RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

Session ID: CDS-F01

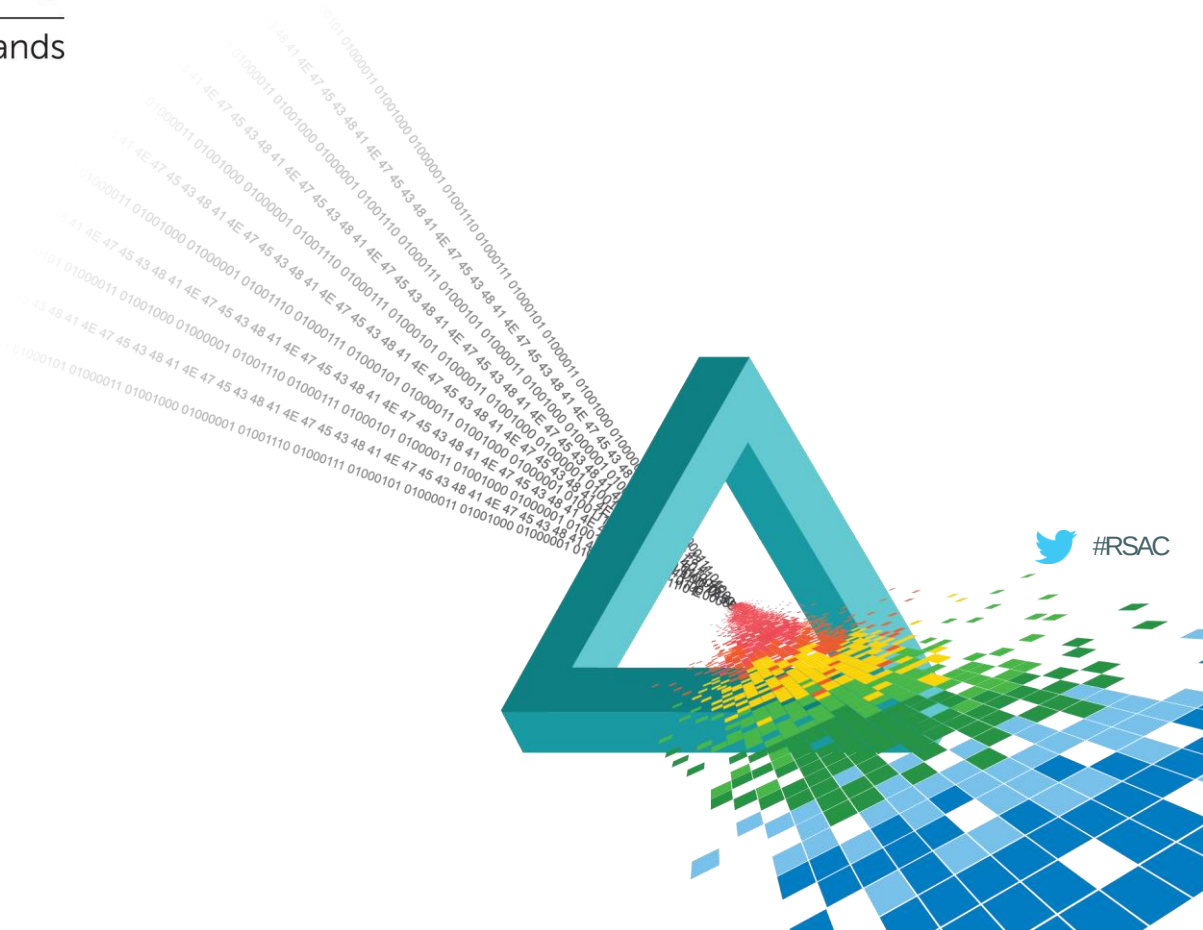
Optimizing the Mobile Cloud Era Through Agility and Automation

#RSAC

Edwin Lee
Director of Enterprise Solutions, ASEAN
AirWatch by VMware

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands



#RSAC

Industry Trends

Explosive Growth of Mobile

Mobile worker population will reach

1.3 Billion in 2015

Source: IDC Worldwide Mobile Worker Population 2011-2015 Forecast

Tablets are forecasted to reach

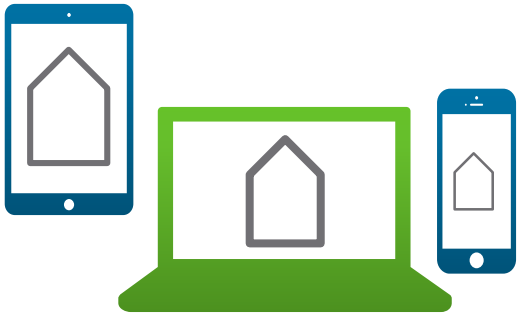
468 Million in 2017

Source: Gartner Forecast: Devices by Operating System and User Type, Worldwide 2010-2017, 3Q13 Update

Smartphones forecasted to reach

2.1 Billion in 2017

Source: Gartner Forecast: Devices by Operating System, Worldwide, 2010-2017, 3Q13 Update



60+%

…of people reported they are using their personal device at work

Source: Gartner Device: The Facts and the Future, 11 April 2013

Business Mobility Transformation

3.5 Billion

Deployed globally by 2019

Source: Forrester Research World Mobile And Smartphone Adoption Forecast, 2014 To 2019 (Global: August 2014)

> 50%

Customer-facing and employee-facing IT investments will be mobile-focused

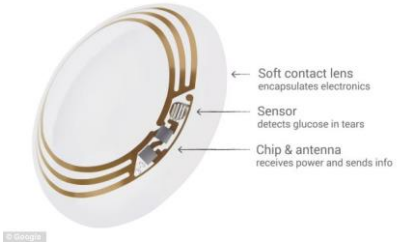
Source: Gartner 2015 CIO Agenda: 2,810 CIOs responded to this year's survey, representing approximately $397 billion in IT spending across 84 countries

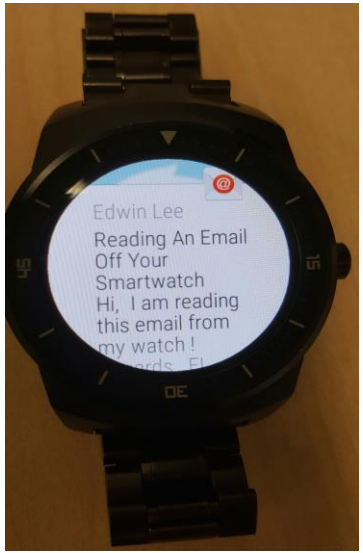
189 Billion

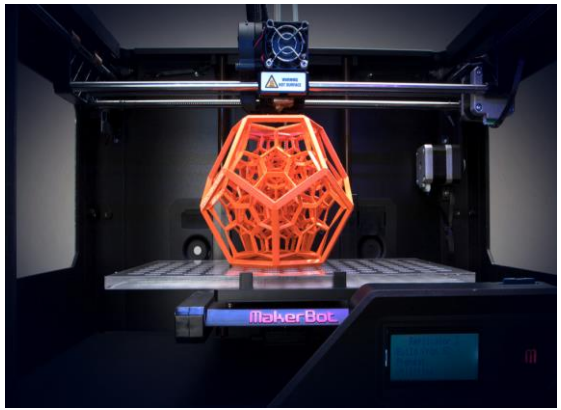
Invested to engineer platforms and processes for mobile engagement in 2017

Source: 2015: The Year Of The Mobile Singularity, Readwrite.com article, December 2014

The Mobile / Cloud Era is Changing How We Work


Soft contact lens
encapsulates electronics
Sensor
detects glucose in tears
Chip & antenna
receives power and sends info


Edwin Lee
Reading An Email Off Your Smartwatch
Hi, I am reading this email from my watch !


MakerBot

What Users Want: Any App on Any Device

What IT Wants: Mobile Cloud Architecture

Our Focus Today

Any Device

Any Application

One Cloud

Harnessing Mobile and Cloud Is Challenging

SECURITY

SLOW REPONSES

SERVICE OUTAGES

PROLIFERATION OF DEVICES

HIGH USER EXPECTATIONS

CLOUD SILOS

DECLINING BUDGET

INTEGRATION PROBLEMS

PRIVACY ISSUES

FRAGMENTED DATA CENTER

SHORTAGE OF RIGHT SKILLS

DIFFERENT APPLICATIONS

AGING INFRASTRUCTURE

LIMITED RESOURCES

New Approach to Mobile Security and Identity

Old Mindset

Only trust devices where you manage the OS

Device Trust established by the Domain

Access Controlled by Network Management

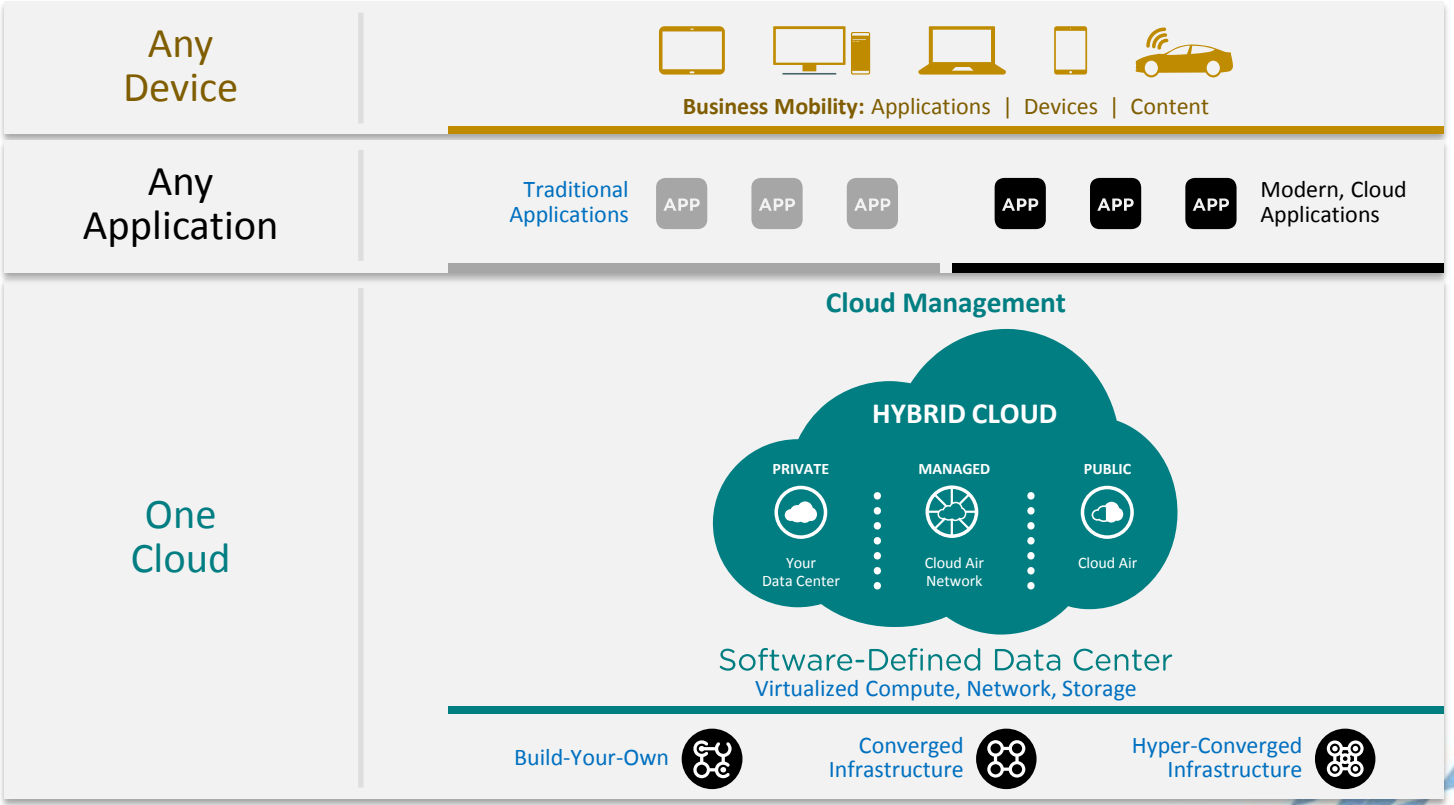
New Approach

Manage and secure apps and content

Device Trust established through enrollment

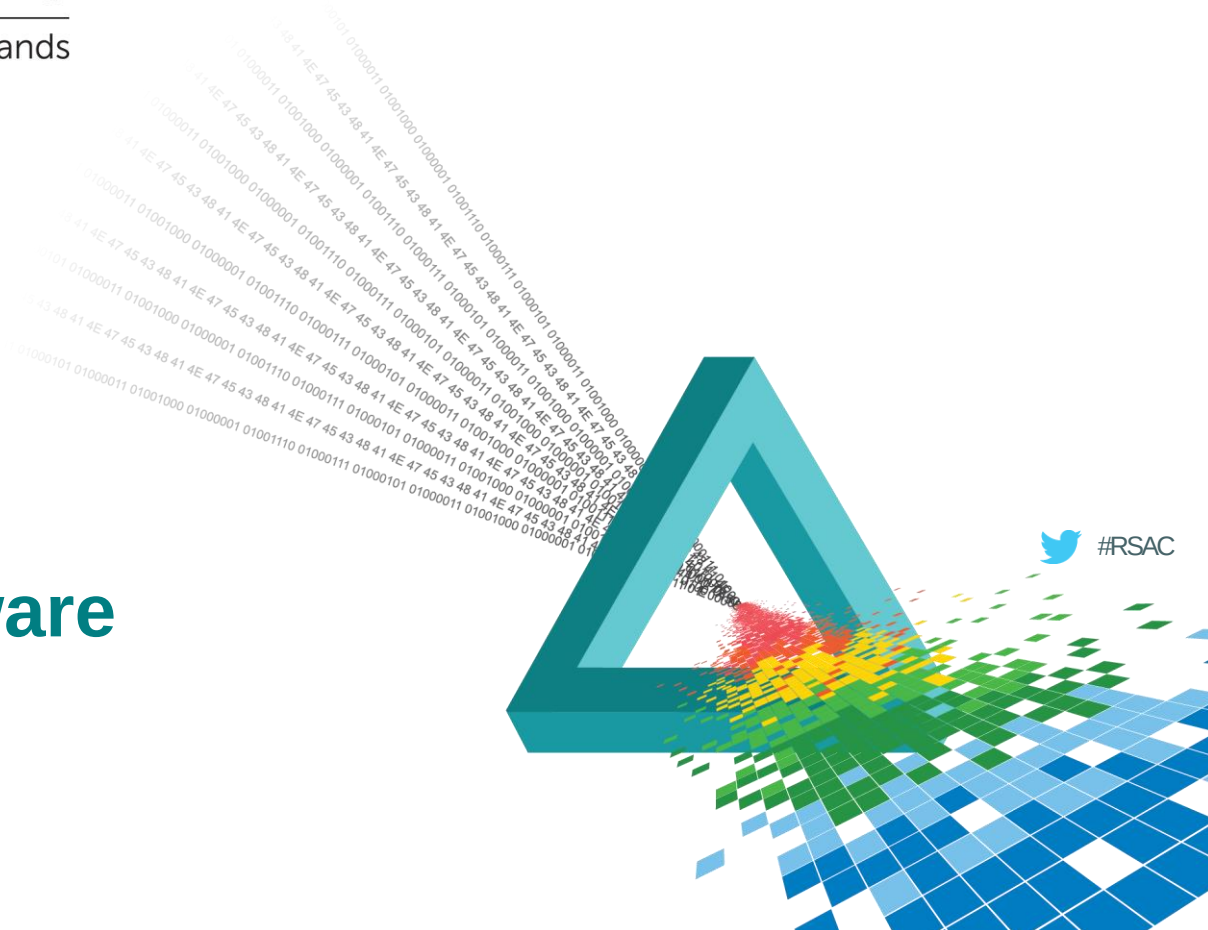
Access Controlled by Identity Management

Mobile Cloud Architecture



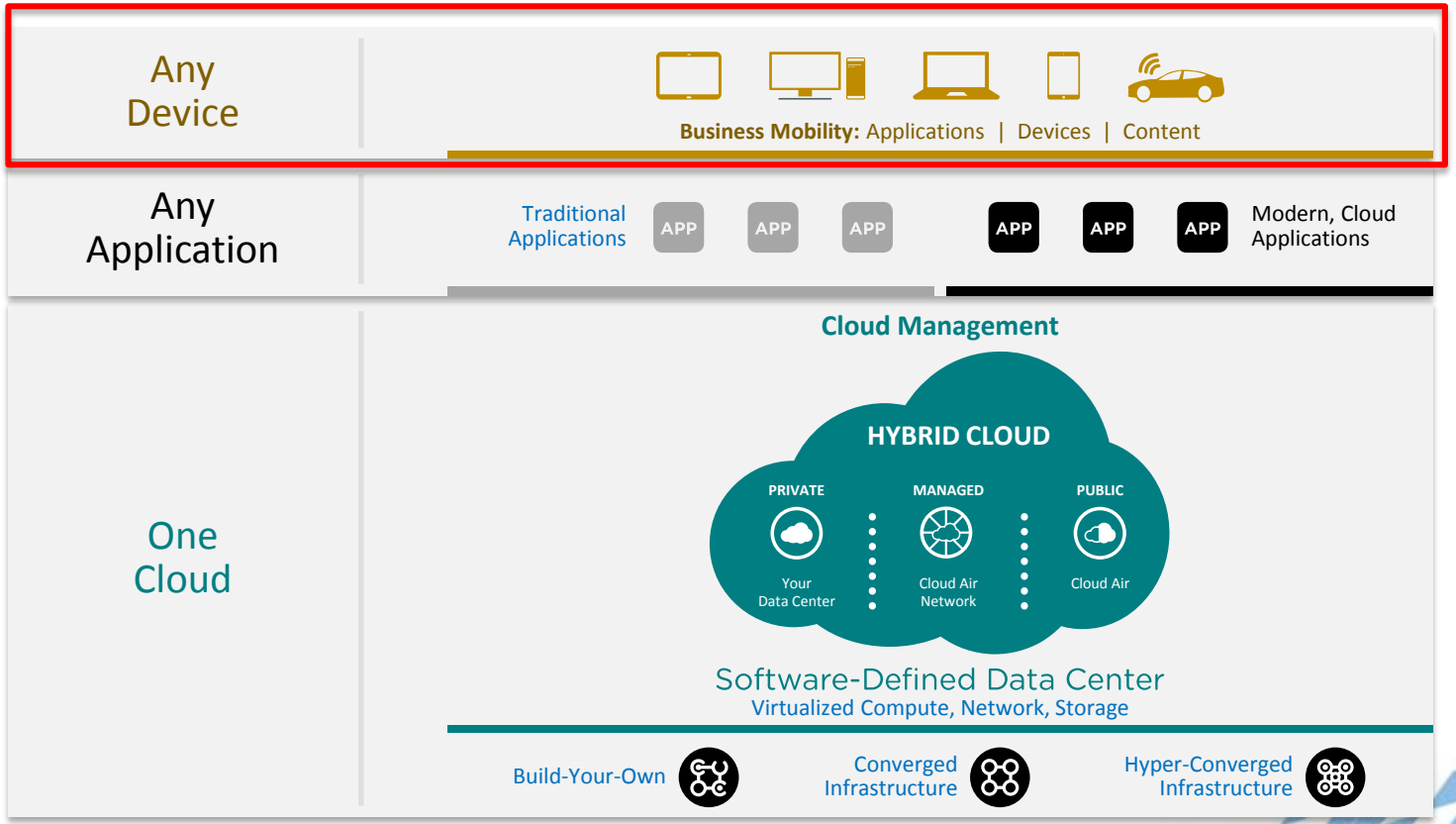
RSAConference2015

Singapore | 22-24 July | Marina Bay Sands



AirWatch by VMware

Mobile Cloud Architecture



Enterprise Mobility Management (EMM)

Apps

Browser

Content

Device

Email

Workspace

Video

Chat

Display

Teacher Tools

Mobile <insert space> Management

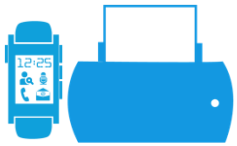
For Unified Endpoint Management

Every Endpoint

Mobile Devices

Laptops

Rugged Devices



Printers & Peripherals

Every OS

Every Use Case

Corporate BYOD

Shared

Line of Business

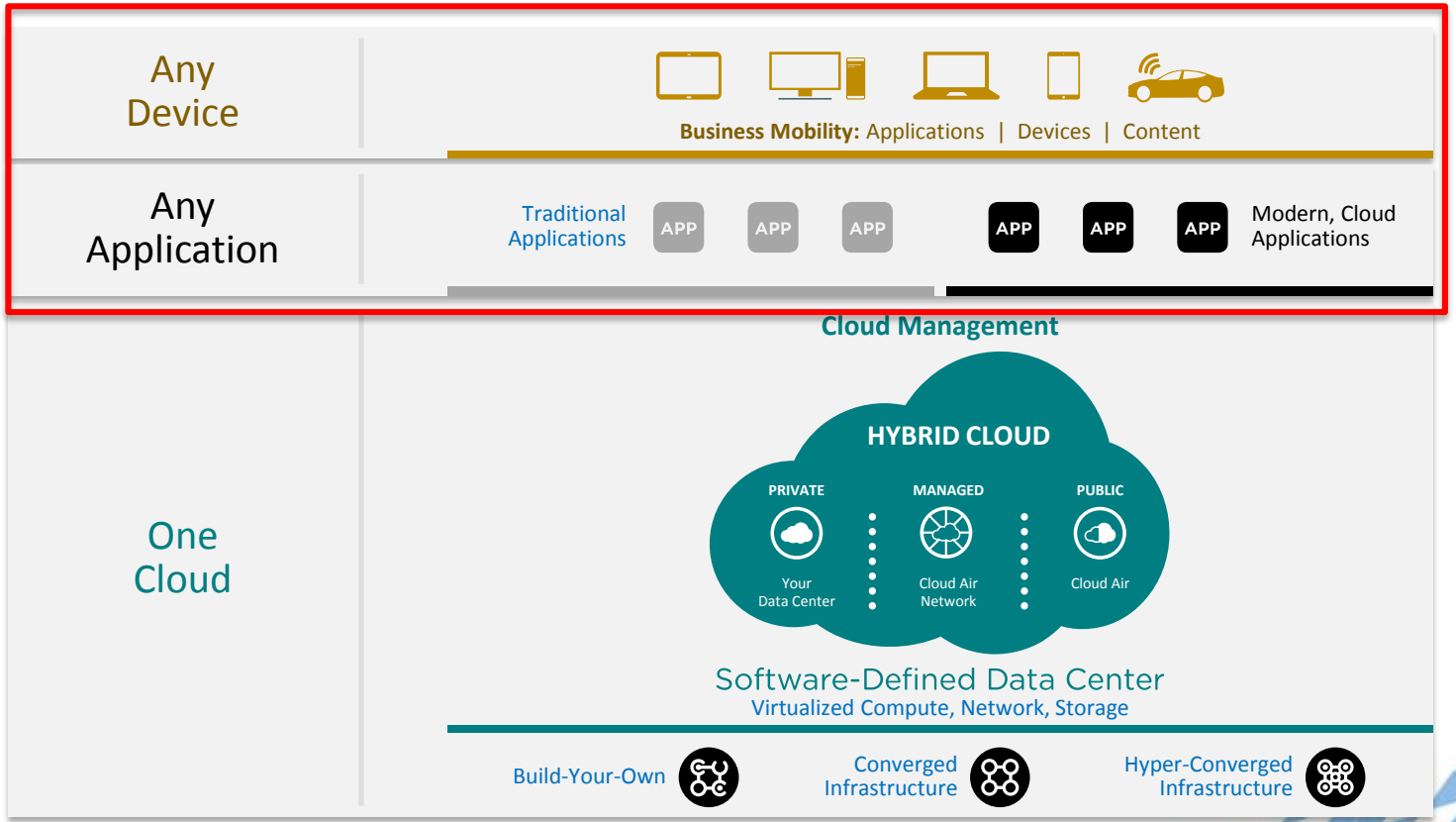
RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

#RSAC

VMware Identity Manager

Mobile Cloud Architecture



The Challenges Customers are Facing with Identity

Enforce security and compliance without hampering workers

Protecting apps and data from unauthorized access is important but authentication and ease of use needs to be straightforward

Time and complexity in delivering new apps and services services

Employees and their devices are increasingly on the go. Access control to apps becomes more important than networks. Device diversity adds to the complexity

Gaining visibility into user access. Who has access to when, and when

Real-time visibility, proactive alerting, reporting and analytics are all required to know what apps are being used, when, and by whom. This helps manage licensing, SLAs, and maintenance windows

Complexity of scale and growth (Operations, Helpdesk)

A general state of readiness to scale as traffic, users and devices grow in number across the organization

vmware®
Identity Manager

Simplify Business Mobility with One-touch From Any Device

- Enterprise Single Sign-On
- Industry leading support for Web, Windows, Native Mobile Apps – All from one place
- Pre-integrated with many enterprise apps

Optimize User Experience And Security with Airwatch® Adaptive Access

- Native integrated app launcher
- Dynamic per-App VPN
- AirWatch smart authentication
- Device Analytics

Empower Employees with a Self-Service App Store

- Self-service app catalog
- Responsive HTML5 app launcher
- User analytics
- Custom Brandable Web Portal
- Application provisioning

Grow with Trusted VMware Enterprise-grade Hybrid Cloud Infrastructure

- Directory integration and federation
- Hybrid deployment model
- Conditional Policy Engine
- Universal Authentication Broker

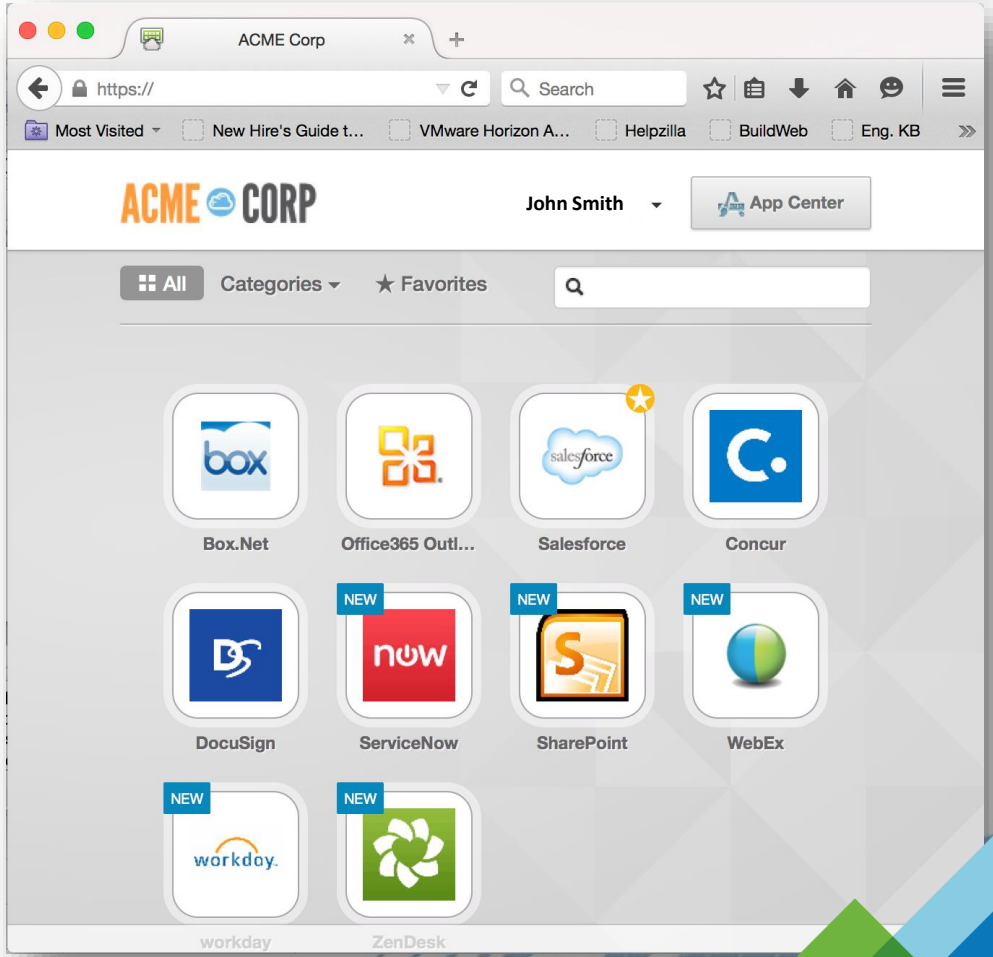
When Identity Management meets AirWatch Mobility Management

Native Mobile Single Sign-On

- ✓ No app wrapping or SDK
- ✓ One-touch authentication
- ✓ Managed or Unmanaged Conditional Access
- ✓ Built in CA
- ✓ Built in VPN
- ✓ Built in IdP
- ✓ Built in Kerb / Cert adapter

Empower employees

- Self-service app catalog
- Responsive HTML5 app launcher
- User analytics
- Custom skinned web portal
- Application provisioning



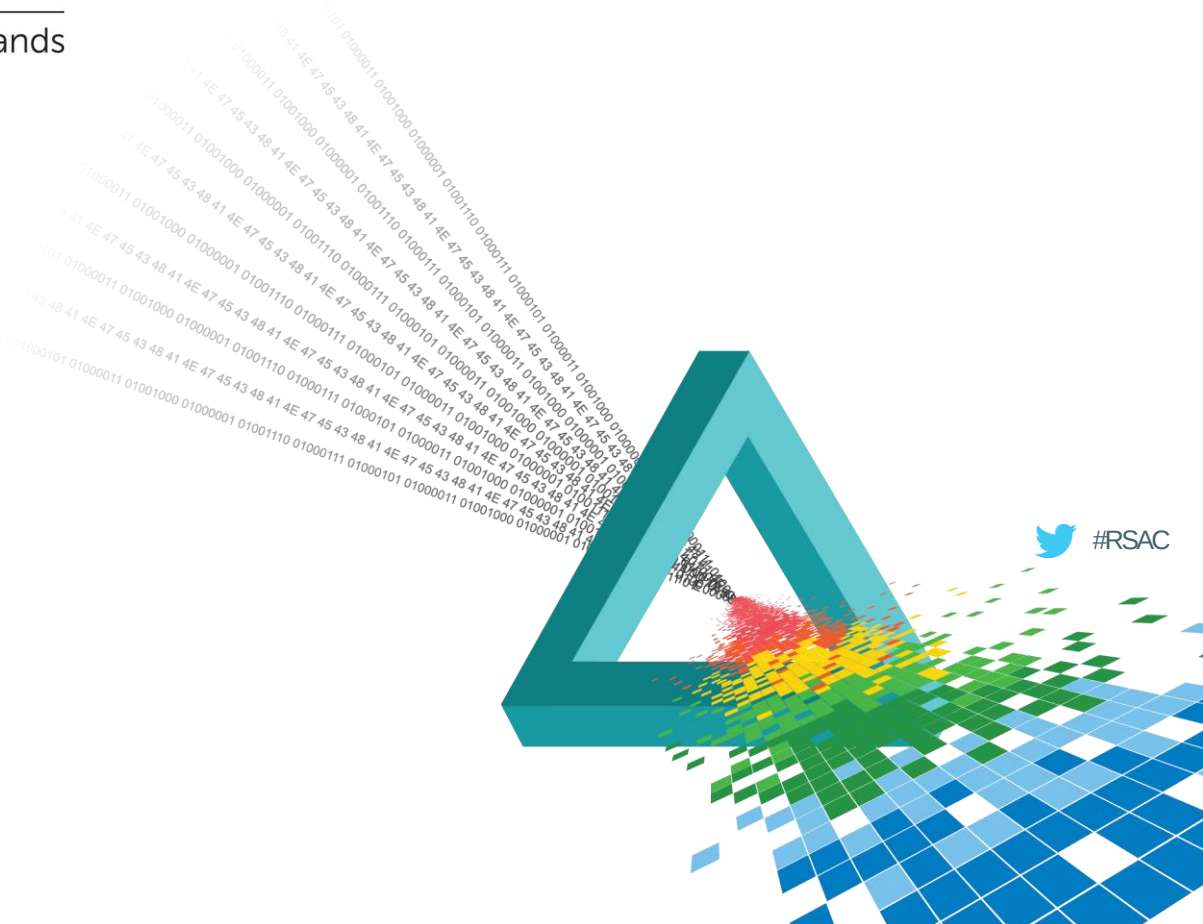
Grow with trusted VMware enterprise-grade infrastructure

- Directory integration and federation
- Hybrid deployment model
- Conditional Policy Engine
- Universal Authentication Broker

RSAConference2015

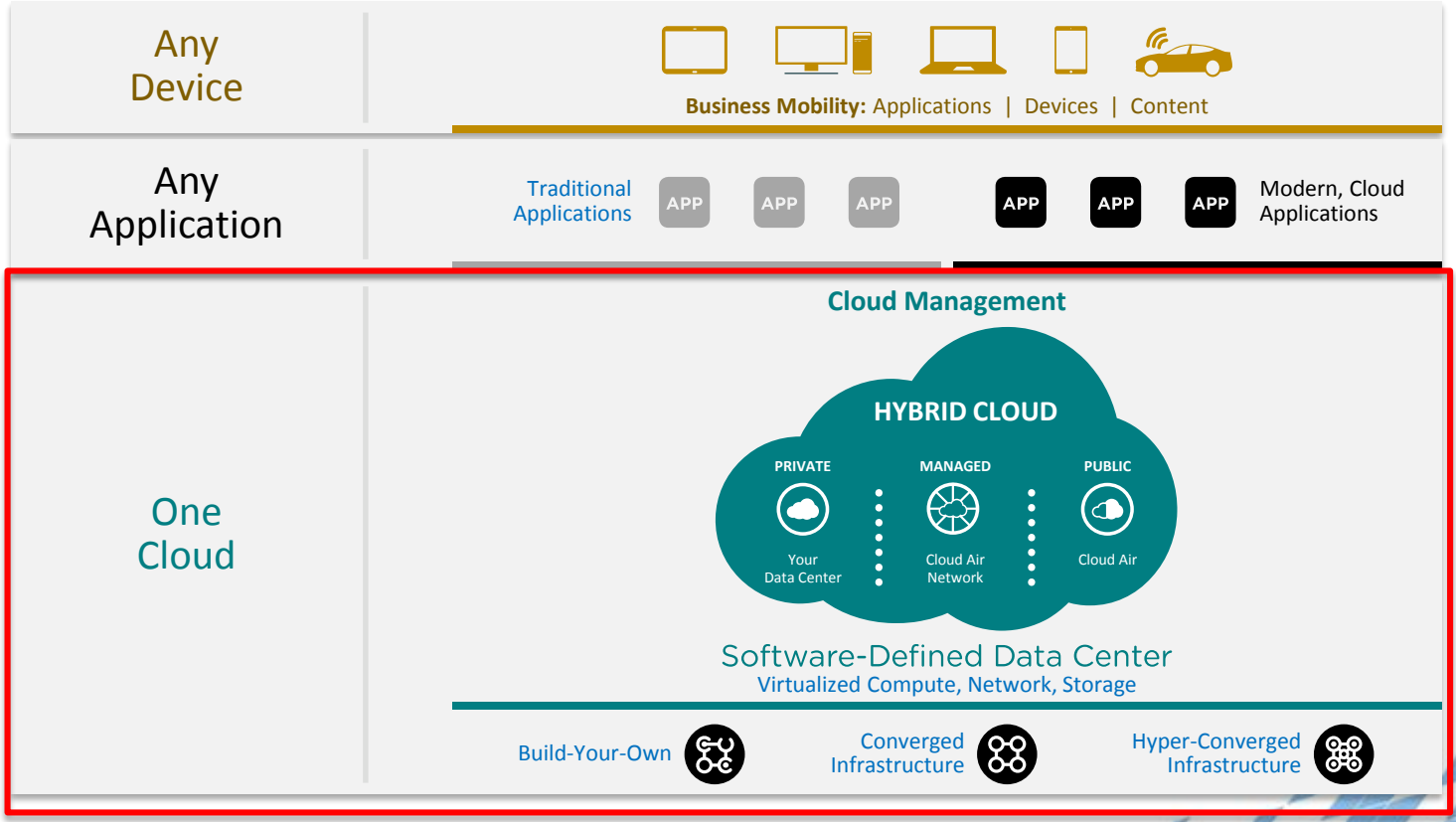
Singapore | 22-24 July | Marina Bay Sands

NSX



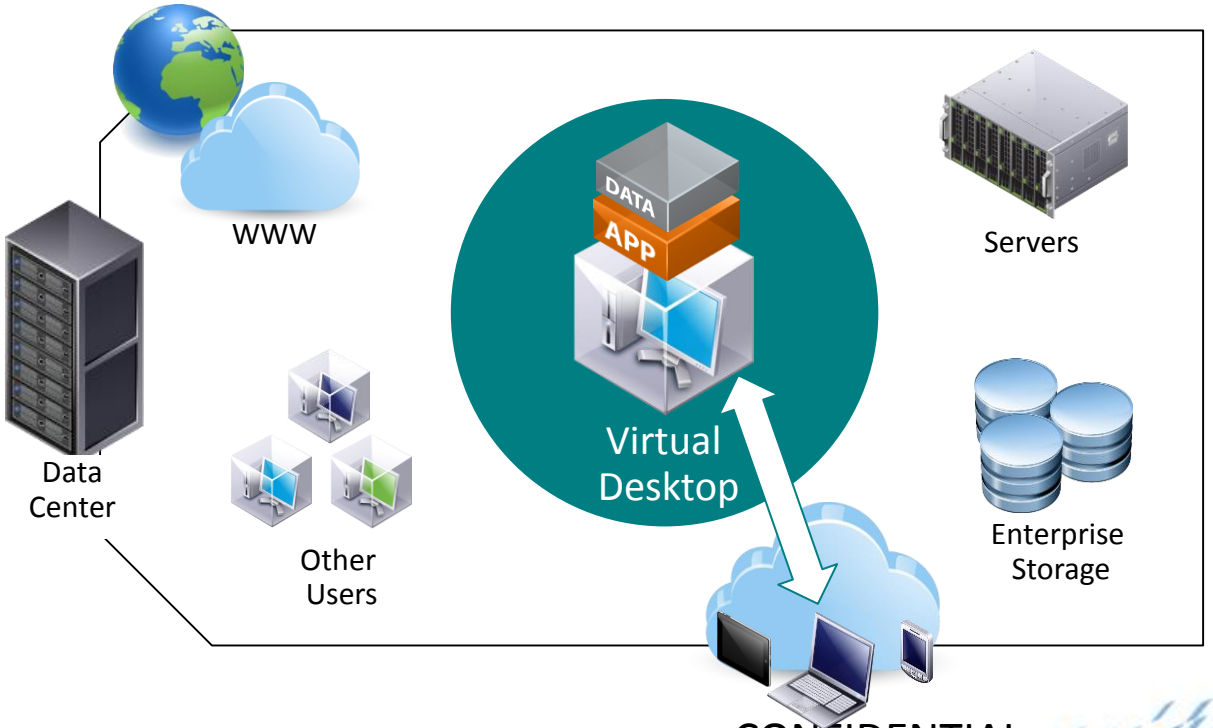
#RSAC

Mobile Cloud Architecture



Desktop & App Virtualization: Better Security for Data at Rest

Desktop and app virtualization places O/S, apps and data in the data center

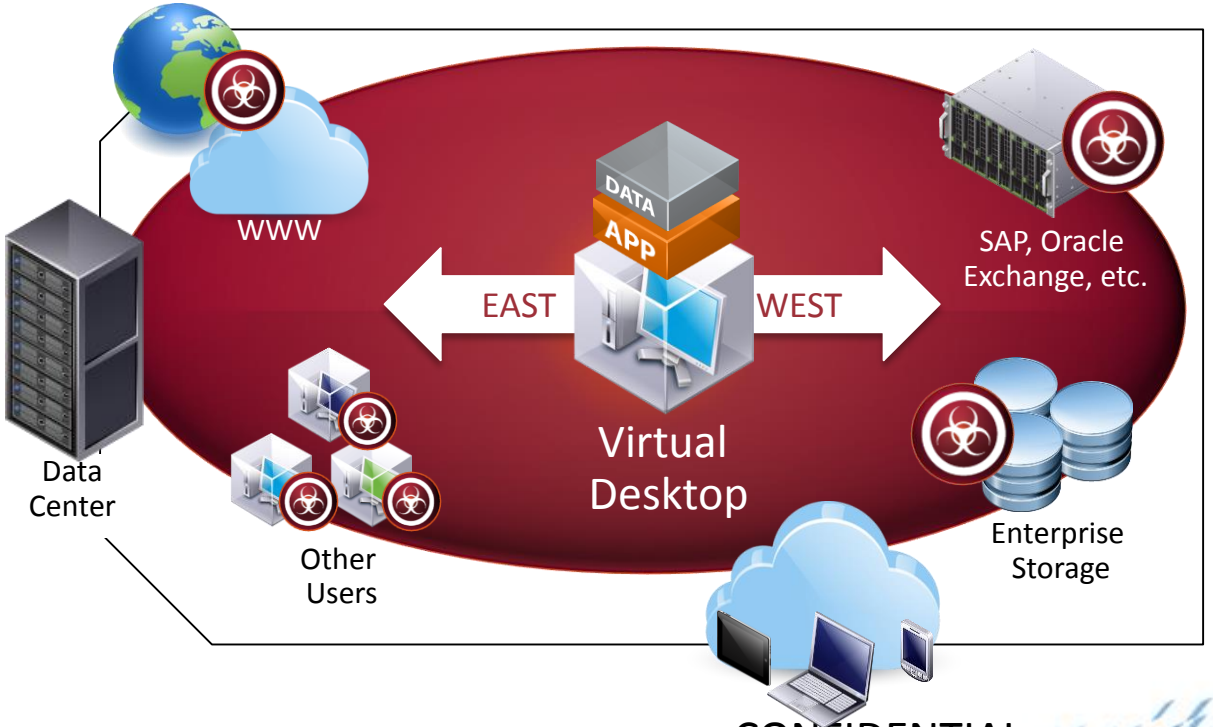


- ✓ Loss of data sitting on devices (device loss, theft, damage)
- ✓ Unauthorized access to sensitive applications installed on devices
- ✓ Reduced branch infrastructure footprint (file/print/email servers etc.)
- ✓ Conducive to efficient, centralized backup
- ✓ Centralized patching against vulnerabilities

Your Data Center = Much Larger Attack Surface

Desktop Virtualization poses new security considerations:

- Exposes very large attack surface within the data center
- Multiple “east-west” flows between users and infrastructure



What VDI Doesn’t Address:

User behaviors

Zero-day threats

Compromised
internet websites

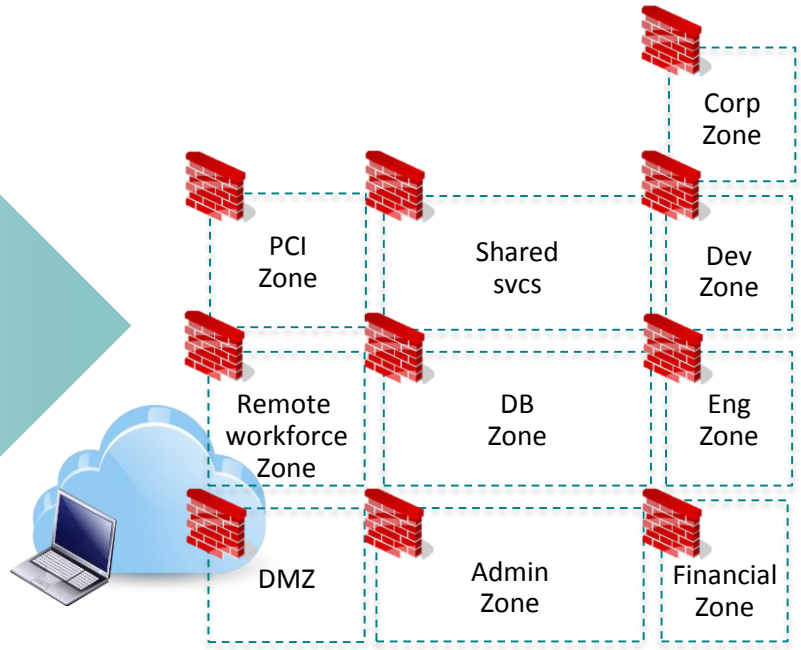
sktop-to-desktop hacking

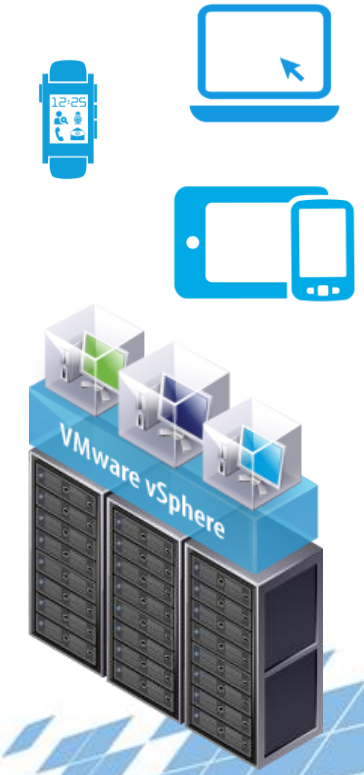
esktop-to-server hacking

Encapsulation

Organizations with focus on compliancy and risk mitigation will implement **security zones to protect East-West flows within the data center**

- Hard to implement
- Lots of physical infrastructure required
- Complex to manage

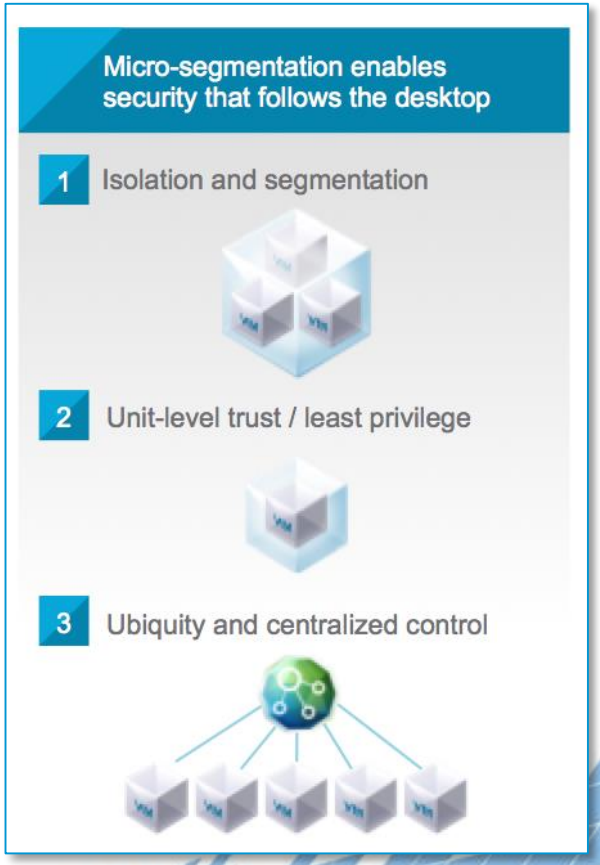




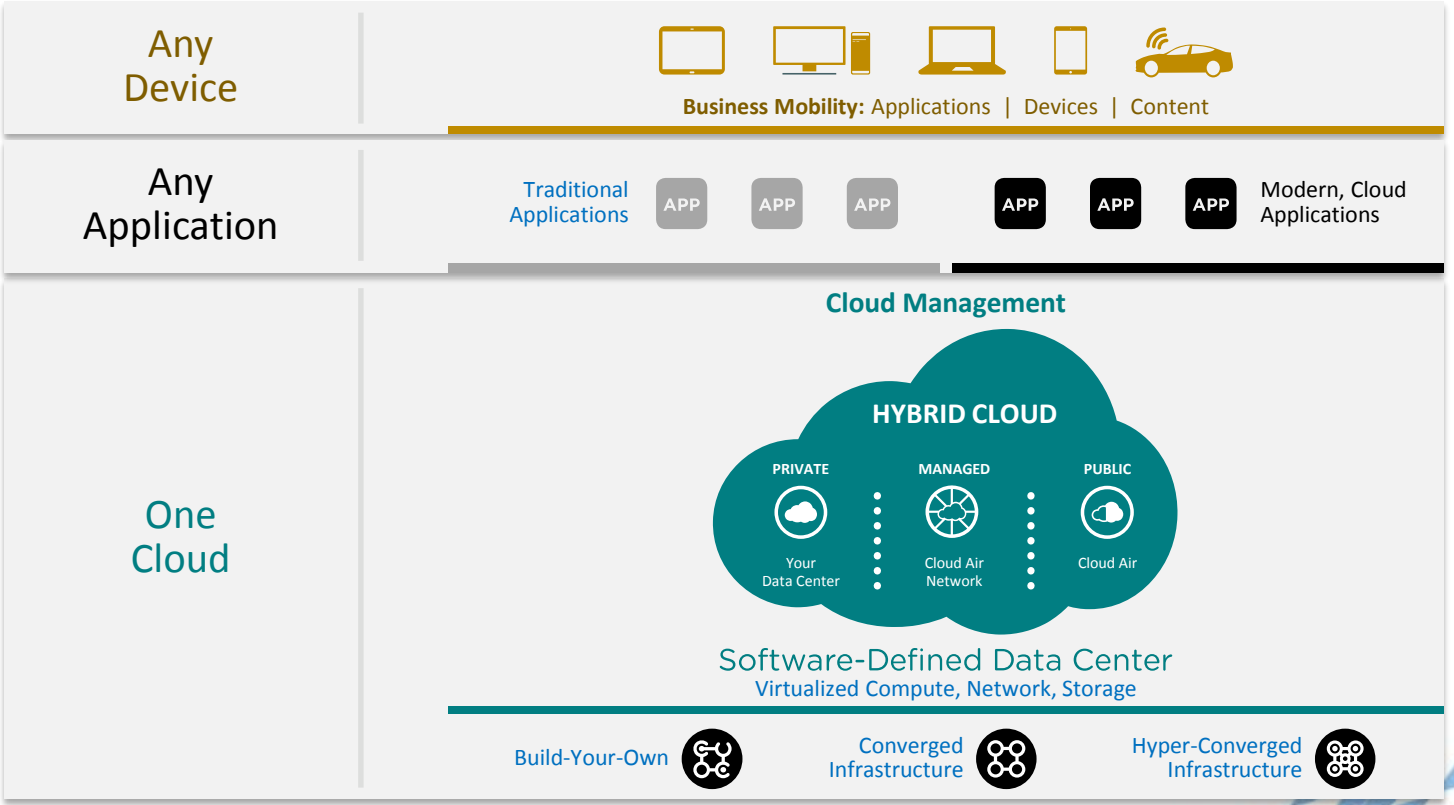
CONFIDENTIAL

NSX Micro-segmentation: Addressing the East-West Challenge

- Establish a **“network of one”** for each desktop
- **Eliminate cross-talk** between networks
- **Minimized attack surface** – keep threats from spreading
- **Policy defined centrally**, automatically attached to VM as created
- **Persistently follows desktop** wherever it resides



Mobile Cloud Architecture



Thank you!