible for security "*in* the cloud," which includes rapidly changing configurations, network security, user access, data security, and application security.

- **There is a severe shortage of talent with cloud security skills**
  It is costly and time-consuming to identify, hire, and retain data scientists and security experts who can build sophisticated AI-powered tools to prevent intelligent attacks.

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 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?

No, 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 (note, however, that Cloud Optix is not integrated into Central at this time; Sophos Central will not show that a Cloud Optix trial is in progress).

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