

# Sophos Cloud Optix

SolutionsDay 2019

Thomas Bonde

Sophos Sales Engineer

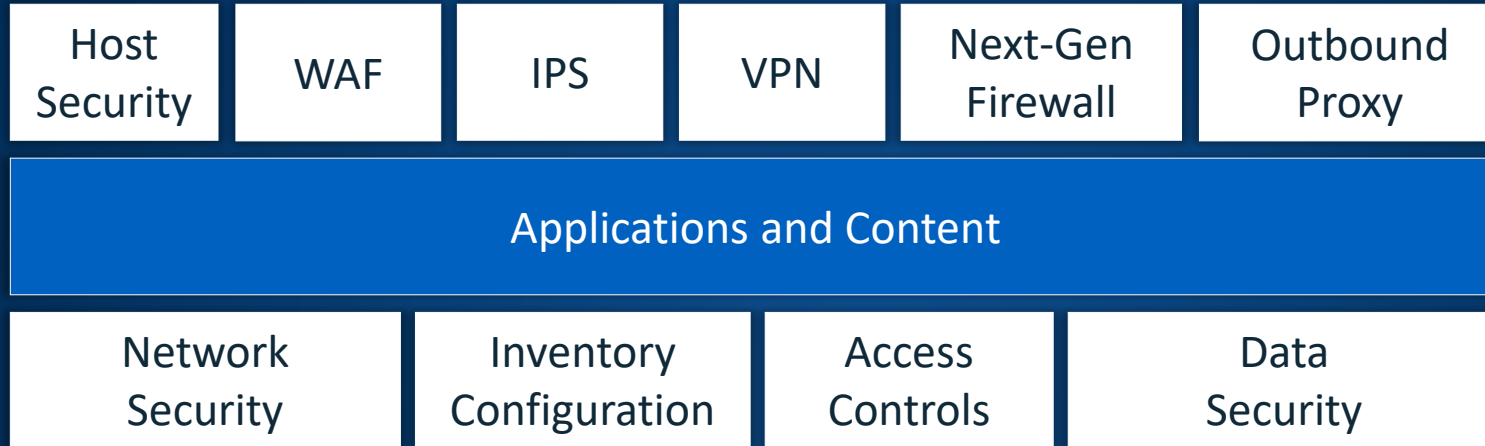
3. Oktober 2019

**SOPHOS**



# Cloud Security is a Shared Responsibility

Security  
**IN** the  
Cloud



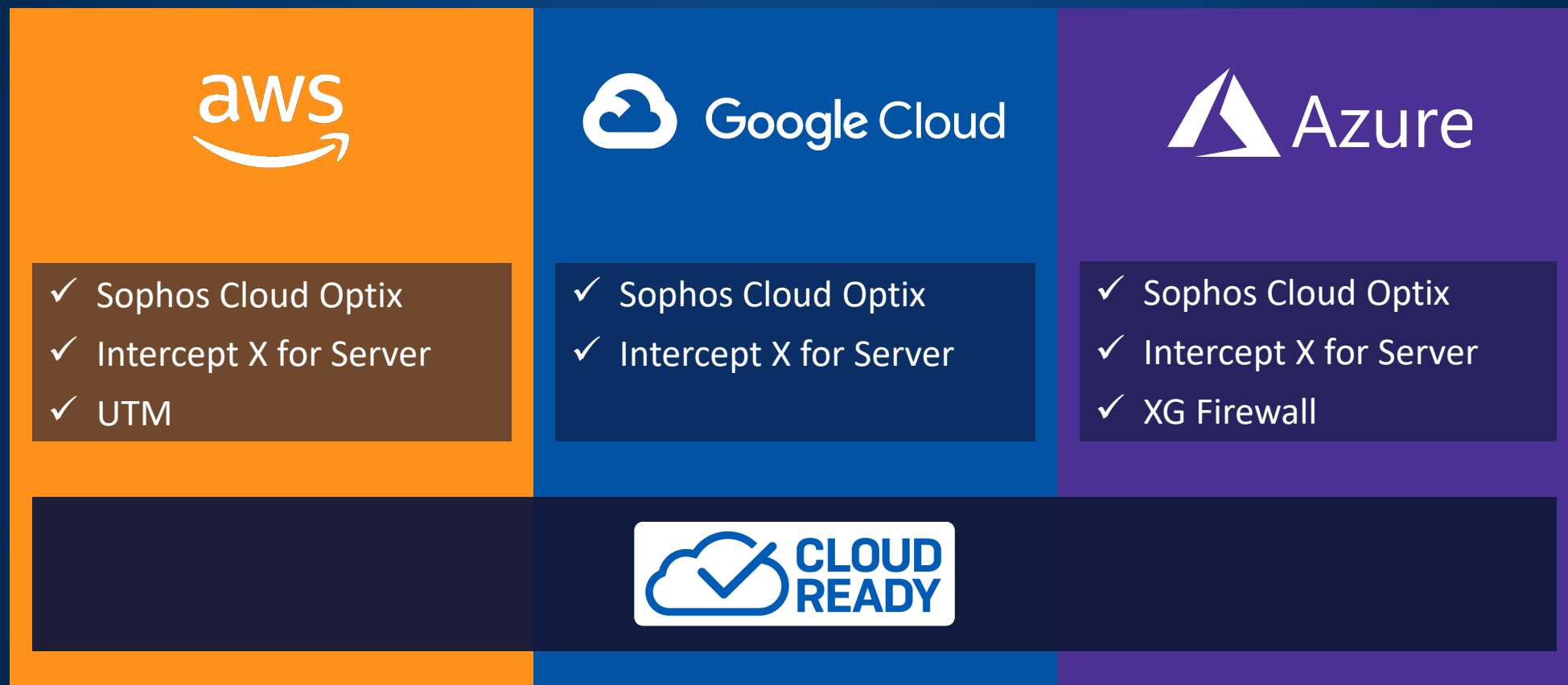
**Your  
Responsibility**

Security  
**OF** the  
Cloud



**Cloud Provider  
Responsibility**  
AWS, Azure, Google

# Sophos Cloud Ready Products



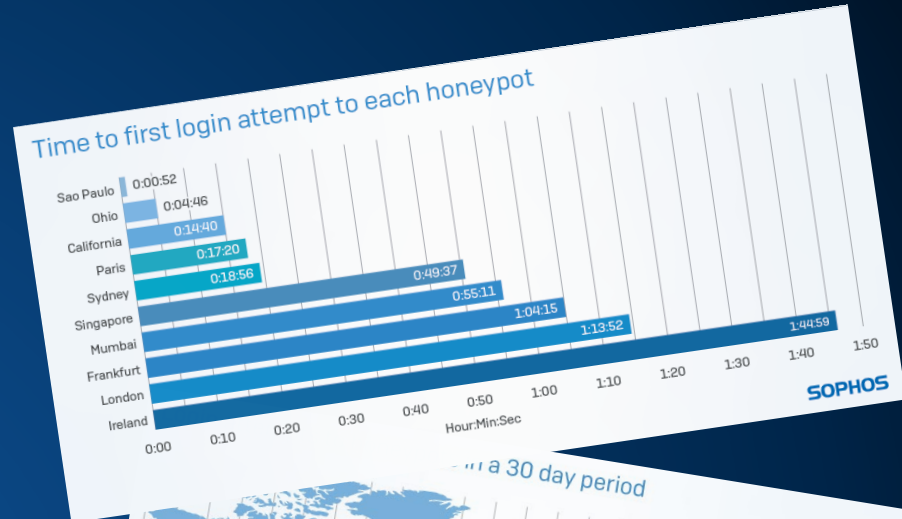
# Automated Attacks

Sophos study of 10 cloud honeypots placed worldwide, reveals the need for visibility

**5 Million**  
attempted logins  
in 30 days

**52**  
seconds to first  
login

**13**  
attempted  
logins per  
minute



# Moving to the Cloud

## The Challenges

### Visibility



If you can't see it, you  
can't secure it

### Compliance



Ever-changing, auto-  
scaling environments

### Response



Complex attacks but  
limited resources

# Sophos Cloud Optix

## The Resolution

### Visibility



If you can't see it, you  
can't secure it

Continuous Visibility

Topology Visualization

Anomaly Detection

### Compliance



Ever-changing, auto-  
scaling environments

Continuous Compliance

Compliance Customization

Compliance Collaboration

### Response



Complex attacks but  
limited resources

Drift Detection

Guardrails and Remediation

Proactive Template Scanning



# Dashboard

SOPHOS

CENTRAL

Admin

Overview

Dashboard

Alerts

Threat Analysis Center

Logs & Reports

People

Devices

Global Settings

Protect Devices

MY PRODUCTS

Endpoint Protection

Server Protection

Mobile

Encryption

Wireless

Email Gateway

Firewall Management

Phish Threat

MORE PRODUCTS

New: Sophos Cloud Optix

Free Trials

central.sophos.com/manage/cloud-optix

Help Thomas Bonde Sophos Super Admin

New: Sophos Cloud Optix

Try out the newest Sophos security solution

Solve the toughest challenges in cloud security

Start a free trial

Existing user sign in

Introducing Sophos Cloud Optix

from Sophos

01:47

Intelligent cloud visibility, compliance and threat response

Continuous visibility of your public cloud infrastructure is vital to ensure security and compliance. Multiple development teams, and an ever-changing, auto-scaling environment all make compliance and security a serious challenge for security teams.

Sophos Cloud Optix combines the power of AI and automation to simplify compliance, governance and security monitoring in the cloud.

Learn more

See everything. Secure everything

Automatic discovery of your organization's assets across AWS, Azure and Google Cloud Platform environments. Giving your team the power to respond to and remediate security risks in minutes, with complete network topology visualization and continuous asset monitoring.

Proactive cloud compliance

Raise standards without added headcount by automatically detecting changes to your cloud environments in real time. Continuously monitor compliance with custom or out-of-the box templates for standards such as CIS, PCI DSS, SOC2 and HIPAA.

AI-powered analytics and monitoring

Shrink incident response and resolution times from days or weeks to just minutes. Powerful artificial intelligence detects risky resource configurations and suspicious network behavior fast - with smart alerts and optional automatic remediation of risks.

SOPHOS


7

# Alerts

## Alerts

Smart alerts for security and compliance







Home / Alerts

 1

Critical Alerts

Alert ID	Severity	Description
A-000335	Critical	Flag resource(s) with public IP and Security Group with ingress from any source on any port

### Details



Critical

**Summary :** Flag resource(s) with public IP and Security Group with ingress from any source on any port

**Description:** This check flags resources that are likely open to the world on all ports. If a resource is flagged on this list, review and change security group and/or other firewall rules to block traffic to all ports.

**Remediation:** Update the rules for the default security group to deny all traffic by default and only allow specific ports as needed. <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#default-security-group>

**Alert Id :** A-000335




**Environment :** Sophos SE (AWS)

**Last Seen :** 2019-09-30 22:56:02 (16 hours ago)

**Ticket ID(s) :**

**Suppressed Resource count :** 1 / 9

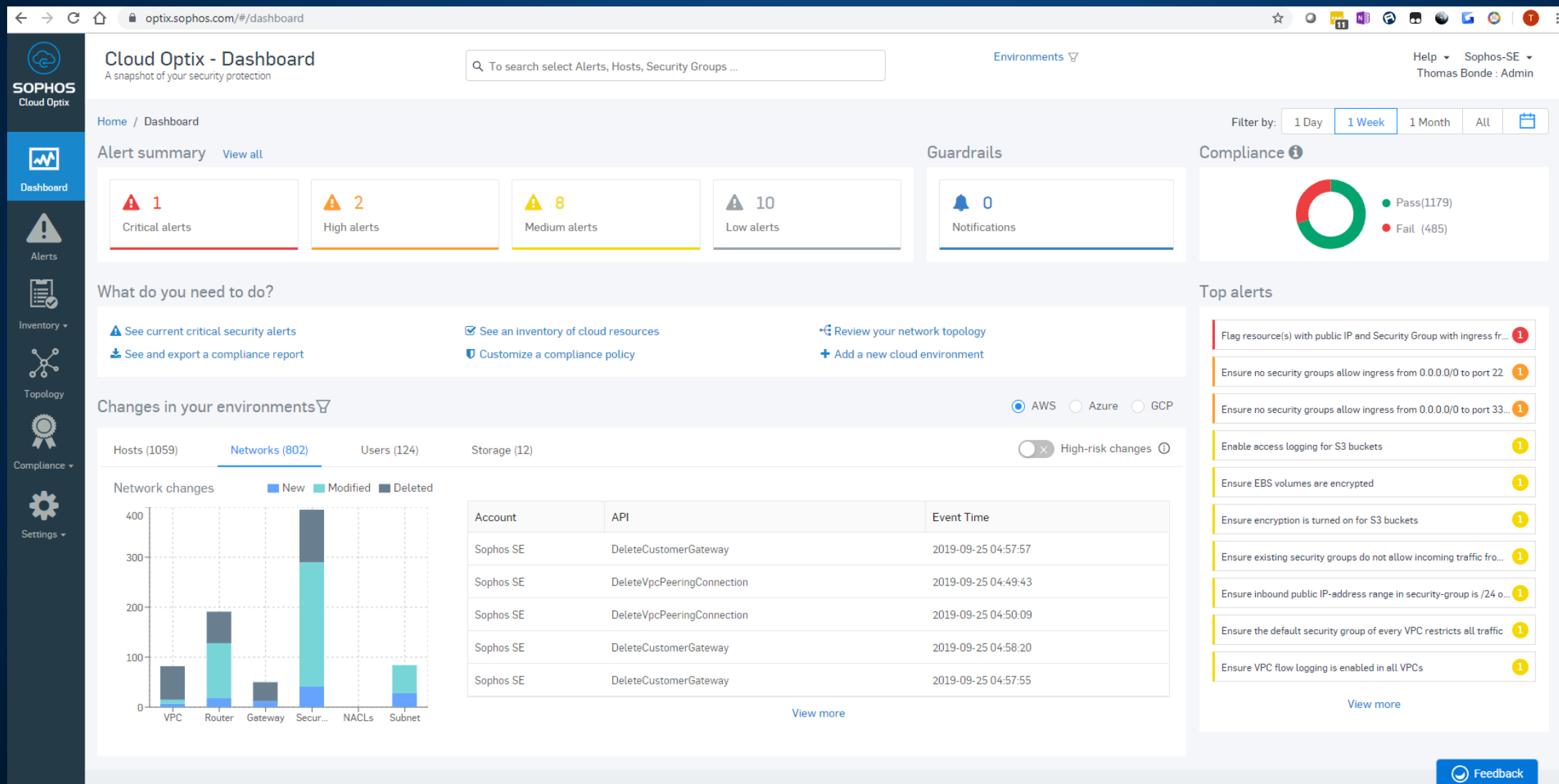
**Affected Resources :**

Resource	Last modified by	FirstSeen
 Queen UTM (i-0cfd2eefb51a7c59a) - EC2	JL-test-UTM-QueenRole-1S5GFF0WTZLVG	16 hours ago
 Worker UTM (i-0a62e736f24995309) - EC2	AWSServiceRoleForAutoScaling	a day ago
 Worker UTM (i-040c9ec6d69d15b1f) - EC2	AWSServiceRoleForAutoScaling	a day ago

Close



# Dashboard



# Inventory

Dashboard

Alerts

Inventory

Host

Containers

Network

Storage

IAM Users

Serverless

Activity Logs

Topology

Compliance

Settings

Home / Inventory / Hosts - AWS

28  
Total

28  
Public

27  
Running

1  
Stopped

0  
Running Containers

Search this page

Reset | Export as

< 1 2 3 > 10 / page

Name/Id	Last modified by	Environment	Size	AZ	Status	Launch Time	Security Group	Public DNS/IP	Patched	View
TAM-PMX i-07d86026a610f2652	NA	Sophos SE	t2.large	us-west-2a	running	2018-08-01 23:33:00 a year ago	smtp-pmx	34.219.75.169		
red-dev-tools-test i-0913adfd07a0e944d	NSGPlayground-SAML-Admin	Sophos SE	t3.medium	eu-west-1a	running	2019-04-25 13:07:19 5 months ago	RED DB-TOOLS RED Base	63.34.107.55		
red-prov-test-01 i-0f18875eed763b4c8	NSGPlayground-SAML-Admin	Sophos SE	t3.medium	eu-west-1a	running	2019-04-25 13:07:13 5 months ago	RED Base RED Prov	34.253.172.52		
Let's Encrypt Monitoring i-00843d820083e6529	NA	Sophos SE	t2.small	us-east-1f	running	2018-11-22 17:16:14 10 months ago	launch-wizard-15	100.24.118.192		
Windows2016CentralServerProtection i-043b663d186c51893	NSGPlayground-SAML-Admin	Sophos SE	t2.medium	ap-southeast-2b	running	2019-01-31 04:32:04 8 months ago	launch-wizard-6	54.252.249.103		
AmazonLinuxPG i-077edf46a71dc7da0	NSGPlayground-SAML-Admin	Sophos SE	t2.micro	ap-southeast-1a	running	2019-05-28 08:02:00 4 months ago	PG SSH from Sydney of fice	13.251.156.222		
Amazon Linux 10.88.1125 i-0b29e967ac2dc1347	NSGPlayground-SAML-Admin	Sophos SE	t2.micro	us-east-1c	running	2019-03-14 14:53:17 7 months ago	launch-wizard-7	54.89.198.59		
i-0b62e4200b69ea4f7	NA	Sophos-SG-Kw	t2.micro	ap-southeast-1a	running	2019-09-19 08:49:01 12 days ago	launch-wizard-1	3.1195.222		
GrantLinuxClient						2019-01-04 22:37:34	GrantTestSG			

S3

Total 59

6  
Total Vnets

7  
Total Sec. Groups

Open

Unused

Disabled

Feedback

Feedback

# Topology

Dashboard

Alerts

Inventory

Topology

Compliance

Settings

Select Tag(s) to collapse

Search Security group(s)

Search (id / name)

Show inferred DBs/Apps

Show K8s nodes

Internet Gateway

vpc-6873ff12

us-east-1f

us-east-1e

us-east-1a

us-east-1b

us-east-1d

us-east-1c

Web-tier

Web-tier

Web-tier

Web-tier

Web-tier

Test-We...

i-Od48of...

Web-tier

Web-tier

Web-tier

OptixDe...

172.31.64.0/20

172.31.0.0/20

172.31.48.0/20

172.31.80.0/20

172.31.32.0/20

172.31.16.0/20

Web-tier

Web-tier

Web-tier

172.31.23.145

34.239.245.167

Inbound traffic ports

8080 : TCP

Outbound traffic ports

None

Feedback

SOPHOS

11

# Compliance

Dashboard

Alerts

Inventory

Topology

**Compliance**

Policies

Reports

Settings

## Compliance

Governance, risk and compliance automation

To search select Alerts, Hosts, Security Groups ...

Environments

Help   Sophos Cloud Optimix Demo   Demo : Read Only

Home / Policies

Select Provider All

Out of the Box Policies 35   Custom Policies 6

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

<input type="checkbox"/>	Name	Provider	Total Rules	Author	Updated On	Enable	Action
<input type="checkbox"/>	AWS - CIS Benchmark v1.1	aws	46	System	2019-08-30 07:10	<input checked="" type="checkbox"/>	Customize
<input type="checkbox"/>	AWS - EBU R 143	aws	33	System	2019-08-30 07:09	<input checked="" type="checkbox"/>	Customize
<input type="checkbox"/>	AWS - FEDRAMP-LowBaseline Compliance	aws	291	System	2019-08-30 07:17	<input checked="" type="checkbox"/>	Customize
<input type="checkbox"/>	AWS - FEDRAMP/NIST800-53-High Compliance	aws	405	System	2019-08-30 07:24	<input checked="" type="checkbox"/>	Customize
<input type="checkbox"/>	AWS - FEDRAMP/NIST800-53-Low Compliance	aws	291	System	2019-08-30 07:15	<input checked="" type="checkbox"/>	Customize
<input type="checkbox"/>	AWS - FEDRAMP/NIST800-53-Moderate Compliance	aws	376	System	2019-08-30 07:23	<input checked="" type="checkbox"/>	Customize
<input type="checkbox"/>	AWS - FFIEC Cybersecurity Assessment	aws	78	System	2019-08-30 07:13	<input checked="" type="checkbox"/>	Customize
<input type="checkbox"/>	AWS - GDPR	aws	95	System	2019-08-30 07:10	<input checked="" type="checkbox"/>	Customize
<input type="checkbox"/>	AWS - HIPAA Security Rule	aws	82	System	2019-08-30 07:14	<input checked="" type="checkbox"/>	Customize

AWS - FEDRAMP-LowBaseline Compliance

46.39%

48.45%

50.52%

49.65%

# Compliance – PCI DSS 3.2

<div>Dashboard</div> <div>Alerts</div> <div>Inventory</div> <div>Topology</div> <div>Compliance</div> <div>Policies</div> <div>Reports</div> <div>Settings</div> <div>Reports</div>	1.0 Secure Network and Systems (Req 1, 2) <b>6 out of 13 Failed</b>					
	Result	#	Rule Summary	Control Id	Rule #	Affected Resources
	Failed	1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic		AZ-2057	Ensure that 'Network security groups' is set to 'On' <a href="#">more details...</a>
	Failed	1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic		AZ-2301	Ensure that RDP access is restricted from the internet • test2-nsg <a href="#">more details...</a>
	Failed	1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic		AZ-2302	Ensure that SSH access is restricted from the Internet • test2-nsg <a href="#">more details...</a>
	Failed	1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.		AZ-2057	Ensure that 'Network security groups' is set to 'On' <a href="#">more details...</a>
	Failed	1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.		AZ-2301	Ensure that RDP access is restricted from the internet • test2-nsg <a href="#">more details...</a>
	Failed	1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.		AZ-2302	Ensure that SSH access is restricted from the Internet • test2-nsg <a href="#">more details...</a>

# Compliance – PCI DSS 3.2

Environment Name:  
PCGOptix Sophos Demo

1.0 Secure Network and Systems

Result	#	Rule Summary
Failed	1.2.1	Restrict in that which data environment other traffic
Failed	1.2.1	Restrict in that which data environment other traffic
Failed	1.2.1	Restrict in that which data environment other traffic
Failed	1.3	Prohibit direct Internet access to cardholder data environment
Failed	1.3	Prohibit direct Internet access to cardholder data environment
Failed	1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.

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 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>

Alert Id :

A-000810

Environment :

PCGOptix Sophos Demo (Azure)

Last Seen :

2019-06-12 10:58:15 (4 months ago)

Suppressed Resource count :

0 / 1

Affected Resources :

Resource	Last modified by	FirstSeen
test2-nsg	NA	4 months ago

Close

AZ-2302

Ensure that SSH access is restricted from the Internet

• test2-nsg  
more details...



# Summary

Continuous Assessments

Unlimited Admin Users

## Multi-Cloud

Amazon Web Services  
Microsoft Azure  
Google Cloud Platform

## Agentless SaaS

Integrates using native  
cloud provider APIs, logs  
and cloud services

## Fast Setup

Simple script creates Read  
Only access, with visibility  
in under 10 minutes

## MULTI PLATFORM

Amazon Web Services, Microsoft Azure,  
and Google Cloud Platform

## 100 ASSETS

Server and database instances

## CONTINUOUS

Compliance assessments

## UNLIMITED

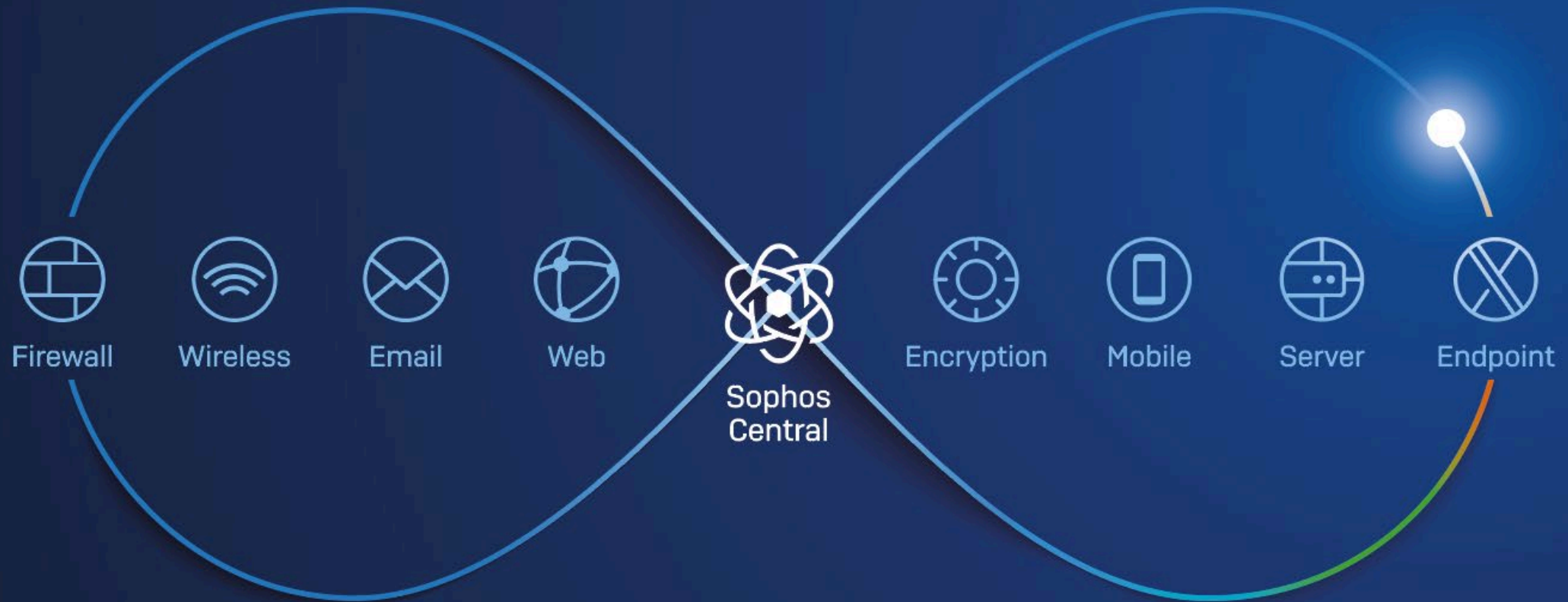
Admin Users

## Simple Licensing



# Synchronized Security

## Cybersecurity as a System



[sophos.com/synchronized](https://sophos.com/synchronized)

# Sophos Produkte

SOPHOS

CENTRAL

Admin

Overview

Dashboard

Alerts

Threat Analysis Center

Logs & Reports

People

Devices

Global Settings

Protect Devices

MY PRODUCTS

Endpoint Protection

Server Protection

Mobile

Encryption

Wireless

Email Gateway

Firewall Management

Phish Threat

MORE PRODUCTS

New: Sophos Cloud Optix

Free Trials

central.sophos.com/manage/cloud-optix

Help Thomas Bonde Sophos Super Admin

New: Sophos Cloud Optix

Try out the newest Sophos security solution

Solve the toughest challenges in cloud security

Start a free trial

Existing user sign in

Introducing Sophos Cloud Optix

from Sophos

01:47

Intelligent cloud visibility, compliance and threat response

Continuous visibility of your public cloud infrastructure is vital to ensure security and compliance. Multiple development teams, and an ever-changing, auto-scaling environment all make compliance and security a serious challenge for security teams.

Sophos Cloud Optix combines the power of AI and automation to simplify compliance, governance and security monitoring in the cloud.

Learn more

See everything. Secure everything

Automatic discovery of your organization's assets across AWS, Azure and Google Cloud Platform environments. Giving your team the power to respond to and remediate security risks in minutes, with complete network topology visualization and continuous asset monitoring.

Proactive cloud compliance

Raise standards without added headcount by automatically detecting changes to your cloud environments in real time. Continuously monitor compliance with custom or out-of-the box templates for standards such as CIS, PCI DSS, SOC2 and HIPAA.

AI-powered analytics and monitoring

Shrink incident response and resolution times from days or weeks to just minutes. Powerful artificial intelligence detects risky resource configurations and suspicious network behavior fast - with smart alerts and optional automatic remediation of risks.

SOPHOS

18

# SOPHOS Cloud ptix

Solve the toughest challenges in cloud security

## Tak for Jeres tid!