Trusted Cloud

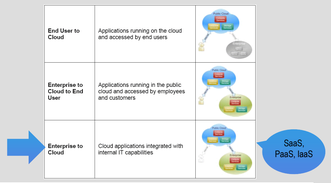
Reference Architecture

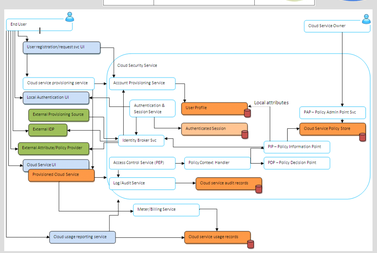
Version 2.0

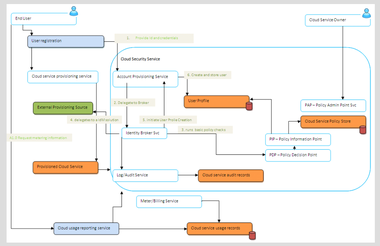
Guiding Principles

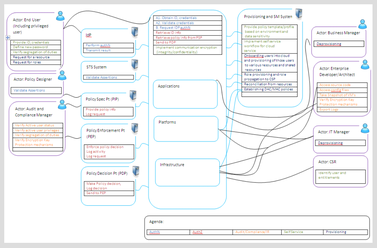
- Define protections that enable trust in the cloud.
- Develop cross-platform capabilities and patterns for proprietary and open-source providers.
- Will facilitate trusted and efficient access, administration and resiliency to the customer/consumer.
- Provide direction to secure information that is 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.

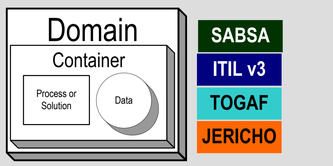
High Level Use Cases











Business Operation Support Services (BOSS)

Compliance

- Audit Planning
- Independent Audits 独立
- Third-Party Audits
- Internal Audits
- Contact/Authority Maintenance
- Information System Regulatory Mapping 监管
- Intellectual Property Protection 知识产权保护

Data Governance

- Data Ownership / Stewardship 管家
- Data Classification
- Handling / Labeling / Security Policy 标签
- Secure Disposal of Data 处置
- Clear Desk Policy
- Rules for Information Leakage Prevention 预防泄露
- Rules for Data Retention 保留

Operational Risk Management

- Operational Risk Committee 委员会
- Crisis 危机 Management
- Business Impact Analysis
- Key Risk Indicators 指标
- 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 日志
- 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

- Architecture Governance
- Standards and Guidelines

Resource Management

- Segregation of Duties 职责分离
- Contractors 承包商

PMO

- Program Mgmnt
- Project Mgmnt
- Remediation 整治

Portfolio Management 组合管理

- Maturity Model 成熟度模型
- Roadmap 战略调整
- Strategy Alignment

Service Delivery

Service Level Management

- Objectives
- Internal SLAs
- OLAs
- External SLAs
- 供应商Vendor Management
- Service Dashboard

Information Technology Resiliency 弹性

- Availability Management
- Resiliency Analysis
- Capacity Planning

Asset Management

- Service Costing
- Operational Budgeting 运营预算
- Charge Back 计费表
- Investment Budgeting 投资预算

Application Performance Monitoring

Service Support

Configuration Management

- Capacity Planning
- Software Management
- Physical Inventory 实物盘点
- Automated Asset Discovery
- Configuration Management

Incident Management

- Security Incident Response
- Automated Ticketing
- Self-Service
- Ticketing
- Cross Cloud Security Incident Response

Problem Management

- Event Classifiation
- Root Cause Analysis
- Trend Analysis 趋势
- Problem Resolution
- Orphan Incident Management

Knowledge Management

- Best practices
- Trend Analysis
- Benchmarking
- Security Job Aids
- Security FAQ

Change Management

- Service Provisioning 供应
- Approval Workflow 批准工作流程
- Change Review Board 配置变更委员会
- Planned Changes
- Project Changes
- Operational Chages
- Emergency Changes

Release Management

- Scheduling
- Testing
- Version Control
- Build
- Source Code Management

Presentation Services

Presentation Modality 展示模式

- 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 输入验证

Security Knowledge Lifecycle

安全设计模式

- Security Design Patterns
- Attack Patterns
- Code Samples
- Security Application Framwrok - ACEGI

Integration Middleware

Development Process

Self-Service 压力测试

- Security Code Review
- Application Vulnerability Scanning
- Stress and Volume Testing

Software Quality Assurance

软件质量保障

Connectivity & Delivery

抽象化

- Abstraction

Information Services

Service Delivery

- Service Catalog
- SLAs
- OLAs
- 服务目录
- Contracts
- Recovery Plans
- 合同

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

Data Governance

- Risk Assessments
- Non-Production Data
- Information Leakage Metadata
- Data Segregation

Security Monitoring

- Session Events
- Authorization Events
- Authentication Events
- Application Events
- Network Events
- Computer Events
- HIPS
- Transformation Services
- NIPS Events
- Database Events
- Privilege Usage Events
- ACLs
- CRLs
- Compliance Monitoring
- NIPS Events
- DLP EVents
- eDiscovery Events

Service Support

- Configuration Rules (Metadata) 元数据
- Service Events
- Knowledge Repository 知识库
- Configuration Management Database (CMDB)
- Change Logs

Risk Management

- GRC
- RA
- BIA
- DR & BC Plans
- VRA
- TVM

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
  - Barriers 障碍
  - Electronic Surveillance
  - Security Patrols
  - Physical Authentication
- Asset Handling
  - Data
  - Hardware
  - Software
- Environmental Risk Management
  - Physical Security
  - Equipment Location
  - Power Redundancy

Patch Management

- Compliance Monitoring
- Service Discovery

Servers

- Secure Build
- Image Management

Equipment Maintenance

End Point

Storage Services

Network Services

- Network Segmentation
- Authoritative Time Source

Availability Services

Virtual Infrastructure

Desktop "Client" Virtualization

- Local
- Remote
  - Session-Based
  - VM-Based (VDI)

Storage Virtualization

- Block-Based Virtualization
  - Host-Based
    - LDM
    - LVM
    - LUN
  - Storage Device-Based
  - Network-Based
    - Appliance
    - Switched
- File-Based Virtualization

Application Virtualization

- Client Application Streaming
- Server Application Streaming

Virtual Workspaces

- Vertical Isolation 垂直隔离

Server Virtualization

Virtual Machines (Hosted Based)

- Full
- Paravirtualization
- Hardware-Assisted 硬件辅助
- OS Virtualization
- TPM Virtualization
- Virtual Memory

Network

Network Address Space

- IPv4
- IPv6
- External (VLAN)
- Internal (VNIC)

- Database Virtualization
- Mobile Device Virtualization
- Smartcard Virtualization

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 权利审查
- Policy Enforcement
- 政策执行点
- Policy Definition
- Policy Management
- 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

风险分类

- Source Code Scanning
- Risk Taxonomy

Infrastructure Protection Services

Server

- Behavioral Malware Prevention
- White Listing
- Sensitive File Protection
- Anti-Virus
- HIPS / HIDS
- Host Firewall

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

Network

- Behavioral Malware Prevention
- Firewall
- Content Filtering
- DPI
- NIPS / NIDS
- Wireless Protection
- Link Layer Network Security
- Black Listing Filtering

Application

- XML Applicance
- Application Firewall
- Real Time Filtering
- Secure Messaging
- Secure Collaboration

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

Cryptographic Services

Key Management

- Symmetric Keys
- Asymmetric Keys
- PKI
- Signature Services
- Data-in-use Encryption (Memory)
- Data-in-Transit Encryption (Transitory, Fixed)
- Data-at-Rest Encryption (DB, File, SAN, Desktop, Mobile)

Policies and Standards

- Operational Security Baselines
- Job Aid Guidelines
- Role Based Awareness
- Information Security Policies
- Technical Security Standards
- Data/Asset Classification
- Best Practices & Regulatory correlation

cloud security alliance℠

Co-Chairs: Jairo Orea, Yaron Levi, Dan Logan.
Team: Richard Austin, Frank Simorjay, Yaron Levi, Jon-Michael Brook, Jarrod Stenberg, Ken Trant, Earle Humphreys, Vern Williams

Date: 02/25/2013