SOPHOS

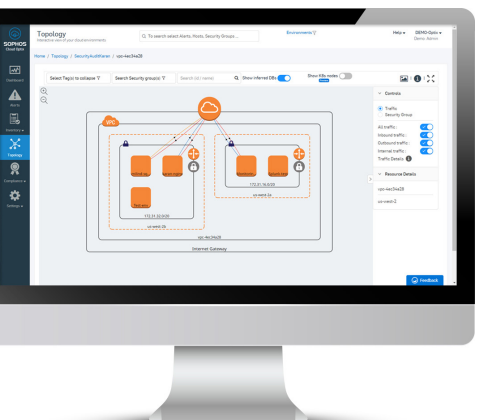
Sophos Cloud Optix

Solve the toughest challenges in cloud security

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

Highlights

- Agentless, SaaS-based service setup in minutes
- Inventory management across multiple-cloud providers
- Complete network topology and traffic flow visualization
- AI-based user behavior and traffic anomaly detection
- Continuous compliance assessments
- Range of out-of-the-box compliance policies
- Alert correlation for faster remediation
- Detect changes to critical settings
- Continuously scan Infrastructure-as-Code templates



See everything, secure everything

Automatic discovery of your organization's assets across Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) environments, giving your team the power to respond to and remediate security risks in minutes – with continuous asset monitoring and complete network topology and traffic visualization, including ingress, egress, and internal traffic.

Proactive cloud compliance

As workloads move to the cloud, identifying which compliance processes will be applicable – not to mention how they'll be implemented – becomes even more difficult. Cloud Optix reduces the cost and complexity of governance, risk, and compliance with out-of-the-box templates, custom policies, and collaboration tools.

Speed up the compliance process

Continuously monitor compliance with custom or out-of-the box templates for standards such as CIS, GDPR, SOC2, HIPAA, ISO 27001, and PCI DSS.

Collaboration made easy

Manage and track compliance to ensure important tasks are never lost, even during a release, using third-party integrations with tools like JIRA and ServiceNow.

AI-powered security analytics and monitoring

Cloud Optix is continuously monitoring and learning about your cloud asset inventory, configurations, and network traffic. AI-powered smart alerts reduce response times and help remediate security risks faster with automated alert ranking combined with contextual information.

- Continuously monitor cloud asset inventory (S3 Buckets, Security Groups, user access key etc.), configurations, and Security Group logs
- Identify anomalous user behavior patterns to detect advanced automated attacks due to stolen user access keys or rogue employees
- Predict how network traffic may flow based on your security settings – preventing potential breach points before attacks start
- Establish guardrails to prevent, detect, and remediate accidental or malicious changes in network configuration

Smarter DevSecOps

The rapid pace of Infrastructure-as-Code changes due to continuous deployment and DevOps practices allows new software to be released multiple times a day. This puts a tremendous amount of pressure on security teams that could leave you exposed. Cloud Optix API-driven architecture enables your DevOps teams to seamlessly integrate security with their DevOps processes – ensuring fast and secure delivery.

Drift detection and guardrails

Continuously monitor and detect drift in configuration standards and prevent changes to critical settings that could leave your organization exposed to security vulnerabilities.

Proactive infrastructure template scanning

Continuously scan Infrastructure-as-Code templates deployed from solutions such as Terraform, Github, or Bitbucket. Identifying mis-configurations that could result in the provisioning of vulnerable infrastructure.

SIEM and DevOps tool integration

Integrate with third party security tools such as SIEM and DevOps tools for CI/CD to simplify security operations.

Simplify management and deployment

Cloud Optix agentless, SaaS-based service works perfectly with your existing business tools.

Connection to cloud accounts in AWS, Azure, or GCP is a simple process due to the provided instructions and scripts, which create Read Only access via the native cloud APIs. Connections can be set up in minutes, and once deployed, Cloud Optix is able to immediately start assessing your cloud environment and providing you valuable information.

Cloud security is a shared responsibility

Public Cloud providers offer a great deal of platform flexibility. But while they're responsible for physical protection at the datacenter, virtual separation of data and environments, whatever you put in the cloud is your responsibility to secure.

With Cloud Optix providing continuous visibility, compliance, and threat response, find out more about the complete range of Sophos public cloud workload protection and next-gen firewall solutions at sophos.com/public-cloud.

Sophos Cloud Optix features	
Single pane of glass across multiple clouds	✓
Topology visualization	✓
Network traffic visualization overlay	✓
Security Group visualization overlay	✓
Anomaly detection – network traffic	✓
Anomaly detection – user login behavior	✓
Inventory – hosts, networks, storage, I AM	✓
Inventory – AWS CloudTrail	✓
Inventory – serverless	✓
Continuous compliance assessments	✓
Compliance policies (CIS, FEDRAMP, FFIEC, GDPR, HIPAA, ISO 27001, PCI DSS 3.2, SOC2, EBU R 143)	✓
CIS benchmark policies	✓
Custom policies	✓
Compliance/best practice alerting and reporting	✓
Remediation and guardrails	✓
DevSecOps script assessment	✓

* Features may vary across AWS, Azure, and GCP platforms, contact us for further details.

Demo or try it now for free

All Cloud Optix features free for 30 days
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

2019-04-11 DS (PC)

SOPHOS