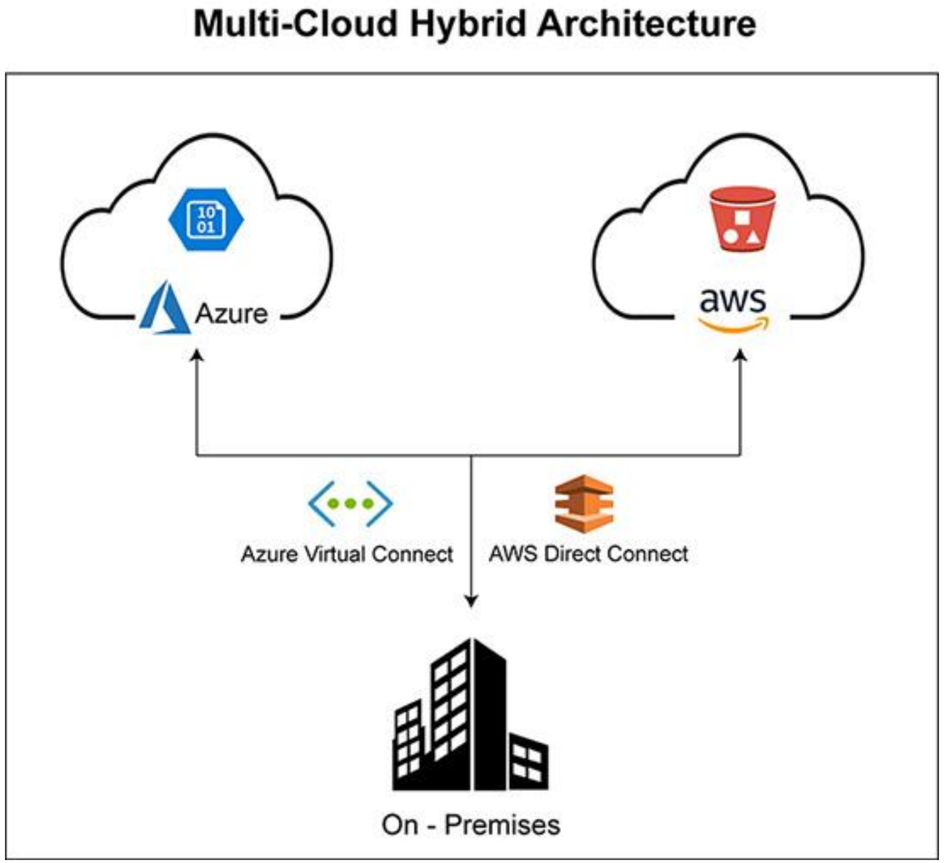
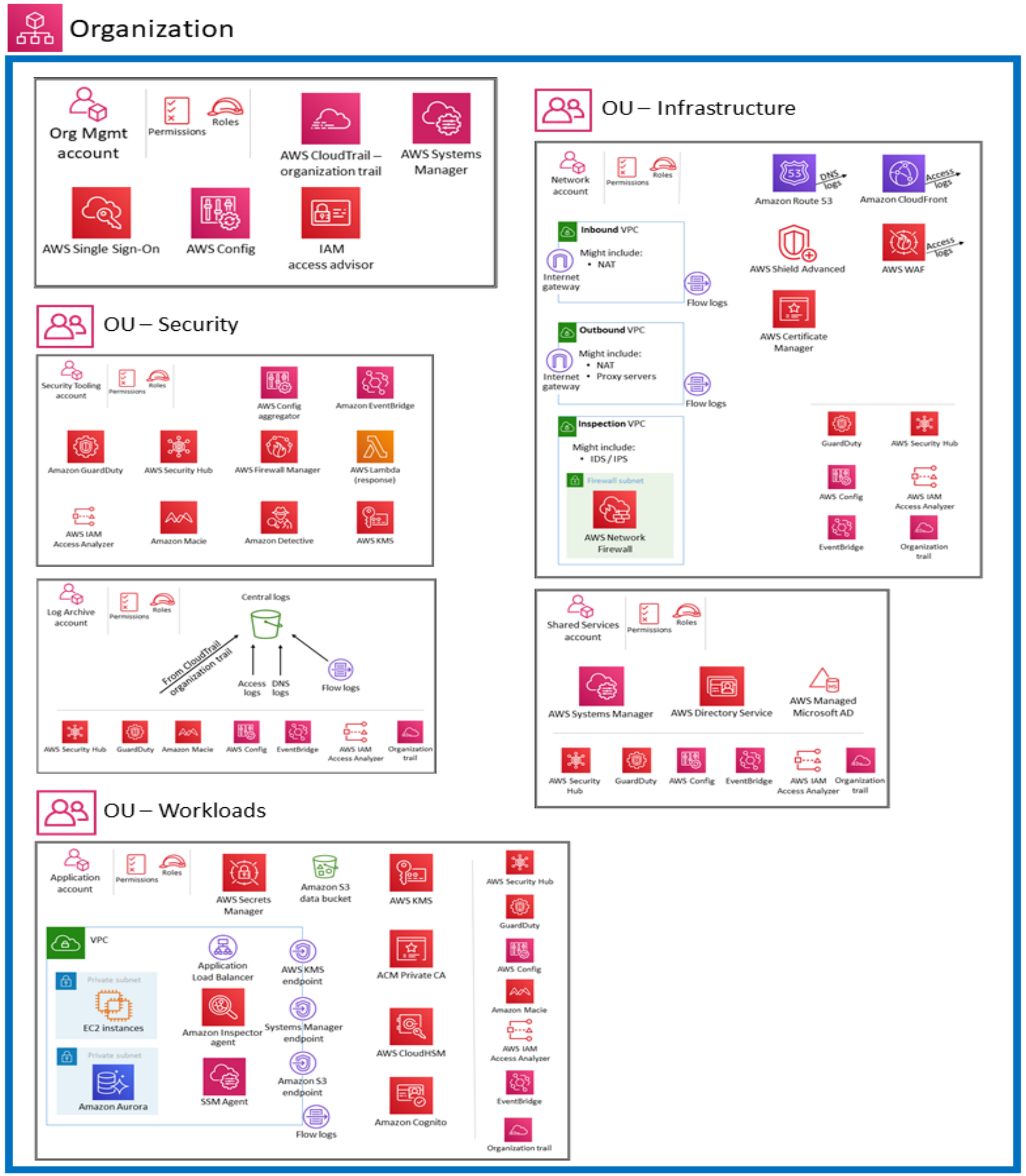
Multiple Cloud strategy

Multi cloud strategy ?

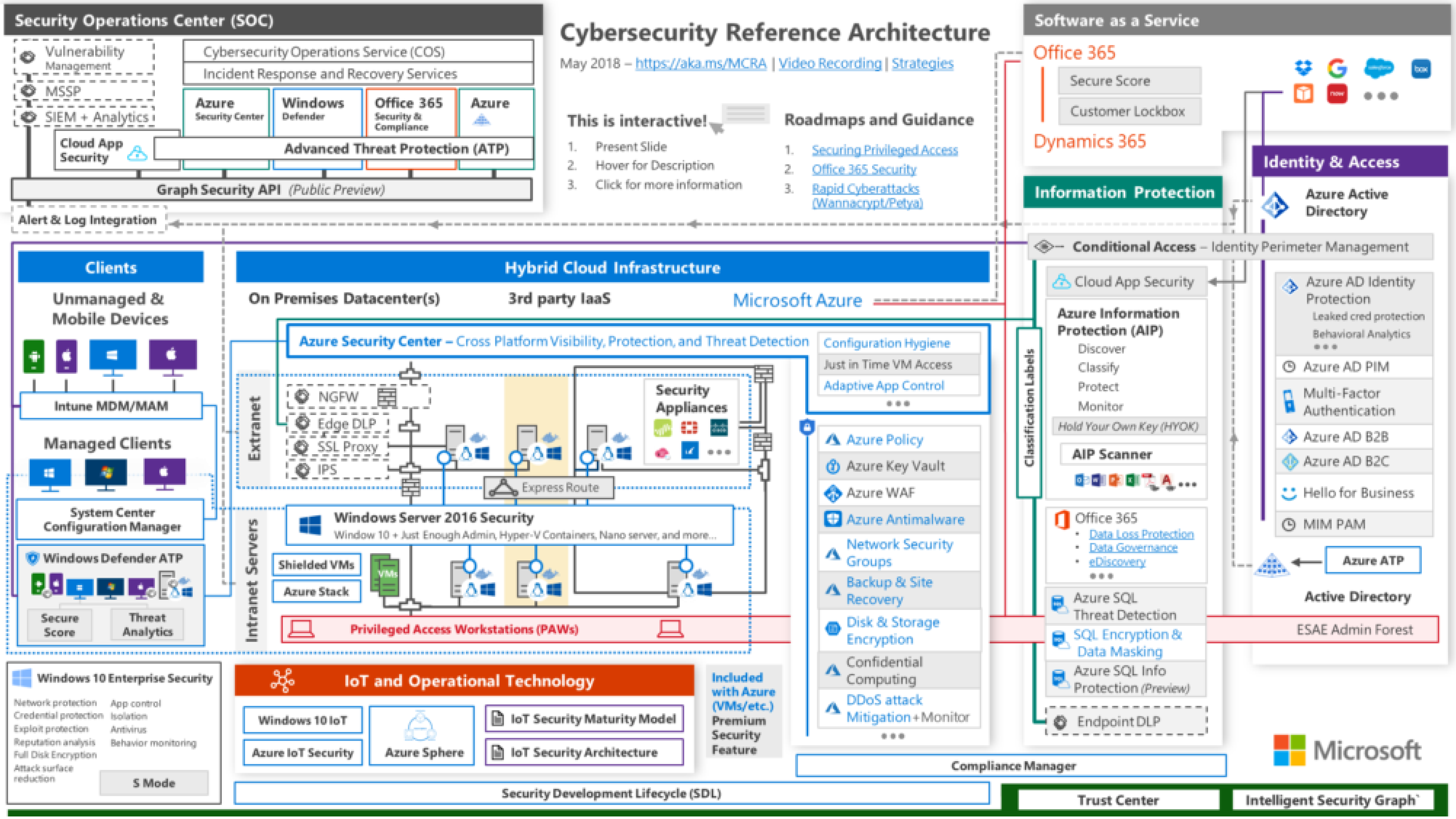


AWS AWS Security Reference Architecture



Cybersecurity Reference Architecture

May 2018 – https://aka.ms/MCRA | Video Recording | Strategies



Security Operations Center (SOC)

Vulnerability Management

MSSP

SIEM + Analytics

Cybersecurity Operations Service (COS)

Incident Response and Recovery Services

Azure Security Center

Windows Defender

Office 365 Security & Compliance

Azure

Cloud App Security

Advanced Threat Protection (ATP)

Graph Security API *(Public Preview)*

Alert & Log Integration

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)

Software as a Service

Office 365

Secure Score

Customer Lockbox

Dynamics 365

Information Protection

Cloud App Security

Azure Information Protection (AIP)

Discover

Classify

Protect

Monitor

Hold Your Own Key (HYOK)

AIP Scanner

Classification Labels

Office 365

- Data Loss Protection
- Data Governance
- eDiscovery

Azure SQL Threat Detection

SQL Encryption & Data Masking

Azure SQL Info Protection *(Preview)*

Endpoint DLP

Identity & Access

Azure Active Directory

Conditional Access – Identity Perimeter Management

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

Clients

Unmanaged & Mobile Devices

Intune MDM/MAM

Managed Clients

System Center Configuration Manager

Windows 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

Security Appliances

Express Route

Intranet Servers

Windows Server 2016 Security

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

Shielded VMs

Azure Stack

VMs

Privileged Access Workstations (PAWs)

Azure Policy

Azure Key Vault

Azure WAF

Azure Antimalware

Network Security Groups

Backup & Site Recovery

Disk & Storage Encryption

Confidential Computing

DDoS attack Mitigation + Monitor

Included with Azure (VMs/etc.)

Premium Security Feature

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

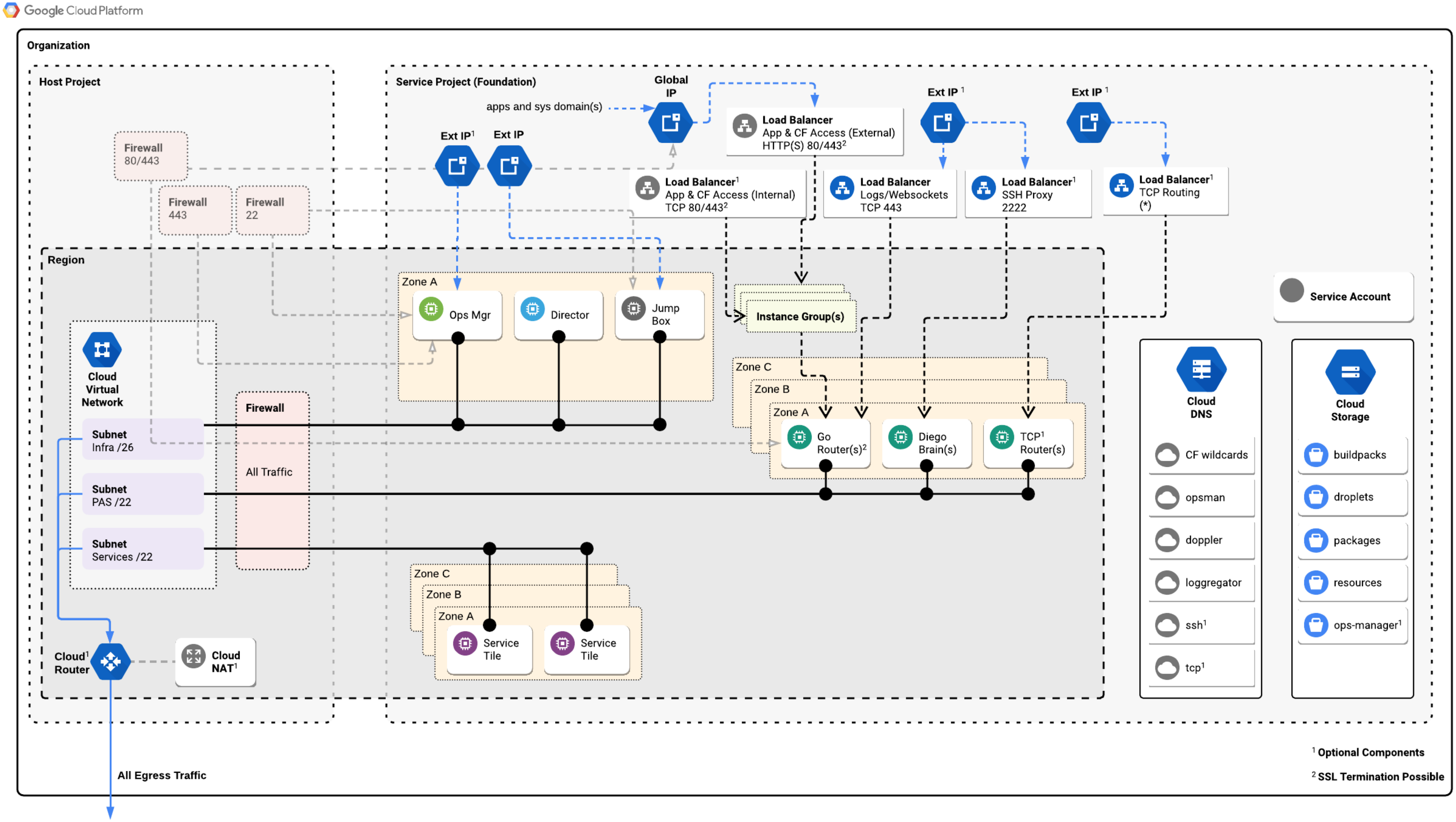
Compliance Manager

Security Development Lifecycle (SDL)

Trust Center

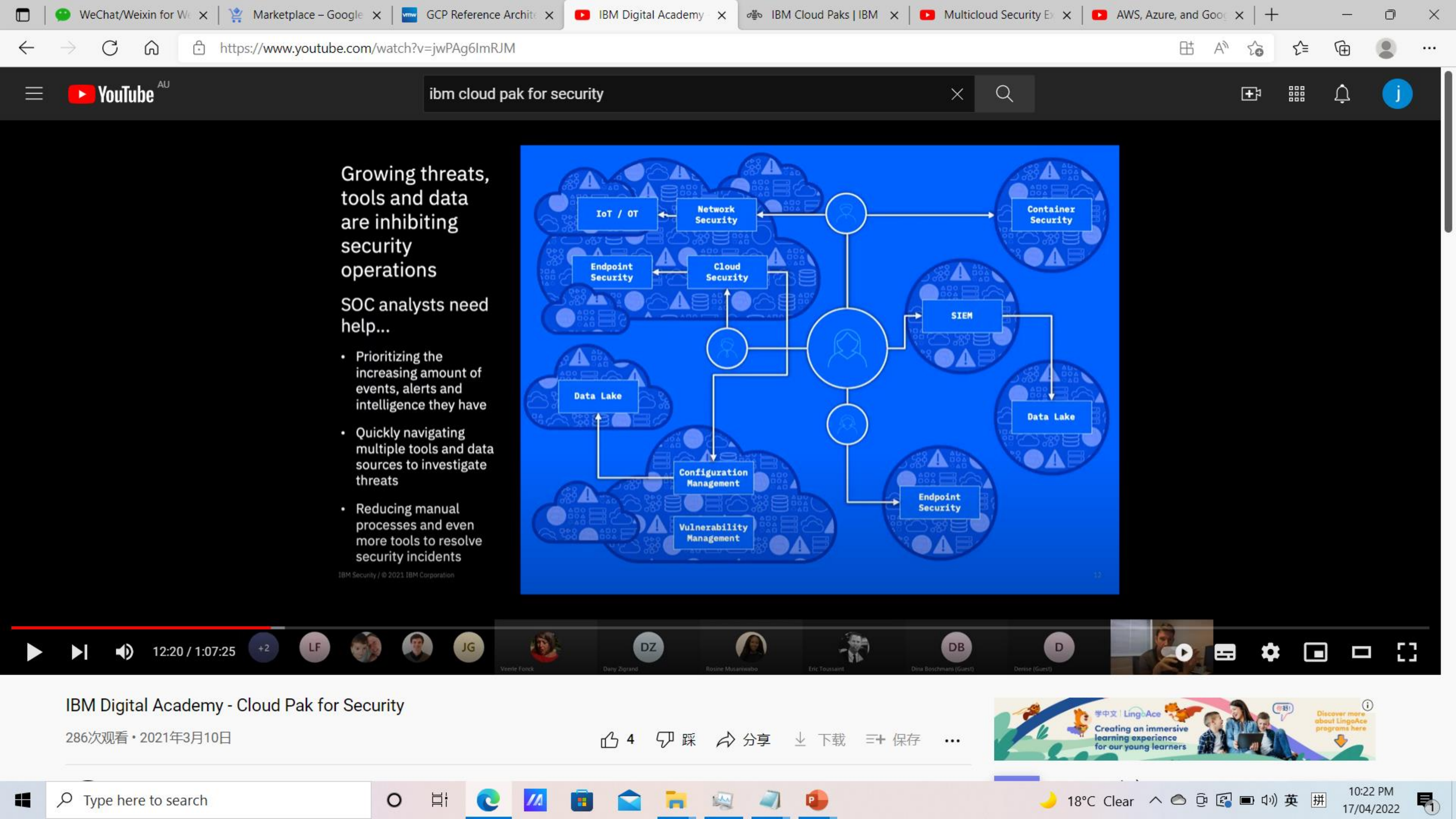
Intelligent Security Graph`

Microsoft


Google Cloud Platform
Organization
Host Project
Service Project (Foundation)
apps and sys domain(s)
Global IP
Load Balancer
App & CF Access (External)
HTTP(S) 80/443[2]
Ext IP [1]
Ext IP [1]
Ext IP[1]
Ext IP
Firewall
80/443
Firewall
443
Firewall
22
Load Balancer[1]
App & CF Access (Internal)
TCP 80/443[2]
Load Balancer
Logs/Websockets
TCP 443
Load Balancer[1]
SSH Proxy
2222
Load Balancer[1]
TCP Routing
(*)
Region
Zone A
Ops Mgr
Director
Jump Box
Instance Group(s)
Service Account
Cloud Virtual Network
Subnet
Infra /26
Subnet
PAS /22
Subnet
Services /22
Firewall
All Traffic
Zone C
Zone B
Zone A
Go Router(s)[2]
Diego Brain(s)
TCP[1] Router(s)
Cloud DNS
CF wildcards
opsman
doppler
loggregator
ssh[1]
tcp[1]
Cloud Storage
buildpacks
droplets
packages
resources
ops-manager[1]
Zone C
Zone B
Zone A
Service Tile
Service Tile
Cloud[1] Router
Cloud NAT[1]
All Egress Traffic
[1] Optional Components
[2] SSL Termination Possible

Ibm cloud pak

- Cloud pak for data
- Cloud pak for security
- Cloud pak for automation
- Cloud pak for network automation
- Ibm cloud pak for applications
- Ibm cloud pak for multicloud management



Growing threats, tools and data are inhibiting security operations

SOC analysts need help...

- Prioritizing the increasing amount of events, alerts and intelligence they have
- Quickly navigating multiple tools and data sources to investigate threats
- Reducing manual processes and even more tools to resolve security incidents

IBM Security / © 2021 IBM Corporation

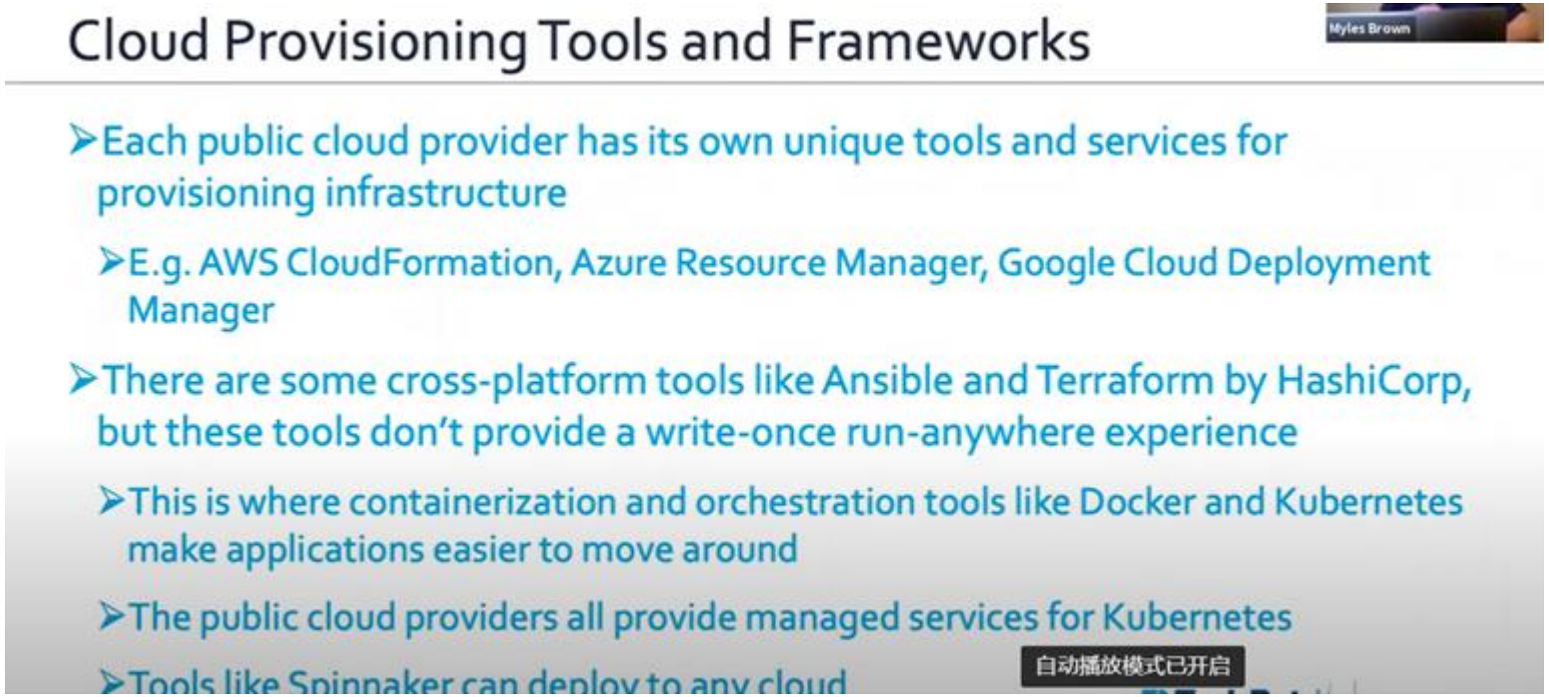
IBM Digital Academy - Cloud Pak for Security

286次观看 • 2021年3月10日

Security control and operation are challenging on the multi cloud strategy

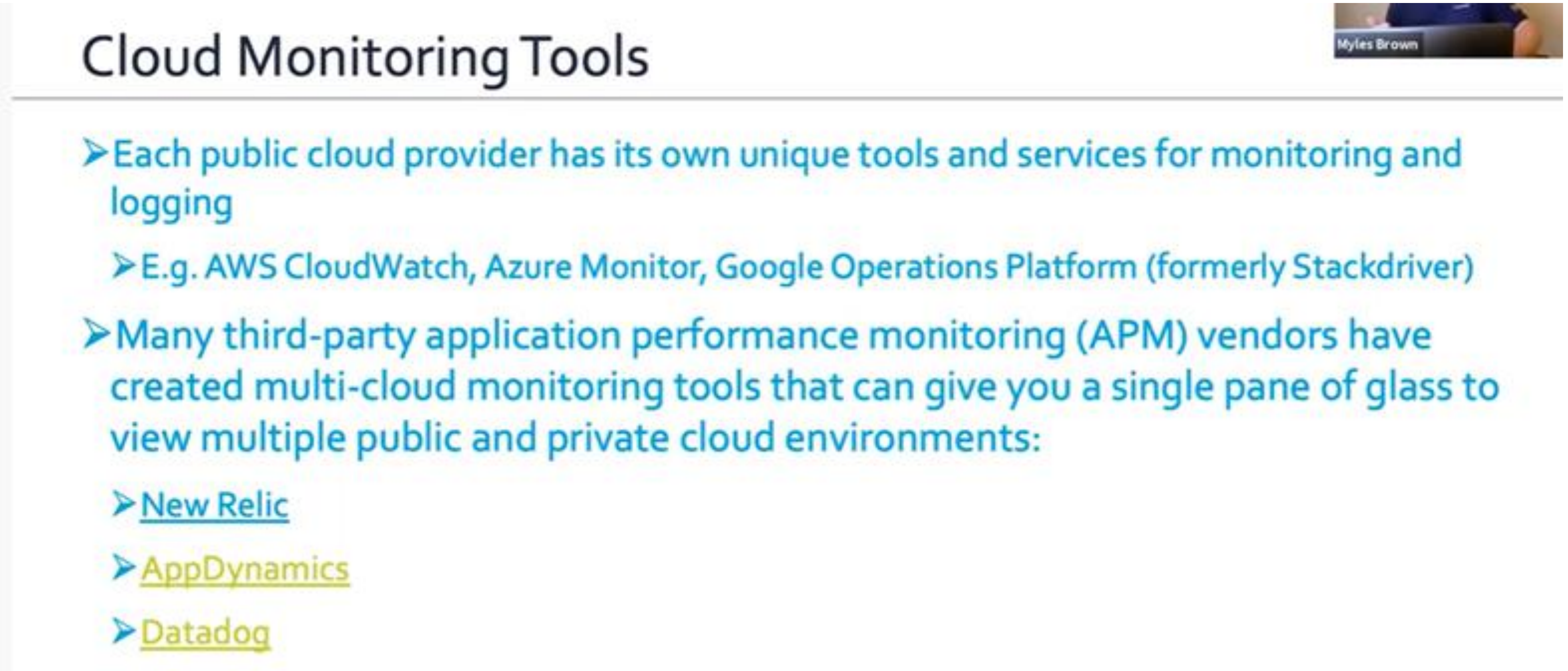
- A. Security will be more challenging as have more surface area to maintain and more architectures for the security team to learn
- B. increase the complexity for single management but for multi cloud

  configuration, deployment, management and monitoring



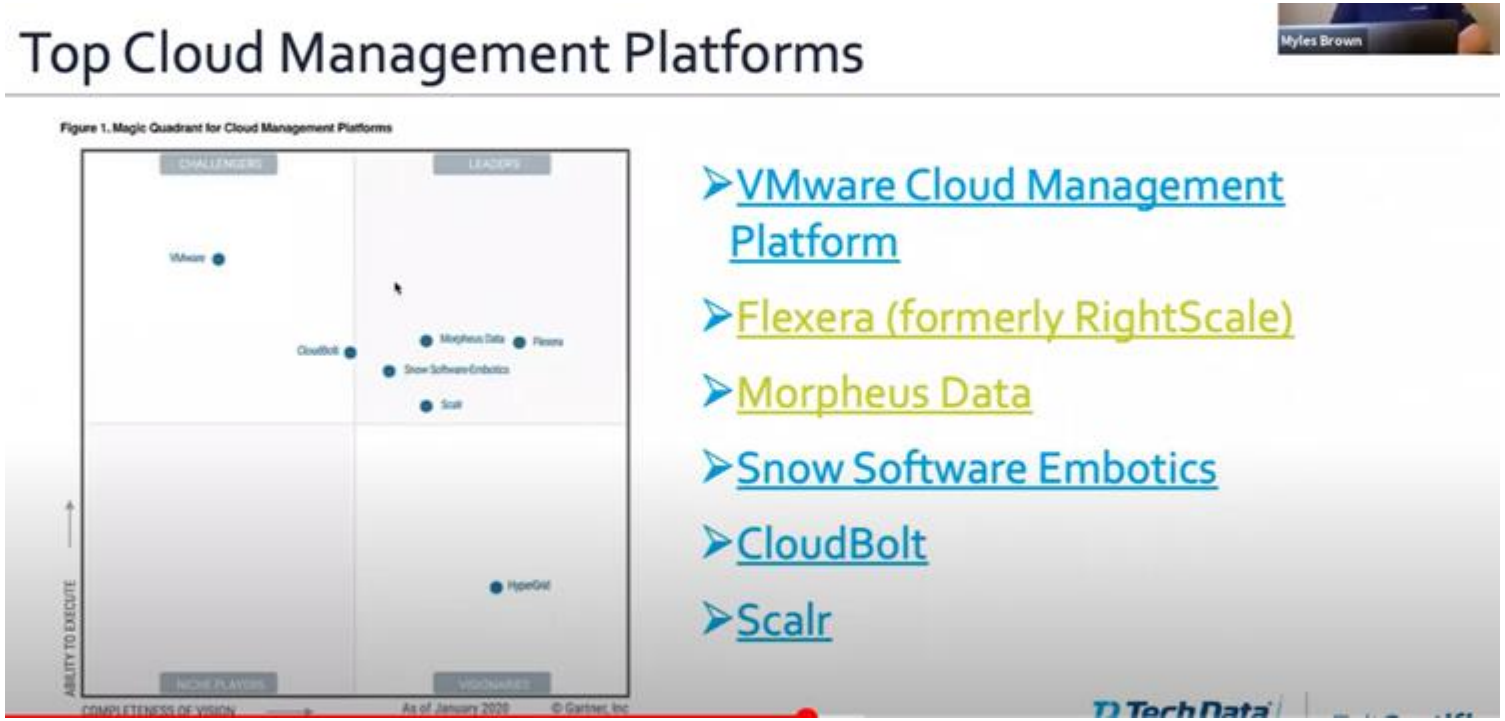
Cloud Provisioning Tools and Frameworks

- Each public cloud provider has its own unique tools and services for provisioning infrastructure
  - E.g. AWS CloudFormation, Azure Resource Manager, Google Cloud Deployment Manager
- There are some cross-platform tools like Ansible and Terraform by HashiCorp, but these tools don't provide a write-once run-anywhere experience
  - This is where containerization and orchestration tools like Docker and Kubernetes make applications easier to move around
  - The public cloud providers all provide managed services for Kubernetes
  - Tools like Spinnaker can deploy to any cloud



Cloud Monitoring Tools

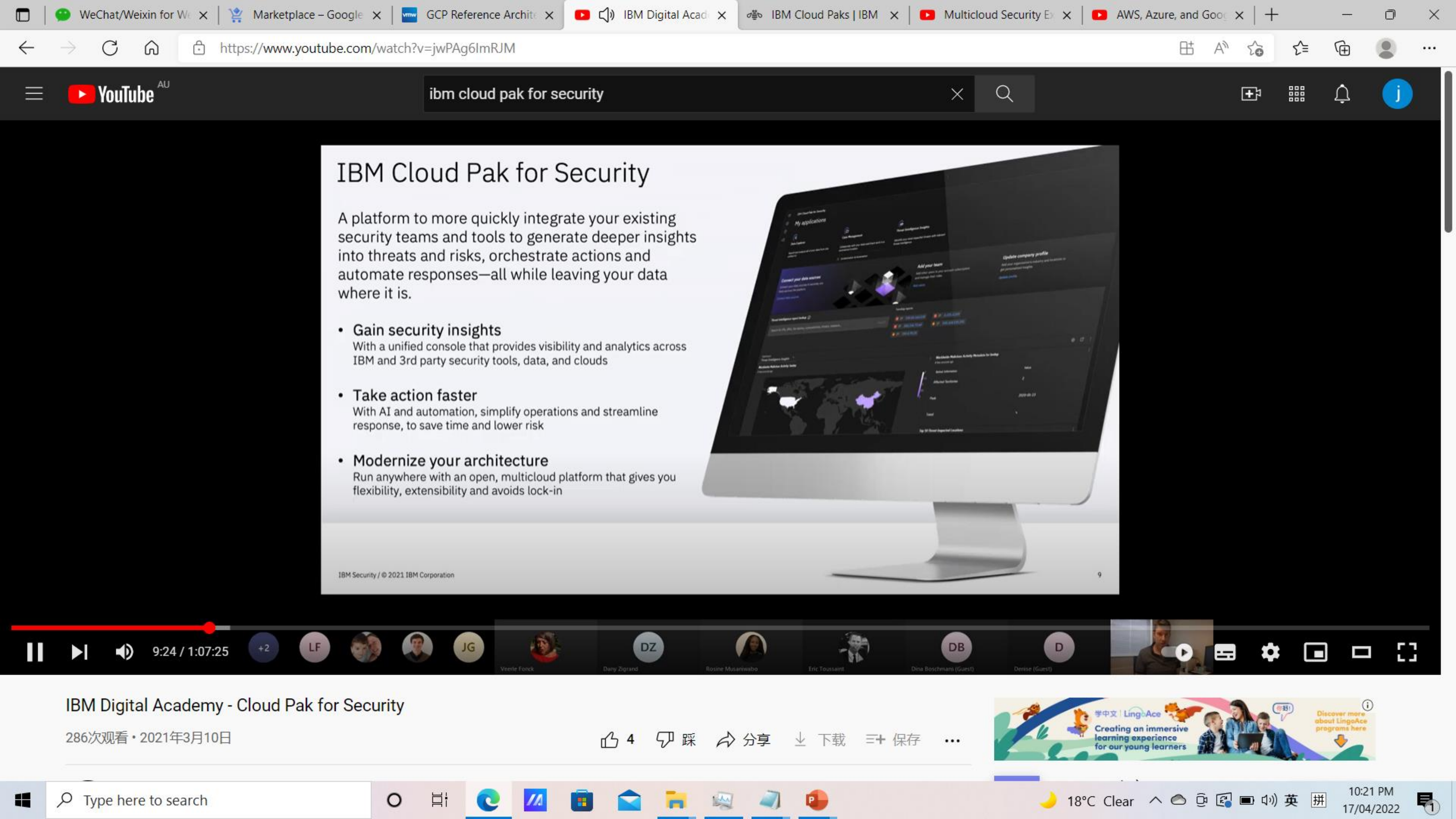
- Each public cloud provider has its own unique tools and services for monitoring and logging
  - E.g. AWS CloudWatch, Azure Monitor, Google Operations Platform (formerly Stackdriver)
- Many third-party application performance monitoring (APM) vendors have created multi-cloud monitoring tools that can give you a single pane of glass to view multiple public and private cloud environments:
  - New Relic
  - AppDynamics
  - Datadog



Top Cloud Management Platforms

Figure 1. Magic Quadrant for Cloud Management Platforms

- ➢VMware Cloud Management Platform
- ➢Flexera (formerly RightScale)
- ➢Morpheus Data
- ➢Snow Software Embotics
- ➢CloudBolt
- ➢Scalr



IBM Cloud Pak for Security

A platform to more quickly integrate your existing security teams and tools to generate deeper insights into threats and risks, orchestrate actions and automate responses—all while leaving your data where it is.

- **Gain security insights**
  With a unified console that provides visibility and analytics across IBM and 3rd party security tools, data, and clouds
- **Take action faster**
  With AI and automation, simplify operations and streamline response, to save time and lower risk
- **Modernize your architecture**
  Run anywhere with an open, multicloud platform that gives you flexibility, extensibility and avoids lock-in

IBM Security / © 2021 IBM Corporation

9

IBM Digital Academy - Cloud Pak for Security

286次观看 • 2021年3月10日

Improving Multi Cloud Security

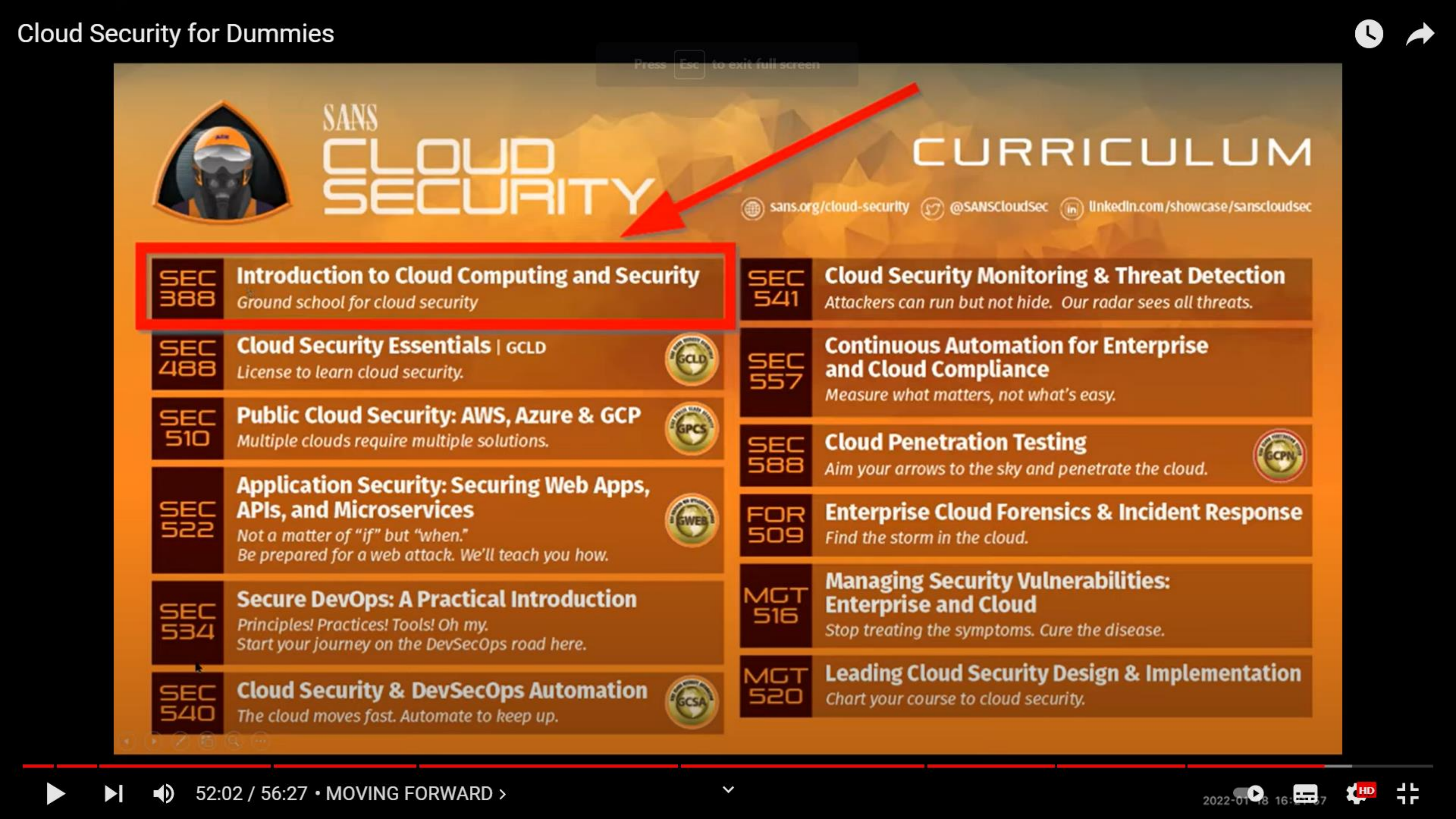
- 1. Synchronize Policies
- 2. Tailor Security Policies to Services
- 3. Automate Security
- 4. Consolidate Monitoring
- 5. Compliance Across Clouds

Multi-Cloud workload protection platform (CWPP) and cloud security posture management (CSPM)

- **Cross-environment segmentation**—Aqua provides a container firewall that segments workloads within the same environment or across clouds, preventing attacks from spreading, the spread of attacks, without interfering with cloud deployments.
- **Multi-tenancy control and security**—Aqua can manage multiple team deployments or customer tenancies from a central console. It maintains separation of data and access, ensuring complete isolation between tenants.
- **Scanning images and functions**—Aqua scans container images and serverless functions for known vulnerabilities, embedded secrets, OSS licensing issues, malware, and configuration issues before they are deployed.
- **Protect serverless workloads**—Aqua protects serverless environments such as AWS Fargate and Azure Container Instances, from a single console with consistent policy enforcement.
- **Infrastructure Security** — Aqua Cloud Security Posture Management (CSPM) provides scanning, monitoring, and remediation of configuration issues in public cloud accounts.
- **Multi-Cloud Visibility**—Aqua CSPM continually audits cloud accounts for security risks and misconfigurations across hundreds of configuration settings and compliance best practices to enable consistent, unified multi-cloud security.
- **Rapid Remediation of Misconfigurations**—Aqua provides self-securing capabilities to ensure cloud accounts do not drift out of compliance and delivers detailed, actionable advice and alerts, or choose automatic remediation of misconfigurations with granular control over chosen fixes.
- **Enterprise Scale**—Aqua supports hundreds of cloud accounts using an extensible plugin architecture. It is also API/Cloud Dev friendly, uses SSO with SAML 2.0 and integrates with many popular productivity tools.

- What is Multi-Cloud and How Does It Affect Security? | F5 Labs
- **Cloud Workload Protection Platforms (CWPP)** for reviewing server security configurations on cloud systems, and **Cloud Security Posture Management (CSPM)** for inventory and compliance testing. Another tool, **Cloud-Native Application Protection Platform (CNAPP)** combines the functionality of CWPP and CSPM. There are other specialized tools for reviewing the security of CaaS configurations such as **Kubernetes Security Posture Management (KSPM)**
- CNAPP, CSPM, CWPP; What’s the Difference and How Can They Improve My Cloud Security? – YouTube
- cloud application security brokers (CASB), cloud security posture management (CSPM), cloud application workload protection platforms (CWPP), cloud infrastructure entitlement management (CIEM)

- Enable security and automated continuous compliance using CloudGuard from AWS Marketplace | AWS Marketplace (amazon.com)



Cloud Security for Dummies

SANS CLOUD SECURITY CURRICULUM

sans.org/cloud-security @SANSCloudSec linkedin.com/showcase/sanscloudsec

SEC 388	**Introduction to Cloud Computing and Security** *Ground school for cloud security*
SEC 488	**Cloud Security Essentials** | GCLD *License to learn cloud security.*
SEC 510	**Public Cloud Security: AWS, Azure & GCP** *Multiple clouds require multiple solutions.*
SEC 522	**Application Security: Securing Web Apps, APIs, and Microservices** *Not a matter of "if" but "when."* *Be prepared for a web attack. We'll teach you how.*
SEC 534	**Secure DevOps: A Practical Introduction** *Principles! Practices! Tools! Oh my.* *Start your journey on the DevSecOps road here.*
SEC 540	**Cloud Security & DevSecOps Automation** *The cloud moves fast. Automate to keep up.*
SEC 541	**Cloud Security Monitoring & Threat Detection** *Attackers can run but not hide. Our radar sees all threats.*
SEC 557	**Continuous Automation for Enterprise and Cloud Compliance** *Measure what matters, not what's easy.*
SEC 588	**Cloud Penetration Testing** *Aim your arrows to the sky and penetrate the cloud.*
FOR 509	**Enterprise Cloud Forensics & Incident Response** *Find the storm in the cloud.*
MGT 516	**Managing Security Vulnerabilities: Enterprise and Cloud** *Stop treating the symptoms. Cure the disease.*
MGT 520	**Leading Cloud Security Design & Implementation** *Chart your course to cloud security.*

Press Esc to exit full screen
GCLD
GPCS
GWEB
GCSA
GCPN
52:02 / 56:27 • MOVING FORWARD ›
HD
2022-01-18 16: