Are You Prepared for the Cloud?

Nick Kael
Principal Security Strategist
Symantec

What is Cloud Computing?

– Cloud Computing refers to the delivery of software (SaaS), infrastructure (IaaS), and/or platform (PaaS) as a service.

- Service Characteristics: Broad Network Access, Rapid Elasticity, Measured Service, On-Demand Self-Service, Resource Pooling.
- Adaptive and Consumption-based: Can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down; providing for an on-demand utility-like model of allocation and consumption.
- Can be provided privately or publicly, internally (on premises) or externally (off-premises) or a hybrid of the two

Symantec

Essential Characteristics

- On Demand Self Service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service

Service Models

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Deployment Models

- Public
- Private
- Community
- Hybrid

NIST Visual Model of Cloud Computing Definition

Symantec

Cause for Concern

IDC Enterprise Survey on the Cloud

- 74% of people regarded security as a significant or very significant challenge in adopting cloud-based applications

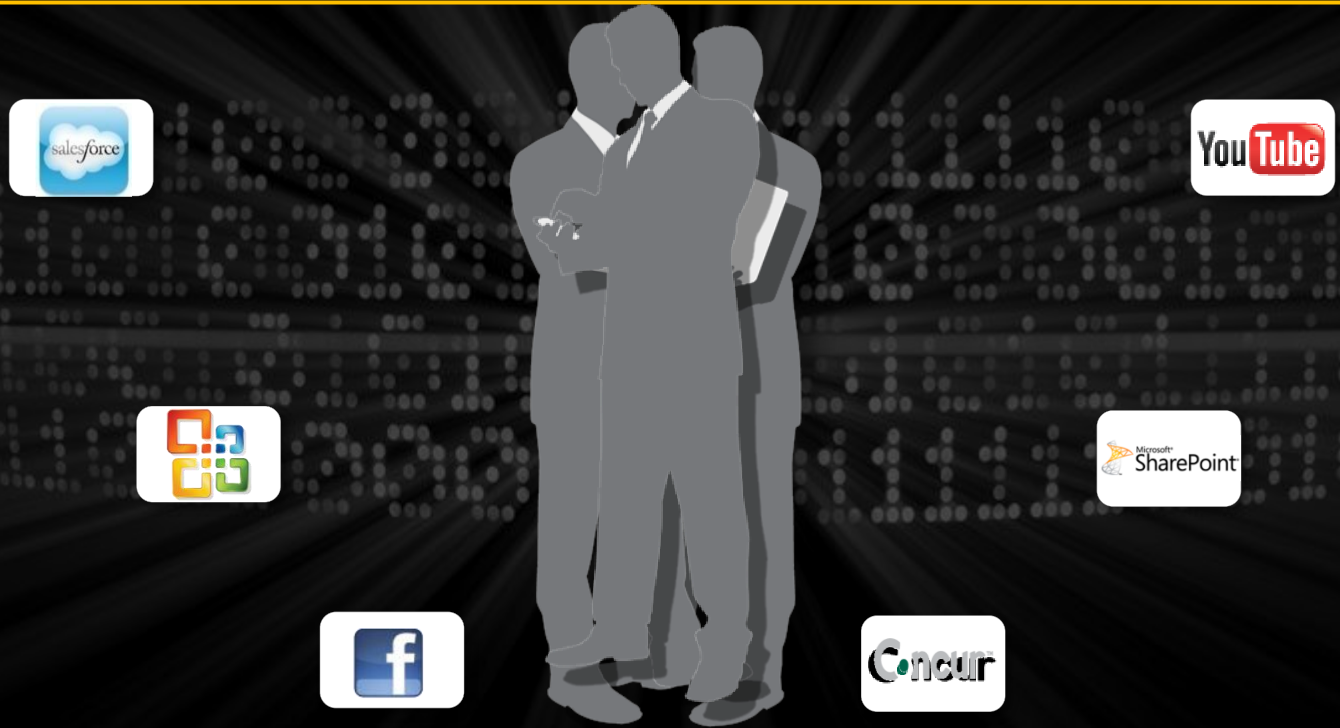
2010 Ponemon Institute report

- Most U.S. organizations lack the procedures, policies, and tools to ensure their sensitive information in the cloud remains secure. Despite security concerns and the expected growth in cloud computing, only 27 percent of respondents said their organizations have procedures for approving cloud applications that use sensitive or confidential information.

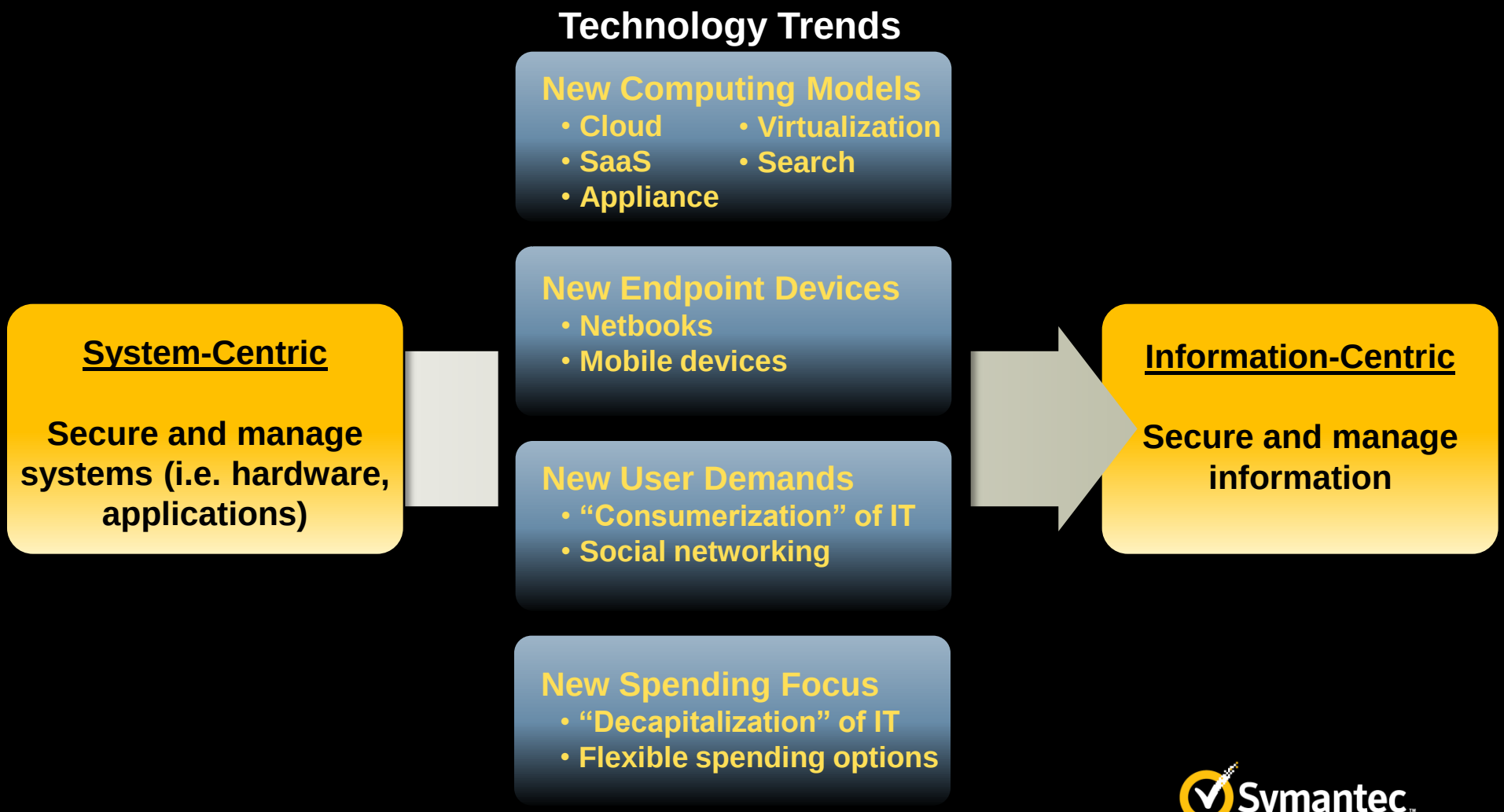
Symantec

Employees Connect In A Whole New Way

Edits ROI models with his team on Office Live.
Downloads latest sales presentation on SharePoint.
Updates his status on Facebook profile.



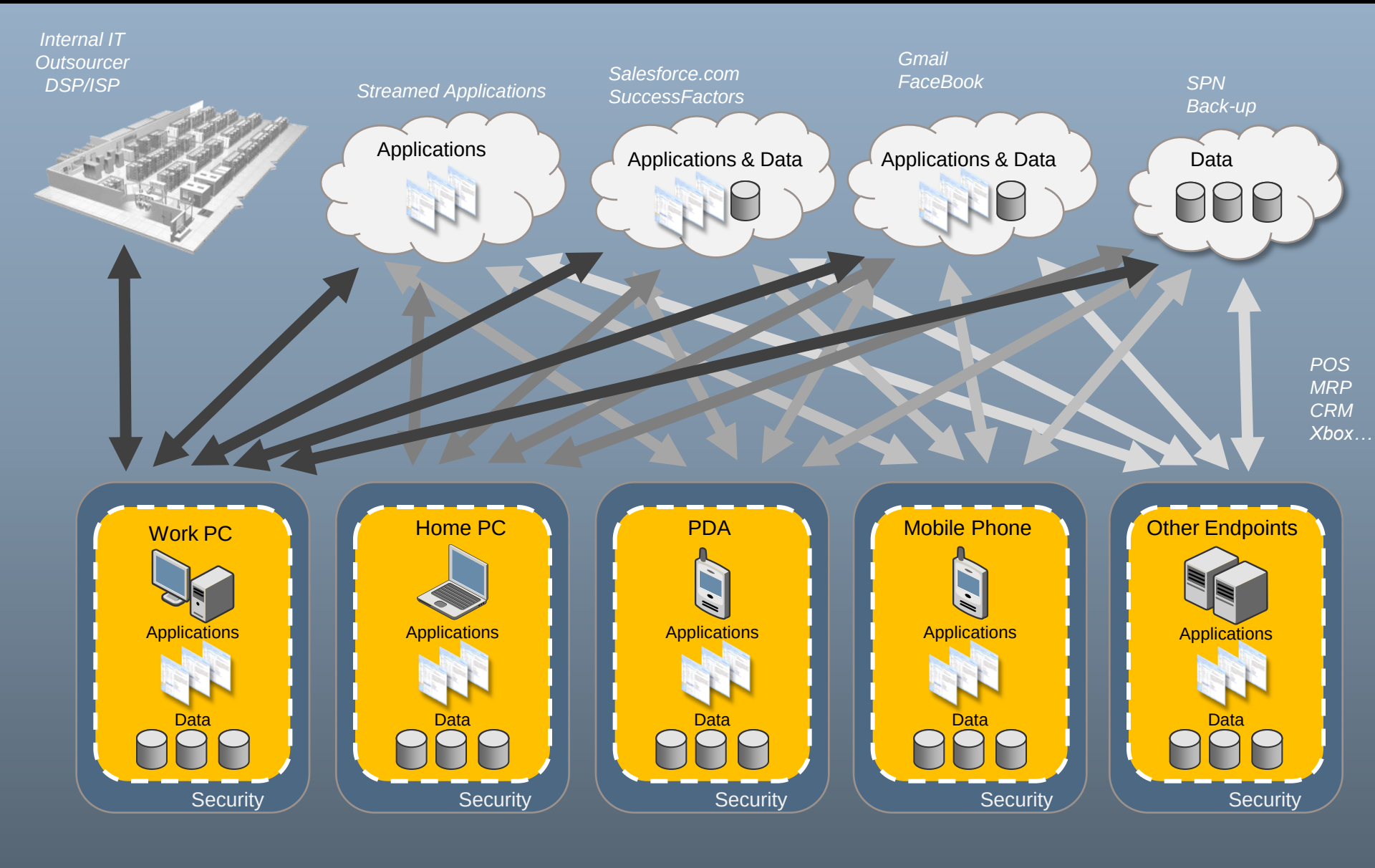
Technology Trends: Information Increasingly Independent of Systems



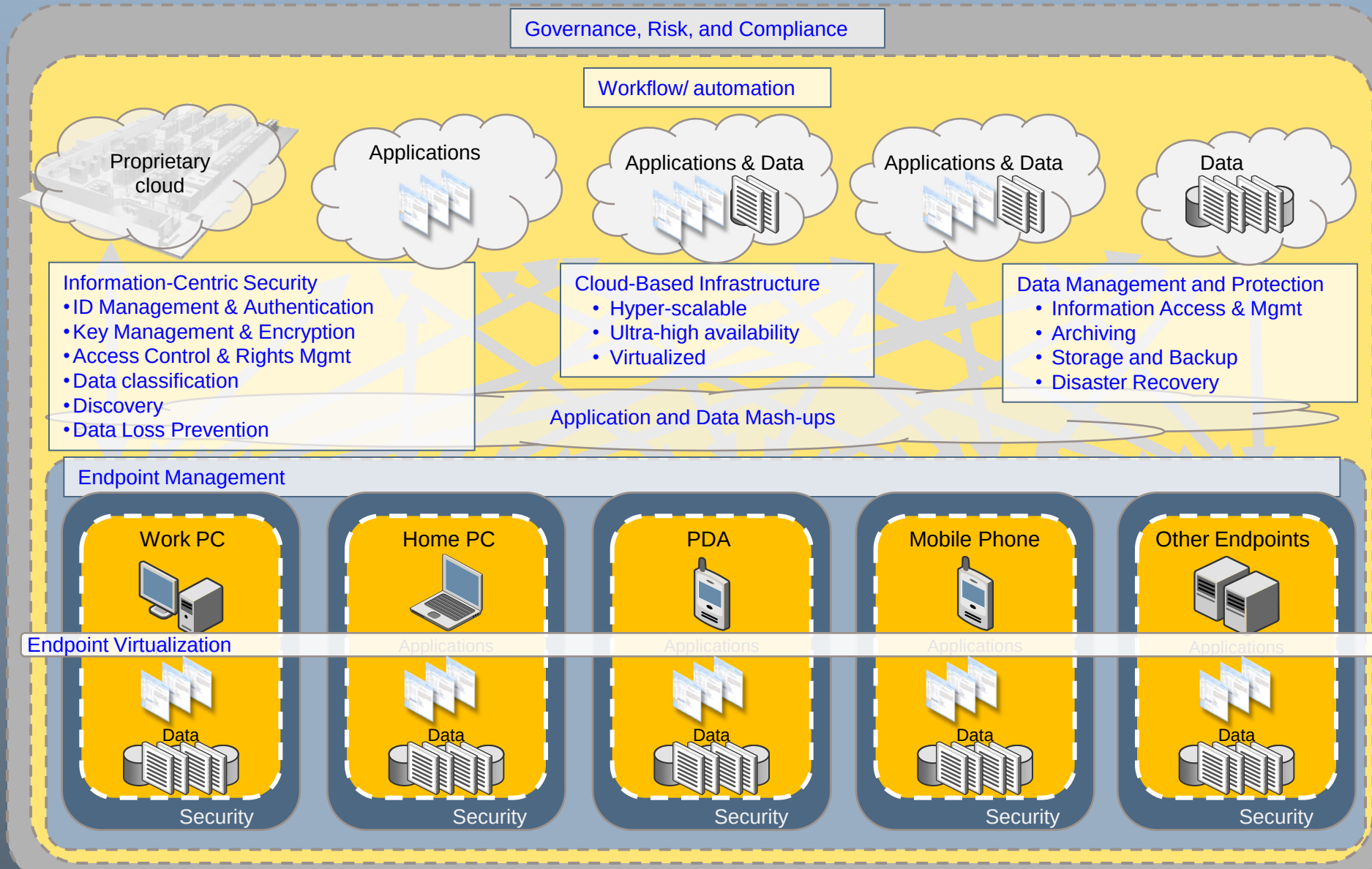
Symantec

What does that mean for IT Security?

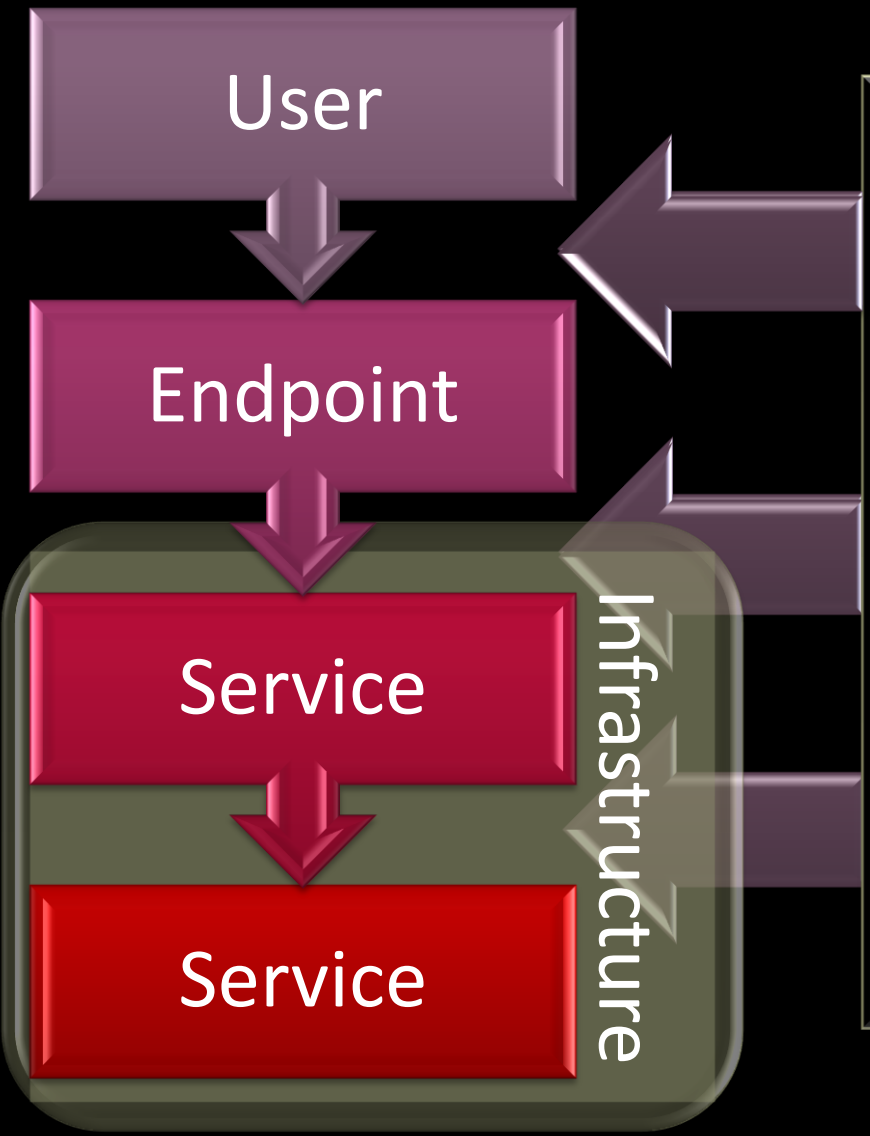
YIKES!



Next Generation IT Evolving Toward "Information-Centric" Computational Architectures



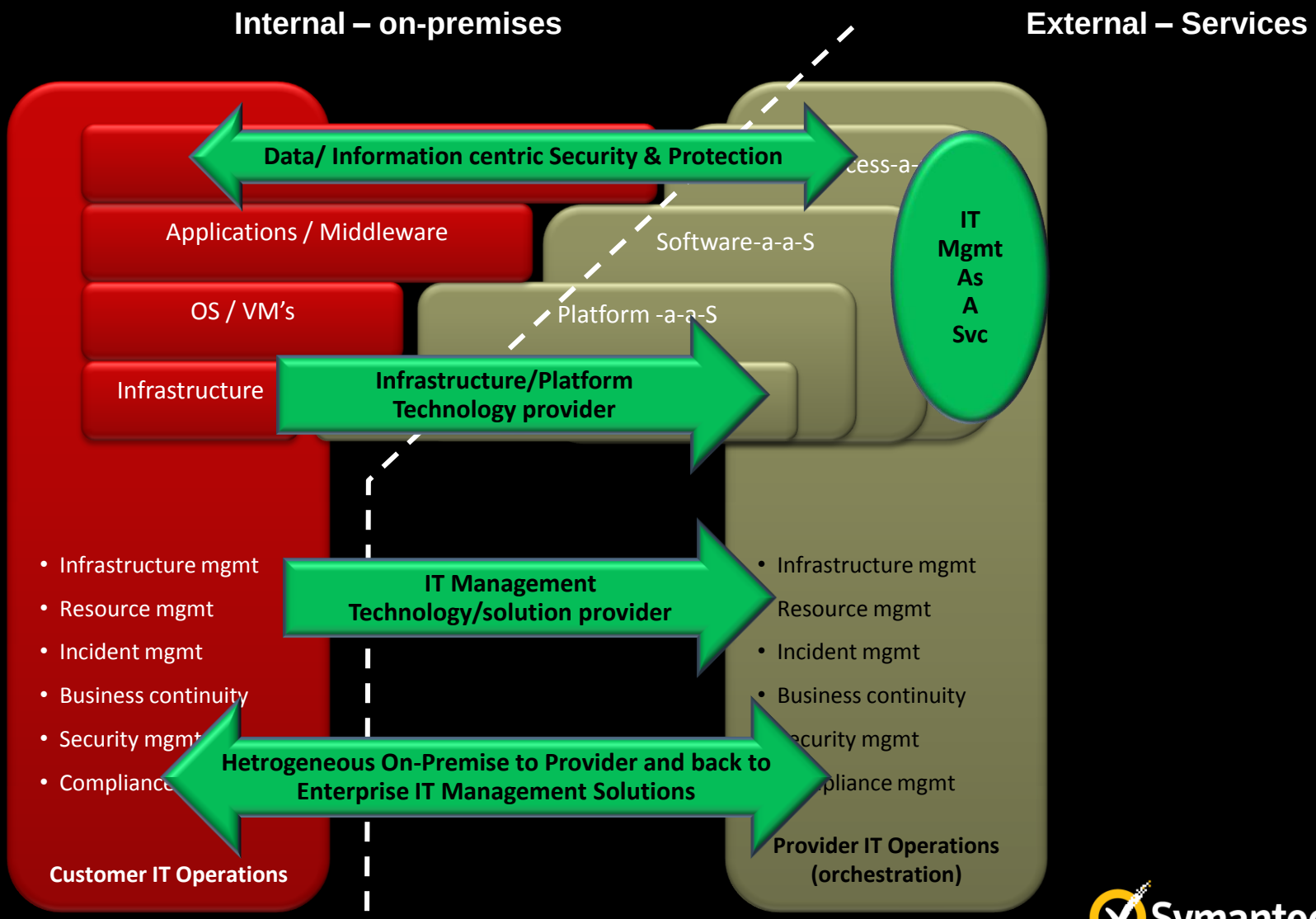
Cloud Paradigms Center on Interfaces: Solutions Needed on Both Sides



- Security – endpoint, DLP, IPS
- Access control (assessment against policy, attestation of compliance, remediation)
- Endpoint management, virtualization, and provisioning
- Reputation/trust – each side must attest and assess credentials of the other (identity)
- Virtualization and abstractions – endpoint, storage, data/backup availability
- Data and service mobility and availability – clustering, backup, and portability of services/applications

Symantec

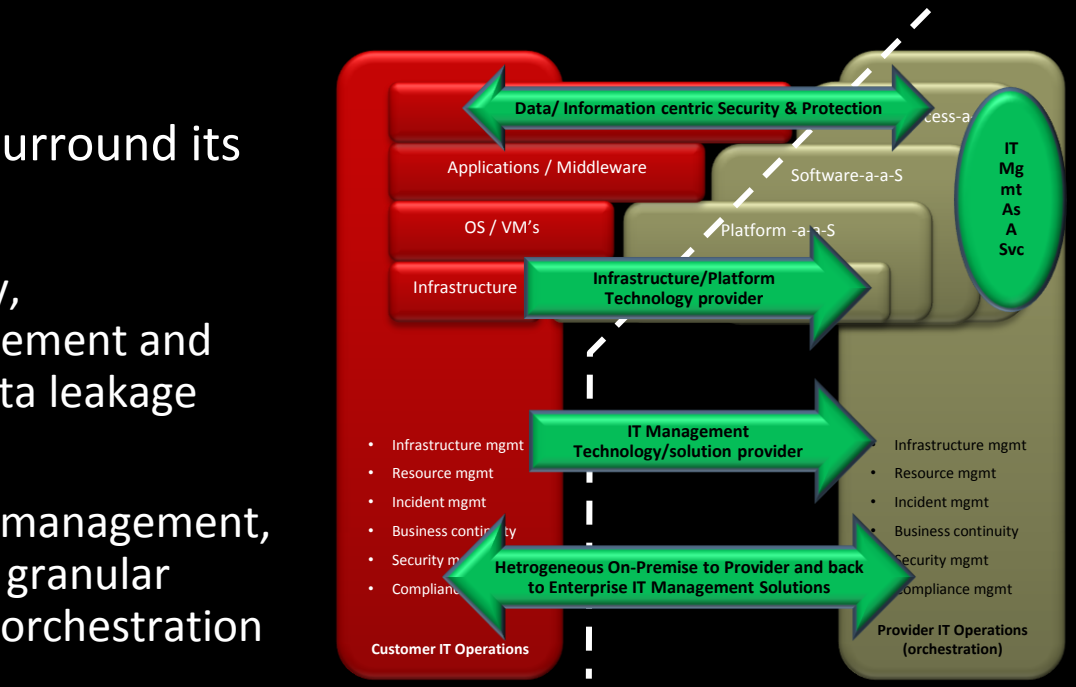
Interfacing with the Cloud



Symantec.

Approach

- Cloud computing challenges surround its interfaces
  - Security – attestation, identity, authentication, policy measurement and remediation, antimalware, data leakage prevention
  - Availability – backup, storage management, H/A failover, application level granular measurement and migration, orchestration
  - Endpoint management
- Building OnRamps to the Cloud
  - Build internal models to understand requirements and issues and to provide transition path
  - Gain benefits of cloud computing attributes with existing architectures



Symantec

Moving to the Cloud

Things to consider as you move to the Cloud

- Identify the Asset for Cloud Deployment ?
  - Data
  - Application/Functions or Processes
- Evaluate the asset to be moved to the cloud based on Risk/impact to your business.
  - How would we be harmed if …….
- Map that asset to the possible Cloud deployment models ?
  - Public
  - Private
  - Community
  - Hybrid
- Evaluate the Cloud Models and Possible Service Providers
- Map Potential Data Flows

Symantec

Moving to the Cloud

Things to consider as you move to the Cloud

- Mapping the Cloud Model to the Security Controls and Compliance Model
- Areas of critical focus:
- Governance
  - Governance & Enterprise Risk Management
  - Legal and Electronic Discovery
  - Compliance & Audit
  - Information Lifecycle
  - Portability & Interoperability
- Operational
  - Traditional Security, Business Continuity, Disaster Recovery
  - Data Center Operations
  - Incident Response, Notification and remediation
  - Application Security
  - Encryption & Key Management
  - Identity & Access Management
  - Virtualization

Credit : Cloud Security Alliance

Symantec

Secure Cloud Enablement

How does your enterprise enable secure Cloud ?

Leverage existing capabilities to enable a "Cloud Ready" enterprise

- What is the critical information to protect? Where is this data? How will it be used?
- Does the critical information have the right level of control?
- How will heterogeneous access and broad network connectivity be controlled?
- How will security and performance be managed in a highly virtualized environment?
- How can automation be used to abstract services from the infrastructure that provides them?

Symantec

Sources

- NIST
- Cloud Security Alliance- CCSK Certification

Symantec

Thank You !

Nick L. Kael

Principal Security Strategist

Symantec – Security Business Practice

nick_kael@symantec.com

Symantec