CYBERSECURITY

SESSION 4

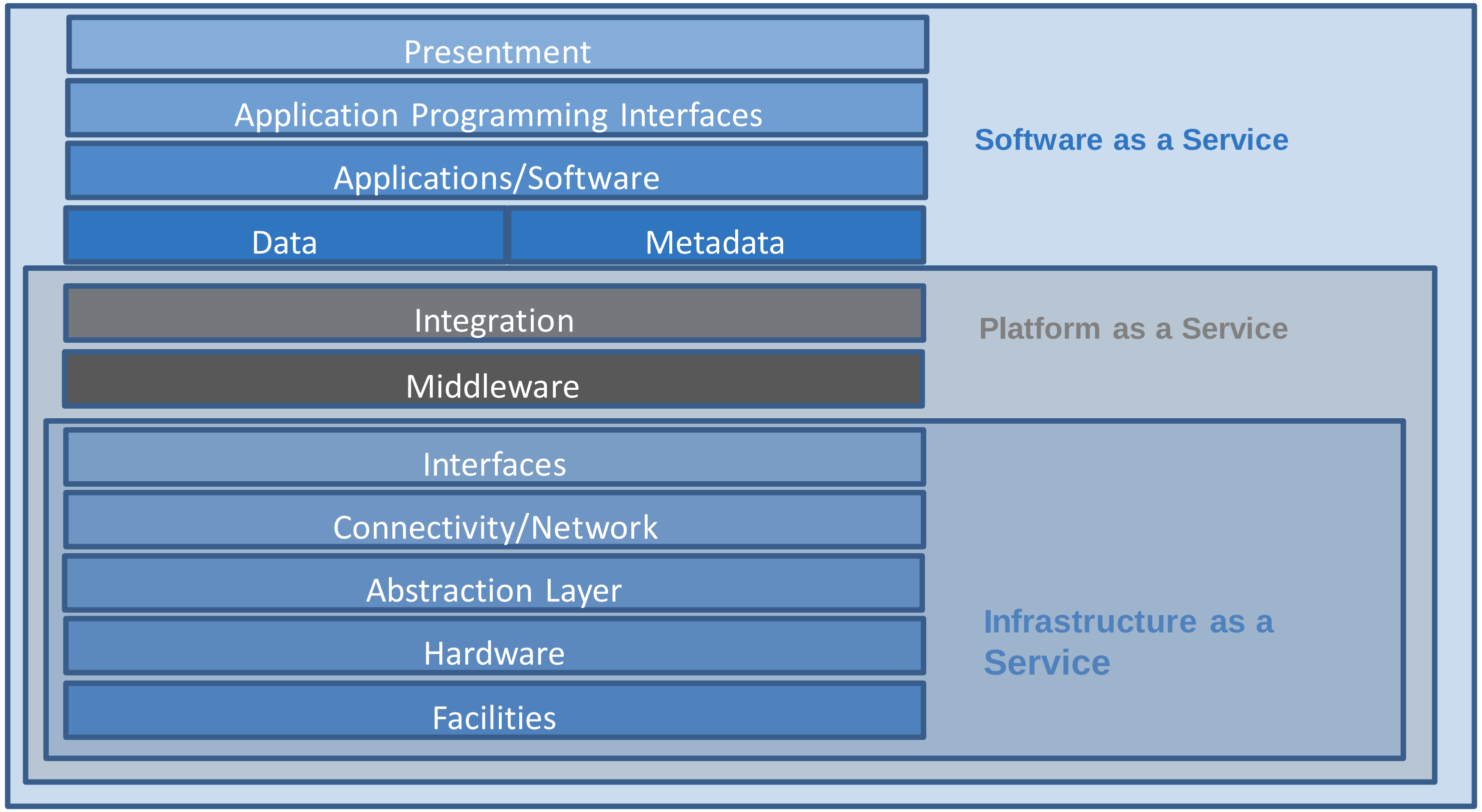
TEXAS SKILLS DEVELOPMENT FUND
TRAINING PARTNERSHIP

AUSTIN COMMUNITY COLLEGE DISTRICT

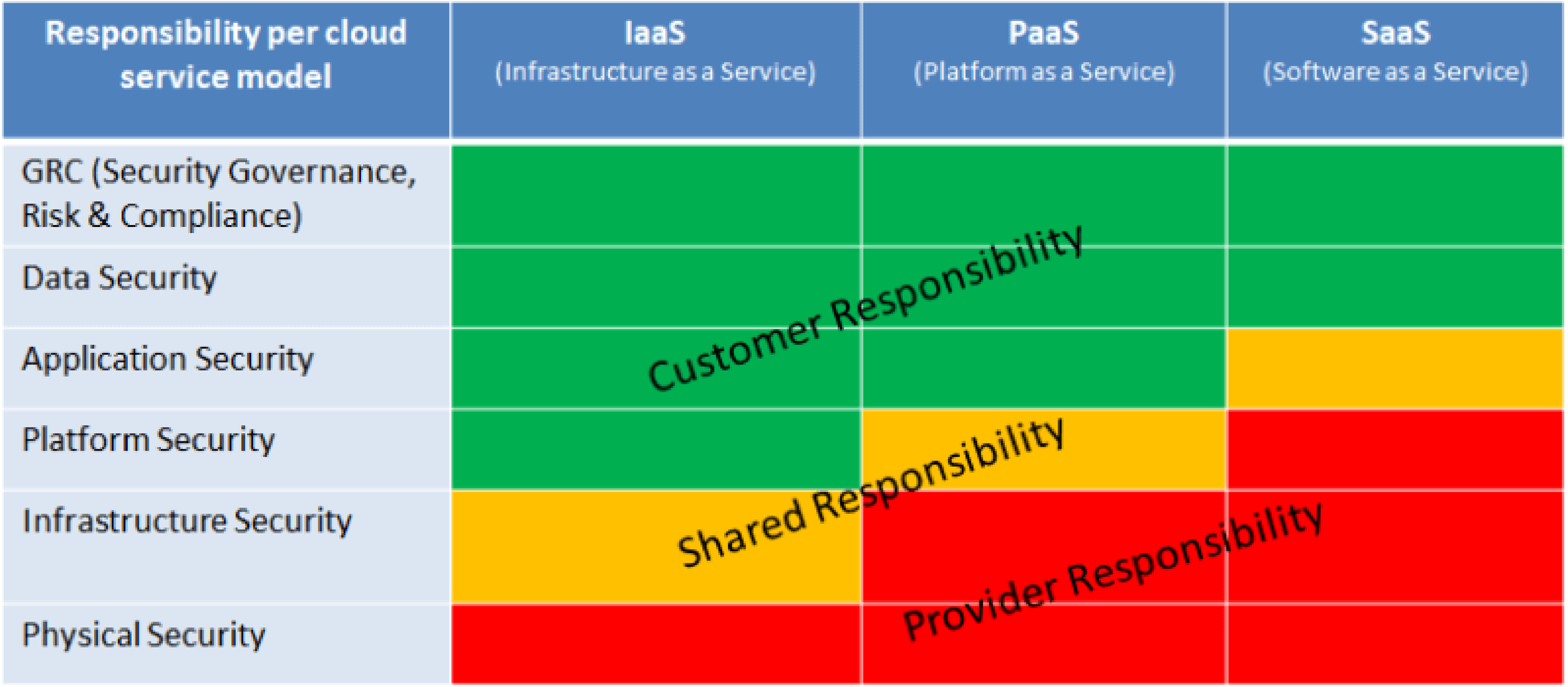
Cloud Security

Cloud Services Security

Cloud Service Models



Shared Responsibility Model

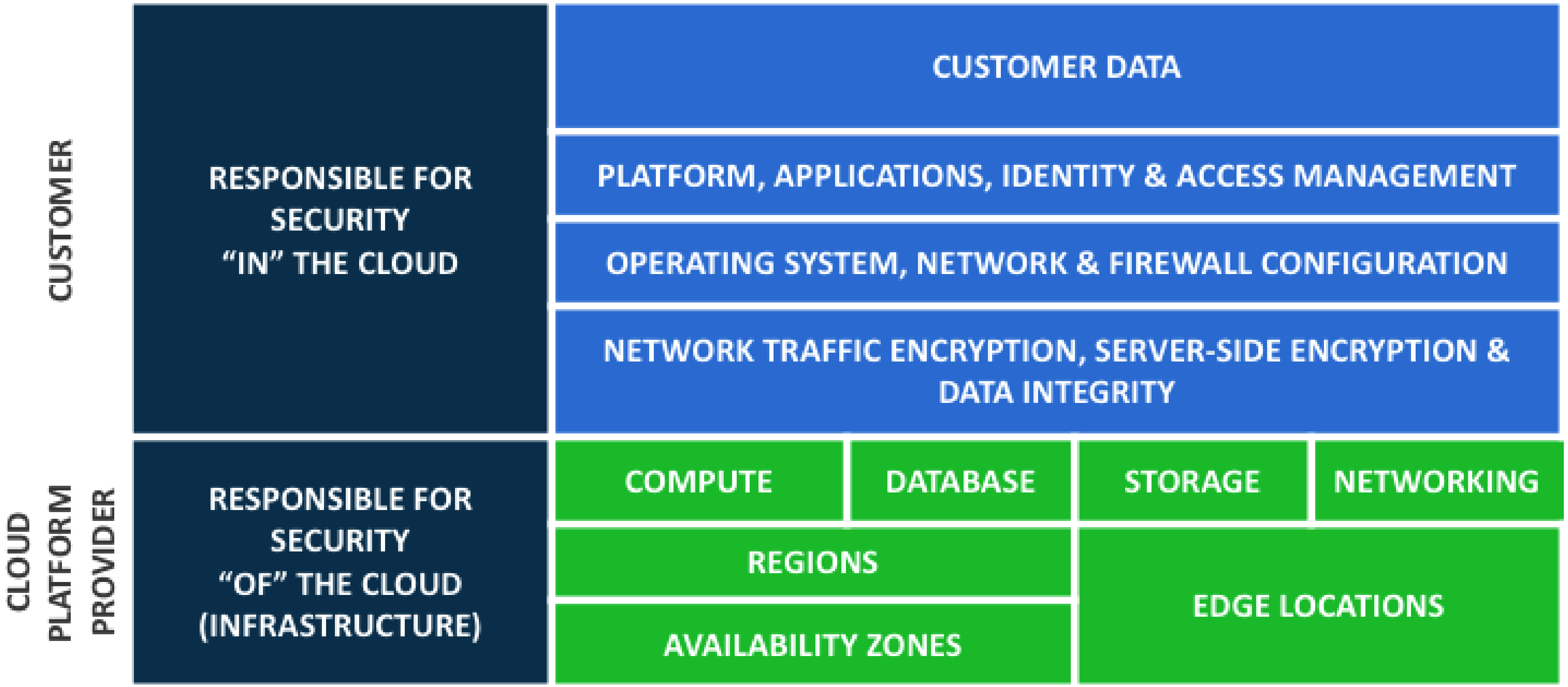


Responsibility per cloud service model	IaaS (Infrastructure as a Service)	PaaS (Platform as a Service)	SaaS (Software as a Service)
GRC (Security Governance, Risk & Compliance)	🟩	🟩	🟩
Data Security	🟩	🟩	🟩
Application Security	🟩	🟩	🟨
Platform Security	🟩	🟨	🟥
Infrastructure Security	🟨	🟥	🟥
Physical Security	🟥	🟥	🟥

Customer Responsibility
Shared Responsibility
Provider Responsibility

Source: https://www.peerlyst.com/posts/how-to-deal-with-the-shared-responsibility-model-in-public-cloud-part-1-guy-bertrand-kamga

Shared Responsibility Model



CUSTOMER

RESPONSIBLE FOR SECURITY “IN” THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

NETWORK TRAFFIC ENCRYPTION, SERVER-SIDE ENCRYPTION & DATA INTEGRITY

CLOUD PLATFORM PROVIDER

RESPONSIBLE FOR SECURITY “OF” THE CLOUD (INFRASTRUCTURE)

COMPUTE

DATABASE

STORAGE

NETWORKING

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

https://cloudcheckr.com/cloud-security/shared-responsibility-model/

Shared Responsibility Model

- **Inherited Controls** – Controls which a customer fully inherits from Cloud Provider
  - Physical and Environmental controls
- **Shared Controls** – Controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives
  - Provider covers the requirements for the infrastructure and the customer must provide their own control implementation within their use of Cloud services.

    Examples:
  - Patch Management – Provider is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.
  - Configuration Management – Provider maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.
  - Awareness & Training - Provider trains its employees, but a customer must train their own employees.
- **Customer Specific** – Controls which are solely the responsibility of the customer based on the application they are deploying within Cloud services. Examples include:
  - Service and Communications Protection or Zone Security which may require a customer to route or zone data within specific security environments.

Cloud Services Security

- Cloud access security broker
  - Enforces Enterprise security policies:
    - Authentication, authorization, encryption, tokenization
  - Hybrid cloud
- Micro-segmentation
  - Enhanced network security at individual workload level
- Web Application Firewall
  - Customizable firewall filters and blocks malicious web-traffic

- Managed services
  - On-premise and private, public and hybrid cloud application protection
- Center for Internet Security Controls
  - Proactive threat mitigation based on Forensic reports
- Automation
  - Orchestration & automation for infrastructure:
    - Operations, threat intelligence, anomaly detection, analytics, compliance, forensics, incident response etc.

Cloud Services Security

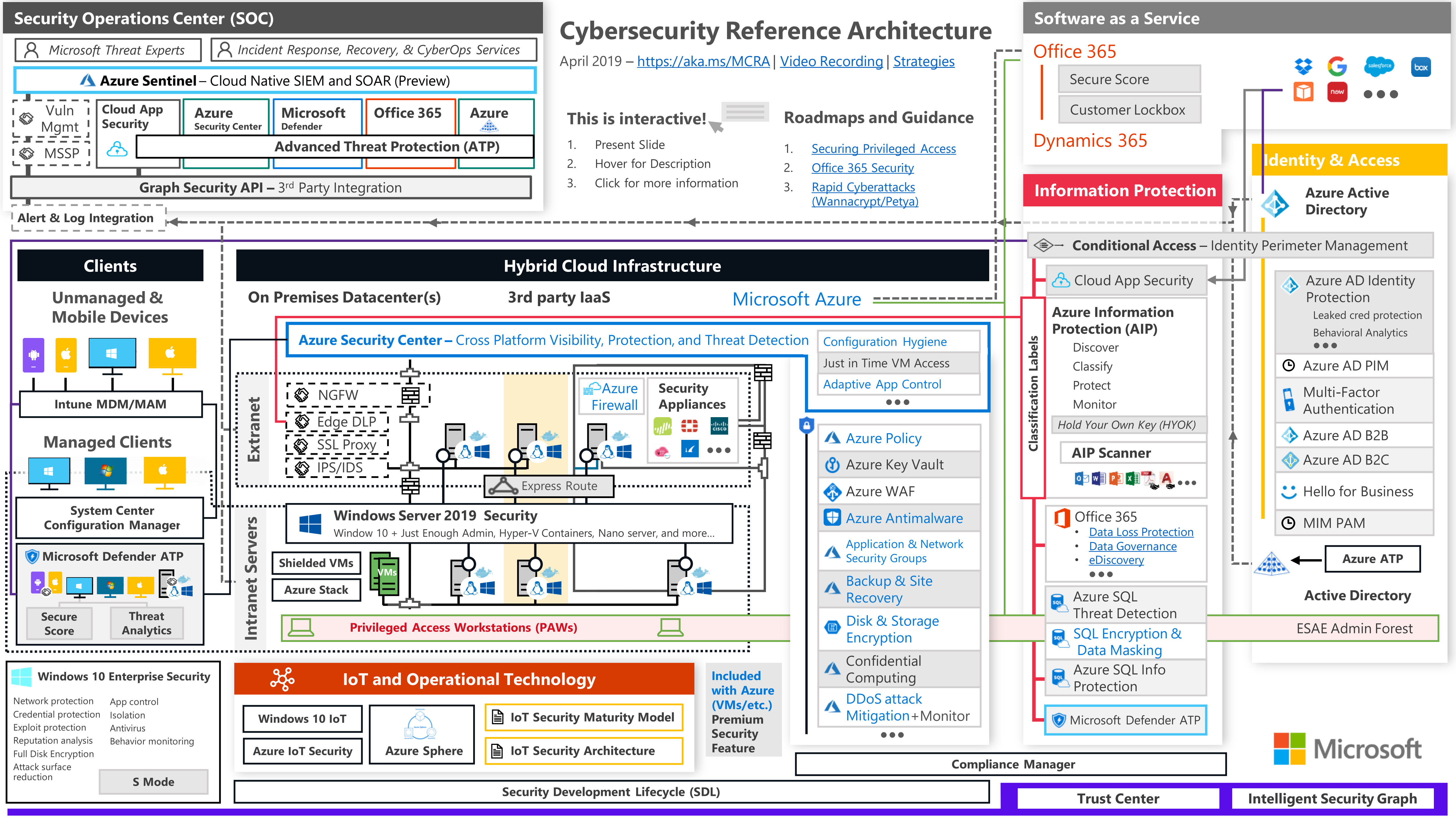
- Compliance
  - Automation of compliance with laws and regulations
  - Visibility, assessments, secure migration, security effectiveness metrics
  - Micro-segmentation, automated remediation
- Container security
  - Tools and policies to protect container infrastructure, software supply chains, runtime end-to-end
- Cloud workspace protection
  - Protect workloads in dynamic cloud environments with frequent configuration changes and evolving industry/regulatory compliance

Cloud Services Categories

- Compute
- Storage
- Database
- Migration & Transfer
- Networking & Content Delivery
- Developer Tools
- Robotics
- Blockchain
- Satellite
- Quantum Technologies

- Management & Governance
- Media Services
- Machine Learning
- Analytics
- Security, Identity, & Compliance
- Customer Enablement
- Mobile
- AR & VR
- Application Integration
- Cost Management

- Business Applications
- End User Computing
- Internet Of Things
- Game Development
- Containers



Cybersecurity Reference Architecture

April 2019 – https://aka.ms/MCRA | Video Recording | Strategies

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Security Operations Center (SOC)

Microsoft Threat Experts

Incident Response, Recovery, & CyberOps Services

Azure Sentinel – Cloud Native SIEM and SOAR (Preview)

Vuln Mgmt

MSSP

Cloud App Security

Azure Security Center

Microsoft Defender

Office 365

Azure

Advanced Threat Protection (ATP)

Graph Security API – 3rd Party Integration

Alert & Log Integration

Software as a Service

Office 365

Secure Score

Customer Lockbox

Dynamics 365

Information Protection

Identity & Access

Azure Active Directory

Conditional Access – Identity Perimeter Management

Cloud App Security

Azure AD Identity Protection

Leaked cred protection

Behavioral Analytics

•••

Azure AD PIM

Multi-Factor Authentication

Azure AD B2B

Azure AD B2C

Hello for Business

MIM PAM

Azure ATP

Active Directory

ESAE Admin Forest

Classification Labels

Azure Information Protection (AIP)

Discover

Classify

Protect

Monitor

Hold Your Own Key (HYOK)

AIP Scanner

•••

Office 365

- Data Loss Protection
- Data Governance
- eDiscovery

•••

Azure SQL Threat Detection

SQL Encryption & Data Masking

Azure SQL Info Protection

Microsoft Defender ATP

Clients

Unmanaged & Mobile Devices

Intune MDM/MAM

Managed Clients

System Center Configuration Manager

Microsoft Defender ATP

Secure Score

Threat Analytics

Hybrid Cloud Infrastructure

On Premises Datacenter(s)

3rd party IaaS

Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

Configuration Hygiene

Just in Time VM Access

Adaptive App Control

•••

Extranet

NGFW

Edge DLP

SSL Proxy

IPS/IDS

Azure Firewall

Security Appliances

•••

Express Route

Windows Server 2019 Security

Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more…

Shielded VMs

Azure Stack

VMs

Intranet Servers

Privileged Access Workstations (PAWs)

Azure Policy

Azure Key Vault

Azure WAF

Azure Antimalware

Application & Network Security Groups

Backup & Site Recovery

Disk & Storage Encryption

Confidential Computing

DDoS attack Mitigation+Monitor

•••

Windows 10 Enterprise Security

Network protection

Credential protection

Exploit protection

Reputation analysis

Full Disk Encryption

Attack surface reduction

App control

Isolation

Antivirus

Behavior monitoring

S Mode

IoT and Operational Technology

Windows 10 IoT

Azure IoT Security

Azure Sphere

IoT Security Maturity Model

IoT Security Architecture

Included with Azure (VMs/etc.)

Premium Security Feature

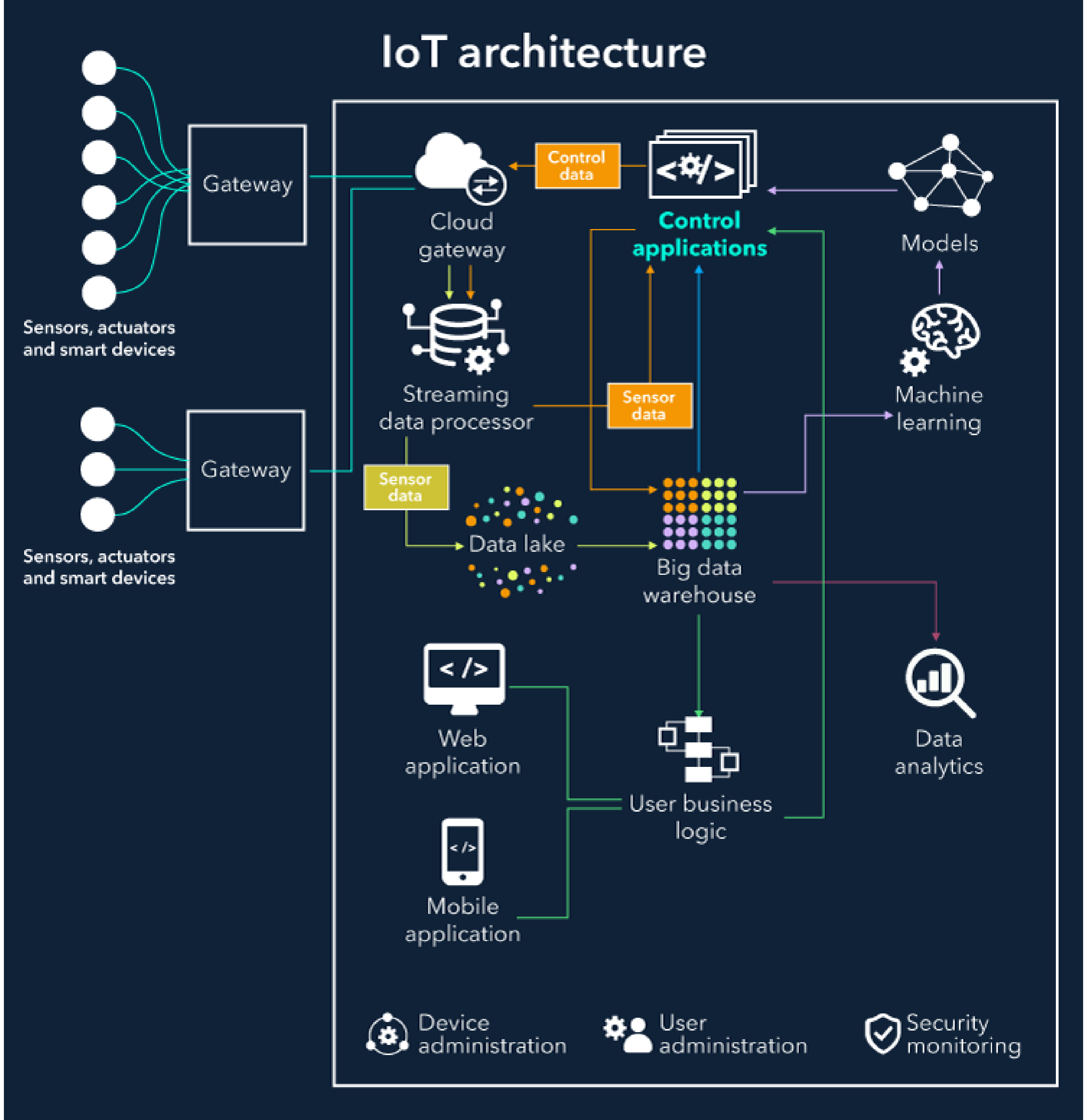
Compliance Manager

Security Development Lifecycle (SDL)

Trust Center

Intelligent Security Graph

Microsoft



IoT architecture – Security Domains

Technical Infrastructure

- Global-scale technical infrastructure for:
  - Secure deployment of services
  - Secure storage of data
  - Secure communications between services
  - Safe operation by administrators

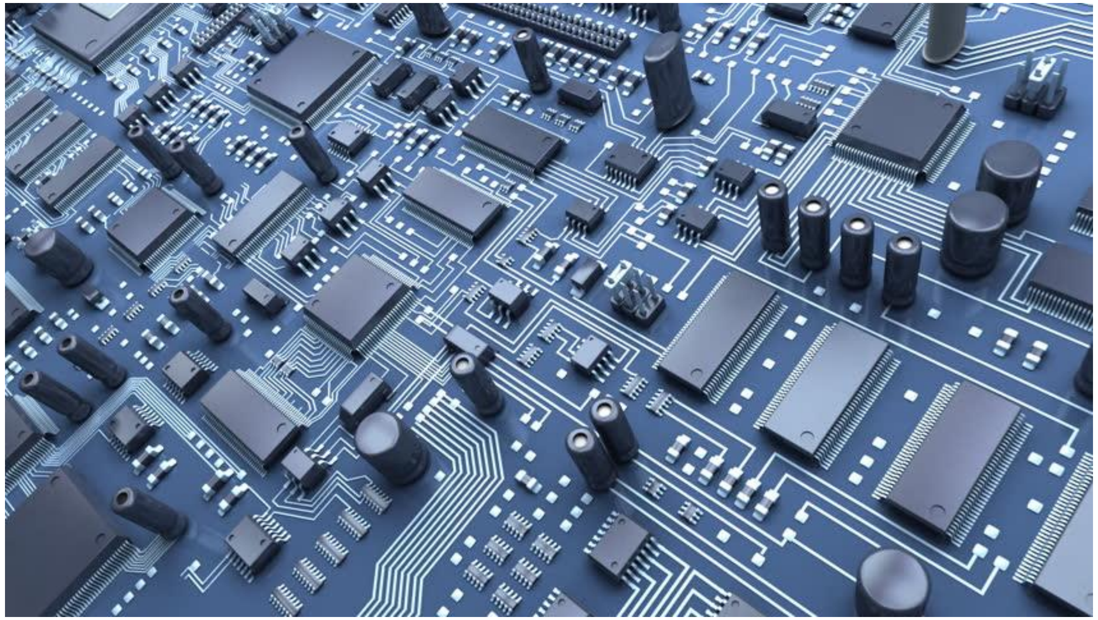
Security Components

- Operational Security
- Internet Communication
- Storage Services
- User Security
- Service Deployment
- Hardware Infrastructure

https://cloud.google.com/security/infrastructure/design

Hardware Infrastructure

- State-of-the-art data centers
- Security of physical premises
- Hardware design and provenance
  - Custom server boards, integrated circuits, hardware security chip (Titan)
- Secure boot stack and machine identity
  - Cryptographic signatures only boot authorized software



Secure Service

- Cryptographic privacy and integrity RPC data on the network
- Automatically encrypts RPC traffic in transit between data centers
- Central source code repository with two-party review of new code.
- Developer libraries to prevent certain classes of security bugs.
- **External bug bounty program for discovery and information of bugs in GCP infrastructure or applications**

User Identity

- Intelligent challenge for additional info
  - Risk actors – device, location
- Multifactor authentication
  - Universal 2nd Factor open standard
- To guard against phishing attack, all Google employee accounts use U2F security keys

Storage Services

- Encryption at rest by default
  - Google-managed keys
  - Customer-managed with KMS
  - Customer-supplied
- Asset inventory end-to-end
  - Acquisition, installation, retirement, destruction
- Hard drive retirement
  - 0’s imprinted, multi-stage destruction
  - Customer deleted data purged within 180 days

Internet Communication

- Service Registration
  - Google Front End
- Connection checks
  - Certificates, best practices, strong encryption, DoS
  - Google global scale (40% web)
    - Multi-tier, multi-layer DoS shield
    - Google Cloud Load Balancer
- Transport Encryption
  - On-premise connection

Operational Security

- Security Culture
  - Hiring, onboarding, offboarding
  - Awareness, training

Architecture Layers

- VPC Network Security
  - Globally isolated network
  - Controlled Ingress & Egress
- Operational Monitoring
  - Application analysis, network forensics
  - Access patterns, performance profiling
  - GCP Stackdriver

- Regulatory Compliance
  - Independent verification
  - Security, privacy, compliance
    - Compliance Center

Threat Mitigation

“Absorbing the largest attacks requires the bandwidth needed to watch half a million YouTube videos at the same time...in HD.”

- Dr. Damian Menscher

Denial of Service Protection

- GCP Global Scale networking
  - Central DoS mitigation service
  - Multi-tier, multi-layer protection
- Pro-active detection
  - Load Balancer DoS activation
  - Drop or throttle traffic
- No additional configuration required
- GCP
  - Cloud Load Balancing
  - Cloud Armor

#67076092

Data Transparency

- Google statement:
  - Customer data not scanned for advertisements or 3rd party
- Google Access Transparency
  - Near-time oversight regardless of GCP engagement
    - Different from standard audits
- Data Export
  - No penalties but egress charge
  - Google Transfer Appliance
    - 100s TB on a single appliance

Data Privacy

- Access Approval API
  - With Access Transparency
  - Require explicit approval
- Project level
  - Email or Pub/Sub
  - Console or API
- Access Approval Config Editor IAM Role
  - Location, Time, Interval
  - Reason, Status
- May increase support times

- Exclusions (Will not trigger)
  - System access to user content
  - Lower level storage
  - Legal reasons
  - Outage
- System access requires separate process
- Legal and outage scenarios by-pass Access Approval

Foundations of GCP Security

Security Components

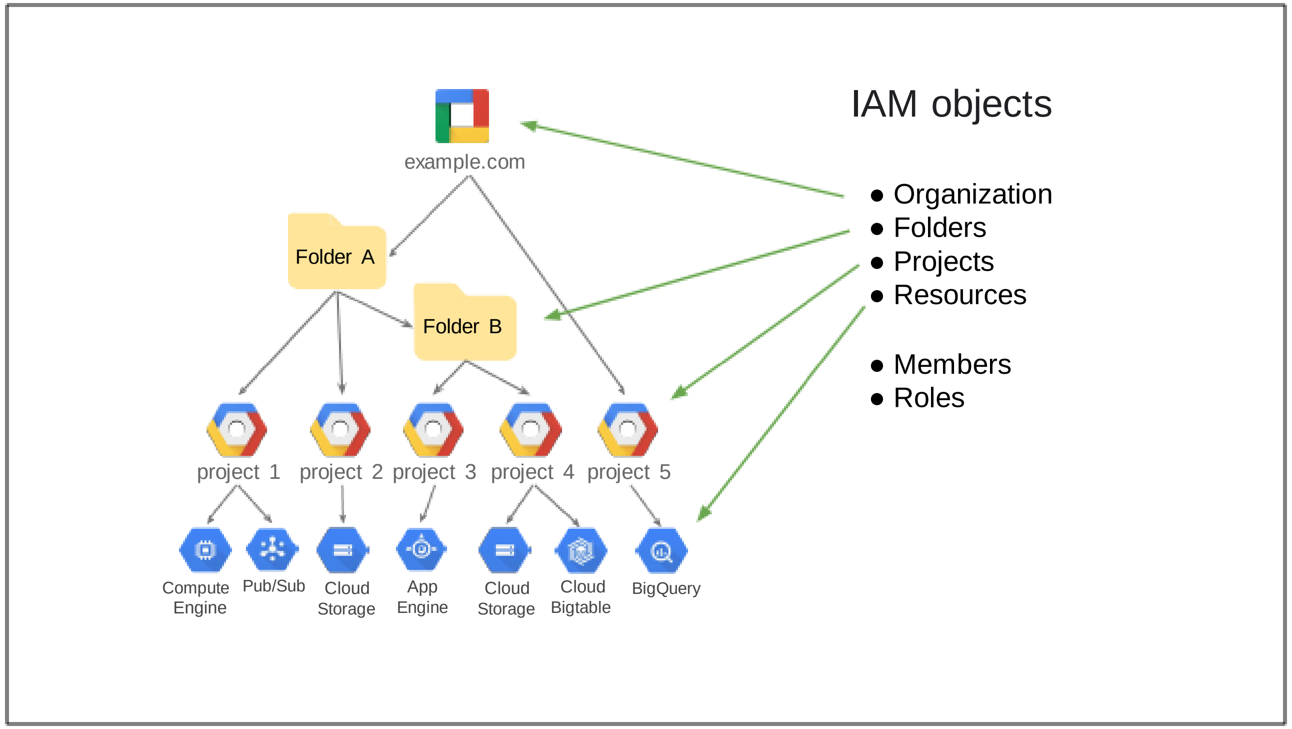
User Identity

- Intelligent challenge for additional info
  - Risk actors – device, location
- Multifactor authentication
  - Universal 2nd Factor open standard
- To guard against phishing attack, all Google employee accounts use U2F security keys

GCP IAM Best Practices

- Use Groups
- Assign Roles to Groups
- Use GCP Predefined Roles
  - Less Admin overhead
  - Managed by Google
  - Custom Roles unmanaged
- Use Audit Logs
  - Project-level permission changes
- Audit policy changes
- Use Cloud storage for logs

GCP IAM Resource Management

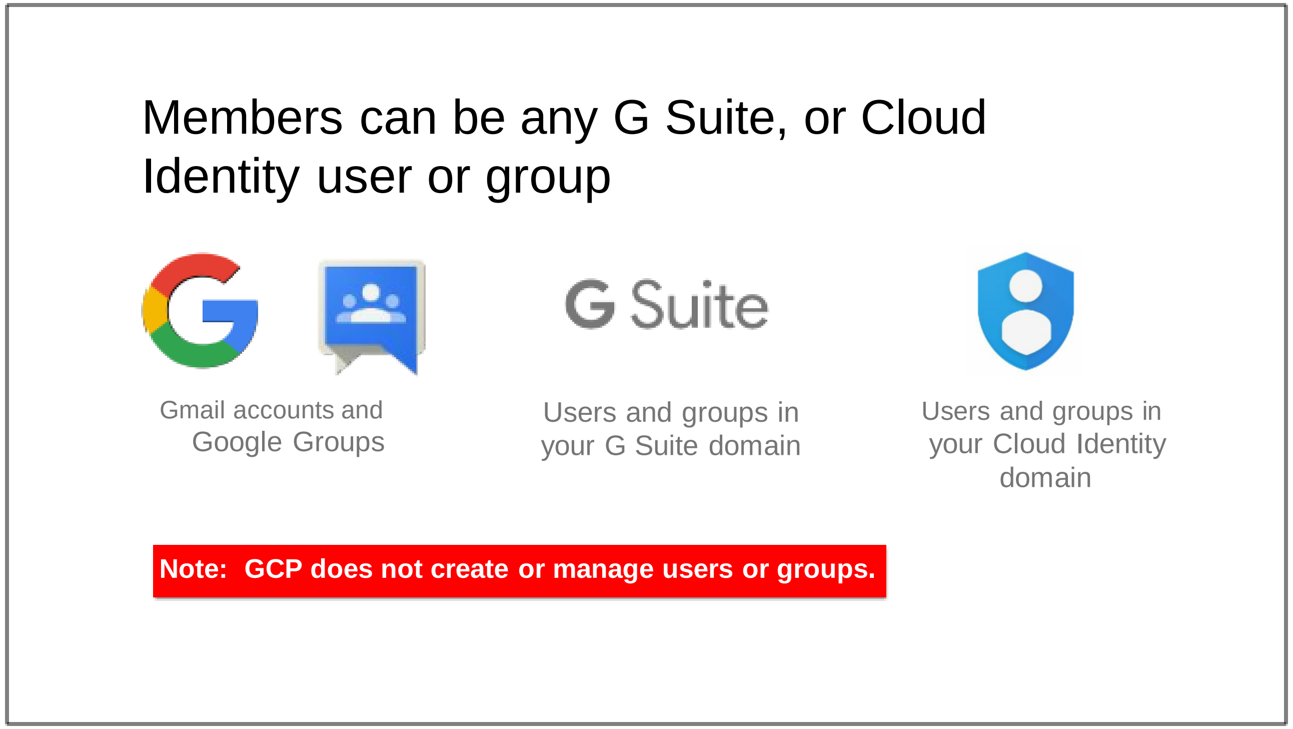


IAM objects

- Organization
- Folders
- Projects
- Resources

- Members
- Roles

GCP IAM Resource Management



Members can be any G Suite, or Cloud Identity user or group

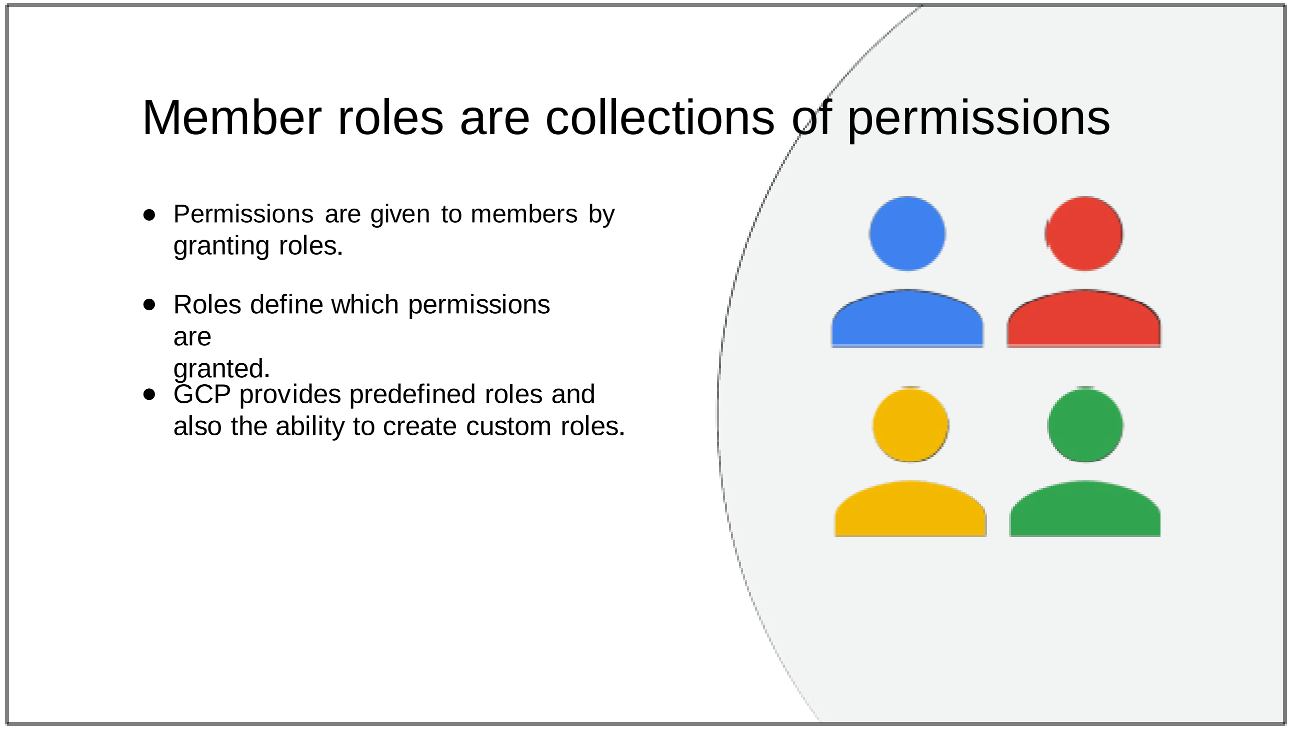
Gmail accounts and Google Groups

Users and groups in your G Suite domain

Users and groups in your Cloud Identity domain

Note: GCP does not create or manage users or groups.

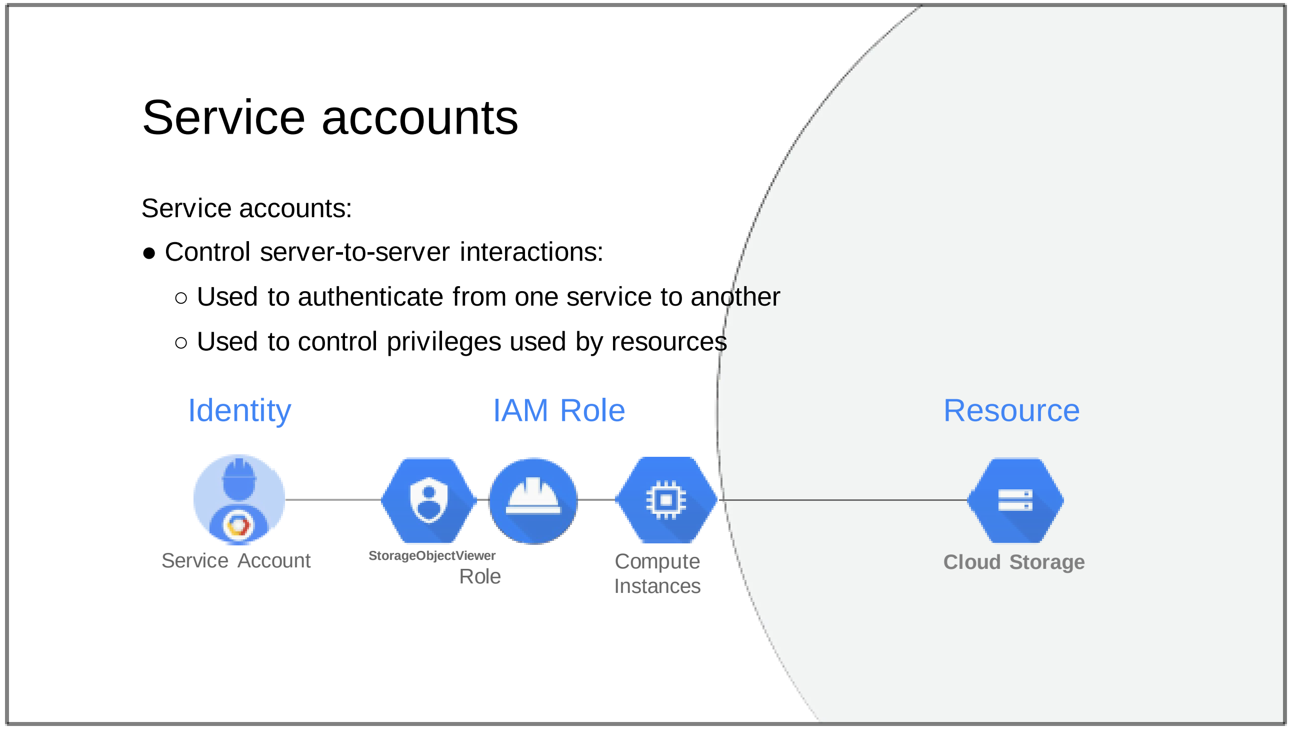
GCP IAM Resource Management



Member roles are collections of permissions

- Permissions are given to members by granting roles.
- Roles define which permissions are granted.
- GCP provides predefined roles and also the ability to create custom roles.

GCP IAM Resource Management



Service accounts

Service accounts:

- Control server-to-server interactions:
  - Used to authenticate from one service to another
  - Used to control privileges used by resources

GCP IAM Resource Management

There are two types of Google Service Accounts

Google-managed service accounts

All service accounts have Google-managed keys

Google stores both the public and private portion of the key.

Each public key can be used for signing for a maximum of two weeks

Private keys are never directly accessible

User-managed service accounts

Google only stores the public portion of a user-managed key.

Users are responsible for private key security.

Can create up to 10 user-managed service account keys per service.

Can be administered via Cloud IAM API, gcloud, or the Console.

```
gcloud  iam  service-accounts  keys  list  --iam-account  user@email.com
```

GCP IAM Resource Management

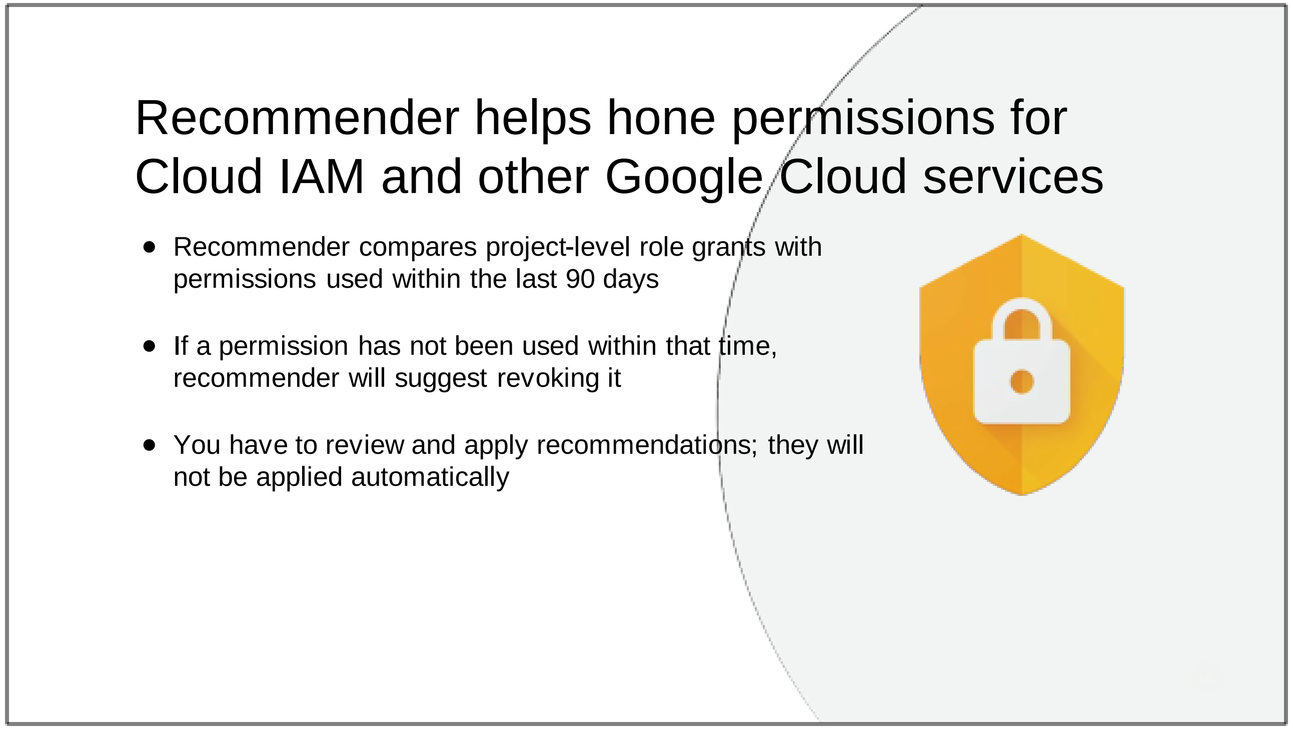
There are three kinds of IAM roles in GCP

Primitive

Predefined

Custom

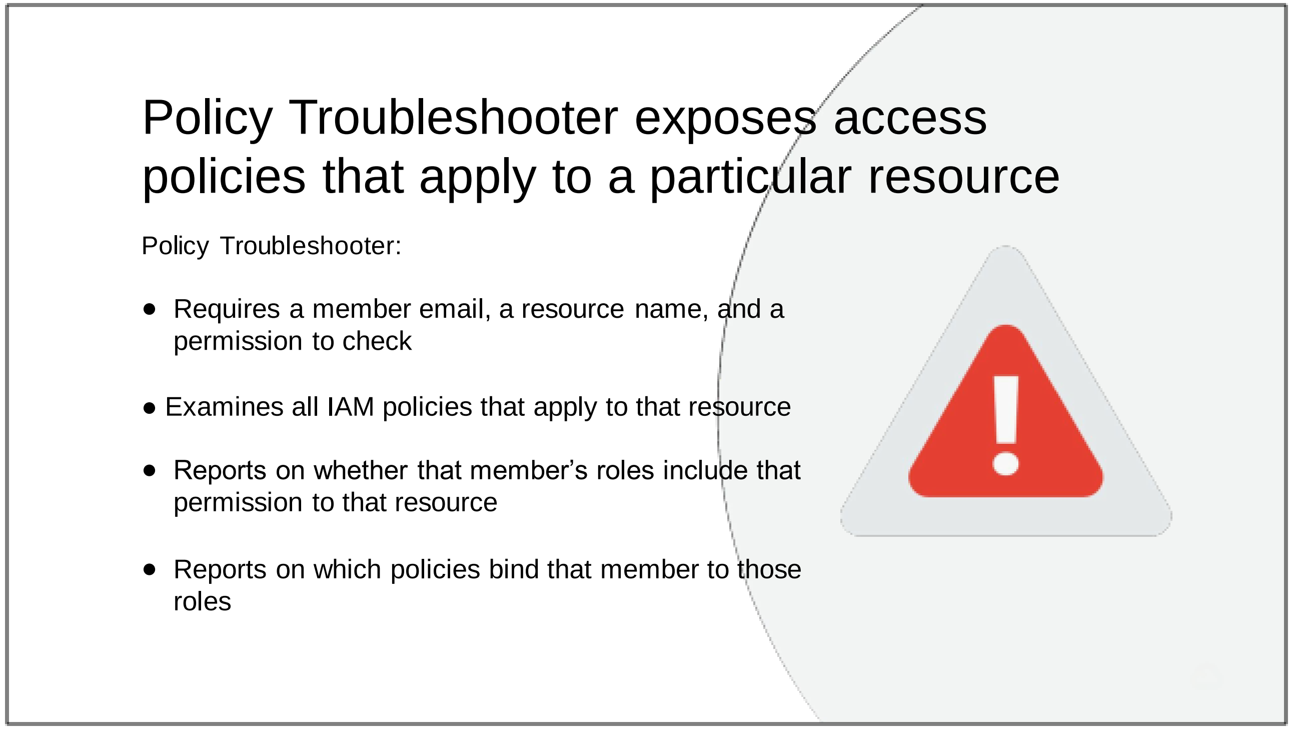
GCP IAM Resource Management



Recommender helps hone permissions for Cloud IAM and other Google Cloud services

- Recommender compares project-level role grants with permissions used within the last 90 days
- If a permission has not been used within that time, recommender will suggest revoking it
- You have to review and apply recommendations; they will not be applied automatically

GCP IAM Resource Management



Policy Troubleshooter exposes access policies that apply to a particular resource

Policy Troubleshooter:

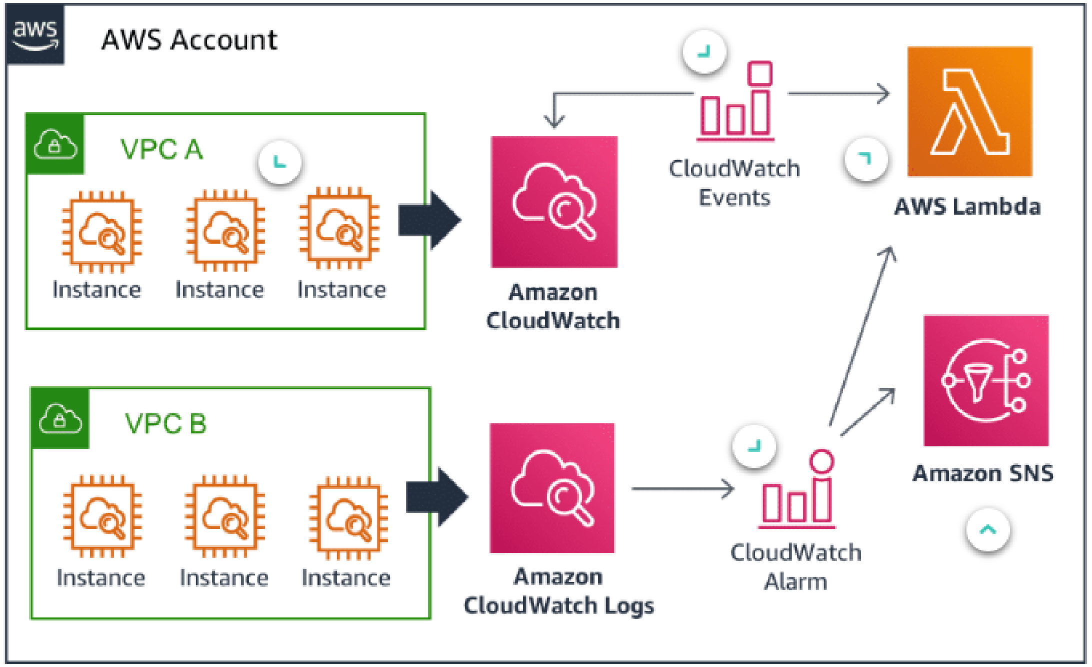
- Requires a member email, a resource name, and a permission to check
- Examines all IAM policies that apply to that resource
- Reports on whether that member’s roles include that permission to that resource
- Reports on which policies bind that member to those roles

GCP IAM Best Practices

- Use Groups
- Assign Roles to Groups
- Use GCP Predefined Roles
  - Less Admin overhead
  - Managed by Google
  - Custom Roles unmanaged
- Use Audit Logs
  - Project-level permission changes
- Audit policy changes
- Use Cloud storage for logs

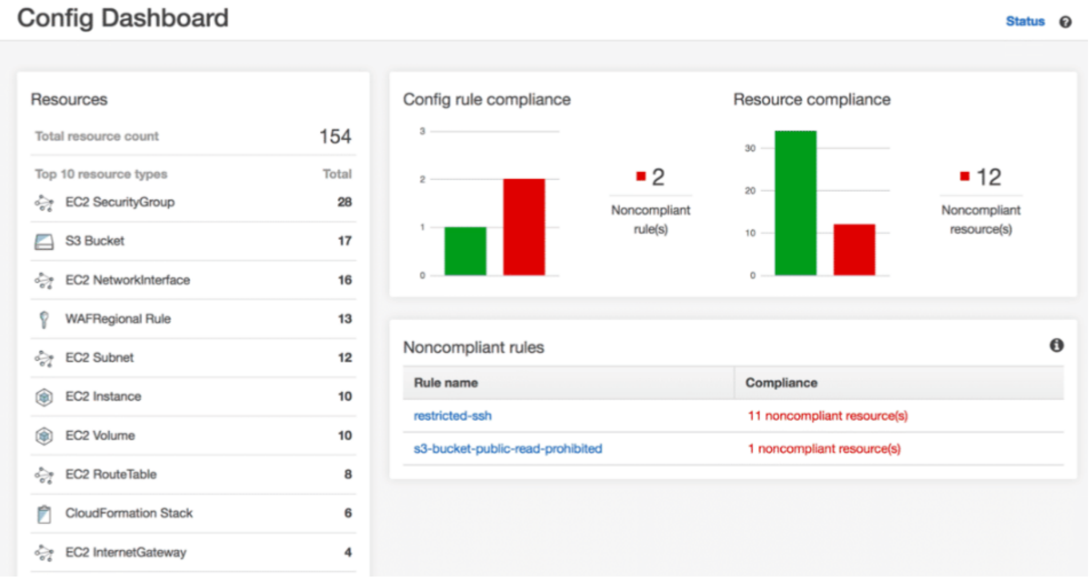
Detective Controls

- Capturing & Collecting Logs
  - CloudTrail
  - Part of proving compliance
- Monitoring & Notification
  - CloudWatch
- Audit
  - S3 Access logs, Access Logs,
  - CloudWatch Logs & Events
  - VPC Flow logs
  - CloudTrail



Detective Controls

- GuardDuty
  - Threat detection
- Trusted Advisor
  - Best Practices
- Security Hub
  - Alerts & Compliance
  - Single pane of glass
- Config
  - Continuous monitoring & assessment



Config Dashboard

Resources

Total resource count	154
Top 10 resource types	Total
EC2 SecurityGroup	28
S3 Bucket	17
EC2 NetworkInterface	16
WAFRegional Rule	13
EC2 Subnet	12
EC2 Instance	10
EC2 Volume	10
EC2 RouteTable	8
CloudFormation Stack	6
EC2 InternetGateway	4

Noncompliant rules

Rule name	Compliance
restricted-ssh	11 noncompliant resource(s)
s3-bucket-public-read-prohibited	1 noncompliant resource(s)

[Amazon CloudWatch Events](#) [Security at Scale: Logging in AWS](#) [Cloud Audit Academy](#)

Design Principles

Implement strong identity foundation

Enable traceability

Apply security at all layers

Automate security best practices

Protect data at rest and in transit

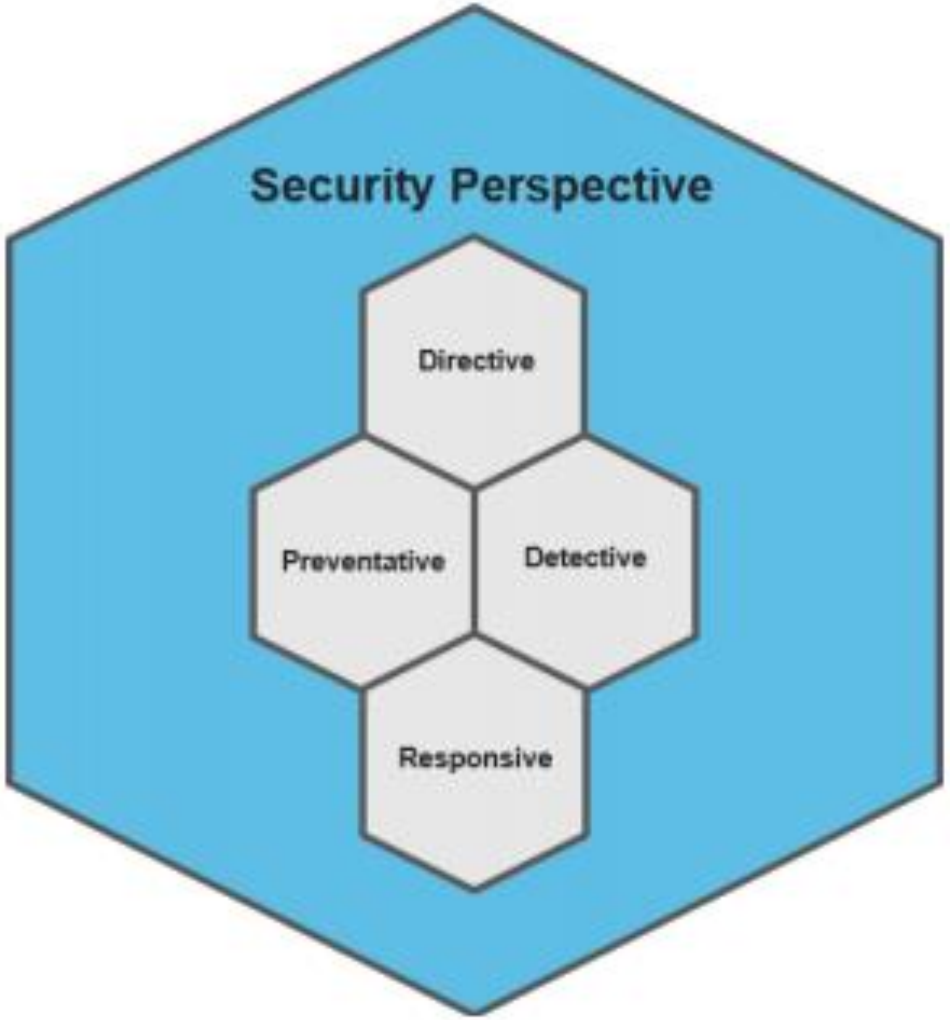
Enforce the principle of least privilege

Prepare for security events

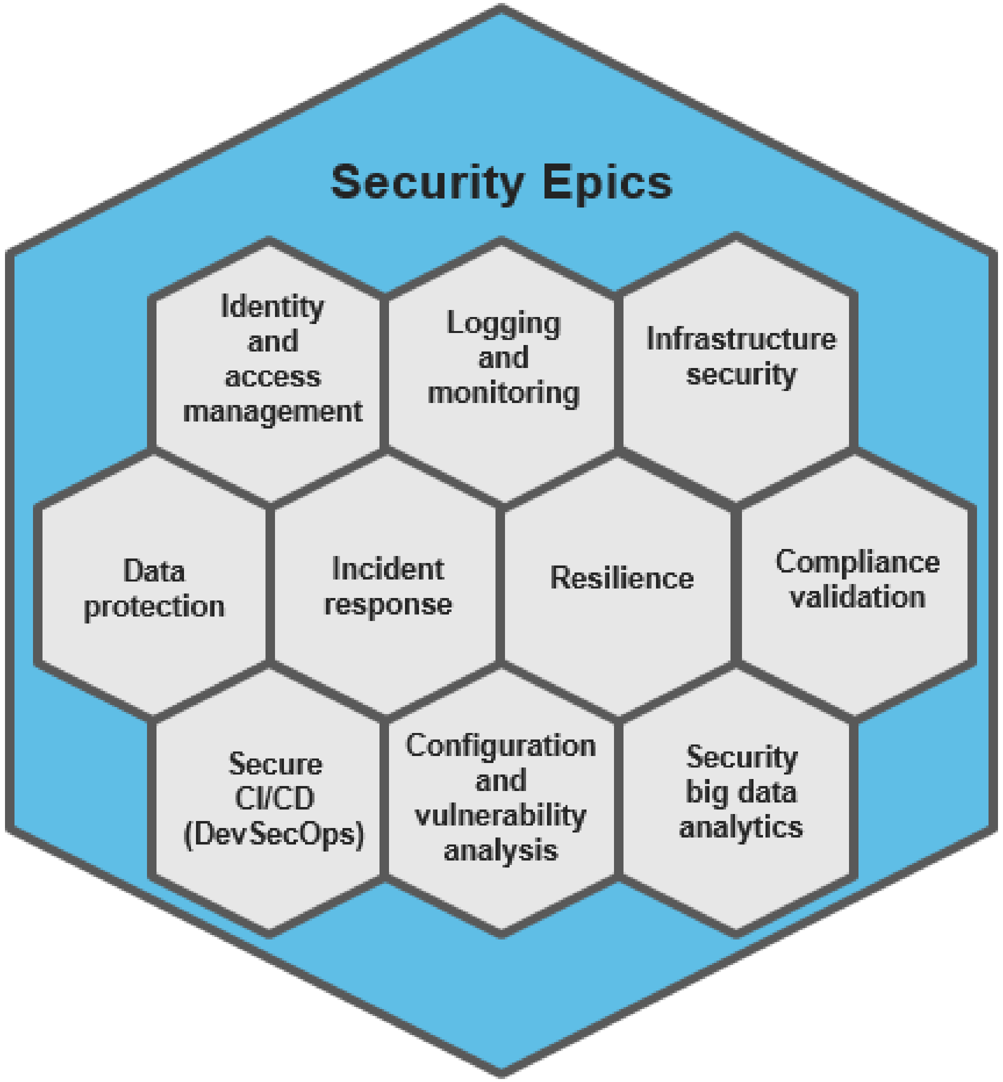
- Principle of least privilege
  - Separation of duties, authorization
- Monitor, alert & audit actions/changes
  - Integrate logs & metrics for auto-response
- Defense-in-depth approach controls
- Controls defined & managed in codes
  - Version-controlled templates
- Classify sensitive data – encryption
- Deny access by default
- Incident management process
  - Simulation, automation tools:
  - Detection, investigation, recovery

Security Perspective

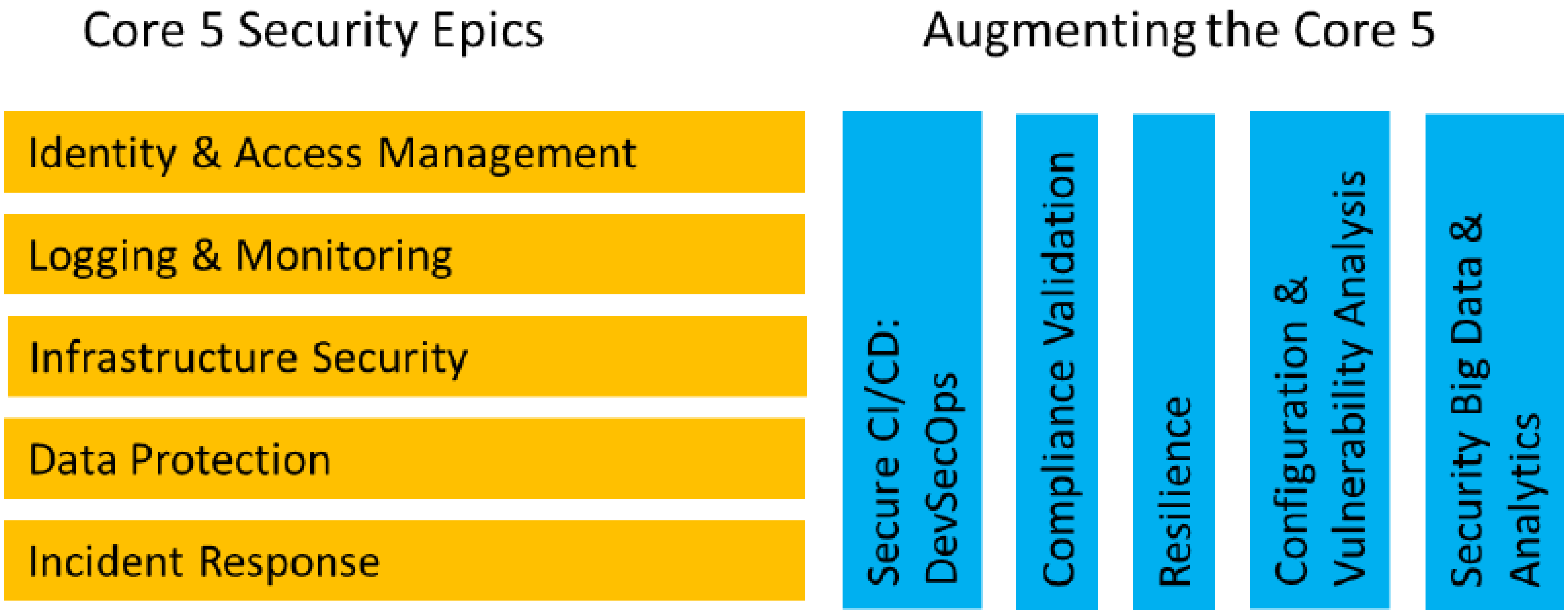
- Directive controls establish the governance, risk, and compliance models the environment will operate within.
- Preventive controls protect workloads and mitigate threats and vulnerabilities.
- Detective controls provide full visibility and transparency over the operation of cloud deployments.
- Responsive controls drive remediation of potential deviations from security baselines.



Security Topics



Security Topics



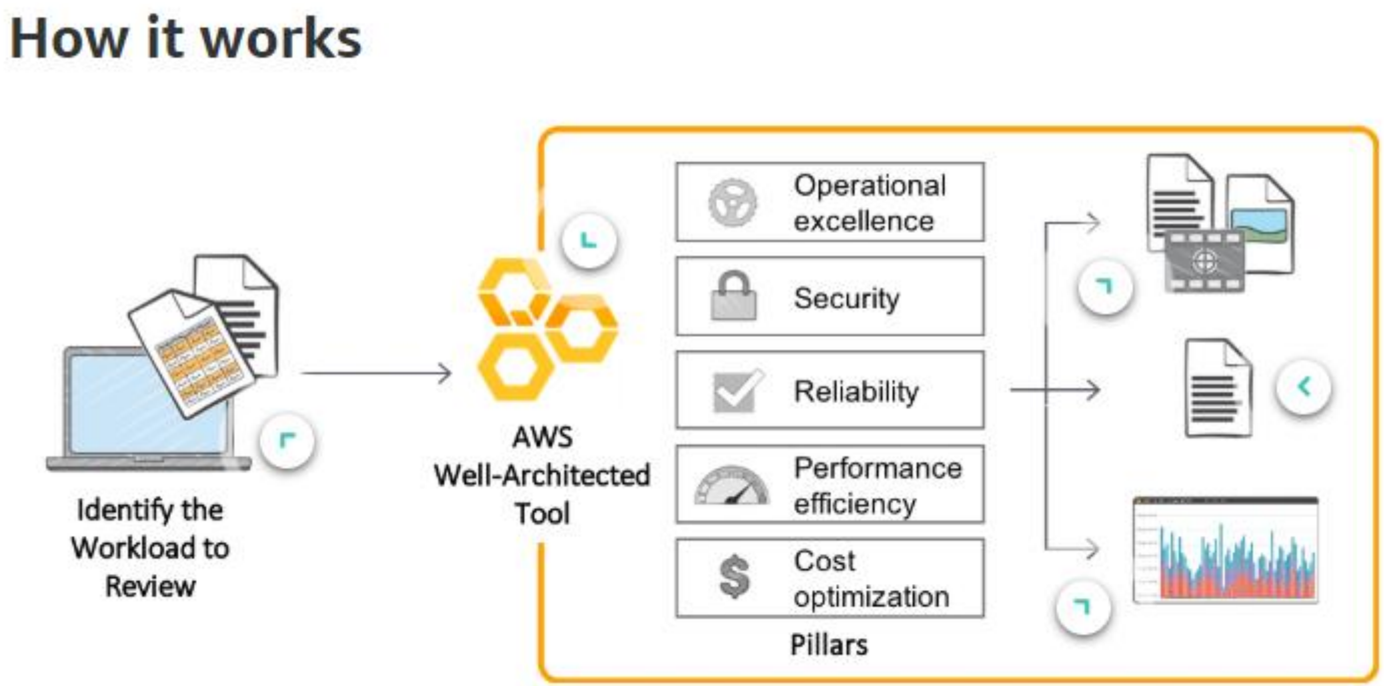
Core 5 Security Epics

- Identity & Access Management
- Logging & Monitoring
- Infrastructure Security
- Data Protection
- Incident Response

Augmenting the Core 5

- Secure CI/CD: DevSecOps
- Compliance Validation
- Resilience
- Configuration & Vulnerability Analysis
- Security Big Data & Analytics

Well-Architected Tool



https://docs.aws.amazon.com/wellarchitected/latest/userguide/wellarchitected-ug.pdf