RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: CSV-R09

Untangling SaaS Security in the Enterprise

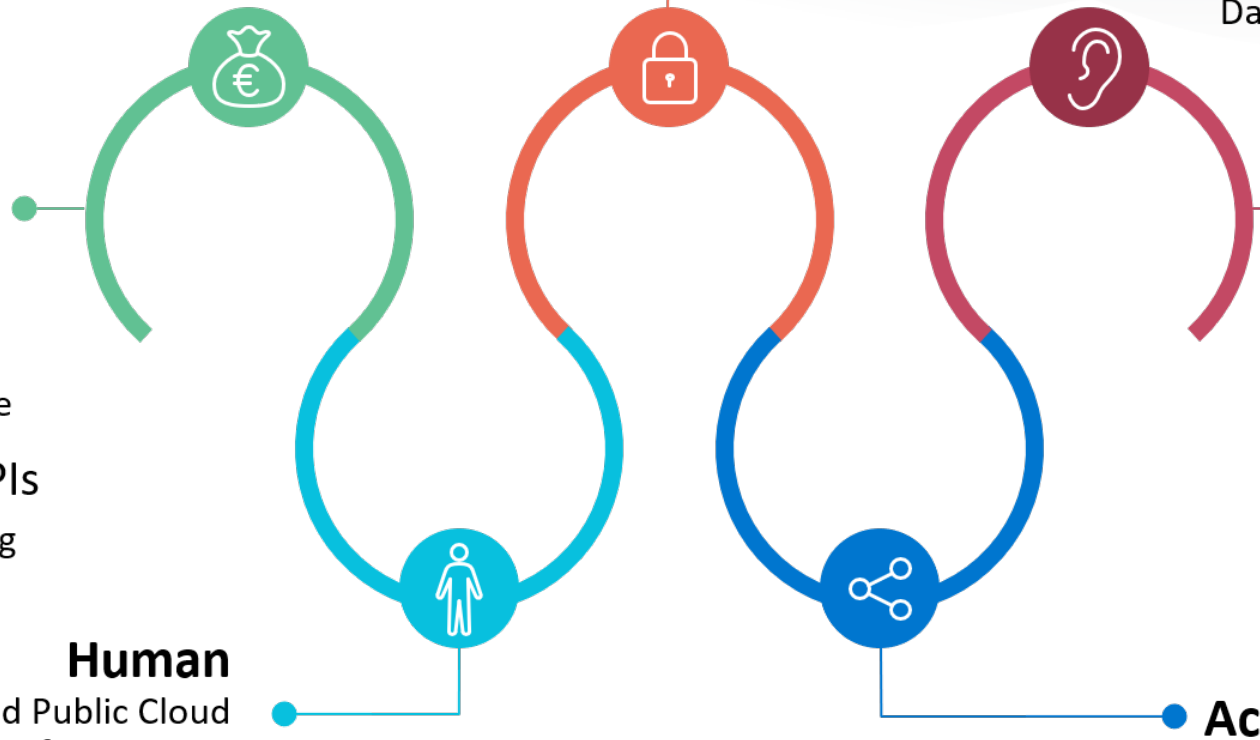
Rehman Khan

Director, Cloud & Data Security
TD Ameritrade
https://www.linkedin.com/in/rehmankhan/
@cryptorak

Brajesh Moni

Sr. Security Consultant, Cloud & Data Security
TD Ameritrade
https://www.linkedin.com/in/brajeshmoni/

Public Cloud Security Threats



Exposure
Sensitive Data Shared Publicly

Theft
Data Exfiltration Via Unmanaged Cloud

Disruption
Hybrid Threats That Use Cloud & Web

Unauthorized Access
- Account compromise

Insecure Interfaces/APIs
- External Data Sharing
- Malicious Insider

Human
Misconfigured Public Cloud Infrastructure

Access
Download To Personal Device

Misconfiguration of Cloud Platform Setup
- Malware Infections
- Data Exposure
- Vulnerability Exploitation

Public Cloud Business Drivers

- Disrupt legacy competitors using public cloud economy of scale
- Rapid businesses pace & agility due to competition

- Acquisitions continue to pressure the markets demanding agility
- Aspirations of social integration, digital innovation, agility, and scale rapidly
- Access to information anywhere from any device by authorized users

- Developers wanting to experiment IOT, AI, Analytics, and APIs
- Innovation focus to transform business and technology foot print

Enterprise SaaS Expansion

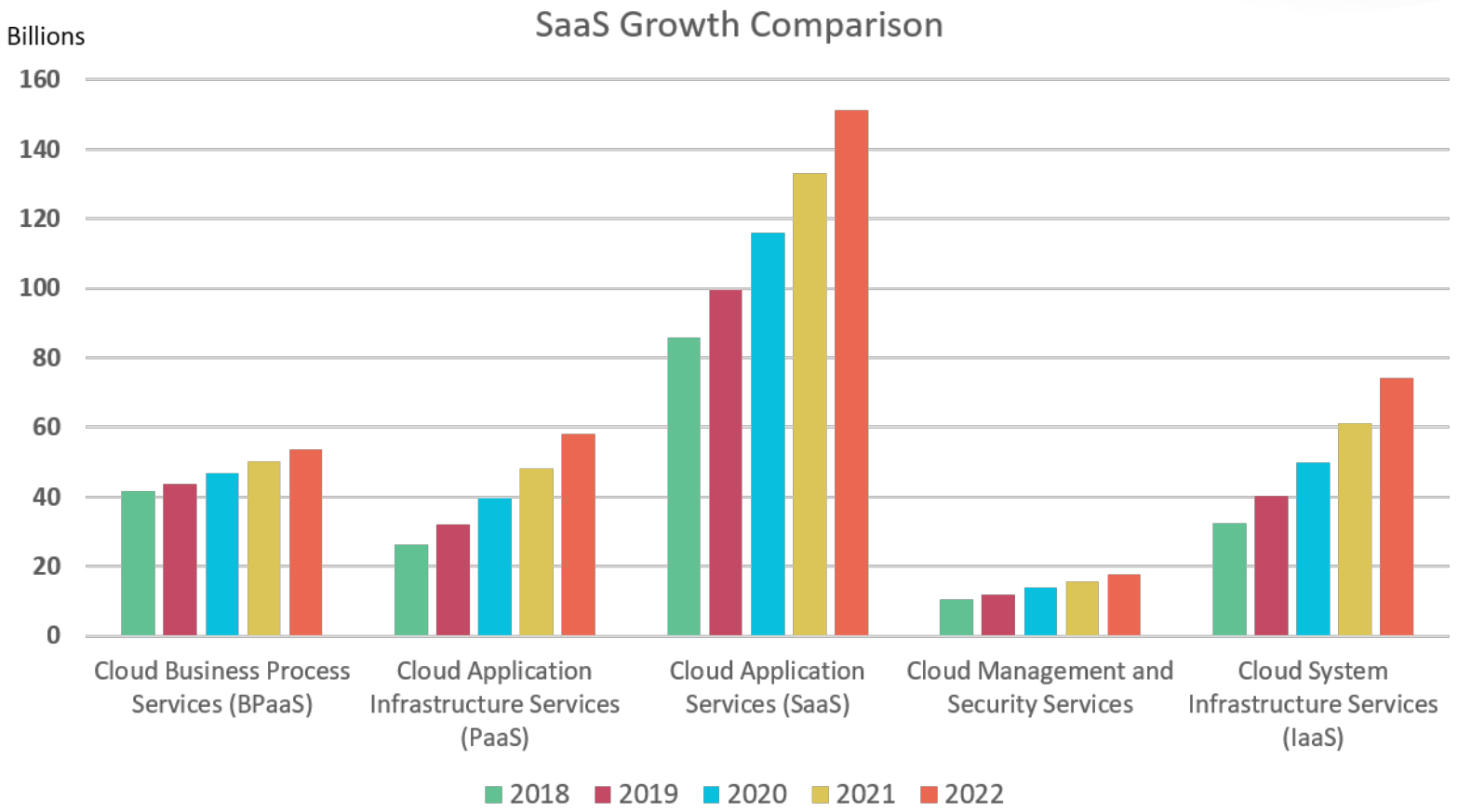
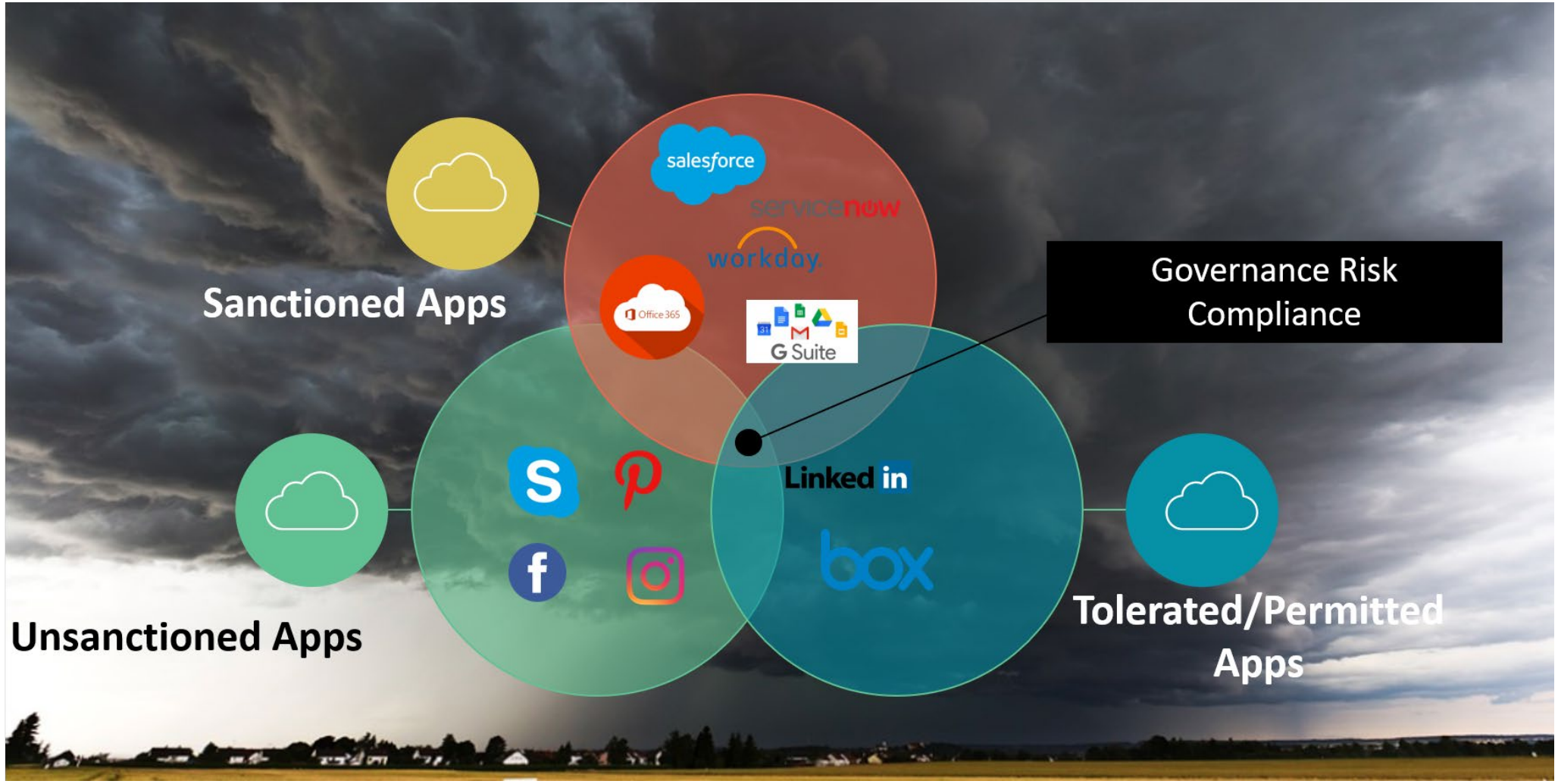


Table 1. Worldwide Public Cloud Service Revenue Forecast (Billions of U.S. Dollars)

	2018	2019	2020	2021	2022
Cloud Business Process Services (BPaaS)	41.7	43.7	46.9	50.2	53.8
Cloud Application Infrastructure Services (PaaS)	26.4	32.2	39.7	48.3	58.0
Cloud Application Services (SaaS)	85.7	99.5	116.0	133.0	151.1
Cloud Management and Security Services	10.5	12.0	13.8	15.7	17.6
Cloud System Infrastructure Services (IaaS)	32.4	40.3	50.0	61.3	74.1
Total Market	**196.7**	**227.8**	**266.4**	**308.5**	**354.6**

https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020

What is the SaaS Security Problem ?



Public Cloud Security Program

Cloud Foundational Security
Establishing the foundational security controls for SaaS and IaaS-PaaS public cloud services (Azure, AWS and GCP)

Security Solution Deployment
Engineering and operationalizing required platform security tooling (CASB, CWPP, and CSPM)

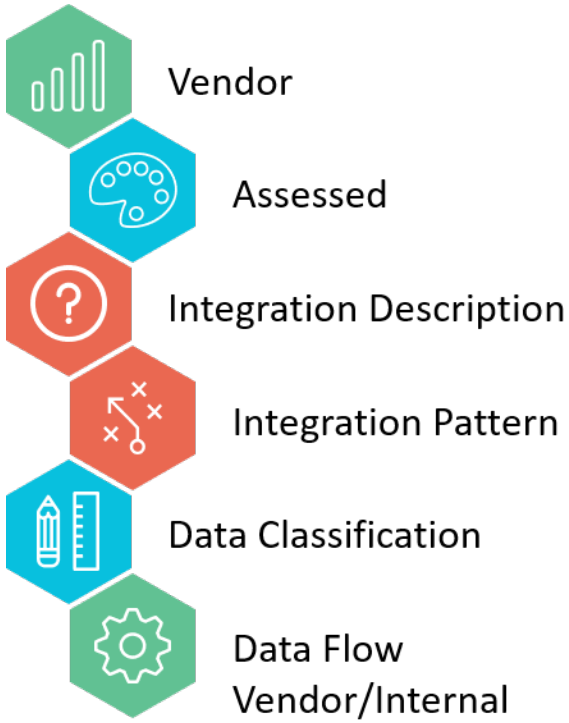
Cloud Project Engagement
Establishing security requirements for SaaS and public cloud initiatives to ensure secure by design principles

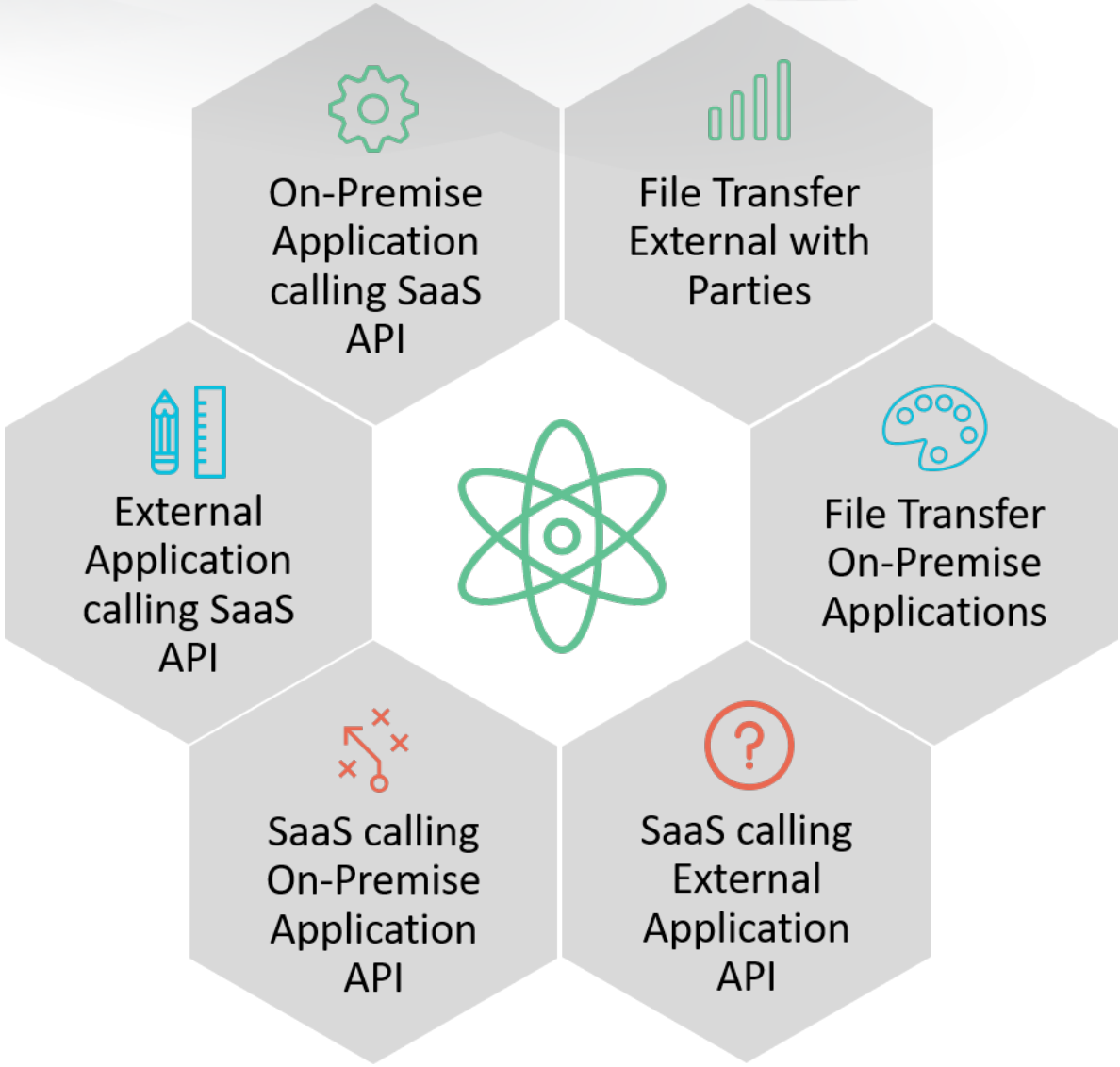
Cloud Risk Management
Identifying, scoring and reporting risk for SaaS and public cloud initiatives

Security Automation
Deploying security controls as code through CI/CD and agile principles

Research & Development
Investing in innovation, and continuous education on new cloud technologies and addressing emerging risk

Data Security Is Key !





Cloud Security SaaS Engagement Model

Vendor Management

Build relationship with vendor assessment and procurement team

Cloud Security

Introduce cloud security assessment questionnaire to SaaS vendors based on cloud security standards

Business Engagement

Identify and build trust relationships with innovation teams, business areas that are experimenting with SaaS applications

Communicate Proactively

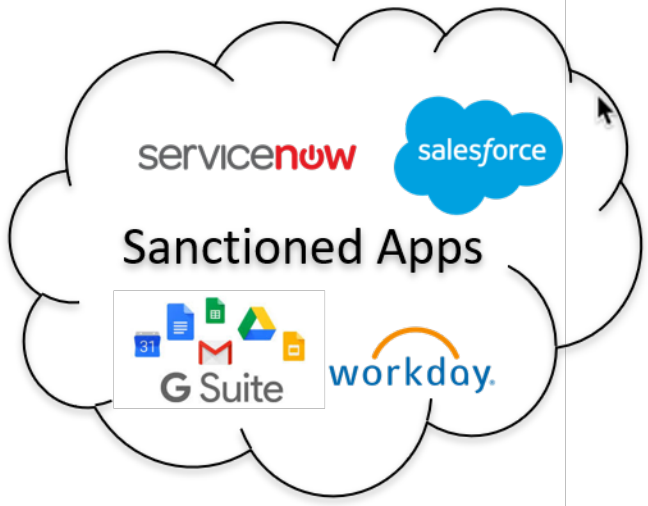
Monthly cloud security tech talks
Cloud security immersion day
Create a collaborative channels for innovators and developers

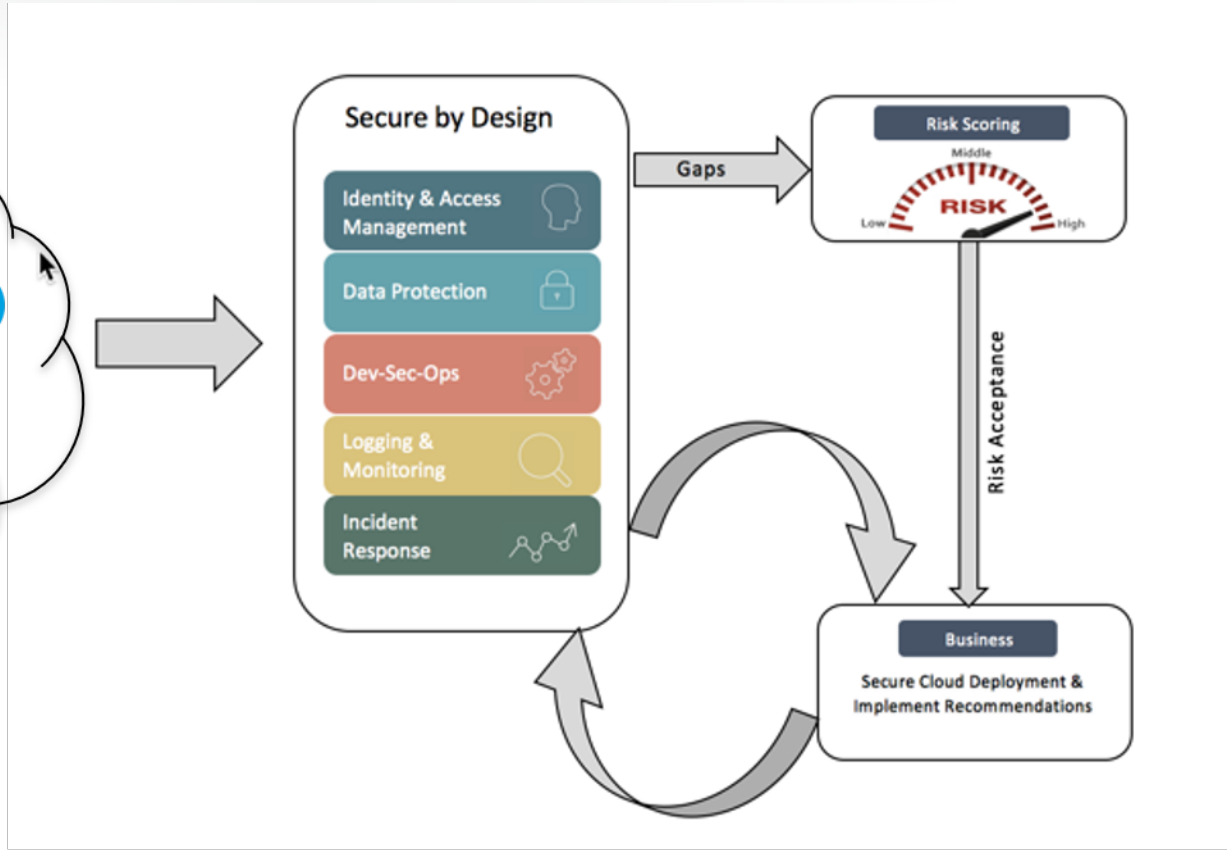
Cloud Risk Management Process

Compliance & Regulatory Requirements

Industry Best Practices Enterprise Security

SaaS Security
Secure coding
Framework
Platform

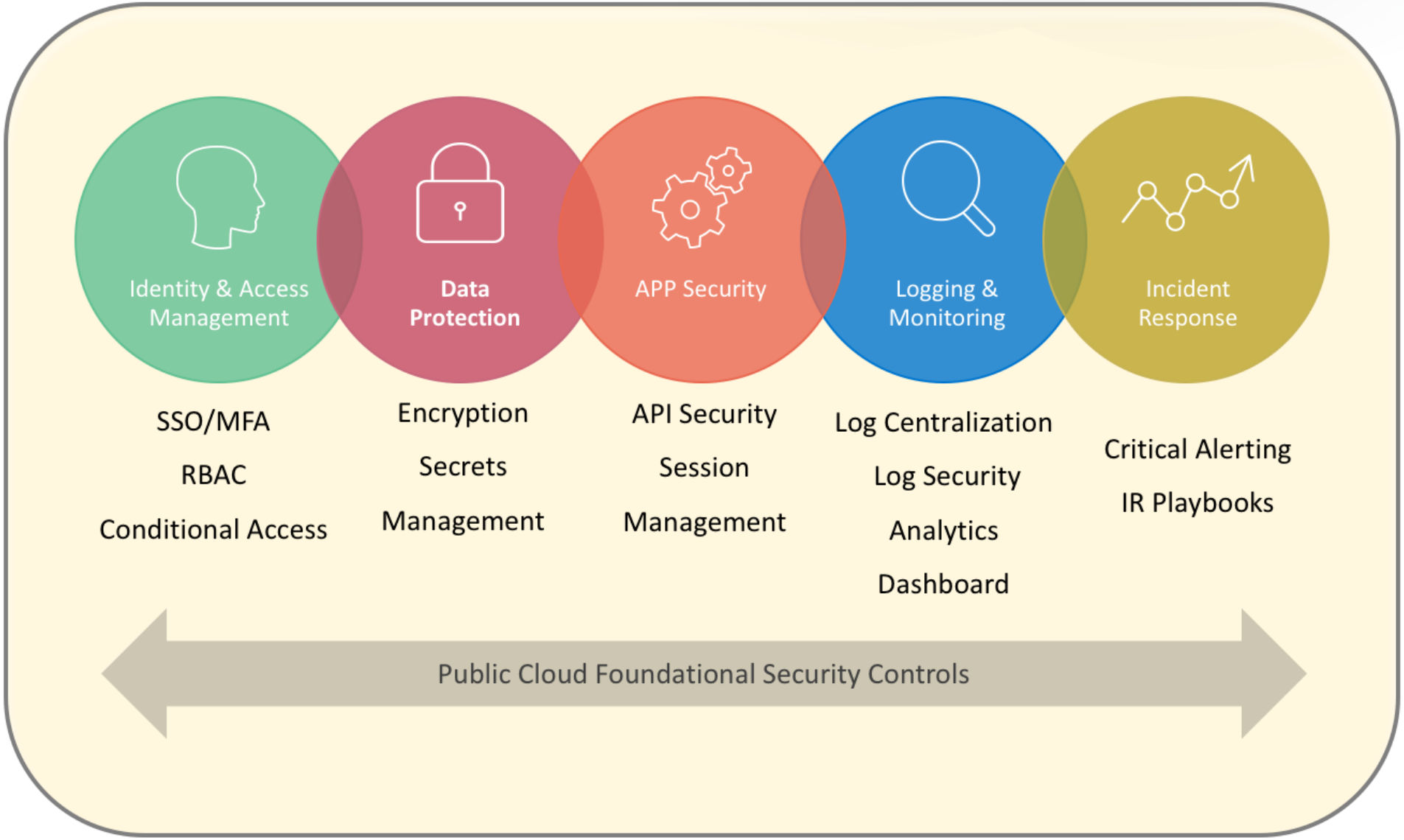




RSAConference2020

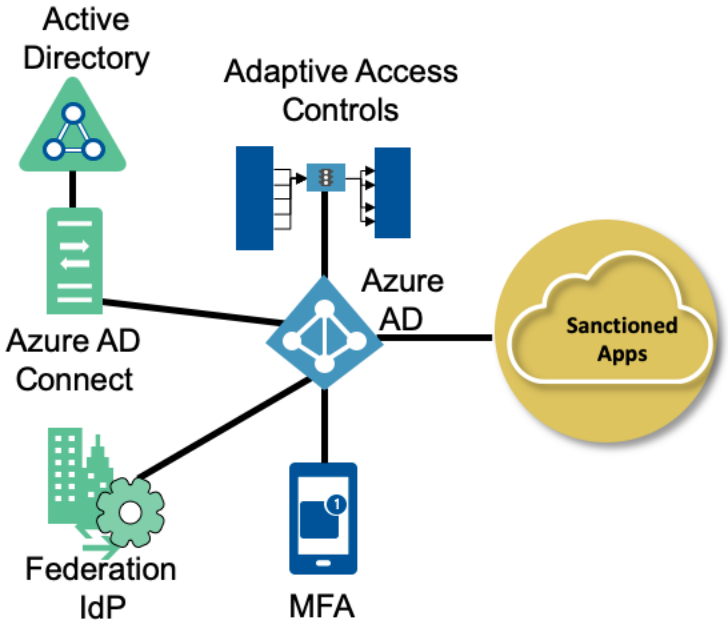
Foundational Cloud Security Controls

Foundational Cloud Security Controls

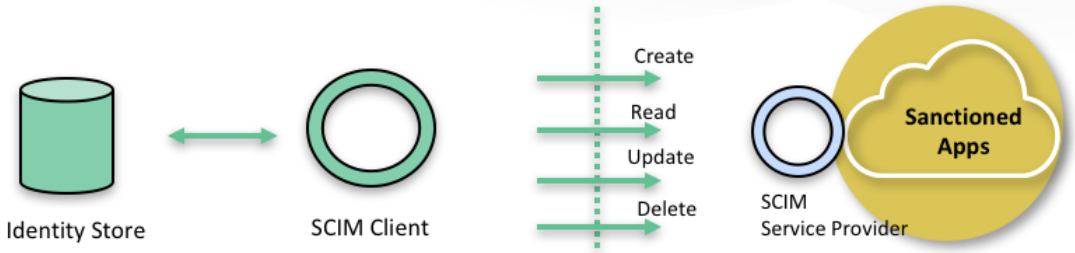


Foundational Cloud Security Controls - IAM

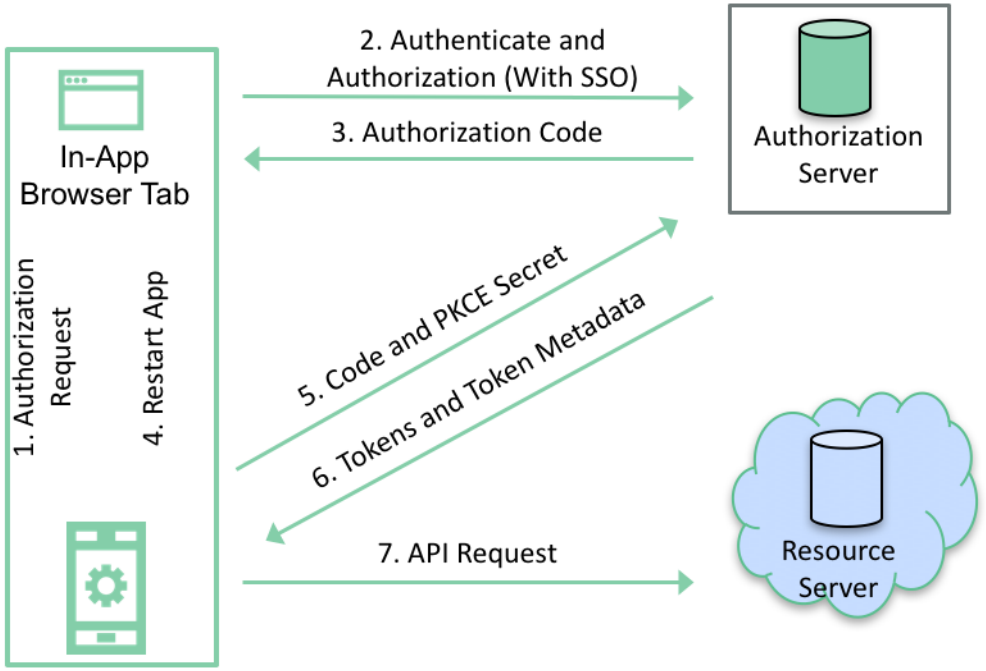
AuthN - SSO,SAML, OpenID



Standardized Provisioning — Without Custom Connectors



AuthZ – OAuth 2.0



Foundational Cloud Security Controls – Data Protection

Data Protection

Proxy Encryption

Managed Devices

Name	Phone Number
Bryan	111-111-1111
Boss	222-222-2222
Victor	333-333-3333

File Encryption/EDRM

CASB

File Encryption/EDRM

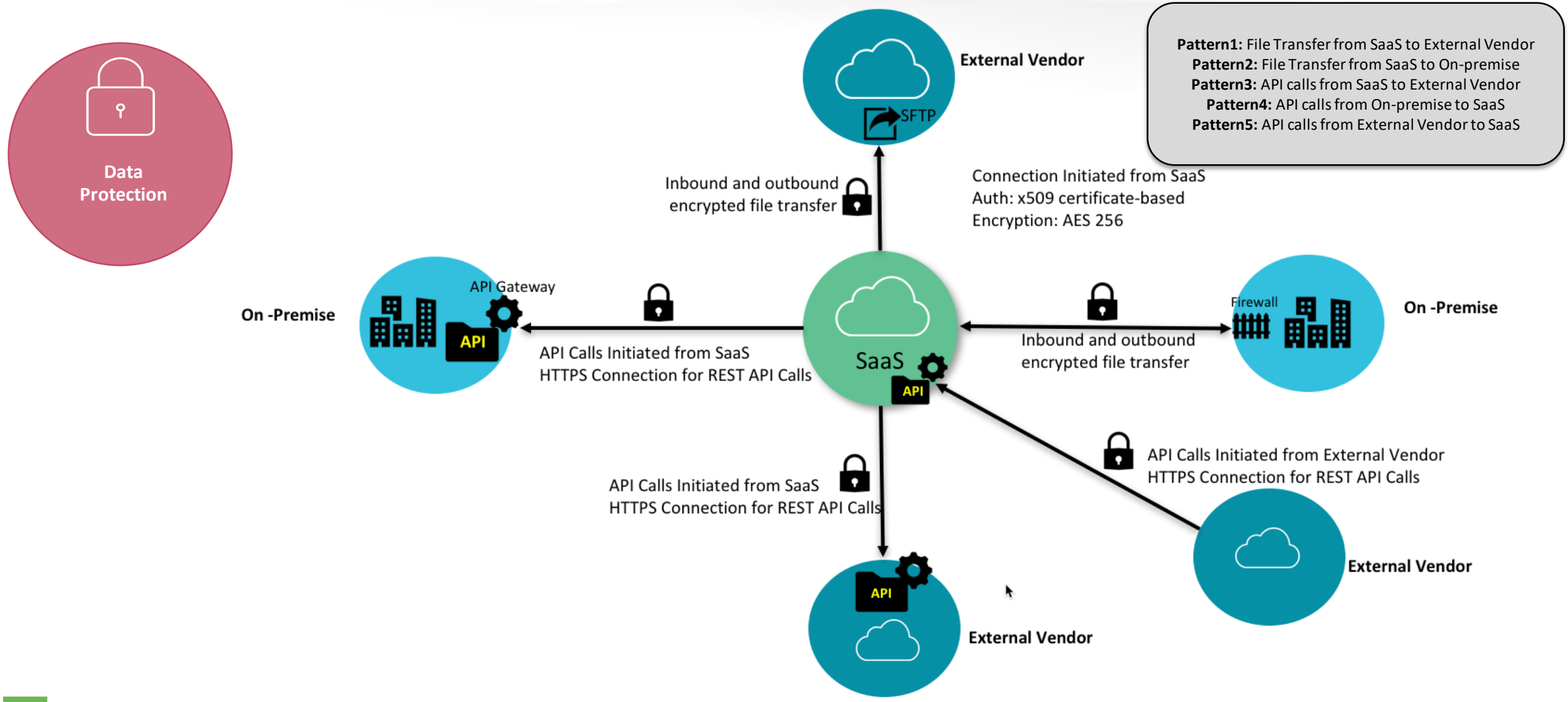
BYOK

Encrypt or Tokenize Fields/Files

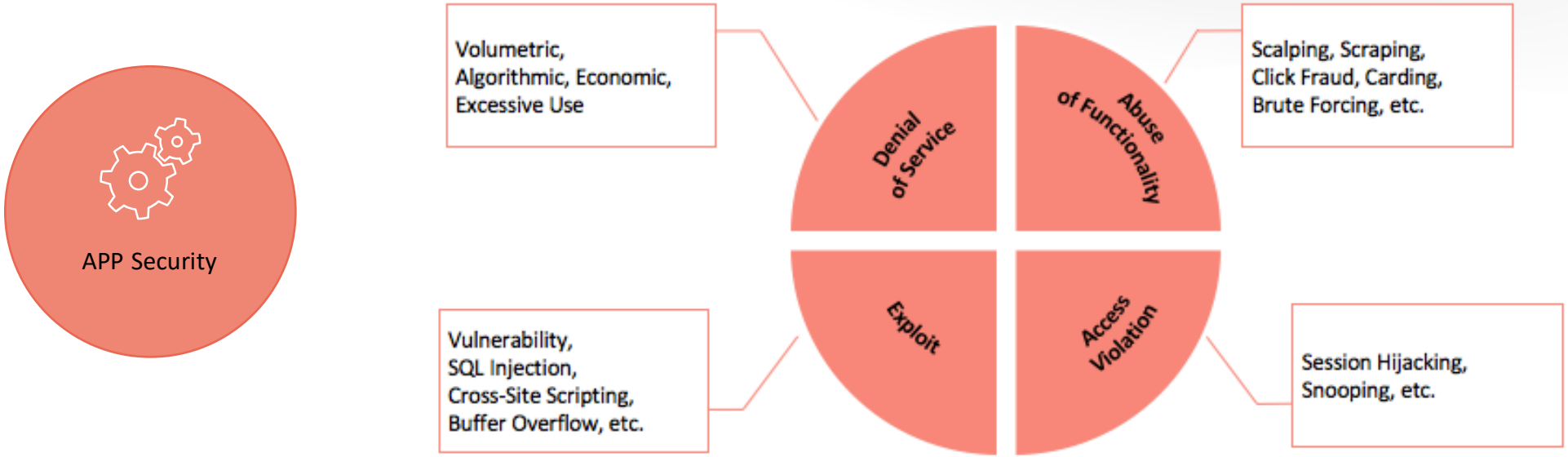
SaaS

Name	Phone Number
DqAZjFc	A40fRhhGmQi1
YP8X8g4	aP1i77rNmP6d
+zHeuU	BpfwCDWQ=

Data Integration Secure Patterns



Foundational Cloud Security Controls – App Security



Risk

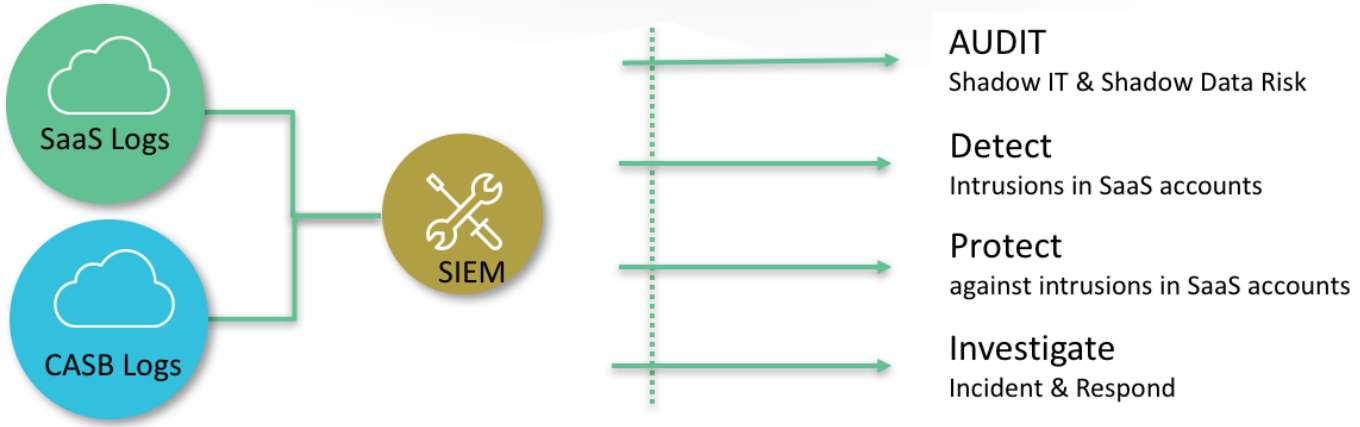
- Access Token Misuse
- Insecure Transmission
- Third party insecure app implementation

Application Security Requirements

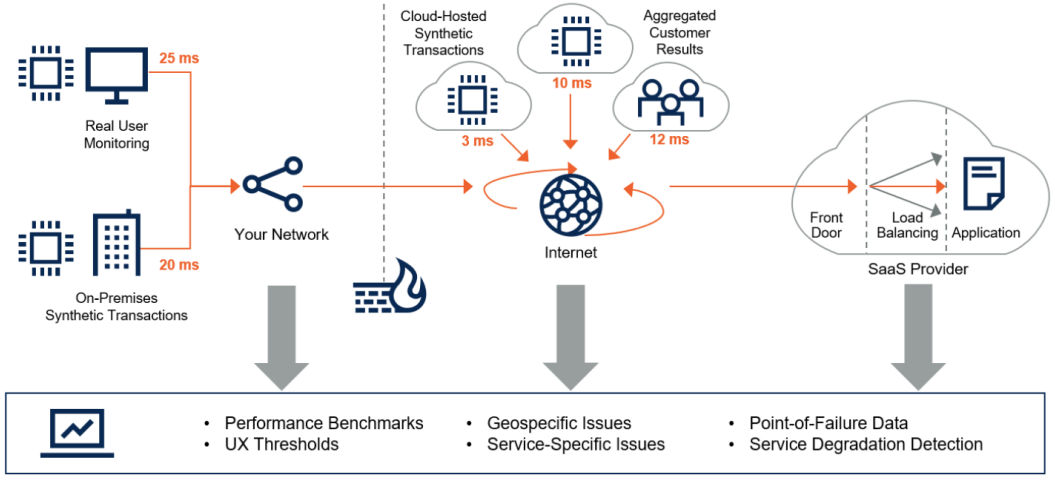
- Secure handling of Access token
- Storage of sensitive Information
- Secure Rest API Implementation
- API access rate/traffic management
- Session Management

Foundational Cloud Security Controls – Logging & Monitoring

SaaS Logging



SaaS Monitoring



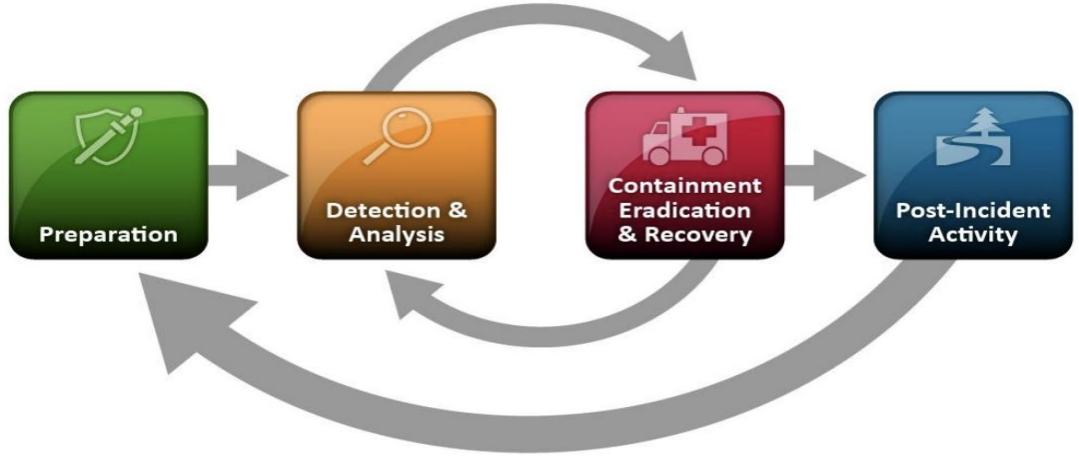
- Centralize & Ingest SaaS cloud Log Data
- Explore the data – for critical operational & security insight.
- Enable native logging and monitoring

Source: Gartner

Foundational Cloud Security Controls – Incident Response

Engage Incident Response team

- Engage SaaS operation team and provide visibility to IR team.
- Establish a joint response plan with the SaaS provider.
- IR team to evaluate the monitoring controls and security measures that are in place for SaaS provider.
- Define alerts, security events categorize & score risk events.
- Update IR playbook.
- Build Recovery Plan.



Source: NIST 800-61

Foundational Cloud Security Controls - Takeaways

Identity & Access Management

- Formalize standards and process for AuthN/AuthZ with SaaS services. [SCIM, SAML, Oauth, OpenID]
- Enable MFA – Send MFA status as an attribute when using federated Auth.
- Privileged Identities – Vaulted, should use MFA always.

Data Protection

- Data Classification, Data Lifecycle, Data Location/Residency
- Encryption Engine – Provider Managed Encryption, Proxy Encryption
- Key management – Customer managed, Provider Managed. – Have control of the key all the time

App Security

- Secure handling of Access token
- Storage of sensitive Information
- Secure Rest API Implementation
- API access rate/traffic management
- Session Management

Logging

- Centralize & Ingest SaaS cloud Log Data
- Explore the data – for critical operational & security insight.
- Enable native logging and monitoring

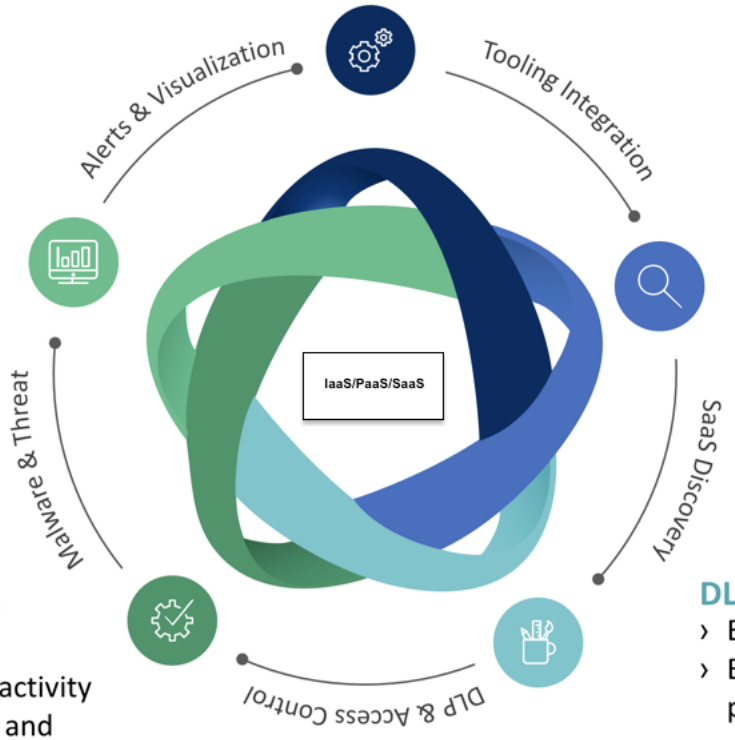
Incident Response

- IR team to evaluate the monitoring controls and security measures that are in place for SaaS provider
- Define alerts, security events categorize & score risk events.
- Update IR playbook
- Build Recovery Plan.

Cloud Access Security Broker - CASB

Integration
› Integrate with existing SIEM, IDP, MFA, web proxy tool sets.

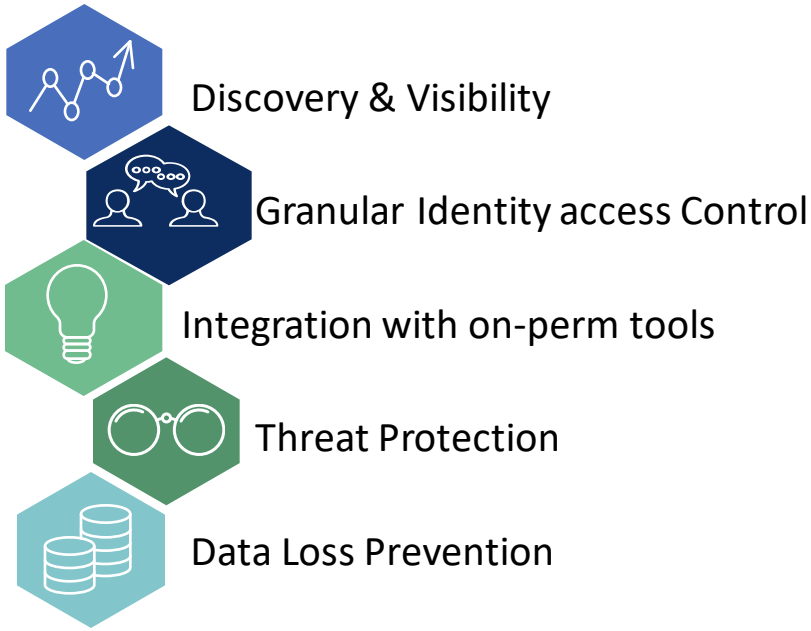
Alerting & Reporting
› Identify and alert on potential data leakage & risky user behavior



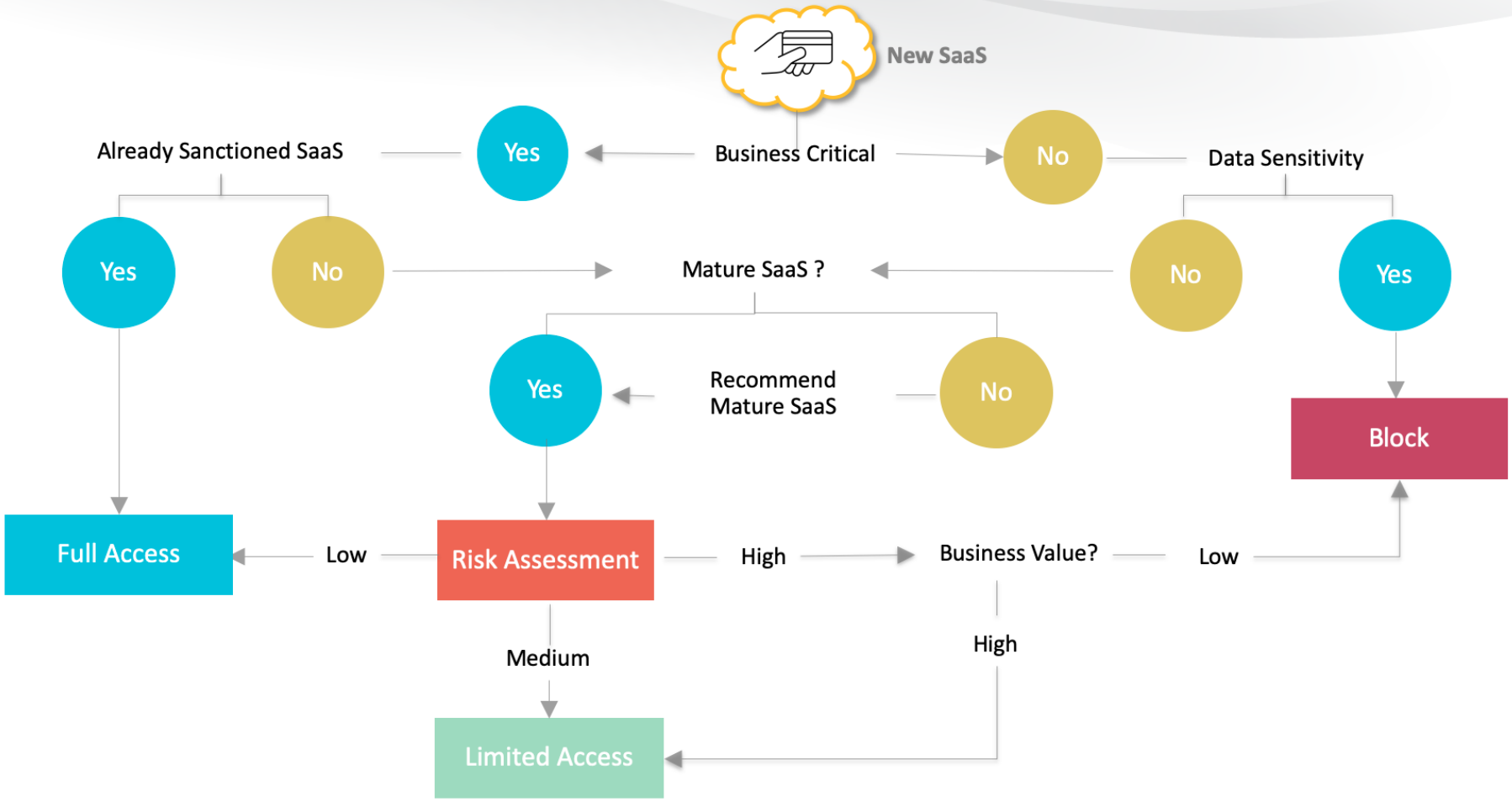
Discovery
› Provides identification and visibility of SaaS app usage from proxy logs

Threat Protection
› Extend ATP to cloud services
› Identify anomalous activity like bulk downloads and impossible travel events

DLP & Conditional Access
› Extend DLP to cloud services
› Enforce conditional access policies



Enterprise SaaS Sanction Process



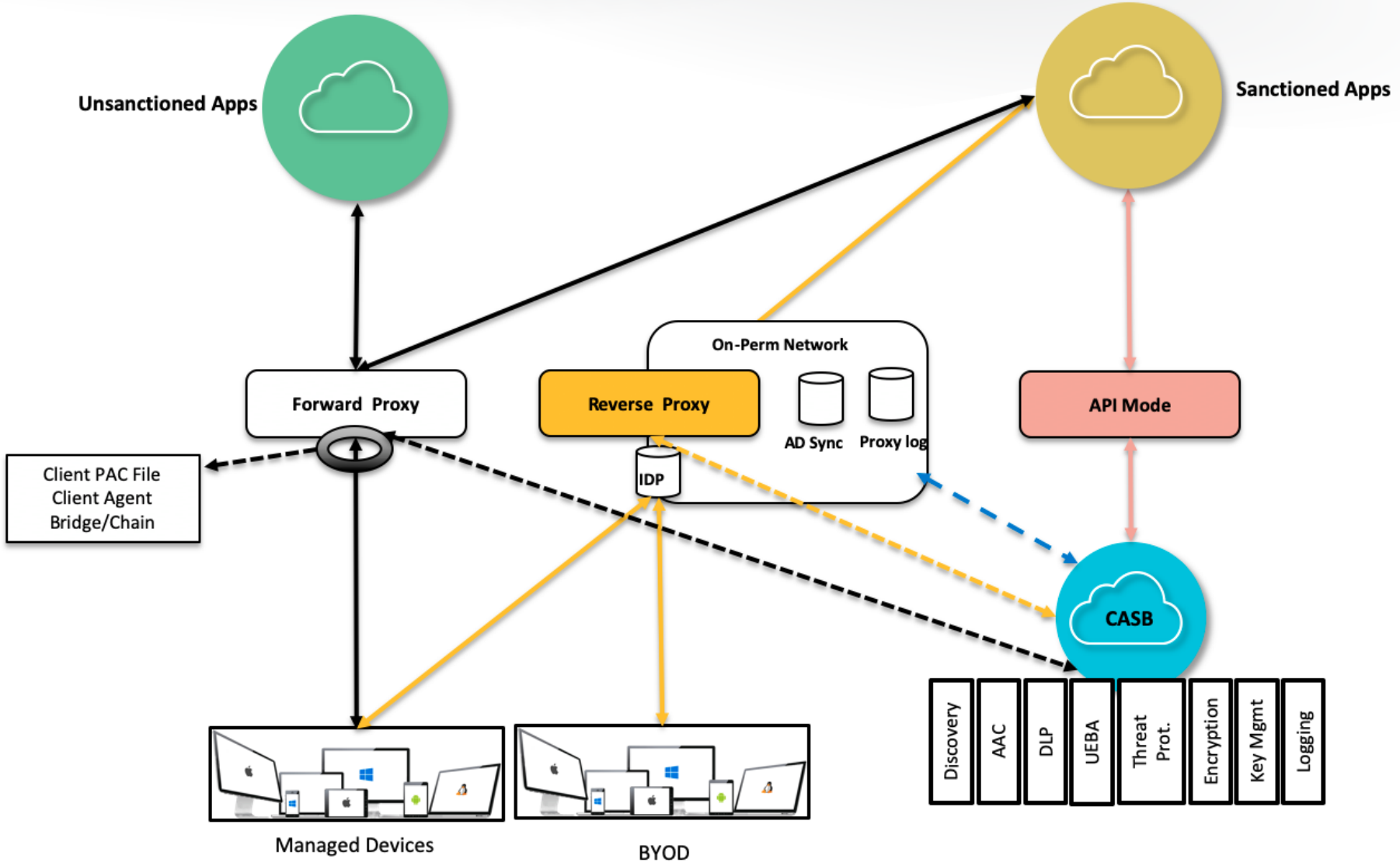
Business Critical

Data Sensitivity

Risk Assessment

Business Value

CASB Architecture and Capabilities

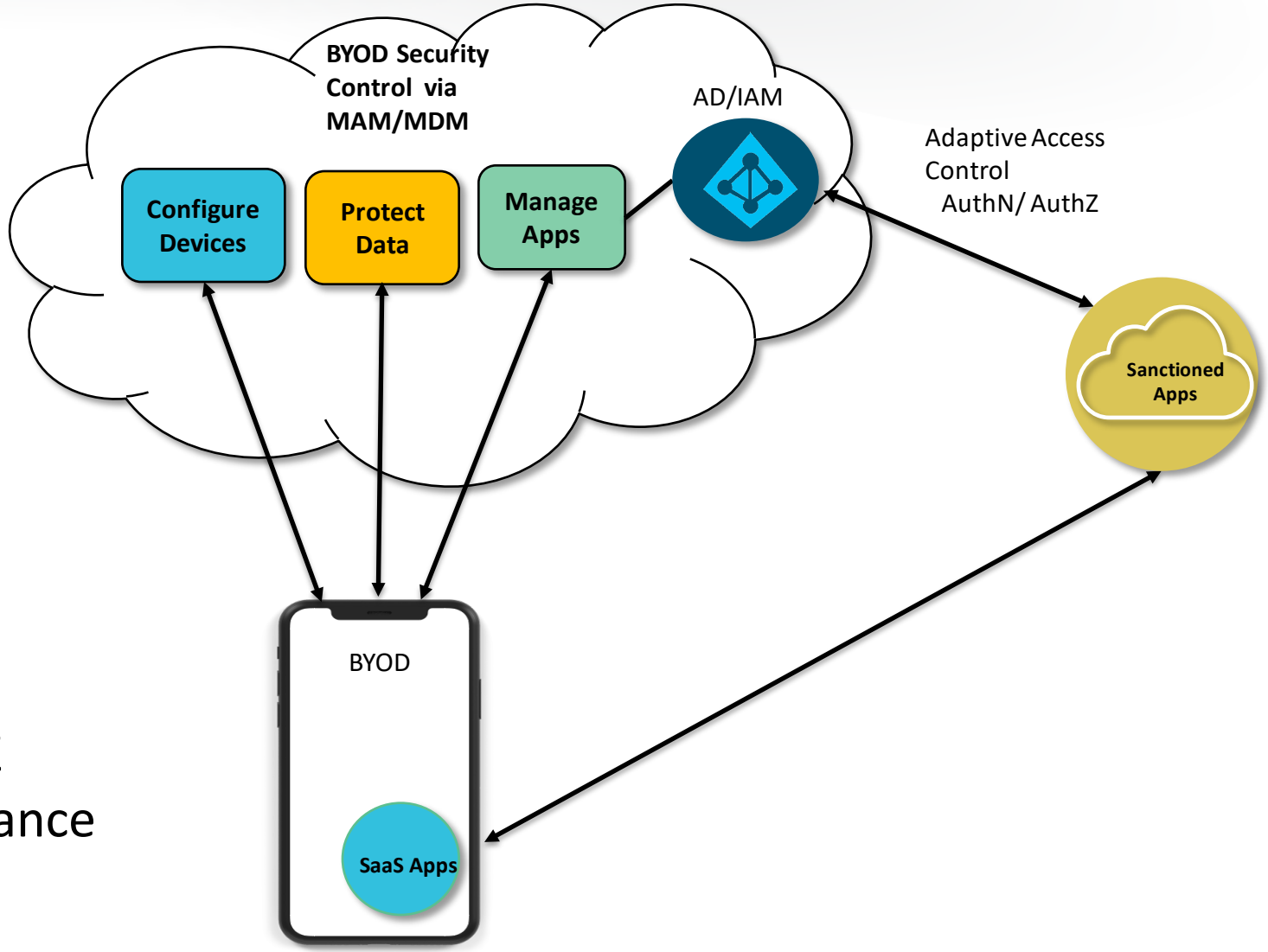


CASB Architecture and Capabilities – Summary Grid

#	CASB Capabilities	Unmanaged Endpoints	Managed Endpoints			
		Sanctioned SaaS	Sanctioned SaaS			Unsanctioned SaaS
		API Mode	Forward Proxy	Reverse Proxy	API Mode	Forward Proxy
1	Discovery	✗	✓	✓	✗	✓
2	DLP – Real Time Monitoring & Enforce on Read	✓	✓	✓	✓	✓
3	Threat Protection [Malware Defense]	✓	✓	✓	✓	✓
4	Pre-Cloud Encryption and Tokenization	✗	✓	✓	✗	✓

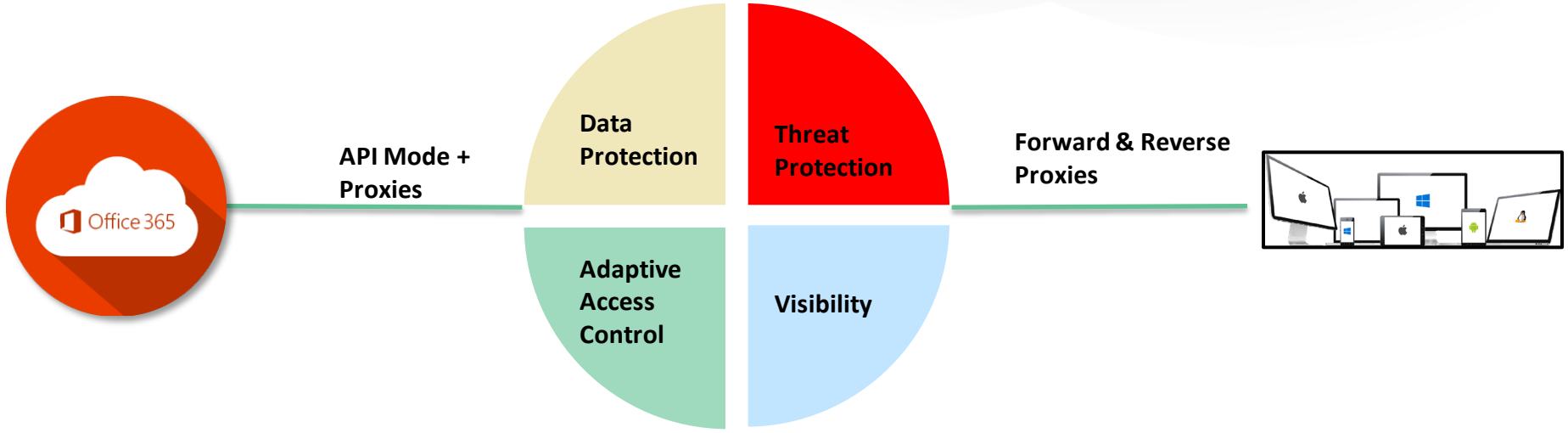
Establish Strong BYOD Controls

- Data Protection
- Data Isolation
- Device Integrity
- Identity AuthN/AuthZ
- Monitoring of compliance



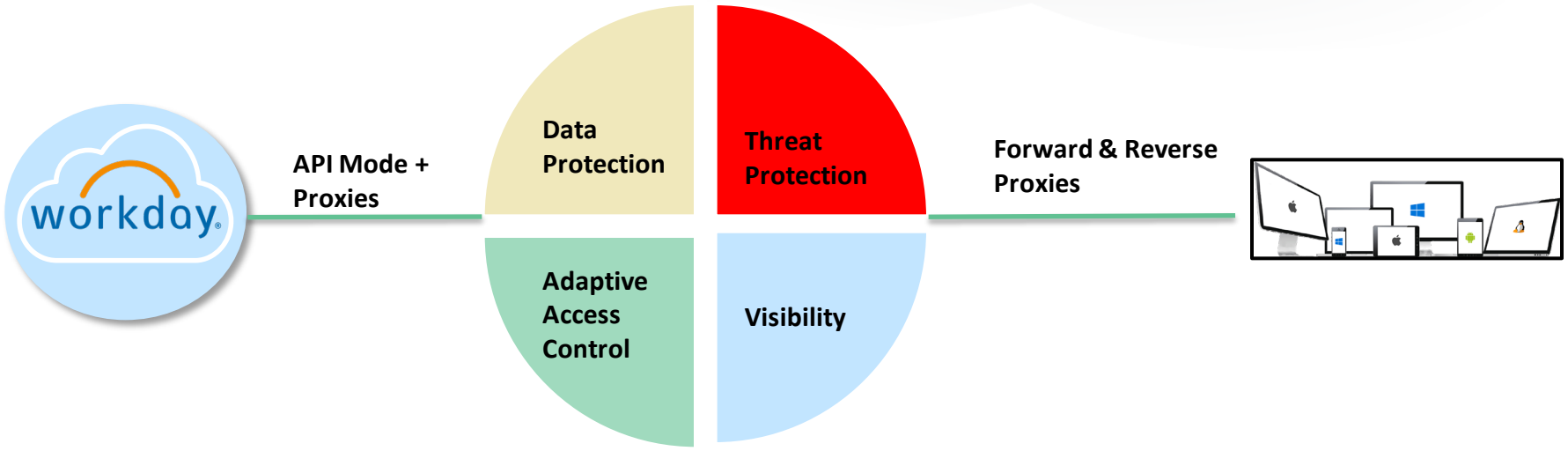
Untangling SaaS Security in the Enterprise

Use Cases: CASB – Office 365



- Adaptive Access Control
- Data Loss Prevention
- Malware Advanced Threat Protection
- User Behavior Analytics
- BYOK

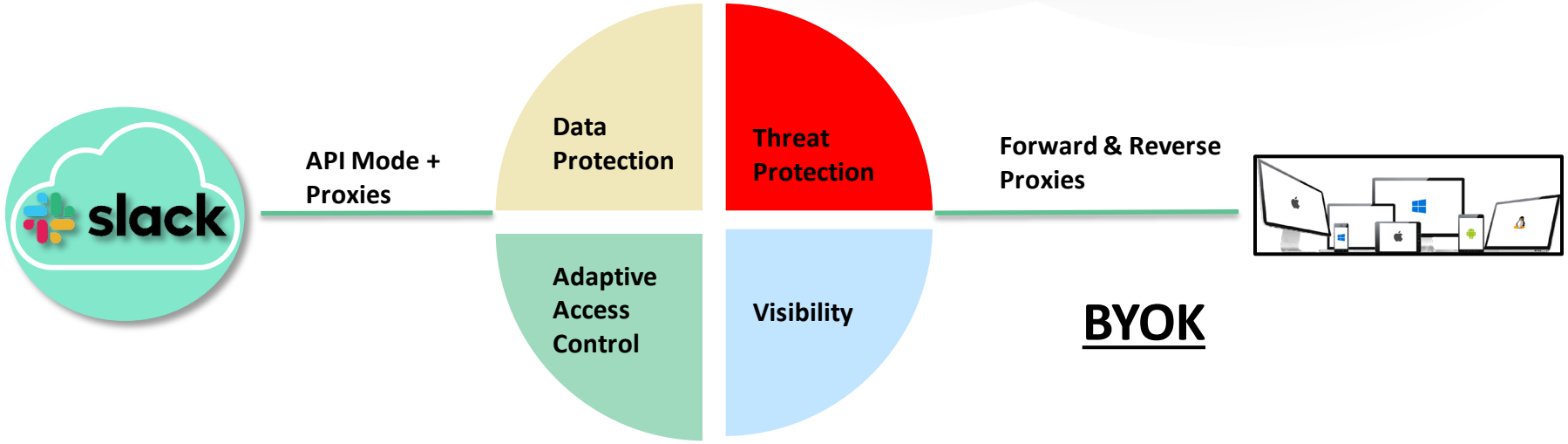
Use Cases: CASB – workday



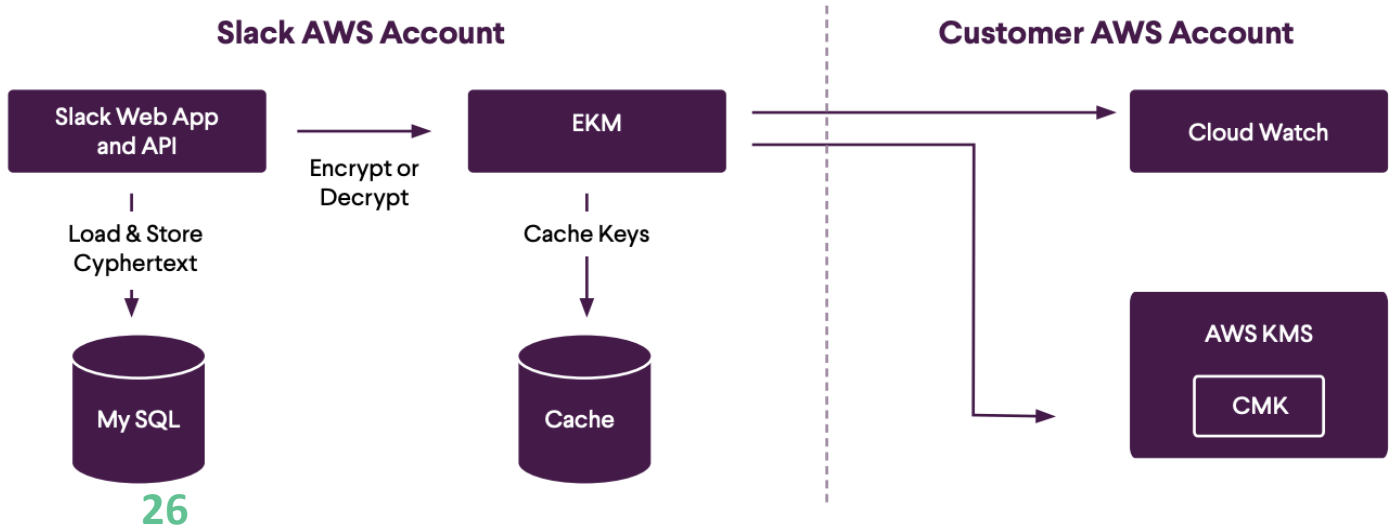
- Adaptive Access Control
- Data Loss Prevention
- Malware Advanced Threat Protection
- User Behavior Analytics

Untangling SaaS Security in the Enterprise

Use Cases: CASB – Slack



- Adaptive Access Control
- Data Loss Prevention
- Malware Advanced Threat Protection
- User Behavior Analytics
- BYOK



Takeaway Checklist

- Establish a SaaS Cloud Security with a Governance program
- Establish SaaS Security Engagement Model
- Engage Vendor Assessment/Supply Chain
- Establish SaaS sanction Process
- Establish strong foundational security components for SaaS security deployment
- Deploy CASB Controls – Discovery & Visibility
- Deploy CASB –API & Proxy mode
- Establish Strong BYOD controls

Useful Links

- **SaaS Security Resources**

https://wa.aws.amazon.com/wat.pillar.security.en.html

https://cloudsecurityalliance.org/research/cloud-controls-matrix/

https://www.owasp.org/index.php/OWASP_Proactive_Controls

https://www.sans.org/reading-room/whitepapers/cloud/paper/37960