Challenges for Cloud Hybrid Data Center and Large Security Tech Portfolio

1. **Huge Footprint with a Variety of Cloud Services**
   - IT assets on premise + various cloud (IaaS, PaaS, and SaaS)
   - Sensitive & regulated data in a cloud hybrid environment

2. **Want Speed & Great Security**
   - Achieve mission and response to customer demands faster
   - Environment can facilitate innovation & faster DevSecOps
   - Integrated security consistently executed

3. **Tech Portfolio with Overlaps and Gaps**
   - Typical CISO shop: 100-200 security tools & cloud security services
   - Overlap = potential wasted money
   - Gap = potential security risks

- **Comprehensive Cloud Security Architecture (CSA) Capability Framework**
- **State-of-the-art Built-in Defense**
- **Security Technologies Rationalization (STR)**
Threat Landscape & Assumptions for CSA Capability Framework

**Cloud Hybrid Data Center**
- IaaS (AWS)
- PaaS (Azure)
- SaaS (O365)

**Assumptions**
- Cloud tenancies are **NOT** hermetically sealed
- Direct Internet connections
- Connections from partners
- Run high-risk workloads with sensitive or regulated data
- All cloud deployments are **PUBLIC**

- Direct Internet connections
- Connections from partners
- Run high-risk workloads with sensitive or regulated data
- All cloud deployments are **PUBLIC**

- SharePoint
- OneDrive
- Sensitive Files
- Sensitive Emails

- Company Tenancy
- Private Value Added Networks
- Regional/Shared Services (S3, RDS, Glacier)
- Workloads (High Risk)
- Company VPC

- On-Premise Network
- Internet

- IOT
- Non-Company Voted
- Company Voted
- Mobile

- Attackers
- Partners
- Company Personnel

- Cloud tenancies are **NOT** hermetically sealed
- All cloud deployments are **PUBLIC**
Approach to Develop Build-in Security for Cloud Hybrid Data Center

What Defense to Build into Information Systems

- Public Standard (NIST 800-53)
  - Used NIST High baseline
  - Included 30 optional controls: DLP, Static Code Analysis

- Counter Top Cloud Sec Risks
  - Countermeasures to top cloud security risks
  - Threat model & risk scenarios

- Regulatory Boost
  - FFIEC
  - PCI DSS
  - GLBA
  - SOX
  - Internal Security Controls

173 Blocks of Vetted Cloud SA Requirements

How To Do (CSA Capability Framework)

- Security Arch Capability Framework
  - DLP
  - Data-at-Rest Encryption
  - AuthN/AuthZ
  - Vulnerability Scan

- Security Tools & Services
  - Vontu
  - AWS Encryption, KMS
  - AD/ADFS
  - Qualys
  - Splunk

Cloud SA Requirements

- Data at-rest encryption shall be implemented for all data processed & stored in cloud environments

SA Domain

- Data Security

SA Capabilities

- Data At-Rest Encryption
- Data Loss Prevention (DLP)

Sec. Tools and Services

- AWS Encryption, KMS, SafeNet KeySecure
- Symantec DLP, Mimesweeper, Q365 DLP
Key Technical Capabilities in Representative Security Domains

- 44 Capabilities in 9 security domains are needed to satisfy 173 blocks of Cloud Security requirements
- Remaining 48 capabilities are used to satisfy enterprise security and financial fraud management requirements
Cloud Security Architecture (CSA) Capability Framework Gives you a 2-Way Clarity

- Countermeasures to Top Cloud Security Risks, Attack Patterns, and Abuse Cases
- Internal Risk Mgmt Controls (NIST 800-53)
- IT Security Laws (GLBA, SOX), Regulations (FFIEC), Bank Policies, and Industry Standards (PCI)
- Control Objectives
- Security Arch Guidelines/Requirements
- Security Scenarios
- Security Architecture Capabilities
- Security Architecture Patterns
- Justification
- Traceability

- On Premise Security Tools
- Security Services in IaaS (AWS)
- Security Services in PaaS (Azure)
- Security Services in SaaS (O365)

- Secure Config Std.
- Acct Structure, Role Policy
- Secure Network Config
- AWS Cloud Formation Template
CSA Capability Framework Can Rationalize Your Security Technologies

Clarify & Simplify Your Portfolio
- Top 20 View
- Full Portfolio View
- Heatmap

Reduce Security Risks
- Portfolio Level
- Tool Level

Save Money
- Common tools
- Identify & retire duplicative & EOL tools

Better Cost Efficiency
- Feature Utilization
- License Utilization
Thank You. Any Questions?

- Lian Jin
- 301-684-8439
- liansec2012@hotmail.com
- https://www.linkedin.com/in/lian-jin-1484401/
Appendix

Security Architecture Capability Framework

- They represent common state-of-the-art technical capabilities that can be built-into information system to protect data & IT assets in a cloud hybrid DC
- 96 technical capabilities are divided into 10 security domains + a Financial Fraud Management (FFM) domain

### Server/Workload Security
- Anti-Malware on Server
- Advanced Malware on Server
- Sensitive File Protection
- Server Virtualization Security
- Host Firewall on Server
- HIPS/HIDS & Anomaly Detection
- App White Listing on Server
- Secure Configuration & Server Lockdown
- Trustworthiness Protection

### Network Security
- Network Firewall, Gateway
- Network Segmentation, Flow Control
- Secure Wireless
- NIDS/NIPS
- Content Filtering, Proxy, SSL Visibility
- Secure DNS, DHCP, IPAM, L2D
- Network Access Control (NAC)
- Email Protection (Network Based)
- Secure Remote Access (VPN)
- Advanced Malware Detection & Mgmt.
- Network Anomaly Detection
- DDoS Mitigation

### Endpoint / Mobile Security
- Anti-Malware on Endpoint
- App White Listing on Endpoint
- Host Firewall on Endpoint
- Advanced Malware Mgmt. & EDR
- MOM/NAM Security
- Mobile Anti-Malware
- Secure Configuration & Endpoint Lockdown
- Trustworthiness Protection

### Financial Fraud Management
- Transaction Anomaly Detection & Response
- Behavioral Fraud Detection
- Consumer Endpoint Fraud Protection
- Brand Protection
- Financial Threat Intelligence

### Identity and Access Management
- Authoritative Directory Service
- Identity Management
- Authentication Management
- Privileged Access Management
- IAM Governance
- Credential Management

### Application / Middleware Security
- Web Application Firewall
- API/SOA Protection
- AppSec Frameworks, Libraries, Components
- Static Code Analysis
- Dynamic App Scan
- Threat Modeling
- Code Hardening / Reverse Eng. Protection

### Data Security
- Data-at-Rest Encryption
- Encryption Key Mgmt.
- Data-in-Transit Encryption
- Data Loss Prevention (DLP)
- Secure Data Backup & Recovery
- Database Protection
- Data Tokenization, Truncation
- Data Obfuscation, Masking, Redaction
- Digital Signature / eSignature
- Secure Disposal of Data
- File/Data Integrity Protection
- Data Discovery, Classification, Tagging
- Digital Rights Management
- eDiscovery Email / IM Journaling

### Governance Risk & Compliance (GRC)
- IT Security Risk Management
- Policy & Standard Management
- Compliance & Audit Management
- Mandatory Security Control

### Security Operations
- Automated System Risk Analysis
- Security Awareness & Training, User Testing
- Security Asset Mgmt.
- Security Patch Mgmt.
- Incident Response
- Containment and Malware Analysis
- User Behavior Analytics and Insider Threat
- Packet Captures

### Threat and Vulnerability Management (TVM)
- Vulnerability Scan and Mgmt.
- Compliance Testing & Mitigation
- Penetration Testing
- Threat Intel, Hunting & Mgmt.
- Deception, Honey Pot
## Sample CSA Capabilities to NIST Controls Mapping

<table>
<thead>
<tr>
<th>Security Architecture Capability</th>
<th>NIST Control Family &amp; Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMS: Dynamic Application Scanning</td>
<td>RISK ASSESSMENT</td>
</tr>
<tr>
<td></td>
<td>RA-5 (VULNERABILITY SCANNING)</td>
</tr>
<tr>
<td>AMS: SOA / API Firewall</td>
<td>SYSTEM AND COMMUNICATIONS PROTECTION</td>
</tr>
<tr>
<td></td>
<td>SC-7 (BOUNDARY PROTECTION)</td>
</tr>
<tr>
<td></td>
<td>SC-23 (SESSION AUTHENTICITY)</td>
</tr>
<tr>
<td></td>
<td>SYSTEM AND INFORMATION INTEGRITY</td>
</tr>
<tr>
<td></td>
<td>SI-3 (TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS)</td>
</tr>
<tr>
<td>AMS: Static Code Analysis</td>
<td>SYSTEM AND SERVICES ACQUISITION</td>
</tr>
<tr>
<td></td>
<td>SA-11 (1) (STATIC CODE ANALYSIS)</td>
</tr>
<tr>
<td>AMS: Web Application Firewall</td>
<td>SYSTEM AND COMMUNICATIONS PROTECTION</td>
</tr>
<tr>
<td></td>
<td>SC-7 (BOUNDARY PROTECTION)</td>
</tr>
<tr>
<td></td>
<td>SYSTEM AND INFORMATION INTEGRITY</td>
</tr>
<tr>
<td></td>
<td>SI-3 (TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS)</td>
</tr>
<tr>
<td>DS: Data Discovery, Classification, and Tagging</td>
<td>ACCESS CONTROL</td>
</tr>
<tr>
<td></td>
<td>AC-16 (1) (DYNAMIC ATTRIBUTE ASSOCIATION)</td>
</tr>
<tr>
<td></td>
<td>AC-4 (1) (OBJECT SECURITY ATTRIBUTES)</td>
</tr>
<tr>
<td>DS: Data Loss Prevention (DLP)</td>
<td>ACCESS CONTROL</td>
</tr>
<tr>
<td></td>
<td>AC-4 (4) (CONTENT CHECK ENCRYPTED INFORMATION)</td>
</tr>
<tr>
<td></td>
<td>AUDIT AND ACCOUNTABILITY</td>
</tr>
<tr>
<td></td>
<td>AU-13 (1) (USE OF AUTOMATED TOOLS)</td>
</tr>
<tr>
<td></td>
<td>SYSTEM AND COMMUNICATIONS PROTECTION</td>
</tr>
<tr>
<td></td>
<td>SC-7 (10) (PREVENT UNAUTHORIZED EXFILTRATION)</td>
</tr>
<tr>
<td></td>
<td>SYSTEM AND INFORMATION INTEGRITY</td>
</tr>
<tr>
<td></td>
<td>SI-4 (18) (ANALYZE TRAFFIC / COVERT EXFILTRATION)</td>
</tr>
<tr>
<td></td>
<td>SI-4 (4) (INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC)</td>
</tr>
</tbody>
</table>

AMS - Application/Middleware Security  
DS - Data Security