

Sophos Cloud Security Posture Management

Sophos Cloud Optix, the Sophos Cloud Security Posture Management solution, proactively reduces business risk from unsanctioned activity, vulnerabilities, and misconfigurations across Amazon Web Services [AWS], Microsoft Azure, and Google Cloud Platform public cloud environments.

Complete Cloud Security Posture Management

Sophos Cloud Optix provides a complete picture of cloud resources across multi-cloud environments. Monitoring costs, detecting insecure configurations and deployments, access anomalies, over-privileged IAM roles, and compliance failures from development to the ongoing security of live services.

Identify and Respond to Threats Faster

Focus on and fix your most critical security vulnerabilities before they are identified and exploited in cyberattacks. By identifying and risk-profiling security, compliance, and cloud spend risks, Cloud Optix ensures teams respond faster, providing contextual alerts that group affected resources with detailed remediation steps.

Security at The Pace of DevOps

Block vulnerabilities in container images and infrastructure-as-code templates pre-deployment with Cloud Optix. Seamlessly integrate Sophos security and compliance checks at any stage of development to maintain the pace of DevOps without introducing threats into production environments.

Manage Permissions Before They're Exploited

Cloud Optix analyzes complex, interwoven Identity and Access Management (IAM) roles to visualize relationships, making it simpler to manage access privileges for user, group and cloud service roles. Guiding you on where to make IAM policy updates with the cloud provider before over-privileged IAM access is exploited.

Reduce Compliance Cost and Complexity

Sophos Cloud Optix reduces the cost and complexity of compliance with policies that automatically map to your environments, producing audit-ready reports without diverting resources from other projects. Compliance and security best practice policies include: GDPR, HIPAA, PCI DSS, SOC2, ISO27001, FFIEC, EBU R 143, FedRAMP, CIS Benchmark Level 1 and Level 2 for AWS, Azure, Google Cloud and Kubernetes.

Highlights

- Monitor AWS, Azure, Google Cloud, and Kubernetes
- Multi-cloud asset and network traffic visibility
- Risk-based prioritization of security issues with guided remediation
- Optimize spend and identify unusual activity
- Identify overprivileged user and role-based access
- Block vulnerabilities pre-deployment with DevOps integrations

Optimize Cloud Costs and Improve Security

Track cloud services side-by-side for improved visibility, receive recommendations to optimize AWS and Azure spend, and identify unusual activity indicative of abuse or account compromise.

Integrate Seamlessly

Integrate with cloud provider native services to unlock even greater value. Cloud Optix automated analysis and risk prioritization of security alerts from cloud provider services including AWS CloudTrail, Amazon GuardDuty, AWS Security Hub, Azure Sentinel and many more ensures security teams responds faster and more efficiently to events. While access to Cloud Optix features programmatically via a REST API and integration with third-party services such as SIEM and DevOps tools help to streamline security operations and improve collaboration. The full range of integrations can be found here sophos.so/cloud-integrations.

Extend your data sources with XDR

Detect AWS, Azure and Google Cloud environment API, CLI, and management console activities with Cloud Optix. Then investigate findings with additional context from Sophos

Intercept X for Server workload protection agents running on EC2 Instances and virtual machine workloads in the cloud. Requires Cloud Optix Advanced and Intercept X Advanced for Server with XDR.

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 Google Cloud is a simple process due to the provided instructions and scripts which create read-only access via the native cloud APIs.

The Sophos Cloud Security Platform

Cloud Optix is part of Sophos Central, a single intuitive hybrid cloud security management platform to enable your digital transformation. Our award-winning solutions are easy to deploy, manage, and are highly effective at stopping today's cyberattacks. Enabling organizations to secure cloud access, applications, and infrastructure with ease.

The World's Most Trusted Unified Cloud Security Platform

 CONNECT SECURELY	 PROTECT WORKLOADS	 SECURE THE NETWORK	 INTEGRATE WITH DEVOPS
Protect credentials and securely access services	Detect, query and secure hybrid cloud workloads	Cloud network security and automated threat response	Embed security into development processes
Secure Access	Workload Protection and EDR	Firewall, WAF and VPN	CI/CD Integration
Endpoint Security	Cloud Security Posture Management	Application Visibility	Container Image Scanning
Phishing Protection	Overprivileged IAM Role Detection	Security Automation	Threat Intelligence APIs
24/7 Threat Hunting, Detection, and Response			

Demo or try it now for free

Assess your cloud security and compliance status today at 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