

SOPHOS DISCOVER 2019

EVOLVE

Breakout session
Sophos Cloud Optix

Sophos Cloud Optix

Secure your Cloud environment

Letterio La Spada
Sales Engineer - Italy

14 Giugno 2019 – Italian Sophos Evolve Event

SOPHOS

SOPHOS
Cloud  ptix

See everything. Secure everything

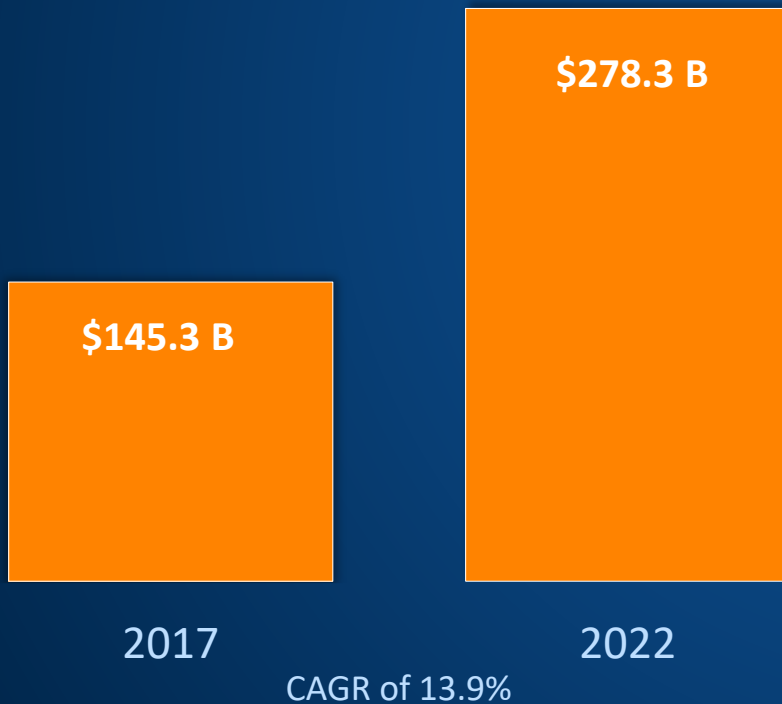
SOPHOS

Cloud Security Market

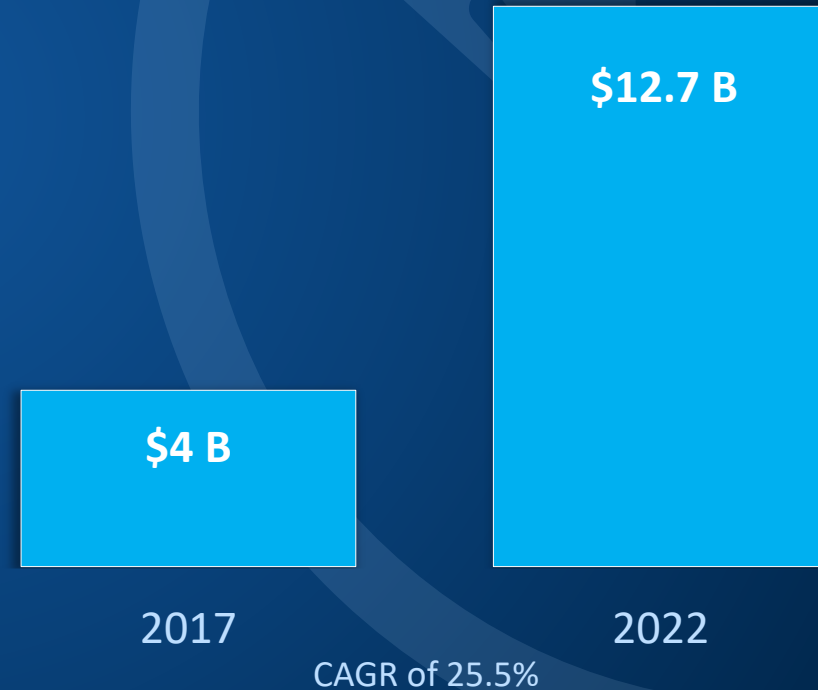
SOPHOS

Growth of Public Cloud Security

Worldwide public cloud services revenue growth
(Billions USD)



Global cloud security market growth
(Billions USD)



Public Cloud Revenue Forecast

Worldwide Public Cloud Service Revenue Forecast (Billions of USD)

	2017	2018	2019	2020	2021
Cloud Business process Services (BPaaS)	42.2	46.6	50.3	54.1	58.1
Cloud Application Infrastructure Services (PaaS)	11.9	15.2	18.8	23	27.7
Cloud Application Services (SaaS)	58.8	72.2	85.1	98.9	113.1
Cloud Management and Security Services	8.7	10.7	12.5	14.4	16.3
Cloud System Infrastructure Services (IaaS)	23.6	31	39.5	49.9	63
Total Market	145.3	175.8	206.2	240.3	278.3

BPaaS = business process as a Service; IaaS = Infrastructure as a Service; PaaS = Platform as a Service; SaaS = Software as a Service.

Note: Total may not add up due to rounding | Source: Gartner (Sept 2018)

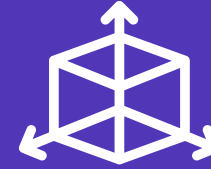
Benefits of Cloud Computing



**Trade CapEx
for OpEx**



**Benefit from massive
economies of scale**



**Stop Guessing
Capacity**



**Increase Speed
and Agility**



**No more expensive
data centers**

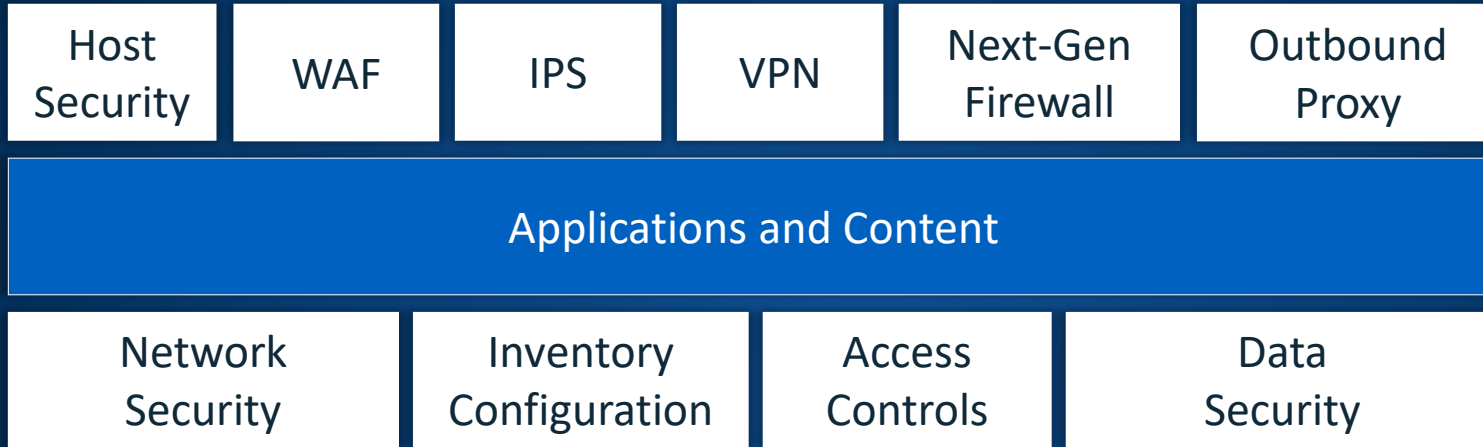


**Go global in
minutes**

Shared Security Model

Cloud Security is a Shared Responsibility

Security
IN the
Cloud



**Your
Responsibility**

Security
OF the
Cloud



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

Security Best Practices

The screenshot shows a web browser window with the URL <https://docs.microsoft.com/en-us/azure/security/azure-security-network-security-best-practices>. The browser's address bar and a row of bookmarks (Sophos Hub, Staff Info, Wiki Sophos, OCP Catalog, Salesforce, SalePartnerConnect, CSP Partner Dashboa, Expenses & Travel) are visible. On the left, a navigation sidebar is shown with a search box labeled 'Filter by title'. The sidebar menu includes categories like 'Infrastructure security', 'IaaS security', 'Identity management', 'Network security', and 'Resources'. Under 'Network security', 'Best practices' is selected and highlighted in blue. The main content area features the heading 'Use virtual network appliances' followed by a paragraph explaining that NSGs and user-defined routing provide network security at the network and transport layers of the OSI model, but virtual network security appliances are recommended for high-level security. A list of capabilities is provided, including firewalls, intrusion detection, vulnerability management, application control, anomaly detection, web filtering, antivirus, and botnet protection. The text concludes by directing users to the Azure Marketplace to find these appliances.

connections to the internet from your Azure virtual machines.

Use virtual network appliances

NSGs and user-defined routing can provide a certain measure of network security at the network and transport layers of the [OSI model](#). But in some situations, you want or need to enable security at high levels of the stack. In such situations, we recommend that you deploy virtual network security appliances provided by Azure partners.

Azure network security appliances can deliver better security than what network-level controls provide. Network security capabilities of virtual network security appliances include:

- Firewalling
- Intrusion detection/intrusion prevention
- Vulnerability management
- Application control
- Network-based anomaly detection
- Web filtering
- Antivirus
- Botnet protection

To find available Azure virtual network security appliances, go to the [Azure Marketplace](#) and search for "security" and "network security."

Public Cloud Security Breaches

1 in 6

of Amazon's S3 storage
buckets leaking sensitive data
and company secrets

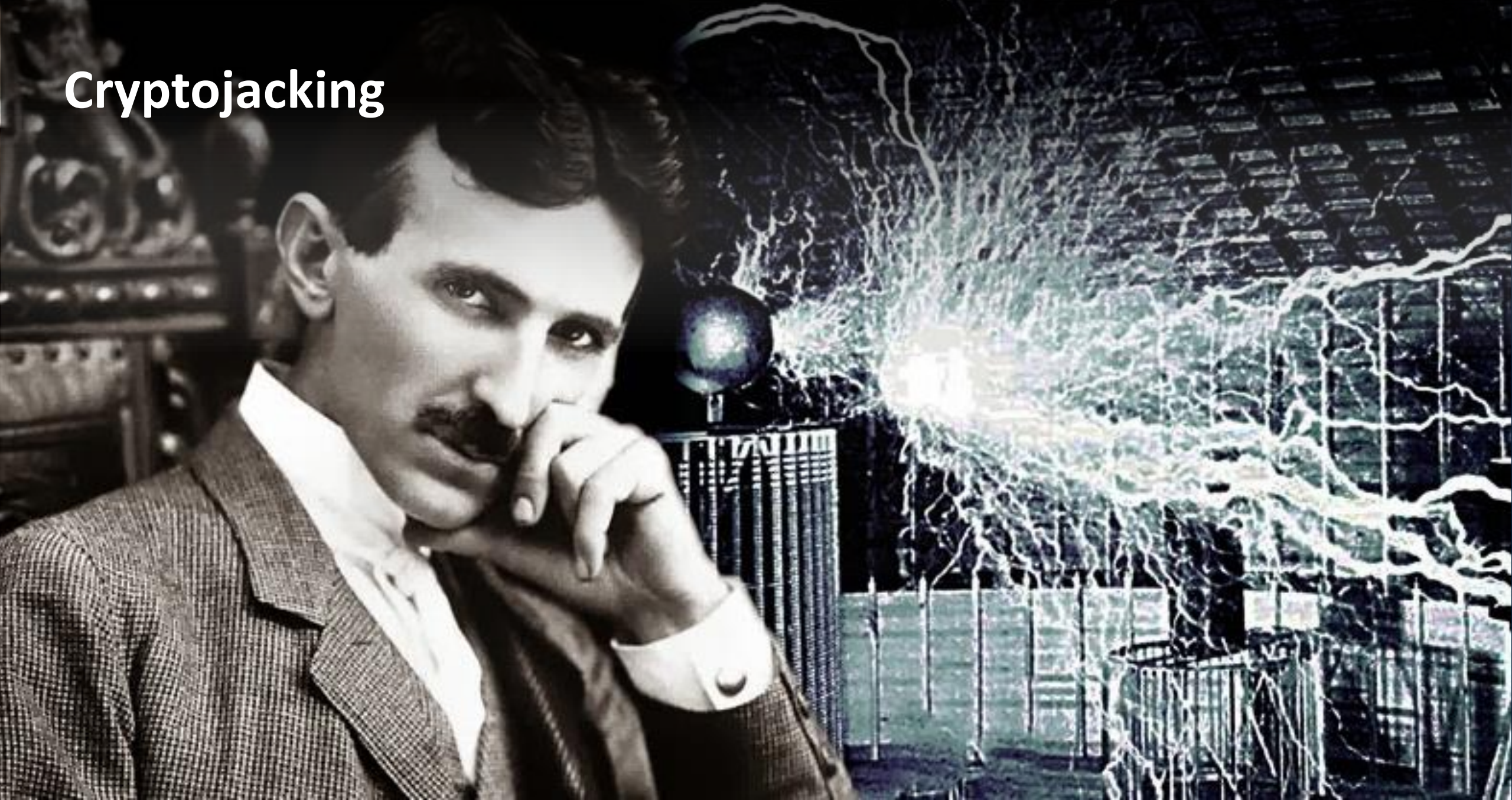
Private bucket

```
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>7F3987394757439B</RequestId>
  <HostId>kyMIhkpoWafjruFFairkfim383jtznAnwiyKSTxv7+/CIHqMBcqrXV2gr+EuALUp
</Error>
```

Public bucket

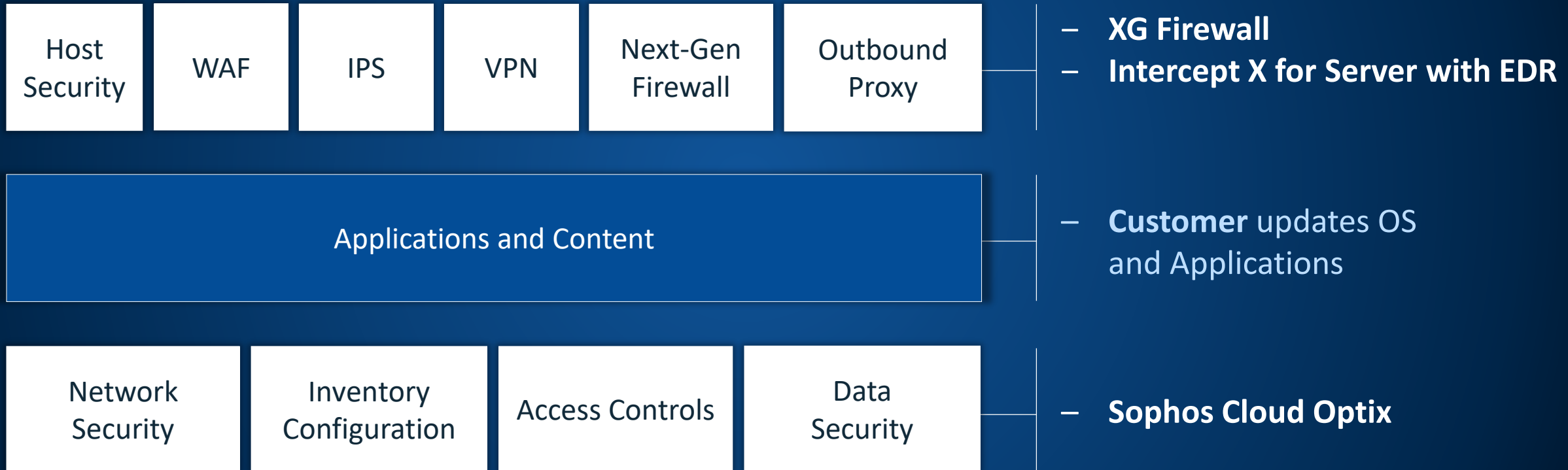
```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>digipublic</Name>
  <Prefix></Prefix>
  <Marker></Marker>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>>false</IsTruncated>
</ListBucketResult>
```

Cryptojacking



Your Responsibilities

Security IN the Cloud



Sophos Cloud Ready Products



- ✓ Sophos Cloud Optix
- ✓ Intercept X for Server
- ✓ XG Firewall



- ✓ Sophos Cloud Optix
- ✓ Intercept X for Server



- ✓ Sophos Cloud Optix
- ✓ Intercept X for Server
- ✓ XG Firewall



Moving to the Cloud

The Challenges

Visibility



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

Compliance



Ever-changing, auto-scaling environments

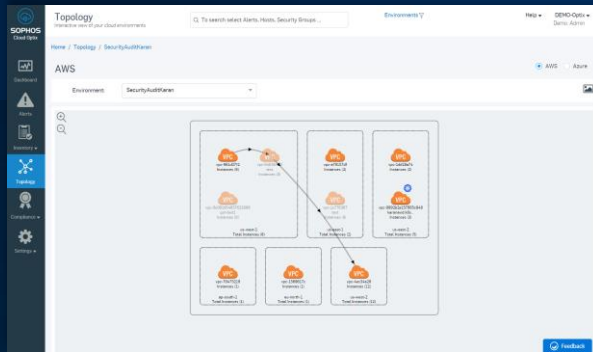
Response



Complex attacks but limited resources

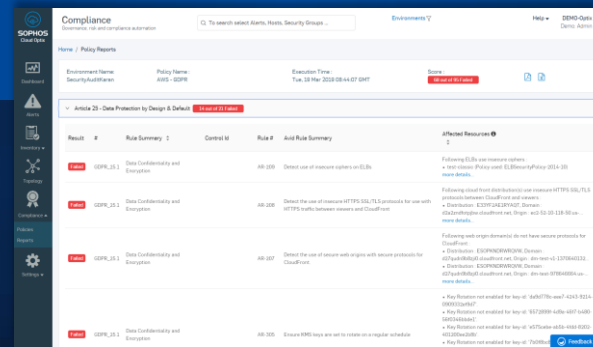
VISIBILITY

Assets in AWS, Microsoft Azure, and Google Cloud Platform



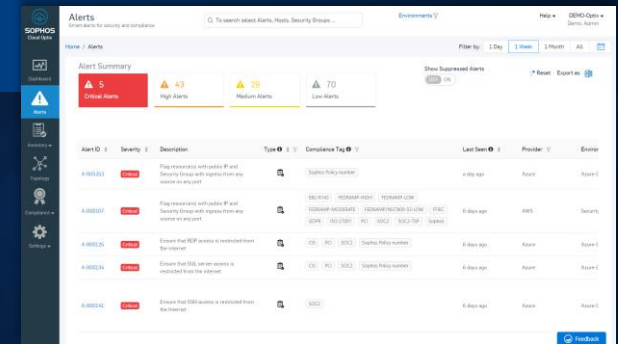
COMPLIANCE

Reporting and adherence based on behaviors and best practices



RESPONSE

Instant remediation and incident response




SOPHOS
Cloud  optix

See everything. Secure everything

Smart Visibility

/ vpc-29214950

Automatically categorizes hosts running database applications such as MongoDB, MySQL and Postgres

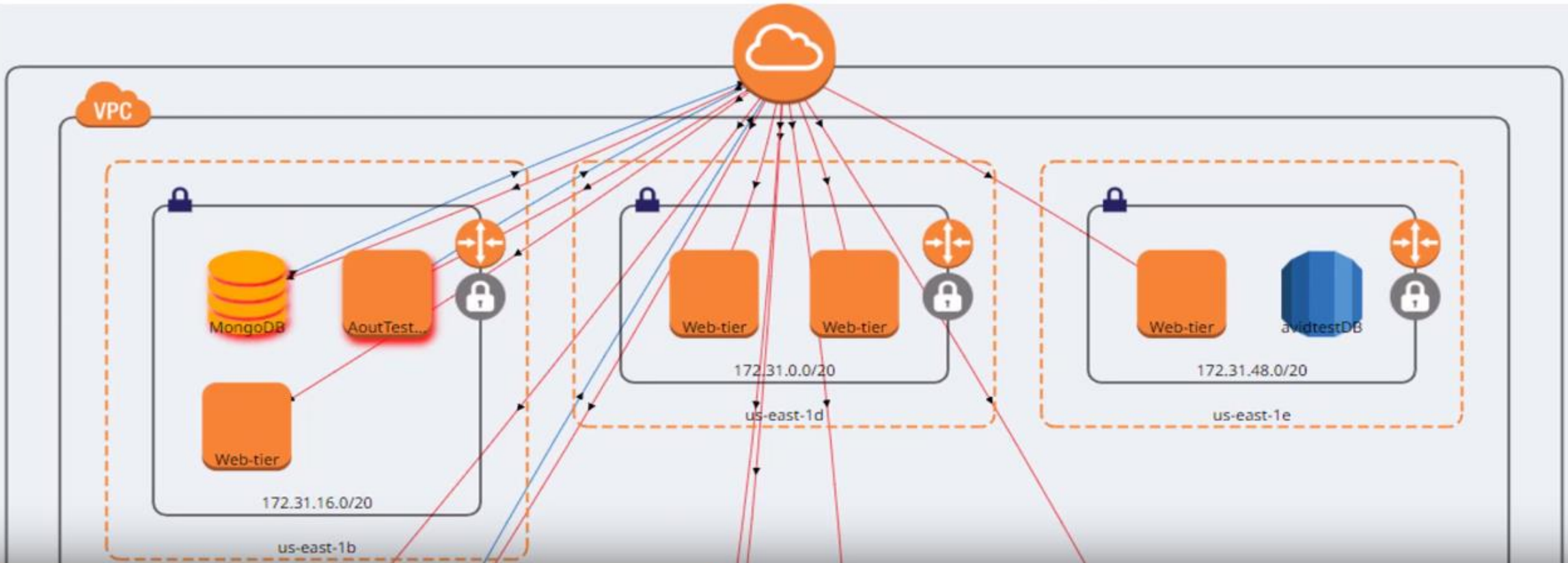
Search Security group(s) 

Search (id / name) 

Show inferred DBs

Show K8s nodes

[Preview](#)



Continuous Compliance

Compliance
Governance, risk and compliance automation

Home / Policies

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

Result	#	Rule Summary	Control Id	Rule #	Sophos Optix Rule Summary	Affected Resources
Failed	GDPR_25.1	Data Confidentiality and Encryption		AR-266	Ensure EBS volumes are encrypted	<ul style="list-style-type: none"> vol-041c3f22a59e669d1 vol-0966aa40b626c9ecc vol-0c5b72df6346e870f vol-06316106af4975c1a vol-08adf1d0ce6883019 + 3 more...
Failed	GDPR_25.1	Data Confidentiality and Encryption		AR-257	Setup Encryption at rest for RDS instances	Following RDS instance(s) do not have Encryption enabled : <ul style="list-style-type: none"> OptixDemodb more details...
Passed	GDPR_25.1	Data Confidentiality and Encryption		AR-209	Detect use of insecure ciphers on ELBs	more details...
Passed		Data Confidentiality and Encryption			Detect the use of insecure HTTPS SSL/TLS protocols for use with	

Jira Software
servicenow

CIS, SOC2, HIPAA, ISO 27001 and PCI DSS

JIRA & ServiceNow integration

AI-Powered Alerts and Response

The screenshot displays the Sophos Cloud console interface. At the top, there is a search bar with the text "To search select Alerts, Hosts, Security Groups ...". Below the search bar, there are several summary cards: "Critical Alerts" with a count of 2, "High Alerts" with a count of 31, and "Low Alerts" with a count of 166. A tooltip is overlaid on the "High Alerts" card, listing four alert types: 1. Security Monitoring: Alerts from the continuous security checks running on your cloud environments. 2. Anomaly (AI): Alerts generated for anomalous activity using the Sophos Cloud Optix AI models. 3. AWS GuardDuty: Alerts from AWS GuardDuty if you have the Integration enabled. 4. Dev: Alerts from the continuous security checks running on your development environments and templates. Below the summary cards, there is a table with columns for "Severity", "Description", "Type", and "Affected Resources". The first row in the table shows a "Critical" alert with the description "Flag resource(s) with public IP and Security Group with ingress from any", a "Type" icon, and "Affected Resources" including "bv-test-splunk (i-07d272175a3a6cf36) - EC2".

- Detect suspicious traffic patterns
- Scan Infrastructure as Code templates
- Identify shared access keys
- Close open storage buckets and ports
- Detect configuration drift
- Set preventative guardrails

Intuitive Dashboard

The dashboard provides a comprehensive overview of security protection. It features a search bar for Alerts, Hosts, and Security Groups, and navigation options for Environments, Help, and user information (Sophos Cloud Optix Demo).

Alert Summary: A filter by time period (1 Day, 1 Week, 1 Month, All) is available. The summary shows 1 Critical Alert, 3 High Alerts, 12 Medium Alerts, and 31 Low Alerts.

Compliance: A donut chart indicates a 79% pass rate (79 Pass) and a 21% fail rate (47 Fail).

What do you need to do?: Action items include viewing critical security alerts, inventory of cloud resources, network topology, compliance reports, and customizing policies.

Changes in your environments: A bar chart shows 8 network changes (all modified) across categories like VPC, Router, Gateway, Security, NACLs, and Subnet. A table lists specific API events for the OptixDemo-AWS account.

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

Top alerts: A list of critical alerts such as 'Ensure multi-factor authentication (MFA) is enabled' and 'Avoid the use of the 'root' account' is provided.

- View alert summary
- At-a-glance compliance status
- View and export compliance reports
- Review inventory
- View network topology
- Identify changes to environments

Governance risk and compliance automation

Details

High

Summary: Ensure no security groups allow ingress from 0.0.0.0/0 to port 22

Description: 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 22. Removing unfettered connectivity to remote console services, such as SSH, reduces a server's exposure to risk.
<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#default-security-group>

Alert Id: A-027993

Environment: Acme-Production (AWS)

Last Seen: 2019-02-26 11:15:47 (a month ago)

Ticket ID(s): JRPRD-29151, INCO010943

Suppressed Resource count: 0 / 7

Affected Resources:

Resource	Last modified by	FirstSeen	Sub tickets
launch-wizard-7(sg-0c3da7489c05f7fed) ingress from 0.0.0.0/0 to port 22	NA	a month ago	JRPRD-29152
launch-wizard-1(sg-5403c32d*) ingress from 0.0.0.0/0 to port 22	NA	a month ago	JRPRD-29153
launch-wizard-2(sg-0a31ee0d*) ingress from 0.0.0.0/0 to port 22	NA	a month ago	JRPRD-29154

Security groups highlighted in yellow are unused i.e. do not have any resources attached to them

Close

- GDPR
- PCI
- HIPAA
- SOC2
- ISO 27001
- Custom Compliance Policies
- Guardrail remediation
- Overall Report
- Identify risky objects
- Create Jira and ServiceNow tickets

Evolution of Synchronized Security with Cloud

Our vision to provide the best protection and visibility, wherever your data resides



Sophos Public Cloud Security - Licencing

MULTI PLATFORM

Three Environments Per License
(e.g. Dev, QA, Prod)

100 ASSETS

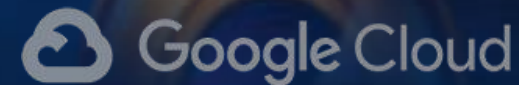
Any Server or Databases Instance

CONTINUOUS

Compliance Assessments

UNLIMITED

Admin Users



Why Cloud Optix



**Quali sono le 3 sfide sulla
sicurezza quando parliamo di
Public Cloud?**



Visibilità limitata
Compliance manuale
Limitate risorse per la gestione

**Perchè scegliere Cloud Optix pur
essendo le piattaforme Cloud di
sicurezza nativa?**



Per ridurre la complessità di gestione.
Ottimizzare il tempo delle risorse IT
utilizzando una sola console anche in
ambienti multi-cloud.



**Quante risorse è possibile gestire
con una licenza Cloud Optix?**



Fino a 3 account Cloud.

100 asset

Fino a 50GB di log giornalieri processati



**Cosa si intende per
Cloud asset?**



Istanze di machine virtuali

Istanze Server

Istanze Database

Customer Stories

Success Stories



“Our compliance team is now able to run reports for compliance audits in seconds, which was previously manual and exceedingly time consuming.”

- Aaron Peck, Vice President and CISO, Shutterfly Inc.



“Sophos Cloud Optix provides us a comprehensive network topology diagram with real-time traffic of our cloud environment. I have better insight into our cloud network security posture than ever before.”

- Jessica Mazzone, Security Engineer, HubSpot Inc.

“Because of the real-time topology visualization diagrams and the out of the box compliance templates in Sophos Cloud Optix, we've saved weeks of time, preparing for our SOC 2 audit and gathering evidence. This is the first time I've looked forward to providing evidence to our auditors.”

- Ryan Stinson, Manager of Security Engineering, HubSpot Inc.

60+ accounts

AWS & Azure

4000+

Servers

1TB+

Traffic ingestion per day

Success Story

Goal

- Move 70 petabytes of data to public cloud

Problem

- Inadequate visibility across multi-cloud environment
- Limited cloud security staff
- Compliance parity in public cloud

Benefits

- Comprehensive inventory and visibility
- Continuous security monitoring and topology visualization
- Compliance collaboration and control mapping
- Process efficiencies
 - Auto discovery of issue ownership
 - Acquisition of Lifetouch

SOPHOS
Cloud  ptix

See everything. Secure everything

Question time!

SOPHOS

SOPHOS

[SOPHOS.COM/CLOUD-OPTIX](https://sophos.com/cloud-optix)

SOPHOS
Cloud  ptix

See everything. Secure everything

Grazie!

SOPHOS

SOPHOS
Cloud  ptix

See everything. Secure everything

SOPHOS

SOPHOS DISCOVER 2019

EVOLVE

Breakout session
Sophos Cloud Optix