

# Proteger la nube pública: 7 prácticas recomendadas



Google Cloud



Azure

**José R. Lara**

ATG / SAVANT CONSULTORES

8 ABRIL 2020

**SOPHOS**



## José R. Lara

Asterisk Technology Group / Savant Consultores

- Sophos Certified Engineer
- CompTia Security+
- PECB ISO/IEC 27001 Implementer
- PECB ISO/IEC 31000 Risk Manager
- PECB ISO/IEC 27032 Cybersecurity Manager
- Mikrotik Certified Security Engineer (MTCSE)

# La nube pública se utiliza de muchas formas



## Almacenar datos

Almacenar archivos que tradicionalmente se almacenaban en servidores locales



## Ejecutar aplicaciones web

Ejecutar sitios web y ofertas de servicios



## Desarrollo de software

Escribir y probar código; crear productos de software



# Y ofrece muchas ventajas



OpEx, no CapEx



Economías de  
escala



Totalmente  
escalable



Más velocidad



Sin centros de  
datos

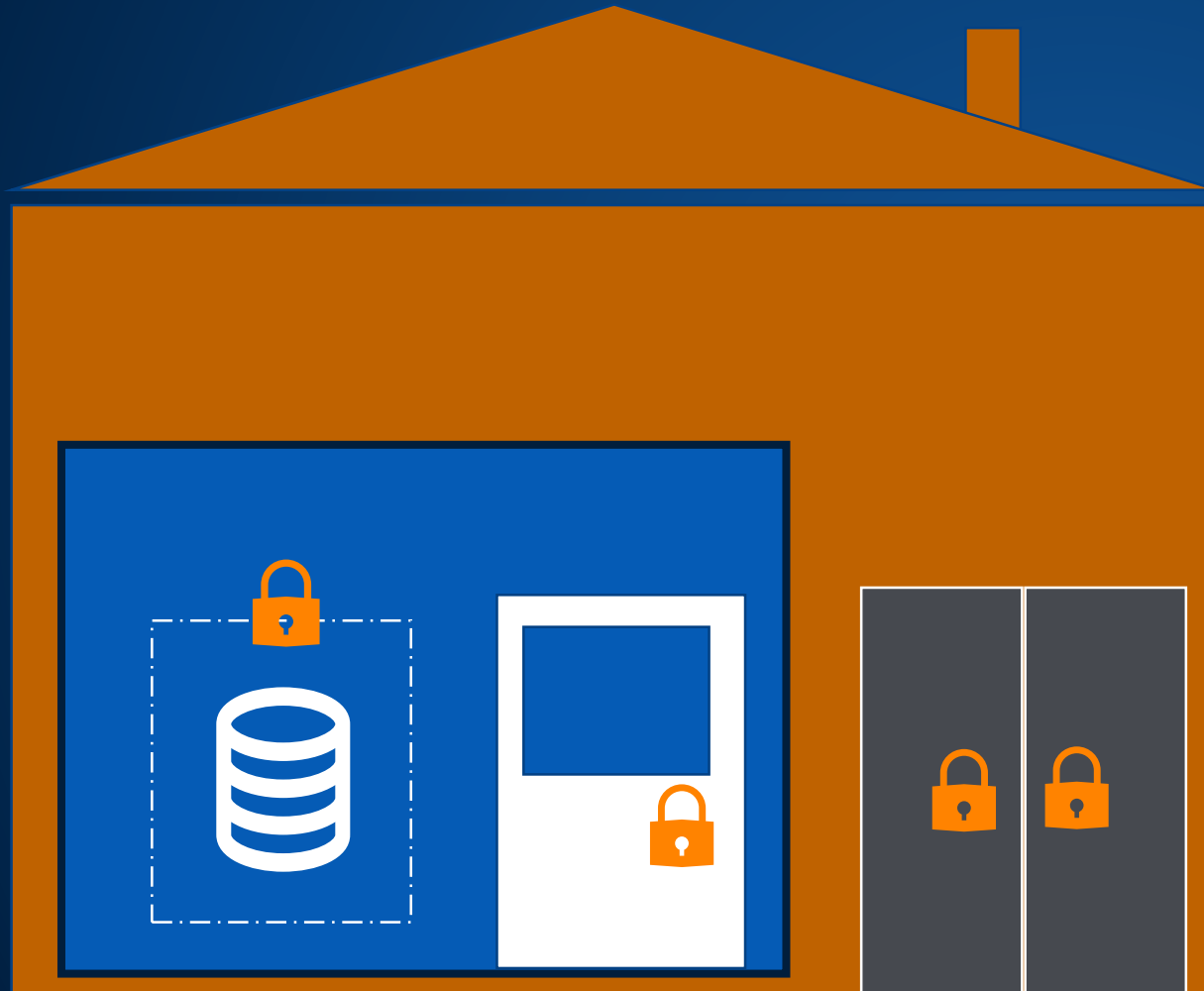


Global

# Seguridad tradicional frente a seguridad en la nube pública



# Seguridad física frente a seguridad lógica

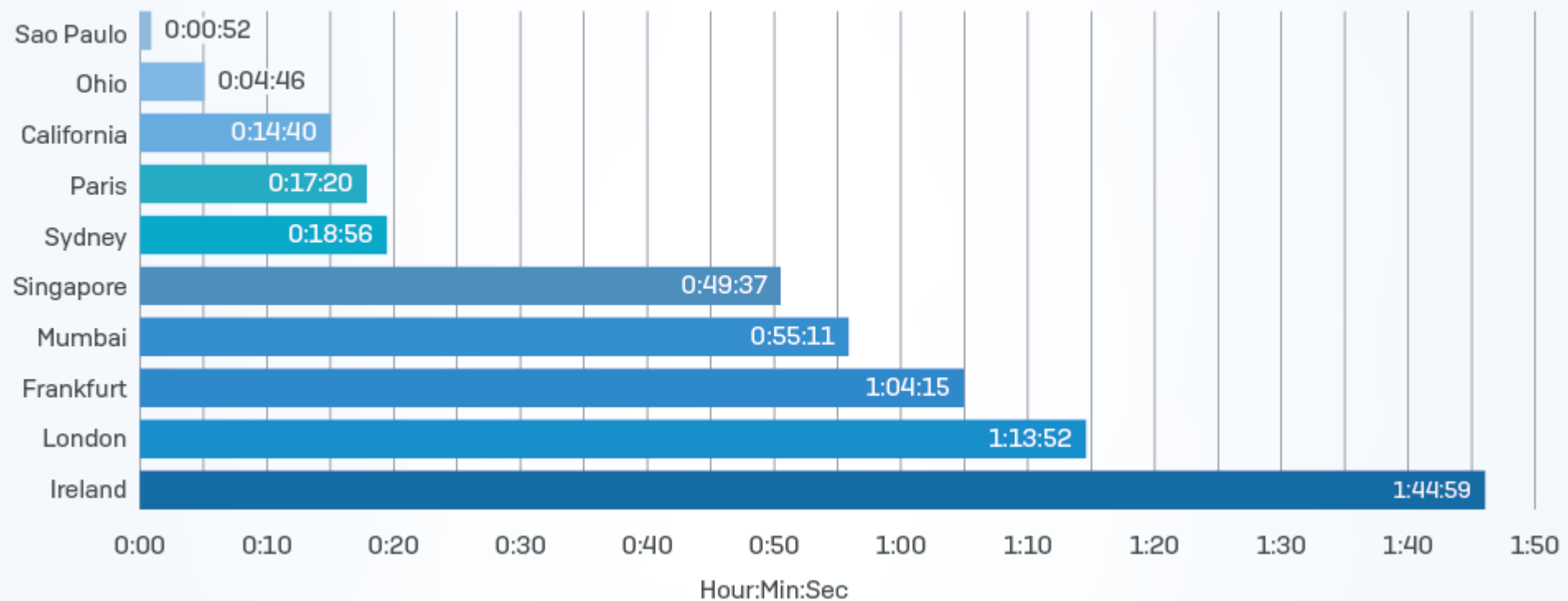


# Consideraciones de la seguridad en la nube

**SOPHOS**

# Ataques automatizados

Time to first login attempt to each honeypot



SOPHOS

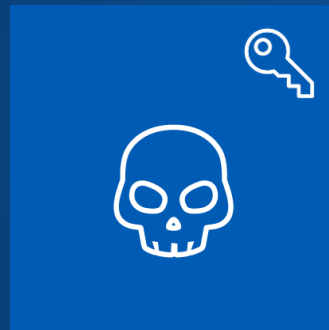


# Ataque de criptojacking automatizado



EQUIPO  
DE DESARROLLO  
GLOBAL

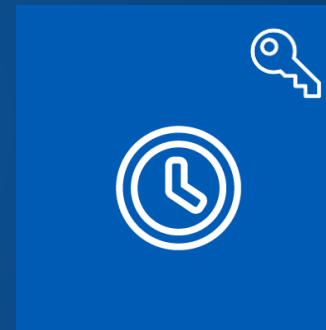
## LÍNEA TEMPORAL DEL ATAQUE ▶



Endpoint  
comprometido/  
clave robada



El atacante  
accede a la  
cuenta en la  
nube



El atacante  
supervisa la  
productividad



Automatiza el  
aprovisionamiento  
de instancias



Endurece la  
configuración y  
revoca el acceso



Acceso mediante credenciales



Acceso mediante API

# Ciclo de lanzamiento más corto



# Retos del cumplimiento



Comprobaciones  
periódicas

Equipos centralizados



Comprobaciones  
continuas

Equipos fragmentados

# Seguridad en la nube pública

**«Casi todos los ataques exitosos contra servicios en la nube se producen porque el cliente establece configuraciones incorrectas, realiza gestiones inadecuadas y comete errores».**













The Gartner logo is displayed in a light blue color, featuring the word "Gartner" in a bold, sans-serif font with a registered trademark symbol.



*Fuente: Gartner Innovation Insight for Cloud Security Posture Management, Neil MacDonald, 25 de enero de 2019*

# 7 prácticas recomendadas

# Conozca sus responsabilidades

# N.º 1

Shared Responsibility Security Model	On-Premises	Public Cloud	Why?
Users			Enforce authentication, define access restrictions, and track credential use.
Data			Stop data loss, define and enforce who can access what data, while ensuring compliance standards are met.
Applications			Prevent application compromise through policy, patching, and security.
Network Controls			Track and enforce network access permissions.
Host Infrastructure			Manage and secure operating systems, storage solutions and related systems to prevent unpatched bugs and privilege escalations.
Physical Security			Restrict physical access to systems and design redundancy to prevent single point of failure.

 Customer       Platform Provider

# Modelo de responsabilidad compartida



# Modelo de responsabilidad compartida





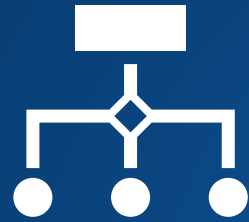
# Planifique para múltiples nubes

# N.º 2

TIPO DE USO	N.º DE NUBES PÚBLICAS (entre usuarios de la nube pública)
Utilizando actualmente	2,0
Experimentando con	1,8
Total	3,8

# Véalo todo

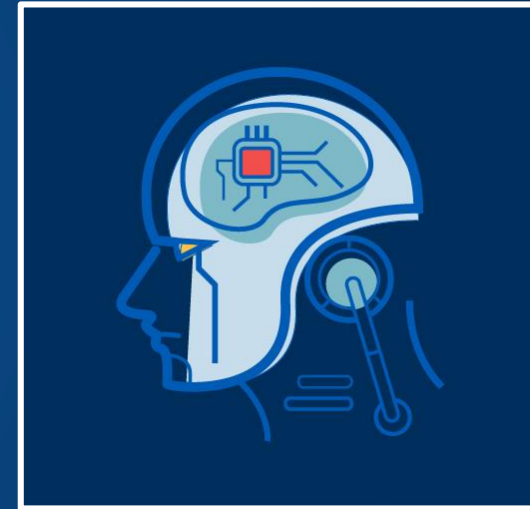
# N.º 3



Topología de la red

Flujo del tráfico

Desglose completo del inventario

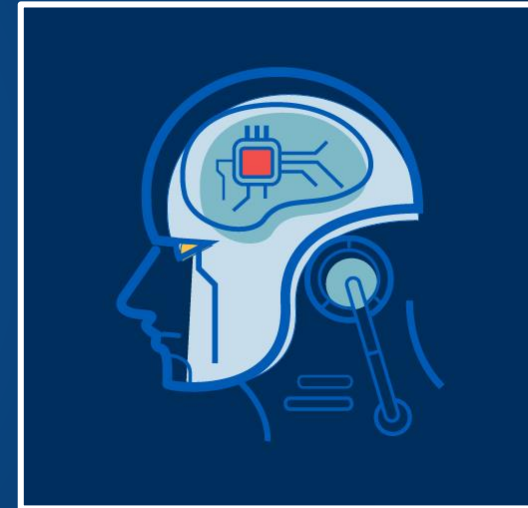




Bases de datos con puertos abiertos

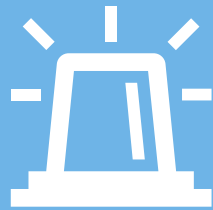
Servicios públicos Amazon Simple Storage Service (Amazon S3)

Comportamientos de inicio de sesión y llamadas a la API sospechosos



# Integre el cumplimiento en los procesos diarios

# N.º 4



 Jira Software

**servicenow**<sup>TM</sup>

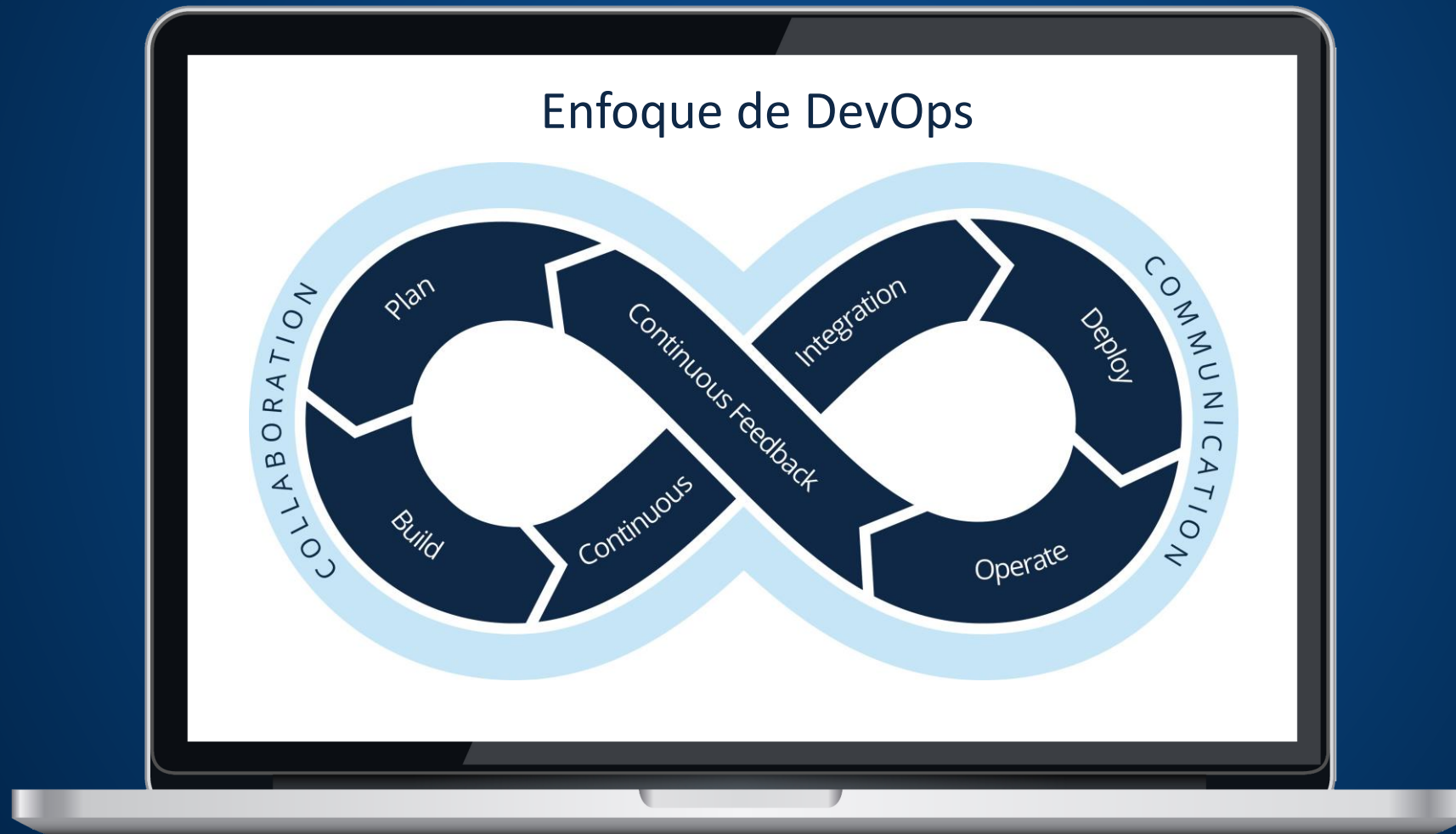


**Instantáneas en tiempo real**

**Detecte cambios automáticamente**

# Automatice sus controles de seguridad

# N.º 5





# Automatice sus controles de seguridad

# N.º 5

VISTO POR  
DESARROLLADORES



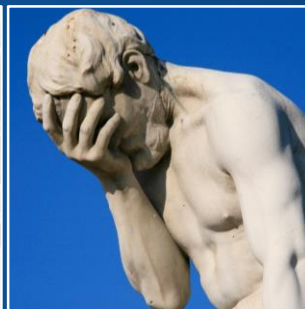
VISTO POR  
DISEÑADORES



VISTO POR  
GESTORES DE  
PROYECTOS



VISTO POR  
CONTROL DE  
CALIDAD



VISTO POR  
ADMINISTRADORES  
DEL SISTEMA



VISTO POR  
SEGURIDAD



DESARROLLADORES

SEGURIDAD



# Automatice sus controles de seguridad

N.º 5

- ✓ Repare automáticamente las vulnerabilidades y los recursos de acceso de los usuarios
- ✓ Identifique llamadas a la API y eventos de inicio de sesión en la consola sospechosos
- ✓ Informe de anomalías en el tráfico de salida
- ✓ Revele cargas de trabajo de aplicaciones ocultas

# Proteja TODOS sus entornos (incluidos los de desarrollo y control de calidad)

# N.º 6





# Aplique sus conocimientos de seguridad local

# N.º 7



**FIREWALL**



**PROTECCIÓN DE  
SERVIDORES**



**PROTECCIÓN DE  
ENDPOINTS**



**PROTECCIÓN DE  
CORREO  
ELECTRÓNICO**

**SOPHOS**  
Cloud  ptix

See everything. Secure everything

## VISIBILIDAD

Recursos en AWS, Microsoft Azure  
y Google Cloud Platform

## CUMPLIMIENTO

Informes y cumplimiento basados en  
comportamientos y prácticas recomendadas

## RESPUESTA

Remediación instantánea y  
respuesta a incidentes



See everything. Secure everything

# Visibilidad inteligente

The screenshot displays the 'Topology' interface of Sophos Cloud Optimizer. The main area shows a network diagram with an Internet Gateway at the top center. Below it, there are two subnets: 'us-east-1d' and 'us-east-1c'. The 'us-east-1d' subnet contains a 'Worker ...' instance (10.88.5.0/24) and a 'Queen U...' instance (10.88.1.0/24). The 'us-east-1c' subnet contains an 'Amazon ...' instance (10.88.100.0/24) and a 'Worker ...' instance (10.88.4.0/24). Additionally, there is a 'LoadBal...' instance (10.88.50.0/24) and a 'bmysql...' instance (10.88.50.0/24) in the 'OGWSubnetAZ1C' subnet. The diagram shows connections between these instances and the Internet Gateway. On the right side, there is a 'Controls' panel with options for 'Traffic' and 'Security Group', and a 'Resource Details' panel.

**Topology**  
Interactive view of your cloud environments

Home / Topology

Select Tag(s) to collapse ▾ Search Security group(s) ▾ Search (id / name) 🔍 Show inferred DBs  Show K8s nodes

**Controls**

- Traffic
- Security Group

All traffic:

Inbound traffic:

Outbound traffic:

Internal traffic:

Diagram Details ⓘ

**Resource Details**

# Cumplimiento continuo

The screenshot displays the Sophos Cloud Optix Compliance dashboard. The main content area shows a policy report for 'Setup Encryption at rest for RDS instances' with a severity of 'Medium'. The report includes a summary, description, remediation steps, alert ID, environment, last seen date, and a table of affected resources.

**Details**

**Medium**

**Summary :** Setup Encryption at rest for RDS instances

**Description:** AWS provides encryption at rest for RDS instances which should be enabled to ensure the integrity and confidentiality of data stored within the databases. This is especially useful if the RDS instance stores sensitive user data like personally identifiable information, credit card details, medical records etc.

**Remediation:** RDS does not currently allow modifications to encryption after the instance has been launched, so a new instance will need to be created with encryption enabled.  
<http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html>

**Alert Id :** A-000054

**Environment :** OptixDemo-AWS (AWS)

**Last Seen :** 2019-03-29 13:23:27 (a day ago)

**Suppressed Resource count :** 0 / 1

**Affected Resources :**

Resource	Last modified by	FirstSeen
OptixDemodb	NA	a day ago

 Jira Software  
 servicenow™

- Supervisión continua
- Políticas personalizadas
- Plantillas predefinidas
- CIS, SOC2, HIPAA, ISO 27001 y PCI DSS
- Integración con JIRA y ServiceNow

# Alertas y respuesta con IA

**Alerts**  
Smart alerts for security and compliance

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

Environments

Help | Sophos Cloud Optix Demo | Demo

Home / Alerts

Filter by: 1 Day | 1 Week | 1 Month | All

Alert Summary

Show Suppressed Alerts: OFF ON | Reset | Export as

Alert ID	Severity	Description	Type	Affected Resources	Last Seen	Provider	Enviro
A-000092	Critical	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have console access		• DemotestIAMUserNoMFA <a href="#">more details...</a>	a day ago	AWS	OptixDe
A-000071	High	Enable MFA delete for cloudtrail bucket deletion		• avid-cloudtrail-760068489120 <a href="#">more details...</a>	a day ago	AWS	OptixDe
A-000059	High	Ensure a log metric filter and alarm exist for CloudTrail configuration changes		• No Metric filters were found for CloudTrail. <a href="#">more details...</a>	a day ago	AWS	OptixDe
A-000055	High	Ensure a log metric filter and alarm exist		• No Metric filters were found for CloudTrail.	a day ago	AWS	OptixDe

- Detecte patrones de tráfico sospechosos
- Escanee las plantillas de infraestructura como código
- Identifique claves de acceso compartido
- Cierre puertos y buckets de almacenamiento abiertos
- Detecte desviaciones en la configuración
- Establezca defensas preventivas



# Panel de control intuitivo

The screenshot displays the Sophos Cloud Optix dashboard. At the top, there's a search bar and navigation options. The main content is divided into several sections:

- Alert summary:** Shows 1 Critical Alert, 3 High Alerts, 12 Medium Alerts, and 31 Low Alerts.
- Compliance:** A donut chart shows 79 Pass and 47 Fail.
- What do you need to do?:** A list of tasks like 'See current critical security alerts' and 'Review your network topology'.
- Changes in your environments:** A bar chart shows 8 network changes (all modified) and a table of events.
- Top alerts:** A list of specific alerts like 'Ensure multi-factor authentication (MFA) is enabled'.

Account	API	Event Time
OptixDemo-AWS	RevokeSecurityGroupIngress	2019-03-29 14:13:02
OptixDemo-AWS	RevokeSecurityGroupIngress	2019-03-29 14:16:48
OptixDemo-AWS	RevokeSecurityGroupIngress	2019-03-29 14:10:42
OptixDemo-AWS	RevokeSecurityGroupIngress	2019-03-29 14:13:42
OptixDemo-AWS	AuthorizeSecurityGroupIngress	2019-03-29 14:16:48

- Veá el resumen de alertas
- Vista rápida del estado de cumplimiento
- Veá y exporte informes de cumplimiento
- Revise el inventario
- Veá la topología de la red
- Identifique cambios en los entornos

# Historias de éxito

The HubSpot logo is displayed in white text on an orange rectangular background. The logo consists of the word "HubSpot" in a sans-serif font, with a stylized robot head icon integrated into the letter "o".

«Porque gracias a los diagramas de visualización de la topología de red en tiempo real y las plantillas de cumplimiento predefinidas, **hemos podido ahorrar semanas de trabajo** a la hora de prepararnos para nuestra auditoría SOC 2.

Esta es la primera vez que he estado deseando proporcionar pruebas a nuestros auditores».

*Ryan Stinson, director de ingeniería de seguridad, HubSpot Inc.*



# Plan de acción en la nube pública de siete pasos

1. Conozca sus responsabilidades
2. Planifique para múltiples nubes
3. Véalo todo
4. Integre el cumplimiento en sus procesos diarios
5. Automatice sus controles de seguridad
6. Proteja TODOS sus entornos (incluidos los de desarrollo y control de calidad)
7. Aplique sus conocimientos de seguridad local

# ¡Gracias!

José R. Lara

Pruebe Sophos Cloud Optix en [es.sophos.com/cloud-optix](https://es.sophos.com/cloud-optix).

**SOPHOS**