Solving the Toughest Challenges in Cloud Security

Chris Howell

Commercial Lead, Public Cloud Group

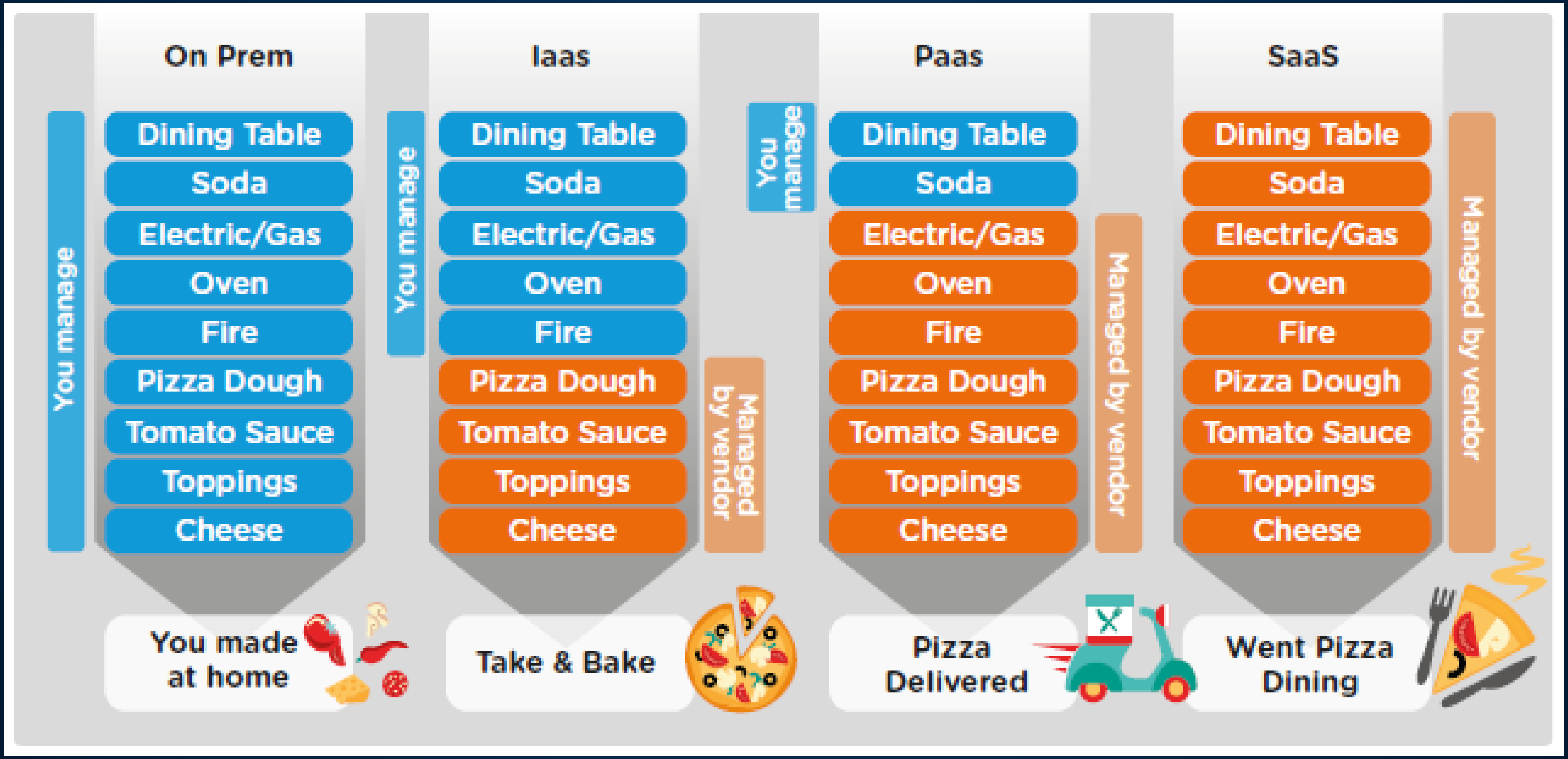
SOPHOS

About Me

- Commercial Lead – Global Public Cloud
- Ex Microsoft & Barracuda Channel Evangelist
    - Specializing in Cloud Migration & Security
- Joined Sophos in June 2018
- Love to build long lasting relationships
- Find the Public Cloud Fascinating
- Keen Football Coach & Secret Karaoke Fan!

Pizza as a Service

The public cloud is defined as computing services offered by third-party providers over the public Internet, making them available to anyone who wants to use or purchase them.



	On Prem		Iaas		Paas		SaaS	
You manage	Dining Table	You manage	Dining Table	You manage	Dining Table		Dining Table	Managed by vendor
	Soda		Soda		Soda		Soda	
	Electric/Gas		Electric/Gas		Electric/Gas	Managed by vendor	Electric/Gas	
	Oven		Oven		Oven		Oven	
	Fire		Fire		Fire		Fire	
	Pizza Dough		Pizza Dough	Managed by vendor	Pizza Dough		Pizza Dough	
	Tomato Sauce		Tomato Sauce		Tomato Sauce		Tomato Sauce	
	Toppings		Toppings		Toppings		Toppings	
	Cheese		Cheese		Cheese		Cheese	
	You made at home		Take & Bake		Pizza Delivered		Went Pizza Dining	

Public Cloud Adoption Drivers

Trade CapEx for OpEx

Benefit from massive economies of scale

Stop Guessing Capacity

Increase Speed and Agility

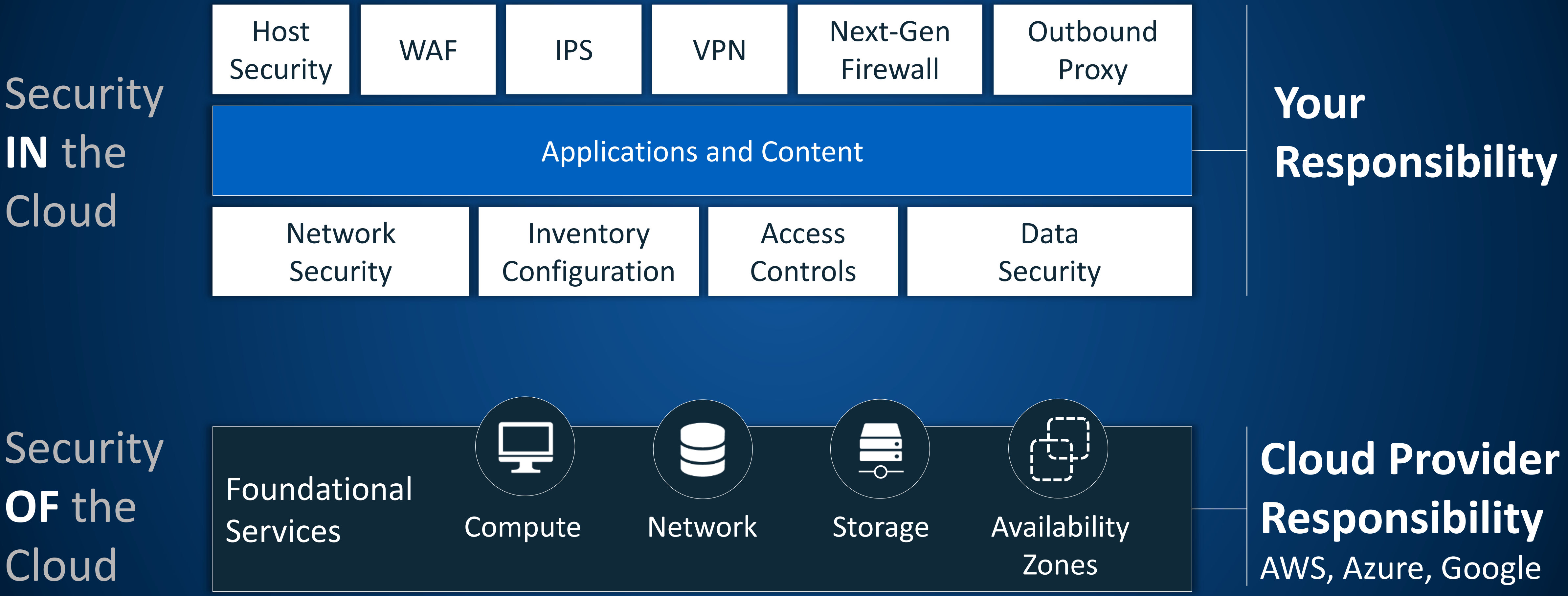
No more expensive data centers

Go global in minutes

Shared Security Model
and Sophos Public Cloud Security

SOPHOS

Cloud Security is a Shared Responsibility



Security **IN** the Cloud

Host Security

WAF

IPS

VPN

Next-Gen Firewall

Outbound Proxy

Applications and Content

Network Security

Inventory Configuration

Access Controls

Data Security

Your Responsibility

Security **OF** the Cloud

Foundational Services

Compute

Network

Storage

Availability Zones

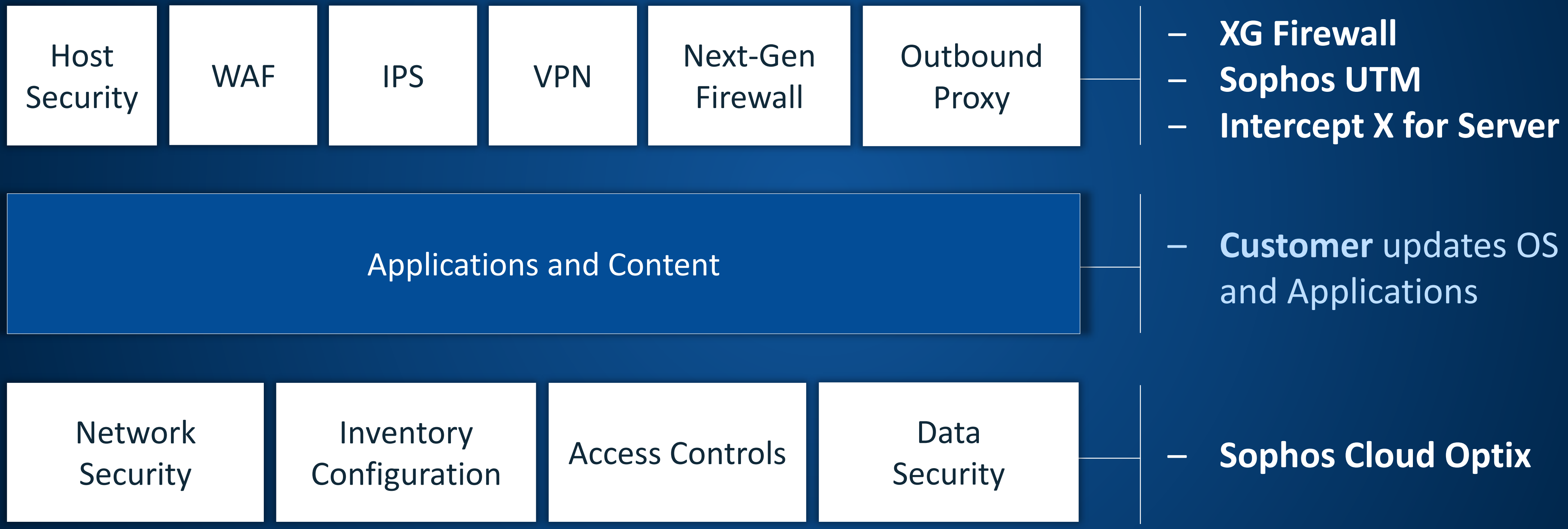
Cloud Provider Responsibility

AWS, Azure, Google

SOPHOS

Your Responsibilities

Security IN the Cloud



Host Security

WAF

IPS

VPN

Next-Gen Firewall

Outbound Proxy

- XG Firewall
- Sophos UTM
- Intercept X for Server

Applications and Content

- **Customer** updates OS and Applications

Network Security

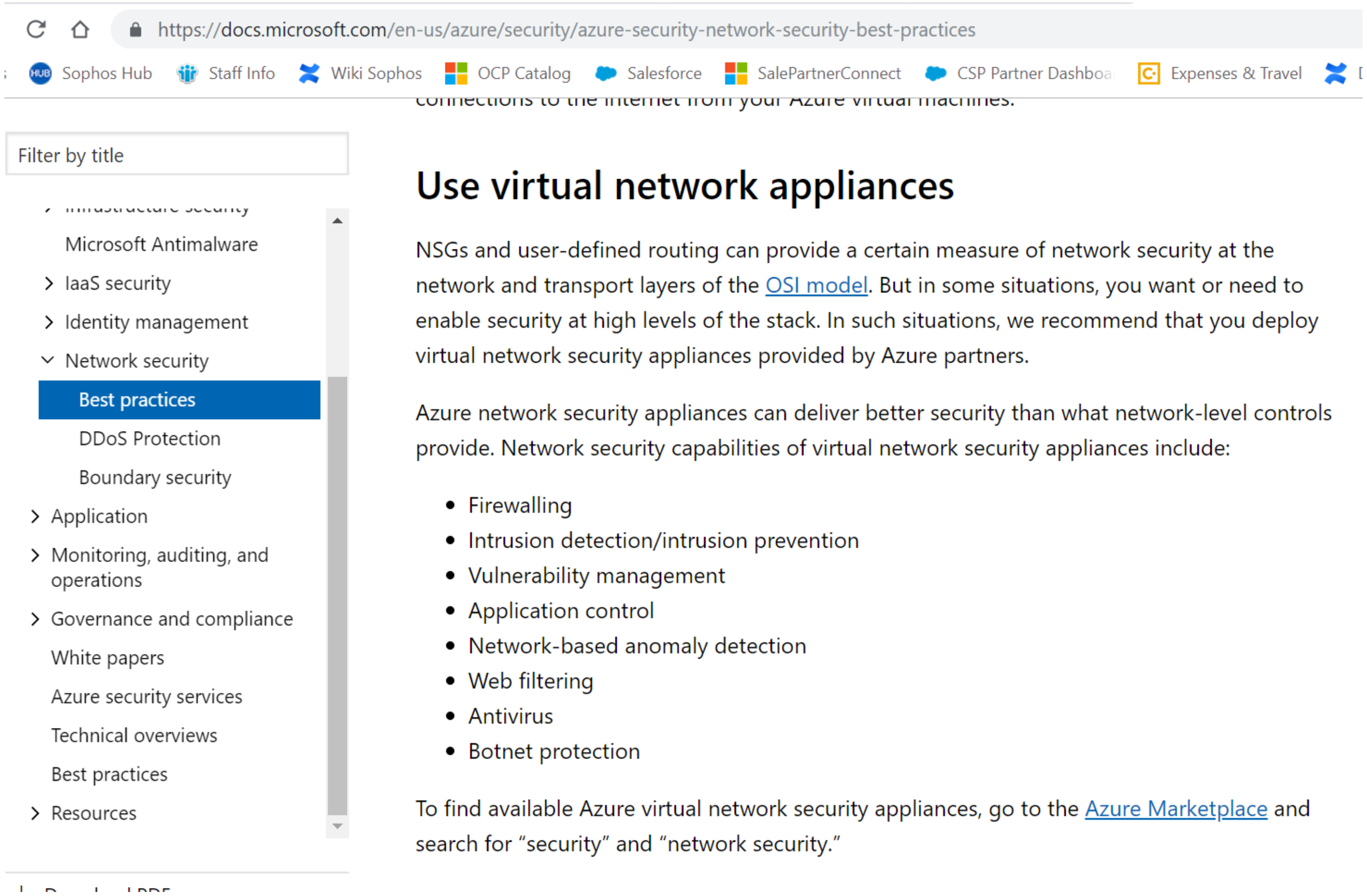
Inventory Configuration

Access Controls

Data Security

- Sophos Cloud Optix

Security Best Practices



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.

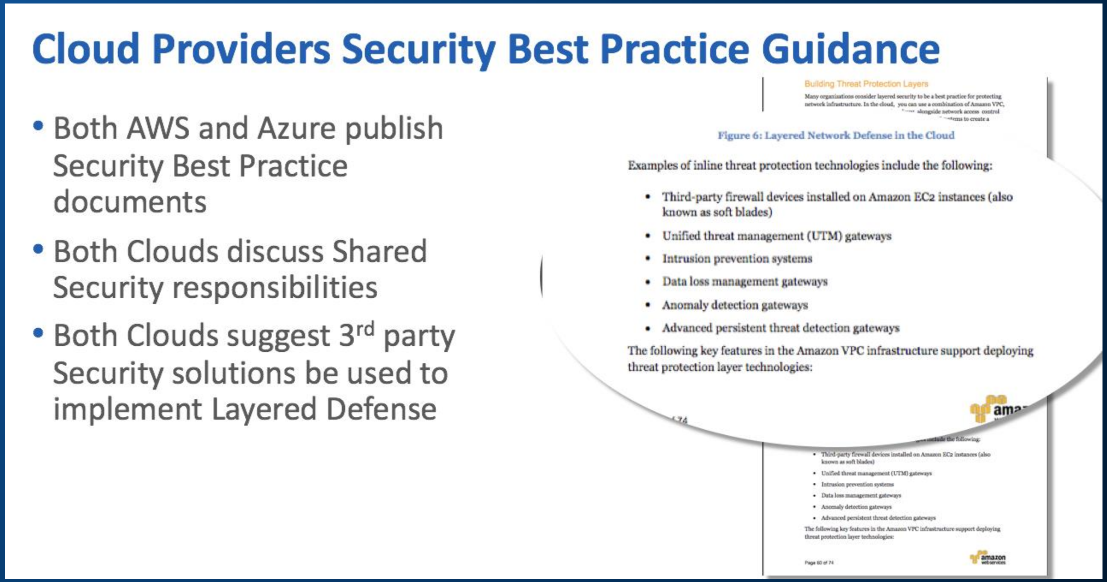
Azure network security appliances can deliver better security than what network-level controls provide. Network security capabilities of virtual network security appliances include:

- 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 Providers Security Best Practice Guidance

- Each of the 3 big Public Cloud providers publish Security Best Practice guides
- All talk about how to:
  - Configure accounts and services
  - Securely manage access
  - Use encryption tools
  - And discuss why additional layers of security
- Each guide is more than 50 pages in length with AWS guide totaling **73 pages!**



Cloud Providers Security Best Practice Guidance

- Both AWS and Azure publish Security Best Practice documents
- Both Clouds discuss Shared Security responsibilities
- Both Clouds suggest 3rd party Security solutions be used to implement Layered Defense

Building Threat Protection Layers

Many organizations consider layered security to be a best practice for protecting network infrastructure. In the cloud, you can use a combination of Amazon VPC, … alongside network access control …stems to create a

Figure 6: Layered Network Defense in the Cloud

Examples of inline threat protection technologies include the following:

- Third-party firewall devices installed on Amazon EC2 instances (also known as soft blades)
- Unified threat management (UTM) gateways
- Intrusion prevention systems
- Data loss management gateways
- Anomaly detection gateways
- Advanced persistent threat detection gateways

The following key features in the Amazon VPC infrastructure support deploying threat protection layer technologies:

…include the following:

- Third-party firewall devices installed on Amazon EC2 instances (also known as soft blades)
- Unified threat management (UTM) gateways
- Intrusion prevention systems
- Data loss management gateways
- Anomaly detection gateways
- Advanced persistent threat detection gateways

The following key features in the Amazon VPC infrastructure support deploying threat protection layer technologies:

Page 60 of 74

Available Solutions

Azure

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

Google Cloud

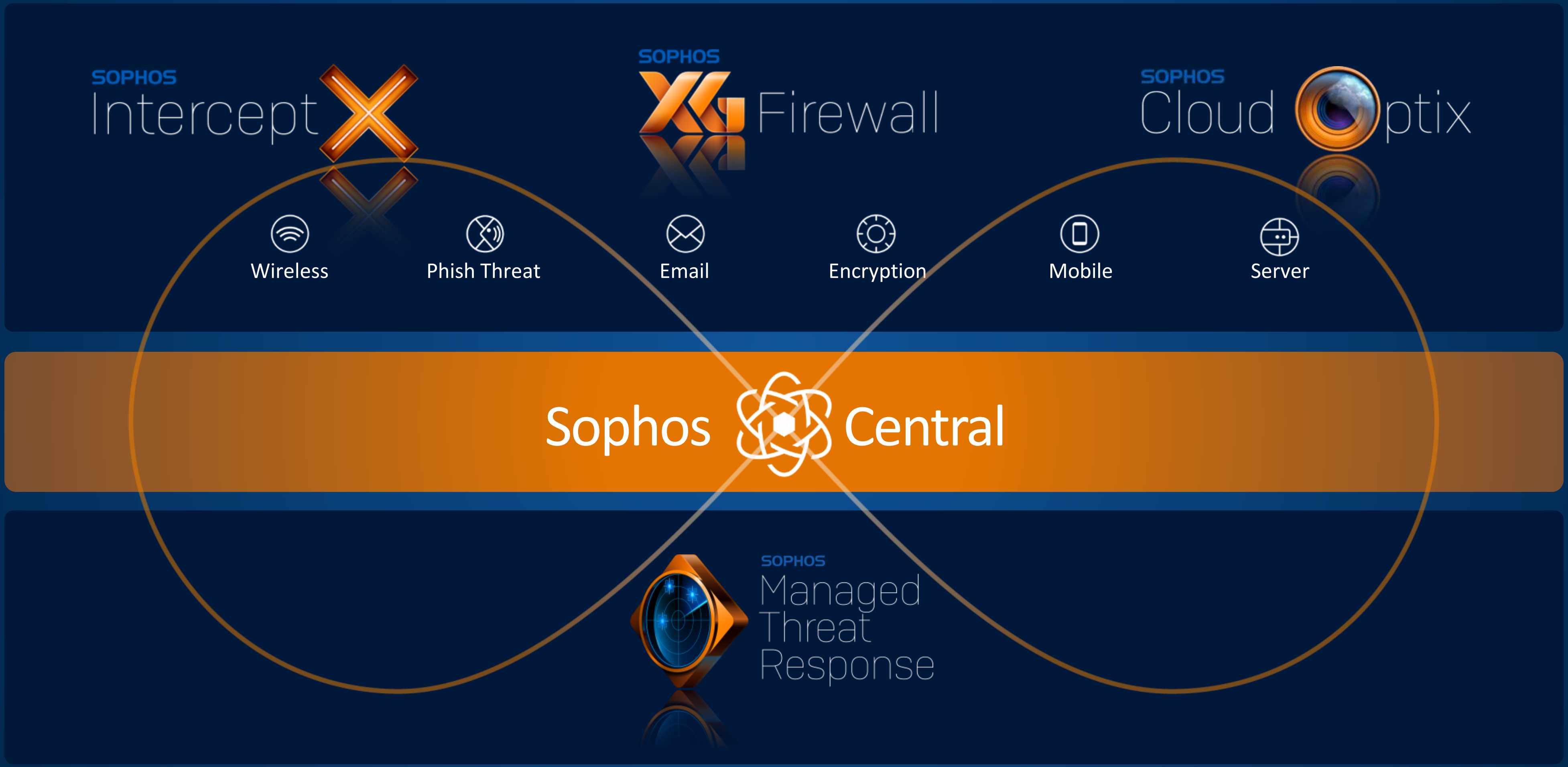
- ✓ Sophos Cloud Optix
- ✓ Intercept X for Server

aws

- ✓ Sophos Cloud Optix
- ✓ Intercept X for Server
- ✓ UTM

CLOUD READY

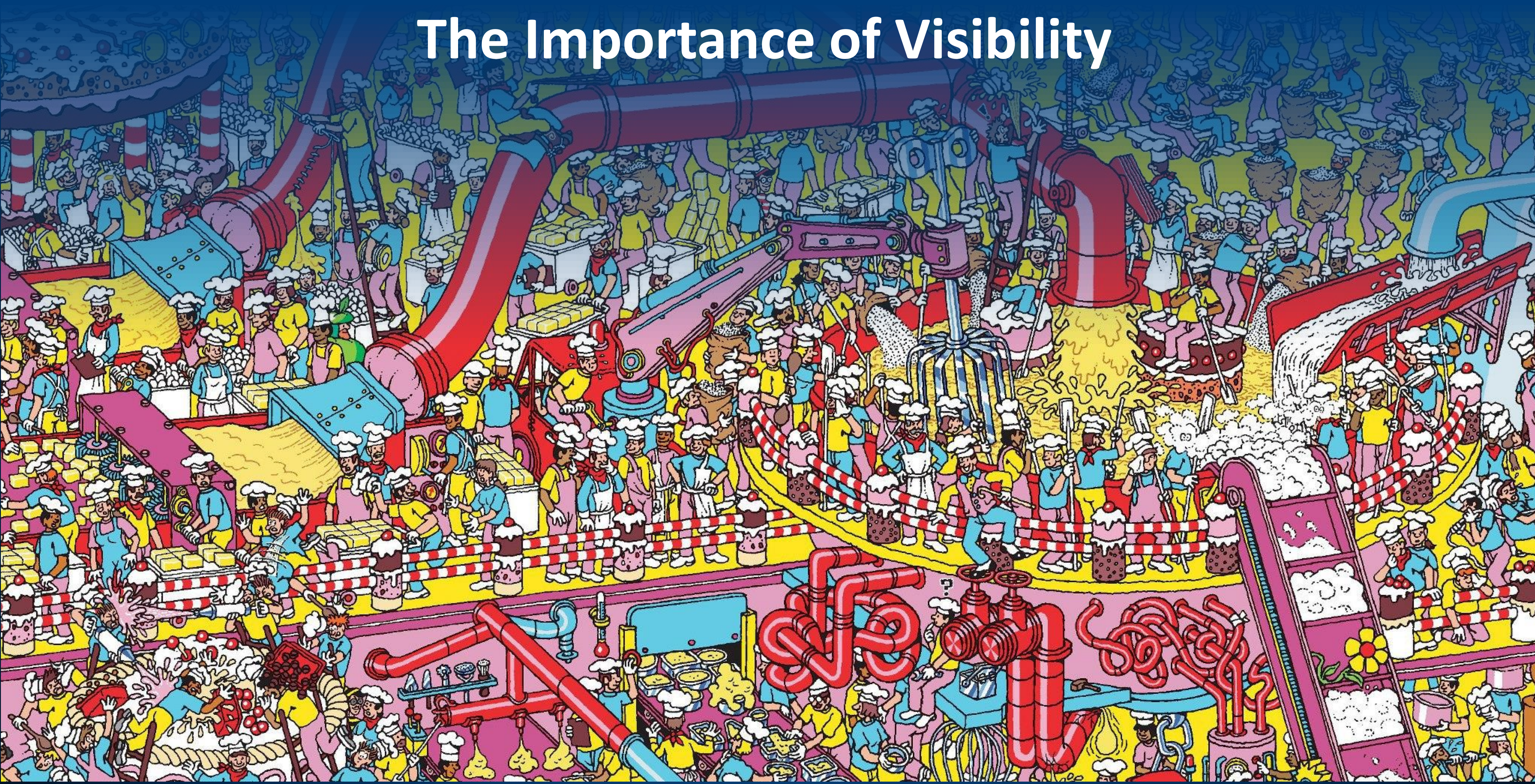
Evolution of Prevention & Response

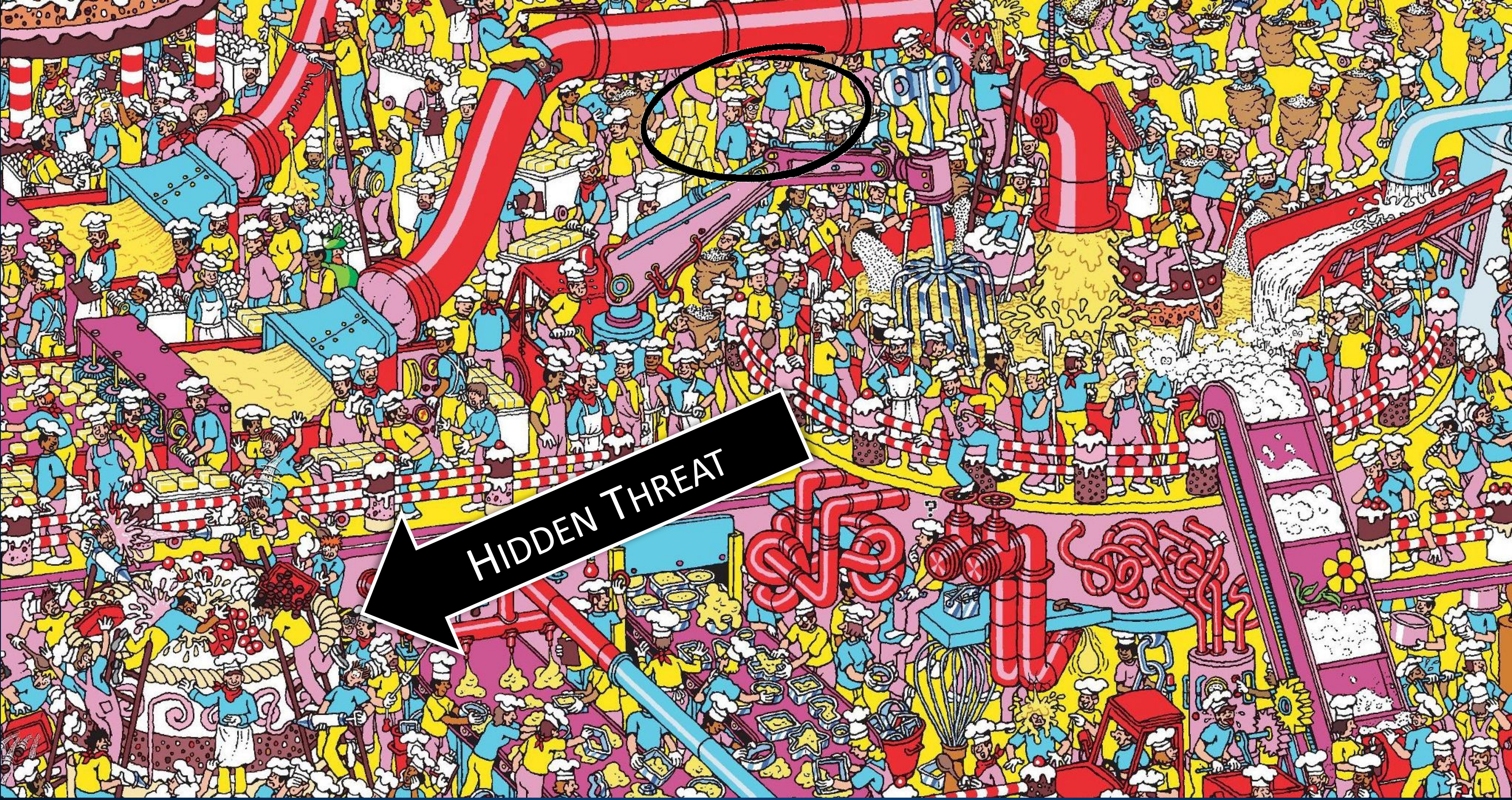


The Importance of Visibility

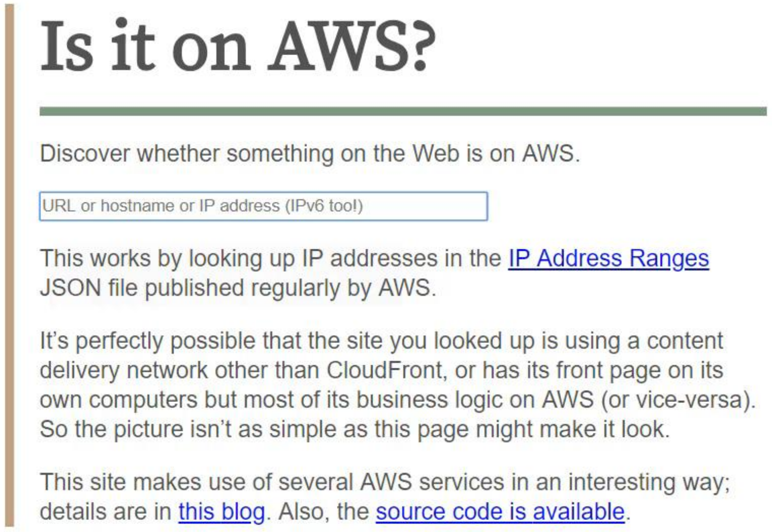
SOPHOS

The Importance of Visibility





Credit: Martin Handford, author/illustrator



Is it on AWS?

Discover whether something on the Web is on AWS.

This works by looking up IP addresses in the IP Address Ranges JSON file published regularly by AWS.

It's perfectly possible that the site you looked up is using a content delivery network other than CloudFront, or has its front page on its own computers but most of its business logic on AWS (or vice-versa). So the picture isn't as simple as this page might make it look.

This site makes use of several AWS services in an interesting way; details are in this blog. Also, the source code is available.

00:00.00

https://isitonaws.com

Public Cloud Security Breaches

By 2020

95%

of cloud security failures will be the customer's fault

Source: Gartner, Clouds Are Secure: Are You Using Them Securely? by Jay Heiser

Six million PII records

Telecommunications company

200k customer call recordings exposed

Holiday bookings service

20 thousand customer records

Large discount brokerage firm

Public Cloud Security Breaches

1 in 6

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

UBER

Source: There's a Hole in 1,951 Amazon S3 Buckets, Rapid 7

Automated Attacks

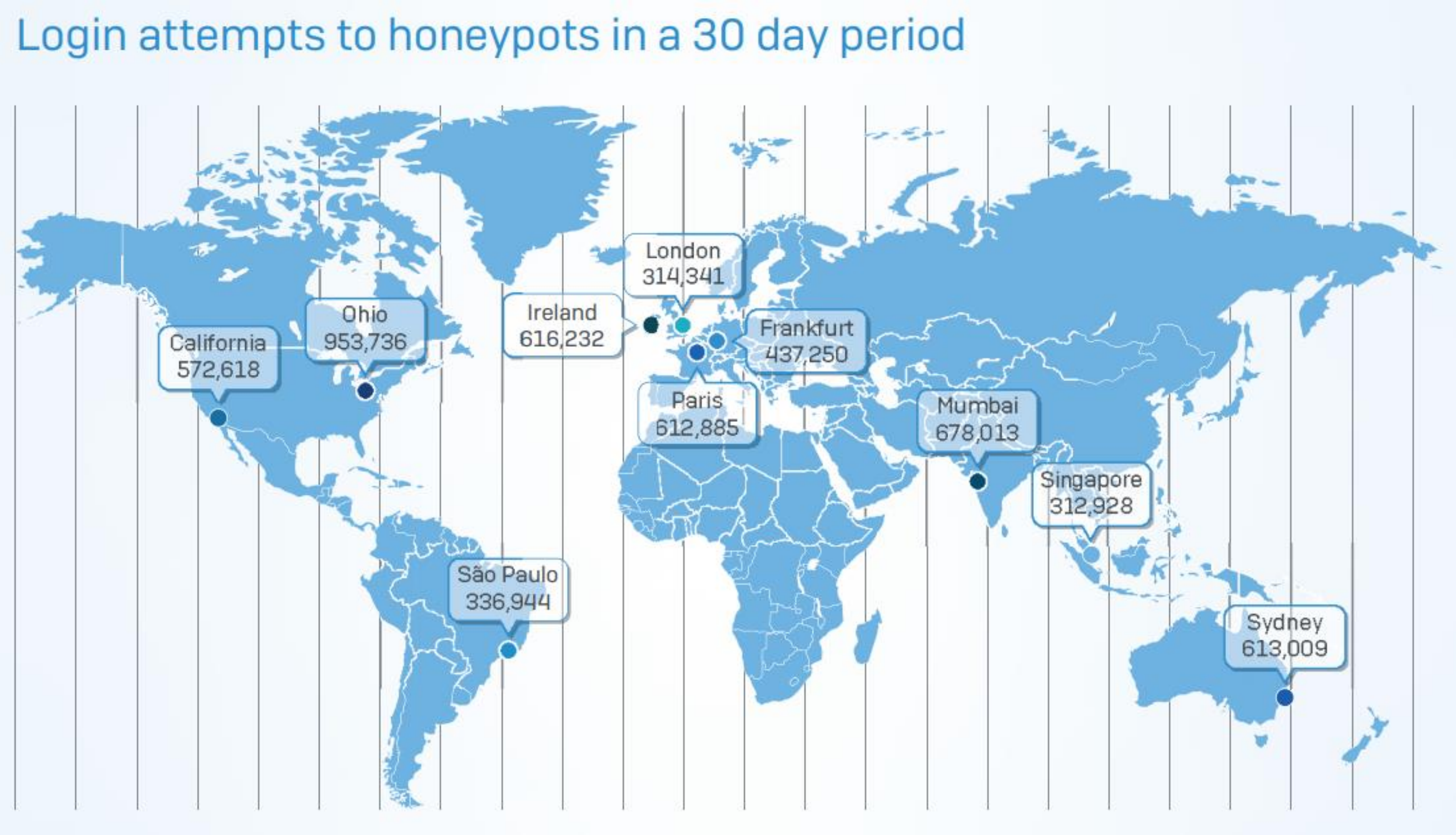
5 Million

Attempted Logins In 30 days

Sao Paulo
52 Seconds!

Paris
17 min 20 Secs

Sydney
18 min 56 Secs


Login attempts to honeypots in a 30 day period

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

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

SOPHOS XG Firewall

SOPHOS Intercept X

Gartner

NSS LABS RECOMMENDED

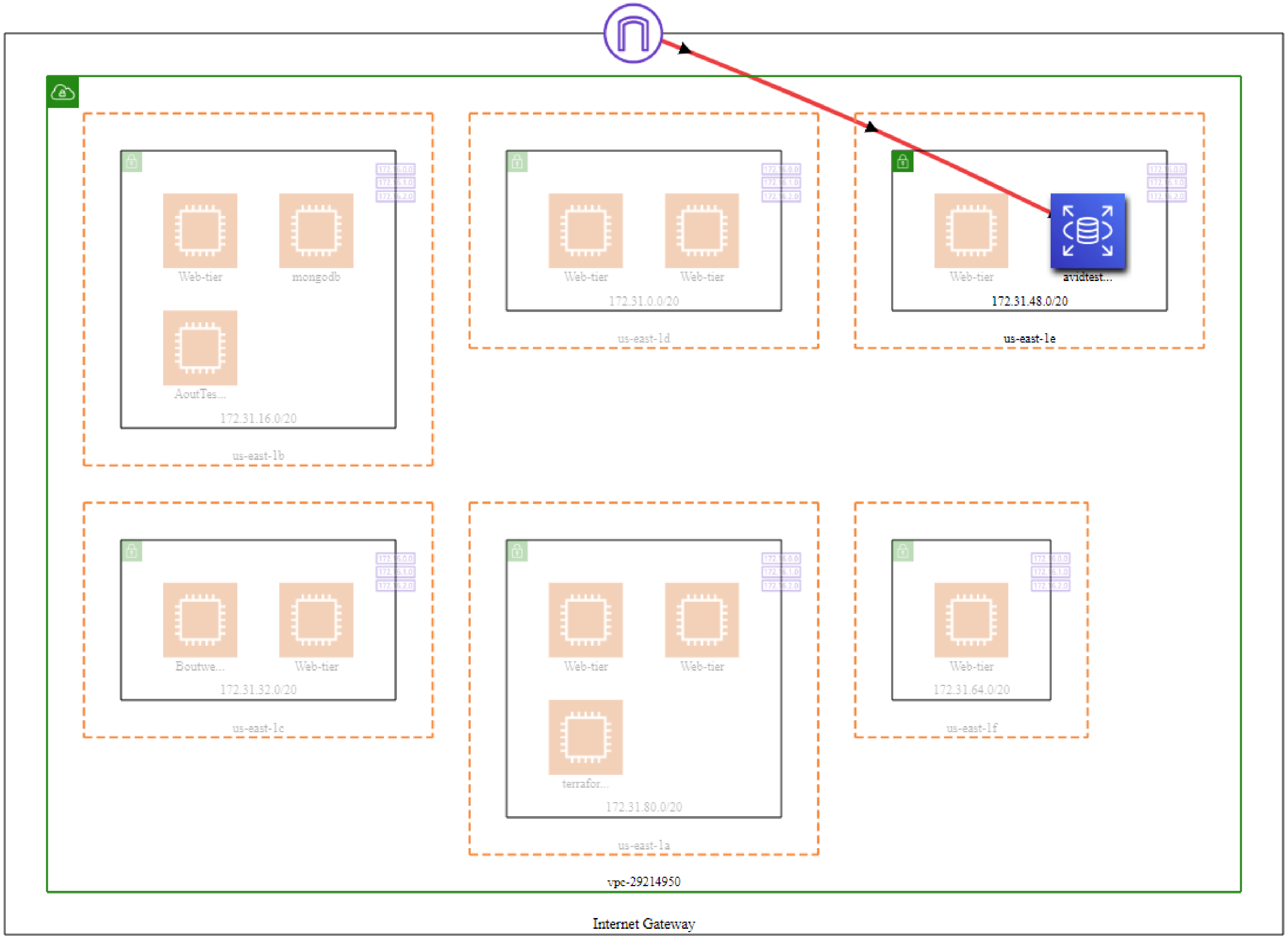
Synchronized Security

SE Labs AAA ENTERPRISE ENDPOINT PROTECTION APR-JUN 2018

FORRESTER®

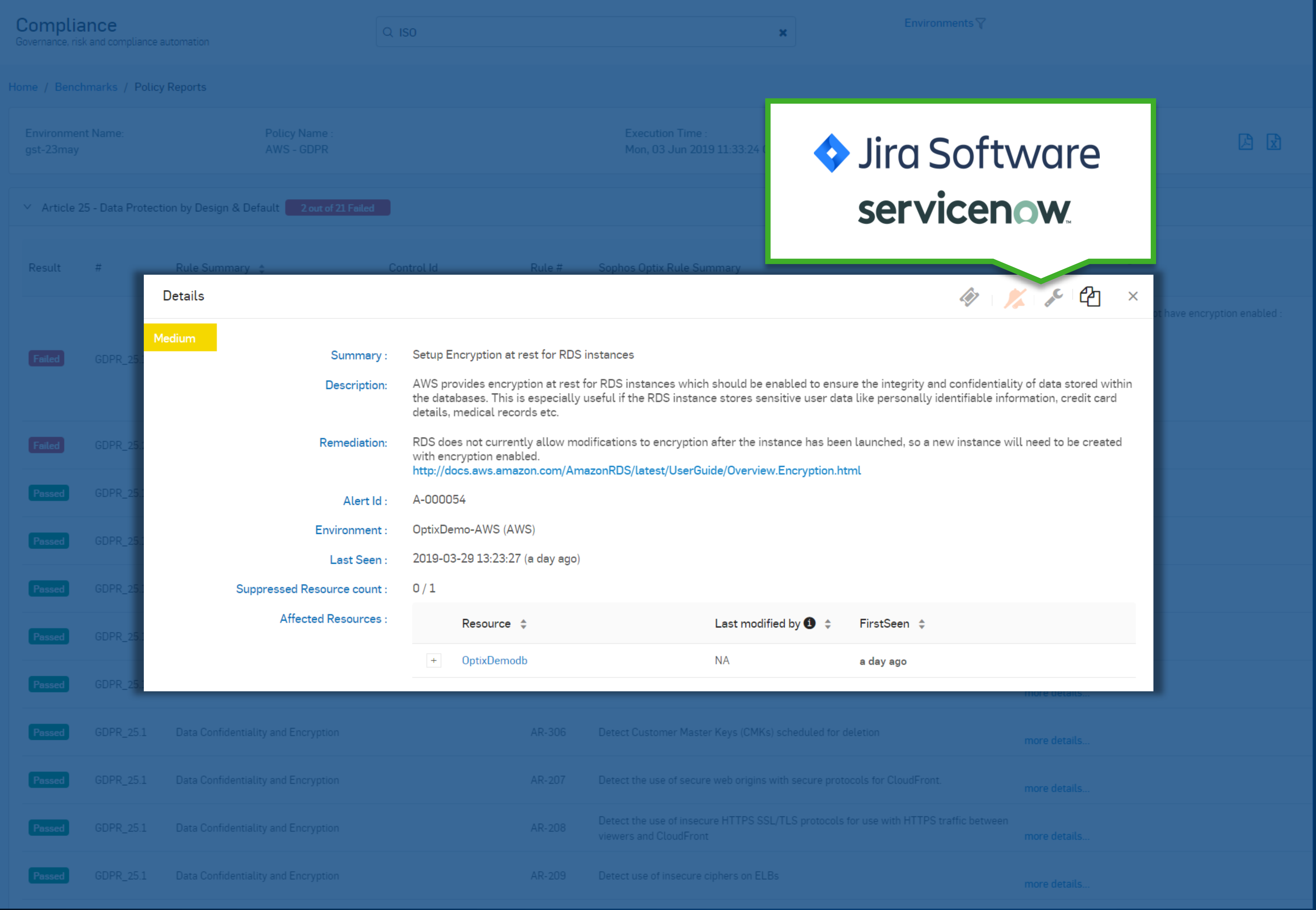
SOPHOS Cloud Optix

See everything. Secure everything



END-TO-END VISIBILITY

- Full asset inventory (AWS, Azure, and GCP)
- Network topology visualisation
- View traffic flow (ingress/egress/ internal)
- Security Group analyses how traffic may flow
- Analyse Host traffic for hidden vulnerability i.e. open databases



Compliance
Governance, risk and compliance automation

ISO

Environments

Home / Benchmarks / Policy Reports

Environment Name: gst-23may
Policy Name : AWS - GDPR
Execution Time : Mon, 03 Jun 2019 11:33:24

Article 25 - Data Protection by Design & Default 2 out of 21 Failed

Result	#	Rule Summary	Control Id	Rule #	Sophos Optix Rule Summary	
Failed	GDPR_25				…t have encryption enabled :	
Failed	GDPR_25					
Passed	GDPR_25					
Passed	GDPR_25					
Passed	GDPR_25					
Passed	GDPR_25					
Passed	GDPR_25					more details...
Passed	GDPR_25.1	Data Confidentiality and Encryption		AR-306	Detect Customer Master Keys (CMKs) scheduled for deletion	more details...
Passed	GDPR_25.1	Data Confidentiality and Encryption		AR-207	Detect the use of secure web origins with secure protocols for CloudFront.	more details...
Passed	GDPR_25.1	Data Confidentiality and Encryption		AR-208	Detect the use of insecure HTTPS SSL/TLS protocols for use with HTTPS traffic between viewers and CloudFront	more details...
Passed	GDPR_25.1	Data Confidentiality and Encryption		AR-209	Detect use of insecure ciphers on ELBs	more details...

Jira Software
servicenow

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)

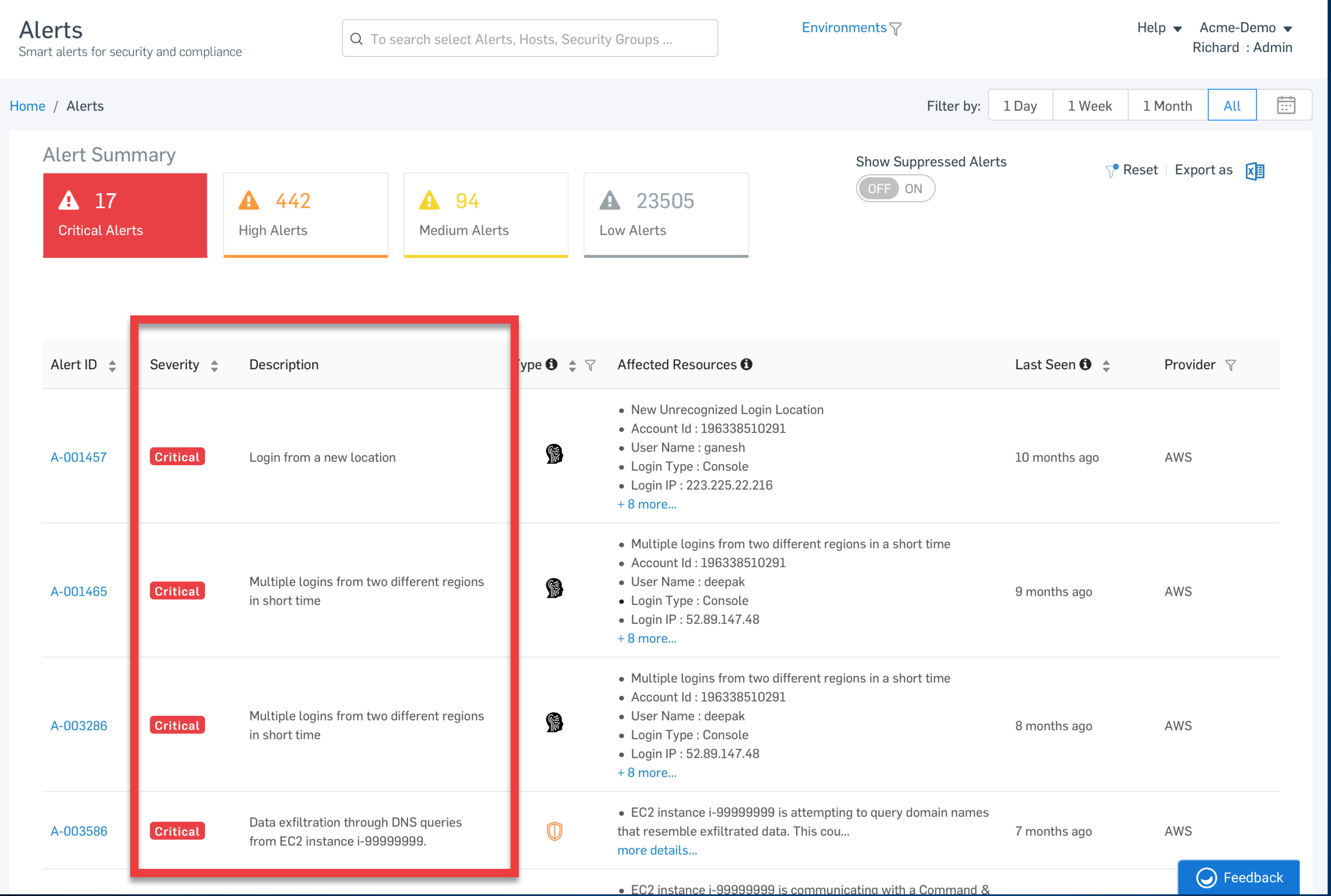
Suppressed Resource count : 0 / 1

Affected Resources :

	Resource	Last modified by	FirstSeen
+	OptixDemodb	NA	a day ago

CONTINUOUS COMPLIANCE

- Continuous monitoring
- Custom policies
- Out of the box templates
- GDPR, CIS, SOC2, HIPAA, ISO 27001 and PCI DSS
- Guardrails prevent changes to critical systems
- Jira and ServiceNow integration



Alert Summary

17 Critical Alerts	442 High Alerts	94 Medium Alerts	23505 Low Alerts

Alert ID	Severity	Description	ype	Affected Resources	Last Seen	Provider
A-001457	Critical	Login from a new location		New Unrecognized Login Location Account Id : 196338510291 User Name : ganesh Login Type : Console Login IP : 223.225.22.216 + 8 more...	10 months ago	AWS
A-001465	Critical	Multiple logins from two different regions in short time		Multiple logins from two different regions in a short time Account Id : 196338510291 User Name : deepak Login Type : Console Login IP : 52.89.147.48 + 8 more...	9 months ago	AWS
A-003286	Critical	Multiple logins from two different regions in short time		Multiple logins from two different regions in a short time Account Id : 196338510291 User Name : deepak Login Type : Console Login IP : 52.89.147.48 + 8 more...	8 months ago	AWS
A-003586	Critical	Data exfiltration through DNS queries from EC2 instance i-99999999.		EC2 instance i-99999999 is attempting to query domain names that resemble exfiltrated data. This cou... more details...	7 months ago	AWS
				EC2 instance i-99999999 is communicating with a Command &		

AI-POWERED ALERTS AND RESPONSE

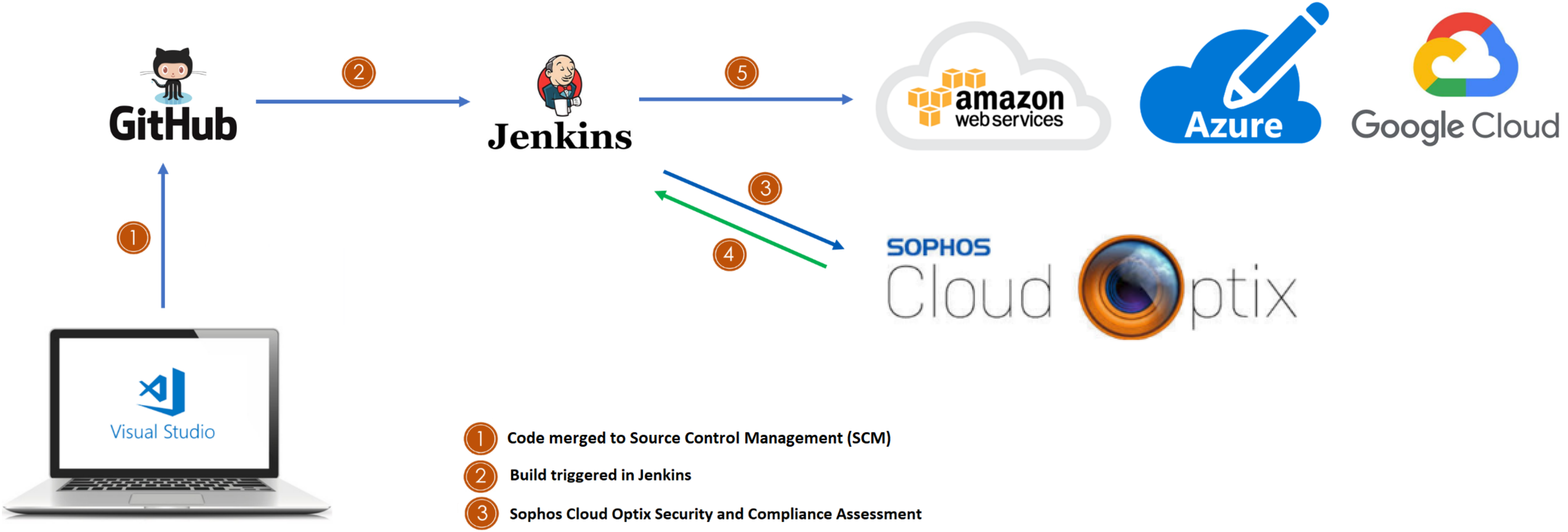
- Identify suspicious logins and API calls
- Detect suspicious traffic patterns
- Close open storage buckets (S3) and ports
- Detect configuration drift
- Scan IaC templates in Github, Bitbucket and Jenkins Pipeline

Worked fine in Dev

Credit: Reddit u/Marthy_Mc_Fly

Cloud Optix: Security + DevOps Sample Workflow

DevSecOps



1. Code merged to Source Control Management (SCM)
2. Build triggered in Jenkins
3. Sophos Cloud Optix Security and Compliance Assessment
4. Security and Compliance Assessment result sent to Jenkins
5. Pipeline deployment to AWS/Azure/GCP stops or proceeds based on Cloud Optix Security and Compliance Assessment results

Success Stories

HubSpot

"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.

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.

"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.

MULTI PLATFORM

Amazon Web Services, Microsoft Azure, and Google Cloud Platform

ASSET BUNDLES

Server and database instances

CONTINUOUS

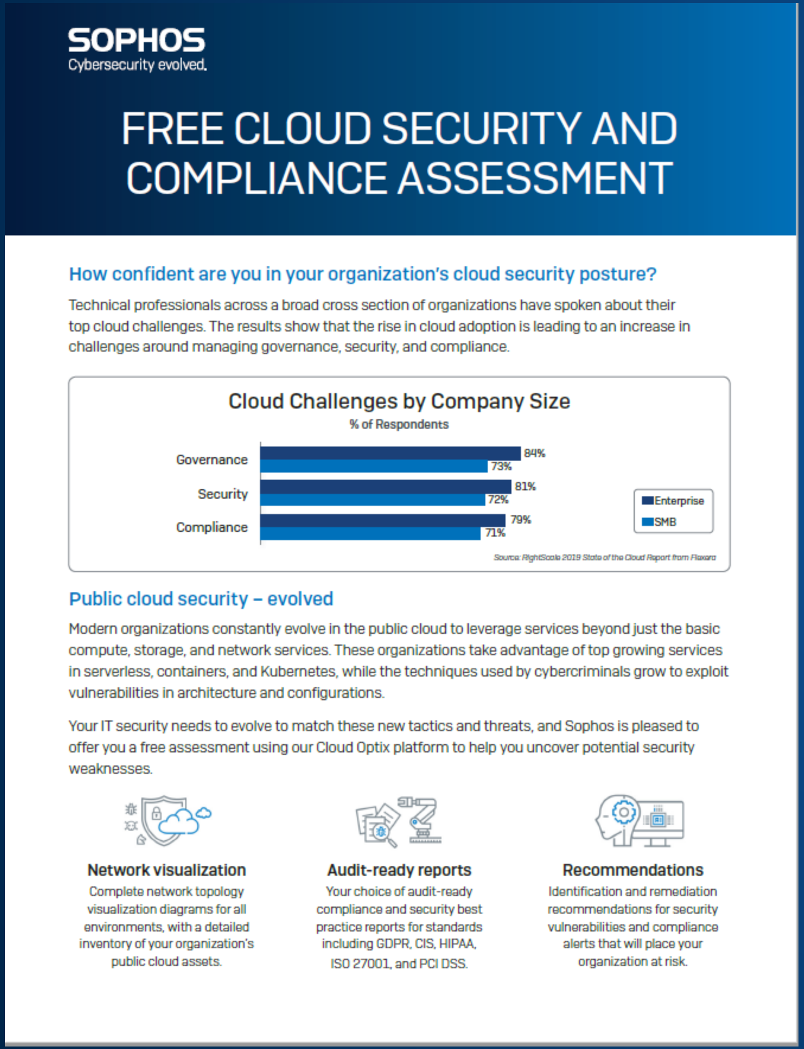
Compliance assessments

UNLIMITED

Admin Users

Simple Licensing

New Assets Available to Customer



SOPHOS
Cybersecurity evolved.

FREE CLOUD SECURITY AND COMPLIANCE ASSESSMENT

How confident are you in your organization's cloud security posture?

Technical professionals across a broad cross section of organizations have spoken about their top cloud challenges. The results show that the rise in cloud adoption is leading to an increase in challenges around managing governance, security, and compliance.

Cloud Challenges by Company Size

Source: RightScale 2019 State of the Cloud Report from Flexera

Public cloud security – evolved

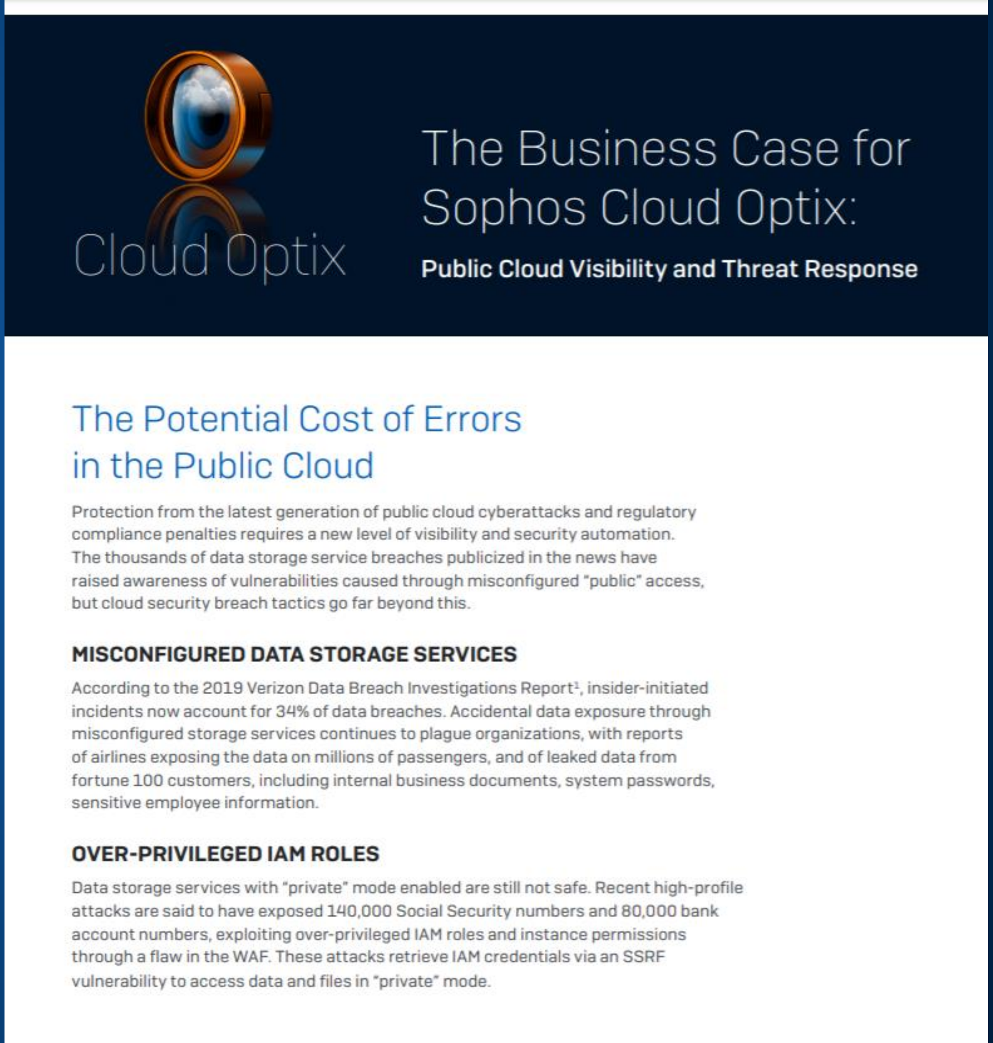
Modern organizations constantly evolve in the public cloud to leverage services beyond just the basic compute, storage, and network services. These organizations take advantage of top growing services in serverless, containers, and Kubernetes, while the techniques used by cybercriminals grow to exploit vulnerabilities in architecture and configurations.

Your IT security needs to evolve to match these new tactics and threats, and Sophos is pleased to offer you a free assessment using our Cloud Optix platform to help you uncover potential security weaknesses.

Network visualization
Complete network topology visualization diagrams for all environments, with a detailed inventory of your organization's public cloud assets.

Audit-ready reports
Your choice of audit-ready compliance and security best practice reports for standards including GDPR, CIS, HIPAA, ISO 27001, and PCI DSS.

Recommendations
Identification and remediation recommendations for security vulnerabilities and compliance alerts that will place your organization at risk.



The Business Case for Sophos Cloud Optix:

Public Cloud Visibility and Threat Response

The Potential Cost of Errors in the Public Cloud

Protection from the latest generation of public cloud cyberattacks and regulatory compliance penalties requires a new level of visibility and security automation. The thousands of data storage service breaches publicized in the news have raised awareness of vulnerabilities caused through misconfigured "public" access, but cloud security breach tactics go far beyond this.

MISCONFIGURED DATA STORAGE SERVICES

According to the 2019 Verizon Data Breach Investigations Report[1], insider-initiated incidents now account for 34% of data breaches. Accidental data exposure through misconfigured storage services continues to plague organizations, with reports of airlines exposing the data on millions of passengers, and of leaked data from fortune 100 customers, including internal business documents, system passwords, sensitive employee information.

OVER-PRIVILEGED IAM ROLES

Data storage services with "private" mode enabled are still not safe. Recent high-profile attacks are said to have exposed 140,000 Social Security numbers and 80,000 bank account numbers, exploiting over-privileged IAM roles and instance permissions through a flaw in the WAF. These attacks retrieve IAM credentials via an SSRF vulnerability to access data and files in "private" mode.

Q & A

SOPHOS

SOPHOS

Security made simple.