RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: SPO1-R03

Limiting the Spread of Threats: A Data Center for Every User

Geoff Huang
Director Product Marketing
VMware

Tony Paikeday
Senior Product Marketing Manager
VMware

Why do breaches still occur?

Today's data centers are protected by strong perimeter defense.

But threats and exploits still infect servers. Low-priority systems are often the target.

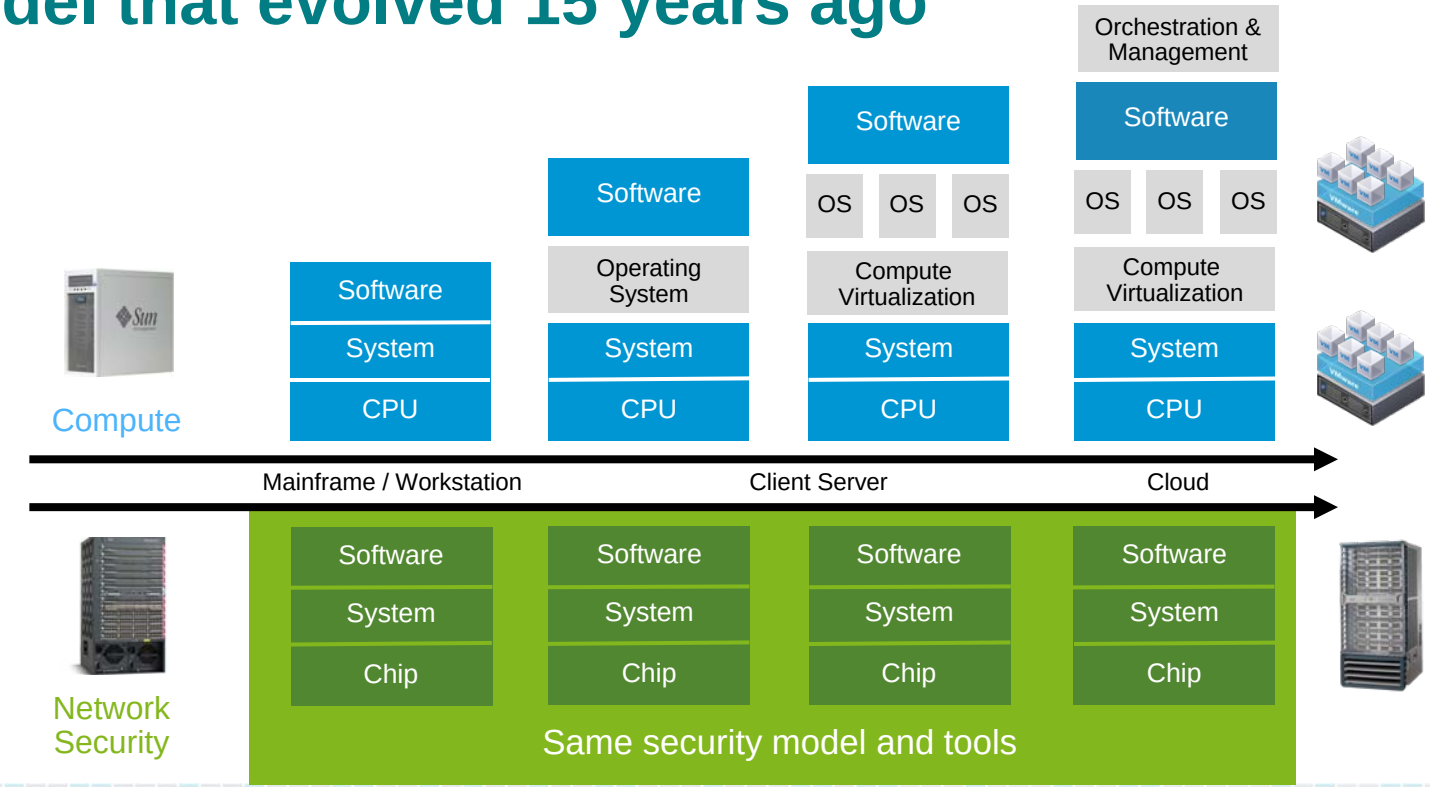
Threats can lie dormant, waiting for the right moment to strike.

Attacks spread inside the data center, where internal controls are often weak. Critical systems are targeted.

Server-server traffic growth has outpaced client-server traffic. The attack spreads and goes unnoticed.

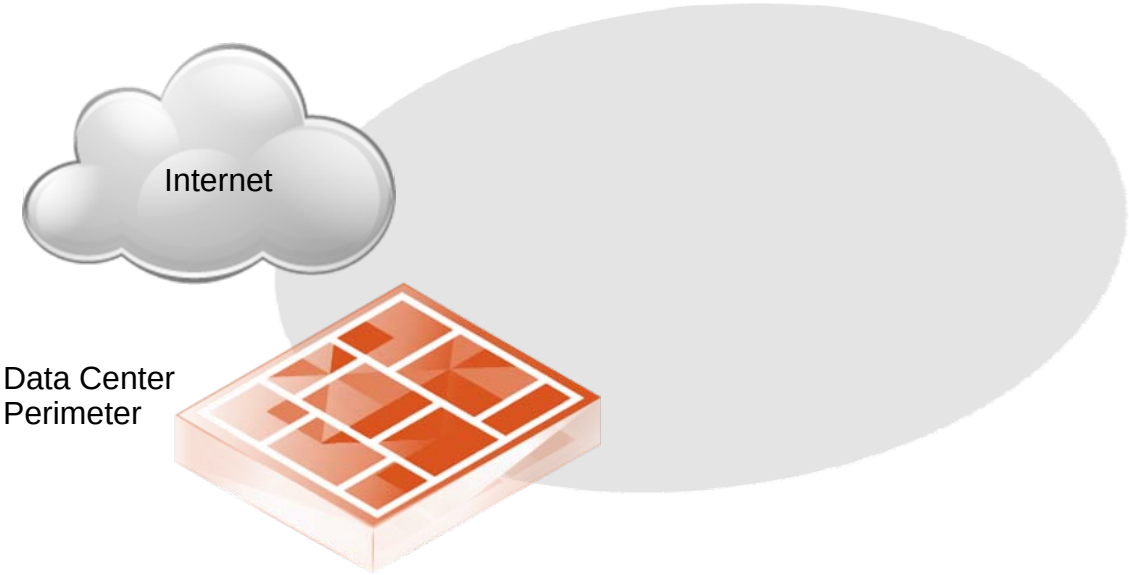
Possibly after months of reconnaissance, the infiltration relays secret data to the attacker.

Breaches are still occurring because of a security model that evolved 15 years ago



The legacy security model emphasized perimeter security

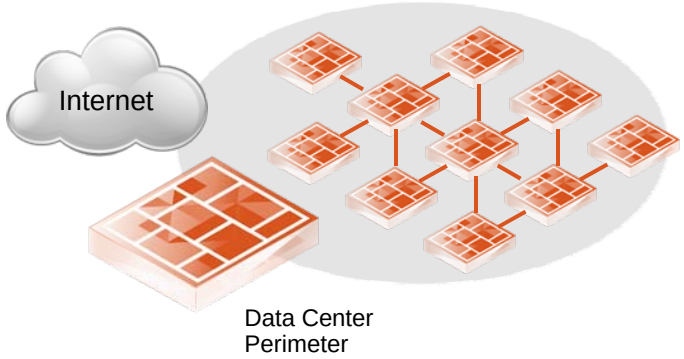
Perimeter-centric network security has proven insufficient



And is incompatible with a world where security is needed everywhere

Adding more internal security…

requires placing more firewalls across workloads



Physical Firewalls

Cost prohibitive with complex configurations

Virtual Firewalls

Slower performance, costly and complicated

What’s needed: a new architectural approach

Software-Defined Data Center

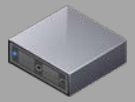
Applications

Virtual Machines

Virtual Networks

Virtual Storage

Data Center Virtualization



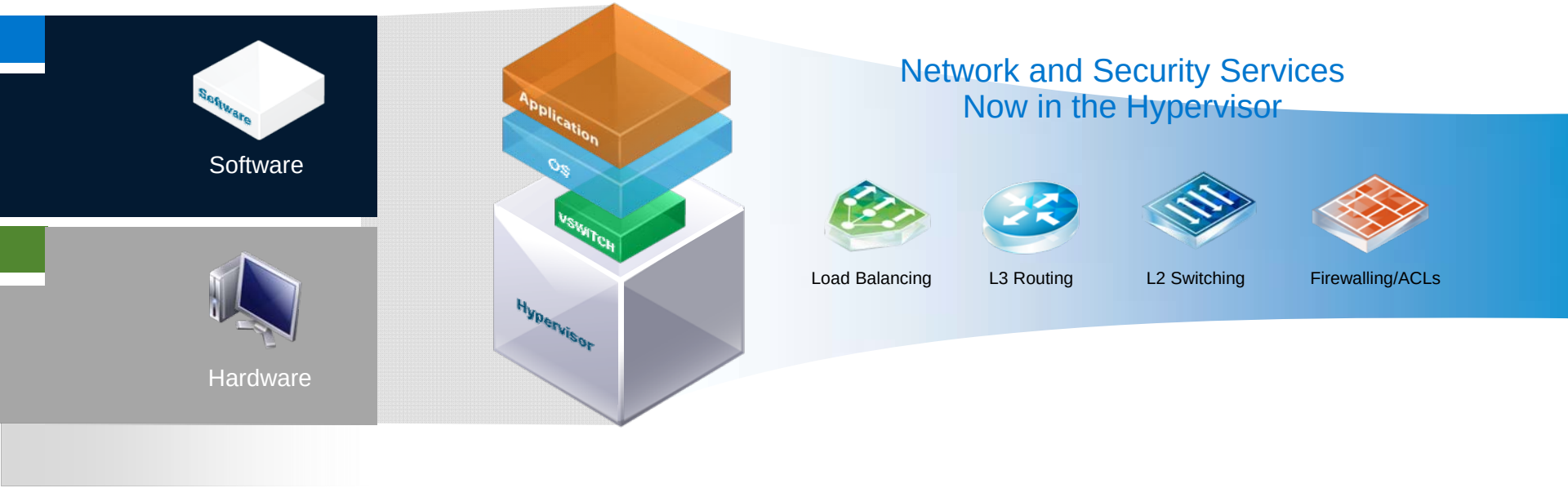
Compute Capacity

Network Capacity

Storage Capacity

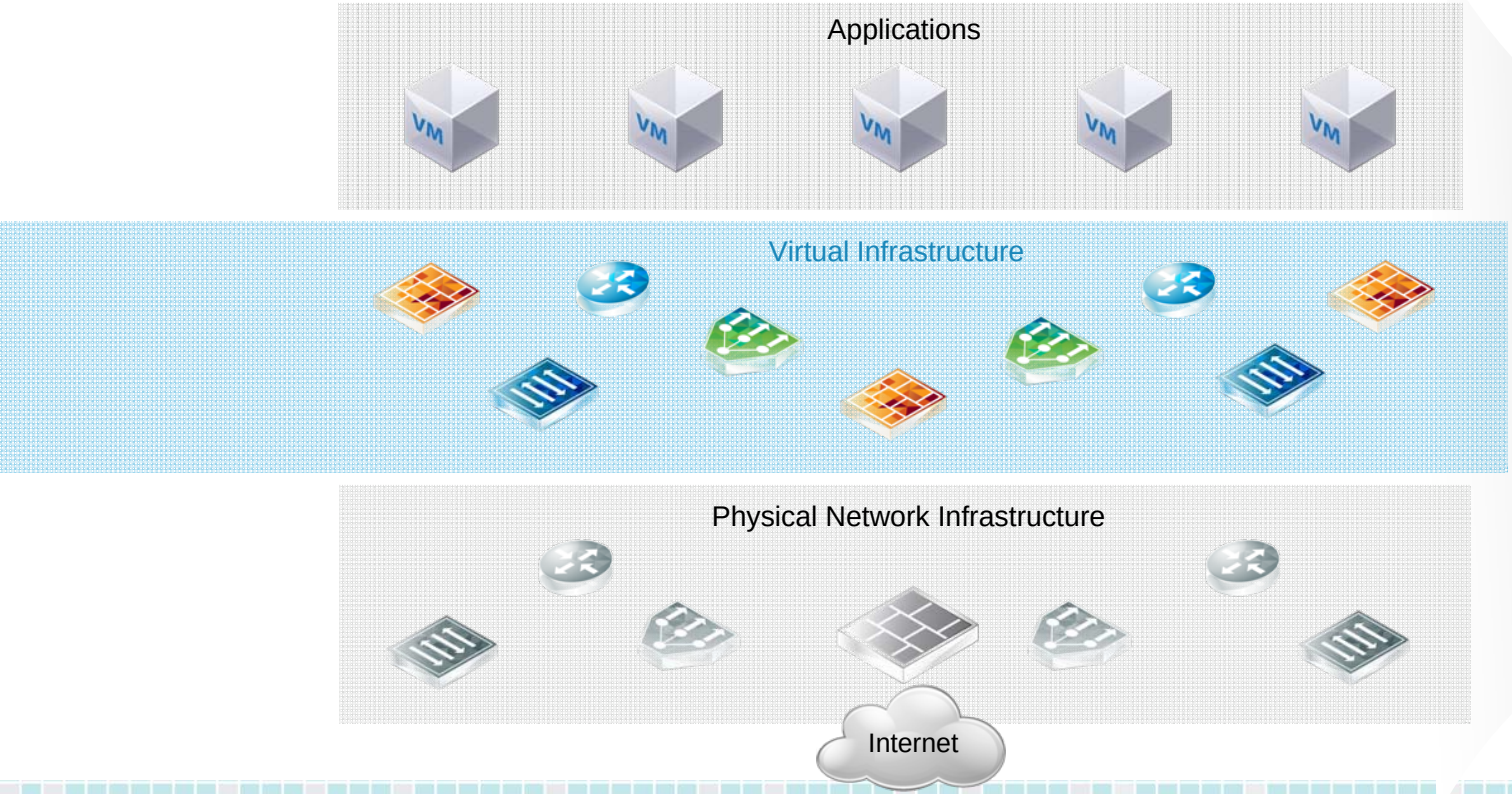
Location Independence

The next-generation networking model

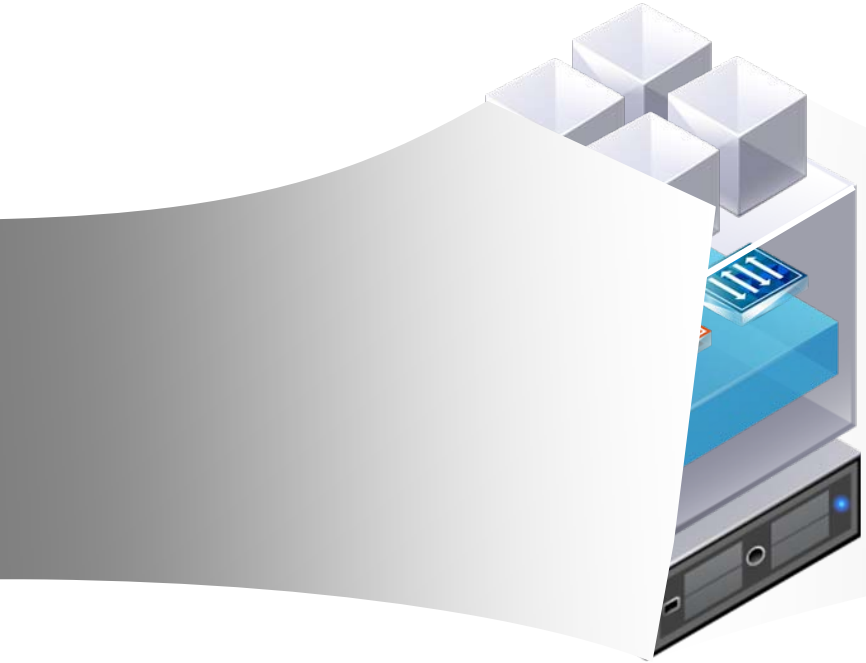


Visibility

Hypervisor is uniquely positioned to see everything

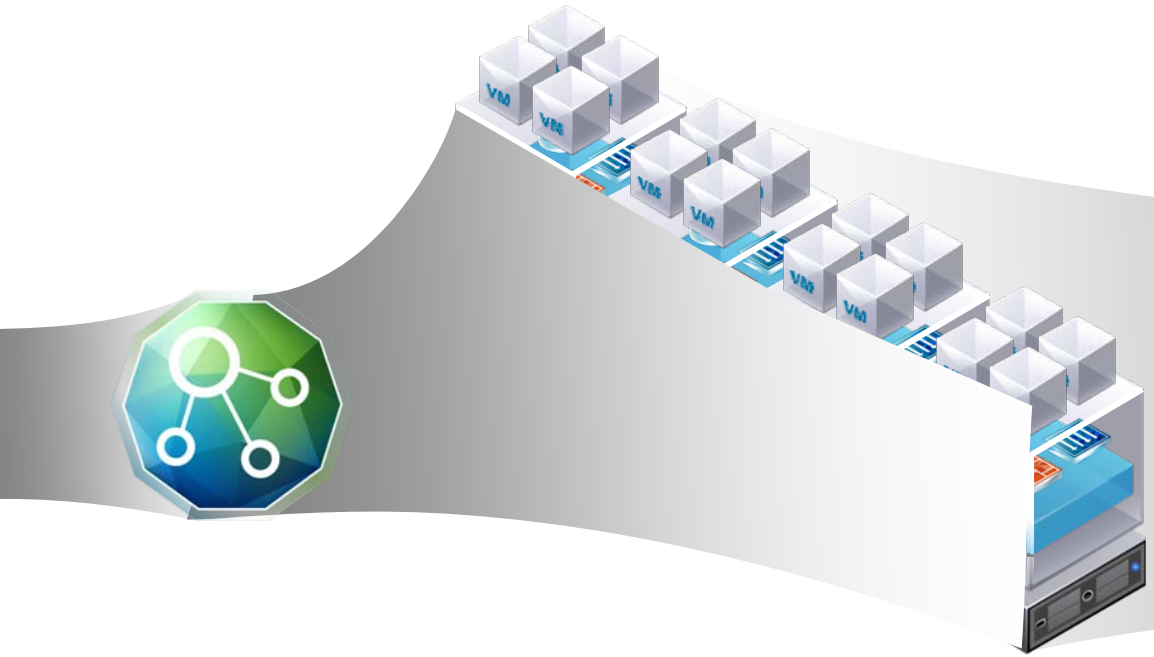


Granular control becomes possible



- High throughput rates on a per-hypervisor basis
- Every hypervisor adds additional east-west firewalling capacity

Delivering better security automation



Platform-based automation

- Automated provisioning and workload adds/moves/changes
- Accurate firewall policies follow workloads as they move
- Centralized management of single logical, distributed firewall

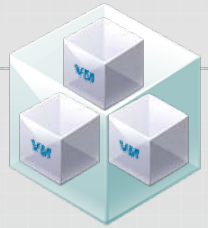
Delivering higher levels of data center security

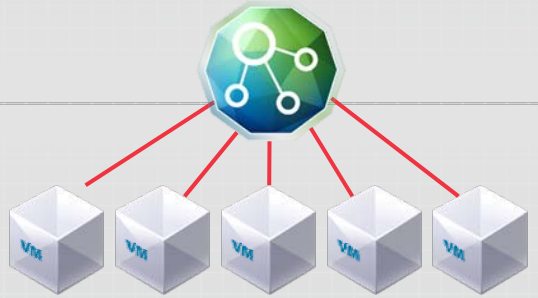
Micro-segmentation

1 Isolation and segmentation

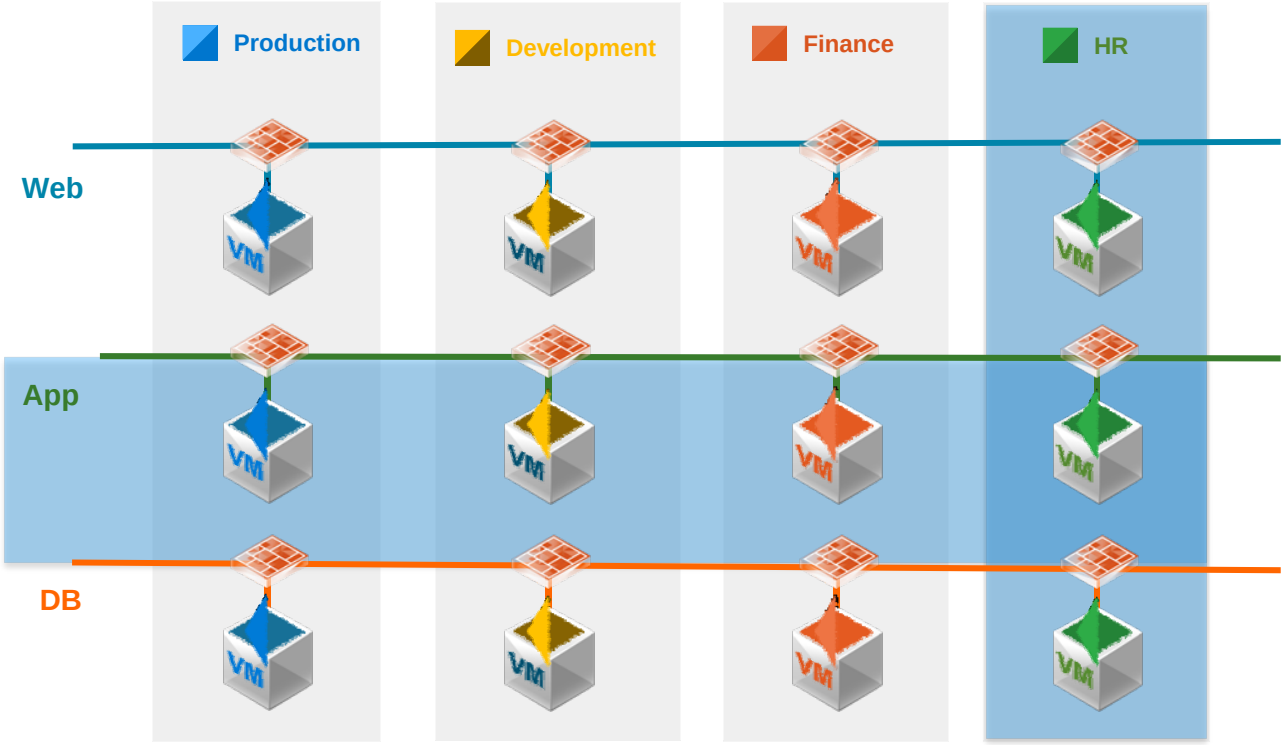
2 Unit-level trust / least privilege

3 Ubiquity and centralized control





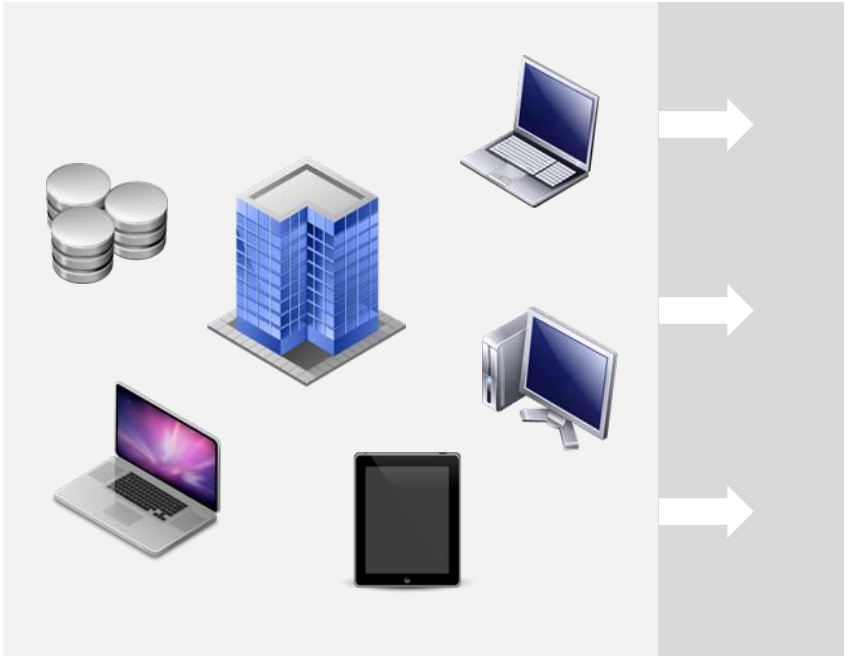
Simplifying network security

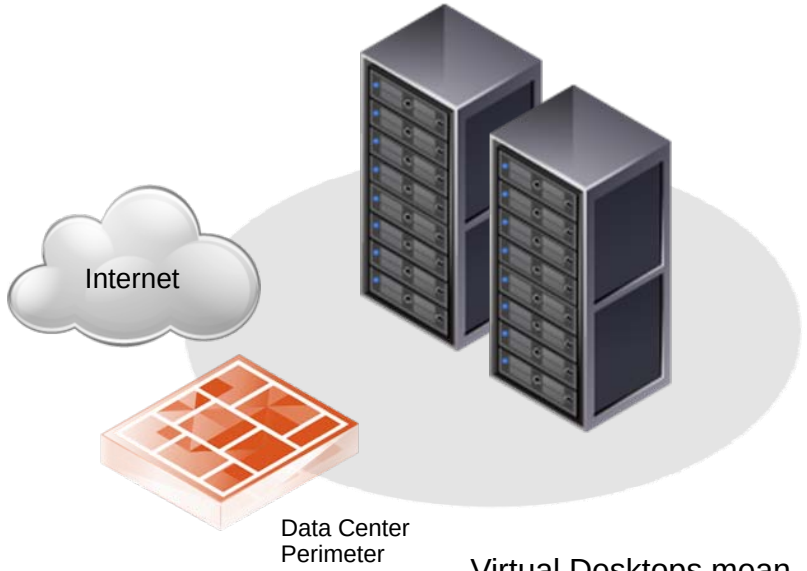


- Security policies no longer tied to network topology
- Logical groups can be defined
- Prevents threats from spreading

What does micro-segmentation look like applied beyond just application servers inside the data center?

Desktop and App Virtualization are the next logical steps

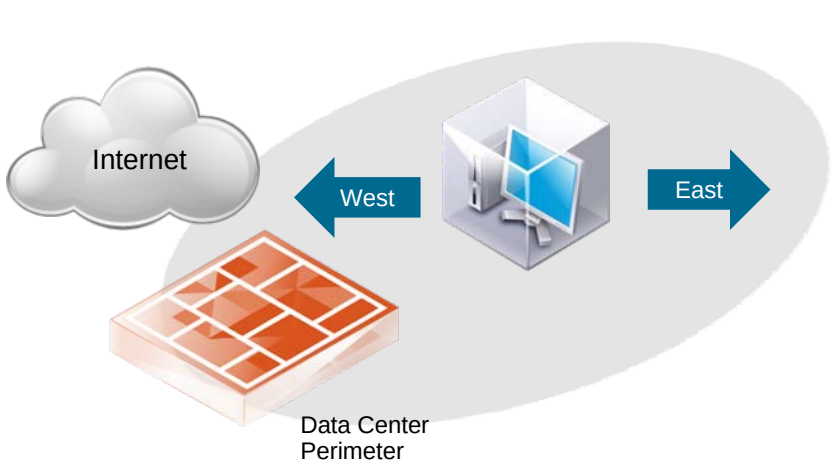




Virtual Desktops mean centralization of activity within the data center.

With VDI your data center has a much larger security surface area

A converged infrastructure means virtual desktops run on the same infrastructure as servers.

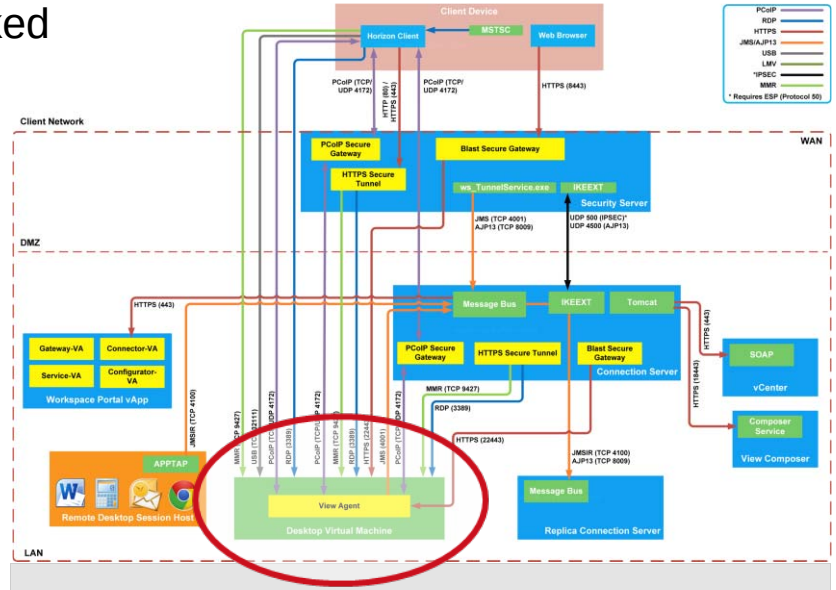


Network considerations for VDI environments

With desktop virtualization, the network matters more than ever. Virtual desktops are a networked entity sitting inside your datacenter.

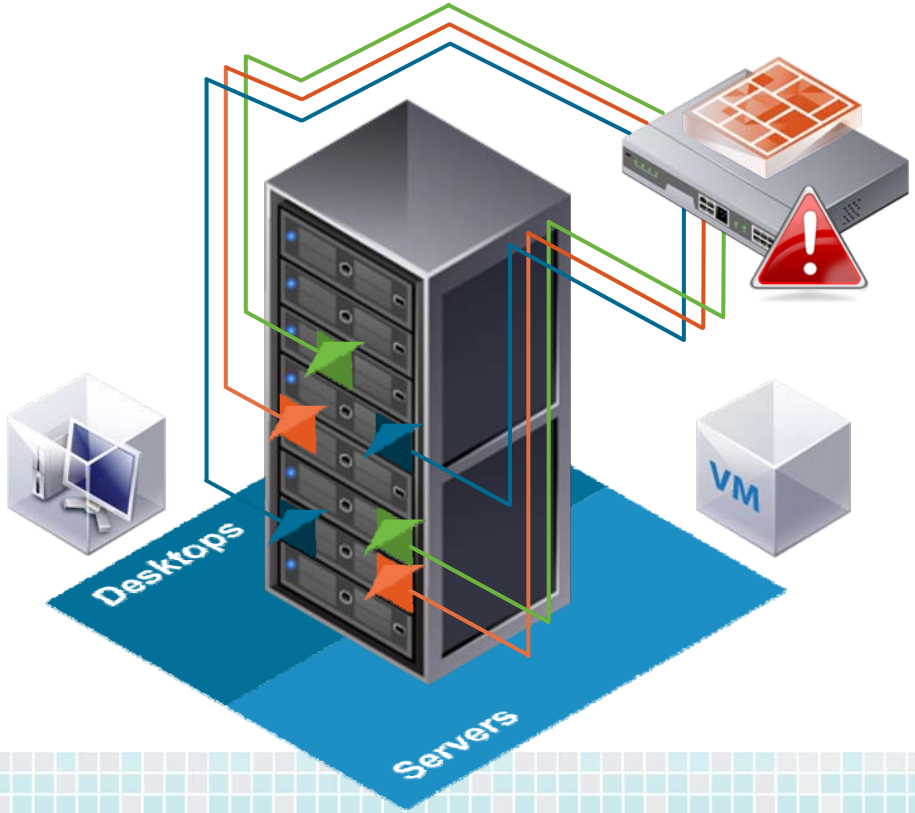
By 2018, 75% of all data center traffic will be “east-west” in nature

- Desktop Virtualization scales up the volume of east-west traffic within the data center
- Multiple discrete flows for each VM: between users, servers, storage, other hosts, and WWW



User desktops now sit amidst a much larger attack surface, inside the data center.

A matrix of policies is needed on centralized, choke-point firewalls for the correct security posture

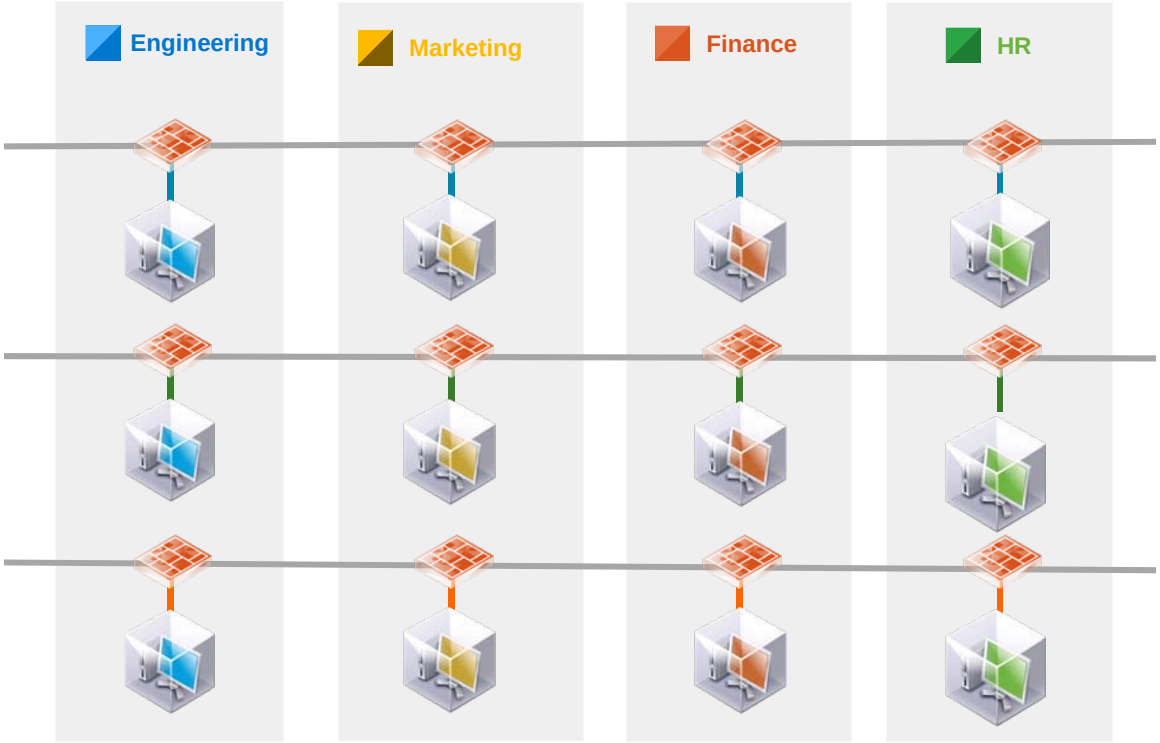


Finance

HR

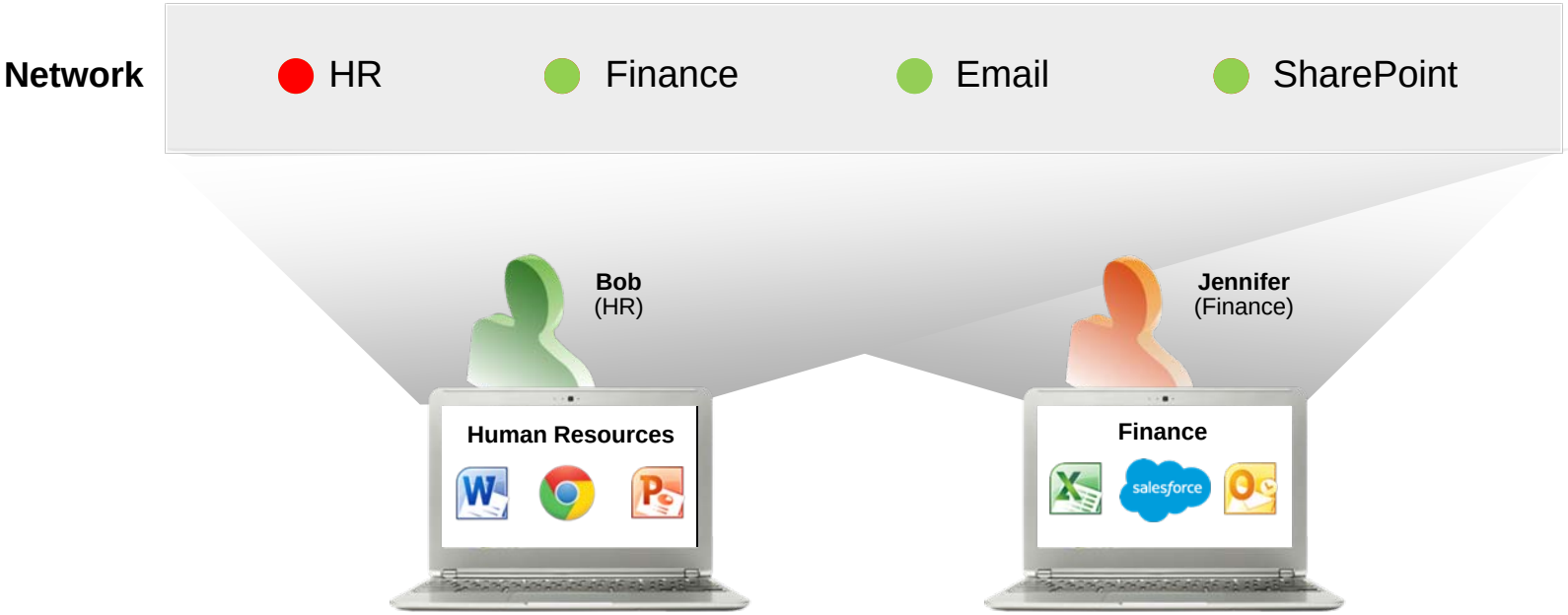
Engineering

NSX simplifies VDI



- Firewall and filter traffic based on logical groupings
- Simplified, programmable, automated application of network/security policy to desktop users/pools
- Service-chaining with AV and NGFW partners to deliver automated, policy-integrated AV / malware protection, NGFW, IPS, etc.

Virtual networking: fast, easy, and extensible

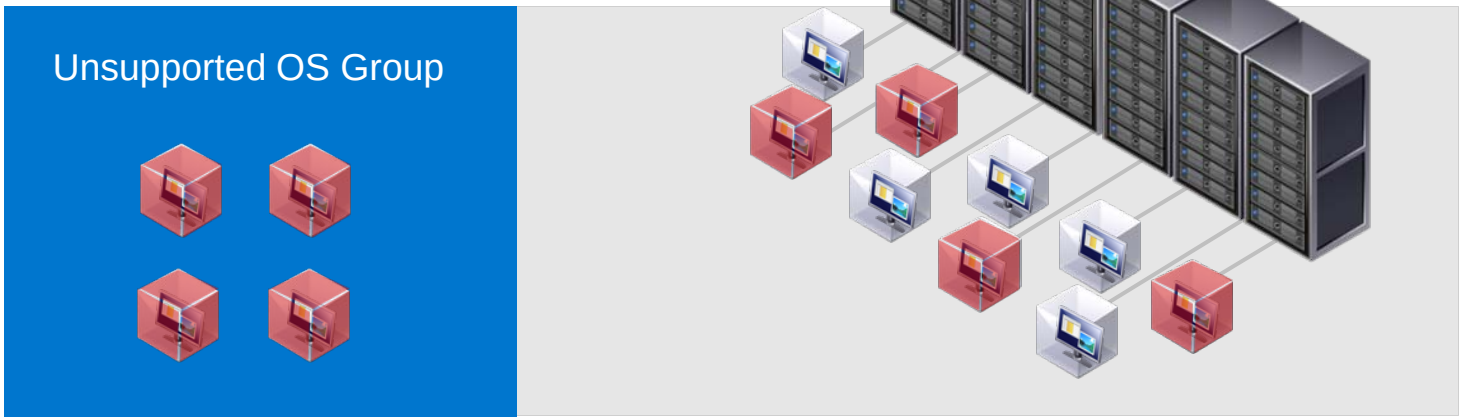


Use case: VDI

Situation

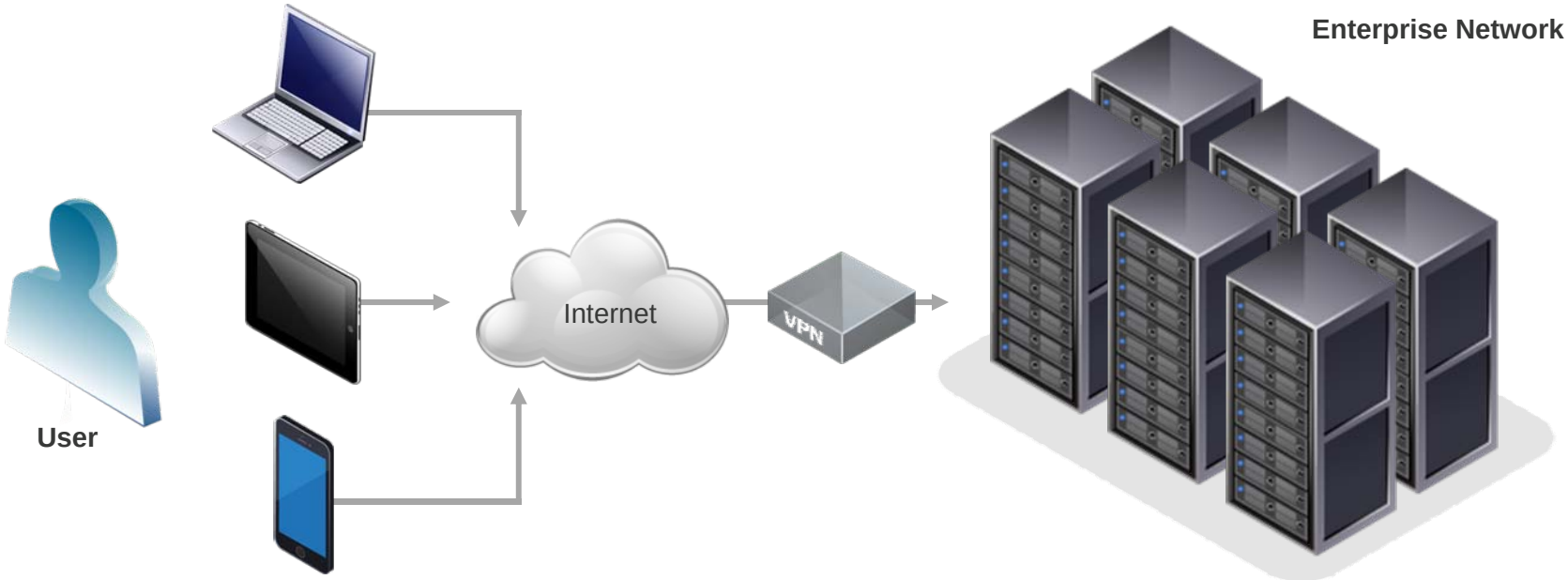
OS no longer supported on several systems

These systems need policy which restricts access to only email servers.

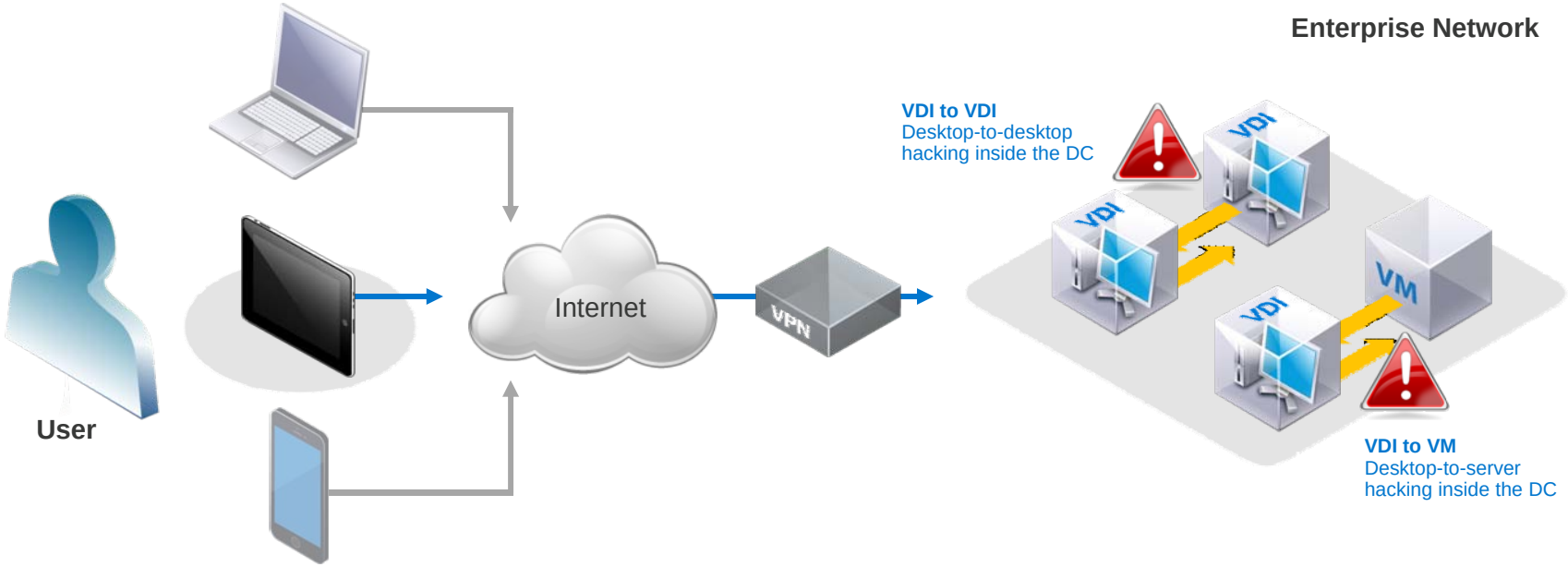


What about micro-segmentation applied even closer to the user?

Our problem: it's not a 1:1 world anymore



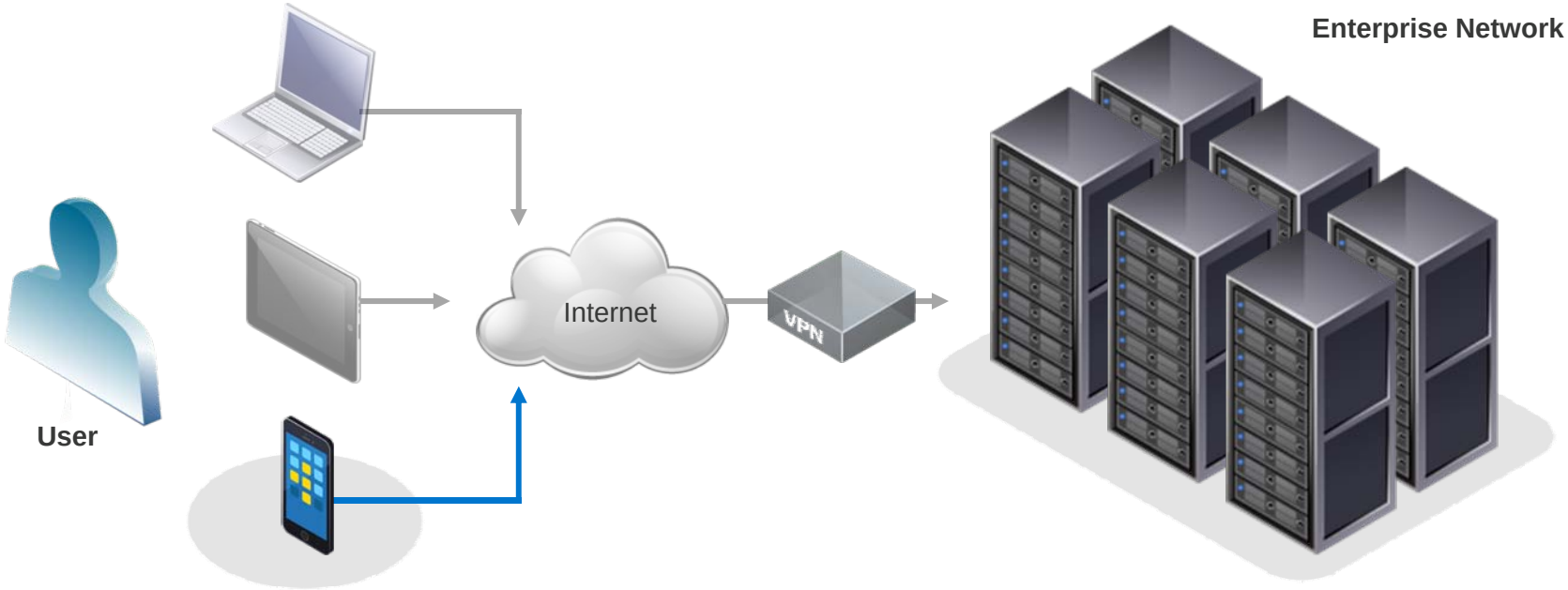
Our problem: it's not a 1:1 world anymore



A converged infrastructure means virtual desktops run on the same infrastructure as servers.

Bringing desktops into the data center opens up new risks for attack.

Our problem: it's not a 1:1 world anymore

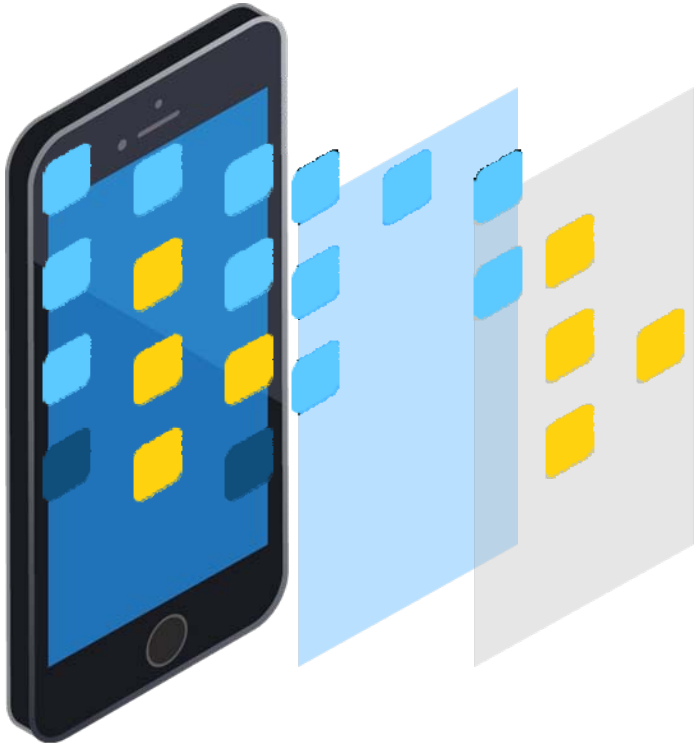


All mobile apps can access enterprise network.

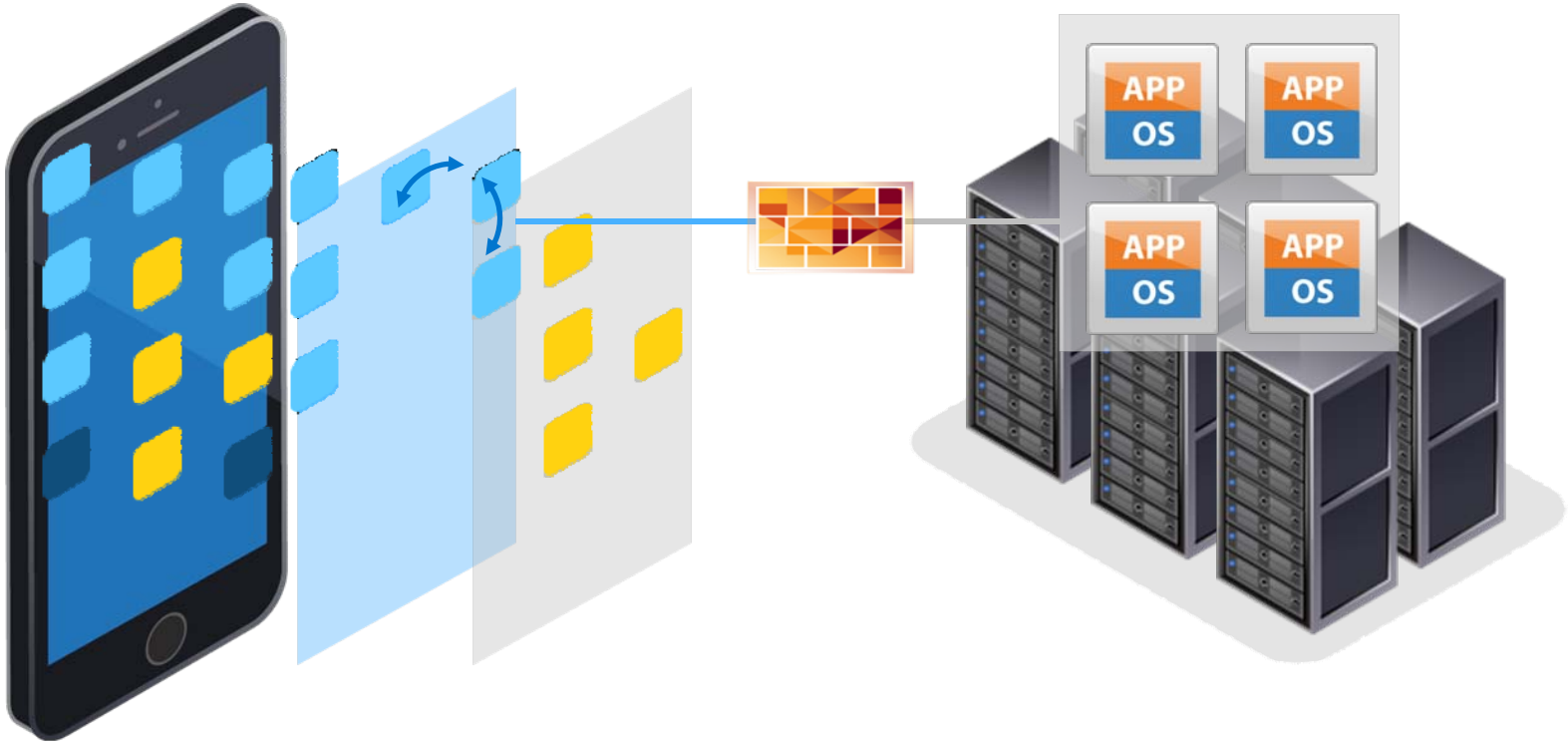
All data center apps can be accessed.

Modern mobility: personal and managed

Modern mobility



Modern mobility

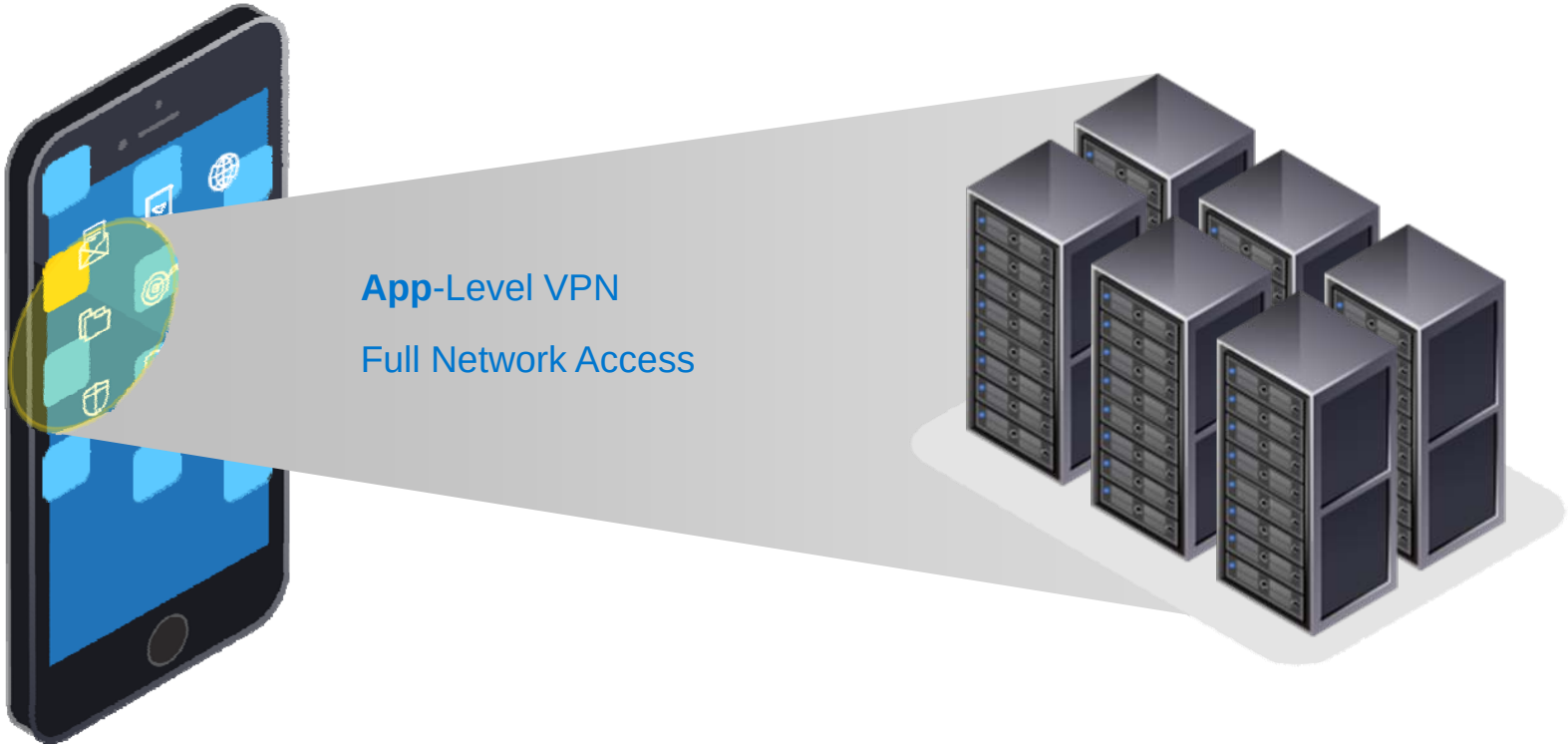


Evolving to intelligent networking

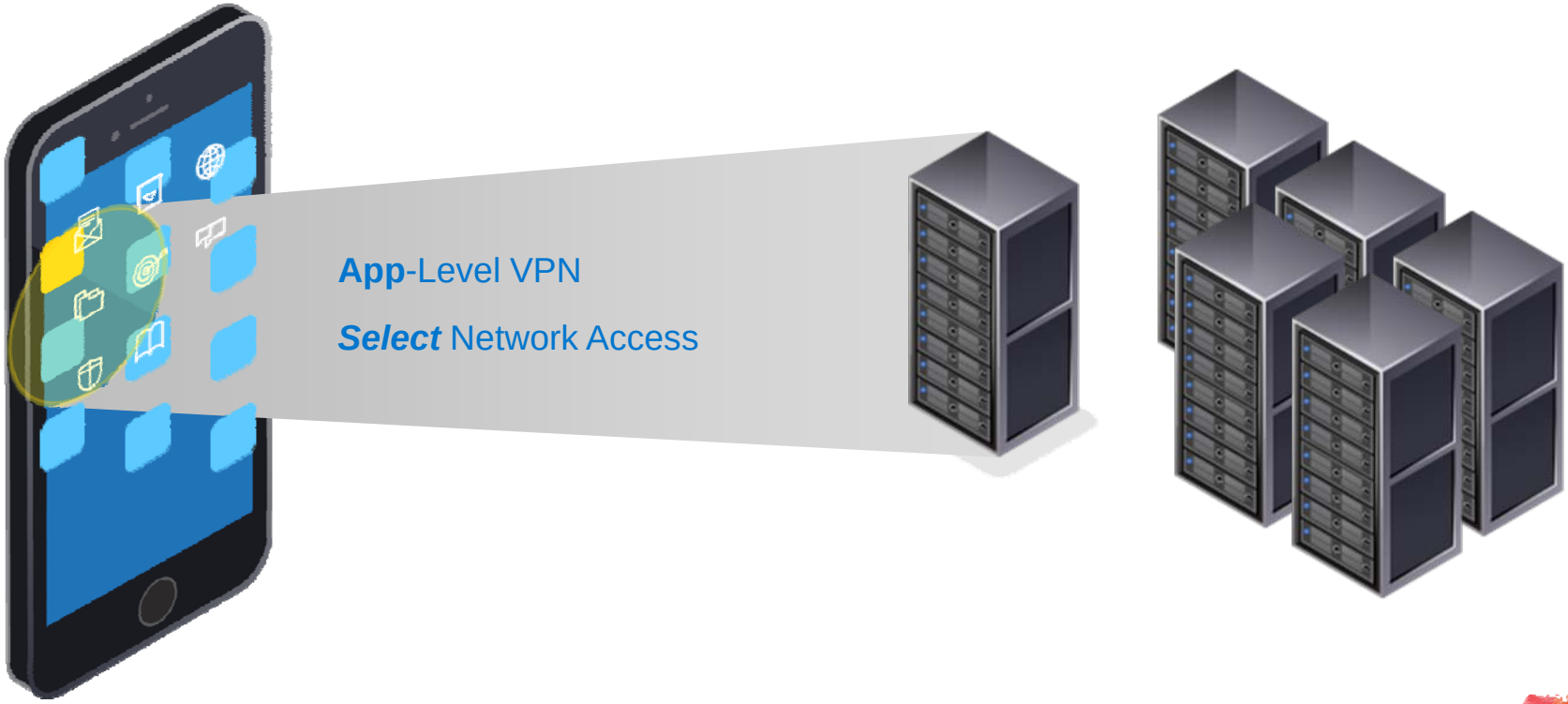
Device-Level VPN

Full Network Access

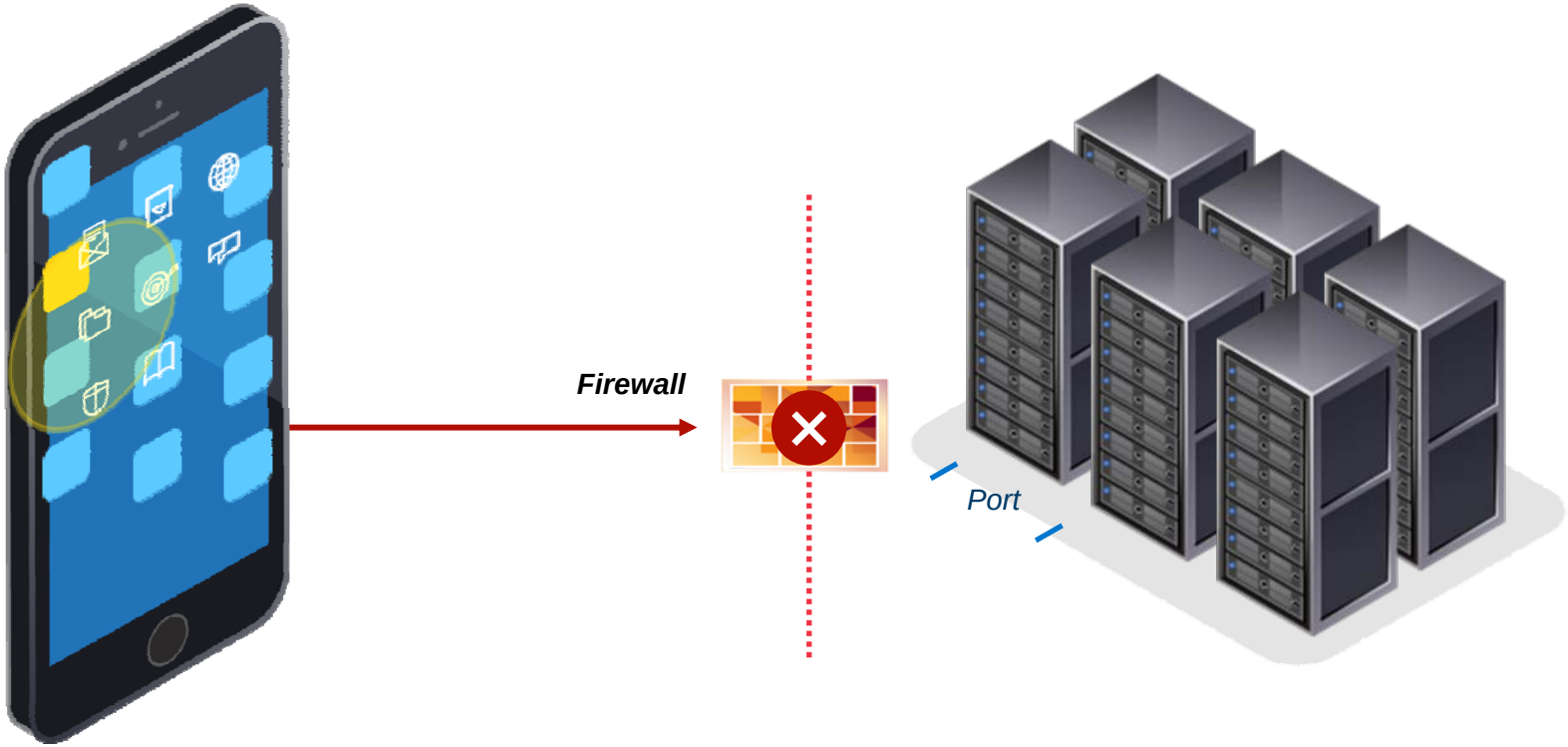
Intelligent networking



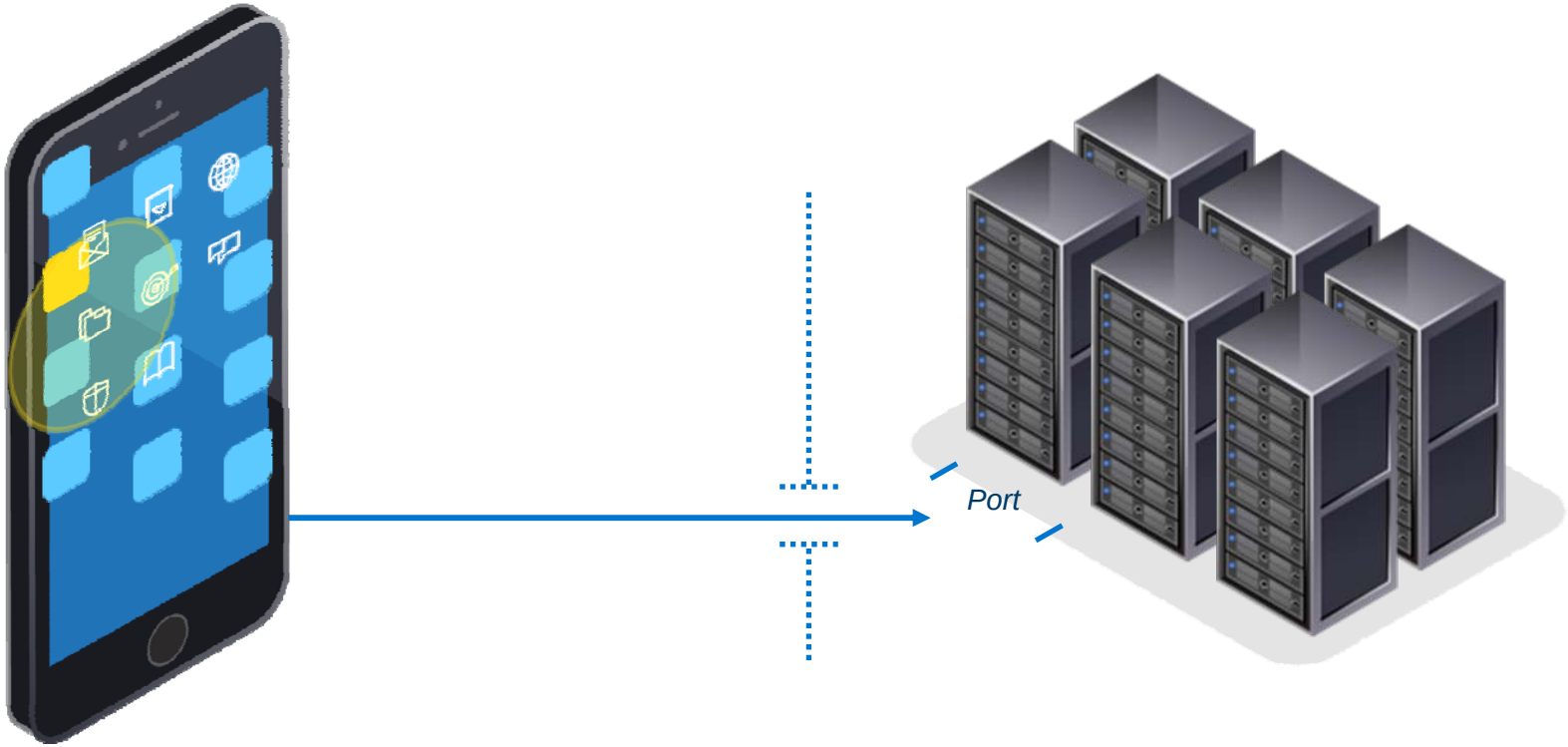
Intelligent networking



Intelligent networking and automation



Intelligent networking and automation



Better context, better tools, better visibility

Users	Who is this person?
Apps	Who is using what apps?
Devices	Has the device been jail broken?
Systems	Who has been accessing what?
Data	What class of data is this?
Network	Are they on cellular or Wi-Fi?

Imagine granular user security

A personalized DMZ,
tailored for each unique situation

Learn more

- **Attend other sessions to learn how VMware is transforming security:**
  Micro-segmentation: How to create a more secure Data Center Network
  Wednesday, 4:30pm, Briefing Center, North Hall

  WestJet's Security Architecture Made Simple – We finally got it right!
  Thursday, 10:20am, Moscone West, Room 3004

  Limiting the Spread of Threats: A Data Center for Every User
  Thursday, 10:20am, Moscone North, Room 130

  Automating Security Workflows: The SDDC Approach
  Thursday, 11:30am, Moscone North, Room 130
- **Visit the VMware booth: South Hall (#1315)**
- **Learn more about micro-segmentation and Horizon:**
  http://www.vmware.com/go/nsx
  http://www.vmware.com/go/horizon

Apply What You Have Learned Today

Next week	In 3 months	In 6 months
▪ Review your organization's workflows for end user computing security	▪ Assess your organization's ability to cope with changes and deal with threats inside the data center	▪ Adopt a plan for providing fine-grained security in the data center and on mobile devices

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Thank you

Geoff Huang

Tony Paikeday