How Good Security Architecture Saves Corporate Workers from Covid-19

Narudom Roongsiriwong, CISSP

MiSSConf(SP6), June 6, 2020

WhoAmI

- Lazy Blogger
  - Japan, Security, FOSS, Politics, Christian
  - http://narudomr.blogspot.com
- Information Security since 1995
- Web Application Development since 1998
- SVP, Head of IT Security, Kiatnakin Bank PLC (KKP)
- Committee Member, Thailand Banking Sector CERT (TB-CERT)
- APAC Research Advisory Council Member at Cloud Security Alliance Asia Pacific
- Consultant, OWASP Thailand Chapter
- Committee Member, National Digital ID Project, Technical Team
- Chief Information Security Officer (CISO) of the Year 2017, NetworkWorld Asia
- Contact: narudom@owasp.org

Me & COVID-19

- Jan 28, The first case was identified in Hokkaido
- Jan 29, An ANA's charter flight evacuating Japanese citizens from Wuhan's quarantined epicenter of the new COVID-19 outbreak arrived Tokyo
- Jan 31, I arrived Tokyo
- Feb 2, I arrived Hakodate, Hokkaido
- Feb 4, I arrived Sapporo, Hokkaido joining Sapporo Snow Festival which has been pinpointed as among a growing cluster of COVID-19 infections across Japan
- Feb 10, I went back to Bangkok
- Feb 14, The first case of an infected person found in Hokkaido
- Feb 24, Kiatnakin Bank announced that who has returned from COVID-19 risky country starting from Feb 11-24 must be inspected for COVID-19 self-quarantined for 14 days


Yakult
SUNTORY
SECOM

COVID-19, My Company & Work from Home

- Late January to March, 2020: Infrastructure preparation
  - Virtual App & Desktop servers setting up and burst licenses but not activated
  - VPN servers and burst licenses for non-production environment
  - Outgoing internet traffic bursting
  - Security redesigns
- March 17, Internal communication on how to Work From Home (WFH) during COVID-19 pandemic, how to install and use Virtual App, how to transfer office telephone to private phone number
- March 18, Delegation revision

ข้อแนะนำด้านความมั่นคงปลอดภัยเมื่อต้องทำงานจากที่บ้าน

Bangkok Post

Bangkok malls to close from Sunday

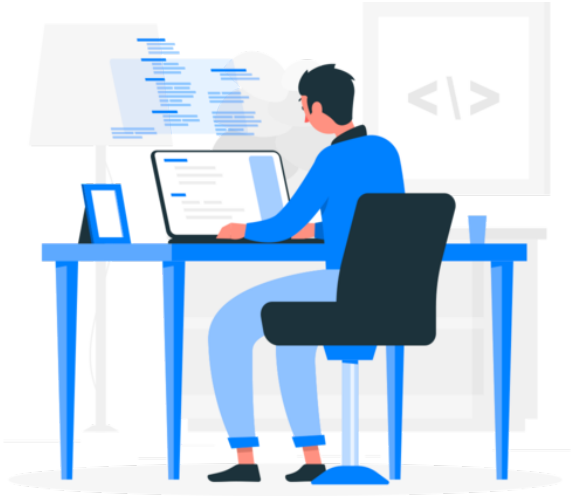
Expanded shutdown to last until April 12, with exceptions for supermarkets, pharmacies and take-out restaurants

PUBLISHED : 21 MAR 2020 AT 15:46
UPDATED: 21 MAR 2020 AT 17:46

WRITER: SUPOJ WANCHAROEN AND ONLINE REPORTERS

COVID-19, My Company & Work from Home

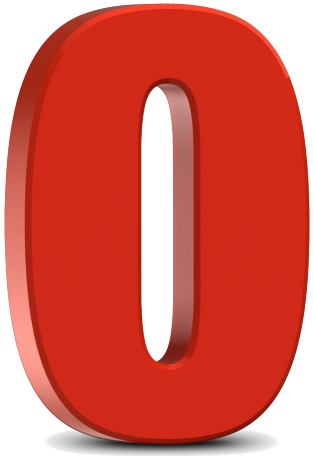
- March 23, Internal communication on rules of using internal systems from personal devices according to Work From Home during COVID-19 pandemic
- March 24, I started working from home



Application Class Restriction

- Financial Transaction Operation → On Premise Only
- On-Premise Non-Transaction Operation → Virtual App
- Cloud Applications → Native from Anywhere
- Non-Production Environment → VPN

KK COVID-19 Related Statistics



Employees Infected

Work from Home

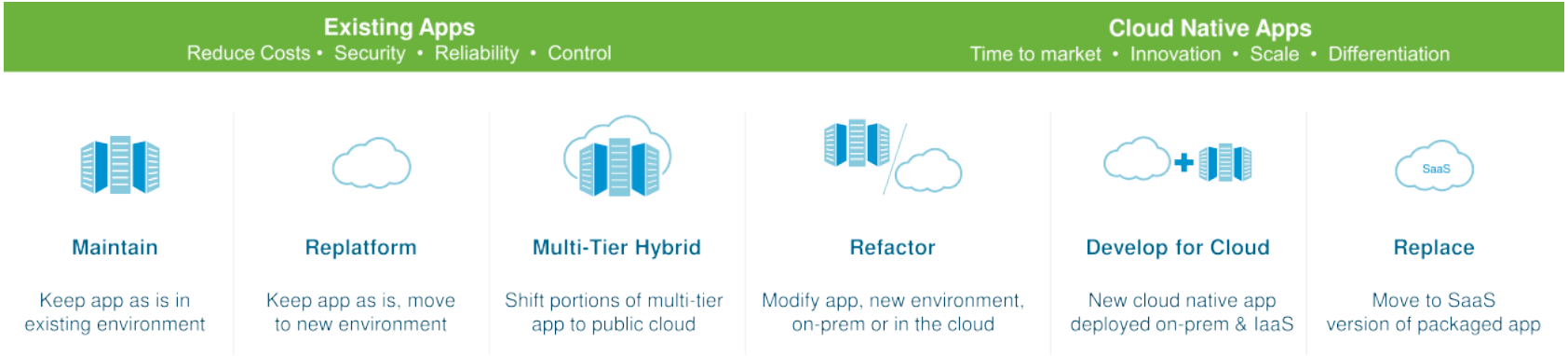
2 Years Ago

- The first cloud based e-learning application was up and running with troublesome for IT help desk

Lessons Learned from the First Move

- Moving to cloud computing without architectural design leads to troublesome
- Without cloud security architecture, it could lead to disaster
- There are missing components those could help moving to cloud computing effectively

Multi-Cloud Architecture



- We adopt many cloud strategies at the same time
- Multi-Cloud is unavoidable

The image is from vmworld2017

What is Multi-Cloud?

This term reflects the strategic decision to use multiple cloud environments—public, private, or hybrid—to run enterprise applications, and the decision to use a mix of cloud service providers.

Why Use a Multi-Cloud Architecture?

- Choice: Flexibility and the ability to avoid vendor lock-in.
- Disaster Avoidance: Ensures that you always have compute resources and data storage available so you can avoid downtime.
- Compliance: Many multi-cloud environments can help enterprises achieve their goals for governance, risk management and compliance regulations.

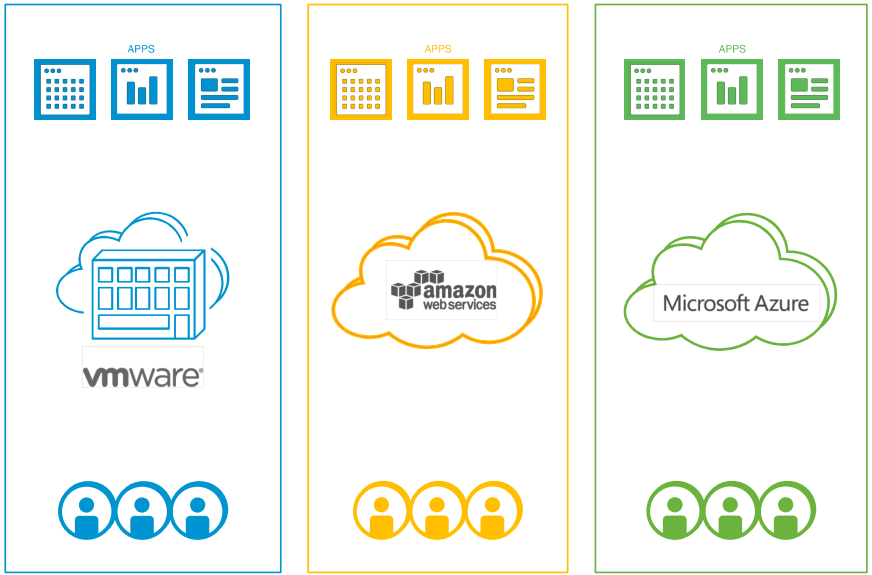
How Secure is Multi-Cloud?

- Multi-cloud security has the specific challenge of protecting data in a consistent way across a variety of cloud providers
- Third-party partners handle different aspects of security
- The importance is to clearly define and distribute security responsibilities among the parties

Design Strategies in Multi-Cloud Architecture

- Maintain Few IaaS Providers
- Secure Identity Management
- Backup Data to On-Premise
- Do Data De-Indentification

Strategy #1: Maintain Few IaaS Providers



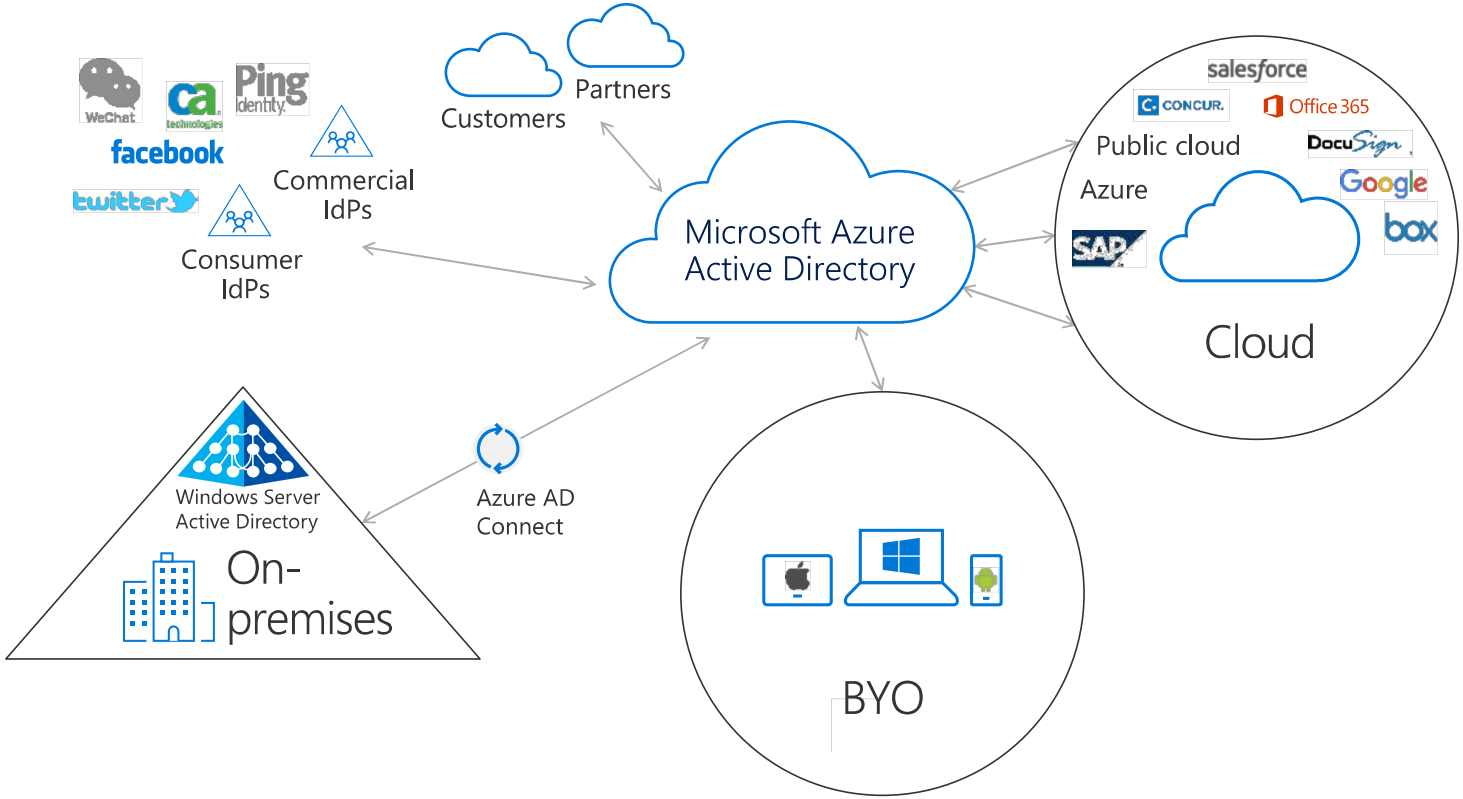
- Limit different expertise, environments and tools
- Reduce operational complexity
- Limit risk exposure

The image is from vmworld2017

Strategy #2: Secure Identity Management

- Retail customer users are not the main problem, all access from the Internet
- Organizational users are the real problem, either SSO or active directory is widely used in the existing environment
- The best way is to export the existing organizational user authentication to centralized cloud identity management for cloud based applications' authentication
- Recommend tactics
  - Always synchronize or export from on premise to cloud
  - Do not allow the external pull user identity but push to the external
  - Store hash of hash on the external

Strategy #2 Example: Microsoft Azure AD



**The image is from Mircosoft Azure*

Strategy #3: Backup Data to On-Premise

- Ensure that we backup necessary data set need to continue running the business
- Incrementally backup to on-premise
- Do not always rely on cloud service providers
- Think if we have to terminate the service provider without data backup

Strategy #4: Do Data De-Identification

- De-identification is the process used to prevent someone's personal identity from being revealed
- Deidentified data cannot be linked to any one individual account
- De-identification techniques include:
  - Pseudonymization
  - Anonymization

Key Components: Office Suite for Business

**The image is from computerworld.com*

Rooms for Security Improvement

- 2nd factor authentication enforcement for cloud applications from day one
- Security redesigns to adopt cloud security services
  - On-premise access controls
  - Cloud-native, security information event management (SIEM) and security orchestration automated response solution

COVID-19 Accelerates Transformation Cycle


Q&A