Cloud Security 101

Kriti Mohun

Security Engineer | Check Point Software Technologies

https://uk.linkedin.com/in/kritim

https://open-security-summit.org/

Agenda

- Cloud Security Mindset
- What lives in the Cloud ?
- Cloud deployment models
- The limitless possibilities of cloud services
- Cloud attacks examples
- Overall Cloud Security Posture
- Assets safeguarding in the cloud
- Demo & Hands-on Labs of Check Point Dome9 – cloud visibility and regulatory compliance

Include learning objectives from this session

- **Adapting to cloud security mindset**
- **Real world problems / challenges with cloud security**
- **Your position in cloud security**
- **Asset Management, Identity safety, regulatory compliance in multi cloud environment**
- **Cloud Security using Check Point Dome9**

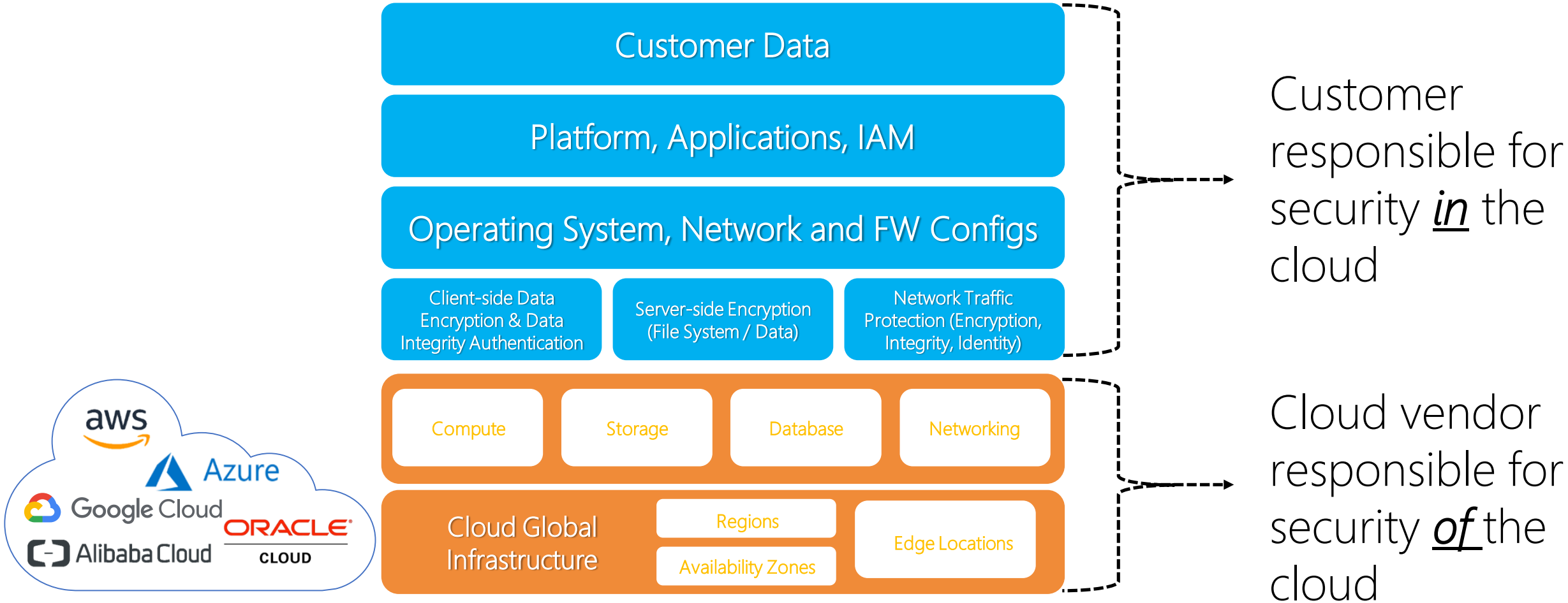
Key: How many points of entry, back doors are being opened ?

What’s in it ?

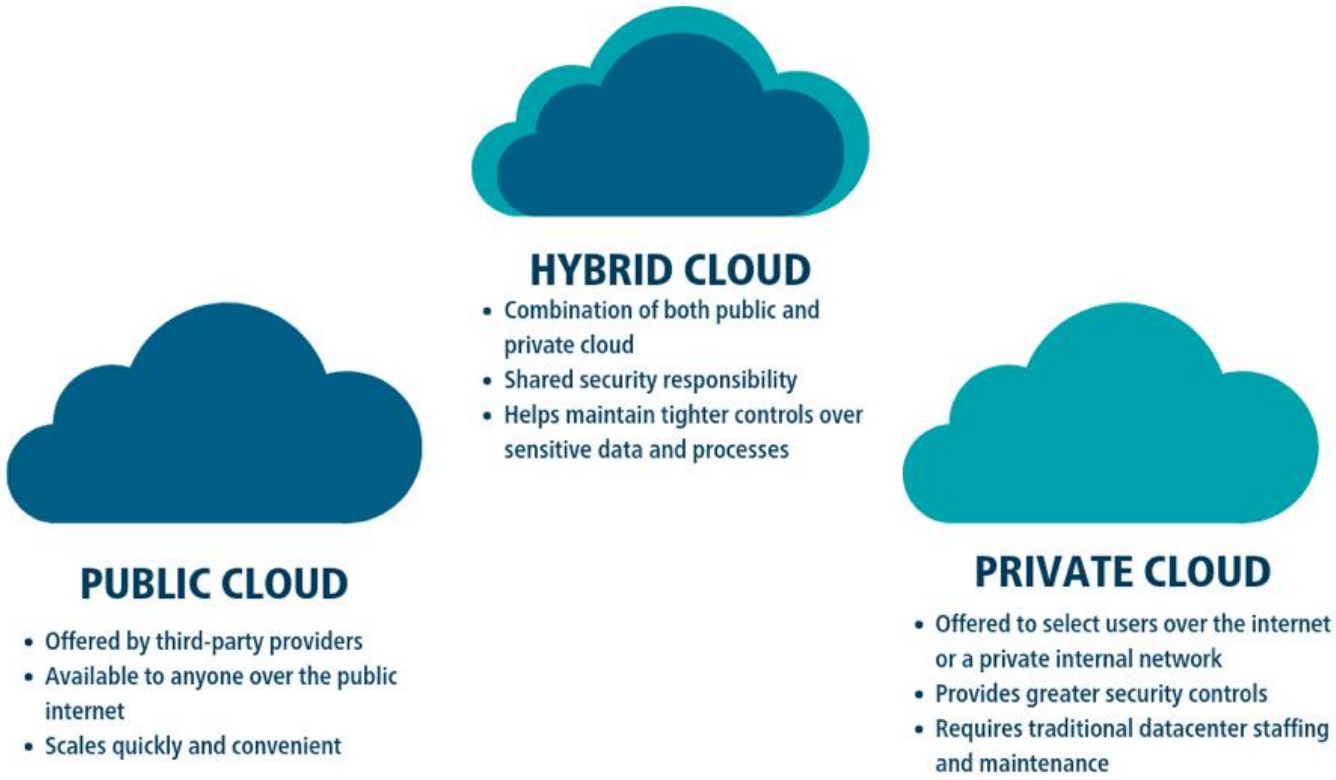
- **Protect your data, protect your assets**
- Infrastructure is shared – trend of using multi cloud platforms
- Different service cloud model requires different Cloud security approach
- Ever expanding cloud services in different environments
- Freedom to manage cloud/cloud segments/different platforms
- DevOps, BI, IoT solution hosting

Agile | Elastic | Cheap | Resilience | Ease of Deployment

CLOUD = SHARED RESPONSIBILITY



Types of Cloud Deployment Model



PUBLIC CLOUD

- Offered by third-party providers
- Available to anyone over the public internet
- Scales quickly and convenient

HYBRID CLOUD

- Combination of both public and private cloud
- Shared security responsibility
- Helps maintain tighter controls over sensitive data and processes

PRIVATE CLOUD

- Offered to select users over the internet or a private internal network
- Provides greater security controls
- Requires traditional datacenter staffing and maintenance

Public Cloud Vendors

amazon web services EC2
Microsoft Azure
heroku
Google Cloud Platform
AWS RDS
Alibaba Cloud

Private Cloud Vendors

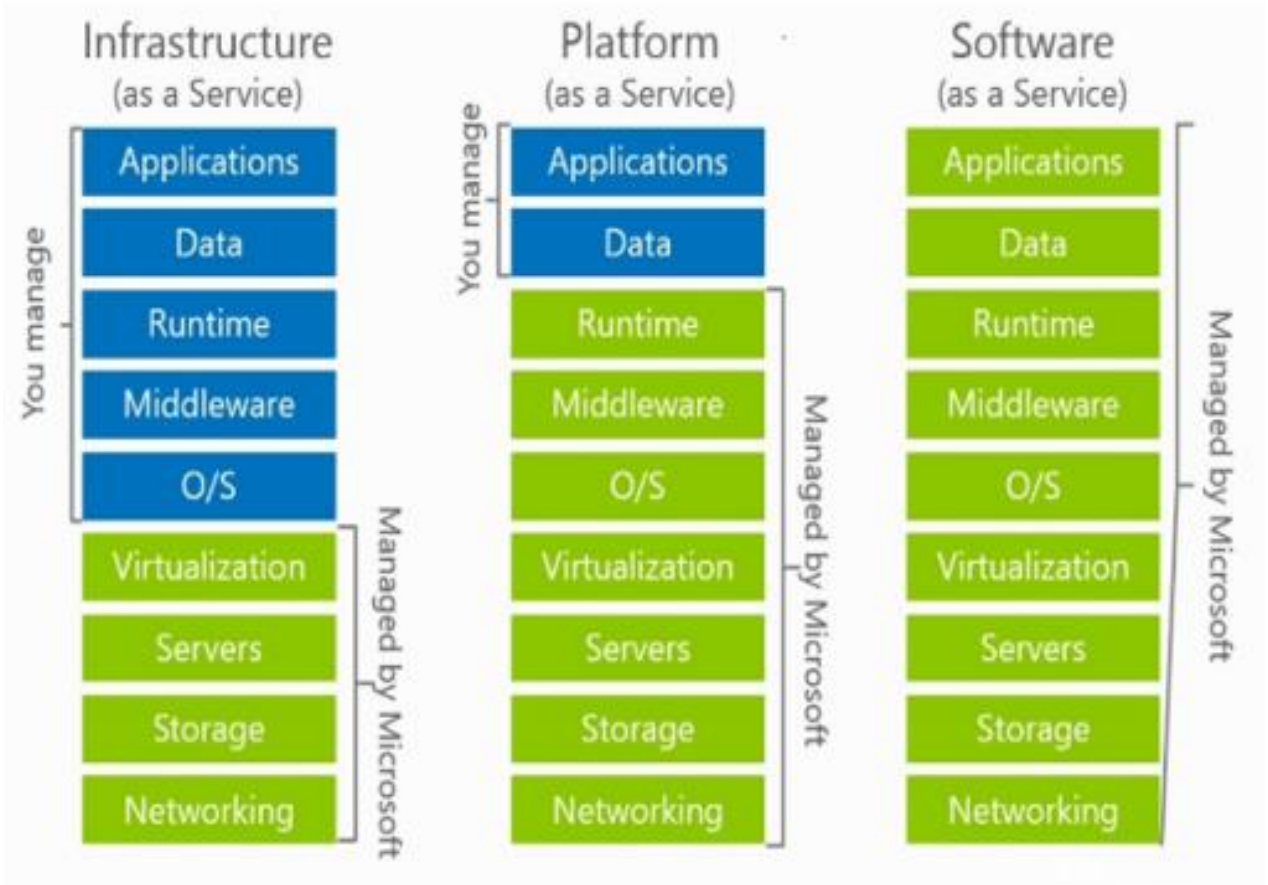
hp
NetIQ
ubuntu
ORACLE
amazon web services
Amazon VPC
CISCO
GOGRID
SUSE
openstack
apachecloudstack
DELL
Microsoft
rackspace
CITRIX
vmware
Eucalyptus
nebula

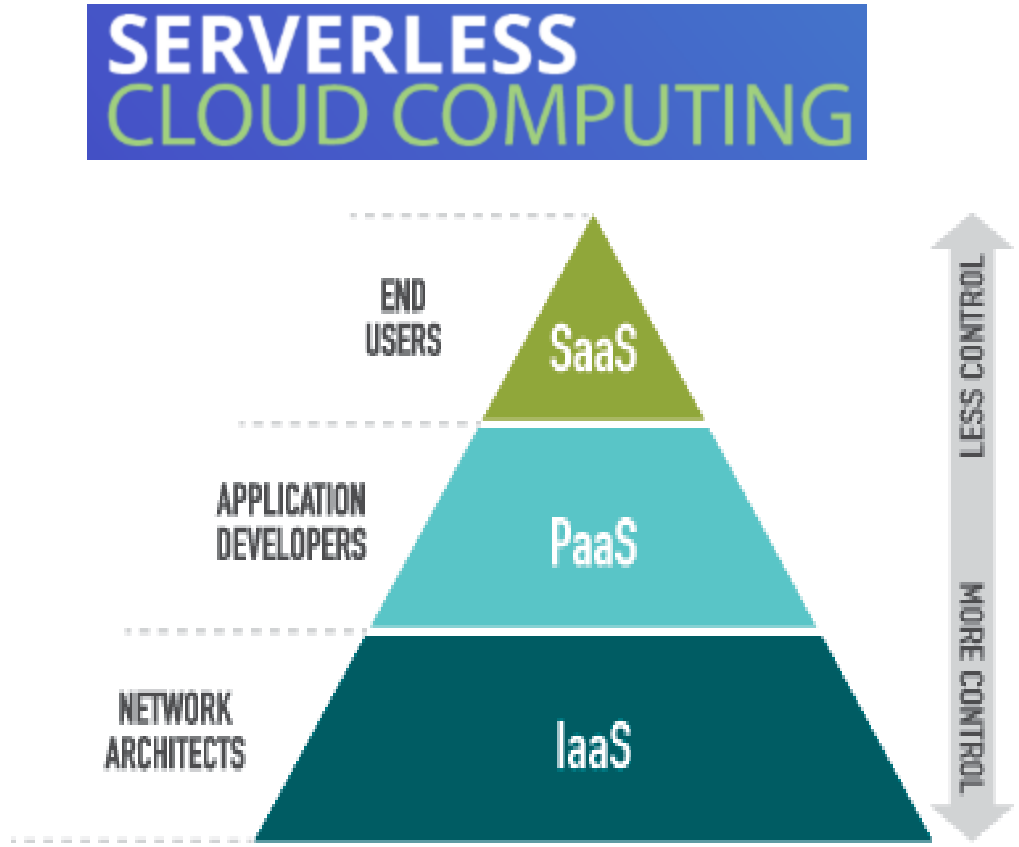
Difference between Private and Public Cloud

Differences: Private Cloud vs Public Cloud

PRIVATE CLOUD	PUBLIC CLOUD
Single client	Multiple clients
On-premises or off-premises	Off-premises
Capital cost to set up and maintain	No capital cost
High IT overhead	Low IT overhead
Fully customizable	Limited customizations
Fully private network	Shared network
Possible under utilization	Scalable with demand

Types of Cloud Service Models





kubernetes

docker

OPEN SECURITY SUMMIT

SaaS

Office 365 slack zendesk salesforce Acquia G Suite SUGARCRM

FaaS

CLOUD FUNCTIONS fn APACHE OpenWhisk™

DaaS

Cloud Datastore CouchDB relax DynamoDB Microsoft SQL Azure cassandra ORACLE DATA CLOUD Cockroach DB

PaaS

Microsoft Azure salesforce platform OpenPaaS Suite OPENSHIFT origin App Engine aws CLOUD FOUNDRY

STaaS

OneDrive ZADARA STORAGE ownCloud Google Drive amazon web services S3 Dropbox iCloud Google Cloud Storage cozy.io

IaaS

amazon web services EC2 Google Compute Engine rackspace the #1 managed cloud company SOFTLAYER an IBM Company openstack. apachecloudstack

Are cloud services easier to hack ?

OPEN SECURITY SUMMIT

Cloud Attacks

Phishing / Spear Phishing

Web API attacks

Supply Chain attacks (Watering hole)

Man-In-The-Cloud

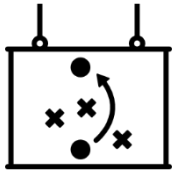
Cloud Malware injection Campaigns

Advanced persistent threats (APTs)

Denial of service attacks

- **Accessibility to cloud platform**
  - **- Log from anywhere via web browser**
  - **- Multi user access**
  - **- lack of Identity Access Management**
  - **- Root account credentials access**
- **Misconfiguration**
- **Unencrypted storage / DBs**
- **Visibility – Lack of Asset management**
- **Insecure interfaces and APIs**
- **Security compliance**

THIS MIGHT EXPOSE YOU TO…



Lateral threat movements

Data breach due to misconfiguration

Abuse of cloud services

API hacking

Malicious insiders

The Big Question ?

Cloud Security Architect

Cloud Security Engineer

Cloud Software Engineer

DevOps

Cloud System Administrator

Cloud Product Manager

Cloud Consultant

CISO

CIO

Trusted Cloud

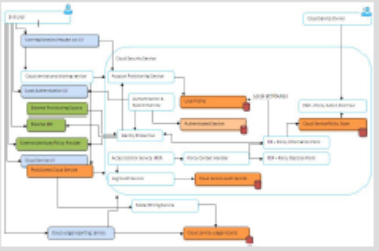
Reference Architecture

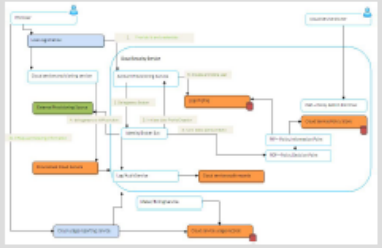
Version 1.1

Guiding Principles

- Define protections that enable trust in the cloud.
- Develop cross-platform capabilities and patterns for proprietary and open-source providers.
- Will facilitate trusted and efficient access, administration and resiliency to the customer/consumer.
- Provide direction to secure information that is protected by regulations.
- The Architecture must facilitate proper and efficient identification, authentication, authorization, administration and auditability.
- Centralize security policy, maintenance operation and oversight functions.
- Access to information must be secure yet still easy to obtain.
- Delegate or Federate access control where appropriate.
- Must be easy to adopt and consume, supporting the design of security patterns
- The Architecture must be elastic, flexible and resilient supporting multi-tenant, multi-landlord platforms
- The architecture must address and support multiple levels of protection, including network, operating system, and application security needs.

High Level Use Cases





Domain

Container

Process or Solution

Data

SABSA

ITIL v3

TOGAF

JERICHO

Business Operation Support Services (BOSS)

Compliance

Audit Planning

Independent Audits | Third-Party Audits | Internal Audits

Contact/Authority Maintenance

Information System Regulatory Mapping

Intellectual Property Protection

Data Governance

Data Ownership / Stewardship | Data Classification | Handling / Labeling / Security Policy

Secure Disposal of Data | Clear Desk Policy | Rules for Information Leakage Prevention

Rules for Data Retention

Operational Risk Management

Operational Risk Committee

Crisis Management | Business Impact Analysis

Key Risk Indicators

Business Continuity

Planning | Testing

Risk Management Framework

Business Assessment | Technical Assessment

Independent Risk Management

Human Resources Security

Employee Termination | Employment Agreements

Background Screening | Job Descriptions

Roles and Responsibilities | Employee Awareness

Employee Code of Conduct

Security Monitoring Services

SIEM Platform | Event Mining | Database Monitoring | Application Monitoring | Honey Pot | End-Point Monitoring

Event Correlation | Cloud Monitoring | E-Mail Journaling | Market Threat Intelligence | Counter Threat Management

SOC Portal

Managed Security Services | Knowledge Base | Branding Protection | Anti-Phishing

Real-time internetwork defense (SCAP) | User Behavior & Profile Patterns

Legal Services

Contracts | E-Discovery

Incident Response Legal Preparation

Internal Investigations

Forensic Analysis | e-Mail Journaling

Information Technology Operation & Support (ITOS)

IT Operation

DRP: Plan Management | Test Management

IT Governance: Architecture Governance | Standards and Guidelines

Resource Management: Segregation of Duties | Contractors

PMO: Program Mgmnt | Project Mgmnt | Remediation

Portfolio Management: Maturity Model | Roadmap | Strategy Alignment

Service Delivery

Service Level Management: Objectives | Internal SLAs | OLAs | External SLAs | Vendor Management | Service Dashboard

Information Technology Resiliency: Availability Management | Resiliency Analysis | Capacity Planning

Asset Management: Service Costing | Operational Budgeting | Charge Back | Investment Budgeting

Application Performance Monitoring

Service Support

Configuration Management: Capacity Planning | Software Management | Physical Inventory | Automated Asset Discovery | Configuration Management

Incident Management: Security Incident Response | Automated Ticketing | Self-Service | Ticketing | Cross Cloud Security Incident Response

Problem Management: Event Classification | Root Cause Analysis | Trend Analysis | Problem Resolution | Orphan Incident Management

Knowledge Management: Best practices | Trend Analysis | Benchmarking | Security Job Aids | Security FAQ

Change Management: Service Provisioning | Approval Workflow | Change Review Board | Planned Changes | Project Changes | Operational Changes | Emergency Changes

Release Management: Scheduling | Testing | Version Control | Build | Source Code Management

Presentation Services

Presentation Modality

Consumer Service Platform: Social Media | Collaboration | Search | E-Mail | e-Readers

Enterprise Service Platform: B2E | B2M | B2B | B2C | P2P

Presentation Platform

End-Points: Mobile Devices | Mobile Device Management | Portable Devices | Fixed Devices

Desktops: Company owned | Third-Party | Public Kiosk

Medical Devices | Smart Appliances

Speech Recognition (IVR) | Handwriting (ICR)

Application Services

Programming Interfaces: Input Validation

Security Knowledge Lifecycle: Security Design Patterns | Attack Patterns | Code Samples | Security Application Framework - ACEGI

Integration Middleware

Development Process

Self-Service: Security Code Review | Application Vulnerability Scanning | Stress and Volume Testing

Software Quality Assurance

Connectivity & Delivery

Abstraction

Information Services

Service Delivery: Service Catalog | SLAs | OLAs | Contracts | Recovery Plans

Reporting Services: Dashboard | Data Mining | Reporting Tools | Business Intelligence

ITOS: PMO | Strategy | Roadmap | Problem Management | Incident Management | CMDB | Knowledge Management | Service Management | Change Management

BOSS: Risk Assessments | Data Classification | Process Ownership | Audit Findings | HR Data (Employees & Contractors) | Business Strategy

Data Governance: Risk Assessments | Non-Production Data | Information Leakage Detection | Data Segregation

Security Monitoring: Session Events | Authorization Events | Authentication Events | Application Events | Network Events | Computer Events | HIPS | Database Events | NIPS Events | Transformation Services | Privilege Usage Events | ACLs | CRLs | Compliance Monitoring | NIPS Events | DLP Events | eDiscovery Events

Service Support: Configuration Rules (Metadata) | Service Events | Knowledge Repository | Configuration Management Database (CMDB) | Change Logs

Risk Management: GRC | RA | BIA | DR & BC Plans | VRA | TVM

User Directory Services: Active Directory Services | LDAP Repositories | X.500 Repositories | DBMS Repositories | Meta Directory Services | Registry Services | Location Services | Federated Services | Virtual Directory Services

Infrastructure Services

Internal Infrastructure

Facility Security: Controlled Physical Access: Barriers | Electronic Surveillance | Security Patrols | Physical Authentication

Asset Handling: Data | Hardware | Software

Environmental Risk Management: Physical Security | Equipment Location | Power Redundancy

Storage Services

Network Services: Network Segmentation | Authoritative Time Source

Patch Management: Compliance Monitoring | Service Discovery

Equipment Maintenance

Availability Services

Servers: Secure Build | Image Management

Virtual Infrastructure

Desktop "Client" Virtualization: Local | Remote | Session-Based | VM-Based (VDI)

Storage Virtualization: Block-Based Virtualization: Disk-Based | Network-Based | LDM | LVM | Storage Device-Based | Appliance | LUN | Switched | File-Based Virtualization

Application Virtualization: Client Application Streaming | Server Application Streaming | Virtual Workspaces

Server Virtualization: Virtual Machines (Hosted Based): Full | Paravirtualization | Hardware-Assisted | OS Virtualization | TPM Virtualization | Virtual Memory

Network: Network Address Space: IPv4 | IPv6 | External (VLAN) | Internal (NIC) | Database Virtualization | Mobile Device Virtualization | Smartcard Virtualization

Security and Risk Management

Governance Risk & Compliance

Compliance Management | Policy Management: Exceptions | Self Assessment

Vendor Management | Audit Management | IT Risk Management

Technical Awareness and Training

InfoSec Management

Capability Mapping

Risk Portfolio Management | Risk Dashboard

Residual Risk Management

Privilege Management Infrastructure

Identity Management: Domain Unique Identifier | Federated IDM | Identity Provisioning | Attribute Provisioning

Authentication Services: SAML Token | Risk Based Auth | Multifactor | OTP | Smart Card | Password Management | Biometrics | Network Authentication | Single Sign On | Middleware Authentication | WS-Security | Identity Verification | OTB AuthN

Authorization Services: Policy Enforcement | Policy Definition | Policy Management | Principal Data Management | Resource Data Management | XACML | Role Management | Obligation | Out of the Box (OTB) AuthZ

Privilege Usage Management: Keystroke/Session Logging | Password Vaulting | Privilege Usage Gateway | Resource Protection

Threat and Vulnerability Management

Compliance Testing: Databases | Servers | Network

Vulnerability Management: Application | Infrastructure | DB

Penetration Testing: Internal | External

Threat Management: Source Code Scanning | Risk Taxonomy

Infrastructure Protection Services

Server: White Listing | Anti-Virus | HIPS / HIDS | Host Firewall

End-Point: Anti-Virus, Anti-Spam, Anti-Malware | HIPS /HIDS | Host Firewall | Media Lockdown | Hardware Based Trusted Assets | Forensic Tools | Inventory Control | Content Filtering | White Listing

Network: Firewall | Content Filtering | DPI | NIPS / NIDS | Wireless Protection | Link Layer Network Security | Black Listing Filtering

Application: XML Appliances | Application Firewall | Real Time Filtering | Secure Messaging | Secure Collaboration

Data Protection

Data lifecycle management: Meta Data Control | Data De-Identification | Data Masking | Data Tagging | eSignature (Unstructured data) | Life cycle management | Data Obscuring | Data Seeding

Data Leakage Prevention: Data Discovery | Network (Data in Transit) | End-Point (Data in Use) | Server (Data at Rest)

Intellectual Property Prevention: Intellectual Property | Digital Rights Management

Cryptographic Services

Key Management: Symmetric Keys | Asymmetric Keys

PKI | Signature Services | Data-in-use Encryption (Memory)

Data-in-Transit Encryption (Transition, Flow) | Data-at-Rest Encryption (DB, File, SAN, Desktop, Mobile)

Policies and Standards

Operational Security Baselines | Job Aid Guidelines | Role Based Awareness

Information Security Policies | Technical Security Standards | Data/Asset Classification | Best Practices & Regulatory correlation

INNOVATION IS THE KEY TO SUCCESS

OPEN SECURITY SUMMIT

DevOps IS THE NEW BLACK

Developers:

- Freedom
- Agility

IT Operators :

- Control
- Efficiency

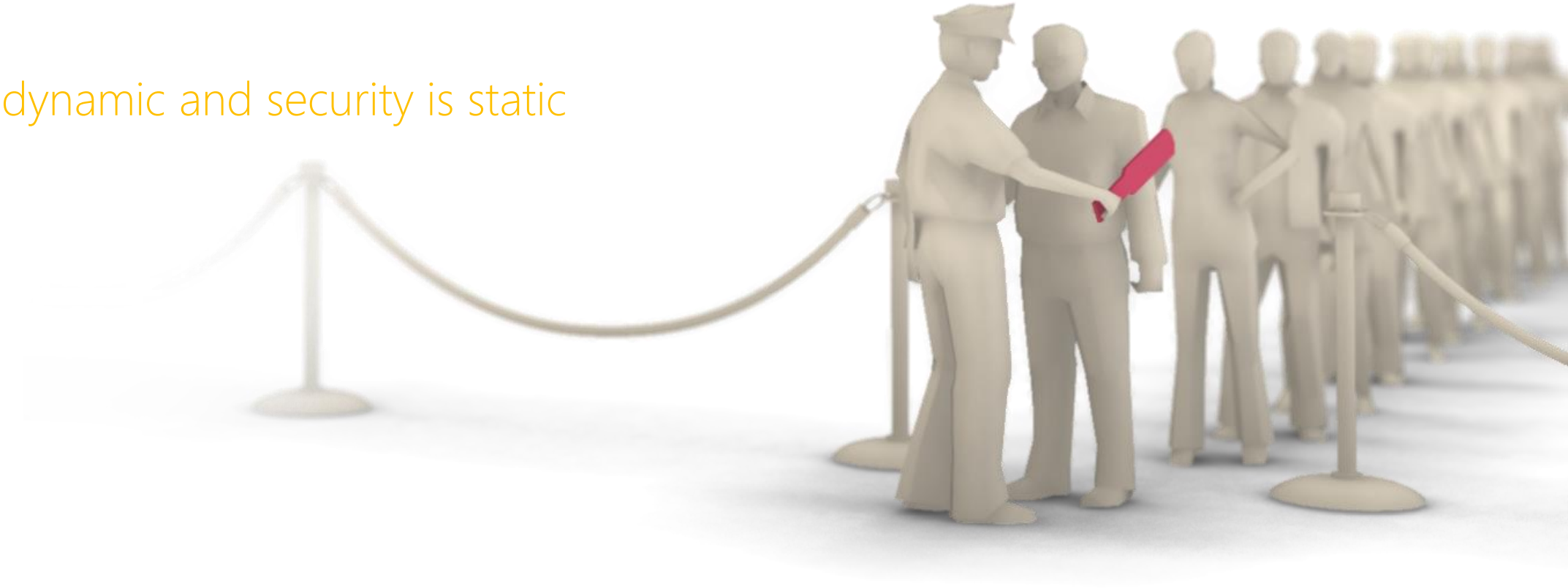
DevOps

Cloud Applications are no longer manually deployed or configured; they are **orchestrated**.

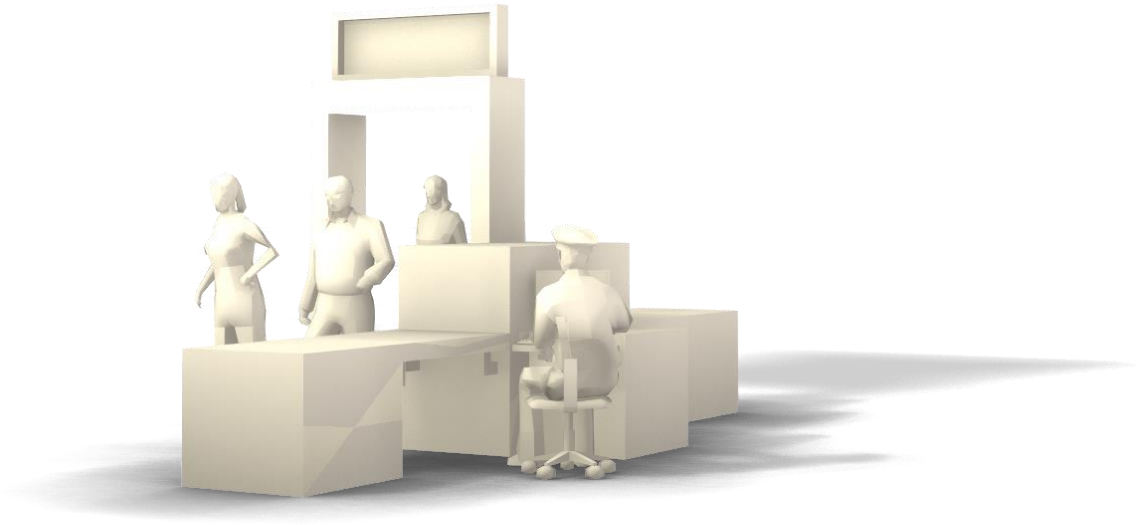
Why legacy security is hard to deploy in the cloud ?

OPEN SECURITY SUMMIT

- Hard to deploy security in the cloud
- Firewall tickets are bottleneck
- Cloud is dynamic and security is static



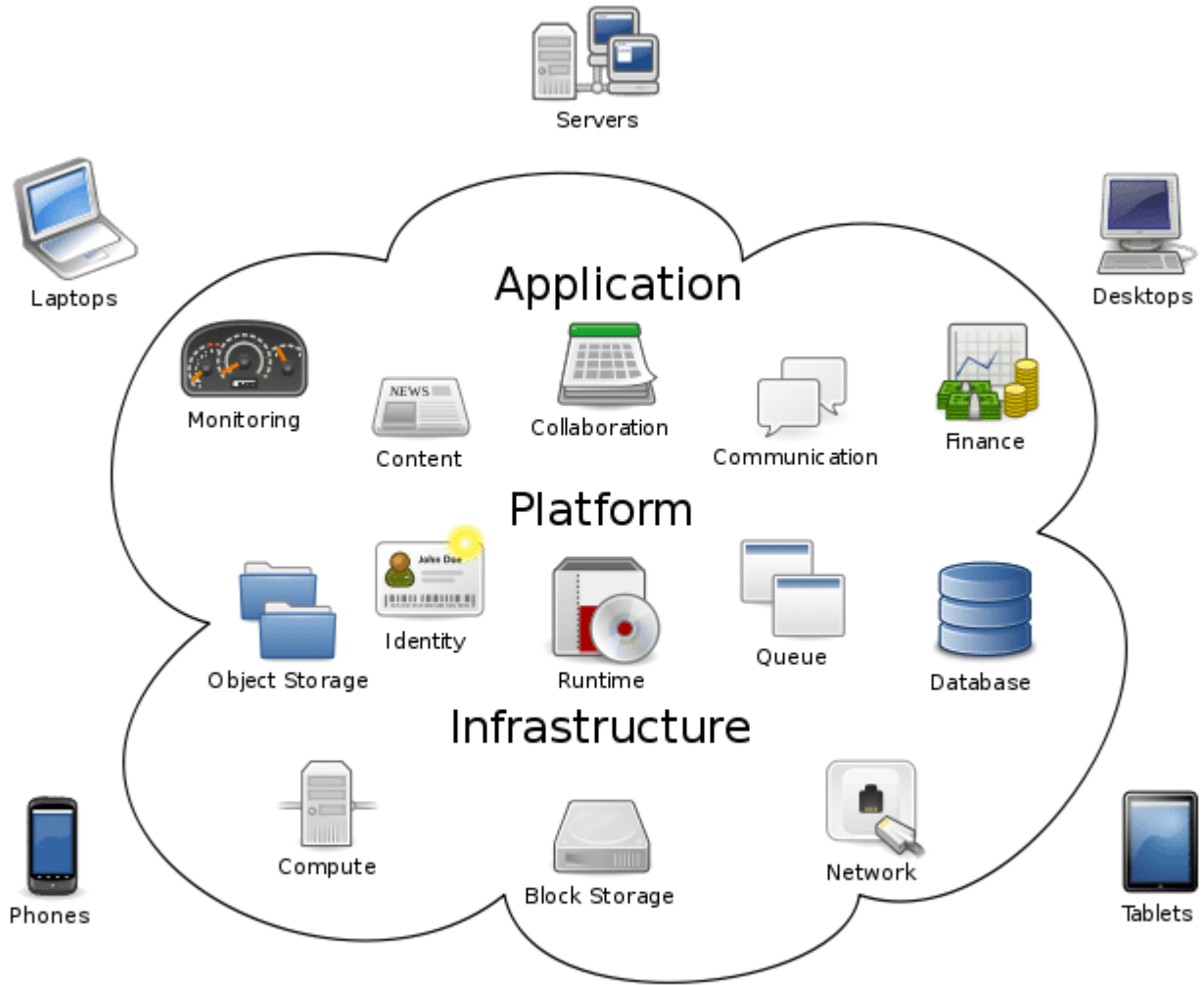
What's your cloud security needs ?



Security must be as agile as your cloud

.....and it must be effective!

NCSC Cloud security guidance:



- Data in transit protection
- Asset protection and resilience
- Separation between users
- Governance framework
- Operational security
- Personnel security
- Secure development
- Supply chain security
- Secure user management
- Identity and authentication
- External interface protection
- Secure service administration
- Audit information for users
- Secure use of the service

Cloud Service Provider assessment

Know your business requirements – availability, continuity are key

Understand Data flow, legal/regulatory implications of any data leak

Identify the risks the business is willing or unwilling to take

Verify the cloud service claims

Validate service supplier assurance claims

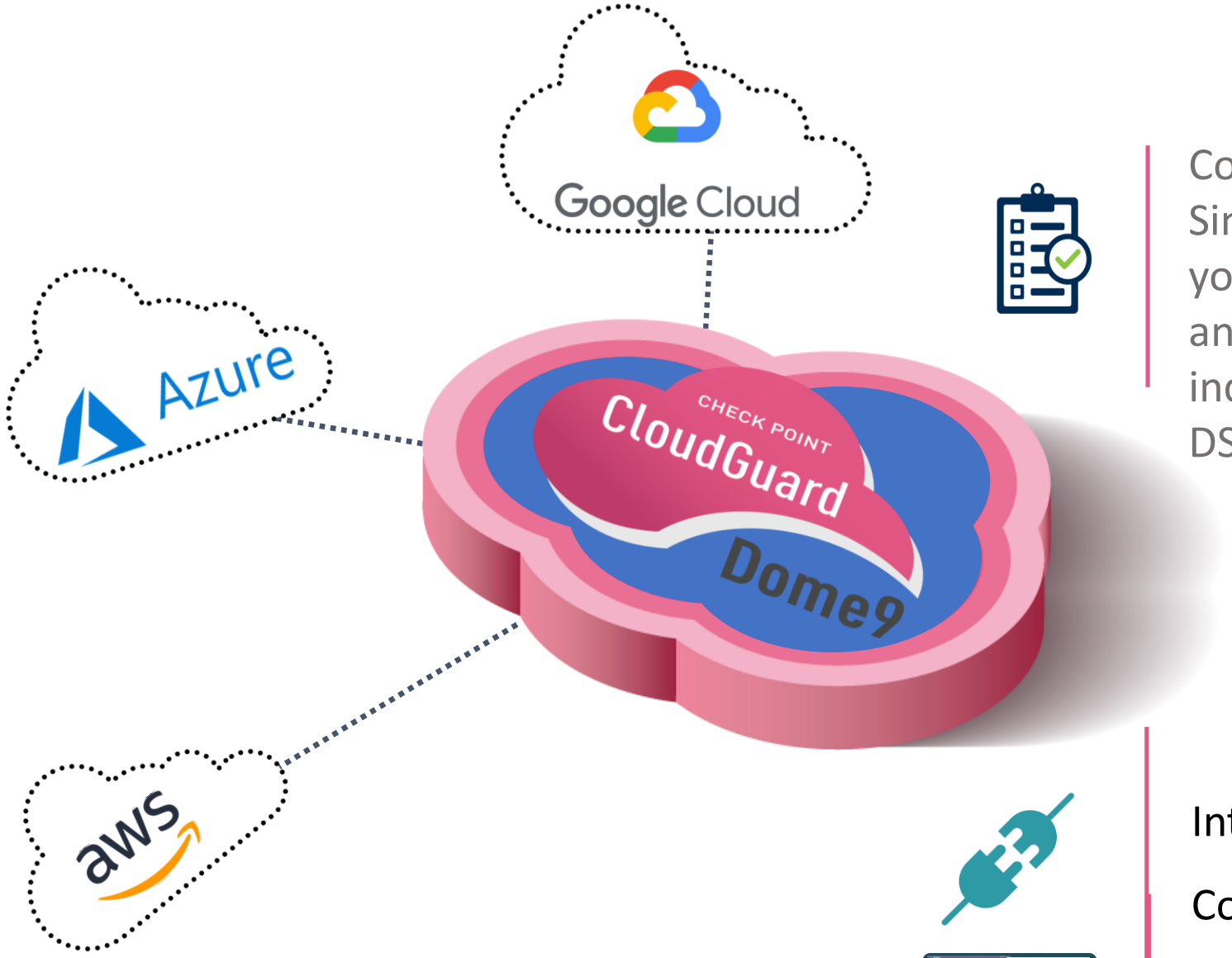
Identify additional risks/mitigations you can apply

Verify if acceptable risks are truly accepted by the business

Have regular service review with your cloud service provider

How to secure data/assets in cloud

- Visibility
- Understanding flow of traffic
- Control on who connects, and user/admin access
- Enforcing policies points
- Asset tagging, automatic enforcement of policies



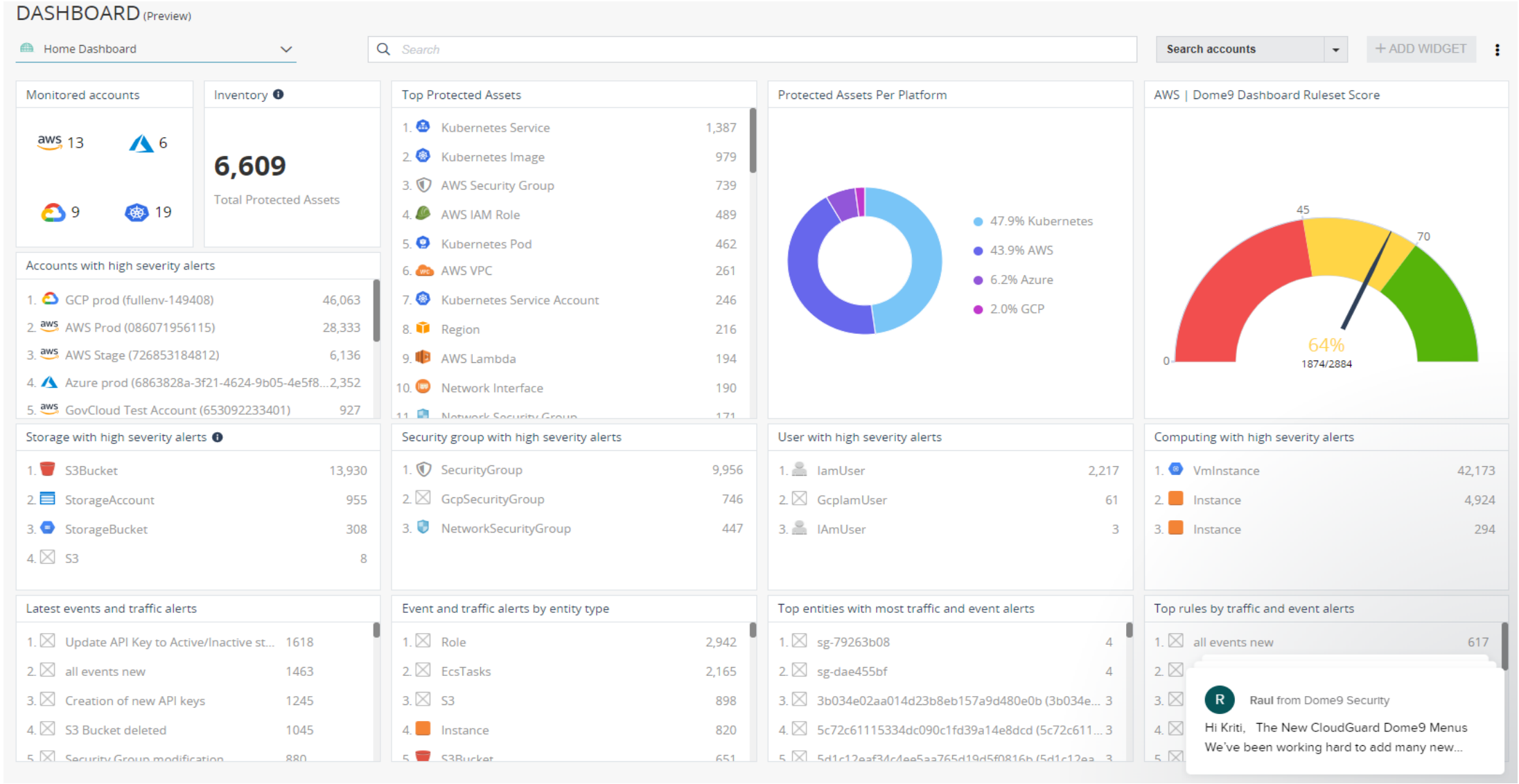
Continuous Compliance and Governance
Single click Compliance assessment of your public cloud to evaluate security and compliance with best practices and industry standards (Such as HIPAA, PCI-DSS and more)

Automated remediation

Integration of Security and Compliance into CI/CD pipeline

Single pane of glass/control plane across the entire cloud footprint

What is CloudGuard Dome9?



Cloudguard Dome9

- For the hands-on Check Point Dome9 Lab: Lab Guide https://shorturl.at/glpM3

- To launch the lab as a user you may visit the lab registration page: https://bit.ly/2TFgaBt

- For the activation code - please contact me/send me a message on Linkedin https://www.linkedin.com/in/kritim

Thank You

https://uk.linkedin.com/in/kritim