RSA Conference2019

San Francisco | March 4 – 8 | Moscone Center

A Cloud Security Architecture Workshop

Dave Shackleford

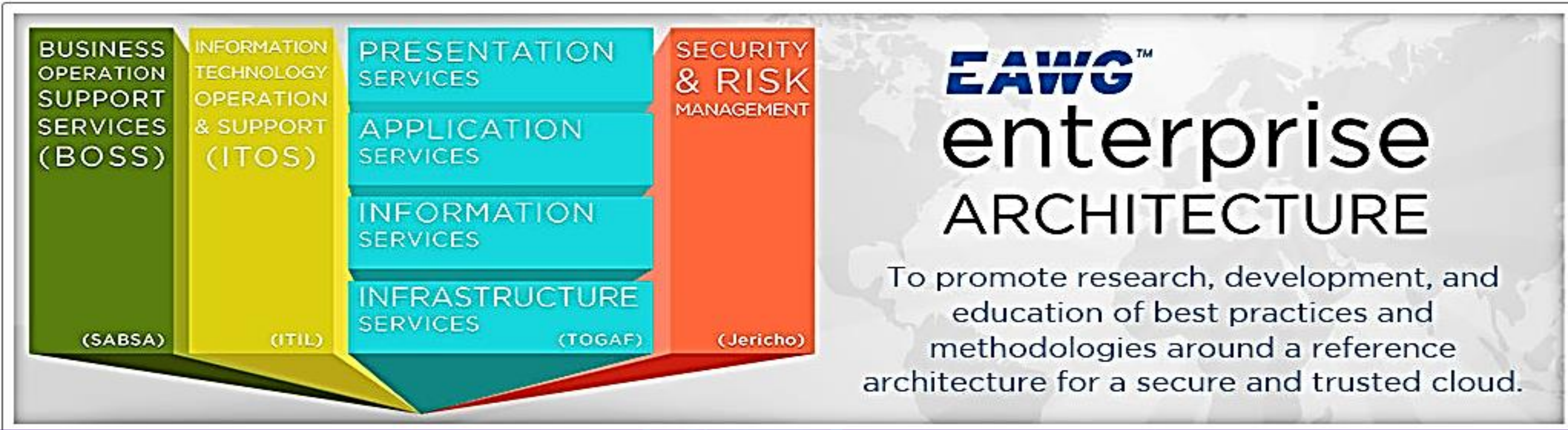
Sr. Faculty
SANS Institute
@daveshackleford

Cloud Security Architecture Overview

- There are some very well-known architectural principles for cloud that apply to security
- Sadly, there are few industry design frameworks that are accepted for secure cloud architecture
- Over time teaching and consulting, I’ve found a number of core best practices that can apply to any IaaS cloud design

CSA's Enterprise Architecture

- Seeks to promote a sound reference architecture with best practices and processes for a secure cloud



To promote research, development, and education of best practices and methodologies around a reference architecture for a secure and trusted cloud.

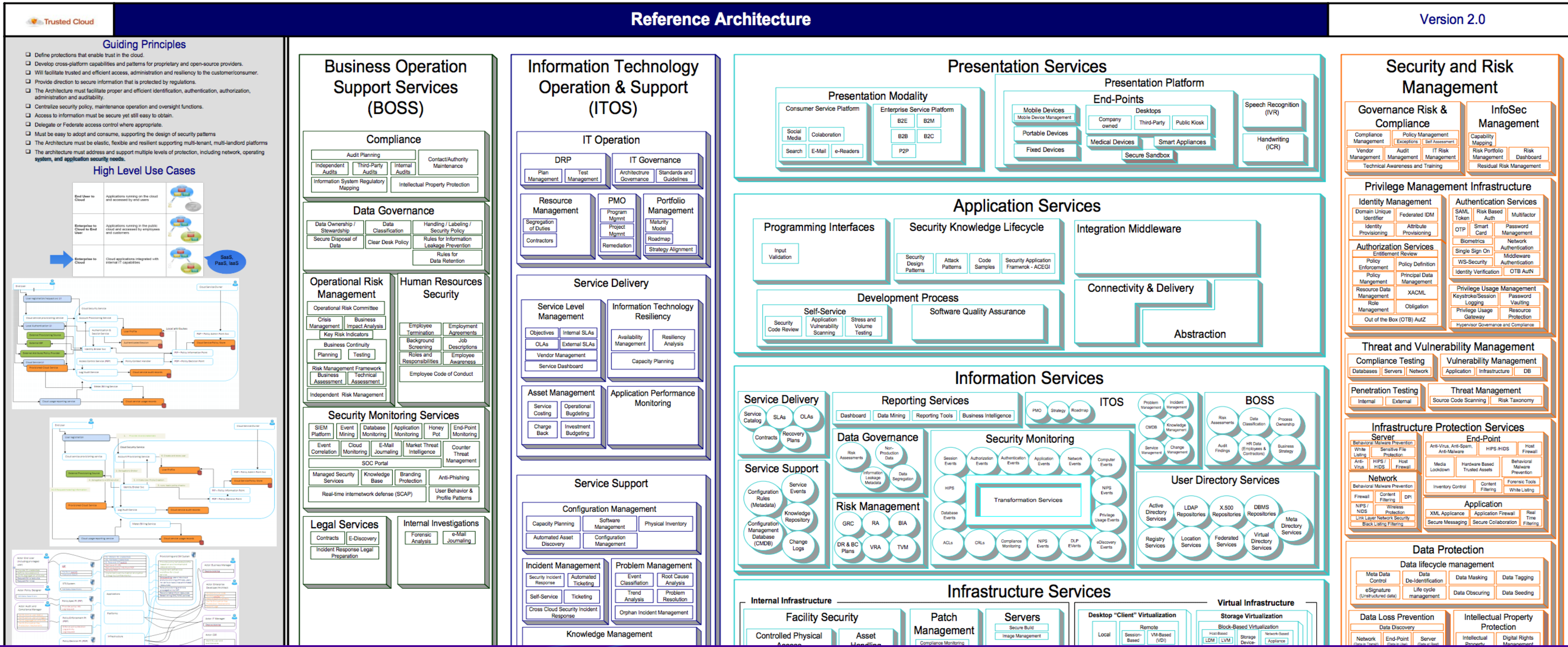
EA Guiding Principles (1)

- 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

EA Guiding Principles (2)

- 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 multitenant, multi-landlord platforms
- The Architecture must address and support multiple levels of protection, including network, operating system, and application security needs

EA Reference Architecture … Ouch.



Trusted Cloud

Reference Architecture

Version 2.0

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

End User to Cloud	Applications running on the cloud and accessed by end users
Enterprise to Cloud to End User	Applications running in the public cloud and accessed by employees and customers
Enterprise to Cloud	Cloud applications integrated with internal IT capabilities

SaaS, PaaS, IaaS

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: Architectrure 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 Bugdeting, 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

Presentation Services

Presentation Modality
Consumer Service Platform: Social Media, Colaboration, 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; Secure Sandbox; Speech Recognition (IVR); Handwriting (ICR)

Application Services

Programming Interfaces: Input Validation; Security Knowledge Lifecycle: Security Design Patterns, Attack Patterns, Code Samples, Security Application Framwrok - 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; Service Support: Configuration Rules (Metadata), Service Events, Knowledge Repository, Configuration Management Database (CMDB), Change Logs; Data Governance: Risk Assessments, Non-Production Data, Information Leakage Metadata, Data Segregation; Risk Management: GRC, RA, BIA, DR & BC Plans, VRA, TVM; Security Monitoring: Session Events, Authorization Events, Authentication Events, Application Events, Network Events, Computer Events, HIPS, NIPS Events, Database Events, Privilege Usage Events, Transformation Services, ACLs, CRLs, Compliance Monitoring, NIPS Events, DLP EVents, eDiscovery Events; 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, Asset Handling); Patch Management (Compliance Monitoring); Servers (Secure Build, Image Management)

Virtual Infrastructure: Desktop "Client" Virtualization (Local; Remote: Session-Based, VM-Based (VDI)); Storage Virtualization (Block-Based Virtualization: Host-Based, LDM, LVM, Storage Device-, Network-Based, Appliance)

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 AutN; Authorization Services: Entitlement Review, Policy Enforcement, Policy Definition, Policy Mangement, Principal Data Management, Resource Data Management, XACML, Role Management, Obligation, Out of the Box (OTB) AutZ; Privilege Usage Management: Keystroke/Session Logging, Password Vaulting, Privilege Usage Gateway, Resource Protection, Hypervisor Governance and Compliance

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

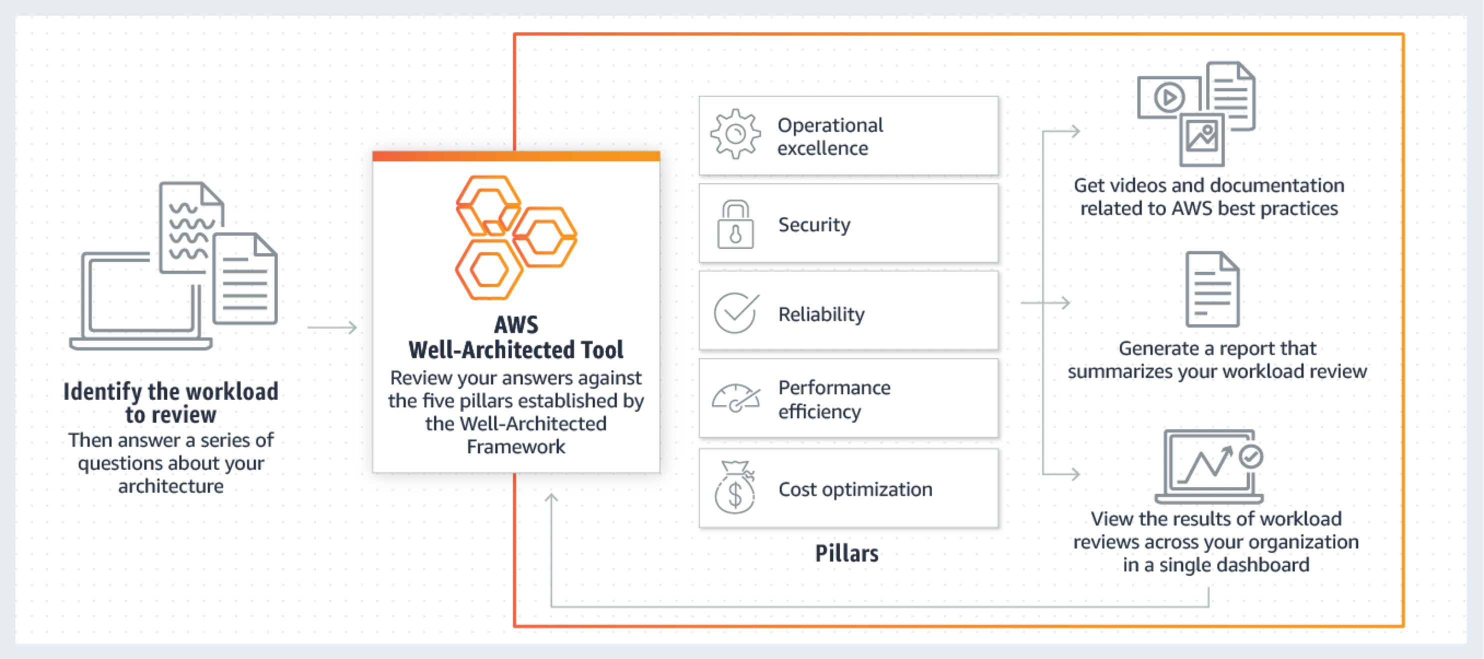
Infrastructure Protection Services
Server: Behavioral Malware Prevention, White Listing, Sensitive File Protection, Anti-Virus, HIPS / HIDS, Host Firewall; Network: Behavioral Malware Prevention, Firewall, Content Filtering, DPI, NIPS / NIDS, Wireless Protection, Link Layer Network Security, Black Listing Filtering; End-Point: Anti-Virus, Anti-Spam, Anti-Malware, HIPS /HIDS, Host Firewall, Media Lockdown, Hardware Based Trusted Assets, Behavioral Malware Prevention, Inventory Control, Content Filtering, Forensic Tools, White Listing; Application: XML Appliance, Application Firewall, Secure Messaging, Secure Collaboration, Real Time Filtering

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 Loss Prevention: Data Discovery, Network (Data in Transit), End-Point (Data in Use), Server (Data at Rest); Intellectual Property Protection: Intellectual Property, Digital Rights Management

SANS

AWS Well-Architected Framework

- AWS has developed a framework called “Well-Architected” that includes five “pillars”:
  - Operational excellence
  - Security
  - Reliability
  - Performance efficiency
  - Cost optimization
- Offers specific best practices and guidance to help design and implement AWS solutions


Identify the workload to review
Then answer a series of questions about your architecture
AWS
Well-Architected Tool
Review your answers against the five pillars established by the Well-Architected Framework
Operational excellence
Security
Reliability
Performance efficiency
Cost optimization
Pillars
Get videos and documentation related to AWS best practices
Generate a report that summarizes your workload review
View the results of workload reviews across your organization in a single dashboard

A Basic Approach to Sound Cloud Design

- There are many ways of defining “architecture” for the cloud
- Core considerations include:
  - Network connectivity
  - Availability and redundancy
  - Resilience
  - Scalability
  - And so on
- We’ve broken cloud architecture into seven themes that must be followed in all cases (next)

SANS Cloud Architecture Principles

- SANS believes the following are the most critical security architecture principles to embed in all designs:
  - Build in security at every layer
  - Think “components”
  - Design for failure
  - Design for elasticity
  - Make use of different storage options
  - ALWAYS think of “feedback loops”
  - Focus on CSA: Centralization, Standardization, Automation

Build in Security at Every Layer (1)

- Every cloud architecture is composed of unique layers that can be coupled and integrated (or not)
- To some degree, each layer must be “self-defending”
- The new cloud infrastructure and application stack have a number of components
- Each layer needs some sort of security integrated and applied to build a sound “defense-in-depth” architecture for the cloud
- Depending on the layer, some will be applied in-house, others in the CSP environment

Build in Security at Every Layer (2)

"Stack" Layer	Controls
Application Logic + Presentation	WAF, IAM, Scans/Pen tests
Operating Systems	Configuration, Vulnerability Scanning, Backups, user/privilege management
Data	Encryption, Backups, DLP
Network	Access Controls, Firewalls, Routing, DDoS Defense
Hypervisor	Configuration, access controls, user/privilege management

Build in Security at Every Layer (3)

- Given the nature of the cloud, IT changes much more dynamically than ever before
- For this reason, all security measures should ideally be “embedded”
- This means:
  - Defining security in code internally
  - Including security configuration parameters in VM definitions
  - Automating security processes and activities
  - Building continuously monitored environments
- Many of these ideas are realized in a sound DevSecOps strategy

Think “Components”

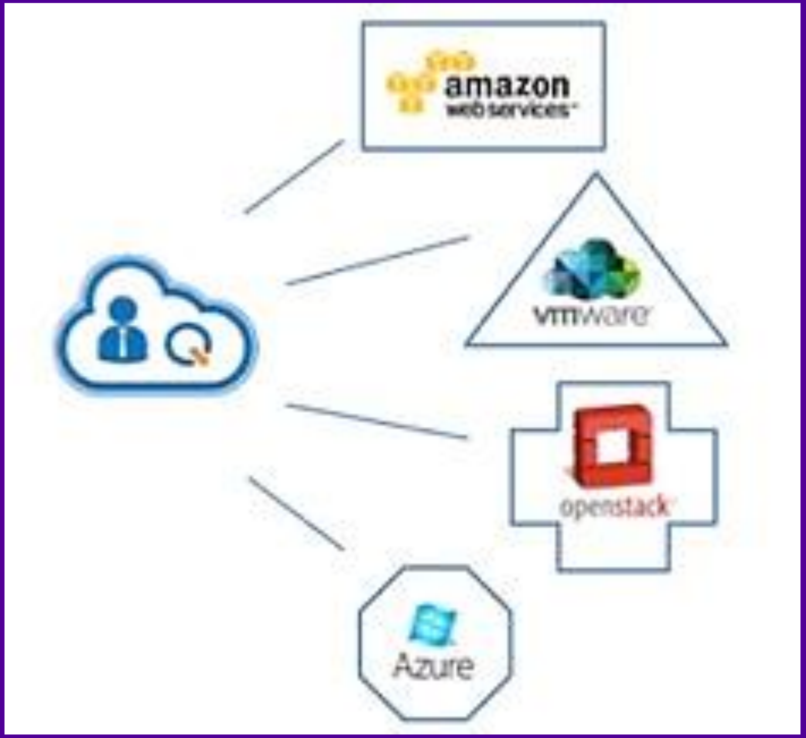
- While this may seem obvious at this point, it’s a major shift for many security professionals
- We’re used to designing IT (and to some degree, security) as “systems”
- While some of that holds, in the cloud, we are actually dealing more with disparate components that can be linked and used together in different ways
- For example, each type of storage within Amazon is a different component with varied security controls

Think "Components": One Ring to Rule Them All

- When designing security for each individual component, the major theme you should keep in mind is centralization
- In other words, are there efficiency opportunities to define and manage security for multiple components in one place?

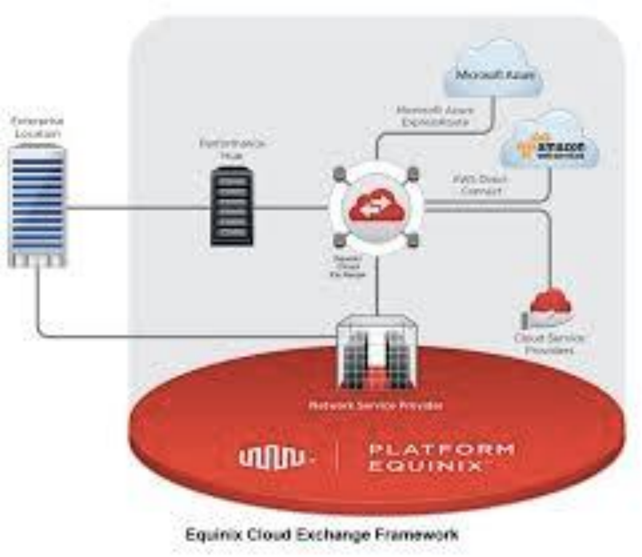
Think “Components”: The Multi-Cloud Problem

- Many organizations use numerous cloud providers in a hybrid configuration
- What security controls are available in each environment?
- This is a perfect example of why each component needs security “baked in” if possible
- This can add to complexity and operational overhead if not managed well (and early)



Multi-Cloud Brokers

- Another option for some organizations is using a multi-cloud brokering model
- Many traditional telecommunications carriers offer MPLS cloud access to CSPs
  - AT&T NetBond is one example
- There are other, dedicated services available too
  - Equinix offers cloud brokering with its Cloud Exchange Framework
- These options are usually very expensive
  - May offer greater flexibility and control



Equinix Cloud Exchange Framework

Design for Failure

- Security professionals don’t like the word “failure” (probably for obvious reasons)
- However, in the cloud, you are likely to encounter failure more often than you would like:
  - Elasticity issues
  - Configuration issues
  - Cloud provider issues
- Not all of these will be within your control, so you will need to plan for things to go wrong (they will)

Design for Failure

- When designing for failure, there are two design aspects to consider:
  - Component level: Each component could fail individually or in some combination
  - Architecture level: The entire environment becomes unavailable
- While unlikely, a provider’s data center could have a problem
  - Or a backbone carrier or other critical aspect could fail
- You need to design redundancy and availability into EVERYTHING within the cloud
  - Or at least those cloud services you care about!

Design for Elasticity

- One of the cloud’s foremost benefits is the ability to rapidly scale up and down as needed for business volume and requirements
- Designing elasticity into your models means considering the following:
  - Vertical or horizontal scaling?
  - What thresholds are appropriate for scaling up and down?
  - How will inventory management adjust to system volume changes?
  - Images new systems are spawned from
  - Where new systems will operate (network locale)
  - Host-based security + licensing

Storage: Explore Your Options (1)

- There are many types of storage available in the cloud
- Understand each type and which are best suited for your deployment
- Each has its own security options available too
- Revisit data classification and data security policy before planning storage security design
  - Performance matters too, of course!

Storage: Explore Your Options (2)

- When looking into storage options in the cloud, here are things to consider and evaluate:
  - Does the storage option work for operations and development?
  - Does the storage option have appropriate SLAs and uptime?
  - Does the storage option have adequate redundancy and archival?
  - Does the storage meet performance requirements?
  - Does the storage option provide native encryption capabilities?
  - Does the storage option provide access controls?
  - Does the storage option allow for adequate logging and event generation?
  - What does the storage option cost?
- Consider all the benefits and drawbacks of each before choosing!

Security: Design in a “Feedback Loop”

- This is one of the most critical elements of cloud security design
- A huge amount of effort goes into securing resources:
  - On their way to the cloud
  - In the cloud
- Given the dynamic nature of cloud computing, things can (and will) change RAPIDLY
- While we’re building in security controls, ensure you plan for alerting and notification capabilities that continually keep us in the loop

Security “Feedback Loops”= Logging

- Your primary source of feedback is LOGS
- Enable logging everywhere you can:
  - Within the cloud environment/account as a whole
  - For instance, OS types
  - For network platforms
  - For all identity and access management activity
  - For all interconnected services and their activity
- Be sure to secure access to logs, as well

Security "Feedback Loops": Other Services

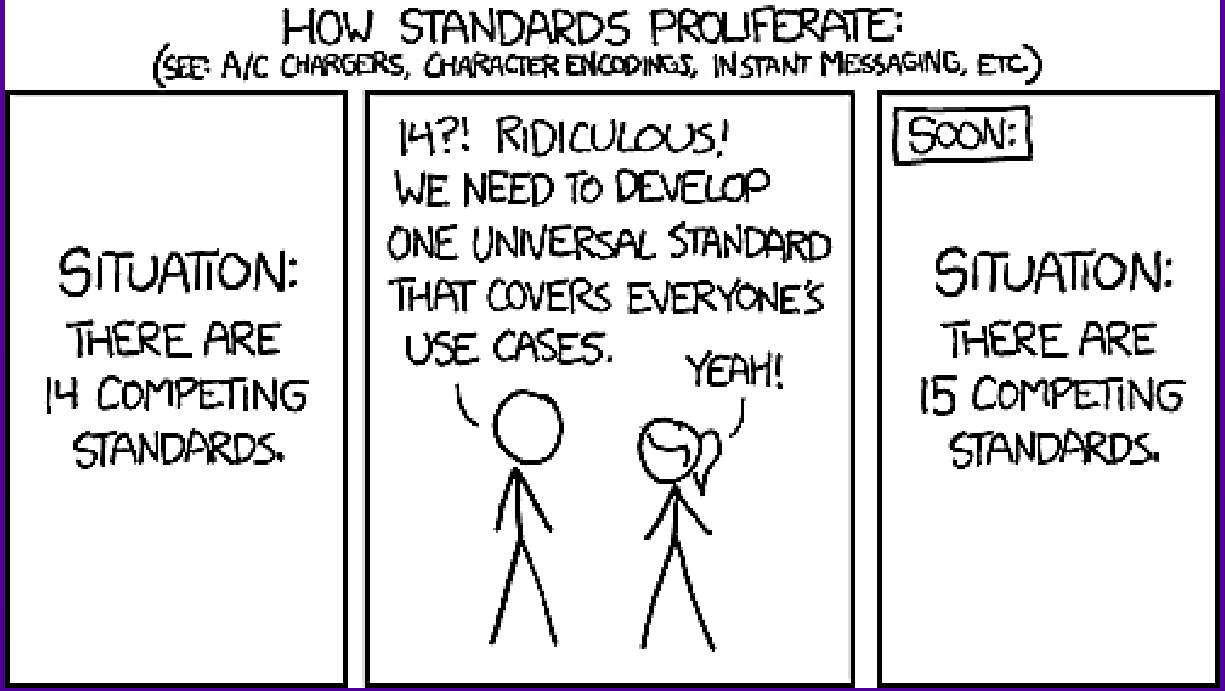
- There are numerous alerting and monitoring mechanisms in major cloud environments
  - CloudTrail logging and Azure Activity Logs
  - CloudWatch alarms
  - Simple Notification Service (SNS) alerts
  - Billing Alerts
- Google StackDriver is an alerting method within the Google cloud
- Azure Monitor is a dashboard that aggregates monitoring like activity logs, diagnostic logs, and metrics
- Azure Advanced Threat Analytics can monitor account behavior

Centralization, Standardization, Automation: Centralization

- As a final major theme for design and architecture in the cloud, we'll touch on CSA: centralization, standardization, and automation
- Centralization is the idea that you need to look at tools and cloud services that ideally integrate into a single dashboard
- It is **very easy** in cloud deployments to end up with numerous management tools, dashboards, and interfaces to keep up with
- This is not exclusive to security tools—operations and development teams are often faced with the same problem
- Using the same vendor products across cloud environments can help with this (if possible)

Centralization, Standardization, Automation: Standardization

- Standardization is fairly straightforward conceptually
- When designing for the cloud, look for ways to leverage well-known standards:
  – SAML and OpenID Connect for IAM
  – YAML for configs
  – AES-256+ for crypto


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

Centralization, Standardization, Automation: Automation

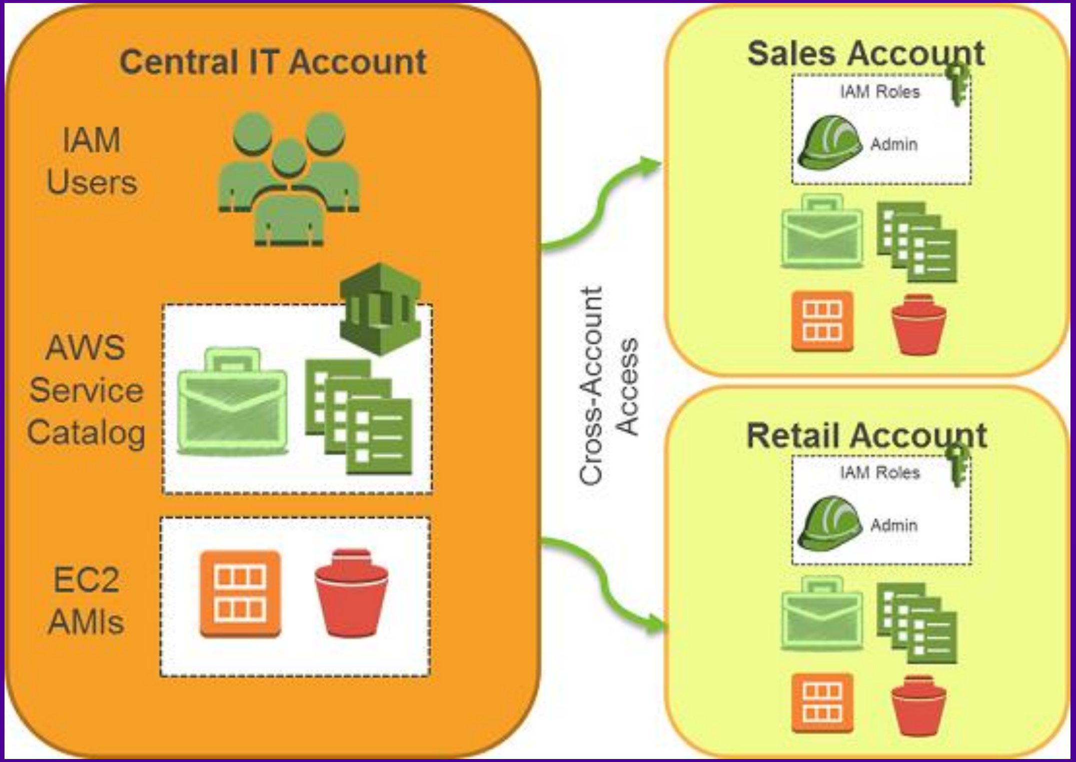
- Automation is the core idea behind DevOps, and DevSecOps by extension
- Manual efforts in the cloud are doomed to fail in many cases, as the environment changes rapidly
- Security teams should explore ways to automate their security controls and feedback loops whenever possible
- Scripting and orchestration tools can help!

Managing the Cloud “Blast Radius”

- One of the core security concepts in the world of DevOps and cloud computing is the “blast radius”
- The blast radius is the amount of damage that could be caused if something goes wrong
  - An account or server gets hacked
  - A component fails
- Design your security model in such a way that you limit the damage any one issue could cause

Multiple Accounts for Limiting Blast Radius

- One cloud security strategy that has emerged in recent years is the use of multiple accounts for limiting blast radius
- Accounts can be created for:
  - Developers
  - Business units
  - Operations
  - Security
- These can then be allowed access to objects and assets in other accounts as needed
- AWS has a service called “Landing Zone” to help set this up
  - A newer service called “Control Tower” is also now available to implement this



Applying This To Your Organization

- Next week you should:
  - Determine your level of overall architecture maturity
- In the first three months following this presentation you should:
  - Ensure you look into multi-account or subscription architectures
  - Ensure centralized, infrastructure-as-code deployments are planned
- Within six months you should:
  - Have a streamlined, central deployment incorporating DevSecOps principles
  - Ensure all feedback loop and storage controls are optimized