Citizens

Cloud Security for Solution Architect Curriculum

Solution Architect Academy

Jan 2021

Cloud Topics

In this section we'll cover cloud Security and what it means in Solution Architecture

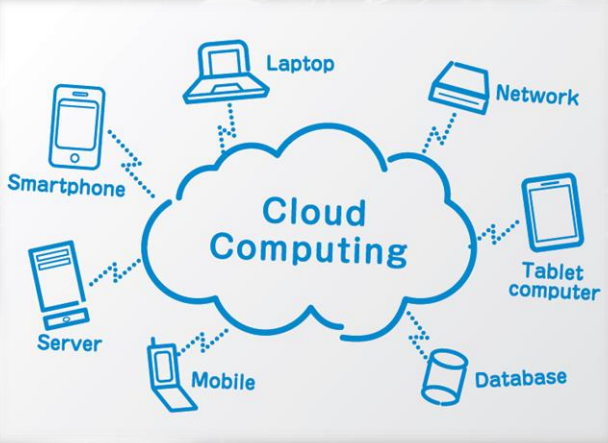
1. Security in the Cloud
2. CFG Cloud Strategy
3. Cloud Service Models and Principles
4. Cloud Architecture (AWS and MS)
5. Logical Architectures

Security Role in Cloud

- *Cloud computing* is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

- Cloud computing needs a change of mindset for security
  - New security skills span strategy, leadership, operational and technical areas of interest
  - Architects must learn core skills and select emerging skills to learn based on their unique circumstances

- Cloud service provider tools and third-party vendor services provide an array of up-to-the-minute capabilities to assemble effective defenses



Use of Cloud Service Providers (CSPs)

Cloud Service Providers (CSPs) provide a cloud services platform offering computing power, database storage, content delivery, and other functionality

Some of the benefits offered by CSPs include:

- Speed to innovate / Speed to market
- Fail fast (and cheap)
- Consumption based model – pay only for what you use
- Scalability
- Next generation tools and services
- Simplicity of automation
- Resiliency and Redundancy – built-in

Establishing Security in the Cloud Environment

The many benefits of CSPs makes them an attractive solution and the use of them will only continue to grow. While many CSPs offer native security capabilities, it is important to understand the risk exposure associated with CSPs and ensure CFG takes the appropriate measures in augmenting those capabilities to secure the cloud environment.

CFG Cloud Strategy

 **Cloud First**	Prioritize delivering IT services using the cloud computing model. Use traditional technology delivery model as an exception. (CFG has also adopted a SaaS First guiding principle.)
 **Hybrid Cloud**	Adopt hybrid cloud services from both a service model and a deployment model perspective.
 **Risk Based Adoption**	Use risk as a key factor to determine the type of cloud (Public, Private, SaaS, etc.) that should be adopted to meet a particular business need.
 **Multi-Vendor Cloud**	Source cloud services from a variety of providers whenever feasible to avoid vendor lock in and take advantage of SaaS model.

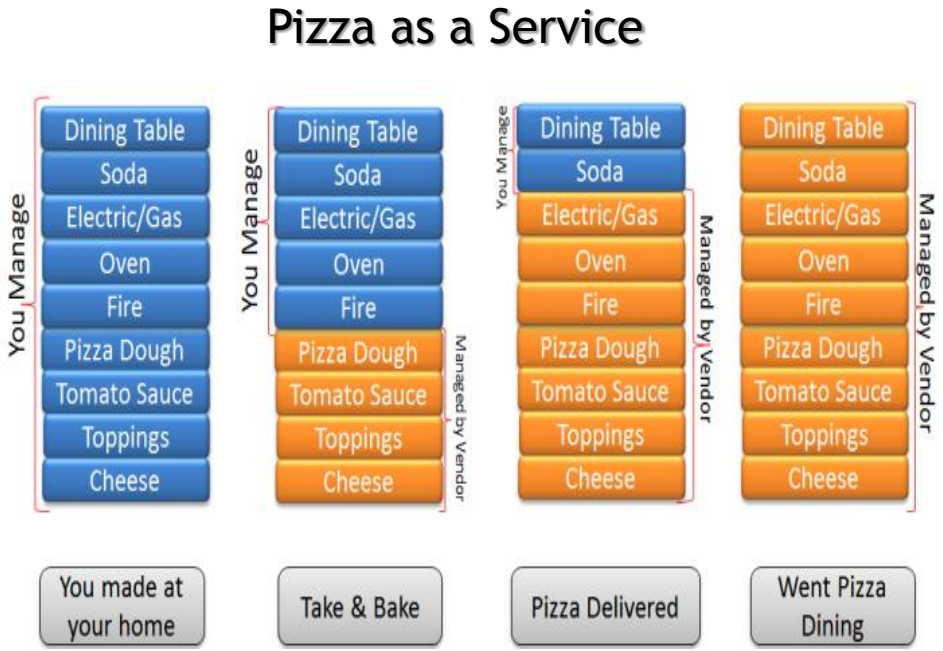
Cloud Service Models*

- **IaaS**: the cloud service model in which the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).
- **PaaS**: the cloud service model in which the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
- **SaaS**: the cloud service model in which the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

* Definitions from Cloud Security Minimum Requirement(MR)

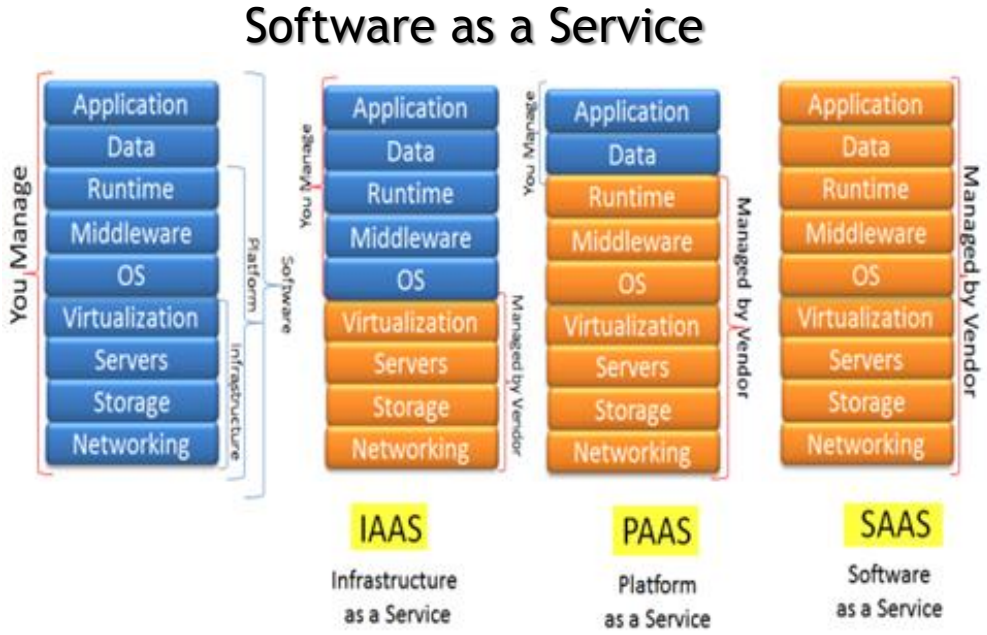
Responsibilities in the Cloud

- The cloud does not take care of security for you
- Depending on your service many on-prem responsibilities follow you and are still your responsibility



Cloud Offerings

- Let’s translate that last example into cloud offerings



Cloud Deployment Models*

- **Public**:
  - the cloud computing deployment model in which the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. (typically multi-tenant)
- **Private**:
  - the cloud computing deployment model in which the cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on-premise or off-premise. (typically single-tenant)
- **Hybrid**:
  - the cloud computing deployment model in which the cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

* Definitions from Cloud Security Minimum Requirement(MR)

Cloud Security Principles

- Identity and Access Management least privileged roles and polices
- Encryption-at-rest with Customer Managed Keys (CMK) based on Data Classification
- Encryption-in-motion with CFG Managed certificates
- Database Logging and Monitoring for GLBA/SOX/Payment systems
- CFG Hardening Standard deployments and monitoring
- Service governance for IaaS/PaaS (AWS Organizations, Azure Mgmt Groups)
- CSP logging and monitoring for all IaaS/PaaS API and network traffic flows
- Integration with enterprise security system
- Integration with enterprise Information Technology Service Management (ITSM)

Risk Management Practices

CFG has taken various steps to appropriately secure the cloud environment including the development and continued refinement of policies, standards, and patterns, establishment and regular testing of cloud controls, monthly reporting of cloud security metrics, and issue remediation.

POLICY

- Cloud Security Minimum Requirement(MR)
  - A minimum requirement under the Cybersecurity Policy.
  - Based on Cloud Security Alliance and The Open Group.
  - First published 2017 and revised annually.
  - Update to Procurement Master Software and Services Agreement (MSSA) in Q4 2018.

STANDARDS

- Configuration Standards
  - CFG Hardening Guidelines based on CIS Benchmarks, STIG and vendor best practices.
  - Configuration validation performed by Qualys and McAfee MVISION (CASB).
- Cloud Services Patterns and Standards
  - In-flight list: Being managed by Cloud Consortium.

CONTROLS

- CASB Related Controls
  - BLCID-0020314: Security capabilities are enabled in the cloud monitoring tool when technically feasible, for cloud service providers, associated CFG managed applications, and newly integrated clouds services to identify potential security threats, unauthorized activity, and malicious traffic.
  - BLCID-0020315: The SEA team ensures platform operational integrity for the successful delivery of security event data to application stakeholders and systems. Additionally, the SEA team provides SIEM integration, AWS Security Compliance reports, and support for ad-hoc information requests.

Risk Management Practices (cont.)

METRICS	▪ Cloud Access Security Broker (CASB) Metrics ▪ Cloud Security Dashboard
ISSUE REMEDIATION	▪ Open Issues ❑ OR-01972 CASB Monitoring - Enhancements to CASB monitoring are needed to more effectively identify potential security threats. ❑ OR-01974 AWS monitoring - Enhancements to AWS monitoring are needed to more effectively identify potential security threats. ▪ Closed Issues ❑ OR-08437 Skyhigh CASB Solution is not integrated with Sailpoint for User Entitlement Reviews

Governance Implementation

CFG has established governance practices within existing organizational processes to ensure cloud service providers (CSPs) are appropriately assessed prior to being brought onboard and continuously assessed going forward to ensure compliance with CFG policies and standards.

	Process Owner	Governance Process	Details
Within CS&R	Cyber Security	Information Security Business Impact Assessment (ISBIA)	▪ Validates CSP against Cloud Security Alliance (CSA) – Consensus Assessments Initiative Questionnaire (CAIQ). ▪ Validates Solution Design against CFG - Cloud Security MR.
	SEA (Cyber Storefront)	Security Requirements	▪ Leverage SD Elements to add security requirements early in lifecycle and populated in Jira Town/Neighborhood/PODs
Outside of CS&R	Third Party Vendor Assessment	Vendor Classification Profile (VCP)	▪ Risk scoring in GRC updated in Q1 2019 with Cloud questions such as Service Model (SaaS, PaaS, IaaS), Deployment Models (Public, Private, Hybrid), Single Tenant / Multi Tenant, 4th party (identify where SaaS vendors services run from AWS, Azure, etc.).
		Vendor Assurance	▪ Onsite visit or paper based assessments incorporating cloud specific controls from Cloud Security Alliance (CSA) - Cloud Controls Matrix (CCM).
	Procurement	Master Software and Services Agreement (MSSA)	▪ Exhibit B – Section 1.g : Added Cloud Security MR specific content not already contained elsewhere in the MSSA.
	Enterprise Architecture	Architecture Review Board (ARB)	▪ Ensure that solution architecture and designs are in alignment with policy and standards (e.g. authentication, multiple geographic regions defined if required, single or multi tenancy design impacts).

How CFG is Securing AWS*?

- Authentication with Okta enabling Single Sign On, and authorization through Okta integration to Active Directory (AD) groups managed by SailPoint.
- Configuration Audit with McAfee MVision (CASB).
- Data-at-rest encryption using keys generated and managed by AWS Cloud HSM and Gemalto KeySecure.
- Data-in-motion encryption using certificates issued centrally from Venafi.
- Logging and Monitoring information collected by Splunk Cloud for security analytics.
- Compliance with CFG Hardening Standards including installation of required OS agent and Qualys executed Threat and Vulnerability Management scans.
- Standard templates to consistently automate the configuration of AWS objects in Hashicorp Terraform with Sentinel policies
- Protection through the appropriate cloud based boundary devices (Palo Alto firewalls, f5, NACL, SG).
- Encryption and management of connectivity between AWS and CFG through CFG on premise firewalls.
- Capture of current and historical configurations for all CFG Accounts.

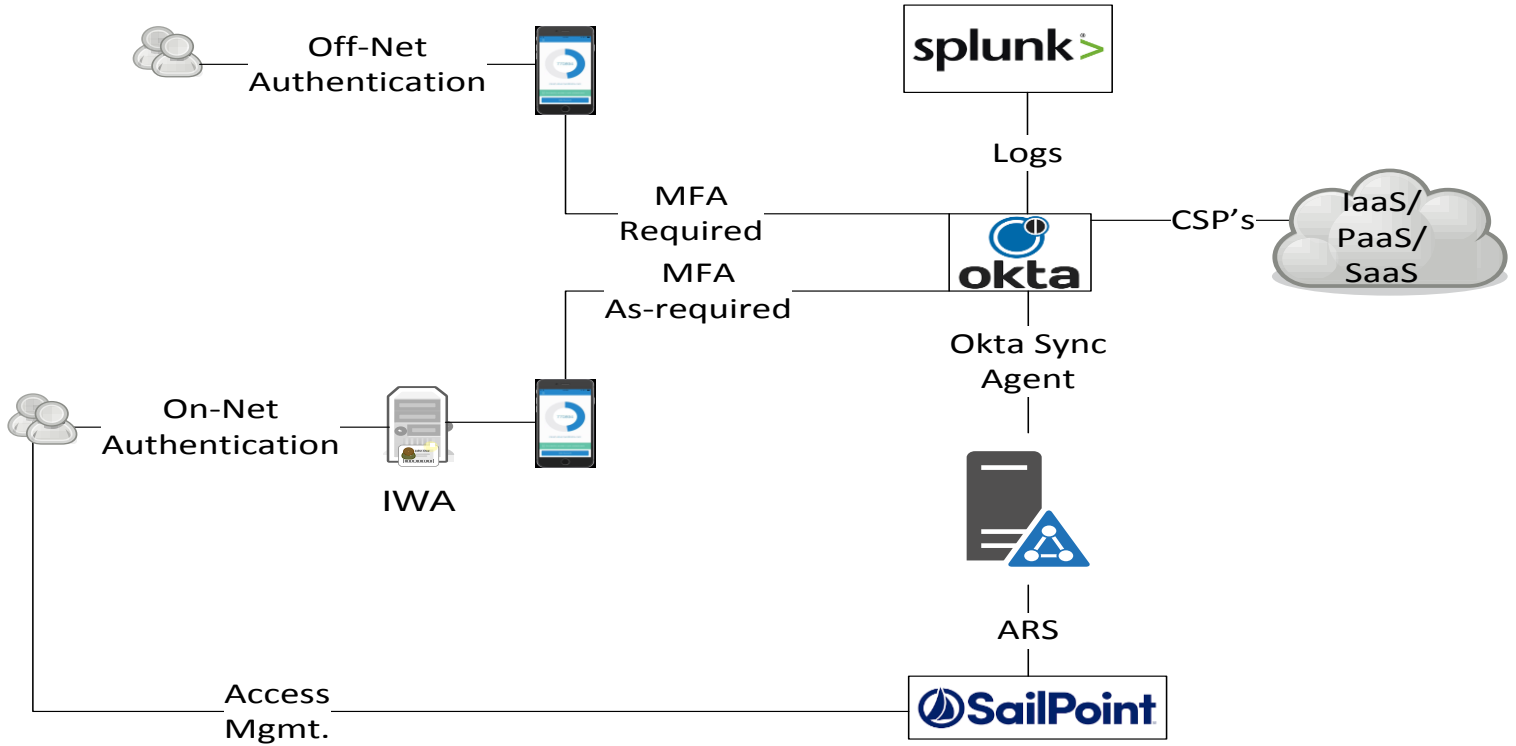
* Integration exceptions and mitigations are captured in the Cloud Security Dashboard

How CFG is Securing Microsoft*?

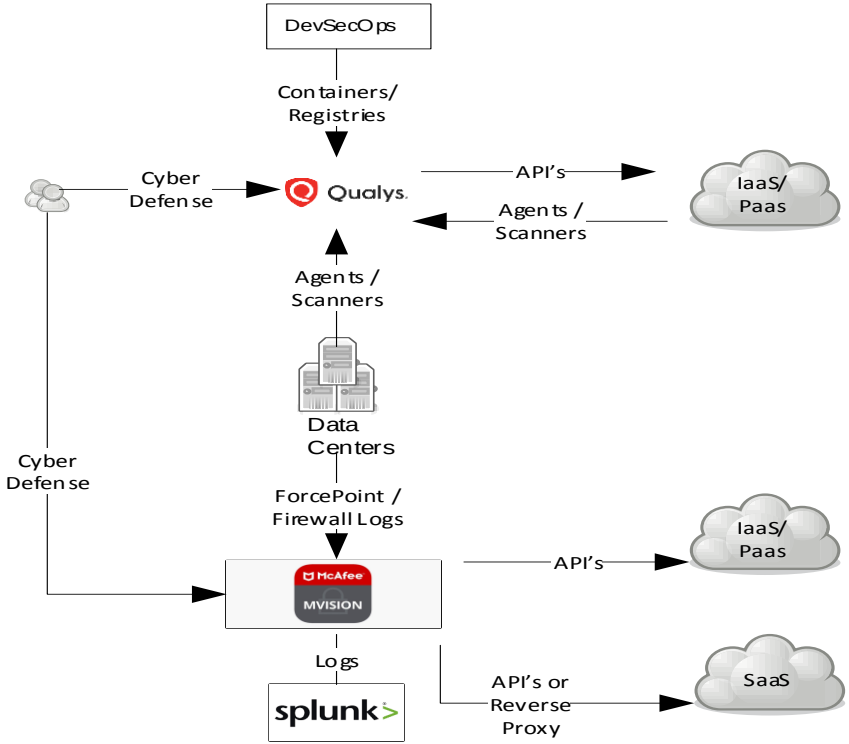
- Authentication with Okta enabling Single Sign On, and authorization through Okta integration to Active Directory (AD) groups managed by SailPoint.
- Azure Configuration Audit with McAfee mVision (CASB).
- DLP controls implemented with Symantec DLP (email), mVision (SharePoint, OneDrive) and Azure Information Protection (Data Classification and Tagging)
- Data-at-rest encryption through Gemalto HSM and KeyVault for Exchange, Sharepoint, OneDrive and based on Data Classification. Data-in-motion encryption using certificates issued centrally from Venafi.
- Logging and Monitoring information collected by Splunk Cloud for security analytics.
- Compliance with CFG Hardening Standards including installation of required OS agent and Qualys executed Threat and Vulnerability Management scans.
- Encryption and management of connectivity between Microsoft and CFG through CFG on premise firewalls and ForcePoint web proxy.
- Windows 10 local administration access managed with Remediant for self service/on-demand privileged access
- MFA required for all administrative accounts via Okta (Verify/RSA) and secondary AD accounts
- Approved mobile devices managed either with BlackBerry or Microsoft Intune

* Integration exceptions and mitigations are captured in the Cloud Security Dashboard

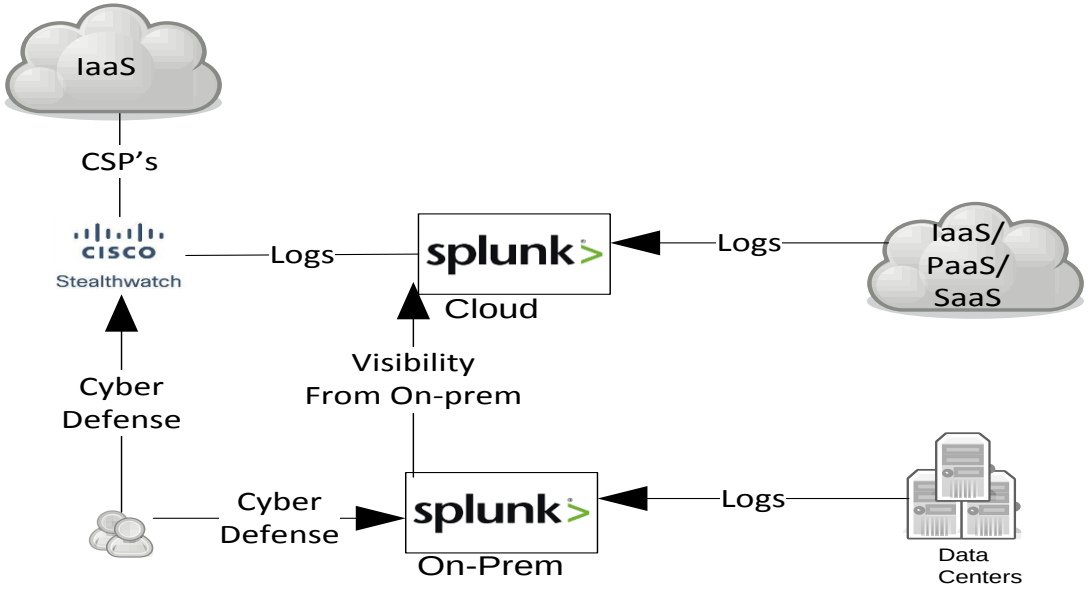
Logical Architecture: Identity & Access Control



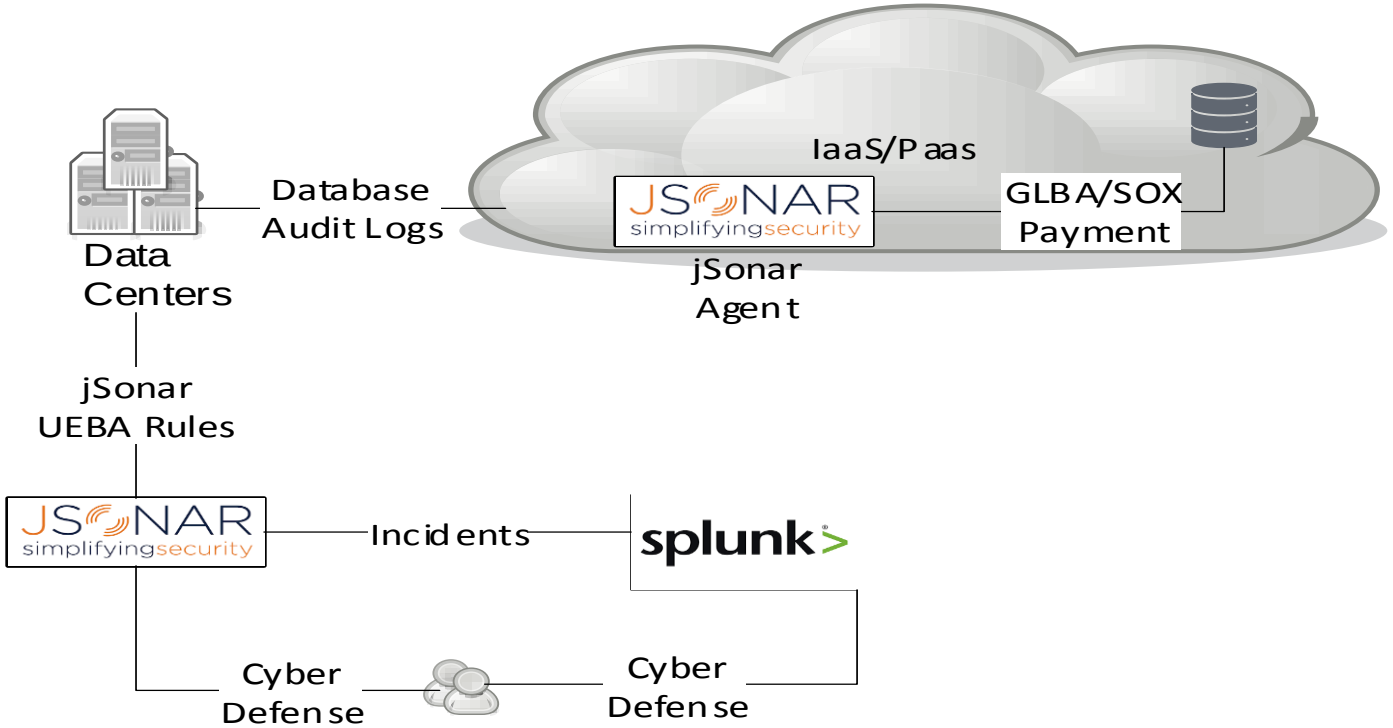
Logical Architecture: Vulnerability Management



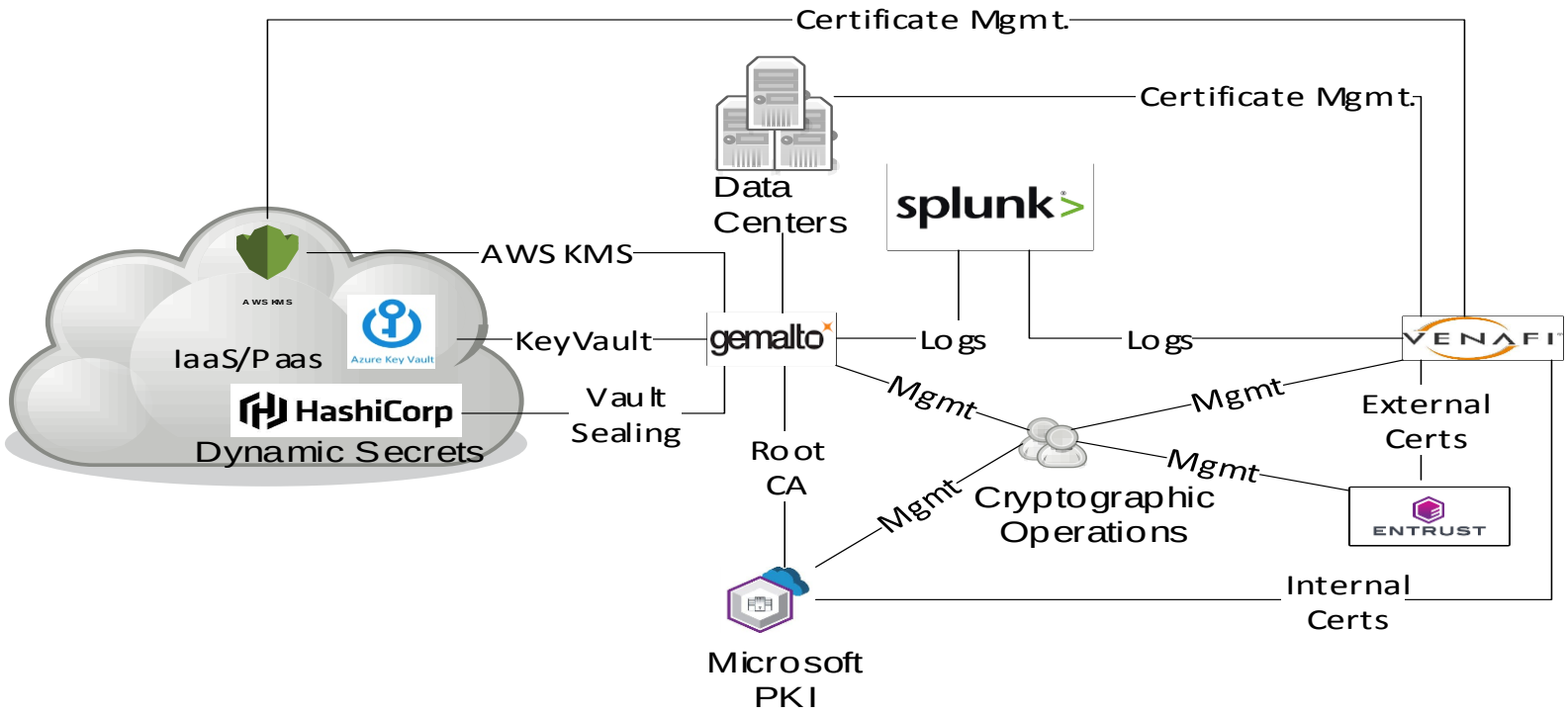
Logical Architecture: Security Visibility / SIEM



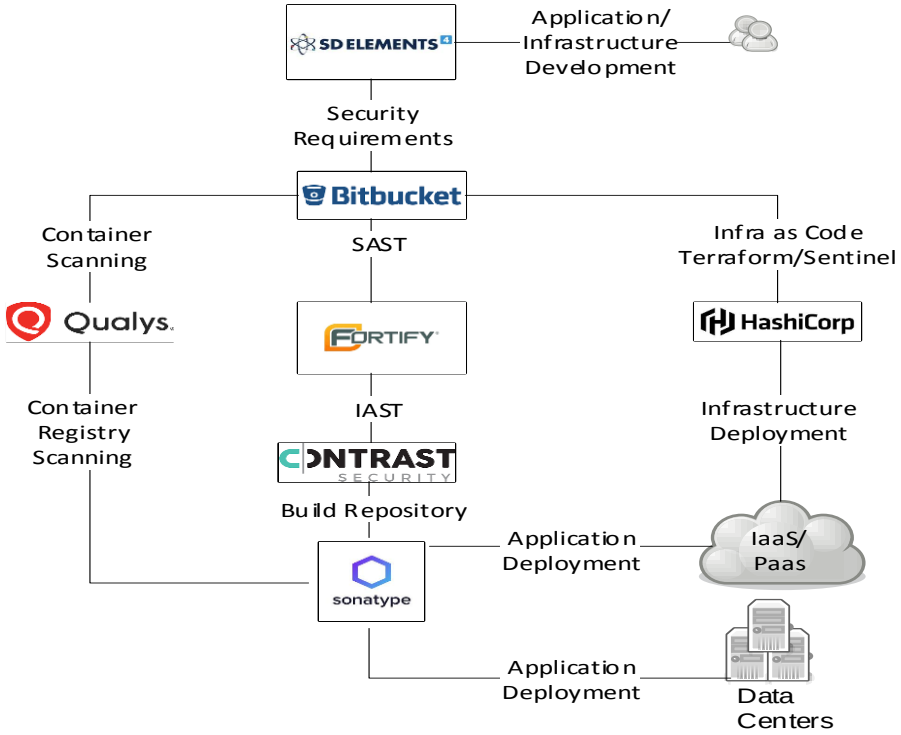
Logical Architecture: Database Logging & Monitoring



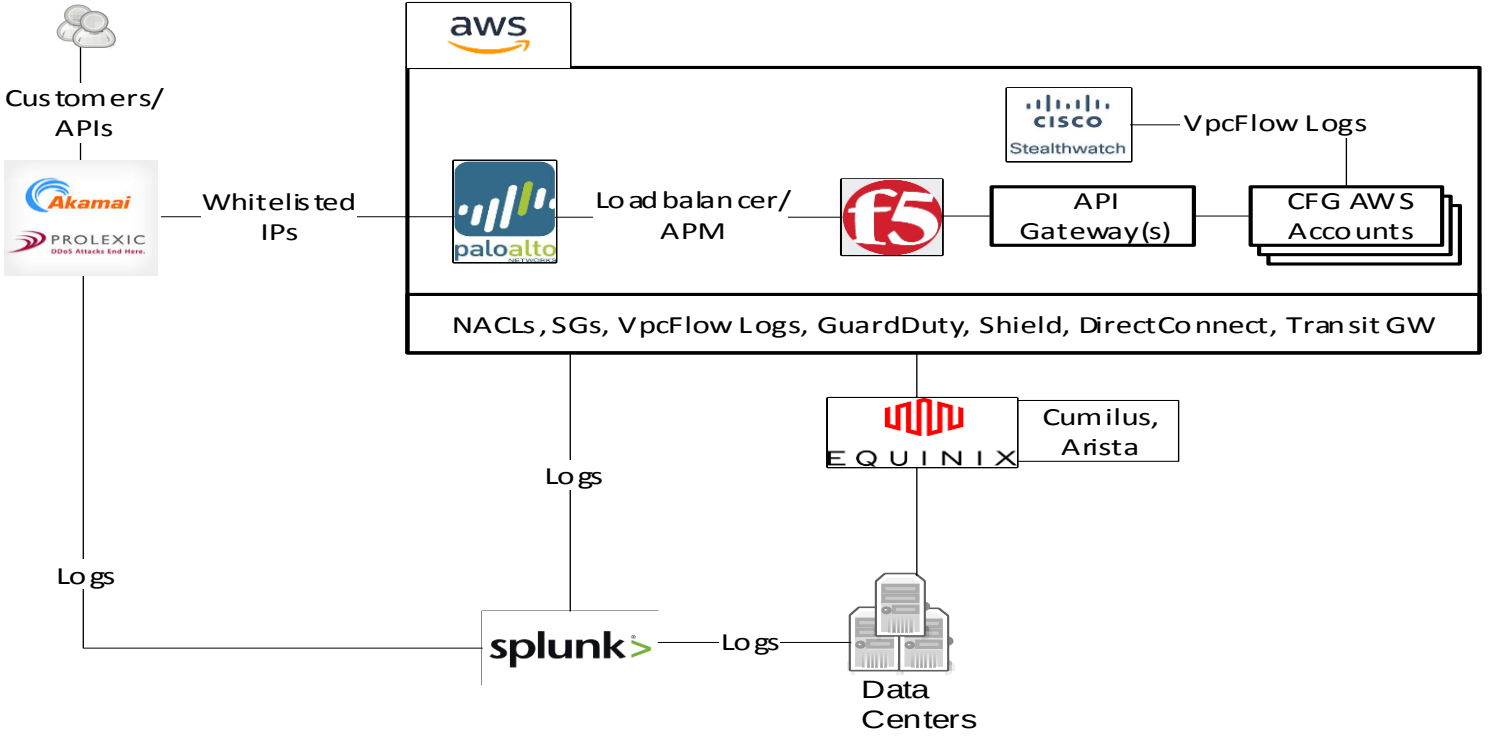
Logical Architecture: Cryptography Management



Logical Architecture: DevSecOps Pipeline



Logical Architecture: Network Security




Citizens™

References

- Strategy, Architecture and Engineering
  https://departments.internal.citizensbank.com/sites/sanda/SitePages/Enterprise%20Architecture%20Services.aspx