

Security Virtual Infrastructure - Cloud

Ramkumar Mohan
Head – IT & CISO
Orbis Financial Corporation Ltd

Agenda

- Cloud
 - Brief Introduction
 - State of Cloud
 - Cloud Challenges
 - Private Cloud
 - Journey to Cloud
- Virtualization Security
 - Quick Stats
 - Most Common Security Risks
 - Security Needs
 - Guidelines
- Private Cloud Security
 - Secure Virtualization to Secure Private Clouds
 - Evolving Security
 - Attributes of Private Security Infrastructure

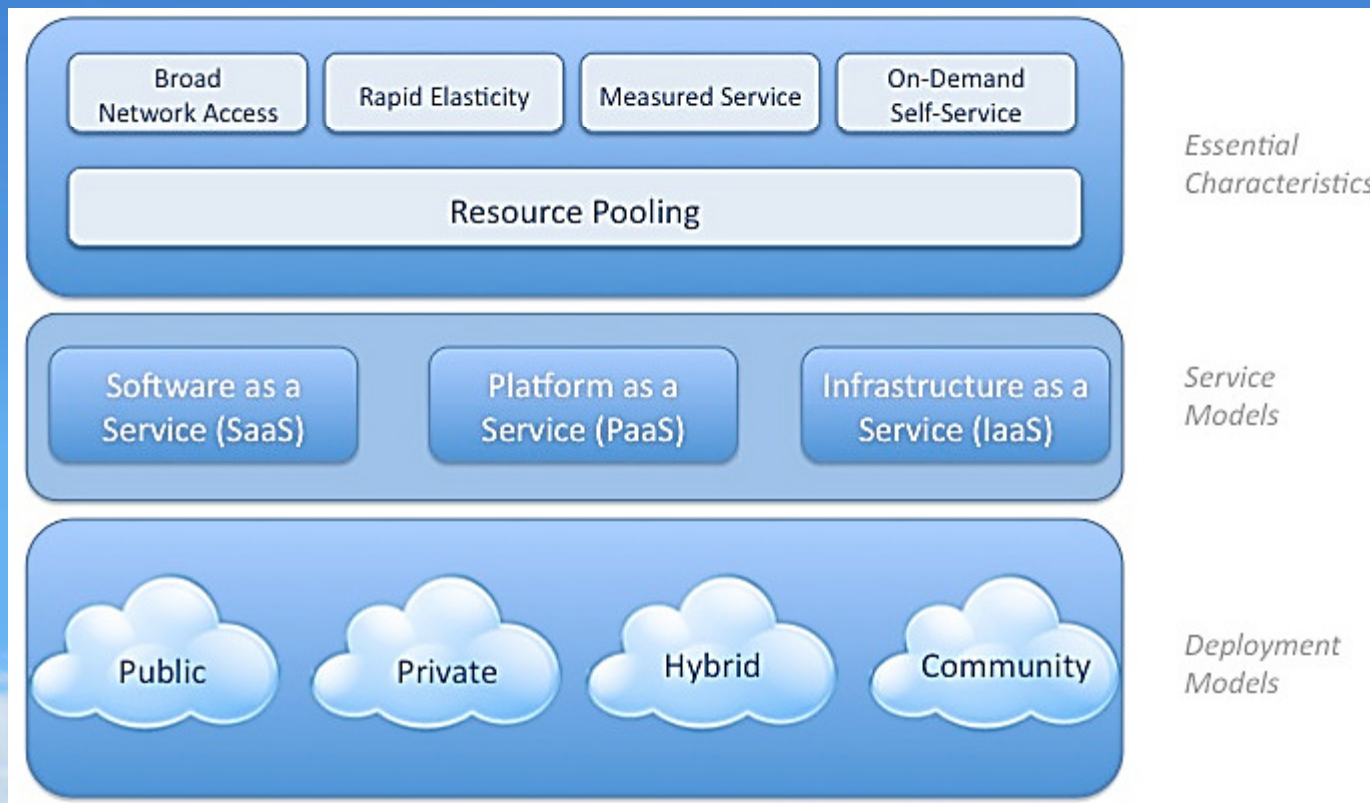
Cautions and Disclaimers

- Virtualization and Cloud Computing is a huge topic. It encompasses diverse models and technologies, and covering all potential security issues in 30 minutes is difficult.
- As Cloud Computing is rapidly evolving, what I share today may quickly become irrelevant or obsolete.
- Views / Opinions contained in this presentation do not necessarily express sufficiency for specific environments and implementations.
- Any mention of a vendor or product is NOT an endorsement or recommendation.




<http://www.youtube.com/watch?v=VjfaCoA2sQk>

NIST Definition Of Cloud Computing

Cloud computing is a model for enabling ubiquitous (omnipresent), convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.



Cloud Computing Deployment Models

	Infrastructure Managed By ¹	Infrastructure Owned By ²	Infrastructure Located ³	Accessible and Consumed By ⁴
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Or Organization Third Party Provider	 Organization Third Party Provider	 On-Premise Off-Premise	 Trusted
Hybrid	<u>Both</u> Organization & Third Party Provider	<u>Both</u> Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

¹ Management includes: governance, operations, security, compliance, etc...

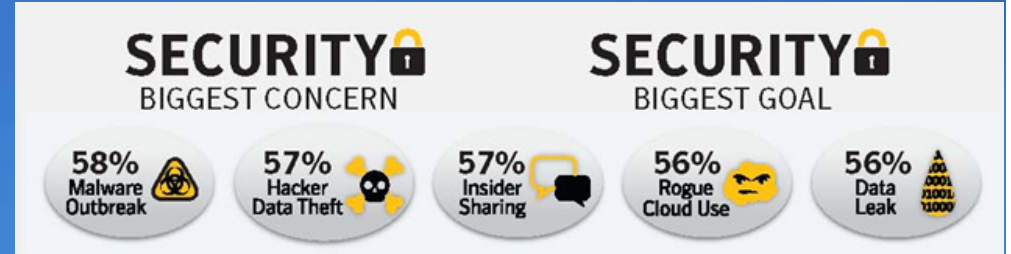
² Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment

³ Infrastructure Location is both physical and relative to an Organization's management umbrella and speaks to ownership versus control

⁴ Trusted consumers of service are those who are considered part of an organization's legal/contractual/policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.

State of Cloud – Symantec Survey Findings

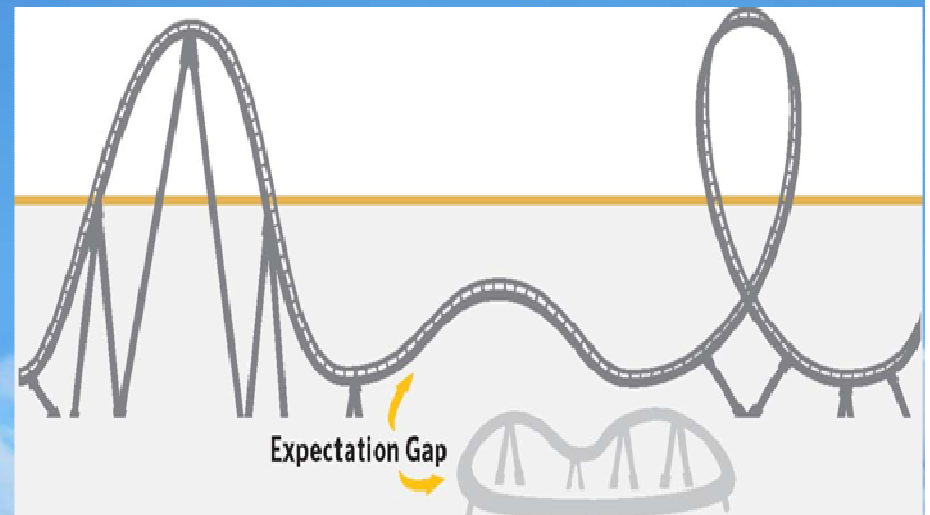
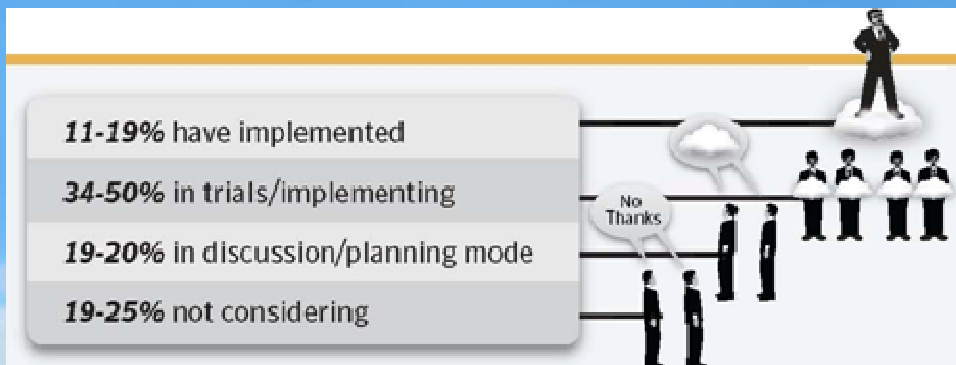
Finding 1:- Cloud security is top goal and top concern



Finding 2:- IT staff not ready for move to cloud

Finding 4:- Reality not meeting expectations

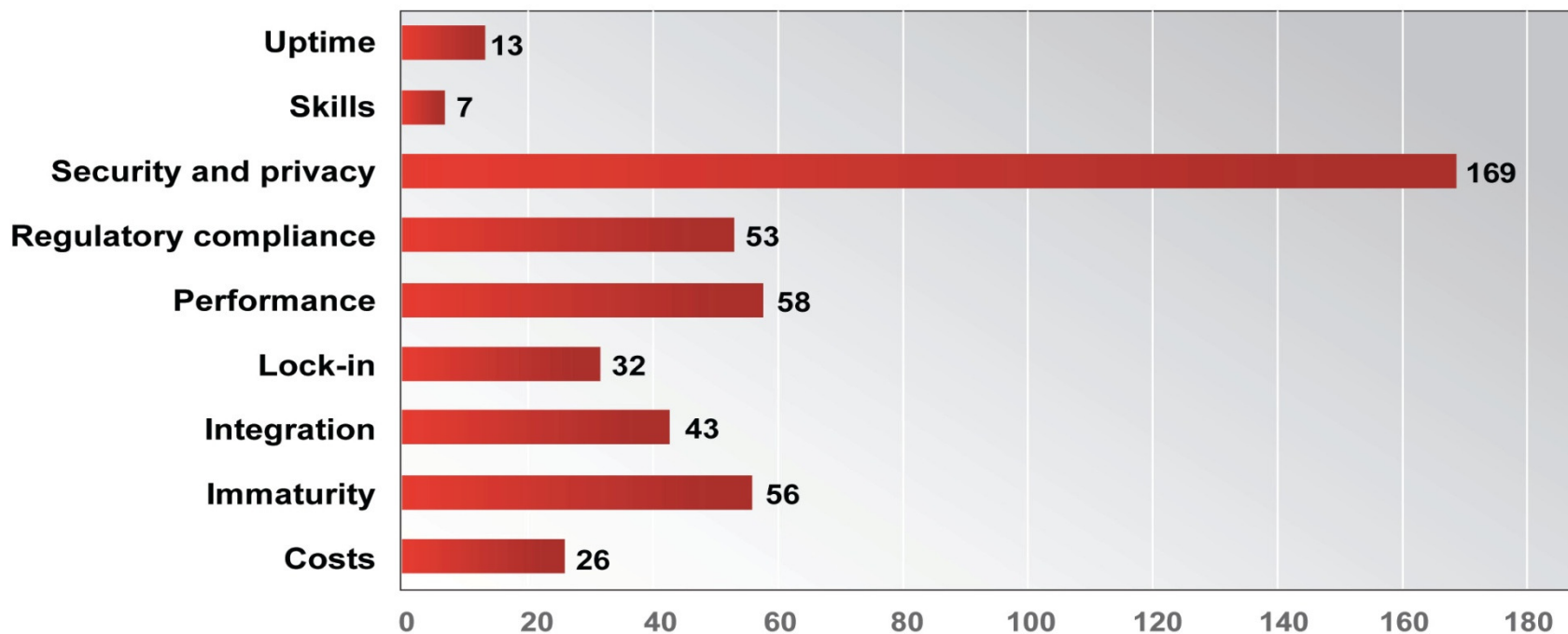
Finding 3:- With cloud, there is more talk than action



Cloud Challenges

Security: the #1 Cloud Challenge

Security and privacy were the foremost concerns by far, with a weighted score higher than the next three (performance, immaturity and regulatory compliance) **combined**.



Gartner (April 2010)

Copyright 2009 Trend Micro Inc. 7



Private Cloud Adoption – Ahead of Public Cloud?

- Through 2014, IT organizations will spend more money on private-cloud-computing investments than on offerings from public cloud providers.
- By 2015, the majority of private-cloud-computing services will evolve to leverage public cloud services in a hybrid model.
- Through 2014, fewer than 20% of virtualized deployments will be complete private cloud deployments.
- By 2015, the majority of virtualized deployments will evolve to support some private-cloud computing capabilities, but fewer than 20% will be complete private cloud deployments.

Private Cloud vs. Traditional Computing

The traditional data center computing focus on infrastructure and operations and “keeping the lights on” and private cloud is all about “service delivery”.

The core architecture of any private cloud environment is focused squarely on this central tenet of service delivery.

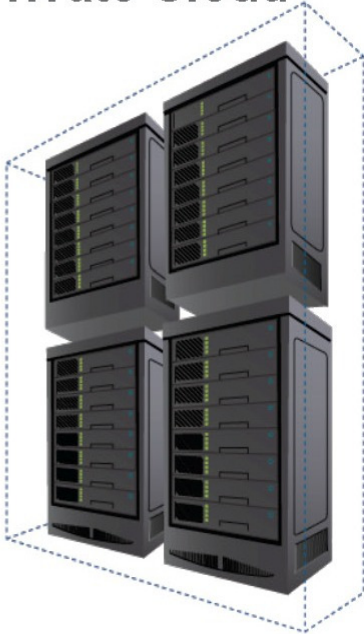
Journey to Cloud



Hybrid / Public



Private Cloud



Virtual



Physical



Traditional datacenter

Servers virtualized with minimal changes to datacenter processes

Servers virtualized in scalable, shared, automated & elastic environment

Select enterprise applications in public cloud

Virtualization Is a Modernization Catalyst and Unlocks Cloud Computing

Attributes of Cloud Computing

Service-Based

Scalable and Elastic

Shared

Metered By Use

Internet Technologies

- Abstracts implementation from users
- Forces service-level discussion
- Technology hoster becoming service provider
- Enables faster delivery and resource changes
- Enables hardware sharing
- Enables economies of scale
- Software pricing and licensing models broken — some kind of usage-based model needed
- Usage tracking and chargeback to manage use



Virtualization Security – Survey Findings

The Dynamic Datacenter

88% of North American enterprises [no] virtualization security strategy

Forrester Research / Info Week

2012, 60% of virtualized servers.. less secure than... physical servers....

"Addressing the Most Common Security Risks in Data Center Virtualization Projects" Gartner, 25 January 2010



Technologies and practices for securing physical servers won't provide sufficient protections for VMs.

Neil MacDonald, Gartner, June 2009

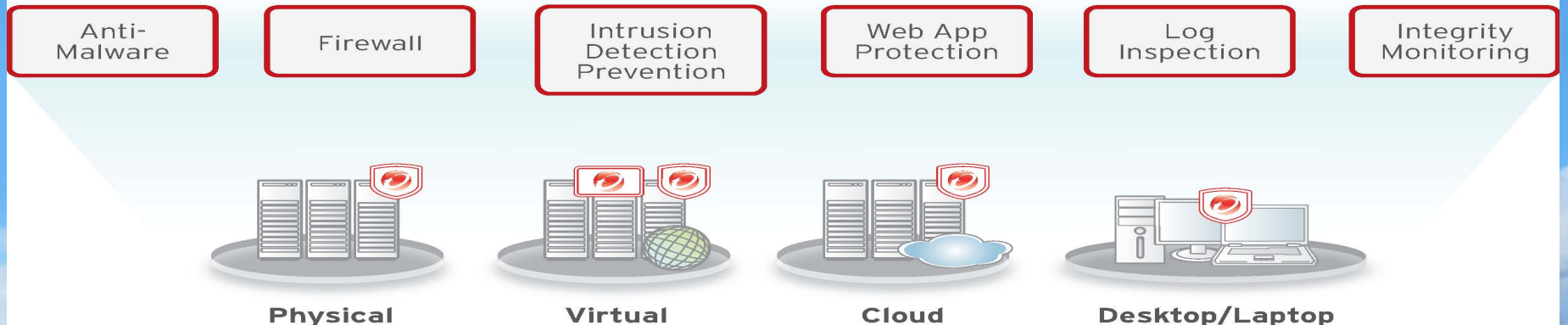
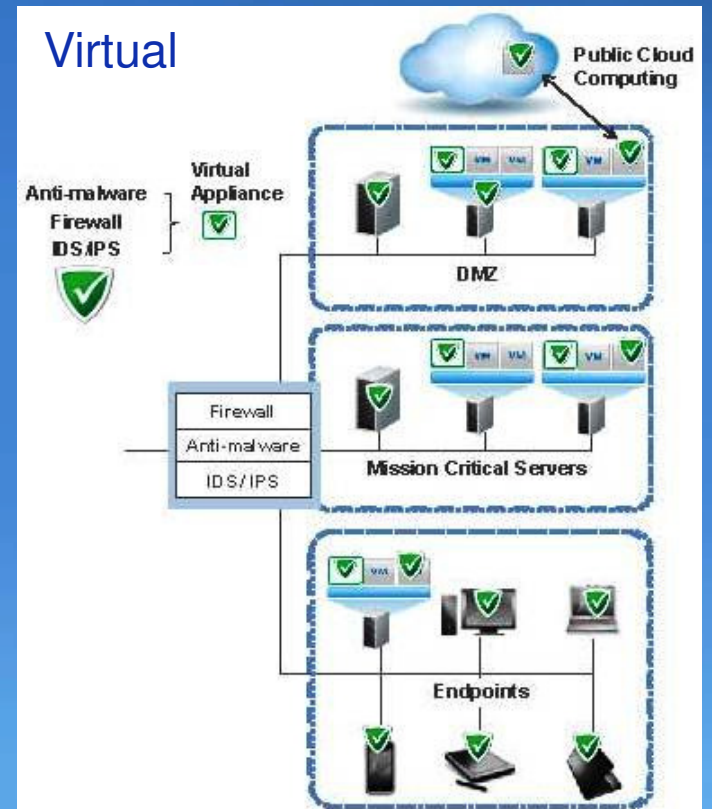
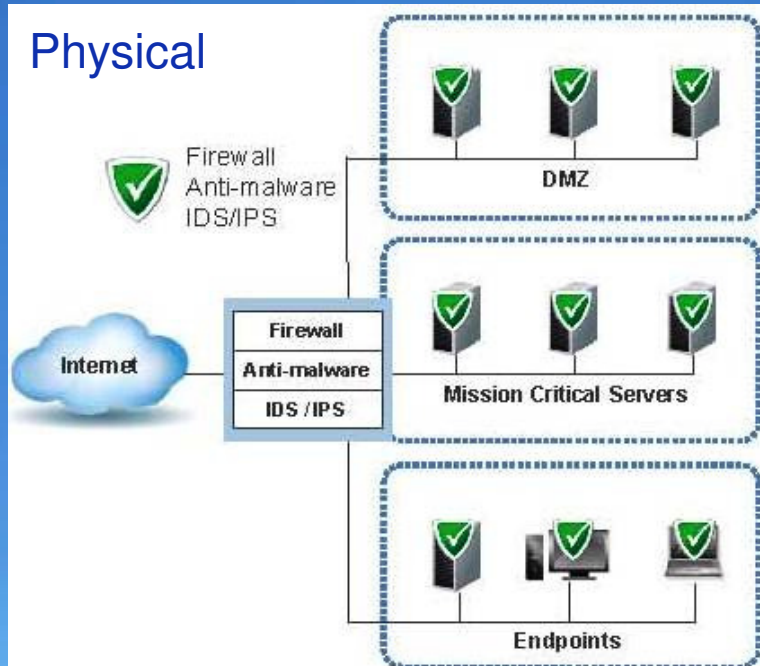
Number one concern (87.5%) about cloud services is security.

Frank Gens, IDC, Senior VP & Chief Analyst

Copyright 2009 Trend Micro Inc.



Virtualization & Private Cloud – Same Security Needs, New Capabilities Required



Virtualization - Security Impediments

Security Challenge	Detail
Host-based controls under-deployed	File Integrity Monitoring, host IDS/IPS and anti-malware are often under-deployed, because of cost, complexity or performance
Inter-VM attacks	Traditional network security devices cannot detect or contain malicious inter-VM traffic
Instant-on gaps	It's all but impossible to consistently provision security to "instant-on" VMs, and keep it up-to-date. Dormant VMs can eventually deviate so far from the a massive security holebaseline that merely powering them on introduces
Mixed trust level VMs	Workloads of different trust levels are likely being consolidated onto a single physical server without sufficient separation
Resource contention	Resource-intensive operations (AV storms & pattern-file updates) can quickly result in an extreme load on the system
Complexity of management	Virtualization has led to the proliferation of more virtual machines (VM sprawl) than their physical predecessors, leading to increased complexity in reconfiguring, patching and rolling out patterns to each VMprovisioning security agents to each VM, and constantly
Compliance/Lack of audit trail	Higher levels of consolidation put greater stress on the ability to ensure compliance, particularly amongst mission critical/Tier 1 applications. As well, virtualization makes it more difficult to maintain audit trails, and understand what, or by whom, changes were made
Data confidentiality & integrity	Unencrypted information in cloud environments is subjected to various risks including theft, unauthorized exposure and malicious manipulation
Data access & governance	RESTful-authentication* in the cloud can be susceptible to brute force and hijacking, attacks allowing unauthorized data access. Breakdown in the separation of duties might allow unauthorized vendor access to data (* REpresentational State Transfer)
Diminished perimeter	Security mechanisms are under the cloud service provider's control and perimeter security mechanisms are significantly diminished
Multi-tenancy	In cloud environments, your VMs exist with other unfamiliar, potentially hostile VMs with unknown security
Data destruction	Some cloud providers do not overwrite storage before recycling it to another tenant; in some cases where the storage is overwritten, data may be vulnerable after a system crash or unexpected termination

Virtualization - Most Common Security Risks

- **Information Security Isn't Initially Involved in the Virtualization Projects**
- **A Compromise of the Virtualization Layer Could Result in the Compromise of All Hosted Workloads**
- **The Lack of Visibility and Controls on Internal Virtual Networks Created for VM-to-VM Communications Blinds Existing Security Policy Enforcement Mechanisms**
- **Workloads of Different Trust Levels Are Consolidated Onto a Single Physical Server Without Sufficient Separation**
- **Adequate Controls on Administrative Access to the Hypervisor/VMM Layer and to Administrative Tools Are Lacking**
- **There Is a Potential Loss of SOD for Network and Security Controls when these are Virtualized**

Securing the Virtualization Platform

a) Platform and installation requirements

- Limit physical access to the host
- Verify integrity of files before installation
- Load and enable only required OS components & Services
- BIOS, boot loader passwords

b) Privileged partition operating system hardening

- Limit VM resource use
- Ensure time synchronization
- Minimize number of accounts with strong authentication
- Uninstall / Disable all unnecessary programs and services
- Configuration Management
- Patch Management
- Hardening guide
- Administrator or root login

Securing the Virtualization Platform

c) Partitioning and resource allocation

- Space restrictions
- Disconnect unused physical devices
- Virtual devices
- Use of virtual trunk ports
- Use Layer2 security configurations

d) Administration and Management

- Strong authentication should be used for host system access
- Do not enable file sharing between host and guest OSs
- Warning banners
- Separation of duties
- Management of hypervisors
- Regular backups
- Follow DR procedures for virtual environment
- Prevent VM sprawl
- Control VM migration
- Same risk level per host
- Separate production from test VMs

Securing the Virtualization Platform

e) Logging and auditing

- Use centralized logging
- Correlate Logs
- Regularly audit virtualized environments
- Root and administrator privileges
- Invalid logical access attempts
- Access to all audit trails
- Initialization of audit logs
- Creation and deployment of VMs, Migration of VMs
- Creation and deletion of system-level objects



f) Platform network security

- Restricted network access
- Use a firewall and restricted access through firewall
- Consider using introspection capabilities
- Static IP addresses
- Separate management network
- Use encrypted communications
- Separate VLANs for host communications with guest OSs

Virtualization Security – Biggest Risk is Disgruntled Insider

In July 2010, Jason Cornish, an IT staff member at Shionogi (a North American subsidiary of a Japanese pharmaceutical firm), who had a difference with his manager and resigned, deleted 88 critical virtual servers including email, blackberry, order tracking and financial management servers.

Virtual & Private Cloud environments are vulnerable to malicious insiders.

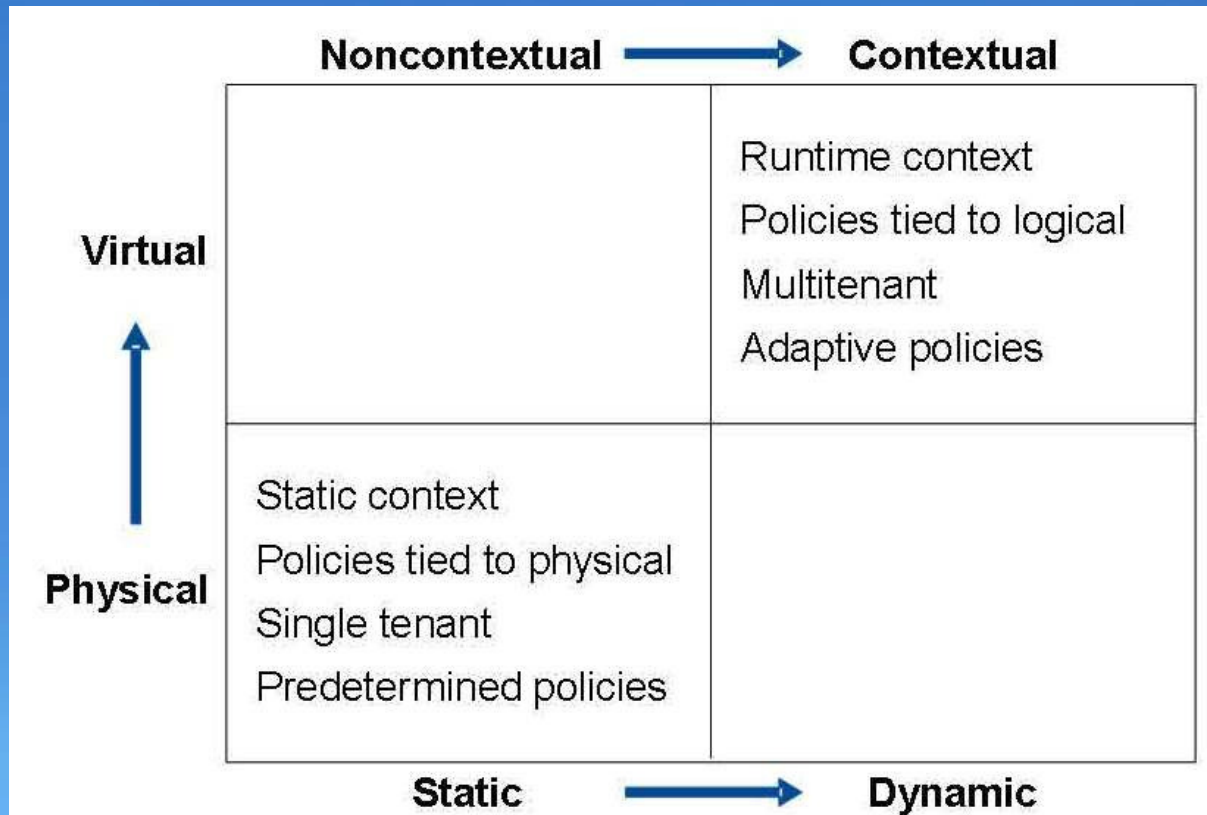
From Secure Virtualization to Secure Private Clouds

- Policies tied to physical attributes, security policy enforcement points embedded within physical appliances will inhibit private cloud adoption.
- Virtualization of security controls is an important step in enabling secure private clouds
- Context enablement, including application, identity and content awareness, will be critical to supporting secure private cloud computing.
- Securing a private cloud can't be just about technology, or it will fail. Changes to processes and a shift in mind-set will also be required.
- The need for security must not be overlooked or "bolted on" later during the transition to private cloud computing.

Private Cloud – Evolving Security

Whether securing physical, virtual or private cloud, the fundamental tenets of information security don't change – ensuring confidentiality, integrity, authenticity, access, and audit of information and workloads.

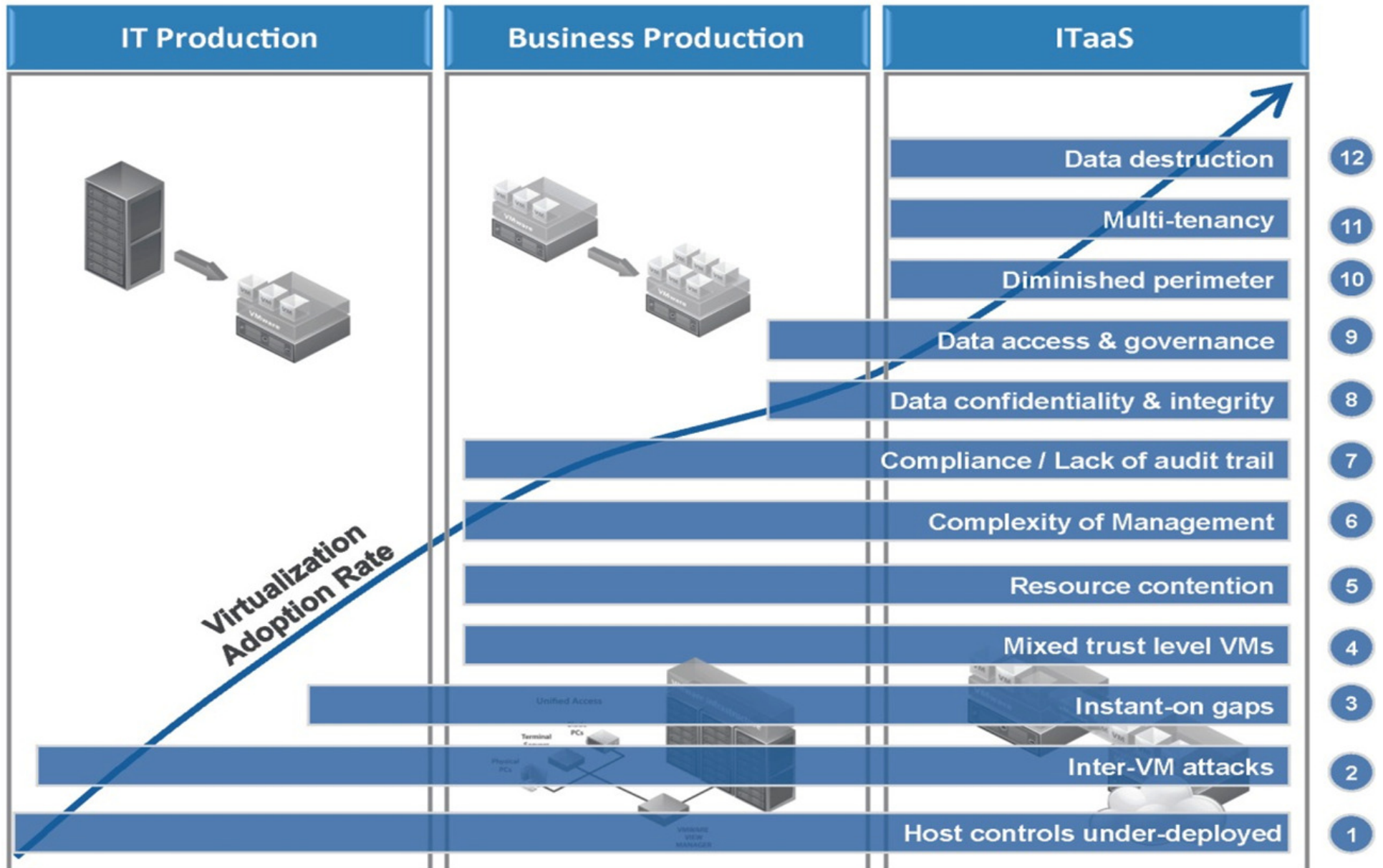
To support secure private cloud computing, security must be an integral, but separately configurable, part of the private cloud fabric, designed as a set of on-demand, elastic and programmable services, configured by policies tied to logical attributes to create adaptive trust zones capable of separating multiple tenants



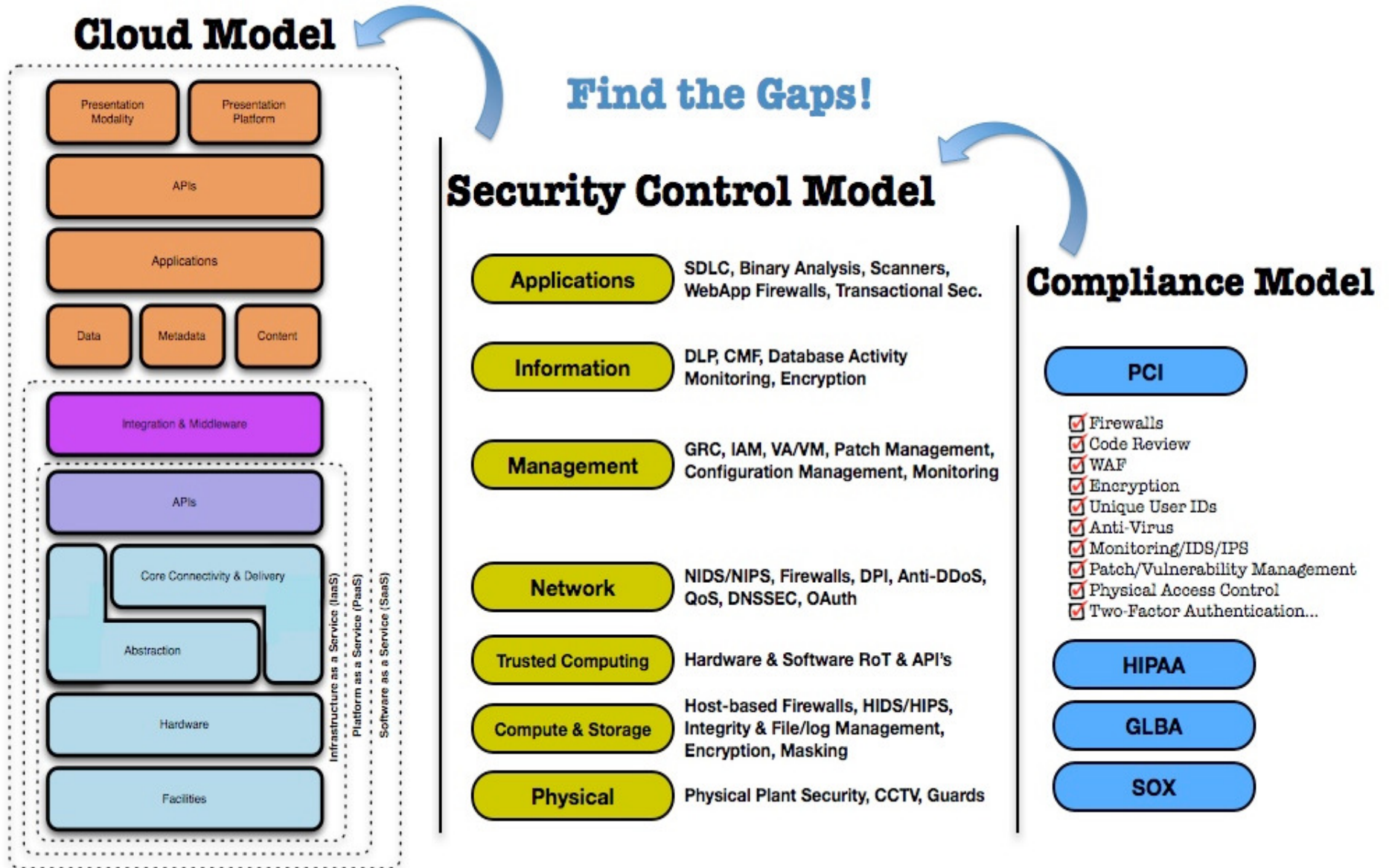
Six Attributes of Private Cloud Security Infrastructure

- A Set of On-Demand and Elastic Services
- Programmable Infrastructure
- Policies That Are Based on Logical, Not Physical Attributes and Are Capable of Incorporating Runtime Context Into Real-Time Security Decisions
- Adaptive Trust Zones That Are Capable of High-Assurance Separation of Differing Trust Levels
- Separately Configurable Security Policy Management and Control
- "Federatable" Security Policy and Identity

Assessing Risk in the Cloud Journey

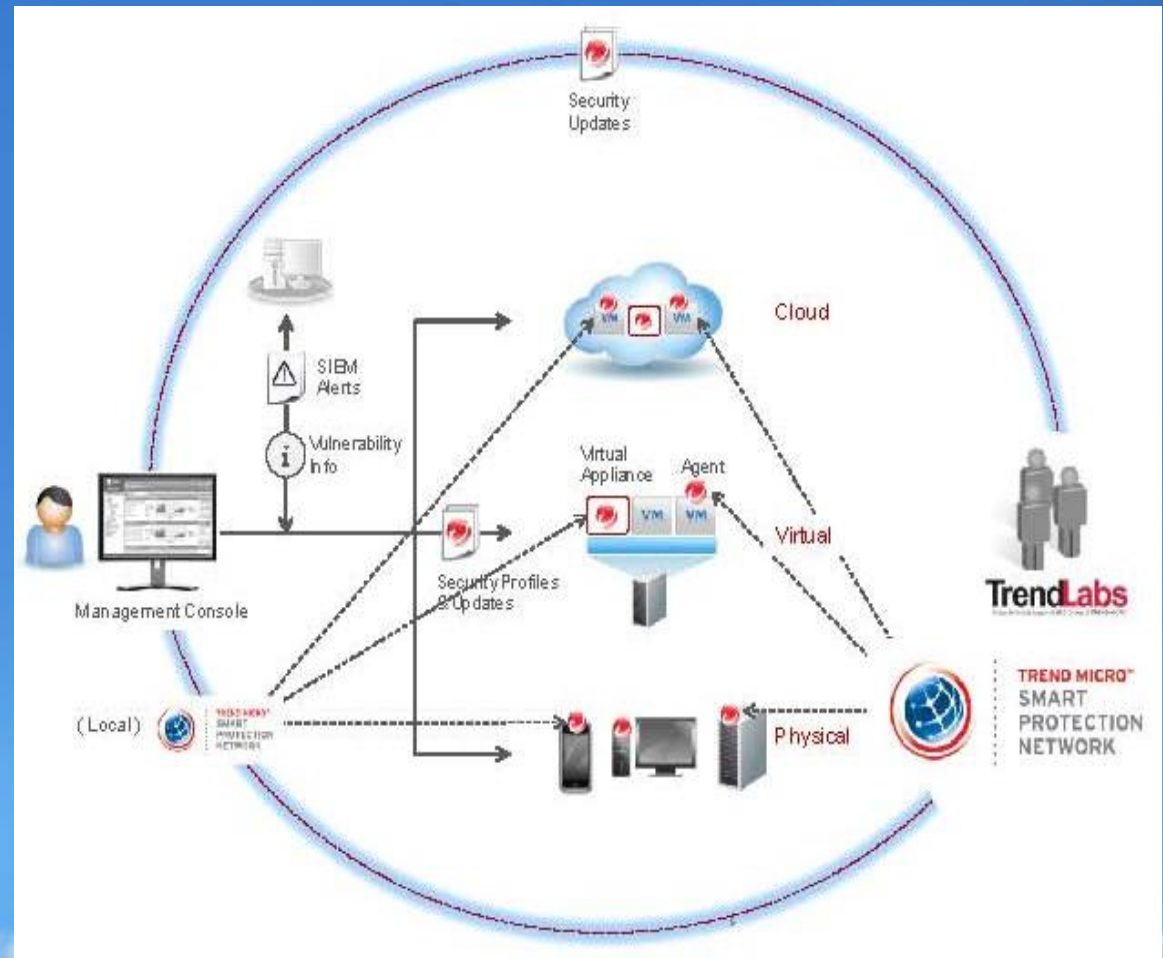


Mapping Cloud to Security Control & Compliance



CHARACTERISTICS OF NEXT GENERATION SECURITY STRATEGY

- Cloud Architecture
- Mobility
- Thin endpoint
- Speed
- Simplicity
- Breadth of protection
- Effective, accessible, supported, and compliant protection



Conclusion

- In the near future, it is anticipated that all aspects of information technology will be movable, dynamic, and interactive – the access, the data, the workload, and all computing.
- End users' mobile devices will access and store hundreds of gigabytes of data.
- Virtual servers will mobilize computing power between network segments, data centers, and even outside of the corporate environment and into the public cloud, where computing power is offered as a utility.
- As a result of these profound changes, all aspects of information security will be challenged and reconsidered.
- Traditional network security, which addressed sets of computing power such as machines and data storage as a guarded walled garden, will no longer apply.
- A new generation of security practices, which emphasize the dynamic aspect of computing power and data, will challenge the status quo.
- However, these revolutionary changes will not take place overnight. The major challenge for enterprises will be how to proceed from where they are today, through a transitional or hybrid period, to where they will be in the future. The solution to this challenge will not be a one-size-fits-all approach; each organization will move forward at its own pace as a function of the requirements that it faces and various other interacting factors.