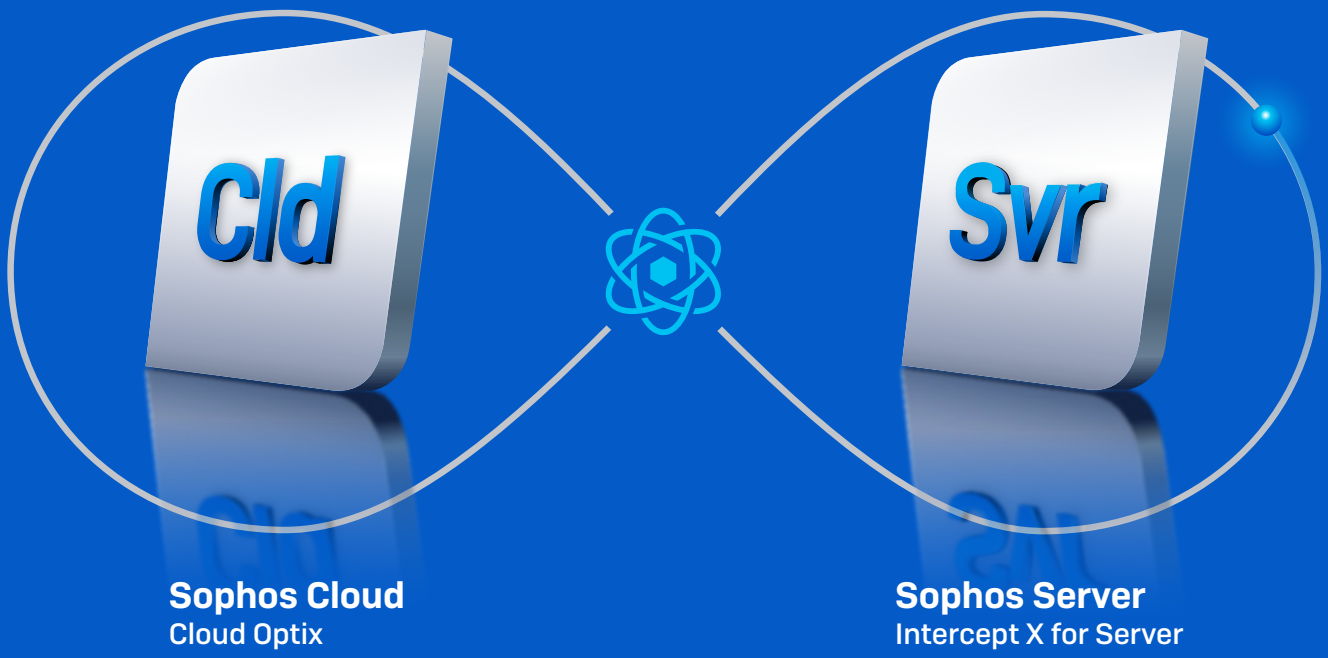
What's New in Sophos Cloud Workload Protection

Intercept X Advanced for Server now incorporates Cloud Security Posture Management



SOPHOS
Cybersecurity evolved.

Expansion of Sophos Cloud Workload Protection

This release brings an exciting expansion to Sophos Cloud Workload Protection that sees Intercept X Advanced for Server incorporate Cloud Security Posture Management with new Sophos Cloud Optix Standard capabilities. This addition extends protection beyond server workloads running in Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) to critical cloud services and provides seamless integration with Sophos server agents running in the cloud.

Sophos Cloud Optix Standard and Advanced

Sophos Intercept X Advanced for Server customers now benefit from Cloud Optix Standard CSPM capabilities, enabling security teams to focus on and proactively fix their most critical cloud security vulnerabilities before they're identified and exploited in cyberattacks.

By identifying and risk profiling cloud workload security configuration issues, suspicious access events, and unusual network traffic vulnerabilities impacting security posture. Cloud Optix Standard ensures teams respond faster, providing contextual alerts that group affected resources with detailed remediation steps.

The full Cloud Optix product is changing to Cloud Optix Advanced. This license update does not alter any of the advanced CSPM features of the previous Cloud Optix license. The update will provide a pathway for organizations using Cloud Optix Standard to the full range of security and compliance monitoring capabilities.

All Cloud Optix customers in Sophos Central now also benefit from a new seamless integration with Intercept X Advanced for Server, automatically removing servers from the Central Admin console when VMs are terminated in AWS and Azure environments.*

New features included with Intercept X Advanced for Server

Cloud Asset Inventory – View a detailed inventory of your entire cloud infrastructure (e.g. IAM roles, security groups, shared storage, databases, serverless, containers and more), eliminating the need for time-consuming manual collation across AWS, Azure, and GCP.

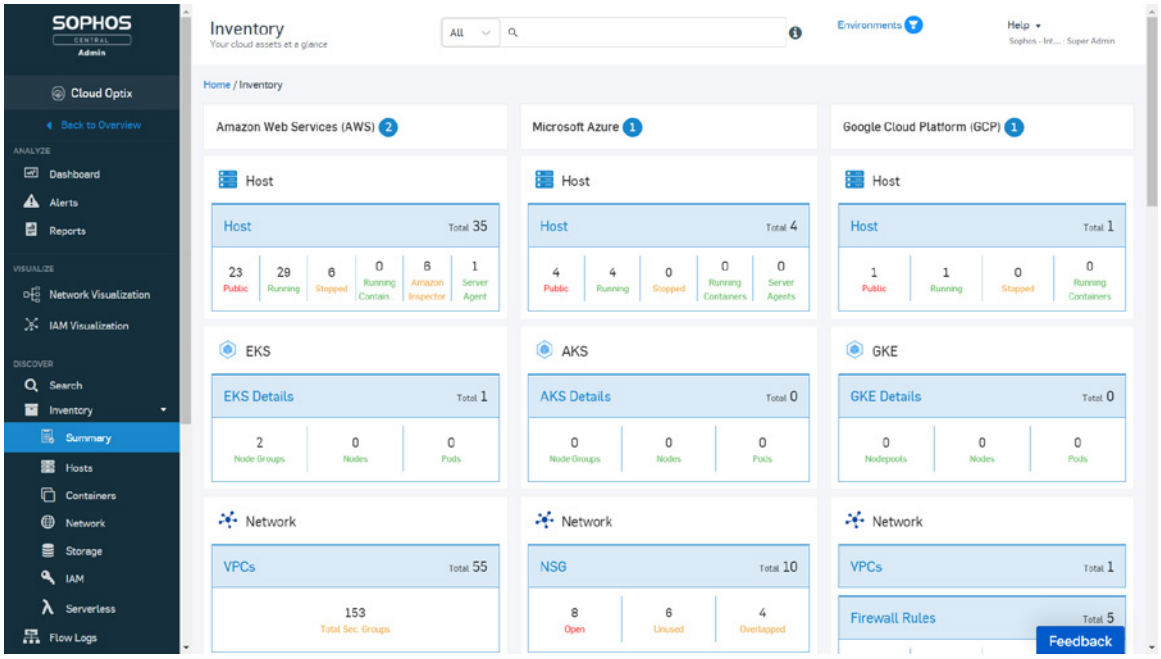
Access and Traffic Anomaly Detection – Unusual login attempts, and suspicious traffic patterns are automatically detected, and teams alerted.

Security Scans – Daily and on-demand scans monitor your cloud environment to ensure its on-going security health. Alerts are automatically prioritized by risk level, while guided response provides detailed information and instructions to resolve the issue.

Security Best Practice – Detect when cloud accounts and the configuration of deployed resources do not align to security best practices with Center for Internet Security (CIS) Benchmark policies, helping keep security posture at its best.

Alert Management Integrations – receive email notifications when manual intervention is required.

* Requires Intercept X Advanced for Server license



Comparison of Cloud Optix Standard and Advanced

Feature	**Cloud Optix Standard** Included with Intercept X Advanced for Server term licenses	**Cloud Optix Advanced**
Cloud Environments	Amazon Web Services, Microsoft Azure, Google Cloud Platform, and Kubernetes	Amazon Web Services, Microsoft Azure, Google Cloud Platform, and Kubernetes
Cloud Asset Inventory and Search	✓	✓
Intercept X Advanced for Server Integration: Agent discovery	✓	✓
Intercept X Advanced for Server Integration: Automatic agent removal from Sophos Central Admin	✓ New	✓ New
Configuration Security Scans	Daily and on-demand	Configurable and on-demand
Security and Compliance Policies	CIS Benchmarks	Compliance, Security best practices, Custom policies, Additional rules
AWS and Azure Service Integrations	✓	✓
User and Network Anomaly Detection	✓	✓
Spend Monitoring		✓
Container Image Scanning		✓ New
Network Visualization		✓
IAM Visualization		✓
Infrastructure-as-Code Scanning		✓
Rest API		✓
Alert Integrations (Jira, Slack, Webhooks, etc.)		✓
SophosLabs Malicious Traffic Alerts		✓ New
Sophos XDR Data Lake Hydration		Coming soon

A full summary of features can be found at https://www.sophos.com/en-us/products/cloud-optix/tech-specs.aspx

Frequently asked questions

Do I need to add Cloud Optix Standard to my Sophos Central account?

The experience for customers with Sophos Intercept X Advanced for Server term licenses is seamless, with these new Cloud Optix Standard capabilities automatically available in the Central Admin console for all eligible customers. Simply log into Sophos Central and select Cloud Optix from the product menu where customers will be guided through the onboarding process of public cloud environments. Sophos Cloud Optix setup is simple, with no software to install, and only 'read only' access required to safely and securely assess the security posture of the customer's cloud environments.

There are no additional costs, licenses, or license keys required to activate this new functionality. Note that this enhancement will apply to term licenses only and will not apply to MSP Flex monthly accounts.

How many Cloud Assets do I get with Cloud Optix Standard?

Nothing changes for Intercept X Advanced for Server customers. The added Cloud Optix Standard capabilities work on a 20% uplift to the server license entitlement. For example, customers with 100 Intercept X Advanced for Server licenses are given a Cloud Optix Standard entitlement to monitor 120 cloud assets.

How does Cloud Optix count cloud assets?

A cloud asset is a single virtual machine instance (including any server instance or database instance) or container image, within a cloud environment that benefits from, or whose configuration is accessed by, Sophos Cloud Optix. A full description of these assets can be found online at https://docs.sophos.com/pcg/optix/help/en-us/pcg/optix/concepts/SophosCloudOptixLicensing.html

Will Cloud Optix Standard be available separately?

Cloud Optix Standard is only available as part of the Intercept X Advanced for Server term license. This addition ensures organizations deploying Intercept X Advanced for Server licenses in the cloud build security best practices in from the outset of a cloud migration to create a secure foundation for growth. Cloud Optix Advanced is available all organizations separately.

Learn more

Learn more about Cloud Workload Protection
sophos.com/cwp

21-05-14 WP-EN (DD)

SOPHOS