Bezpieczeństwo chmury publicznej

Damian Przygodzki
System Engineer

Dlaczego firmy korzystają z chmury publicznej?

Koszty operacyjne vs inwestycje

Szybka
Nieskomplikowana
Skalowalna

Nieograniczona pojemność

Szybkość i zwinność

Prywatna chmura jest za droga

ad hoc IT

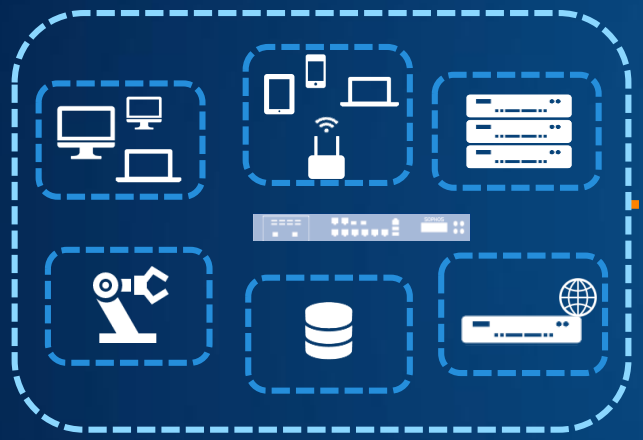
SOPHOS

Chmura, jaka chmura?

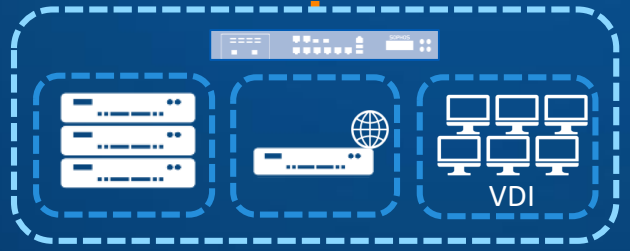
On-Premise, Chmura prywatna, Chmura publiczna

Procesy Biznesowe jako usługa

Oprogramowanie jako usługa



On-Premise

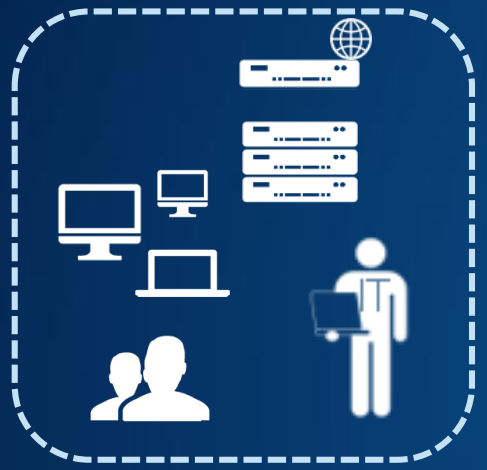


Zewnętrzne Centrum Danych
Chmura Prywatna

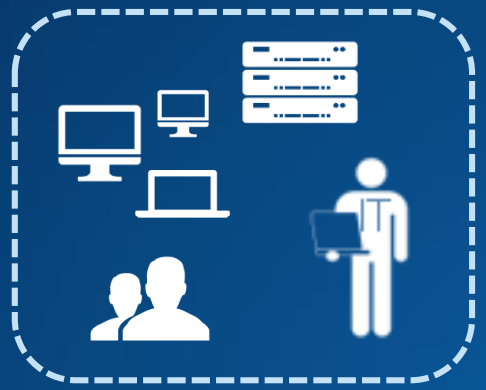
Chmura publiczna

SOPHOS

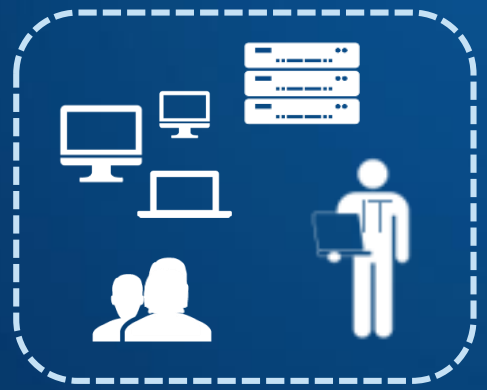
W stronę chmury



Główna siedziba
Kraków



Warszawa



Wrocław

Zewnętrzne
Centrum Danych

Chmura Prywatna

sdworx SAP

Procesy Biznesowe jako usługa

Office 365 SOPHOS CENTRAL salesforce

Oprogramowanie jako usługa

Infrastruktura jako usługa

Chmura Publiczna

SOPHOS

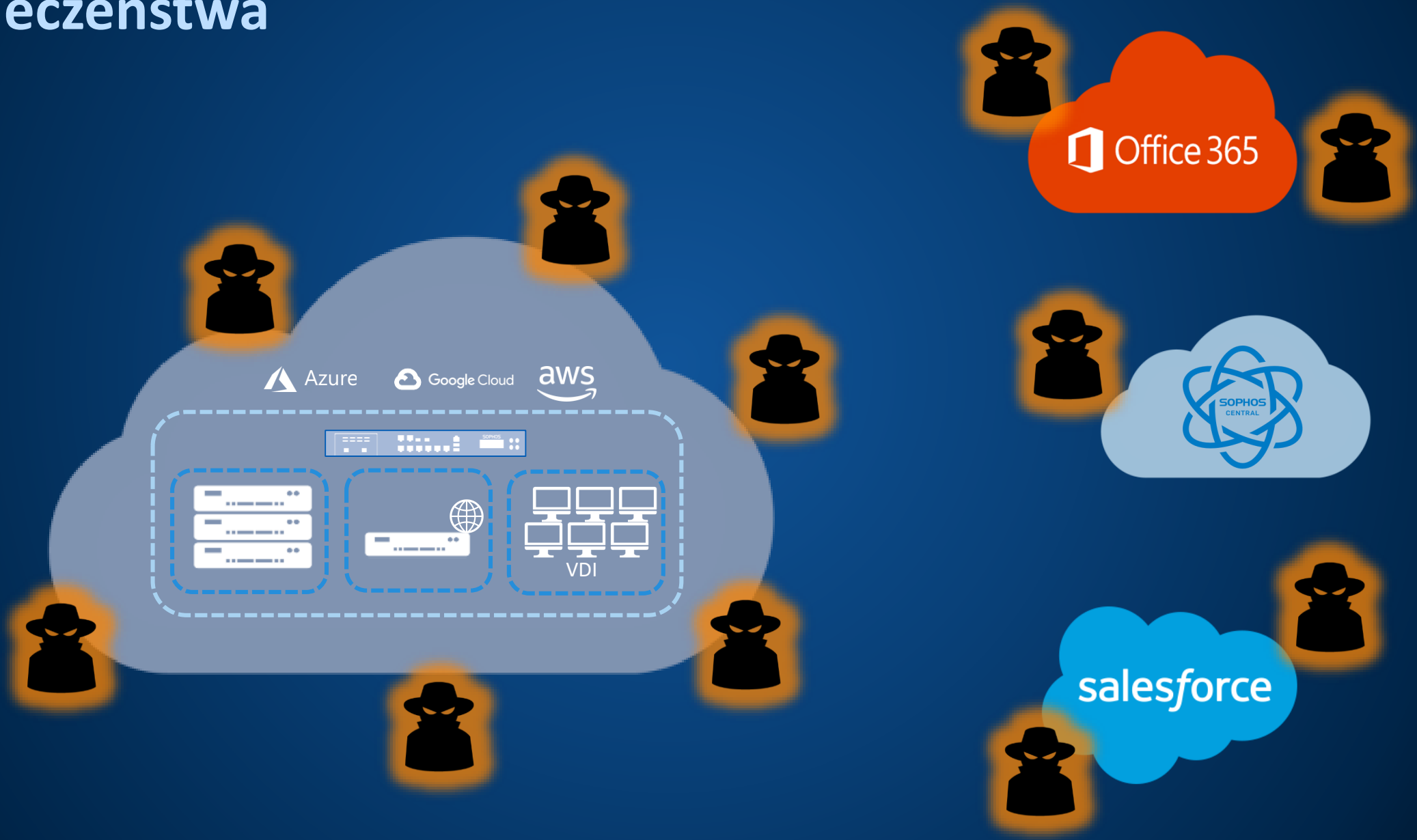
Co jest bezpieczniejsze- On-premise czy Chmura?

SOPHOS

On Premise Security – Wszystko pod konktrolą(?)

Chmura – więcej płaszczyzn ataku, ale..

Chmura – Operatorzy przykładają dużo uwagi do bezpieczeństwa



Co dalej?

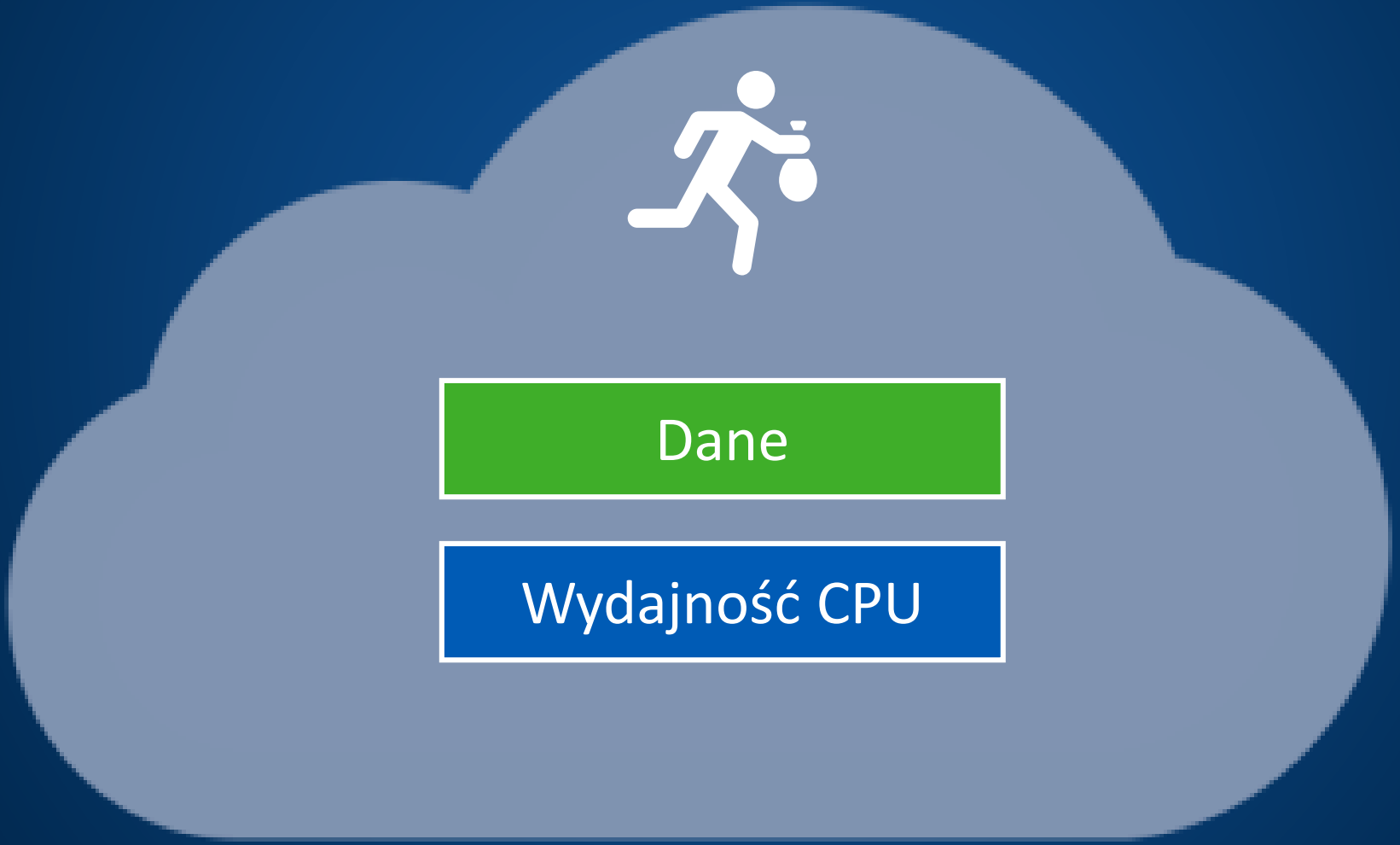
On-Premise

- Komputery i urządzenia pamięci masowej pod moją (fizycznną) kontrolą
- -> Muszę się zajmować ich bezpieczeństwem/dostępnością
- Konieczna ochrona przed hakerami
  -> tym również muszę się zająć

Chmura Publiczna

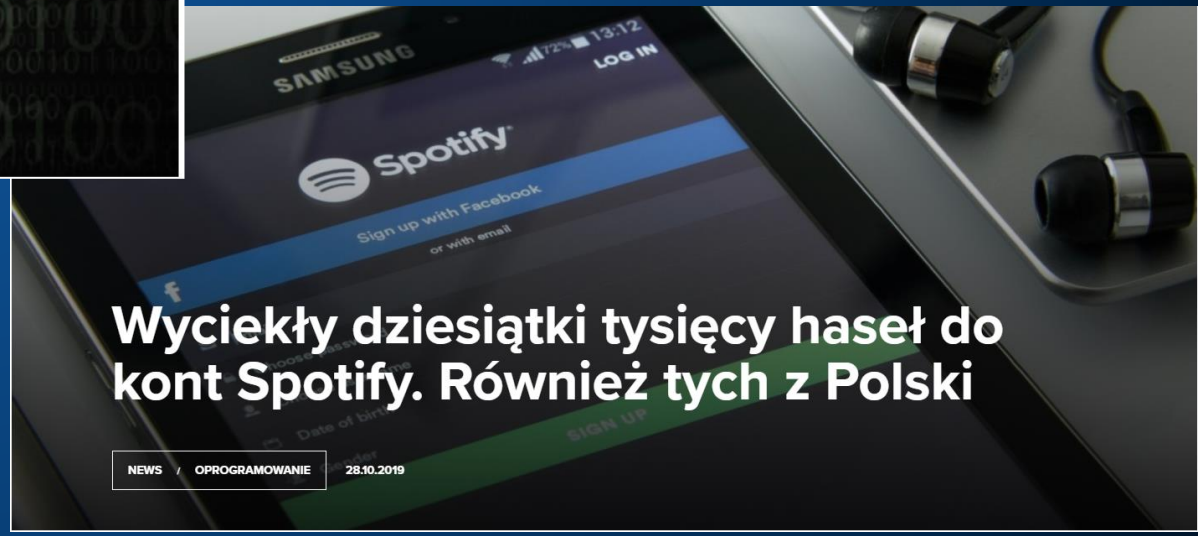
- Komputery i wirtualny storage
  ->Operator usługi Chmurowej świadczy opiekę nad bezpieczeństwem i dostepnością
- Ochrona przed hakerami
  -> Dostawca usług w chmurze bardzo sumiennie chroni swoje zasoby
  -> opcjonalnie: chronię również zwirtualizowane komputery

Co jest celem hakerów?



Co się stanie jeśli nie będzie dobrej kontroli?

Wyciek danych



Wyciek Danych

IT Mobiles Entertainment Wissen Netzpolitik Wirtschaft Journal

TOPTHEMEN: RASPBERRY PI DSGVO 5G HUAWEI WINDOWS 10 E-AUTO ANZEIGE: CLO

heise Developer ⟩ 7-Tage-News ⟩ 05/2019 ⟩ Samsung: Sourcecode und Zugangsdaten waren öffentlich einsehbar

Samsung: Sourcecode und Zugangsdaten waren öffentlich einsehbar

Ein grober Fehler bei den Einstellungen des GitLab-Repositorys erlaubte zeitweilig unter anderem Zugang zum SmartThings-Sourcecode.

Lesezeit: 1 Min. In Pocket speichern 33

(Bild: dpa, Yonhap South)

09.05.2019 11:34 Uhr | Developer

Bloomberg the Company & Its Products | Bloomberg Anywhere Remote Login | Bloomberg Terminal Demo Request

Menu Search **Bloomberg** Sign In **Subscribe**

Photographer: Bloomberg/Bloomberg

Cybersecurity

Ford, TD Bank Files Found Online in Cloud Data Exposure

Information management company Attunity left emails, log-ins and project plans open to public view

By Nico Grant and Josh Eidelson
27. Juni 2019, 19:45 MESZ

LISTEN TO ARTICLE
▶ 6:11

SHARE THIS ARTICLE
Share

Attunity Ltd., a company that manages and safeguards data, left internal files exposed on the internet for clients including Ford Motor Co., and the Toronto-Dominion Bank, in the latest example of sensitive information being publicly accessible on the web.

LIVE ON BLOOMBERG
Watch Live TV ›
Listen to Live Radio ›

Most Read

MARKETS

SOPHOS

Wyciek Danych z Amazon S3 Buckets

List of AWS S3 Leaks

Feel free to send in a PR if you know of other leaks

Date	Description	Notes
Mar 2018	Medical Records and Patient-Doctor Recordings Were Exposed	information for employees of 181 business locations, as well as personally identifiable information (PII) for nearly 3,000 individuals was publicly exposed in an unsecured
Mar 2018	Jewelry site accidentally leaks personal details (and plaintext passwords!) of 1.3M users	addresses, zip-codes, e-mail addresses, and IP addresses. He also claims the database contained plaintext passwords
Feb	S3 bucket open to world : Octoly	real names, addresses, phone numbers, email addresses
Jan 22	Sensitive medical records on AWS bucket found to be publicly accessible	
Dec 2017	Alteryx leave S3 bucket open for anonymous user : 120m american households exposed	Home addresses, contact information, mortgage status, financial histories
Nov 2017	111 GB of internal customer information from National Credit Federation, a Tampa, Florida-based credit repair service	- SSN - Drivers licesne, credit reports
Nov 2017	Uber, the hack happend couple months back was brought to light in Nov 2017>	personal information of 57 million Uber users and driver's license numbers
Nov 2017	NSA leak exposes Red Disk, the Army's failed intelligence system	100 gigabytes of data from an Army intelligence project, codenamed "Red Disk."
Nov 2017	Australia data leak: Nearly 50,000 government and private staffers' sensitive data publicly exposed	S3 bucket left open by a contractor

- An unsecured S3 server exposed thousands of FedEx customer records
- An AWS S3 error exposed GoDaddy business secrets
- Accenture left a huge trove of highly sensitive data, including "keys to the kingdom," on exposed servers
- Customer records for at least 14 million Verizon subscribers, including phone numbers and account PINs, were exposed via an S3 bucket
- A Verizon AWS S3 bucket containing over 100 MB of data about the company's internal billing system was also found exposed online
- An S3 database left exposed leaked the personal details of job applications that had Top Secret government clearance
- Another S3 server exposed the details of 198 million American voters
- National Credit Federation leaked US citizen data through unsecured AWS bucket
- Nigerian airline Arik Air also leaked customer data via an exposed S3 bucket
- Pocket iNet ISP exposed 73GB of data including secret keys, plain text passwords
- An S3 leak at Alteryx left 123 million American households exposed to fraud and spam
- AgentRun, an insurance startup, also leaked sensitive customer health data via amisconfigured Amazon S3 bucket
- Donald Trump's campaign website also leaked intern resumes via an S3 bucket
- Spyware firm SpyFone also left customer data, recordings exposed online via an S3 server
- Booz Allen Hamilton, a top DOD contractor, leaked 60,000 files, including employee security credentials and passwords to a US government system
- An AWS S3 server leaked the personal details of over three million WWE fans who registered on the company's sites
- An auto-tracking company leaked over a half of a million car and car owner details.
- Voting machine firm Election Systems & Software (ES&S) left an S3 bucket exposed online that contained the personal records of 1.8 million Chicago voters
- Dow Jones leaked the personal details of 2.2 million customers
- An S3 bucket leaked data of thousands of Australian government and bank employees

https://github.com/nagwww/s3-leaks

Co się dzieje??

Bezpieczeństwo Chmury Publicznej

„Prawie wszystkie udane ataki na usługi w chmurze są wynikiem błędnej konfiguracji klienta, niewłaściwego zarządzania i błędów”.

Gartner®

Source: Gartner Innovation Insight for Cloud Security Posture Management, Neil MacDonald, 25 January 2019

Jakie mamy różnice w chmurze?

On Premise Security

SOPHOS

On Premise

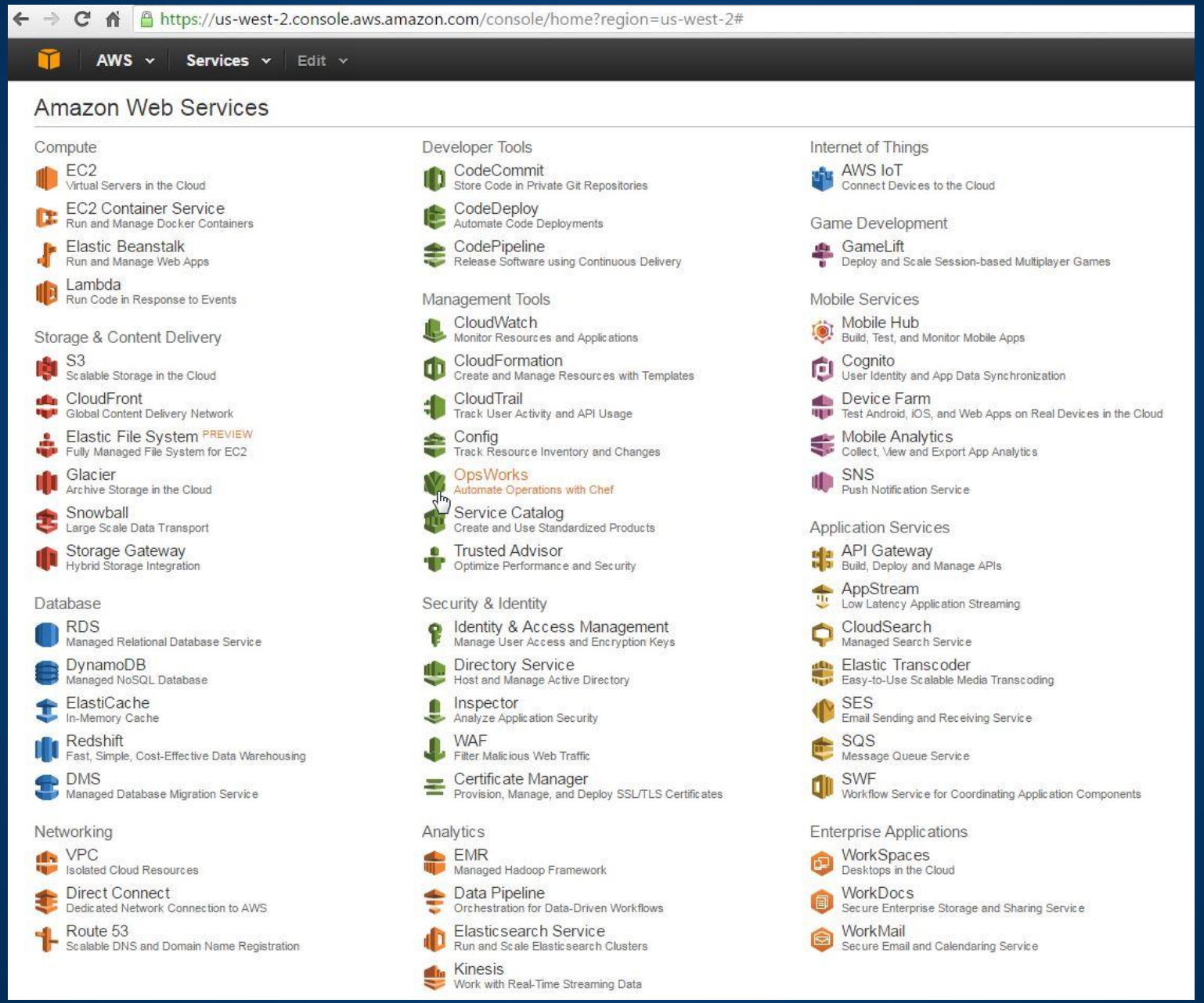
SOPHOS

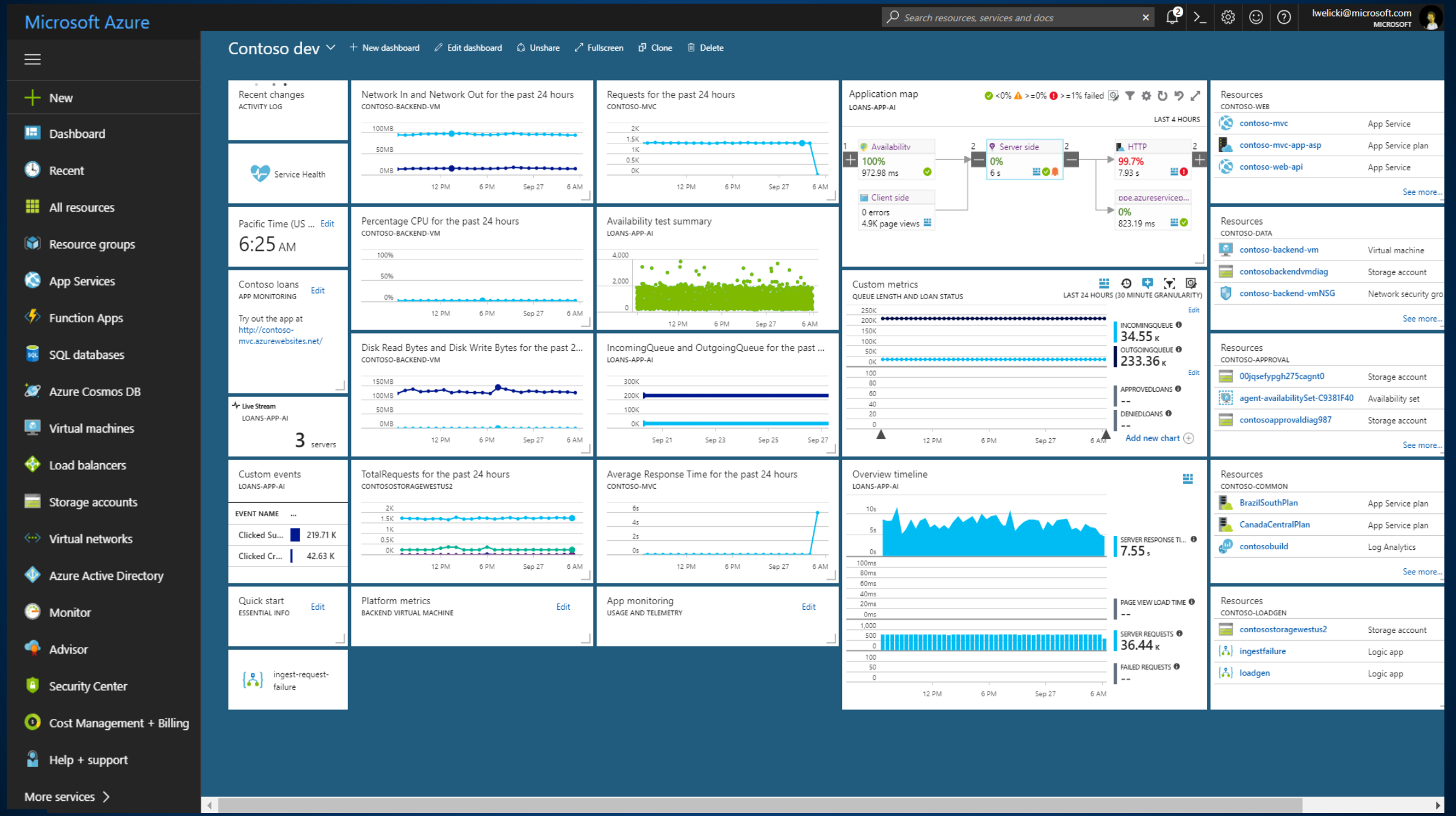
Bezpieczeństwo Chmury- wszystko wirtualne

SOPHOS


Tradycyjne Usługi
ON
OFF


Chmurowe Usługi
ON
OFF

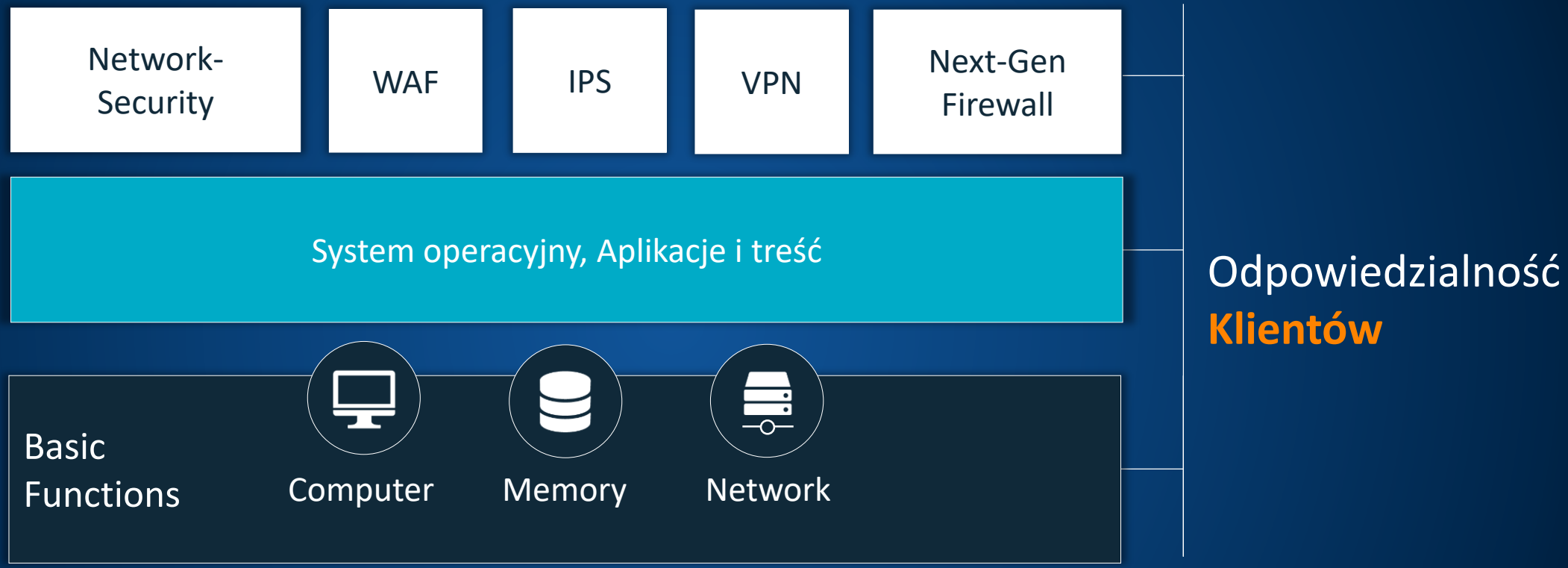

https://us-west-2.console.aws.amazon.com/console/home?region=us-west-2#
AWS
Services
Edit
Amazon Web Services
Compute
EC2
Virtual Servers in the Cloud
EC2 Container Service
Run and Manage Docker Containers
Elastic Beanstalk
Run and Manage Web Apps
Lambda
Run Code in Response to Events
Storage & Content Delivery
S3
Scalable Storage in the Cloud
CloudFront
Global Content Delivery Network
Elastic File System PREVIEW
Fully Managed File System for EC2
Glacier
Archive Storage in the Cloud
Snowball
Large Scale Data Transport
Storage Gateway
Hybrid Storage Integration
Database
RDS
Managed Relational Database Service
DynamoDB
Managed NoSQL Database
ElastiCache
In-Memory Cache
Redshift
Fast, Simple, Cost-Effective Data Warehousing
DMS
Managed Database Migration Service
Networking
VPC
Isolated Cloud Resources
Direct Connect
Dedicated Network Connection to AWS
Route 53
Scalable DNS and Domain Name Registration
Developer Tools
CodeCommit
Store Code in Private Git Repositories
CodeDeploy
Automate Code Deployments
CodePipeline
Release Software using Continuous Delivery
Management Tools
CloudWatch
Monitor Resources and Applications
CloudFormation
Create and Manage Resources with Templates
CloudTrail
Track User Activity and API Usage
Config
Track Resource Inventory and Changes
OpsWorks
Automate Operations with Chef
Service Catalog
Create and Use Standardized Products
Trusted Advisor
Optimize Performance and Security
Security & Identity
Identity & Access Management
Manage User Access and Encryption Keys
Directory Service
Host and Manage Active Directory
Inspector
Analyze Application Security
WAF
Filter Malicious Web Traffic
Certificate Manager
Provision, Manage, and Deploy SSL/TLS Certificates
Analytics
EMR
Managed Hadoop Framework
Data Pipeline
Orchestration for Data-Driven Workflows
Elasticsearch Service
Run and Scale Elasticsearch Clusters
Kinesis
Work with Real-Time Streaming Data
Internet of Things
AWS IoT
Connect Devices to the Cloud
Game Development
GameLift
Deploy and Scale Session-based Multiplayer Games
Mobile Services
Mobile Hub
Build, Test, and Monitor Mobile Apps
Cognito
User Identity and App Data Synchronization
Device Farm
Test Android, iOS, and Web Apps on Real Devices in the Cloud
Mobile Analytics
Collect, View and Export App Analytics
SNS
Push Notification Service
Application Services
API Gateway
Build, Deploy and Manage APIs
AppStream
Low Latency Application Streaming
CloudSearch
Managed Search Service
Elastic Transcoder
Easy-to-Use Scalable Media Transcoding
SES
Email Sending and Receiving Service
SQS
Message Queue Service
SWF
Workflow Service for Coordinating Application Components
Enterprise Applications
WorkSpaces
Desktops in the Cloud
WorkDocs
Secure Enterprise Storage and Sharing Service
WorkMail
Secure Email and Calendaring Service


Microsoft Azure
Search resources, services and docs
lwelicki@microsoft.com
MICROSOFT
New
Dashboard
Recent
All resources
Resource groups
App Services
Function Apps
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
More services
Contoso dev
New dashboard
Edit dashboard
Unshare
Fullscreen
Clone
Delete
Recent changes
ACTIVITY LOG
Service Health
Pacific Time (US ... Edit
6:25 AM
Contoso loans
APP MONITORING
Edit
Try out the app at http://contoso-mvc.azurewebsites.net/
Live Stream
LOANS-APP-AI
3 servers
Custom events
LOANS-APP-AI
EVENT NAME ...
Clicked Su... 219.71 K
Clicked Cr... 42.63 K
Quick start
ESSENTIAL INFO
Edit
ingest-request-failure
Network In and Network Out for the past 24 hours
CONTOSO-BACKEND-VM
Requests for the past 24 hours
CONTOSO-MVC
Percentage CPU for the past 24 hours
CONTOSO-BACKEND-VM
Availability test summary
LOANS-APP-AI
Disk Read Bytes and Disk Write Bytes for the past 2...
CONTOSO-BACKEND-VM
IncomingQueue and OutgoingQueue for the past ...
LOANS-APP-AI
TotalRequests for the past 24 hours
CONTOSOSTORAGEWESTUS2
Average Response Time for the past 24 hours
CONTOSO-MVC
Platform metrics
BACKEND VIRTUAL MACHINE
Edit
App monitoring
USAGE AND TELEMETRY
Edit
Application map
LOANS-APP-AI
<0% >=0% >=1% failed
LAST 4 HOURS
Availability
100%
972.98 ms
Client side
0 errors
4.9K page views
Server side
0%
6 s
HTTP
99.7%
7.93 s
0%
823.19 ms
Custom metrics
QUEUE LENGTH AND LOAN STATUS
LAST 24 HOURS (30 MINUTE GRANULARITY)
Edit
INCOMINGQUEUE
34.55 K
OUTGOINGQUEUE
233.36 K
APPROVEDLOANS
--
DENIEDLOANS
--
Add new chart
Overview timeline
LOANS-APP-AI
SERVER RESPONSE TI...
7.55 s
PAGE VIEW LOAD TIME
--
SERVER REQUESTS
36.44 K
FAILED REQUESTS
--
Resources
CONTOSO-WEB
contoso-mvc App Service
contoso-mvc-app-asp App Service plan
contoso-web-api App Service
See more...
Resources
CONTOSO-DATA
contoso-backend-vm Virtual machine
contosobackendvmdiag Storage account
contoso-backend-vmNSG Network security gro
See more...
Resources
CONTOSO-APPROVAL
00jqsefypgh275cagnt0 Storage account
agent-availabilitySet-C9381F40 Availability set
contosoapprovaldiag987 Storage account
See more...
Resources
CONTOSO-COMMON
BrazilSouthPlan App Service plan
CanadaCentralPlan App Service plan
contosobuild Log Analytics
See more...
Resources
CONTOSO-LOADGEN
contosostoragewestus2 Storage account
ingestfailure Logic app
loadgen Logic app

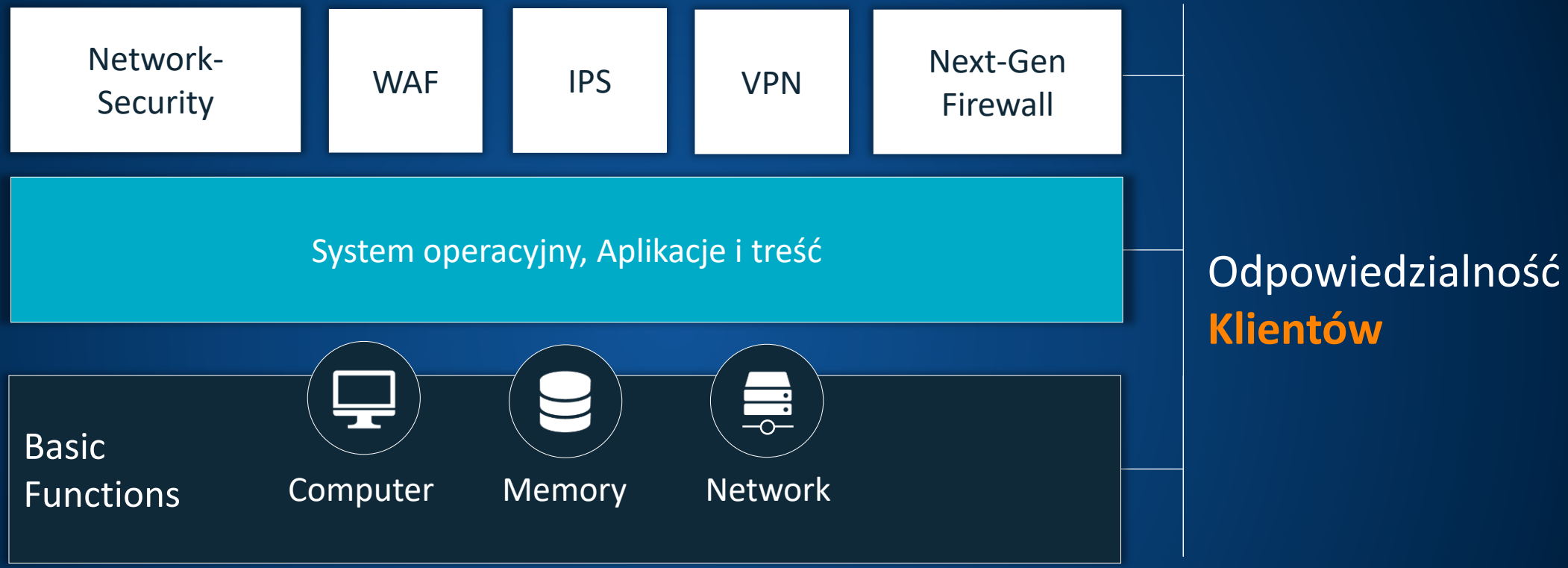
SOPHOS

Jaka jest Twoja odpowiedzialność?

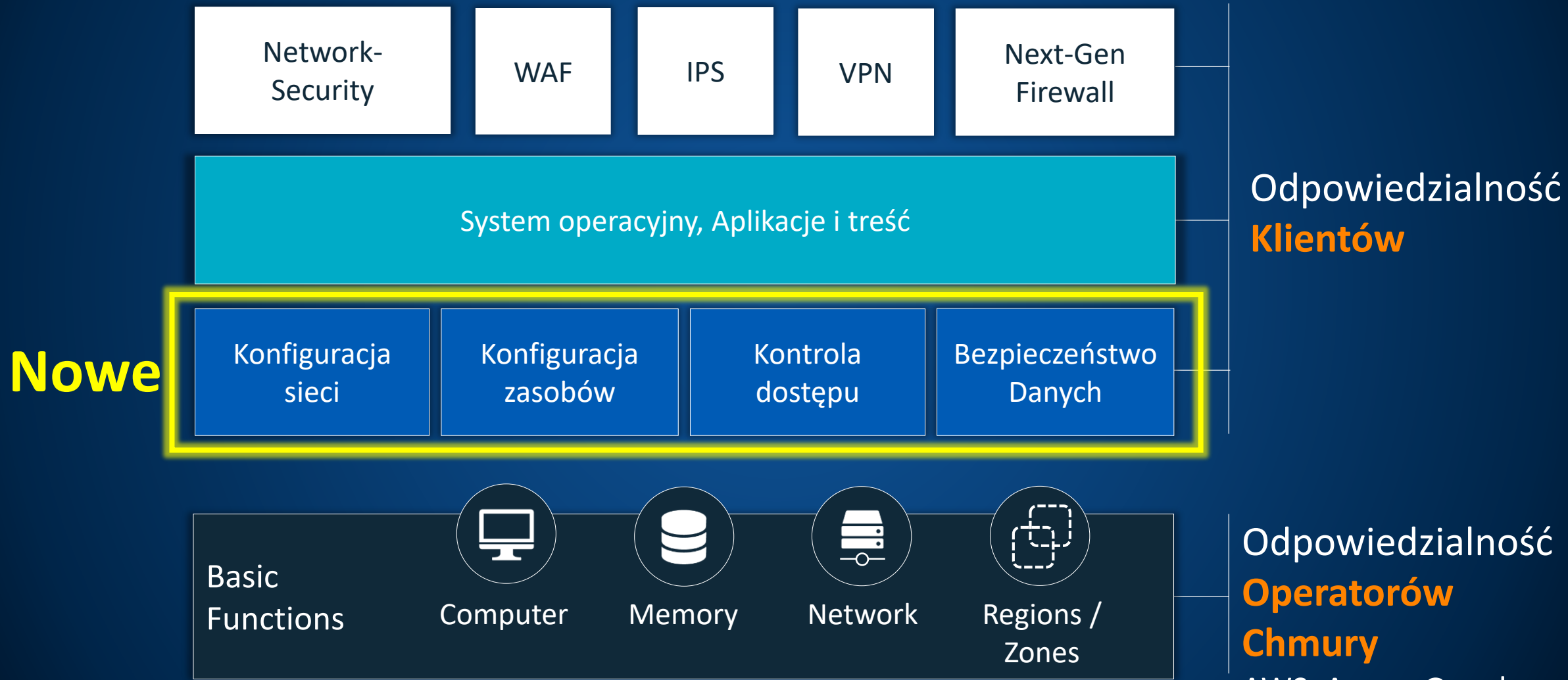
On-Premise


Network-Security
WAF
IPS
VPN
Next-Gen Firewall
System operacyjny, Aplikacje i treść
Basic Functions
Computer
Memory
Network
Odpowiedzialność
Klientów

On-Premise

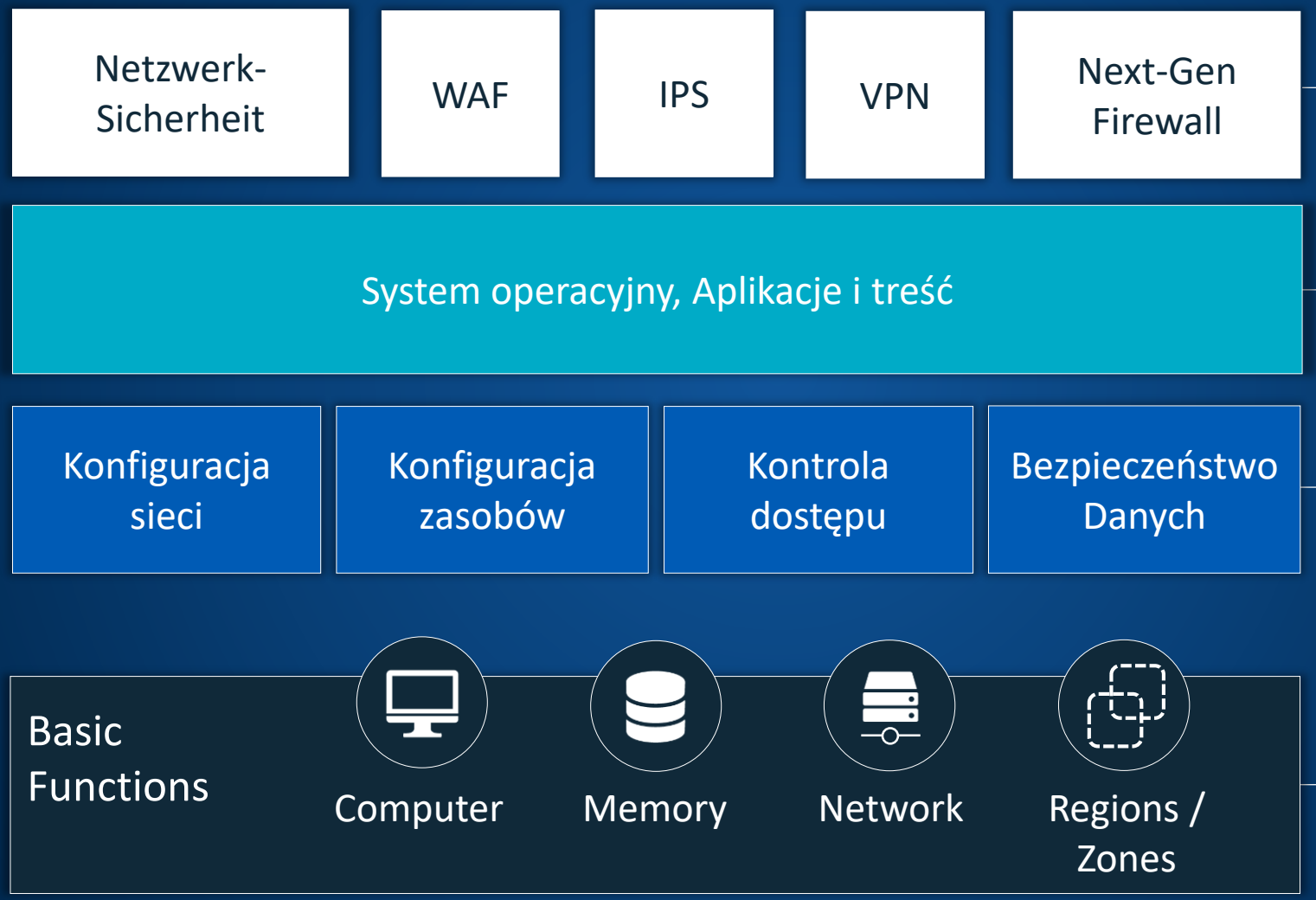

Network-Security
WAF
IPS
VPN
Next-Gen Firewall
System operacyjny, Aplikacje i treść
Basic Functions
Computer
Memory
Network
Odpowiedzialność
Klientów

Chmura – nowa warstwa dostępu do zasobów



SOPHOS

Chmura – wspólna odpowiedzialność



- Firewall
- Bezpieczeństwo hosta

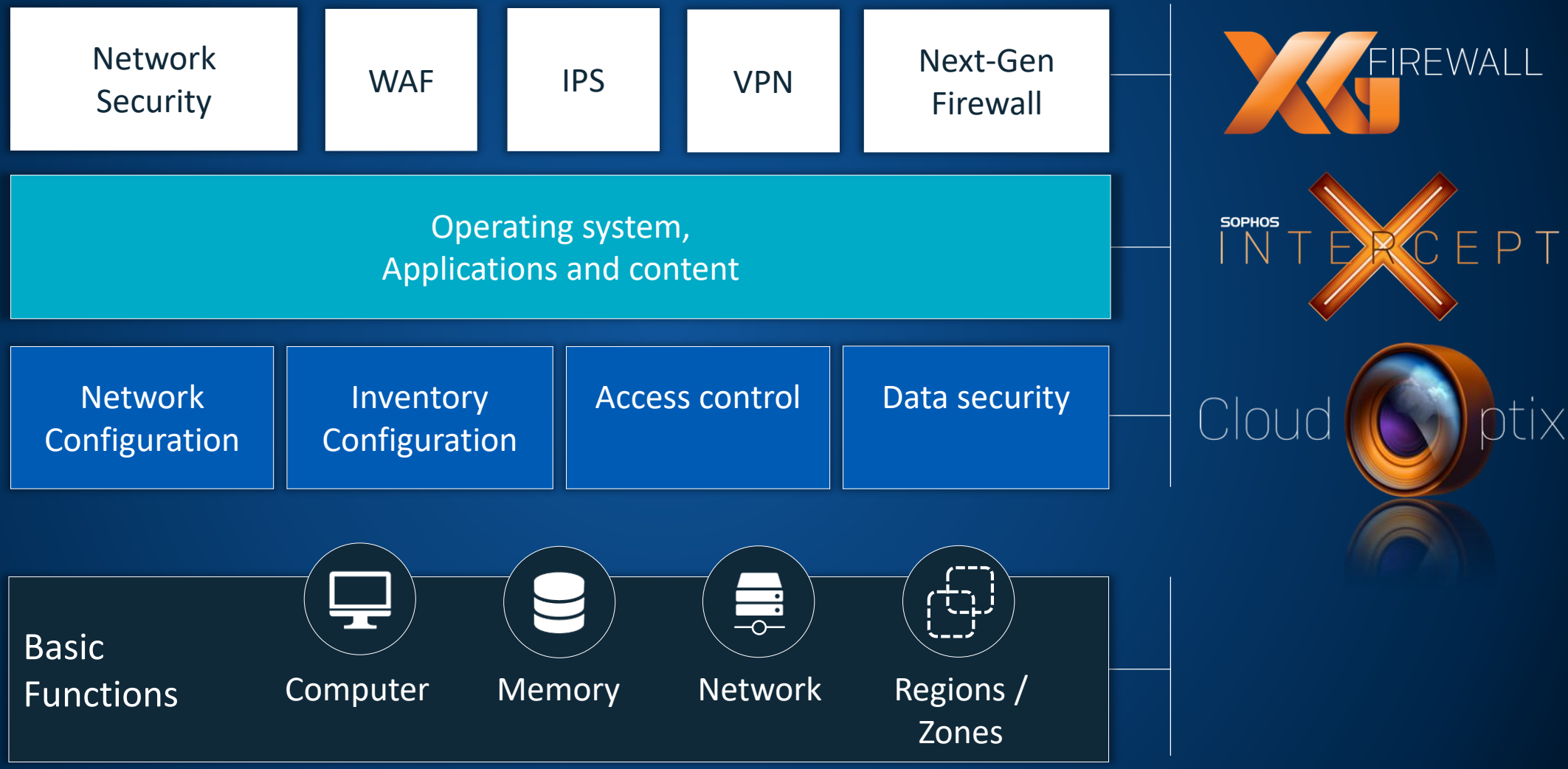
- Bezpieczeństwo danych i aplikacji

- **Bezpieczne zarządzanie dostępem do konfiguracji**

Odpowiezdzialność
Cloud Providers
AWS, Azure, Google

SOPHOS

Jak Sophos może pomóc?



SOPHOS

Cloud Optix

Azure aws Google Cloud

Widoczność

Z których i jakich zasobów chmury korzystam?

Czy zdarzają się teraz i czy to takie zamierzone?

Zgodność

Czy moje środowisko jest zgodne z RODO?

Czy uwierzytelnianie i logowanie są poprawnie skonfigurowane?

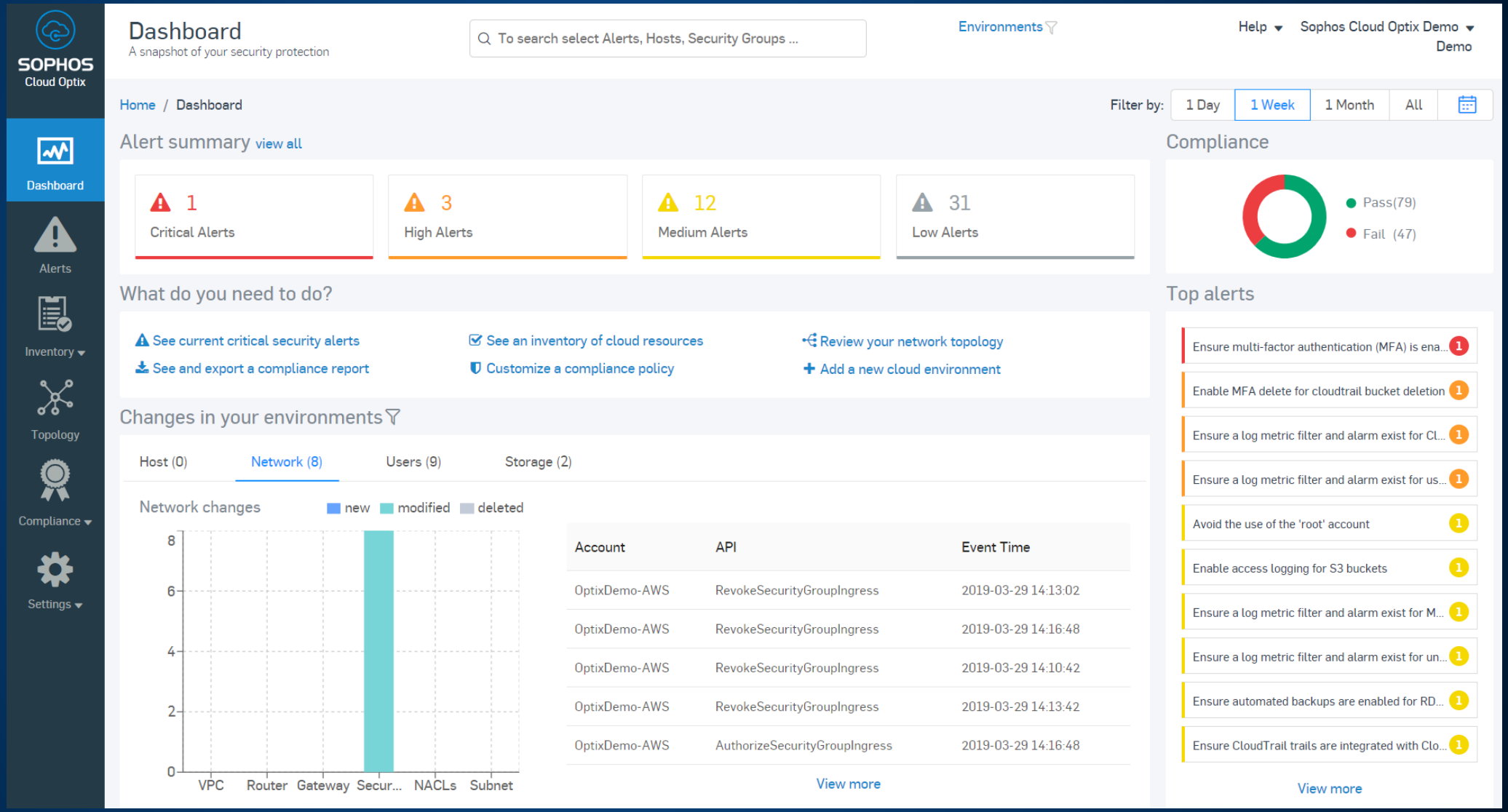
Reakcja

Ataki hakerów są wykrywane i zatrzymywane za pomocą AI

Błędne konfiguracje są automatycznie korygowane

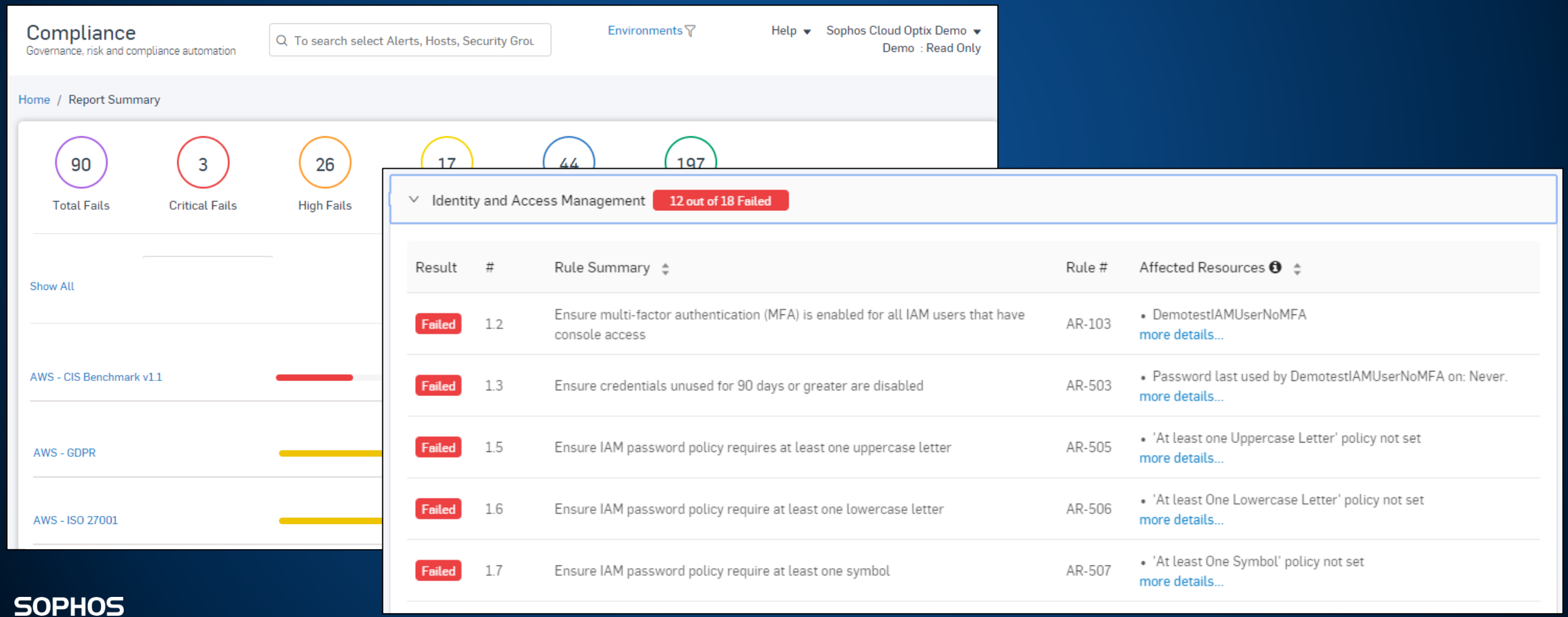
Everything at a glance

- Alarms
- Compliance
- Inventory
- Network
- Changes



Monitorowanie Zgodności

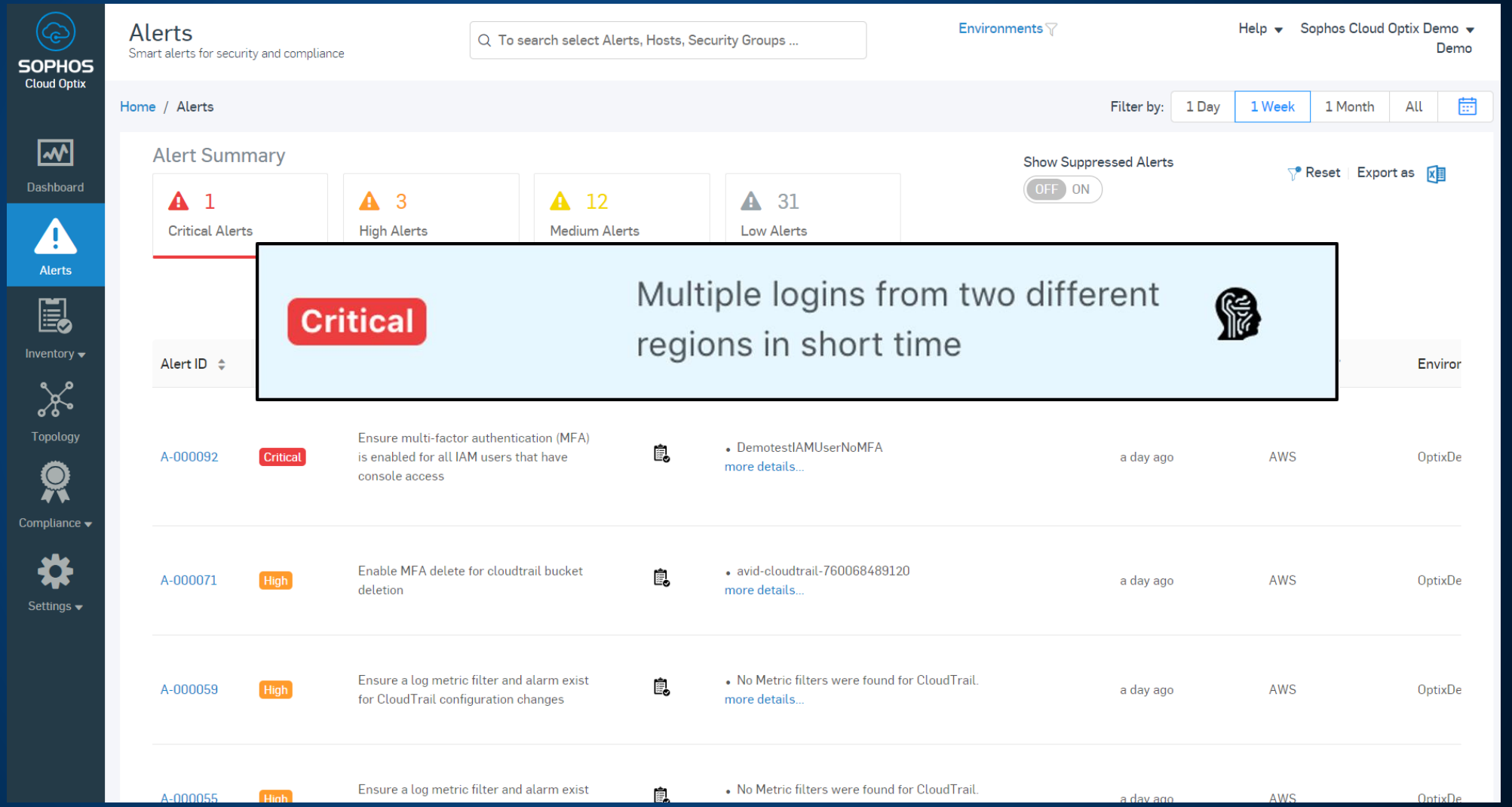
- Czy jestem zgodny z RODO, DSGVO, PCI DSS, SOC 2, …



SOPHOS

Ostrzeżenia i odpowiedzi ze wsparciem AI

- Podejrzany ruch
- Anomalie w rejestracji
- Brak uwierzytelniania wieloskładnikowego
- Closes open S3 buckets and ports
- Wykrywa odchylenia od normalnej konfiguracji



Pytania?

Damian.Przygodzki@Sophos.com

Co dalej ?

Data	Temat
20 Luty 2020	Phishing a prywatność – ochrona tożsamości w świecie wirtualnym

Weź udział i wygraj

Pierwszym 10-ciu uczestnikom, którzy wezmą udział we wszystkich 3 sesjach na żywo podarujemy atrakcyjny plecak Sophos.

Nie zapomnij udostępnić linku rejestracyjnego znajomym i współpracownikowi:
https://attendee.gotowebinar.com/register/5485615647935020035

SOPHOS

Co dalej ?

Phishing and Privacy

Spam i phishing są nadal w dużej mierze wykorzystywane przez cyberprzestępców do atakowania firm. W wielu przypadkach firmowa poczta e-mail jest pierwszą bramą do infrastruktury korporacyjnej. Organizacje mogą opracowywać procesy dotyczące praw osób, których dane dotyczą, przy minimalnej weryfikacji tożsamości w celu uniknięcia grzywien związanych z reklamacjami. Jeśli metody samoobsługi nie są możliwe, w jaki sposób organizacje mogą honorować te prawa, nie będąc ofiarą ataków phishingowych?
Firmy na całym świecie pracują obecnie nad przestrzeganiem unijnego RODO, a phisherzy mogą przygotowywać się do wykorzystania nowych procesów zgodności.

Dołącz do nas jutro, aby uzyskać informację na temat:

- Ochrona Twojej tożsamości/cyfrowej
- Typowe oszustwa związane z wyłudzaniem informacji i sposoby ochrony przed nimi
- Phishing i RODO
- Oszustwa dotyczące wiadomości e-mail i phishingu - studia przypadków