
Advanced Security for your Cloud
Serge Ego
Business

PUBLIC CLOUD GOES MAINSTREAM

More and more business workloads are moving to the public cloud

Why Cloud

AGILITY

Fast to react

ELASTICITY

Fast to grow

Cloud Fundamentals

- Cloud is a **shared** environment
- Cloud is a **connected** environment
- Cloud is a **dynamic** environment

Therefore, cloud is vulnerable and exposed…

Traditional Datacenter vs. Cloud

SIMPLE

TRADITIONAL DATA CENTER

- On-premises infrastructure and applications
- Deployed by highly trained teams
- Tight control over security and compliance

COMPLEX

CLOUD

- Cloud applications and infrastructure
- Deployed by **multiple teams** not under IT control
- High likelihood of inconsistencies and misconfigurations

Security Challenges in the Cloud

Infrastructure Challenges

- Shared Responsibility
- Minimal Visibility
- Ever-Changing workloads
- Multi-Cloud

Internal Risks

- Misconfigurations
- Insider Threat
- Compliance and Regulations

External Threats

- Malware
- Zero-day Threats
- Account Takeover
- Data Leakage

Shared Responsibility

- Cloud providers protect Infrastructure
- Companies must protect Cloud Workloads

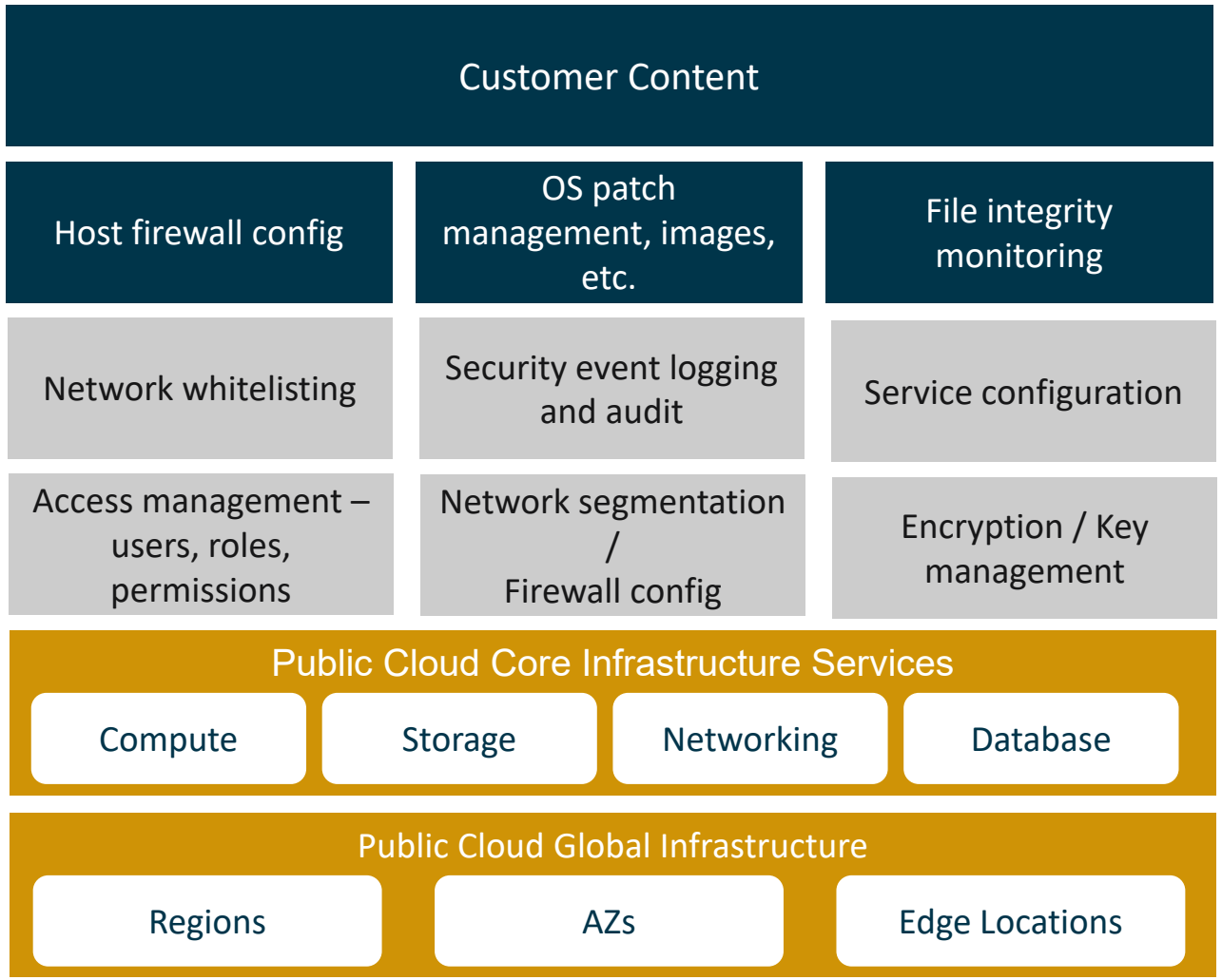
Provider Responsibility

Hardware, SDN, Networking, Internet connection

Customer Responsibility

Application code, Application Data, Application Access, Compliance

Cloud Security is a Shared Responsibility



Gartner®

CIOs must change their line of questioning from:

"Is the cloud secure?"

to

"Am I using the cloud securely? "

The cloud service provider handles this

Solution: Clear Understanding of What A Customer is Responsible For

Minimal Visibility

- Cloud deployments result in challenges around identifying and quantifying assets
- Invisible and unmanaged assets create large gaps in security enforcement

> *Organizations ... are struggling with visibility, making it almost impossible to determine what computing tasks are taking place where, under whose direction.*

Hype Cycle for Cloud Security, Gartner, 7/2018

The Cloud Is Highly Dynamic…and Expanding

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** — 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
- **Device Farm** — Test Android, iOS, and Web App
- **Mobile Analytics** — Collect, View and Export App A
- **SNS** — Push Notification Service

Application Services
- **API Gateway** — Build, Deploy and Manage A
- **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

More Than 300 Services and Assets and Rapidly Growing

Your Cloud Configuration Now…

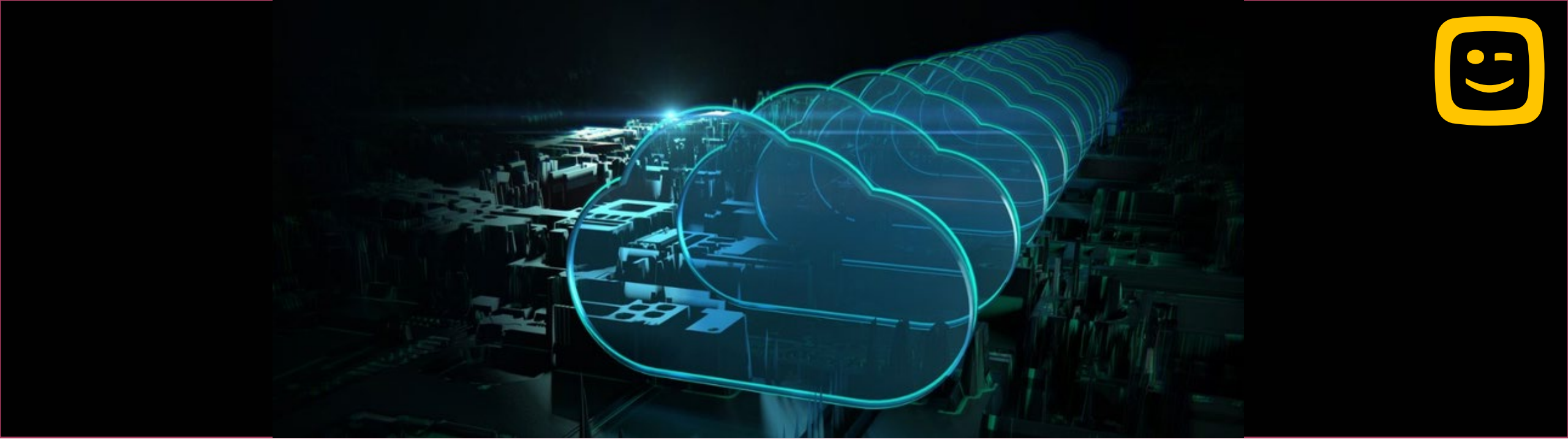
Your Configuration When You Started…

Changing Workloads

- Cloud assets are provisioned and decommissioned dynamically in large scale and fast pace
- Traditional security tools were not developed for the cloud and thus cannot enforce policies in such a flexible environment
- Traditional security can’t work with orchestration tools

> *“Cloud computing is dynamic, with workloads spinning up and spooling down. unprepared organizations are finding that active enforcement of policy becomes increasingly impractical.”*

Hype Cycle for Cloud Security, Gartner, 7/2018



Multi Cloud

Manageability
Relying on the native security controls of the cloud providers limits the ability to manage security in multi-cloud with a unified tool

Consistency
Security posture and governance policies are not consistently applied across on-premises datacenters and cloud providers

Complexity
Difficult to detect and prevent attacks across distributed applications

Flexibility
Cloud environments cannot simultaneously change and apply the security enforcement in real-time

Misconfigurations

Most of the stolen data incidents in the cloud are related to simple human errors rather than concerted attacks

> *Through 2020, 95% of cloud security failures will be the customer's fault*

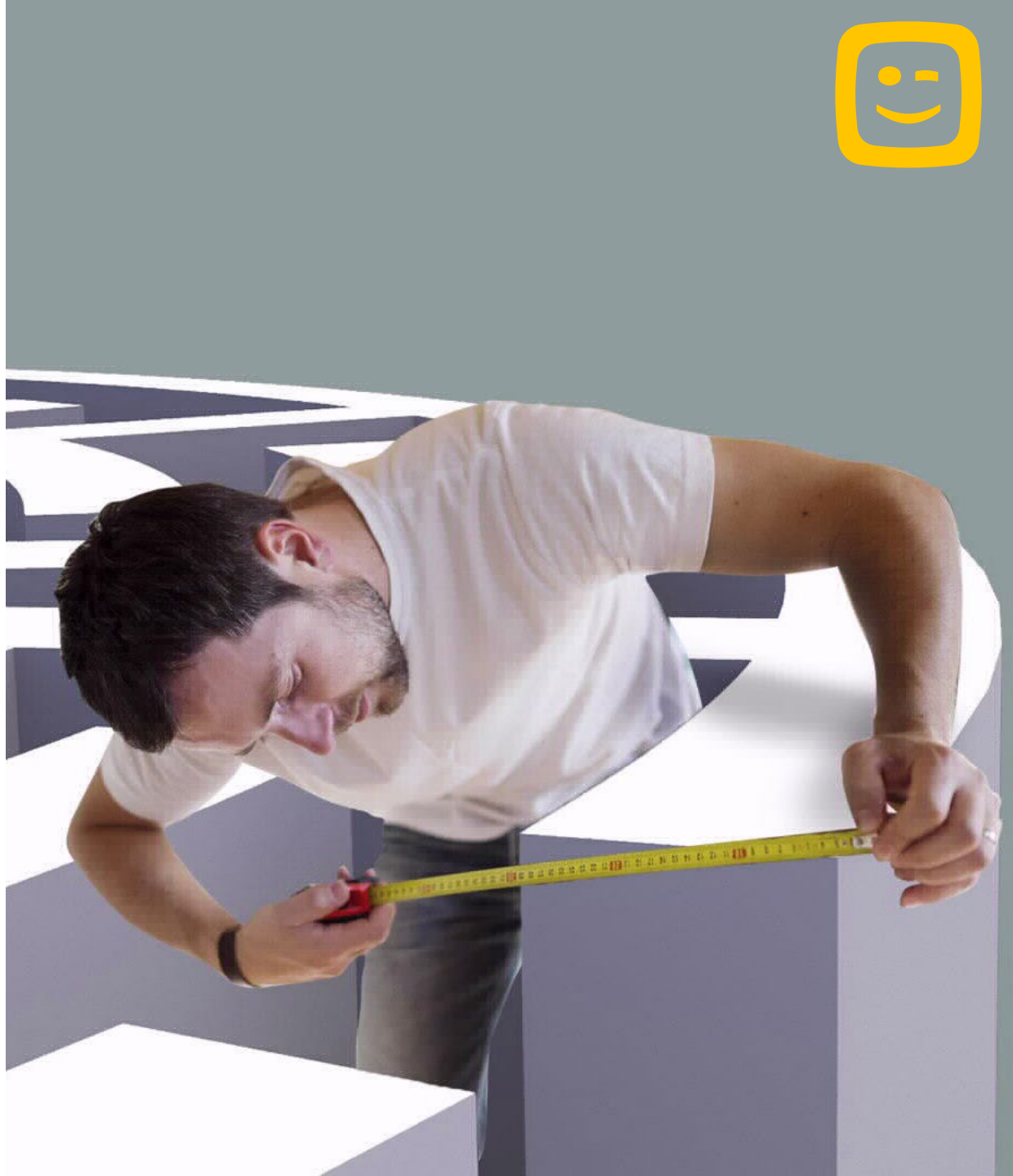
Gartner®

Is the Cloud Secure?
March, 2018

Compliance & Regulations

- Compliance & self governance are highly focused areas for companies in regulated industries (HIPAA, PCI-DSS) or in certain geographical areas (GDPR)

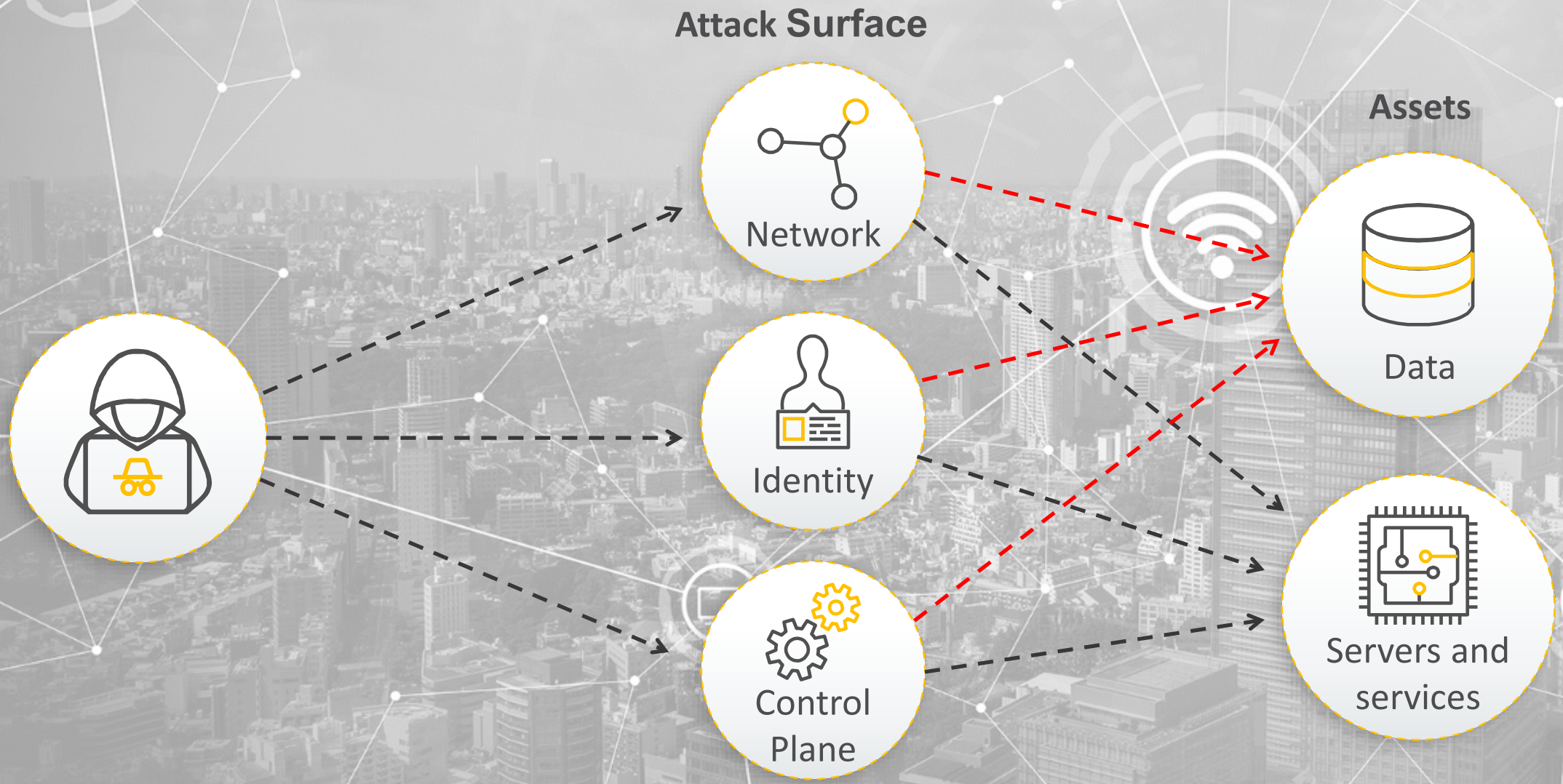
- Lack of visibility, the dynamic nature of cloud and lack of certainty regarding the location of the payload, all make compliance a challenging task.



Zero-day

- Attackers are targeting cloud workloads because they can be accessed via the internet and not hidden inside the on-premises LAN
- Thru lateral movements, once an asset gets infected, both the cloud and On-premises infrastructures are at risk (the cloud can be a bridge to the on-premises datacenter)
- The cloud is a company's new data center. It is exposed to the same threats as the on-premises data center and possibly even more, such as: Worms / Crypto locker / Bot attacks

The Cloud Attack Surface



Insider Threat

- Rogue employees, disgruntled or recurred by attacker can leverage misconfigurations to create massive damages.
- An administrator with access to the root account of a cloud service can easily duplicate this info to other places.
- Companies are saving source code on external repositories, such as GitHub, with no access restrictions essentially open for all.
- A worker with high-level IT access privileges can load Bitcoin mining software onto the cloud workload

Rethink Your Security

- Changing the way security is implemented in the cloud
- Security that is more flexible and agile
- Security that enables the business
- Security that prevents advanced threats

Security Solutions for the Cloud

Infrastructure Challenges

1. One Policy to Manage Everything
2. Visibility of the Assets

Internal Risks

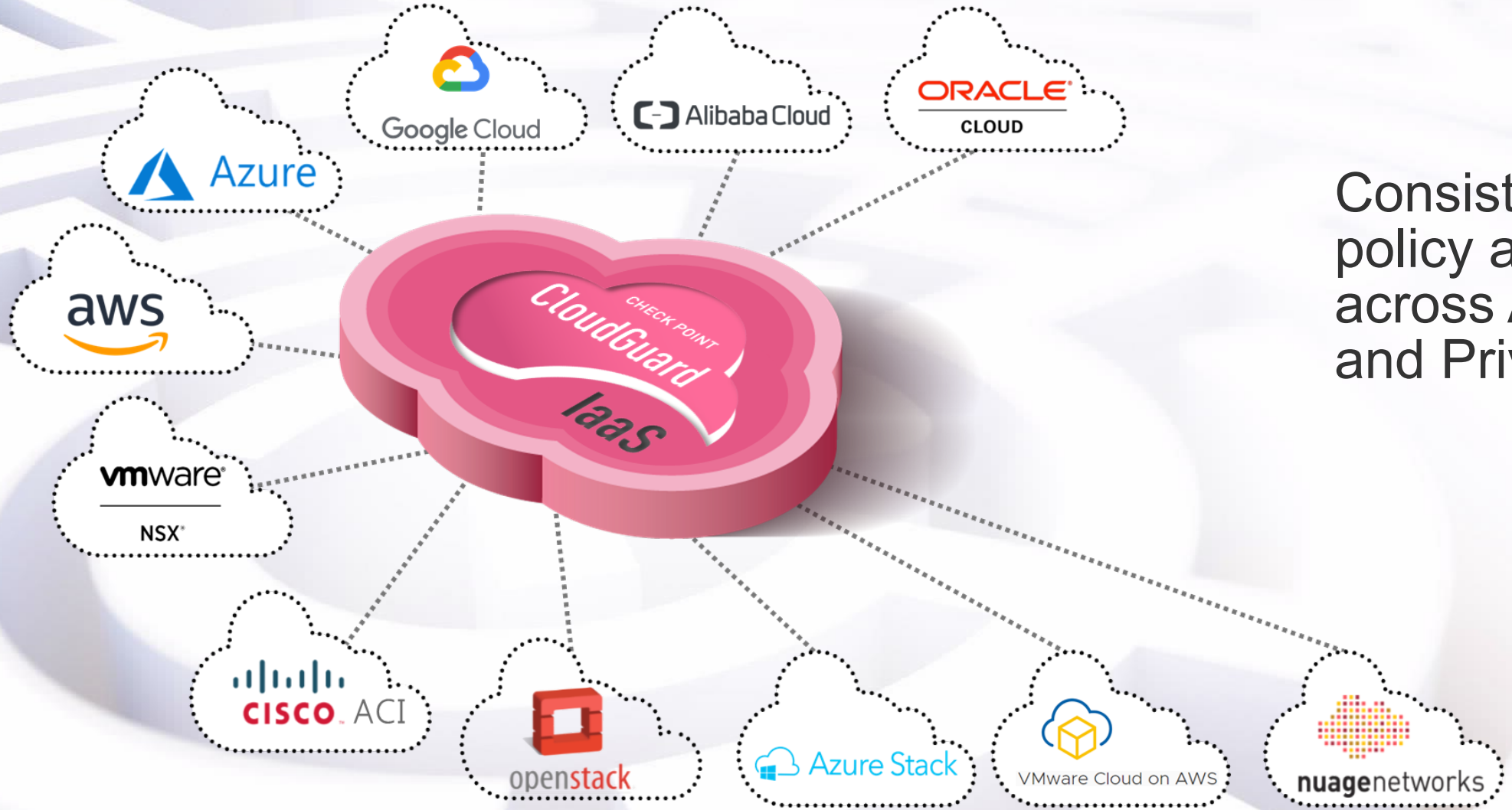
3. Cloud Compliance and Best Practices

External Threats

4. Advanced threat prevention

5. True Visibility of the Users

1. One Policy to Manage Everything



Consistent security policy and control across ALL Public and Private Clouds

Name	Source	Destination	Services & Applications	Data	Action	Install On
Outbound access	production_net	Internet	Any	Any	AccessSubLayer	Policy Targets
Social media for marketing	marketing_role John	Internet	Twitter LinkedIn Instagram	Any	Accept	SG13800
Developers upload	developer_role	Internet	Dropbox Box	Any Direction Source Code - JAVA	Accept	SG13800 Cisco ACI
Access Sensitive Servers	Any	Any	Any	Any	SensitiveServers	Policy Targets
Mobile Access	Mobile Devices	MailUS	MailServer	Any	Accept	Mobile
Access to Web Server	Any	WebServer	https	Any	Accept	AWS VMWare

Consistent Policies
Cloud Freedom
Fastest Time to Service
Visibility

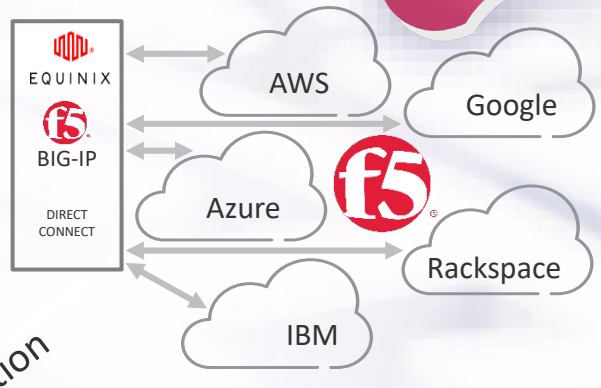
Private Cloud

Workload Migration

Managed Hosting

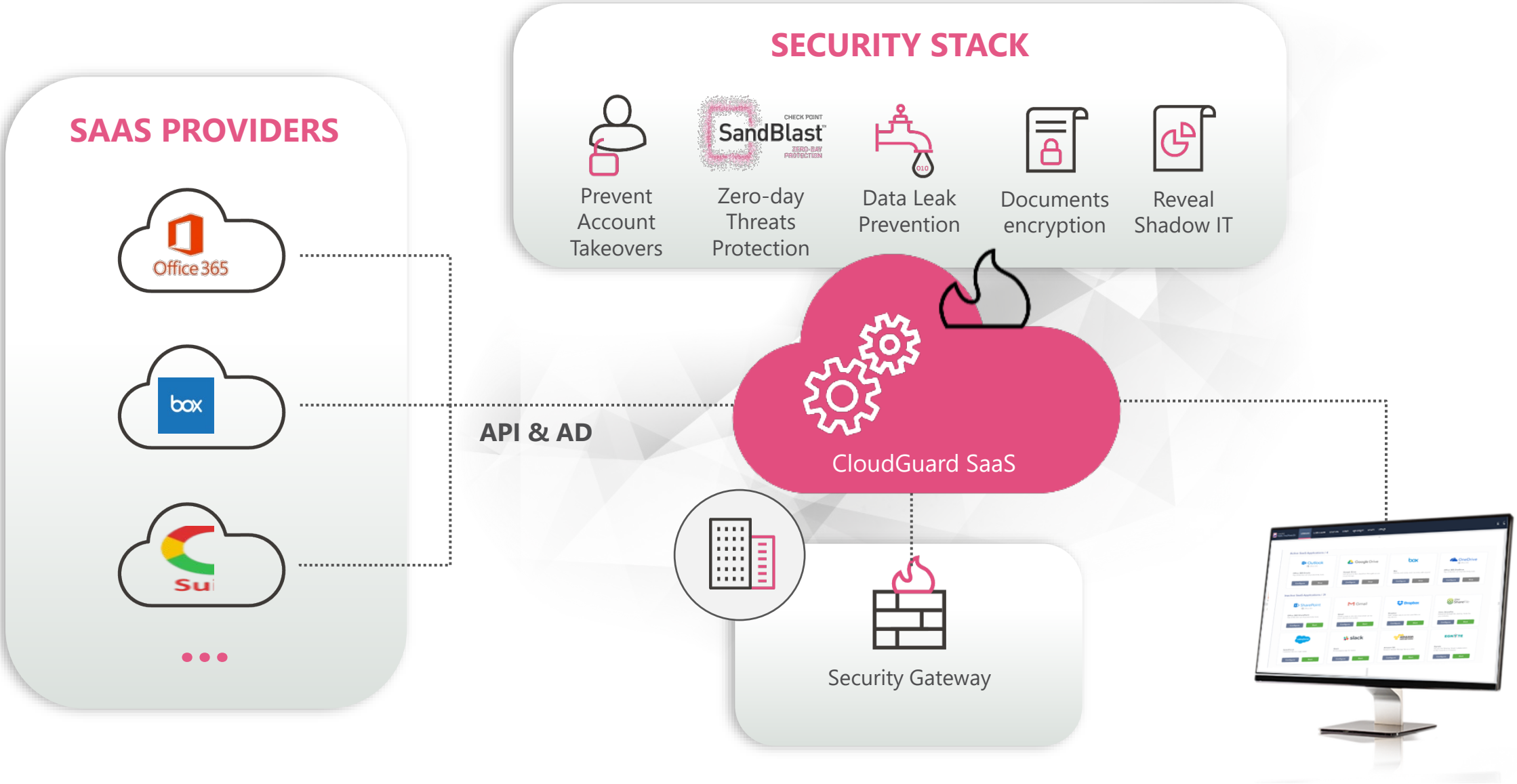
Traditional Data Center

Workload Migration

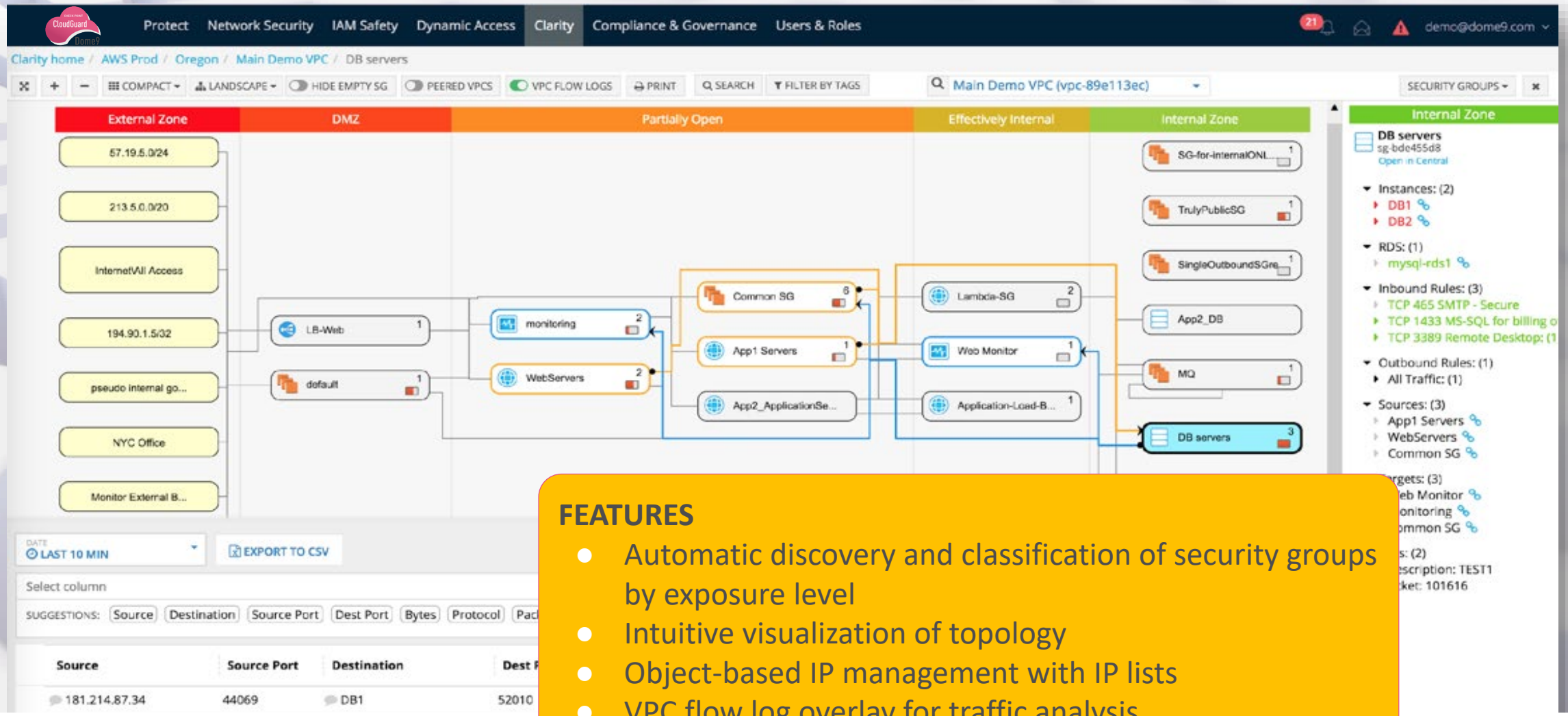


CoLo/Public Cloud

One Policy to Manage SaaS



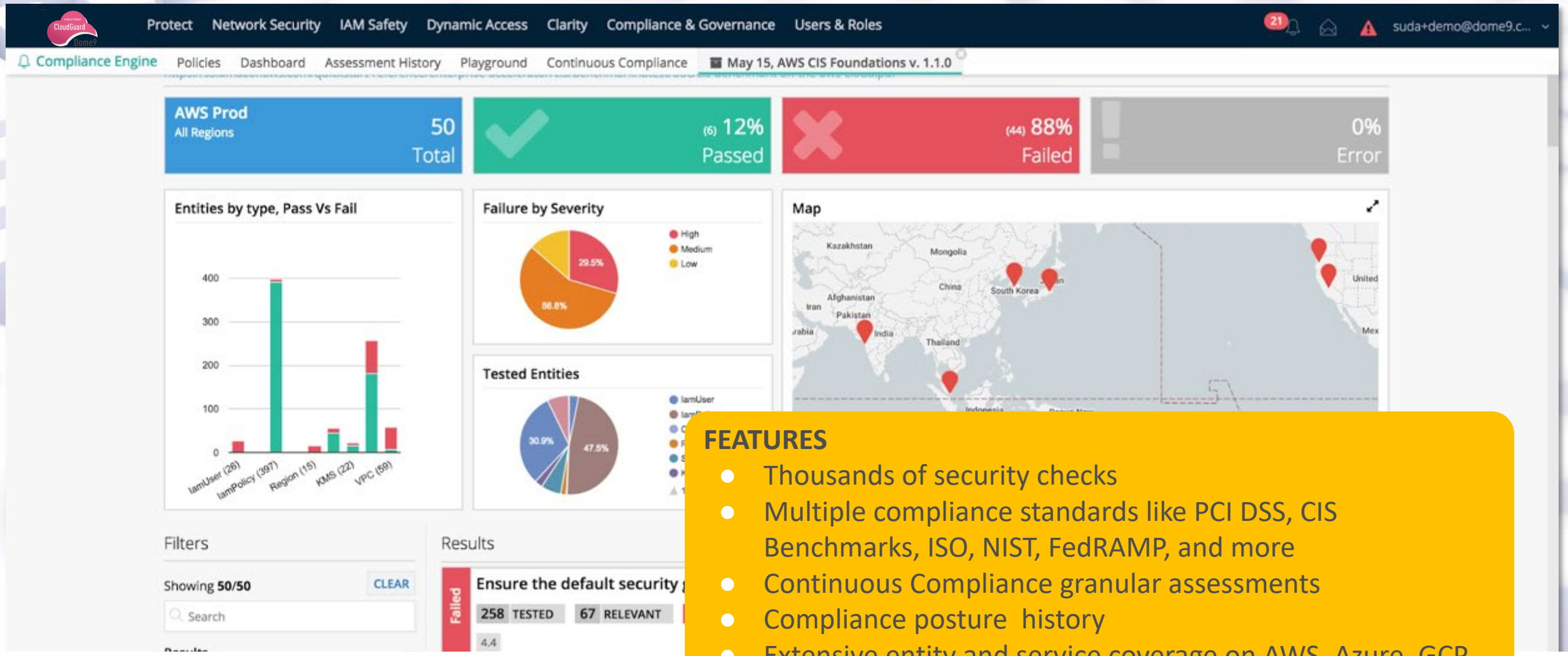
2. Visibility of the Assets



FEATURES

- Automatic discovery and classification of security groups by exposure level
- Intuitive visualization of topology
- Object-based IP management with IP lists
- VPC flow log overlay for traffic analysis
- Click-through remediation

3. Cloud Compliance and Best Practices

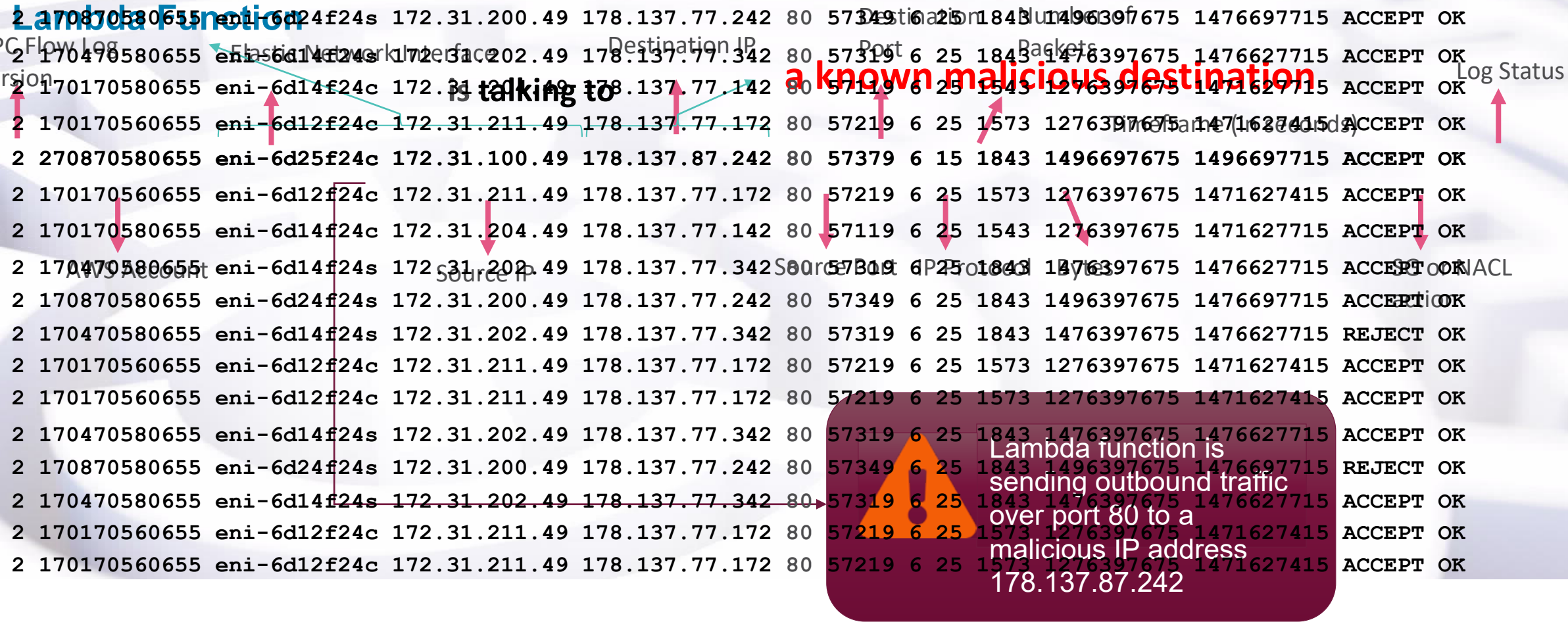


FEATURES

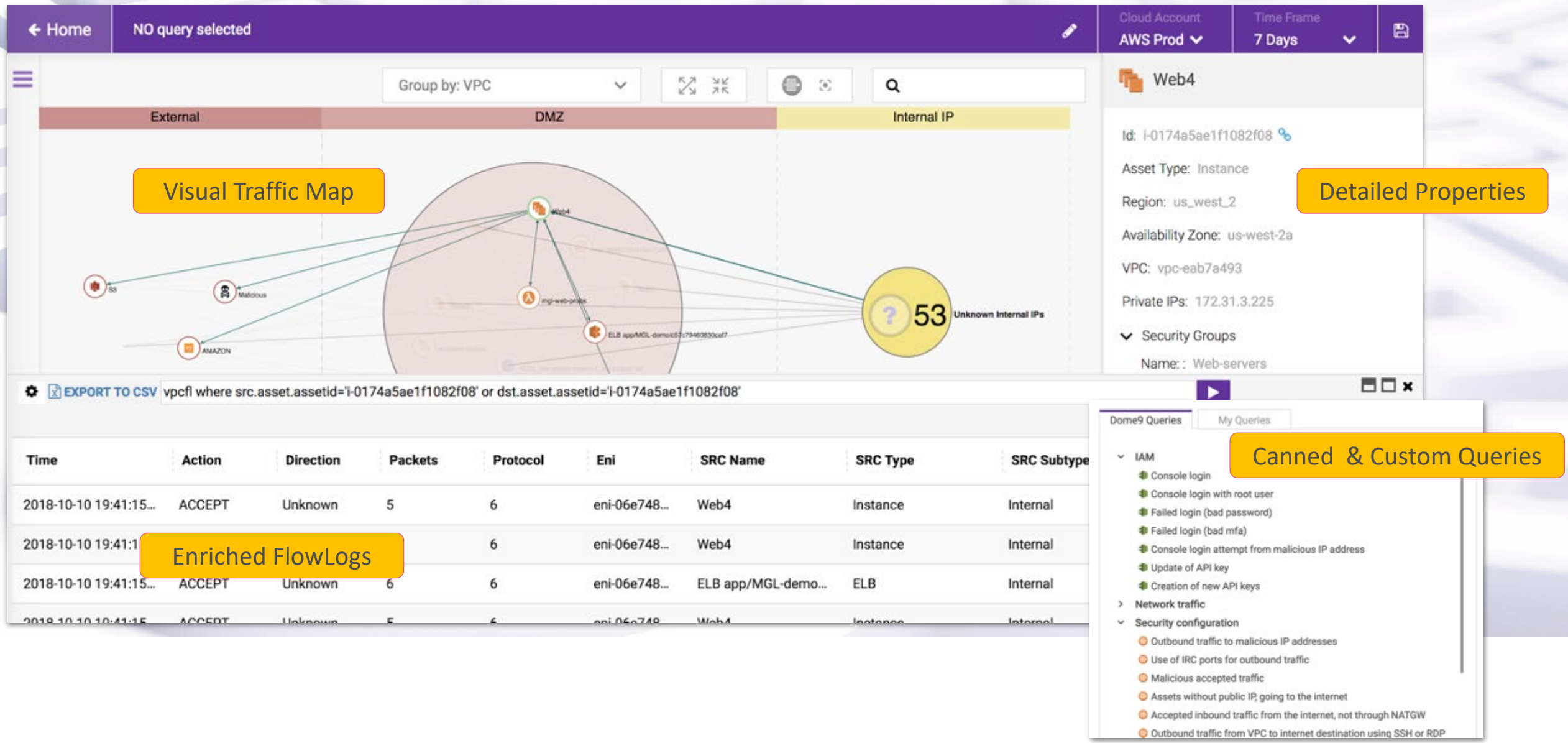
- Thousands of security checks
- Multiple compliance standards like PCI DSS, CIS Benchmarks, ISO, NIST, FedRAMP, and more
- Continuous Compliance granular assessments
- Compliance posture history
- Extensive entity and service coverage on AWS, Azure, GCP
- Printable reports

4. Advanced Threat Prevention

Analyzing Cloud Traffic Is Hard



2	170870580655	eni-6d24f24s	172.31.200.49	178.137.77.242	80	57349	6	25	1843	1496397675	1476697715	ACCEPT OK
2	170470580655	eni-6d14f24s	172.31.202.49	178.137.77.342	80	57319	6	25	1843	1476397675	1476627715	ACCEPT OK
2	170170560655	eni-6d14f24c	172.31.204.49	178.137.77.142	80	57119	6	25	1543	1276397675	1471627715	ACCEPT OK
2	170170560655	eni-6d12f24c	172.31.211.49	178.137.77.172	80	57219	6	25	1573	1276397675	1471627415	ACCEPT OK
2	270870580655	eni-6d25f24c	172.31.100.49	178.137.87.242	80	57379	6	15	1843	1496697675	1496697715	ACCEPT OK
2	170170560655	eni-6d12f24c	172.31.211.49	178.137.77.172	80	57219	6	25	1573	1276397675	1471627415	ACCEPT OK
2	170170580655	eni-6d14f24c	172.31.204.49	178.137.77.142	80	57119	6	25	1543	1276397675	1471627715	ACCEPT OK
2	170470580655	eni-6d14f24s	172.31.202.49	178.137.77.342	80	57319	6	25	1843	1476397675	1476627715	ACCEPT OK
2	170870580655	eni-6d24f24s	172.31.200.49	178.137.77.242	80	57349	6	25	1843	1496397675	1476697715	ACCEPT OK
2	170470580655	eni-6d14f24s	172.31.202.49	178.137.77.342	80	57319	6	25	1843	1476397675	1476627715	REJECT OK
2	170170560655	eni-6d12f24c	172.31.211.49	178.137.77.172	80	57219	6	25	1573	1276397675	1471627415	ACCEPT OK
2	170170560655	eni-6d12f24c	172.31.211.49	178.137.77.172	80	57219	6	25	1573	1276397675	1471627415	ACCEPT OK
2	170470580655	eni-6d14f24s	172.31.202.49	178.137.77.342	80	57319	6	25	1843	1476397675	1476627715	ACCEPT OK
2	170870580655	eni-6d24f24s	172.31.200.49	178.137.77.242	80	57349	6	25	1843	1496397675	1476697715	REJECT OK
2	170470580655	eni-6d14f24s	172.31.202.49	178.137.77.342	80	57319	6	25	1843	1476397675	1476627715	ACCEPT OK
2	170170560655	eni-6d12f24c	172.31.211.49	178.137.77.172	80	57219	6	25	1573	1276397675	1471627415	ACCEPT OK
2	170170560655	eni-6d12f24c	172.31.211.49	178.137.77.172	80	57219	6	25	1573	1276397675	1471627415	ACCEPT OK

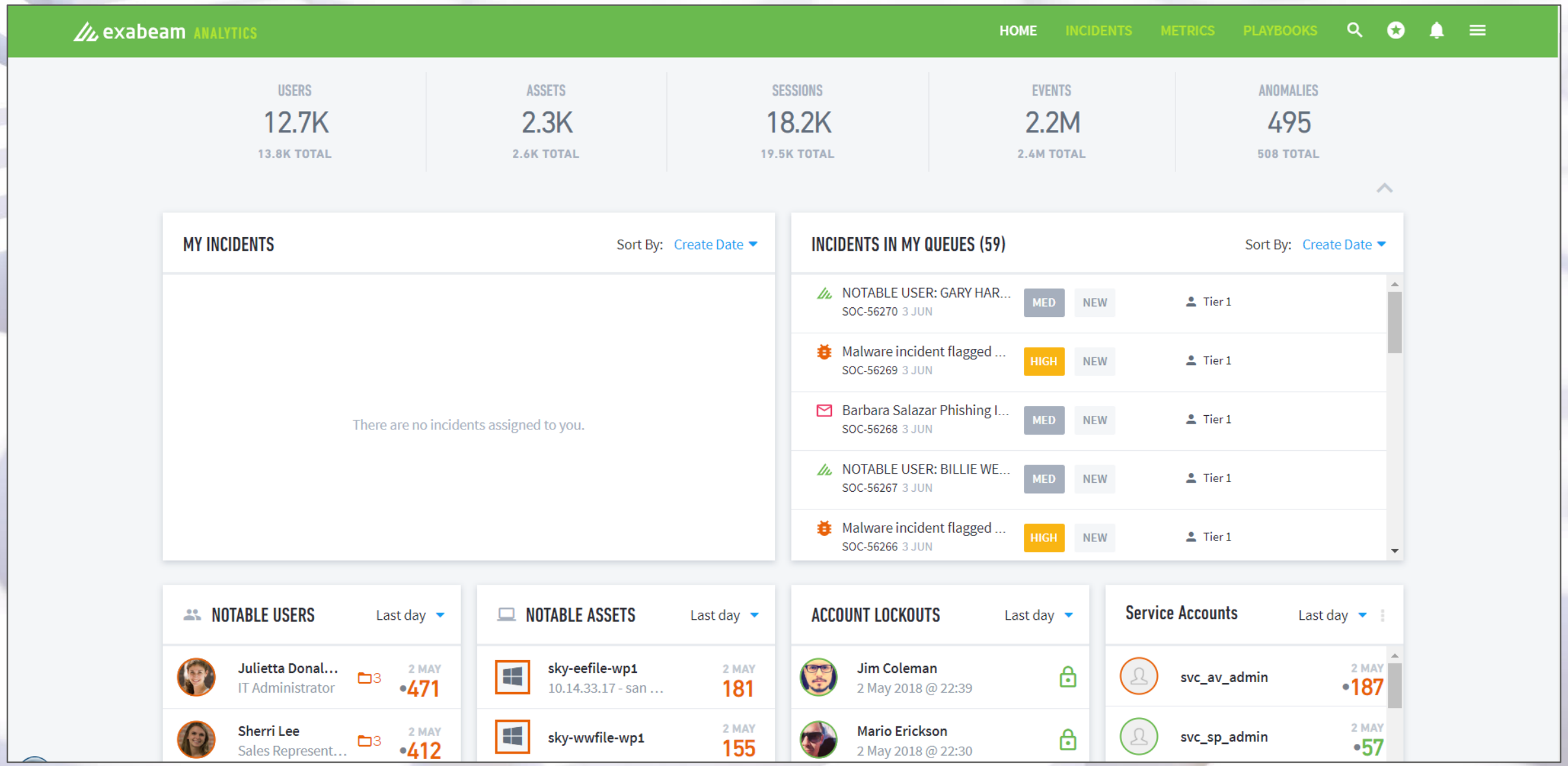

Home
NO query selected
Cloud Account
AWS Prod
Time Frame
7 Days
Group by: VPC
External
DMZ
Internal IP
Visual Traffic Map
53
Unknown Internal IPs
Web4
Id: i-0174a5ae1f1082f08
Asset Type: Instance
Region: us_west_2
Availability Zone: us-west-2a
VPC: vpc-eab7a493
Private IPs: 172.31.3.225
Security Groups
Name: : Web-servers
Detailed Properties
EXPORT TO CSV
vpcfl where src.asset.assetid='i-0174a5ae1f1082f08' or dst.asset.assetid='i-0174a5ae1f1082f08'
Time
Action
Direction
Packets
Protocol
Eni
SRC Name
SRC Type
SRC Subtype
2018-10-10 19:41:15...
ACCEPT
Unknown
5
6
eni-06e748...
Web4
Instance
Internal
2018-10-10 19:41:1
6
eni-06e748...
Web4
Instance
Internal
2018-10-10 19:41:15...
ACCEPT
Unknown
6
6
eni-06e748...
ELB app/MGL-demo...
ELB
Internal
Enriched FlowLogs
Dome9 Queries
My Queries
IAM
Console login
Console login with root user
Failed login (bad password)
Failed login (bad mfa)
Console login attempt from malicious IP address
Update of API key
Creation of new API keys
Network traffic
Security configuration
Outbound traffic to malicious IP addresses
Use of IRC ports for outbound traffic
Malicious accepted traffic
Assets without public IP, going to the internet
Accepted inbound traffic from the internet, not through NATGW
Outbound traffic from VPC to internet destination using SSH or RDP
Canned & Custom Queries

5. True Visibility of the Users

Focus on scalability of security resources & proactivity

Traditional SIEM	Nextgen SIEM/ UEBA: true visibility
Log tracking	User & entity tracking
Static (manual) correlation	Dynamic correlation (AI & ML based)
For on premise logs	For hybrid environment
Alert fatigue	High fidelity alerts
No integration Endpoint Protection Platform	integration Endpoint Protection Platform

Do you know what you don’t know?


exabeam ANALYTICS
HOME
INCIDENTS
METRICS
PLAYBOOKS
USERS
12.7K
13.8K TOTAL
ASSETS
2.3K
2.6K TOTAL
SESSIONS
18.2K
19.5K TOTAL
EVENTS
2.2M
2.4M TOTAL
ANOMALIES
495
508 TOTAL
MY INCIDENTS
Sort By: Create Date
There are no incidents assigned to you.
INCIDENTS IN MY QUEUES (59)
Sort By: Create Date
NOTABLE USER: GARY HAR...
SOC-56270 3 JUN
MED
NEW
Tier 1
Malware incident flagged ...
SOC-56269 3 JUN
HIGH
NEW
Tier 1
Barbara Salazar Phishing I...
SOC-56268 3 JUN
MED
NEW
Tier 1
NOTABLE USER: BILLIE WE...
SOC-56267 3 JUN
MED
NEW
Tier 1
Malware incident flagged ...
SOC-56266 3 JUN
HIGH
NEW
Tier 1
NOTABLE USERS
Last day
Julietta Donal...
IT Administrator
3
2 MAY
471
Sherri Lee
Sales Represent...
3
2 MAY
412
NOTABLE ASSETS
Last day
sky-eefile-wp1
10.14.33.17 - san ...
2 MAY
181
sky-wwfile-wp1
2 MAY
155
ACCOUNT LOCKOUTS
Last day
Jim Coleman
2 May 2018 @ 22:39
Mario Erickson
2 May 2018 @ 22:30
Service Accounts
Last day
svc_av_admin
2 MAY
187
svc_sp_admin
2 MAY
57

Security Services for the Cloud

1. Cloud Security Design
Best practices for setting up cloud firewalls, load balancers, WAF, …

2. Cloud Security CheckUp
Do I miss extra features?

3. Cloud Security Assessment
Is my cloud security well implemented?

4. Implementation and Configuration
Help of a cloud security specialist.

5. Managed Cloud Security MCS/MSS
Lets us do the job.

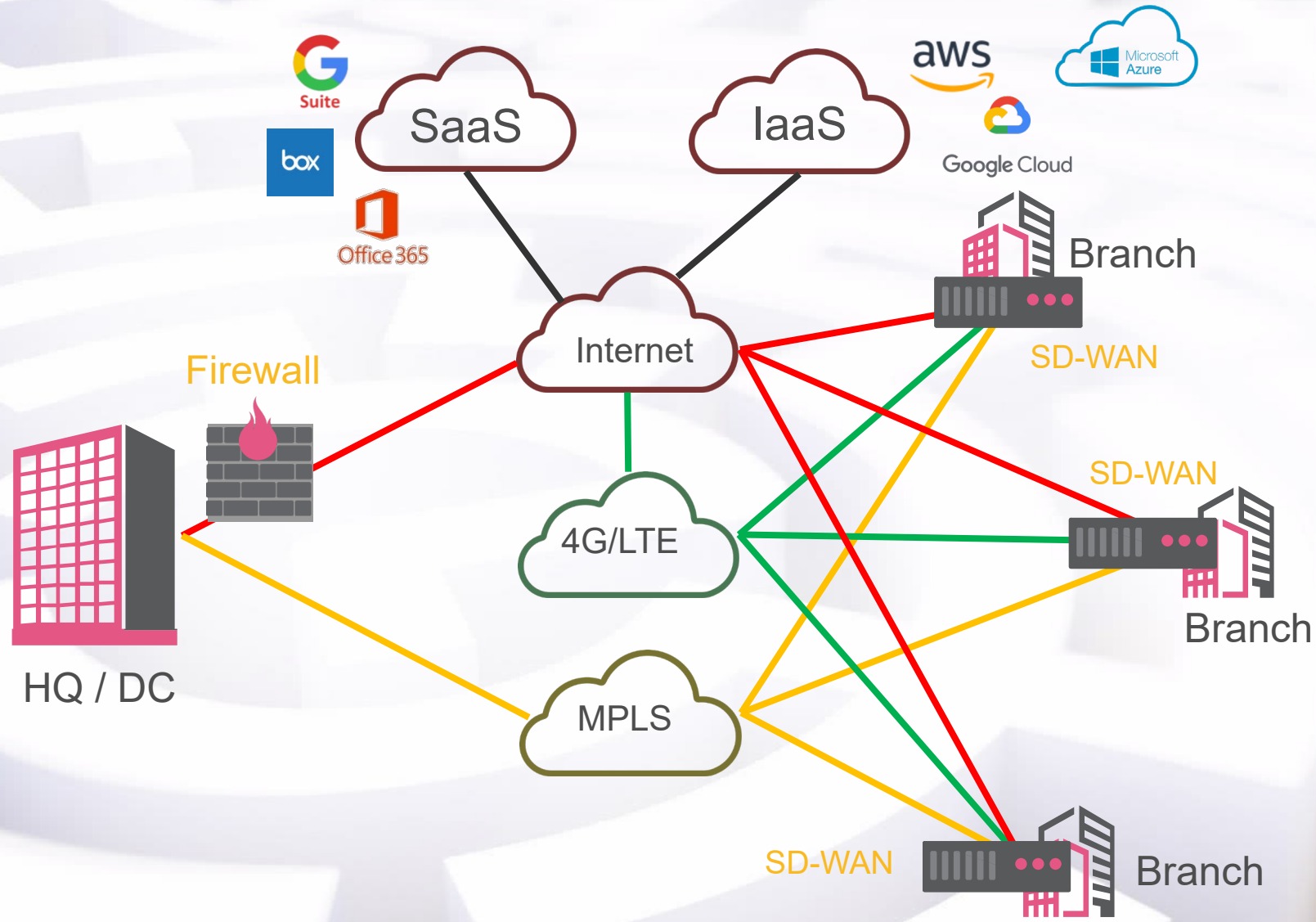
6. Cloud Threat Monitoring
Advanced reporting and user behaver analytics

Secure Connectivity for the Cloud

Infrastructure Challenges

1. Telenet FWaaS
2. Telenet CloudExpress

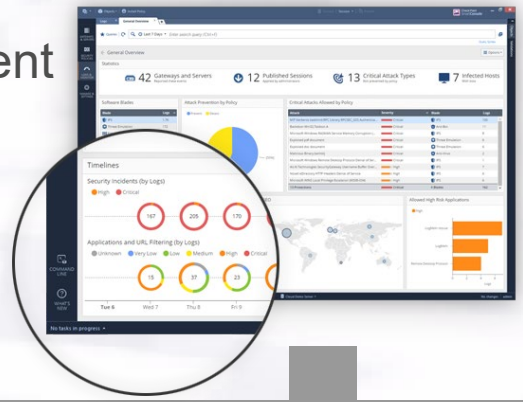
1. Telenet FWaaS



Applications:

- VoIP
- Data
- Backup

Central Management Platform



SaaS

IaaS

HQ / DC

Telenet FWaaS

SD-WAN

Branch

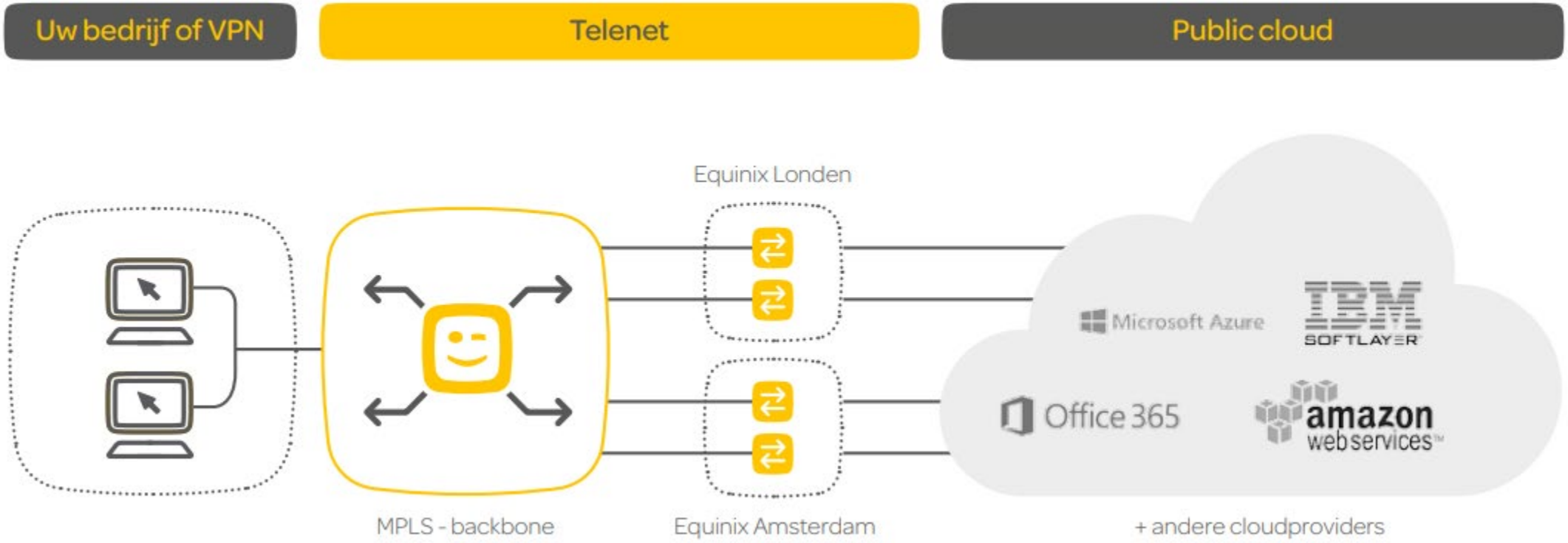
Branch Gateway

SD-WAN

Branch

2. Telenet CloudExpress

YOUR PRIVATE DATA CONNECTION TO THE PUBLIC CLOUD



CloudXpresS in a Nutshell

A direct connection to the public cloud: private, safe, reliable and flexible to fit your needs

Network

From an E-LINE or IP-VPN via the Telenet / LG MPLS backbone to the Equinix data centers in London and Amsterdam (Frankfurt will soon be added)

Provider

Already operational:

Microsoft Azure

amazon web services

Future extensions:

Google Cloud

ORACLE Cloud

SOFTLAYER an IBM Company

Speeds

50 Mbit/s – 100 Mbit/s – 200 Mbit/s – 500 Mbit/s – 1 Gbit/s – 10 Gbit/s

CloudExpress High Reliability

AVAILABILITY GUARANTEED BY SLA: 99,95%

- Fully redundant set-up
  - ✓ Several POPs: London, Amsterdam and soon also Frankfurt
  - ✓ All circuits from the data centers to the MPLS Core are type 7*
  - ✓ 2 separate connections per Equinix data center
  - ✓ Double equipment per data center
- Active-Passive setup
- Latency < 10 ms

* Redundancy of remote customer sites depends on the local connection to the MPLS backbone (local tail type)

Product Portfolio Overview

Check Point
SOFTWARE TECHNOLOGIES LTD

CHECK POINT
CloudGuard

paloalto
NETWORKS®

exabeam

Telenet FWaaS
Connected Security
CloudExpress


Thank you!
Business