

Sophos Cloud Optix

Proof of Concept Guide

Cloud  ptix

INTRODUCTION	4
Overview	4
How does Cloud Optix work?	4
Signing up for a Cloud Optix trial account	5
Logging into Cloud Optix for the first time	5
INITIAL DEPLOYMENT AND ADMINISTRATION	6
Confirming successful environment connections	7
Reviewing main dashboard features	9
Checklist	10
VISIBILITY	11
Inventory section	12
Checklist	15
Topology section	16
Show inferred databases	20
Checklist	21
CONTINUOUS SECURITY AND COMPLIANCE	22
Compliance summary dashboard	23
Policies	23
Checklist	26
Reports	27
Checklist	29

RESPONSE	30
Guardrails	32
Checklist	33
Alerts correlation and remediation	33
Alert types	37
Checklist	40
PROOF OF CONCEPT TESTING FRAMEWORK	41
Day one activities	41
Day two-ten activities	42
Day 10-20 activities	43
DAY 30 PROOF OF CONCEPT REVIEW	43

Introduction

This guide has been designed to help customers get the most out of their Cloud Optix POC testing. In this guide, we'll provide a brief overview of Cloud Optix, define its three-pronged approach to security and compliance in the public cloud, and detail suggested configuration options to show the true value of the solution.

At the end of the guide we've also included a suggested testing framework which can be used by Sophos Sales Engineer and partner teams to help customers test during the 30-day trial period.

For more information on Cloud Optix or to view resources such as guides, datasheets, videos, whitepapers, and an FAQ, please visit the Cloud Optix landing page at <https://www.sophos.com/en-us/products/cloud-optix.aspx>. For any questions on this guide or for sales or technical questions, please reach out to the Sophos Public Cloud team using our team alias publiccloud@sophos.com.

Overview

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.

VISIBILITY	COMPLIANCE	RESPONSE
If you can't see it, you can't secure it	Ever-changing, auto-scaling environments	Complex attacks but limited resources
Real time inventory of all assets Network and traffic flow visualization Anomaly detection	Continuous GRC monitoring Compliance policy customization Auditor ready reports	Guardrails Alert correlation and remediation Proactive template scanning

How does Cloud Optix 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.

Signing up for a Cloud Optix trial account

Cloud Optix trial accounts are available for 30 days and provide access to the full functionality available in the solution. Trials are easy to start, do not require the installation of any software, and by default use 'Read Only' access to safely and securely gather information from customers AWS, Azure, or GCP environments. If you have not yet started your 30-day free trial of Cloud Optix, please visit <https://sophos.com/cloud-optix> and click on any free trial link in this area.

Logging into Cloud Optix for the first time

Once signed up for a Cloud Optix account, customers will log in to their management console using the Cloud Optix console URL:
<https://optix.sophos.com>.

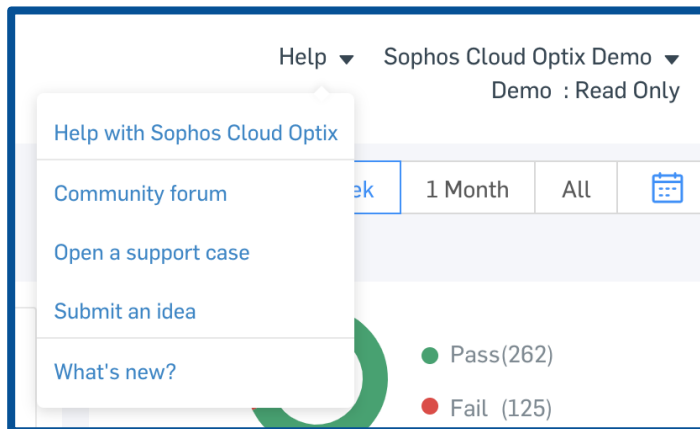
Initial deployment and administration

This section should help you understand the value of Cloud Optix features as they relate to multi-account and multi-cloud environments and demonstrate how Cloud Optix administrative features can help with day-to-day management of the overall cloud infrastructures security posture. Some questions to consider:

1. What type of cloud accounts are in use across the organization – AWS, Azure, GCP?
2. Is [Kubernetes](#) being used currently, or does the organization have plans to use it to help orchestrate and manage their containers?
3. How easy it is to determine when changes are being made to these environments, and what those changes are?
4. Is just a single team responsible for deploying, managing, securing, and ensuring compliance of workloads deployed into the cloud? Or do multiple teams participate in these activities?

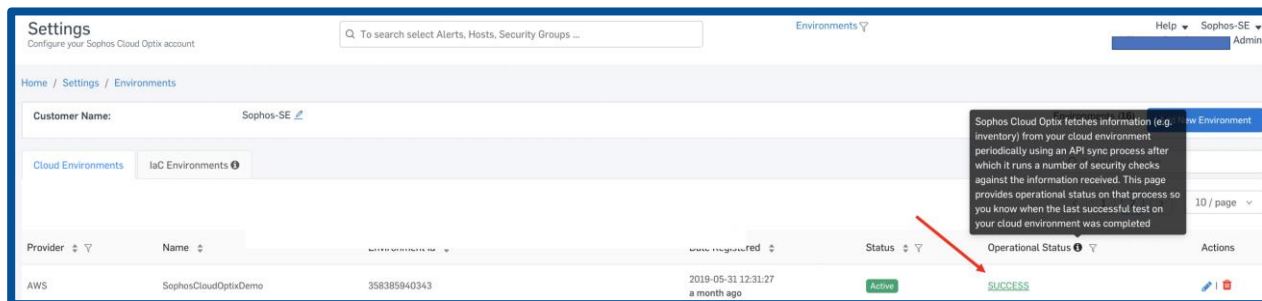
Upon initial login, the Cloud Optix console will be empty, with connections to cloud [environments](#) required before Cloud Optix can start showing its value. It's suggested that multiple cloud environments be configured, using multiple cloud providers so that you can see the importance provided by the single pane of glass view.

Detailed information on adding each environment type, as well as how Cloud Optix [gathers it's data](#) and what [permissions](#) are needed, is available in the Cloud Optix help documentation, which can be accessed by clicking on the inline 'Help' icon located in the upper right corner of the Optix console, or by navigating directly to the URL <https://docs.sophos.com/pcg/optix/help/en-us/index.html>.

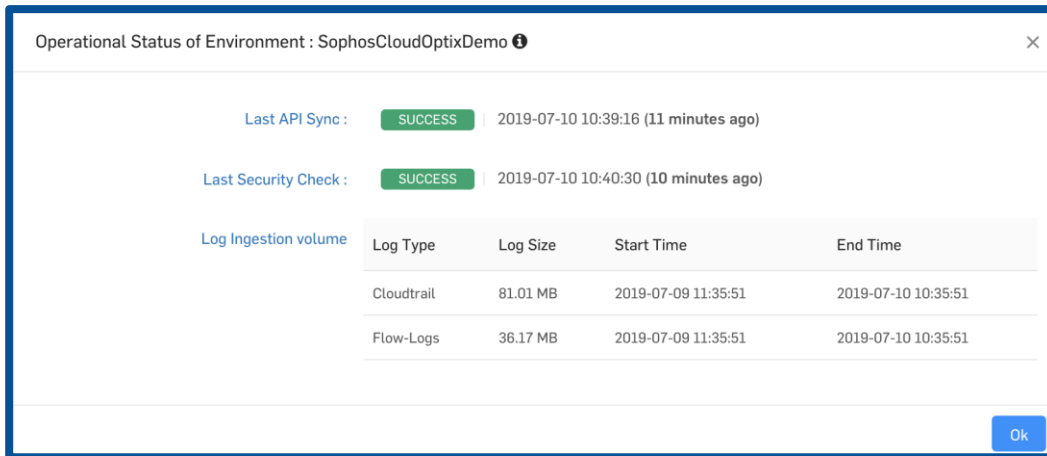


Confirming successful environment connections

Once environments are added, Cloud Optix begins the process of syncing and running an initial security check or assessment using the built-in policies found in the [Compliance](#) section. To ensure that the connection has succeeded, and that both the 'API Sync' and 'Security Check' are functioning as expected, navigate to the **Settings>Environments** section to view the status of all connections. **Click on the status link shown under the 'Operational Status' column** to view the details about the connection.



Both the API sync and Security Check indicators should show success, though it will typically take between 15-30 minutes for the first success notifications to appear.



Operational Status of Environment : SophosCloudOptixDemo

Last API Sync : **SUCCESS** | 2019-07-10 10:39:16 (11 minutes ago)

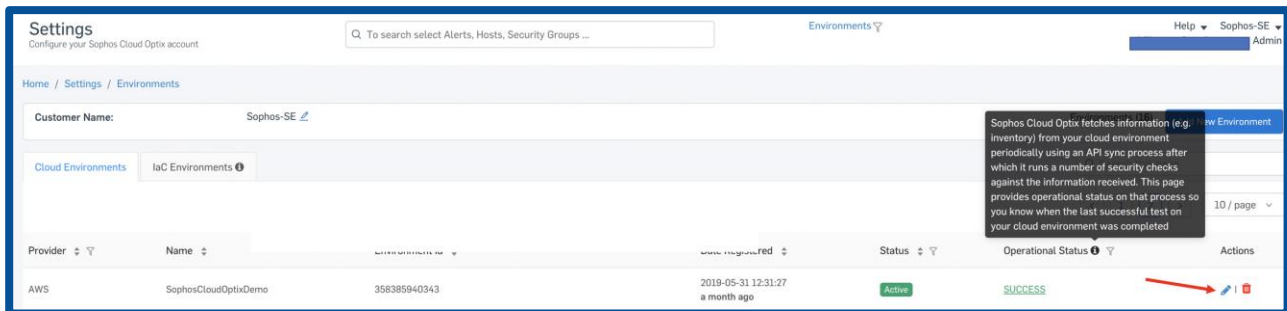
Last Security Check : **SUCCESS** | 2019-07-10 10:40:30 (10 minutes ago)

Log Ingestion volume

Log Type	Log Size	Start Time	End Time
Cloudtrail	81.01 MB	2019-07-09 11:35:51	2019-07-10 10:35:51
Flow-Logs	36.17 MB	2019-07-09 11:35:51	2019-07-10 10:35:51

Ok

Note that on the far right of your environment connection there are two icons. The trashcan icon is used to **Delete** your environment. The pencil icon is used to **Edit**.





Settings

Configure your Sophos Cloud Optix account

Environments

Customer Name: Sophos-SE

Cloud Environments

Provider	Name	Account ID	Created	Status	Operational Status	Actions
AWS	SophosCloudOptixDemo	358385940343	2019-05-31 12:31:27 a month ago	Active	SUCCESS	 

Sophos Cloud Optix fetches information (e.g. inventory) from your cloud environment periodically using an API sync process after which it runs a number of security checks against the information received. This page provides operational status on that process so you know when the last successful test on your cloud environment was completed.

Editing your environment allows you to change the Optix account **Name**, the **API**, and **Security Check** scan period, and it also allows you to provide additional permissions to Cloud Optix. These additional permissions are needed if you wish to provide Cloud Optix the ability to **remediate** issues for you, either manually or automatically. Those options are described in more detail in later sections.

Settings
Configure your Sophos Cloud Optix account

Home / Settings / Environments / 358385940343

Edit Environment

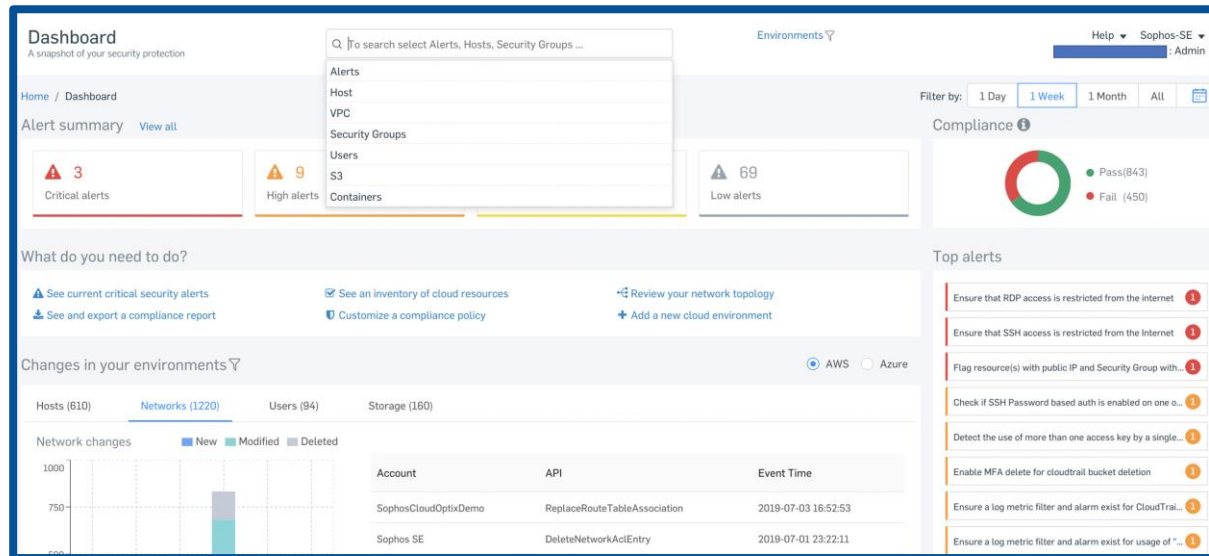
Cloud Provider	AWS
Environment Name	SophosCloudOptixDemo
Environment Id	358385940343
Scan frequency	Every 30 minutes
External Id	7e1507cb-e389-43d4-bbad-1a495f6d938d
Role ARN	arn:aws:iam::358385940343:role/Av
Remediate Role ARN	
Remediate External Id	
Status	Active

[Click here](#) for the instructions to generate the "Remediate Role ARN" and "Remediate External Id" via automated script.

Reviewing main dashboard features

Once a cloud environment connection has been configured, it will usually take between 15- 30 minutes for information to start populating to the Cloud Optix console. Once information appears you can use it to start familiarizing yourself with the easy-to-use main dashboard, which features filter and search options, alert summary information, quick links to common administrative tasks, change log information, a compliance status indicator, and a top alerts summary. While waiting, you may want to review the short videos available on the [Cloud Optix home page](#), as they contain useful information on Cloud Optix capabilities as well as an explanation of the public cloud shared security model.

Sophos Cloud Optimx: Proof of Concept Guide



Checklist

Please read the below checklist and ensure that all items have been reviewed.

DESCRIPTION	VALUE PROVIDED	COMPLETE?
Successfully add cloud account(s).	Single pane of glass view across all cloud environments.	
Review Dashboard – Changes in your environments; note values for new, modified, and deleted; review for host, networks, users, and storage.	Quick summary highlights most important items to look at first in terms of security, compliance, and changes to environments.	
Filter on different time periods.	View posture at different time periods to gauge progress or to support incident investigation.	
Filter on one or more cloud environments.	Different teams may be responsible for different cloud accounts/providers.	
Review quick links in 'What do you need to do?' section.	Intuitive UI eases administration.	
Review search box options.	Quickly find resources using intelligent search options.	

Visibility

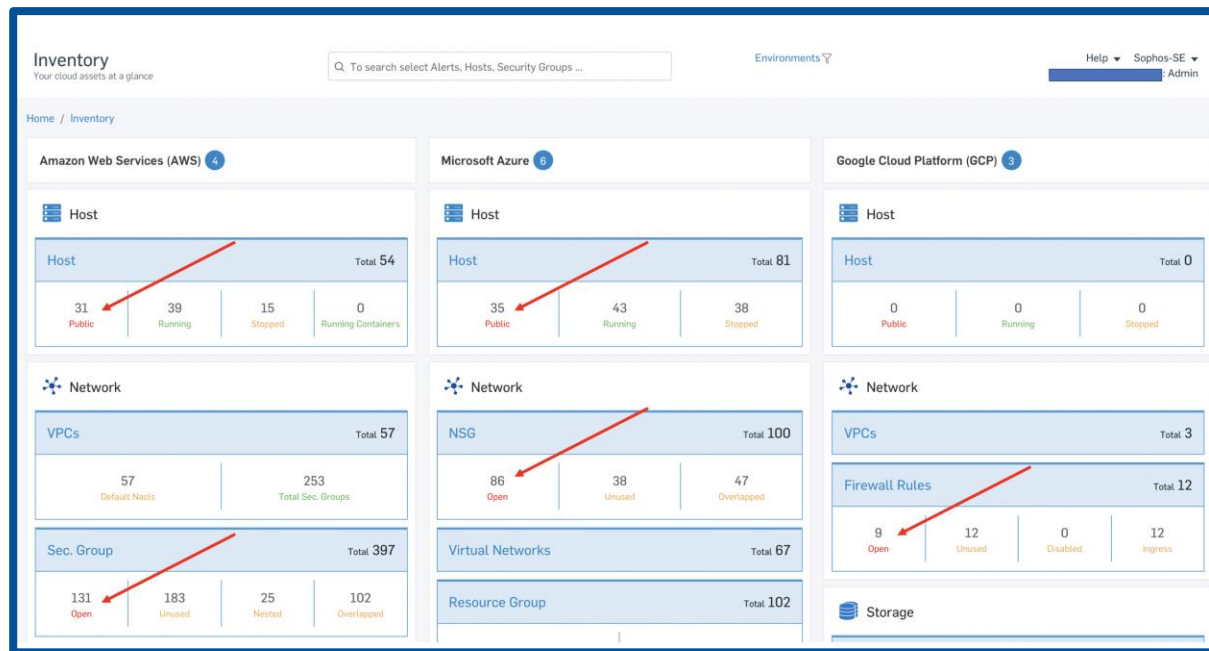
Visibility is one of the greatest challenges in cloud security. It's common for customers to deploy workloads in multiple accounts across multiple cloud providers, and it is often difficult to determine **how the hosts supporting applications are connected to each other and to the public internet.**

The dynamic nature of the cloud, along with the ease with which resources can be deployed, make it difficult to determine where assets are deployed, how many there are, if they're in use and still needed, and who may be using them. As cloud usage grows, [security hygiene](#) is critical to ensuring that an organization is not left open to attack due to unused or improperly secured assets. Some questions to consider while exploring these features are:

1. What does your organization currently do to enforce security hygiene across all their cloud environments?
 - a. Do you audit how deployed hosts are connected to each other and to the public internet?
 - b. Do you track and delete unused security groups to reduce the attack surface?
 - c. Do you audit storage buckets to ensure they're both private and encrypted, to avoid data exploits?
 - d. Do you audit IAM users to identify changes being made, ensure MFA is used, and ensure access keys are properly rotated according to best practices?
 - e. Do you have good visibility into the use of emerging technology, such as serverless and containers services, across their cloud accounts?
2. Are you able to easily view all changes made across all accounts to spot issues and errors that could result in security incidents?
3. What tools does the organization use to visualize network topology?
4. How do you verify both real-time and potential traffic patterns?
5. How easy is it for the organization to produce accurate and up-to-date network drawings for internal or external auditors?

Inventory section

Navigate to the 'Inventory' section of Optix to view the default high level aggregated view of all currently deployed assets across connected cloud environments. Use this section to immediately identify possible security issues including misconfigurations and unused security groups, which will be color coded red.



Drill down into asset types for full information showing where it is located and all identifying information including account details, any tags, and who last touched it. For example, the below screenshot shows how we can look at just AWS accounts, and filter just on 'stopped' hosts. As part of our security hygiene exercise, we can reach out to the person that last touched this instance to see if it is still needed. If not, perhaps it makes sense to remove.

Sophos Cloud Optimx: Proof of Concept Guide

The screenshot shows the 'Inventory' page for AWS hosts. The top navigation bar includes 'Home / Inventory / Hosts - AWS'. A search bar at the top right says 'To search select Alerts, Hosts, Security Groups ...'. Below the search bar, there are filters for 'Public' (1), 'Running' (30), 'Stopped' (1), and 'Running Containers' (0). A red arrow points to the 'Stopped' filter. The main table lists hosts with columns: Name/Id, Last modified by, Environment, Size, AZ, Status, Launch Time, Security Group, Public DNS/IP, Patched, and View. The first row shows a host with ID 'i-09b1fdd5f73e87976' and status 'stopped'. Below the table, there is a 'Description' tab showing details like Account Id, Image Id, Subnet Id, VPC Id, and VPC Name.

Navigating to the **Networks>Security Groups** section gives us another example of how we can use the Cloud Optimx filters to identify unused resources. In this example we're looking at unused [Security Groups](#). Note that the Security Group view also provides an option to manually remove unused Security Groups directly from the Optimx console. To use this feature, you must first give additional [remediation rights](#) as described in the inline help and mentioned during the initial environment onboarding discussion.

The screenshot shows the 'Inventory' page for Security Groups. The top navigation bar includes 'Home / Inventory / Networks - AWS'. A search bar at the top right says 'To search select Alerts, Hosts, Security Groups ...'. Below the search bar, there are filters for 'Total' (183), 'Open' (131), 'Unused' (183), 'Nested' (25), and 'Overlapped' (102). A red arrow points to the 'Unused' filter. The main table lists Security Groups with columns: Name, Last modified by, Environment, VPC ID, Region, Instances, View, and Action. The first row shows a Security Group named 'Sophos UTM 9 Standalone or HA ...' with VPC ID 'vpc-08a91710986147b8d' and Region 'eu-west-1'. A red arrow points to the 'Action' column, which contains a trash icon for each row.

Navigating to the Networks section shows us all the information related to our cloud networks, in an easy-to-understand view. Again, **red** color-coding highlights areas of interest. In the below example, we can see that Cloud Optimx has identified the Security Groups assigned to this network as potentially containing a security issue.

Drilling down further, we can see that the problem is that the rules are configured to allow all port 22 access from any network (0.0.0.0/0). Now, there may be valid reasons to have that sensitive port open to the entire internet, but it is something that should be looked at more closely. To help with that, Cloud Optimx provides additional tools, such as a link to the associated network diagram, and the ability to view any outgoing traffic associated with this network. We'll talk a bit more about how those features can help with security as we continue exploring the functionality.

The screenshot shows the 'Inventory' page for AWS environments. The 'Security Groups' tab is active, displaying a table of security groups. A red arrow points to a rule in the 'launch-wizard-1' security group that allows TCP traffic on port 22 from the IP range 0.0.0.0/0. Another red arrow points to a 'Diagram' link in the top right corner of the table row.

Subnets	Network ACLs	Gateways	Route Tables	Security Groups																			
CloudOptimxUTM vpc-03b550163eeaeabb5	PUBLIC-CLOUD-OPTIX-DEMO-SAML-ADMIN acl-00a696cdc3b018418	SophosCloudOptimxDemo	10.90.0.0/16	us-east-1	false	launch-wizard-1 Sophos UTM 9 Standalone or HA - BYOL-9-603-AutogenByAWSMP-default	Diagram																
<table border="1"><thead><tr><th>Security Group Id: sg-01d00871a8a0a8d46</th><th colspan="3">Name: launch-wizard-1</th></tr><tr><th>Protocol</th><th>Type</th><th>Port</th><th>IP Range</th></tr></thead><tbody><tr><td>tcp</td><td>Ingress</td><td>22</td><td>0.0.0.0/0</td></tr><tr><td>All</td><td>Egress</td><td>All</td><td>0.0.0.0/0</td></tr></tbody></table>								Security Group Id: sg-01d00871a8a0a8d46	Name: launch-wizard-1			Protocol	Type	Port	IP Range	tcp	Ingress	22	0.0.0.0/0	All	Egress	All	0.0.0.0/0
Security Group Id: sg-01d00871a8a0a8d46	Name: launch-wizard-1																						
Protocol	Type	Port	IP Range																				
tcp	Ingress	22	0.0.0.0/0																				
All	Egress	All	0.0.0.0/0																				

Checklist

Please read the below checklist and ensure that all items have been reviewed.

DESCRIPTION	VALUE PROVIDED	COMPLETE?
Review inventory main page and confirm summary info shows for all connected accounts.	Quickly summarizes all deployed cloud assets and resources in single view.	
Review hosts with public access. Click on 'Public' (if there are none, skip); confirm that a list of hosts is displayed, showing all metadata.	Color coding identifies possible misconfigurations and/or security issues.	
Select a host and expand (+) and confirm description details are displayed, and any tags.	Full detail on resource can be used to provide context and aid in understanding how it may impact security.	
Click on 'Stopped' to identify if any hosts are launched but not being used.	Stopped hosts may no longer be needed. Cleaning up can remove attack surface and possibly reduce costs.	
Select a host, confirm the last icon under View at the far right is not greyed out. Click on this to review outbound traffic data such as source, outgoing IP addresses, and port.	Easily view outgoing traffic aids with security investigations and troubleshooting.	
Click on Inventory>Networks Security Groups and click on Unused Security groups.	Unused Security Groups can sometimes become attack vectors. Also, providers by default limit number of resources allowed. Remove unused assets to avoid bumping up against limits that may impact deployments.	
Assets/workloads/services with direct connectivity to the internet. Review other assets such as storage accounts, SQL servers for public connectivity.	Quickly identify assets that may be vulnerable to port scans or direct attacks to gain full picture of attack surface across all accounts.	
Navigate to Inventory>IAM AWS Users and confirm if any users are listed under 'MFA Disabled'.	Identify and control user login behavior to ensure it is secure and in line with GRC policies.	
Review IAM Access Key creating information to see if it's in line with security standards.	Regular key rotation is highly recommended to avoid security issues.	
Click on Inventory>Activity Logs to review information provided on changes.	Aggregated change information available to help with troubleshooting and issue investigation.	

Topology section

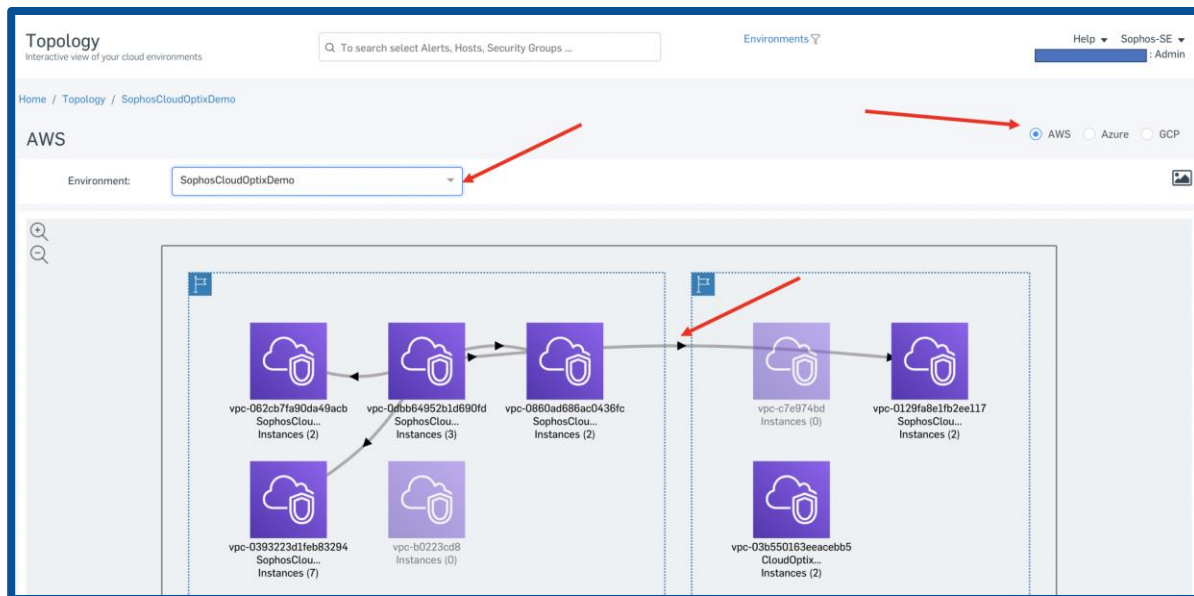
It's often very difficult for administrators to determine what their cloud architecture looks like, how systems interconnect, and what traffic is traversing their environments. Without this type of view, it is very challenging to understand network traffic flows to determine if you may have assets which are exposed unnecessarily.

This type of view can also be useful when trying to determine where it may make sense to install additional security to [build protection layers](#), something recommended by cloud providers depending on the sensitivity of the workload. Examples of a protection layer include third-party security solutions such as web application firewalls (WAF), next-gen firewalls, and host security agents.

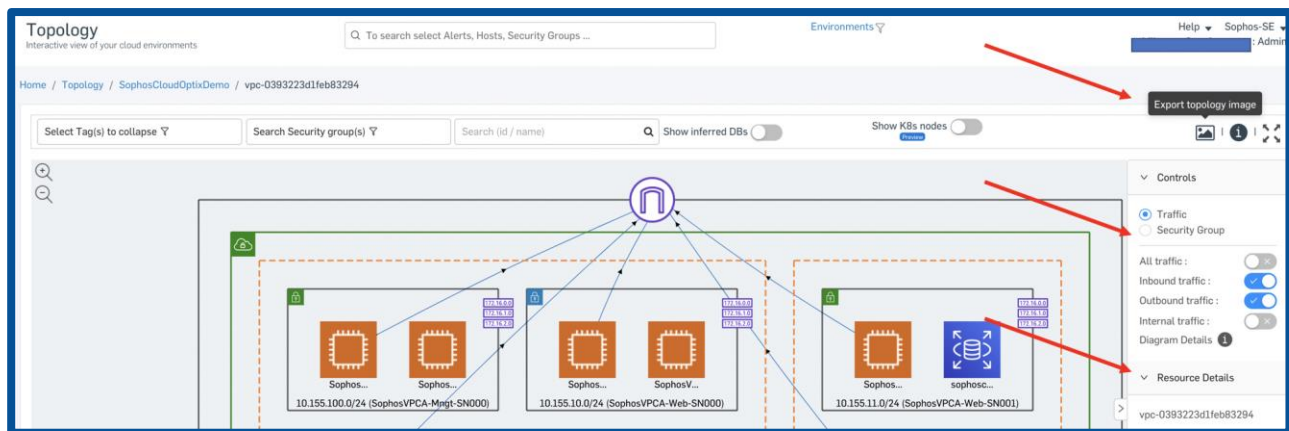
Up-to-date network diagrams are also sometimes required by compliance auditors or internal security teams. Cloud Optimix provides this architectural view of cloud networks and hosts in the **Topology section**, which can be accessed directly from the left side menu, or from the **Inventory Diagram** icons shown in the earlier screenshot.

Navigating directly to the Topology section will default to showing one of your AWS environments. This view can be changed by selecting another environment and/or cloud provider. This default view will show details on the cloud network name, ID, and indicate if there are running hosts. This view will also show any **peer** connections configured between cloud networks. This is a common type of misconfiguration or forgotten configuration which is often difficult to spot, but which should be addressed as part of proper security hygiene. Unknown connections between networks can lead to security issues or cause problems during security and compliance audits. Below is an example from the default AWS environment, but the same options shown are also available for both Azure and GCP.

Sophos Cloud Optim: Proof of Concept Guide



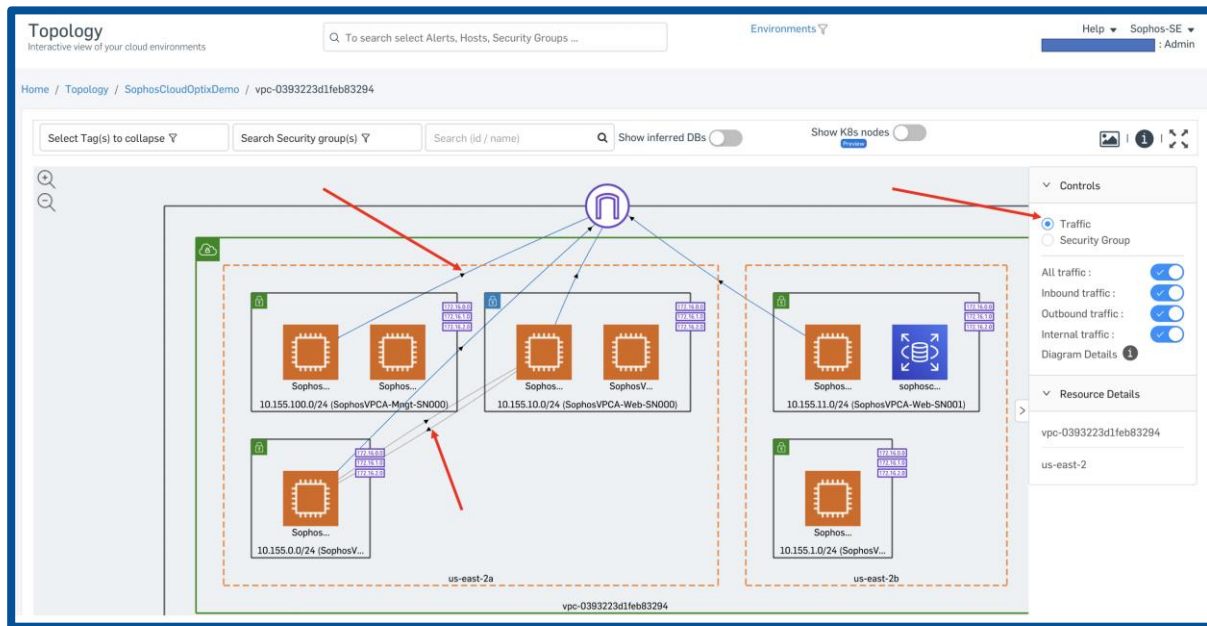
Clicking into any shown network provides a visual of the network hosts, traffic flows, resource details, and provides an option to **export** the image which can be used for audits or for internal documentation purposes.



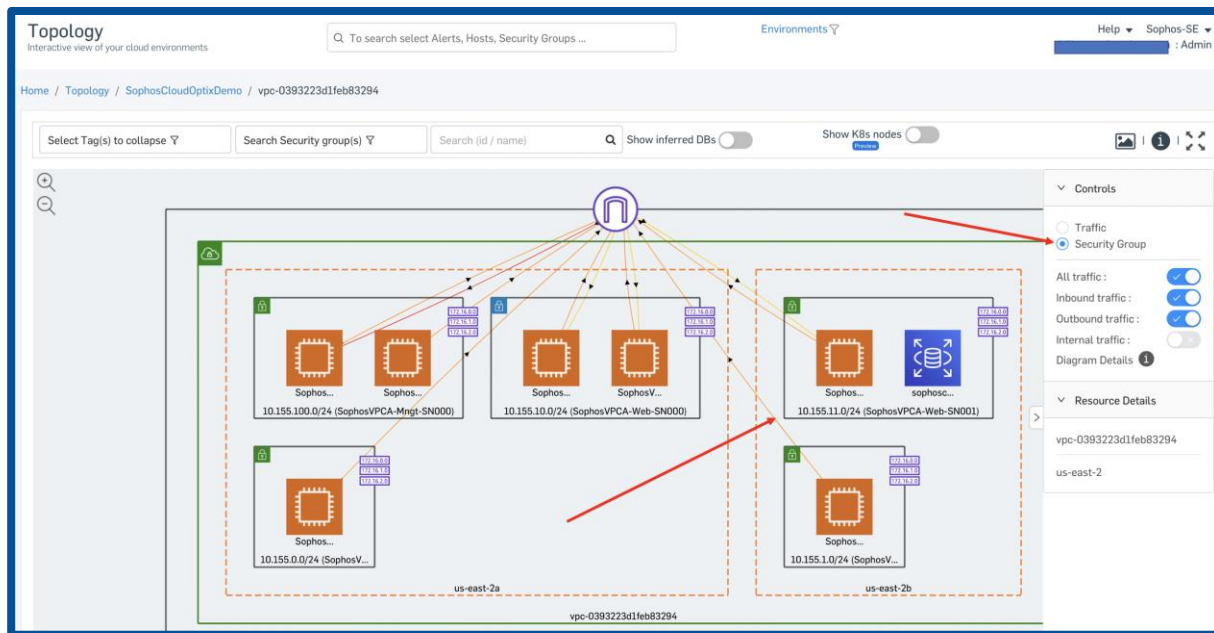
Changing Topology view options is another important capability to explore. The default setting **Traffic** shows actual traffic flows based on ingested log information.

Potential traffic flows can be seen by changing the view to the **Security Group** setting. This can be seen by comparing the two views below. On the left, you can see that we have chosen the **Traffic** view and made sure to click on the **Internal**

Traffic button. That view then shows various real time traffic flows as highlighted by the **red arrows**.



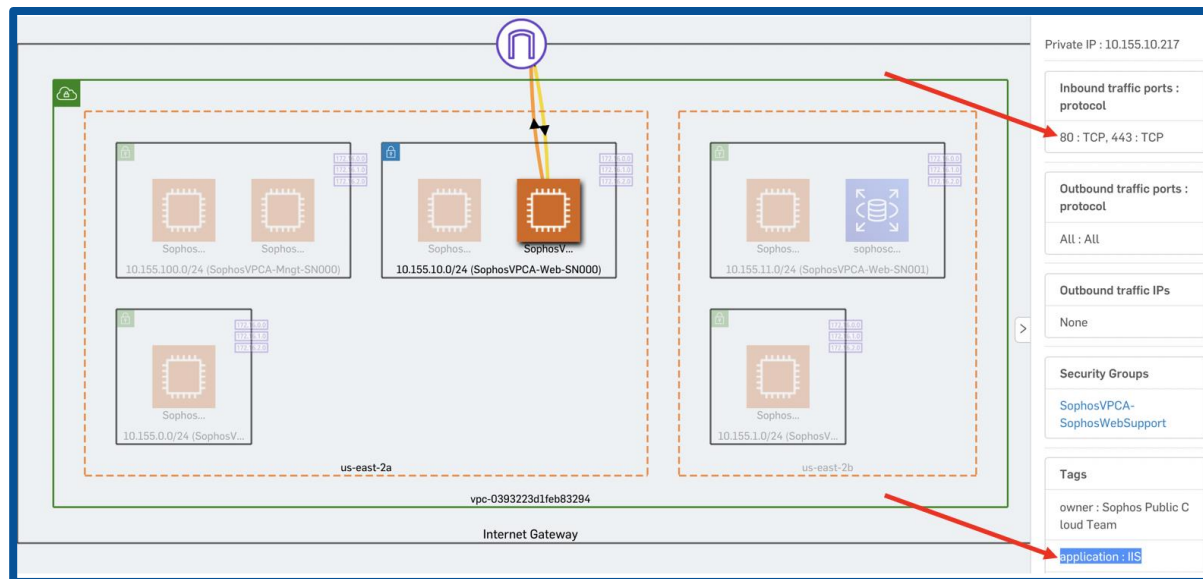
Real-time traffic flow info is very useful to have but note that if we then change the setting to **Security Group** as shown below, we then have *possible* traffic flows shown as indicated by the **red arrow** pointing to the host in the middle of the picture. What that is highlighting is that even though there is no current traffic, that host has a connection to the public internet, something we would want to get more information on.



Clicking on the host we're interested in allows us to drill down further to get more useful information. In this case, what we can see is that the host is allowing traffic inbound on standard web ports, and the tag info shows that it's an IIS server.

This could be an example of how we could determine the need for the additional levels of protection mentioned earlier. In this case, it may make sense to look at putting a WAF in place to protect this IIS server. Note also that the details provided include information on not only the open ports, but also on any detected outgoing traffic.

As this server is set up to receive traffic, outgoing traffic would be something we would want to better understand as it could indicate malicious activity, such as data exfiltration. Of course, any traffic shown may be valid and related to something like software updates, in either case it's something the security teams would likely be interested in understanding.

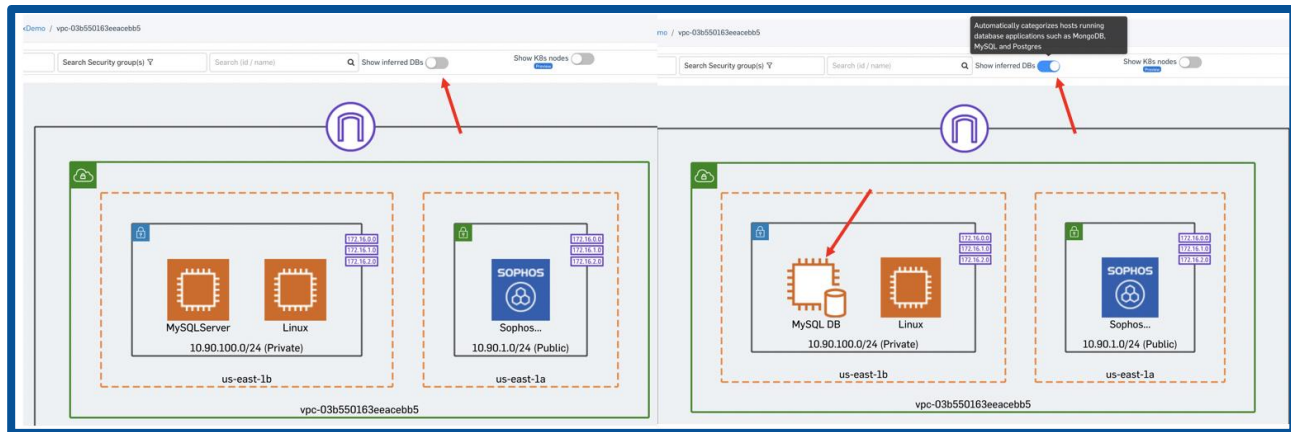


Show inferred databases

The **Topology** feature also has another valuable option which can help identify high-value workloads. This feature is turned on by clicking the button labeled 'Show Inferred DBs' which is located at the top of the network diagram.

Clicking this button will show any hosts which have been identified as running database applications. Databases are considered high-value targets for attack, and so it is very useful to know which hosts may be potential targets so you can consider options for providing additional protection. This is another example of where a customer may benefit from installing additional protection layers – in this case, something like a next-gen firewall could be used to 'hide' the database host from potential attackers, or an inline IPS could help identify and block attacks against the known DB ports used by the application.

In the screenshots below we can see on the left side that, without this feature enabled, the two hosts shown on the left appear the same, and it would be up to the administrator to properly tag the resources to help highlight what they do. With the Show Inferred DBs option enabled, we can quickly spot which is the high-value host that may benefit from additional protection.



Checklist

Please read the below checklist and ensure that all items have been reviewed.

DESCRIPTION	VALUE PROVIDED	COMPLETE?
Navigate to the Topology section and review for any peer connections between networks. Make sure to review all environments and cloud providers.	Ensuring that all network connections are known and validated can help avoid accidental data exposure and other security incidents.	
Drill down into each VPC/Vnet; review traffic flows and compare to Security Group settings to identify instances online but not receiving or sending traffic.	A proper understanding of actual and potential traffic flows can help ensure proper security and saves time when investigating issues and troubleshooting problems.	
Click 'Internal Traffic' radial button and review internal host connections.	Understanding how internal hosts are connecting to each other helps avoid east/west traffic exploits.	
Drill down into each host and review resource details.	Provides an understanding of what IPs and ports each host is connecting to and using.	
Identify hosts connected to the internet and review Resource Details to identify potential misconfigurations and/or areas where additional security may be needed.	Layered security is often recommended to provide adequate protection to high-value resources.	
Click on 'Show Inferred DBs' button to identify high-value instances.	Identifying high value instances can be difficult.	
Export topology diagram as an image by clicking on the landscape icon.	Always up-to-date network diagrams can be provided on demand to auditors.	

Continuous security and compliance

Security in the cloud is a [shared responsibility](#), with the cloud provider ensuring the cloud itself is secure, while leaving it up to the customer to ensure that they have properly secured anything they put into the cloud, such as data or applications. The idea is that the customer should provide the level of protection they need based on their own governance, risk, and compliance standards. The cloud providers do provide a range of security options and tools to help customers secure their environments and assets and provide guidance on proper usage via various [best practice documents](#) and [governance](#) whitepapers.

The main problem facing most organizations is that following this guidance can be difficult due to the amount of information that must be consumed. And properly configuring any of the offered services or defining what type of baseline security governance to use often requires some cloud security expertise. On top of that, many if not most organizations today operate in multiple clouds. So even if a customer has gained security expertise in one cloud, that knowledge often does not directly translate to other clouds as the services and options are often a bit different.

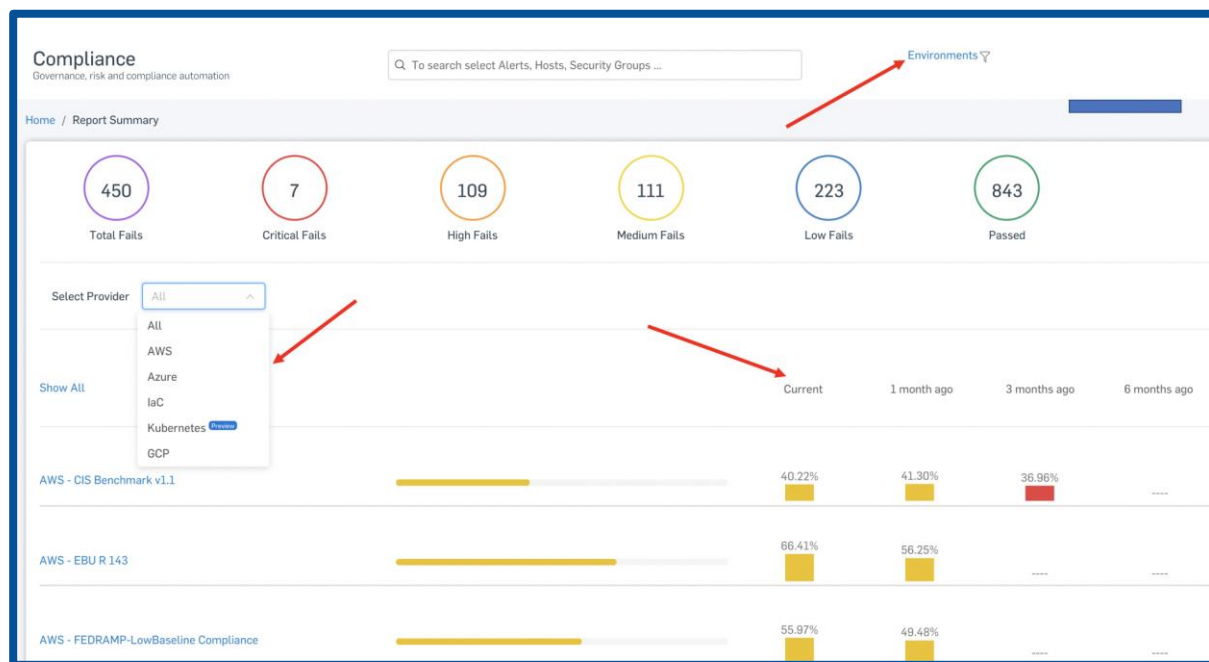
On top of that, organizations also need to understand how the various cloud security controls and services map to external compliance standards, such as GDPR, HIPAA, and PCI. Altogether cloud security and compliance can be very daunting, especially as the dynamic nature of the cloud means that things are always changing, requiring constant attention. Some questions to consider while exploring the Cloud Optimx Continuous Compliance features are:

1. What kind of security governance does your organization follow – CIS Benchmark, SOC2, ISO 27001, other?
2. Do you need to follow any external compliance regulations, such as PCI, HIPAA, or GDPR?
3. Does the organization require proof of compliance for internal or external auditors?
4. Do you have the proper tools needed to measure progress over time?
5. How do you determine which hosts in your environments are in scope for compliance regulations?

6. How cumbersome is it for your organization to create compliance and security reports that focus on what's important, such as production systems, and filters out extraneous information such as dev/test servers or environments?

Compliance summary dashboard

The Report Summary dashboard is displayed when you first click on the **Compliance** menu option. This section provides a high-level view of the customer's Governance, Risk and Compliance (GRC) status, based on the results of all policies enabled on the system. This section is very useful in determining progress over time in addressing security and compliance related issues identified by Optix. The default view aggregates the results based on all environments and cloud providers, but that can be modified as needed to provide different views to different team members.

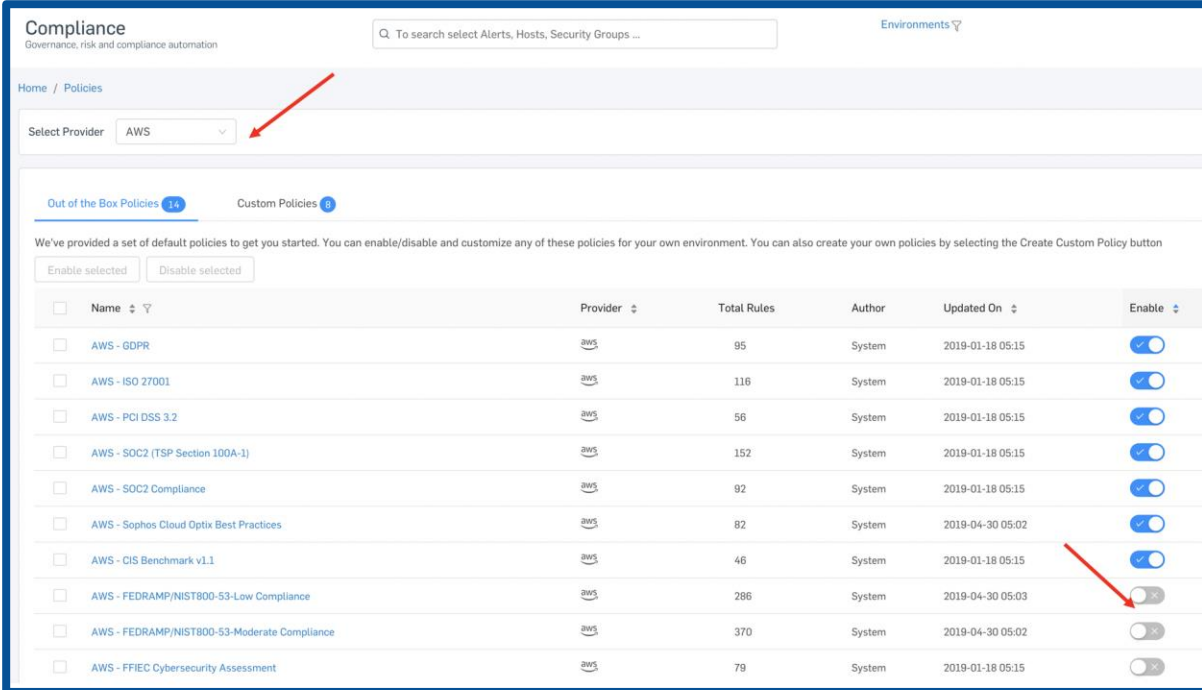


Policies

Cloud Optimx is provided with out-of-the-box security and compliance policies that continually assess a customer's cloud environments. The built-in policies provide a customer with an initial assessment of their security and compliance posture, not long after an environment has been configured in the Cloud Optimx

console. They then will be used on a continuous basis unless disabled. These built-in policies cover standards such as CIS benchmarks, ISO 27001, and SOC2, as well as compliance standards such as HIPAA, PCI, and GDPR.

You can use these policies as a starting point to look at how well they match up to their desired controls. To reduce noise and help focus on what's important to the customer, its suggested that you disable any policies that may not be applicable. For example, below we have filtered on just AWS-related policies, and have chosen to assess our environments against Sophos best practices, CIS Benchmarks, SOC2, GDPR, and PCI. All other policies have been disabled so that we can focus our assessment efforts on these standards.



The screenshot displays the 'Compliance' dashboard in the Sophos Cloud Optimx console. The 'Policies' section is active, showing a list of 'Out of the Box Policies' for the 'AWS' provider. The table lists various compliance standards, including GDPR, ISO 27001, PCI DSS 3.2, SOC2, and CIS Benchmarks. The 'Enable' column shows that most policies are enabled, but the 'AWS - CIS Benchmark v1.1' policy is disabled, as indicated by a red arrow. Another red arrow points to the 'Select Provider' dropdown menu, which is set to 'AWS'.

Name	Provider	Total Rules	Author	Updated On	Enable
AWS - GDPR	AWS	95	System	2019-01-18 05:15	Enabled
AWS - ISO 27001	AWS	116	System	2019-01-18 05:15	Enabled
AWS - PCI DSS 3.2	AWS	56	System	2019-01-18 05:15	Enabled
AWS - SOC2 (TSP Section 100A-1)	AWS	152	System	2019-01-18 05:15	Enabled
AWS - SOC2 Compliance	AWS	92	System	2019-01-18 05:15	Enabled
AWS - Sophos Cloud Optimx Best Practices	AWS	82	System	2019-04-30 05:02	Enabled
AWS - CIS Benchmark v1.1	AWS	46	System	2019-01-18 05:15	Disabled
AWS - FEDRAMP/NIST800-53-Low Compliance	AWS	286	System	2019-04-30 05:03	Disabled
AWS - FEDRAMP/NIST800-53-Moderate Compliance	AWS	370	System	2019-04-30 05:02	Disabled
AWS - FFIEC Cybersecurity Assessment	AWS	79	System	2019-01-18 05:15	Disabled

Policies map rules to specific provider services, summarizing what needs to be done to be compliant, and includes supporting information and a default severity level which can then be used by teams assigning priority to issue resolution. This functionality not only helps an organization with their compliance issue handling, but also helps the teams responsible learn more about the provider services used. In the example below, we can see how proper AWS security group configuration is needed to ensure that PCI Requirement 1.2 is adhered to.

If unfamiliar with AWS controls you may have a difficult time understanding what's needed, and then may not have an easy way to identify what assets are affected in order to fix any issues. With Cloud Optimx policies, this is all done for the customer and on a continuous basis to protect against any changes in the environment.

Home / Policies / Policy Details

Policy Name: AWS - PCI DSS 3.2 Author: System Last Updated: Fri, 18 Jun 2019 10:15:56 GMT Provider: AWS

Compliance Tag: PCI

Selected Accounts: None Resource Tags: None

1.0 Secure Network and Systems (Req 1.2)

#	Rule Summary	Control Id	Rule #	Sophos Optimx Rule Summary	Enabled	Severity	Guardrail
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic	AR-1002	Enable MFA delete for cloudtrail bucket deletion	ENABLED	High	Disabled	
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic	AR-652	Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389	ENABLED	High	Disabled	

Security groups provide stateful filtering of ingress/egress network traffic to AWS resources. It is recommended that no security group allows unrestricted ingress access to port 3389. Removing unfettered connectivity to remote console services, such as RDP, reduces a server's exposure to risk.
<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#default-security-group>

Custom policies are another important tool which can help administrators reduce noise so that they can focus on what is important to them. Cloud environments offer great flexibility to development and test teams who can easily deploy applications and hosts as needed. And while it is important to ensure that these hosts and the networks they reside in are secure, customers may want to limit their compliance scope to just the production assets when running reports related to external compliance. To help with that, Cloud Optimx includes the ability to create custom reports which can then be applied to specific environments, or to specific assets based on [tags](#).

Custom policies can be created from scratch, or an **out-of-the-box** policy can be customized and saved. In both cases, customers can choose a custom name and choose an existing compliance tag or create a new one, which can then be used when filtering alerts.

Home / Policies

Select Provider: All

Create Custom Policy

Out of the Box Policies 35 Custom Policies 11

We've provided a set of default policies to get you started. You can enable/disable and customize any of these policies for your own environment. You can also create your own policies by selecting the Create Custom Policy button

Enable selected Disable selected

<input type="checkbox"/>	Name	Provider	Total Rules	Author	Updated On	Enable	Action
<input type="checkbox"/>	AWS - CIS Benchmark v1.1	AWS	46	System	2019-01-18 05:15	<input checked="" type="checkbox"/>	Customize
<input type="checkbox"/>	AWS - GDPR	AWS	95	System	2019-01-18 05:15	<input checked="" type="checkbox"/>	Customize

Home / Policies / edit

Policy Name: Custom AWS Policy

Compliance Tag: CustomAWS

Author: bill.prout@sophos.com

Select Environments: All selected +

Resource Tags: 1

env: prod

provider: aws

Custom Category

Rule Summary	Rule #	Sophos Optim Rule Summary	Enabled	Severity
+ Avoid the use of the 'root' account	AR-501	Avoid the use of the 'root' account	<input checked="" type="checkbox"/>	MEDIUM
+ Ensure multi-factor authentication (MFA) is enabled for all IAM users that have console access	AR-103	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have console access	<input checked="" type="checkbox"/>	CRITICAL
- Ensure credentials unused for 90 days or greater are disabled	AR-503	Ensure credentials unused for 90 days or greater are disabled	<input checked="" type="checkbox"/>	LOW

Disabling or removing unnecessary credentials will reduce the window of opportunity for credentials associated with a compromised or abandoned account to be used.

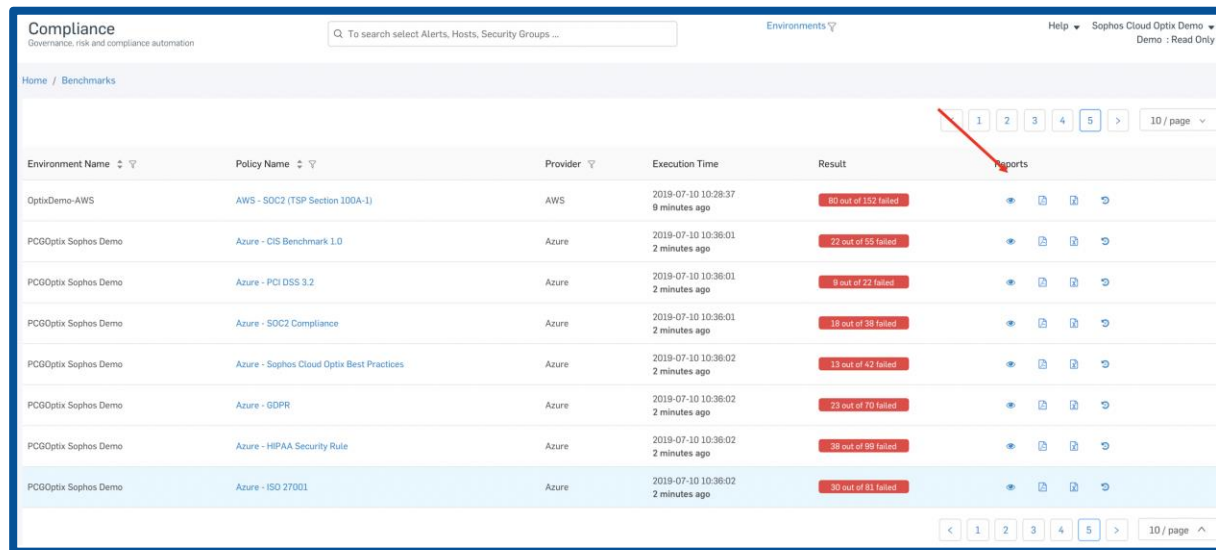
Checklist

Please read the below checklist and ensure that all items have been reviewed.

DESCRIPTION	VALUE PROVIDED	COMPLETE?
Review the out-of-the-box policies; note the provider, total rules, author, updated on, enable status, and action values.	Out-of-the-box policies provide an immediate assessment of cloud environments.	
Identify any policies that are not applicable and disable.	Ability to enable/disable cuts down on noise and provides focus based on the individual organization's needs.	
Choose any policy and click on Name to view details; expand sub-sections and rules to view details.	Policies map provider controls to standards requirements, saving time and effort. Clear rule details provide information needed to educate teams on requirements and standards.	
Return to the list of policies in order to customize the specific policy; click on the Customize button for the policy.	Customized policies allow organizations an easy way to tailor for their environment. Customized policies help with incident prioritization and handling, and can limit policy scope to only desired resources (e.g. just production hosts).	

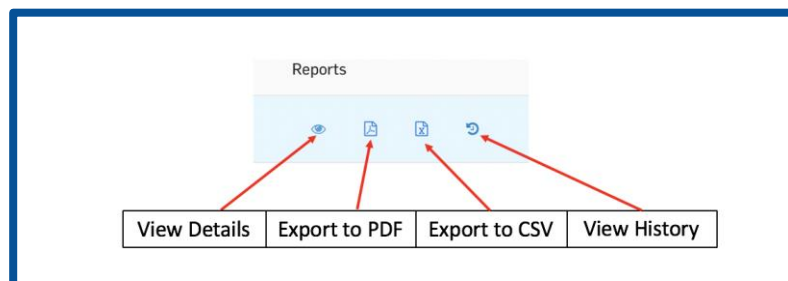
Reports

Each enabled policy on Cloud Optimx will produce corresponding **reports** which are available in the **Compliance>Reports** section. The reports are produced continuously as they are created each time a security scan is done.



Environment Name	Policy Name	Provider	Execution Time	Result	Reports
OptixDemo-AWS	AWS - SOC2 (TSP Section 100A-1)	AWS	2019-07-10 10:28:37 9 minutes ago	80 out of 152 failed	
PCGOptix Sophos Demo	Azure - CIS Benchmark 1.0	Azure	2019-07-10 10:36:01 2 minutes ago	22 out of 55 failed	
PCGOptix Sophos Demo	Azure - PCI DSS 3.2	Azure	2019-07-10 10:36:01 2 minutes ago	8 out of 22 failed	
PCGOptix Sophos Demo	Azure - SOC2 Compliance	Azure	2019-07-10 10:36:01 2 minutes ago	18 out of 38 failed	
PCGOptix Sophos Demo	Azure - Sophos Cloud Optimx Best Practices	Azure	2019-07-10 10:36:02 2 minutes ago	13 out of 42 failed	
PCGOptix Sophos Demo	Azure - GDPR	Azure	2019-07-10 10:36:02 2 minutes ago	23 out of 70 failed	
PCGOptix Sophos Demo	Azure - HIPAA Security Rule	Azure	2019-07-10 10:36:02 2 minutes ago	38 out of 89 failed	
PCGOptix Sophos Demo	Azure - ISO 27001	Azure	2019-07-10 10:36:02 2 minutes ago	50 out of 81 failed	

Reports feature a few options that a customer should be aware of. They can be viewed in the Optimx console, they can be exported in both PDF and Excel formats, and the entire history of all generated reports can be viewed.



Viewing a report provides us with detailed information on which rule checks have passed and which have failed. In both cases, Optimx will group all affected resources or assets together to help reduce the overall number of issues that teams must deal with. This focus on reducing 'noise' can be very beneficial to teams tasked with resolving issues. Note too that at the bottom of the information shown in the 'Affected Resources' column, there is a link for '**more details.**'

Sophos Cloud Optim: Proof of Concept Guide

Home / Benchmarks / Policy Reports

Environment Name: OptixDemo-AWS Policy Name: AWS - SOC2 Compliance custom policy Execution Time: Wed, 10 Jul 2019 18:30:10 GMT Score: 47 out of 91 Failed

> CC3.0 Risk Assessment **All Passed**

> CC4.0 Monitoring Activities **All Passed**

▼ CC6.0 Logical and Physical Access Controls **40 out of 78 Failed**

Result	#	Rule Summary	Control Id	Rule #	Sophos Optim Rule Summary	Affected Resources
Failed	CC6.1	Logical Access		AR-1003	Flag resource(s) with public IP and Security Group with ingress from any source to one or more ports	<ul style="list-style-type: none">terraform-asg-example - LoadBalancer - port(s): (80)Web-tier (i-0886fb7e81bb442e7) - EC2 - port(s): (8080)Test-Web-tier (i-04f06efbc84360c80) - EC2 - port(s): (22)Web-tier (i-0f612ce70e5c64d96) - EC2 - port(s): (8080)Web-tier (i-0f631c0a77365345) - EC2 - port(s): (8080)+ 5 more...
Failed	CC6.1	Logical Access		AR-1002	Enable MFA delete for cloudtrail bucket deletion	<ul style="list-style-type: none">avid-cloudtrail-760068489120 more details...

Clicking on the 'more details' link in a report will bring up a screen similar to what is shown below. As you can see, Cloud Optim provides detail on what the problem is, in what environment it was found, when it was last seen, and which resources are affected. Cloud Optim also provides remediation instructions which explain how to fix this issue, and which also contain a link to official provider information.

Additionally, Cloud Optim provides icons located in the upper right which help teams effectively work together by providing options for manual and automatic remediation of issues. We'll cover those options in the next section which will focus on **response**.

Details

High

Summary: Enable MFA delete for cloudtrail bucket deletion

Description: Requiring MFA to delete the cloudtrail S3 bucket provides a secondary layer of protection against accidental deletion and deletion of log files by a malicious actor in case your AWS access credentials are compromised.

Remediation: MFA delete cannot be enabled via the AWS web console. Execute the CLI command below to enable MFA delete on a bucket.
`aws s3api put-bucket-versioning --bucket [BUCKETNAME] --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa "[MFA_DEVICE_SERIAL] [MFA_CODE]"`
NOTE: Only Bucket Owner (admin) can execute this command.
For additional information please visit <https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html#MultiFactorAuthenticationDelete>

Alert Id: A-000071

Environment: OptixDemo-AWS (AWS)

Last Seen: 2019-03-29 09:23:32 (3 months ago)

Suppressed Resource count: 0 / 1

Affected Resources:

Resource	Last modified by	First Seen
avid-cloudtrail-760068489120	TFDemodeploy	3 months ago

Close

Checklist

Please read the below checklist and ensure that all items have been reviewed.

DESCRIPTION	VALUE PROVIDED	COMPLETE?
Compliance policy visibility and consistent enforcement across multiple cloud providers.	Compliance is difficult to achieve or prove without proper tools and visibility.	
Navigate to Compliance main page; review report summary showing total fails, critical fails, high fails, medium fails, low fails, and passed values.	Summary info on GRC status is crucial to understanding overall status.	
Select the desired provider.	The ability to view per cloud provider allows different teams ability to focus efforts on area of responsibility.	
Review the list of compliance standards and the compliance status of each; note the percentage of compliance against the standard available over time.	Progress shown over time with regards to incident resolution and handling.	
Click on one of the standards to review a high-level summary of the report.	High-level view helps teams understand which environments may need most attention.	
Click on the eye icon to view the current report.	Drilling down into the report shows status per subsections, allowing teams to concentrate on areas with failed checks.	
Review the sections within the report and drill down into desired sections to view which specific rules have passed or failed also note the affected resources.	Grouping of all affected resources under single fail helps with incident management, saving time and effort.	
Export the report to either PDF or CSV format by clicking on the respective icons.	Reports can be exported in multiple formats for hand-off to other teams or auditors.	
Return to the list of compliance standards; it is possible to view historical reports; click on 'Benchmarks' in the breadcrumbs.	Historical reports can be used to look back in time to determine status. Together with change management information, this can be used in incident investigation.	

Response

The Cloud Optix **Response** capabilities are designed to help organizations quickly and effectively respond to security incidents in the cloud. With the use of public cloud, organizations have seen their attack surface greatly increase, while at the same time attacks have become more sophisticated and happen with alarming speed.

Attackers understand the cloud is increasingly used to host important data, and they also are aware that many customers do not have the tools or qualified personnel needed to properly protect themselves against both cyberattacks and cloud infrastructure misconfigurations. Attackers also know that in many organizations, different teams have different responsibilities when it comes to the cloud, something they often look to exploit due to the time it often takes for these teams to coordinate their efforts in response to a security incident.

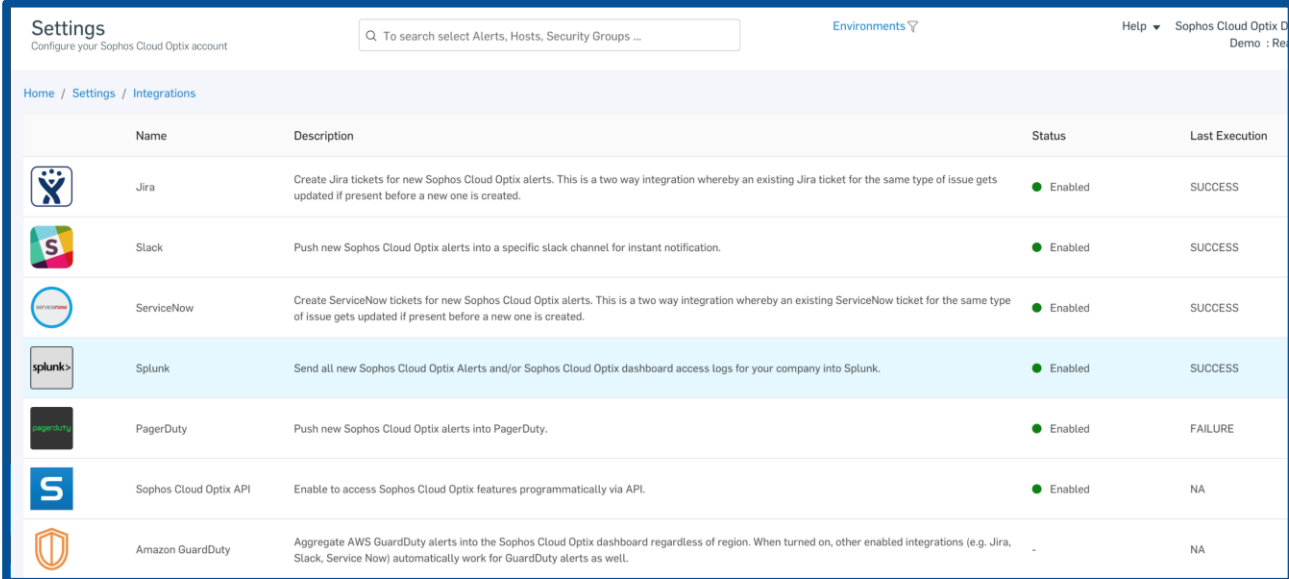
Development teams may be responsible for building cloud infrastructure, operations teams may be responsible for managing the cloud infrastructure, and security teams may be responsible for overall security. What this division of responsibility means in the real world is that development teams may deploy insecure architectures before anyone is aware, operations teams may make changes to security settings that could negatively impact the security posture, and security teams may identify an issue, but then not have an quick and effective way of alerting the teams responsible for remediating the problem. Some questions to consider are:








1. Do multiple teams work on cloud deployment, security, and operations?
2. Is so, how do these teams coordinate responses to governance, risk, and compliance issues?
3. What type of business systems or tools does your organization use?
 - a. Ticketing systems such as Jira or ServiceNow?
 - b. Communication tools such as Slack or PagerDuty?
 - c. A SIEM such as Splunk?
4. How does the organization deploy their cloud infrastructure? Manually or using infrastructure automation tools such as Terraform or CloudFormation?

5. How do you identify suspicious or anomalous activity in your cloud environments?

Cloud Optix supports [integration](#) with some of the most popular business tools today. These tools are used to help customers with cloud security monitoring, governance, risk, and compliance (GRC) and [DevSecOps](#) processes.

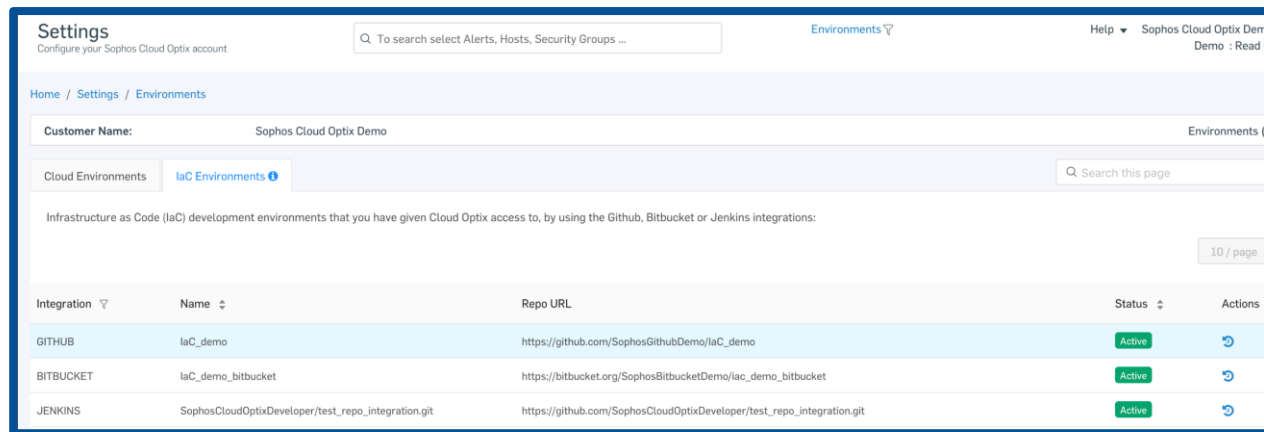
To get the full understanding of how Cloud Optix can assist an organization meet the challenges of securing their cloud infrastructure, it is strongly suggested that you configure one or more of the available Integrations to understand how these features can assist teams involved in cloud deployment and security. Setup is simple with instructions found both in the Cloud Optix help section, as well as available by clicking on any of the supported systems shown.



Settings				
Configure your Sophos Cloud Optix account				
Home / Settings / Integrations				
Name	Description	Status	Last Execution	
	Jira	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 gets updated if present before a new one is created.	● Enabled	SUCCESS
	Slack	Push new Sophos Cloud Optix alerts into a specific slack channel for instant notification.	● Enabled	SUCCESS
	ServiceNow	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 gets updated if present before a new one is created.	● Enabled	SUCCESS
	Splunk	Send all new Sophos Cloud Optix Alerts and/or Sophos Cloud Optix dashboard access logs for your company into Splunk.	● Enabled	SUCCESS
	PagerDuty	Push new Sophos Cloud Optix alerts into PagerDuty.	● Enabled	FAILURE
	Sophos Cloud Optix API	Enable to access Sophos Cloud Optix features programmatically via API.	● Enabled	NA
	Amazon GuardDuty	Aggregate AWS GuardDuty alerts into the Sophos Cloud Optix dashboard regardless of region. When turned on, other enabled integrations (e.g. Jira, Slack, Service Now) automatically work for GuardDuty alerts as well.	-	NA

It is also suggested that at least one [Infrastructure as Code \(IaC\)](#) environment be configured so that the proactive template scanning and response capabilities can be properly tested. If you are automating the buildout of cloud environments, you will likely be storing the [templates](#) built in a repository such as [Github](#) or [Bitbucket](#). If so, then creating a connection to Optix will allow Cloud Optix the ability to **proactively** scan new templates placed into those repositories. This can help ensure that any security misconfigurations built into the templates are identified and fixed before they make it into production. Sophos Cloud Optix can

currently check [Terraform](#), [AWS CloudFormation](#), [Ansible](#), and [Kubernetes](#) template files.



Finally, to properly test out the remediation capabilities, it is suggested that you follow the instructions mentioned earlier which detail how to add a '[remediation](#)' role to your environments. This additional access will allow you to manually and/or automatically remediate issues found in Cloud Optix, which can of course be done safely by using custom policies that apply only to test environments.

Guardrails

[Automatic remediation](#) of key security-related issues is a powerful feature of Cloud Optix. Guardrails allow Cloud Optix to make changes to fix certain issues or misconfigurations, to ensure that the desired security and compliance posture is maintained. Guardrails are enabled in Cloud Optix **custom policies** and relate to high-profile security issues such as IAM and AWS Simple Storage Services (S3) misconfigurations, and help flag vulnerable resources. One of the most common uses of Guardrails is to ensure that AWS Simple Storage Services (S3) are both setup properly, and not accessible via the public internet. Vulnerable S3 Simple Storage Services are a major source of data exploits which has resulted in [free and easy to use tools](#) being made available to help attacks locate attack targets.

Policy Name:
Compliance Tag:
Author:

Select Environments: All selected +
Resource Tags:

env
prod

provider
aws

Custom Category

Rule Summary	Rule #	Sophos Optimx Rule Summary	Enabled <input type="checkbox"/>	Severity	Guardrail
+ Ensure IAM password policy requires at least one uppercase letter	AR-505	Ensure IAM password policy requires at least one uppercase letter	<input checked="" type="checkbox"/>	LOW	<input checked="" type="checkbox"/>
+ Ensure IAM password policy require at least one lowercase letter	AR-506	Ensure IAM password policy require at least one lowercase letter	<input checked="" type="checkbox"/>	LOW	<input checked="" type="checkbox"/>
+ Ensure IAM password policy require at least one symbol	AR-507	Ensure IAM password policy require at least one symbol	<input checked="" type="checkbox"/>	LOW	<input checked="" type="checkbox"/>
+ Ensure IAM password policy require at least one number	AR-508	Ensure IAM password policy require at least one number	<input checked="" type="checkbox"/>	LOW	<input checked="" type="checkbox"/>
+ Ensure IAM password policy requires minimum length of 14 or greater	AR-509	Ensure IAM password policy requires minimum length of 14 or greater	<input checked="" type="checkbox"/>	LOW	<input checked="" type="checkbox"/>
+ Ensure S3 buckets do not allow public read/list permission	AR-251	Ensure S3 buckets do not allow public read/list permission	<input checked="" type="checkbox"/>	HIGH	<input checked="" type="checkbox"/>
+ Ensure S3 buckets do not allow public read/list bucket ACL permissions	AR-252	Ensure S3 buckets do not allow public read/list bucket ACL permissions	<input checked="" type="checkbox"/>	HIGH	<input checked="" type="checkbox"/>
+ Ensure encryption is turned on for S3 buckets	AR-253	Ensure encryption is turned on for S3 buckets	<input checked="" type="checkbox"/>	MEDIUM	<input checked="" type="checkbox"/>

Enable Guardrails to apply remediation automatically for specific rules. You need to run a remediation script to enable this functionality for your environment first; you'll find this on the 'Edit environment' screen in Settings

Checklist

Please read the below checklist and ensure that all items have been reviewed.

DESCRIPTION	VALUE PROVIDED	COMPLETE?
Connect an IaC environment to Cloud Optimx.	Connecting IaC environments provides for DevSecOps capabilities, which allows for proactive scanning vs. reactive incident handling.	
In your IaC environment, create a test template and add a network security group containing a rule that is open to the internet for RDP [3389] and/or SSH [22].	IaC templates containing insecure settings can result in security misconfigurations and issues. A simple test can help show the value of this feature.	
Monitor Cloud Optimx 'alerts' to confirm proactive scanning is complete.	Can be used to show value to development teams who will see how this approach does not slow down their dev and automation efforts.	

Alerts correlation and remediation

The **Alerts** dashboard in Cloud Optimx provides a default view of all alerts, and provides the ability to filter based on environment, date, alert type, or severity,

provides options for exporting the data to .pdf or .csv, and allows for searching based on certain alert characteristics.

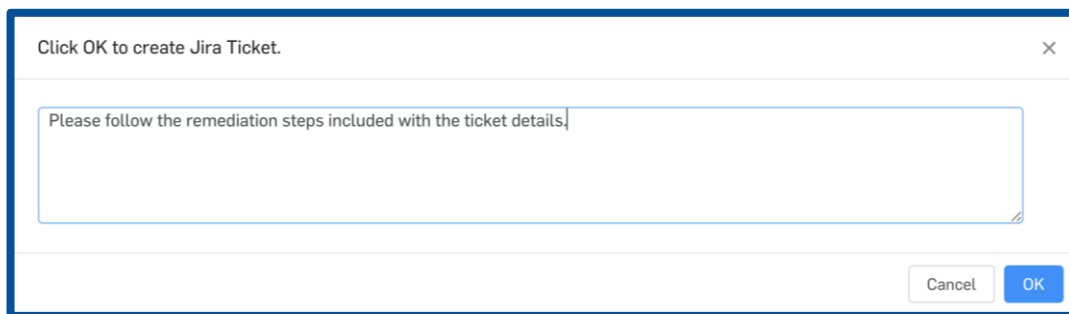
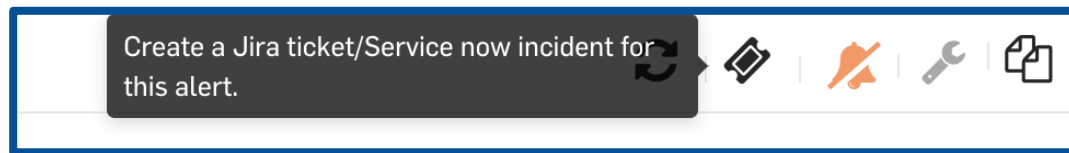
The screenshot shows the Sophos Cloud Optimx Alerts dashboard. At the top, there's a search bar labeled 'Alerts' with a dropdown menu showing options like 'Alerts where id contains', 'Alerts where description contains', and 'Alerts where affected resources contains'. A red arrow points to the search bar. Below the search bar, there are four alert summary cards: Critical Alerts (2), High Alerts (4), Medium Alerts (13), and Low Alerts (50). The main table lists alerts with columns for Alert ID, Severity, Description, Type, Affected Resources, Last Changed, Provider, Environment, and Compliance Tag. Two alerts are visible: A-000320 and A-000701.

Clicking on an **Alert ID** will bring up the same information we reviewed during the **Reports** section, showing both summary and detailed description information, as well as **remediation** instructions. As mentioned earlier, there are a few useful icons located in the upper right that can help teams with issue handling.

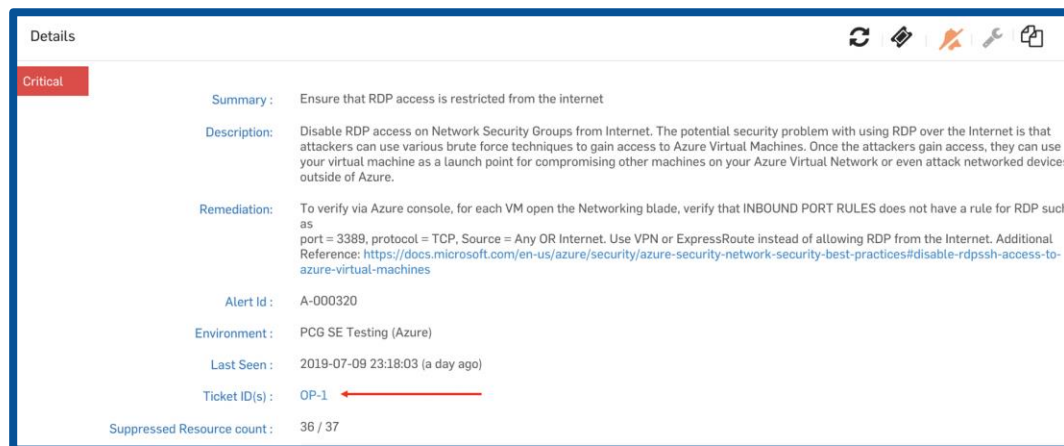
The screenshot shows the details page for alert A-000320. The page has a 'Critical' status bar. The summary is 'Ensure that RDP access is restricted from the internet'. The description is 'Disable RDP access on Network Security Groups from Internet. The potential security problem with using RDP over the Internet is that attackers can use various brute force techniques to gain access to Azure Virtual Machines. Once the attackers gain access, they can use your virtual machine as a launch point for compromising other machines on your Azure Virtual Network or even attack networked devices outside of Azure.' The remediation instructions are 'To verify via Azure console, for each VM open the Networking blade, verify that INBOUND PORT RULES does not have a rule for RDP such as port = 3389, protocol = TCP, Source = Any OR Internet. Use VPN or ExpressRoute instead of allowing RDP from the Internet. Additional Reference: <https://docs.microsoft.com/en-us/azure/security/azure-security-network-security-best-practices#disable-rdpssh-access-to-azure-virtual-machines>'. The alert ID is A-000320, the environment is PCG SE Testing (Azure), and the last seen time is 2019-07-09 23:18:03 (17 hours ago). The ticket ID(s) are not listed. The suppressed resource count is 36 / 37. The affected resources table shows one resource: 'presales-nsg' with a last modified time of NA and a first seen time of 12 days ago.

The **Create a Jira/ServiceNow incident** button does what you would expect in that it allows you to manually create a service ticket in either solution. All the

information from Cloud Optix will be contained in the ticket details, and notes can be optionally added.



The **Ticket ID** will be sent back from Jira or ServiceNow to the Cloud Optix console and displayed in the updated alert as shown below.



Optional Alert Suppression is another feature that can help teams managing alerts in Cloud Optix. Suppressing an alert will hide it in the Cloud Optix console. This can be done per affected resources, or for all resources. Suppressed Alerts can be viewed at any time after by clicking on the 'Show suppressed Alerts' button.

Sophos Cloud Optix: Proof of Concept Guide

Details

Critical

Summary : Ensure that RDP access is restricted from the internet

Description: Disable RDP access on Network Security Groups from Internet. The potential security problem with using RDP over the Internet is that attackers can use various brute force techniques to gain access to Azure Virtual Machines. Once the attackers gain access, they can use your virtual machine as a launch point for compromising other machines on your Azure Virtual Network or even attack networked devices outside of Azure.

Remediation: To verify via Azure console, for each VM open the Networking blade, verify that INBOUND PORT RULES does not have a rule for RDP such

Suppress

Alerts

Smart alerts for security and compliance

Alert Summary

1 Critical Alerts, 4 High Alerts, 11 Medium Alerts, 50 Low Alerts

Alert ID, Severity, Description, Type, Affected Resources, Last Changed, Provider, Error

A-00001 Critical Play resources with public IP and Security Group with ingress from any source on any port

Show Suppressed Alerts

Automation ticket creation is also available per alert level. This can help ensure that tickets are immediately created when alerts of a certain type are seen by Cloud Optix, speeding up the time to resolution, which can be critical when addressing security issues in the cloud.

Jira Integration

This integration requires access to your instance. You can further restrict access by whitelisting the Cloud Optix IP(s): 184.

Enable ☒

Url

UserName

Project Key

Alert Levels → Jira priority

☒ CRITICAL → Highest

☐ HIGH → High

☐ MEDIUM → Medium

☐ LOW → Low

Automatic: ☒

Alert Post By: ☒ Consolidated ☐ AffectedResources

Save **Update API token** **Cancel**

This creates a single Jira ticket created per Alert type. All affected resources are in the same Jira ticket. This is the same as how you see alerts in the Sophos Cloud Optix dashboard.

This creates a parent Jira ticket containing only the title of the alert and for each affected resource creates multiple Jira sub-tasks linked to that parent with the Alert detail and a single affected resource in each.

Alert types

Cloud Optix contains four different types of alerts to help customers respond to issues related to maintaining a secure and compliant cloud infrastructure. The four alert types are shown below, and the alerts dashboard provides the ability to filter by alert type.

The screenshot shows the 'Alerts' dashboard in Sophos Cloud Optix. At the top, there's a search bar and a breadcrumb 'Home / Alerts'. Below this is an 'Alert Summary' section with four cards: 'Critical Alerts' (0), 'High Alerts' (3), 'Medium Alerts' (8), and 'Low Alerts' (34). A tooltip is displayed over the 'High Alerts' card, listing four alert types: 1. Security Monitoring, 2. Anomaly (AI), 3. AWS GuardDuty, and 4. IaC. Below the summary is a table with columns: Alert ID, Severity, Description, Type, and Affected Resources. Two alerts are visible: A-000699 (High) and A-000330 (High). A filter dropdown is open on the right, showing checkboxes for Security Monitoring, Anomaly (AI), AWS GuardDuty, and IaC.

Security Monitoring Alerts are the alerts raised by the security and compliance policies enabled in the Compliance>Policies section of Cloud Optix. Each alert provides information on related policies as shown below.

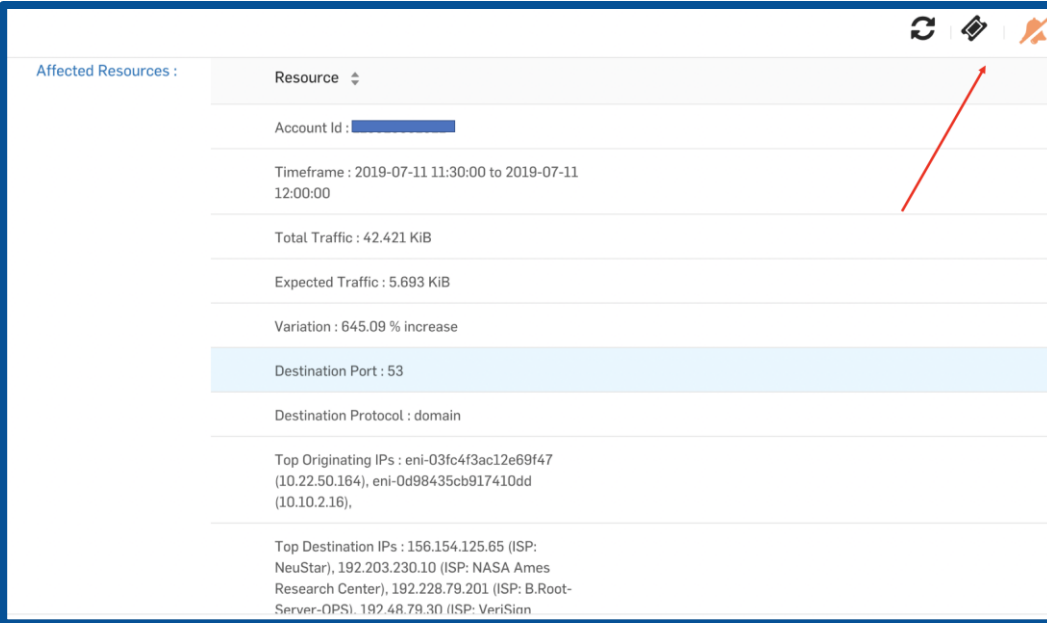
This screenshot shows a close-up of the 'Compliance Tag' filter in the alerts dashboard. A tooltip points to the filter icon, stating 'Indicates which compliance standards are impacted by a given alert'. Below the filter icon, there are five buttons: 'CIS', 'HIPAA', 'ISO 27001', 'SOC2', and 'Sophos'. The page number '10 / page' is visible in the top right corner.

Anomaly alerts are a very useful type of alert, as they help organizations identify out of the ordinary behavior that may indicate malicious activity. Cloud environments generate quite a bit of log data which can be very difficult to manage when looking for suspicious events.

Cloud Optimx AI observes user and network activity logs on a continuous basis and over a period of about three weeks builds a baseline of normal behaviors. It can then raise AI alerts when it sees difficult to spot abnormal behavior such as users logging in from new locations or large increases in the amount of traffic leaving a host or network. The Alert details provide useful information, such as the amount of traffic seen along with source, destination, and protocol. These alerts also contain the manual ticket creation and suppression features discussed earlier, allowing a customer the ability to create and assign tickets to network or applications teams who may be able to aid in the investigation.

Alert ID	Severity	Description	Type	Affected Resources	Last Changed	Provider	Environment
A-001430	Low	177.22 % increase in outbound traffic on destination port '80'	Anomaly (AI)	<ul style="list-style-type: none">Account Id : 115629891621Timeframe : 2019-07-11 09:30:00 to 2019-07-11 10:00:00Total Traffic : 4,206 MiBExpected Traffic : 1,517 MiBVariation : 177.22 % increase+ 4 more...	2 days ago	AWS	Sophos SE
A-001431	Low	645.09 % increase in outbound traffic on destination port '53'		<ul style="list-style-type: none">Account Id : 115629891621Timeframe : 2019-07-11 11:30:00 to 2019-07-11 12:00:00Total Traffic : 42,421 KiBExpected Traffic : 5,693 KiBVariation : 645.09 % increase+ 4 more...	2 days ago	AWS	Sophos SE
A-001432	Low	5136.56 % increase in outbound traffic on destination port '80'		<ul style="list-style-type: none">Account Id : 115629891621Timeframe : 2019-07-11 18:30:00 to 2019-07-11 19:00:00Total Traffic : 55,736 MiBExpected Traffic : 1,064 MiBVariation : 5136.56 % increase+ 4 more...	2 days ago	AWS	Sophos SE

[AWS GuardDuty](#) is an AWS threat detection service that can be integrated with Cloud Optimx via the Cloud Optimx [Integration](#) section. This integration pulls AWS security event information into Cloud Optimx to provide additional context into the overall security posture, and together, this information can help you make better security decisions. For example, an AWS GuardDuty alert may be related to port probing from known bad IPs. That information can be used along with the Cloud Optimx Topology features to give you a better understand of how vulnerable that asset may be.



Affected Resources :	Resource
	Account Id : [REDACTED]
	Timeframe : 2019-07-11 11:30:00 to 2019-07-11 12:00:00
	Total Traffic : 42,421 KiB
	Expected Traffic : 5,693 KiB
	Variation : 645.09 % increase
	Destination Port : 53
	Destination Protocol : domain
	Top Originating IPs : eni-03fc4f3ac12e69f47 (10.22.50.164), eni-0d98435cb917410dd (10.10.2.16),
	Top Destination IPs : 156.154.125.65 (ISP: NeuStar), 192.203.230.10 (ISP: NASA Ames Research Center), 192.228.79.201 (ISP: B.Root-Server-OPS), 192.48.79.30 (ISP: VeriSign)

laC alerts are alerts raised via Integration with [Infrastructure as Code](#) environments as described above. Organizations building out their cloud infrastructure using IaC templates often do so as part of [Continuous Integration/Continuous Development \(CI/CD\)](#) processes.

CI/CD is often used by DevOps focused organizations with the goal of deploying software updates frequently and reliably. And since cloud infrastructures are virtual environments, deploying and updating them can be managed in the same way as with applications.

The challenge security teams face is how to inject security into these processes to ensure that the coded instructions used to build the virtual infrastructure is deploying those assets in a secure manner? Developers are not necessarily security experts, and so may not be aware of what is required by an organization in terms of security and compliance.

By assessing those templates before they are used, Cloud Optix can spot security misconfigurations and raise alerts. Similar to other alerts discussed, IaC alerts options allow administrators to then raise incident tickets containing information on the problem and how to resolve. Those tickets can be assigned to the teams creating the templates so that they can fix the issues via an updated template. This workflow also has the benefit of raising security awareness and knowledge across teams without interrupting the CI/CD process.

Checklist

Please read the below checklist and ensure that all items have been reviewed.

DESCRIPTION	VALUE PROVIDED	COMPLETE?
Alerting on potentially risky new deployments or changes to the cloud environment, hosts, or services.	Understanding how changes are affecting security is key to cloud security. Many of these changes are related to new deployments from teams using automation tools.	
On Main Dashboard, review the top alerts listed.	Quick summary of things to look at helps with speedy incident handling.	
Select the highest severity alert raised and click on it to review details.	Alert severity grouping can help teams with prioritization and/or workload sharing.	
Review Alert ID, type, affected resources, provider, and other details.	Understanding all affected resources in single view helps avoid fixing issues on one system while leaving others vulnerable.	
Select an alert from the list and click on the Alert ID to drill down into the details. Review the Summary, Description, Remediation (if applicable, environment, last seen, suppressed resource count, and affected resources.	Drill down views provides everything needed for incident handling.	
Click on the Ticket icon to review the process to raise a ticket with either Jira or ServiceNow.	Integration with ticketing systems allows for efficient incident handling, speeding up time to resolution.	
Click on the Bell icon to suppress the alert; suppressed alerts will not be visible in the Alerts dashboard unless Show Suppressed Alerts is enabled.	Suppressing alert view helps teams work through alerts in methodical manner.	
Filter by type of alert; click on the funnel icon next to Type, and check one or more of the boxes to limit the alerts shown to specific types, such as security monitoring, anomaly [AI], or IaC.	Viewing by alert type can help divide workload across teams.	
Anomaly [AI] alerts display unusual user or network behavior.	Anomalies can be very difficult to spot when multiple clouds and accounts are used. AI models train themselves to watch for suspicious activity.	

Proof of concept testing framework

The following suggested framework has been designed to help a you get started with your testing of Cloud Optix. The goal is to ensure that you experience the full visibility, compliance, and response capabilities of the solution, and understand how it can assist with managing security and compliance in the cloud.

If at any stage, you would like help to run, or assess the findings of your proof of concept, please contact publiccloud@sophos.com, and we'll be happy to help.

Day one activities

1. Ensure you have signed up for a Cloud Optix trial account, and that the licensing section shows a sufficient number of days available for testing.
2. Configure at least one AWS, Azure, or GCP environment connection in Cloud Optix environments section. Initial connection may take up to 30 minutes to complete. During that time the next few steps can be completed.
3. Review Cloud Optix features and functionality using documentation available on Cloud Optix landing page and/or Partner Portal. Suggested resources include the Cloud Optix datasheet, Cloud Optix FAQ doc, Cloud Optix short videos, and Cloud Optix demo script.
4. Confirm Operational Status of environment connection[s] to ensure both API sync and Security check have completed.
5. Confirm Inventory, Topology and Alerts section are showing information.
6. Review and document Main Dashboard summary information.
7. Review and document key information shown in the **Inventory** section for later comparison during the POC period [screenshots should suffice]. Focus on security-related items color coded **red** and potentially unneeded resources such as unused Security Groups and 'stopped' hosts.
8. Review Topology section to identify possible security architecture misconfigurations such as peer connections and review details of at least one VPC/Vnet to ensure customer knows how to use features to identify real-time and potential traffic flows and identify database instances.

9. Review and document Compliance GRC Dashboard and document 'Report Summary' details for later comparison.
10. Review out-of-the-box policies and disable any that are not applicable. Identify one or more security and one compliance policies which can be used during testing period. These policies and their corresponding reports and alerts will be used to document progress during testing period.
11. Review Alerts section and ensure you know how to work with alert features.
12. Review Integration and IaC environment sections to ensure they are aware of which options are available.
13. Review the 'Help' section of Optimix to ensure you know what resources are available.

Day two-ten activities

1. Review progress from day one. Identify any activities not completed.
2. Review and document Main Dashboard summary information. Compare to information recorded on day one to identify changes.
3. Review and document key information shown in the **Inventory** section. Compare to information recorded on day one to identify changes.
4. Review Topology section to determine what they have found during their more detailed review. Note any identified issues or concerns.
5. Review and document Compliance GRC Dashboard and document 'Report Summary.' Compare to information recorded on day one to identify changes.
6. Review reports for key policies used for security and compliance. Compare most current report to earliest reports to gauge progress.
7. Review how you are managing alerts. Are manually or automatically creating tickets to involve other teams in incident resolution?
8. If you have connected an IaC environment, check for IaC alerts in the alert section using Alert Filter option.
9. Discuss which other teams in org may benefit from access to Cloud Optimix [*e.g. compliance teams, DevOps teams, operations teams*].

Day 10-20 activities

1. Review day 10 goals and results. Identify any activities not completed.
2. Review and document Main Dashboard summary information. Compare to information recorded on day 10 to identify changes.
3. Review and document key information shown in the **Inventory** section. Compare to information recorded on day 10 to identify changes.
4. Review Topology section to determine what you have found during the more detailed review. Note any identified issues or concerns.
5. Review and document Compliance GRC Dashboard and document 'Report Summary.' Compare to information recorded on day 10 to identify changes.
6. Review reports for key policies used for security and compliance. Compare most current report to earlier reports to gauge progress.
7. Review any AI-generated alerts found in Alerts section.
8. Gather feedback from any additional team members using Cloud Optix.

Day 30 proof of concept review

At this point you'll want to use the information gathered during the 30-day trial period to ensure you're able to fully evaluate Cloud Optix.

1. Compare day one **Main Dashboard** information showing the alert summary and compliance scores to days 10, 20, and 30. Has the alert and compliance summary information changed and improved?
2. Compare the **Inventory** information captured during review period. Have you been able to identify unused or unneeded resources?
3. Review your findings that relate to the Topology views. Have you identified any unknown or unneeded peer connections? Have you been able to identify unknown traffic paths or database instances? Have you identified high-value resources or potentially vulnerable instances that would benefit from additional layers of security?

4. Have you seen value in using the continuous compliance reporting dashboard to assess their progress towards improving their GRC posture?
5. Have you configured any custom policies? Have those policies been used to limit scanning to specific environments and/or hosts? How has this benefited the organization?
6. Have you enabled Guardrails in any policies?
7. Have the built-in policies provided you with a better understanding of what controls are needed for security governance and/or external compliance?
8. Have you used the reports to help fix any found issues? Has this been done by just by one person, or by other team members?
9. Have you connected Cloud Optix to Jira, ServiceNow, or Slack in order to test alert handling across teams?
10. Have you seen any AI alerts?
11. Have you used the IaC proactive scanning feature to guard against potential misconfigurations?
12. Based on the Cloud Optix 30-day trial, do you have a better view into your organizations cloud security posture? Has visibility improved? Do you see the value of continuous security and compliance checking? Do you see the value of teams working together to remediate issues in a timely manner? Do you feel more confident should your organization face a security or compliance audit?

To discuss the findings of your Cloud Optix trial, or any other topics related to your cloud security posture, please contact publiccloud@sophos.com.

Thanks for choosing Sophos Cloud Optix.