Cloud Customer Architecture for Securing Workloads on Cloud Services

http://www.cloud-council.org/deliverables/cloud-customer-architecture-for-securing-workloads-on-cloud-services.htm
The Cloud Standards Customer Council

*THE Customer’s Voice for Cloud Standards*

- Provide customer-led guidance to multiple cloud standards-defining bodies
- Establishing criteria for open standards based cloud computing

2017 Projects
- Security for Cloud Services Ref. Architecture
- Impact of Cloud Computing on Healthcare
- Hybrid Integration Ref. Architecture
- API Management Ref. Architecture
- Data Residency discussion paper
- Blockchain Ref. Architecture
- Multi-cloud Management whitepaper
- And more!

2015 Deliverables
- Web App Hosting Ref. Architecture
- Mobile Ref. Architecture
- Big Data & Analytics Ref. Architecture
- Security for Cloud Computing, V2
- Practical Guide to Cloud SLAs, V2
- Practical Guide to PaaS

2013/2014 Deliverables
- Convergence of Social, Mobile, Cloud
- Analysis of Public Cloud SLAs
- Cloud Security Standards
- Migrating Apps to Public Cloud Services
- Social Business in the Cloud
- Deploying Big Data in the Cloud
- Practical Guide to Cloud Computing, V2
- Migrating Apps: Performance Rqmnnts
- Cloud Interoperability/Portability

http://cloud-council.org
This talk introduces the Cloud Customer Architecture for Securing Workloads on Cloud Services

- What are Cloud Solution Architectures?
- CSCC’s Cloud Reference Architecture series
  - Cloud Customer Architecture for Hybrid Integration http://bit.ly/2lHIIs0
Cloud Customer Reference Architectures

Cloud Customer Reference Architectures are...

- straightforward description of elements needed to implement particular application solutions using cloud infrastructure, cloud platforms, cloud software, and cloud services
- deployment neutral (public, private, hybrid) & implementable via IaaS, PaaS, SaaS
- general purpose reusable architectures as well as industry specific architectures
- vendor neutral & open

Important because they...

- enable cloud customers to understand unique features & advantages of using cloud computing
- bridge gap between understanding cloud customer needs and cloud provider offerings
- provide practical guidance on how common business applications can be realized from a cloud customer role perspective
- are stable anchors in a rapidly innovating cloud landscape
- save time, effort & money: be more productive

Useful when...

- those planning to build cloud based applications
- talking with cloud providers about their offerings
- understanding of the common elements and relationships in relevant solutions

Target audience:

- those planning on building/purchasing cloud based applications
- developers, architects, managers

Consistent with ISO/IEC 17789 International Standard Cloud Computing Reference Architecture
Cloud Security Overview

**Key Aspects of Security**
- Manage identity and access
- Protect infrastructure, data, and applications
- Security monitoring and intelligence
- Optimize cloud security operations

**Roles & Responsibilities**
- Security responsibilities split between CSP and cloud customer (ISO/IEC 17789)
- Roles and responsibilities should be documented in cloud service agreement (ISO/IEC 27017)

**Impact of Deployment Models**
- **Public** - resources shared with other tenants; isolation is an issue
- **Private** - no sharing with other organizations; sharing may take place between different parts of customer organization
- **Hybrid** - requires careful analysis of the security elements of each of the connected systems

**Impact of Service Models**
- **IaaS** - customer takes on most responsibility for security of data, applications, systems and networks
- **PaaS** – CSP responsible for security of platform; customer responsible for configuring appropriate security options
- **SaaS** - CSP takes most responsibility for security of cloud services
**Application User**
- Usually have access and control of data which can be sensitive
- Service accounts may have access for bulk data updates in cloud environment

**Cloud Admin**
- Privileged access users
  - Application publishers
  - Operators
  - Cloud administrators
  - Managers and team leads
  - Auditors
- Authorized to read sensitive info and execute potentially destructive actions
- Require an increased level of auditing

**Cloud Developer**
- Create, update, and delete applications
- Create cloud service instances and bind to applications
- Authorized to read sensitive info and manipulate applications
- Require an increased level of auditing
Managed Device – devices that have Directory Services membership and/or are controlled by IT under compliance policies

Unmanaged Device – devices which include personal devices (laptops, mobile devices), printers, cameras, etc.
Enterprise User Directory - store and manage user profiles, associated credentials, password policies and group membership.
Enterprise Application represents applications that run enterprise business processes and logic within existing enterprise systems.

Enterprise Data represents the one or more systems of record, for example, transactional data or data warehouses that represent the existing data in the enterprise.
• **Identity lifecycle management** – management of accounts and roles
• **Segregation of duties** – controlling access to capabilities based on user role
• **Identity-as-a-Service (IDaaS)** – enables cloud apps to externalize user authentication to a range of different identity providers
• **Federation Services** – also known as a Single Sign-on (SSO)
• **Privileged Account Management (PAM)** – a set of additional controls for privileged access accounts
• **Multifactor authentication (MFA)** – additional levels of authentication for higher security
• **Mobile Device Management (MDM)** – ensure that mobile devices are compliant with corporate policies
• **Reporting** – view of access by users
• **Audit and compliance** – validates security controls
• **Cloud Security Services** – tools for handling security across cloud environments
- **Physical security**
  - Implementation guidance is in ISO 27002, PCI DSS 3.2 and other standards
  - Provider should give assurances about physical security - independent SOC 2 report or ISO 27001 certification

- **Infrastructure isolation**
  - Bare metal systems or dedicated hosts provide the most isolation
  - VMs provide a significant amount of isolation
  - Containers provide a lower level of isolation

- **Network security**
  - Proper network segmentation is important
  - Controls, such as firewall rules, between segmented networks are also important
  - Use transport level security (i.e., TLS) in cases where sensitive data is transmitted
  - Employ certificate checking
  - For Internet facing web services consider the use of a Web Application Firewall
  - Consider your audience
---

**Threat modelling**
- Analyze attack surface
- Identify targets of attack
- Document bad actors & motivations
- Assess operational risks

**Secure design**
- Analyze attack surface
- Service and data isolation

**Secure coding**
- Input validation
- Output encoding
- Session management
- Credential and password handling
- Protect sensitive data in storage and in motion
- Error handling and logging
- Protect log information
- Selection and proper use of APIs and network services

**Security testing**
- Attack surface review
- Fuzz testing
- Web app scanning and penetration testing

**Cloud application security controls**
- Cryptography
- Identity & Access Management
- Web Application Firewall
- API security
- Container security

---

**LEGEND**
- Application component
- User
- Infrastructure services
- Data store
- Management
- Security

© 2017 Cloud Standards Customer Council
Data Classification:
- Public, Private, Regulated, Etc.

Data Protection:
- Data de-identification vs encryption
- Scope & technique of encryption
- Importance of key management

Data activity monitoring
- Including tenant specific views

Data access & control
- Secure deletion
- Right to be forgotten
Secure DevOps is an extension of application security

Embed security in a DevOps operational framework

Security testing categories:
- Functional testing for authentication, authorization and identity management
- Non-functional testing for known weaknesses
- Application and infrastructure security scanning
- Testing application logic for vulnerabilities

Security testing activities:
- Static & Dynamic scans
- Manual code review
- Validated testing of integrated services

Secure deployment management
Understand the line of responsibility:
- IaaS, PaaS, SaaS all have very different lines
- Education is essential

Start with an understanding of risk:
- Consider applicable laws, regulations & organizational security policies

Consider policy changes needed for cloud:
- Terminology
- Scope (IaaS, PaaS, SaaS)

Map customer & provider policies

Leverage the value of compliance & industry certifications
Security monitoring enables proactive tracking & reaction to security incidents

Monitoring challenges:
- “Shadow IT”
- Extending corporate security policies to cloud services

Monitoring implementation considerations:
- Proxy
- Mobile device manager (MDM)
- Mobile content manager (MCM)
- Gateway device
- Transparent gateway

Security analytics
- Detect deviations from regular patterns
- Uncover changes in network traffic
- Find activities that exceed defined levels

Vulnerability management focus:
- Subscribe to Common Vulnerability Exposure (CVE) lists
- Analyze CVE data to identify and prioritize relevant vulnerabilities
- Develop a plan to remediate vulnerabilities in a timely manner
- Test to verify vulnerabilities have been remediated

Vulnerability management is multi-phase process
1. Establish policies
2. Scan to identify vulnerabilities
3. Prioritize vulnerabilities
4. Mitigate vulnerabilities
5. Maintain & monitor vulnerabilities
<table>
<thead>
<tr>
<th>Key to Success</th>
<th>Considerations</th>
</tr>
</thead>
</table>
| Manage access to cloud applications and resources | - IdAM for use of cloud services and for the applications and resources within those cloud services  
- Seamless IdAM systems covering cloud services and on-premises systems                      |
| Protect and secure cloud apps, data & infrastructure | - Ensure boundary controls in place for all assets related to cloud services  
- Encrypt sensitive data  
- Encrypt communications                                                                 |
| Gain visibility into all resources on cloud services | - Ensure monitoring of cloud services and the apps/data located on cloud services  
- Integrate cloud service monitoring with monitoring of on-premises resources                  |
| Incorporate security into DevOps for cloud services | - Include “Secure by Design” and “Data Protection by Design” principles into all applications destined to run on cloud services  
- Include security elements into DevOps processes and test security elements before and during production deployment |
| Strong security policy and governance             | - Build a comprehensive security policy for all cloud services  
- Ensure compliance with all corporate, industry and government requirements and regulations  
- Enforce security policy through measurable security controls  
- Check cloud service provider compliance through certifications                                 |
| Automation of security services                   | - Automated, reusable security services provide best support for security standardization and consistency                                          |
Call to Action

▪ Join the CSCC Now!
  – To have an impact on customer use case based standards requirements
  – To learn about all Cloud Standards within one organization
  – To help define the CSCC’s future roadmap
  – Membership is free & easy: http://www.cloud-council.org/become-a-member

▪ Get Involved!
  – Join one or more of the CSCC Working Groups
    http://www.cloud-council.org/workinggroups

▪ Leverage CSCC Collateral
  – Visit http://www.cloud-council.org/resource-hub
Additional Resources from the CSCC

Whitepapers

• *Security for Cloud Computing: 10 Steps to Ensure Success v2.0*

• *Cloud Security Standards: What to Expect and What to Negotiate v2.0*

Cloud Customer Reference Architectures

• *Web Application Hosting*
  http://www.cloud-council.org/deliverables/cloud-customer-architecture-for-web-application-hosting.htm

• *Big Data & Analytics*
  http://www.cloud-council.org/deliverables/cloud-customer-architecture-for-big-data-and-analytics.htm

• *IoT*
  http://www.cloud-council.org/deliverables/cloud-customer-architecture-for-iot.htm

• *Mobile*
  http://www.cloud-council.org/deliverables/cloud-customer-architecture-for-mobile.htm

• *And more!*

View all papers [www.cloud-council.org/resource-hub](http://www.cloud-council.org/resource-hub) and companion webinars [www.cloud-council.org/events](http://www.cloud-council.org/events)
Thank You