Bringing Cloud Security Down to Earth

Ted Ritter, CISSP
Senior Research Analyst
www.nemertes.com

Agenda

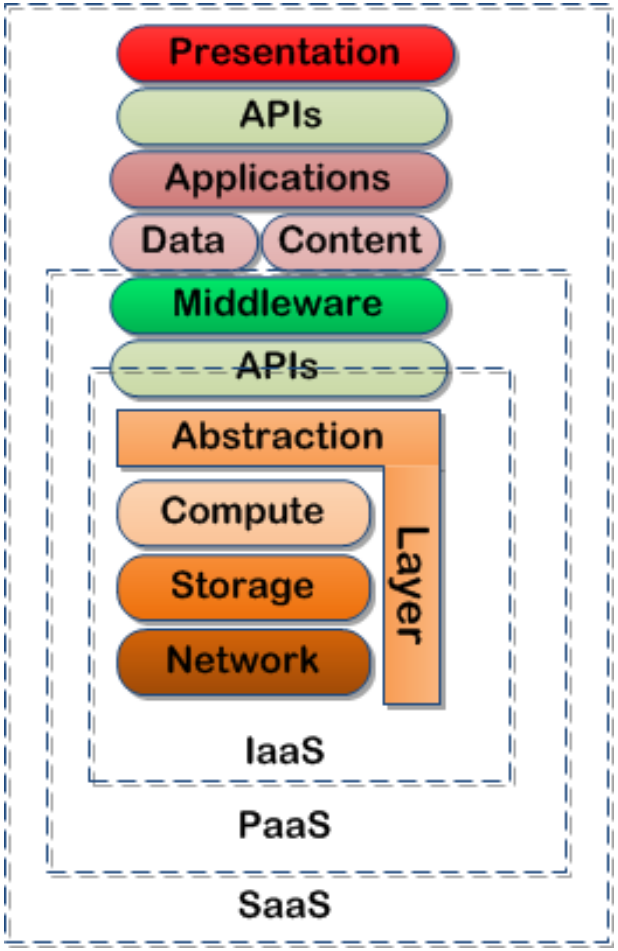
- About Nemertes
- Cloud Dynamics and Adoption
- Assessing Risk of Cloud Services
- Addressing Cloud Security
- Emerging Approaches to Cloud Security
- Virtualization Security Contact Points
- Summary and Conclusions

Nemertes: Bridging the Gap Between Business & IT

- Quantifies the business impact of emerging technologies
- Conducts in-depth interviews with IT professionals
- Advises businesses on critical issues such as:
  - Unified Communications
  - Social Computing
  - Data Centers & Cloud Computing
  - Security
  - Next-generation WANs
- Cost models, RFPs, Architectures,

Cloud Dynamics and Adoption

- IaaS & PaaS adoption < 9%
- SaaS adoption = 52%
- Limitation of IaaS and PaaS adoption is concern over security and compliance
- Virtualization provides agility, flexibility and scalability
- Virtualization Security (VirtSec) is a fundamental aspect of cloud security for all cloud models



*Based on Cloud Security Alliance CSA Guide service model (www.cloudsecurityalliance.org)

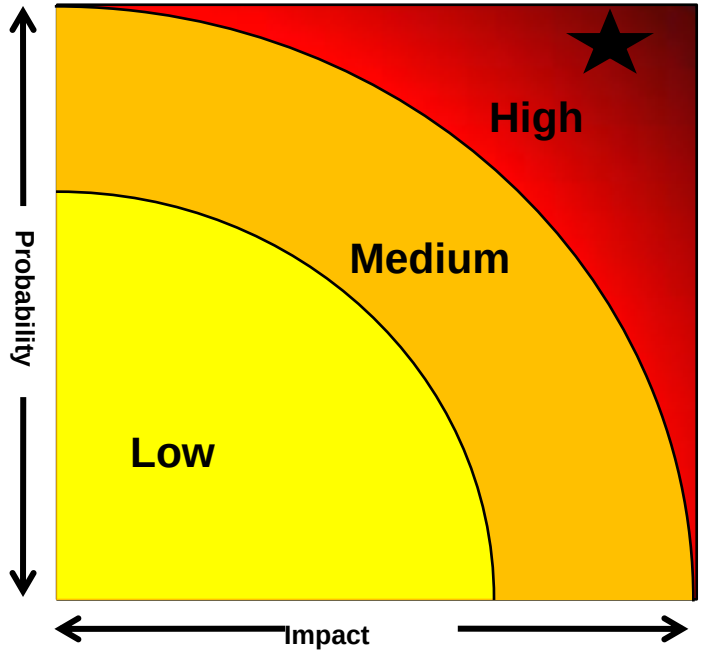
Assessing Risk of Cloud Services

Asset Assessment
- Define assets
- Assign values of asset loss or compromise

Vulnerability Assessment
- Define vulnerabilities
- Assess probability of exploit

Risk Assessment
- Define all risks
- Risk probability
- Risk impact

Risk Mitigation
- Preventive and detective controls
- Compensating controls
- Residual risk

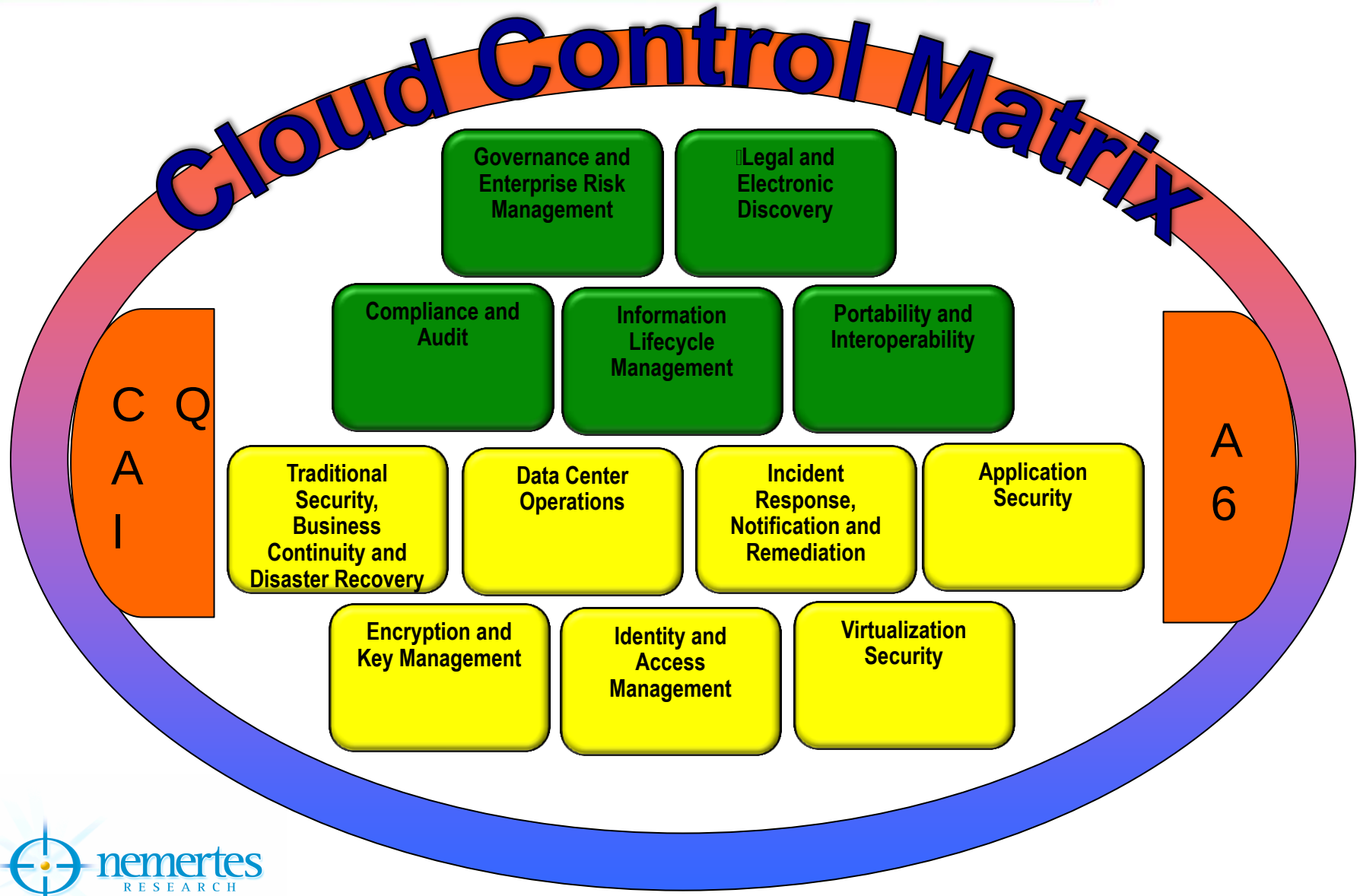


Public Cloud Risks: Top 10

1. Loss of governance
2. Service provider lock-in
3. Compliance risks
4. e-Discovery and litigation support
5. Management interface compromise
6. Network management failure
7. Isolation failure
8. Data protection
9. Insecure/Incomplete data deletion
10. Malicious insider

Addressing Cloud Security

The Cloud Security Alliance



*Based on Cloud Security Alliance guidance (www.cloudsecurityalliance.org)

CSA GRC Stack

- **Governance Risk and Compliance (GRC) Stack**
  - **Toolkit consisting of three components:**
    - **Cloud Audit**
      - **Automated Audit, Assertion, Assessment and Assurance API (A6) via an open, secure, extensible interface and methodology**
    - **Cloud Controls Matrix (CCM)**
      - **Controls framework addressing the security concepts and principles aligned to the CSA guidance 13 domains**
      - **Pulls from other standards – HITRUST CSR, ISO 27001/27002, ISACA COBIT, PCI, HIPAA and NIST 800-53**
    - **Consensus Assessments Initiative Questionnaire (CAIQ)**
      - **Questions a cloud consumer or cloud auditor should ask a cloud provider**

*Based on Cloud Security Alliance guidance (www.cloudsecurityalliance.org)

CSA Governance Domains

Domain	Areas of Focus
Governance and Enterprise Risk Management	• Legal precedence for agreement breaches between provider and customer • Ability to adequately assess risk of a cloud provider • Joint responsibility for data • Managing international boundaries
Legal and Electronic Discovery	• Establishing and enforcing retention policies regardless of data location • Complying with breach disclosure laws • Privacy and regulatory requirements • Complying with international laws
Compliance and Audit	• Compliance with internal, regulatory, industry-specific and legislative rules • Audit roles and responsibilities in support of compliance
Information Lifecycle Management	• Responsibilities for data integrity, confidentiality and availability • General data control and identification in the cloud and between cloud and customer
Portability and Interoperability	• Moving data from one provider to another • Bringing data (and other assets) in-house • Interoperability between providers

*Based on Cloud Security Alliance guidance (www.cloudsecurityalliance.org)

CSA Operational Domains

Domain	Areas of Focus
Traditional Security, Business Continuity and Disaster Recovery	• High-level security discussion relating enterprise risk management to cloud • The role of cloud in BC-DR • Ways in which the cloud may improve security
Data Center Operations	• Provider data center operations and continuity of operations • SAS 70, ISO 27001, NIST, etc.
Incident Response, Notification and Remediation	• Incident detection, response, notification and remediation • Complexity of incidents in the cloud • Coordination between cloud provider and customer
Application Security	• Assessing the role of IaaS, PaaS and SaaS for application security • Coding and implementation best practice
Encryption and Key Management	• The "why" behind the need for encryption in the cloud • Both protecting data and access to cloud resources
Identity and Access Management	• Leveraging directory services to provide access controls • Assessing readiness for cloud-based IAM
Virtualization	• Issues of multi-tenancy at the server virtualization level • VM isolation, co-residence and hypervisor vulnerabilities

*Based on Cloud Security Alliance guidance (www.cloudsecurityalliance.org)

Controls to Address Risk

Model	Preventive Controls	Detective Controls
SaaS	• Identity Management including multi-factor authentication • Browser patching and hardening • Endpoint security	• Access reports
PaaS	• User authentication (multi-factor) • User privilege management • Browser patching and hardening • Endpoint security	• Access reports • Vulnerability scanning (application and user access)
IaaS	• VPN for management access and movement of VMs • Configuration and patch management • Access controls and multi-factor authentication • Host IDS/IPS • VirtSec appliance	• Access reports • Event logging and correlation • Vulnerability scanning (application and user access)

Preventive Control: Identity Management

- **The concept of trust changes with cloud model**
  - **Trust must extend into the cloud (SaaS, PaaS and IaaS)**
- **Three key identity management areas**
  - **User management, Authentication management, Authorization management**
- **Evolving standards**

- SAML – Secure Assertion Markup Language➔ Single Sign-on (SSO)
- XACML – eXtensible Access Control Markup Language ➔ least privilege
- OAuth – Open Authentication ➔ share cloud data

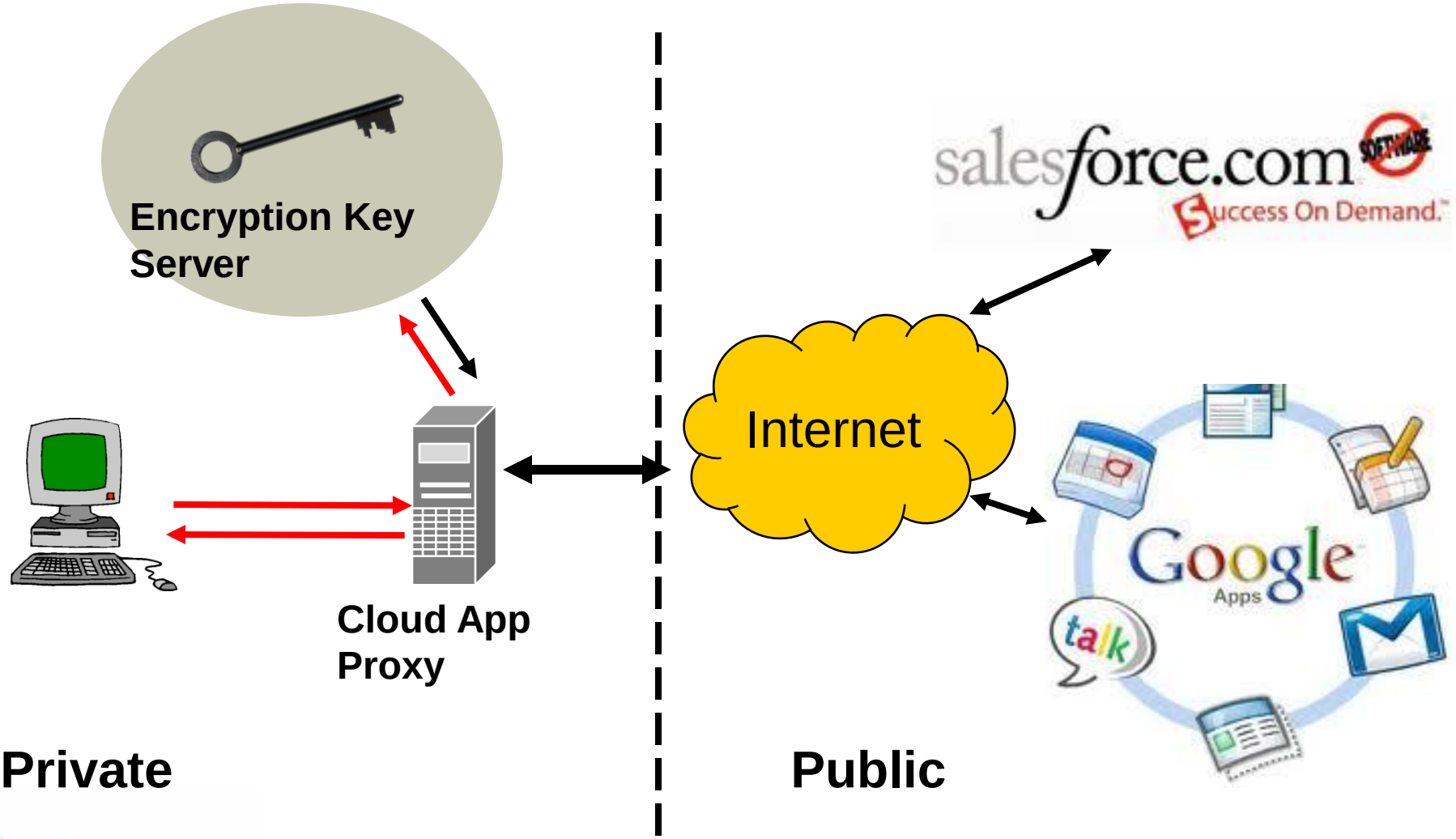
Identity Management Recommendations

IAM Area	Challenge	Recommendation
User Management	• Secure and timely management of onboarding and offboarding cloud users • Extending enterprise IAM systems into cloud	• Avoid building custom interfaces for user provisioning • Push cloud provider to use open standards
Authentication Management	• Credential management • Strong authentication • Delegated authentication	• Manage credentials in own identity solution and federate with cloud provider • When users self-provision services a decentralized standard like OpenID provides authentication to multiple services • For IaaS establish a dedicated VPN or use standard assertion (SAML) with encryption (SSL) • For IaaS, PaaS and SaaS push cloud provider to delegate authentication to the enterprise via SAML or WS-Federation • Multi-factor authentication is essential

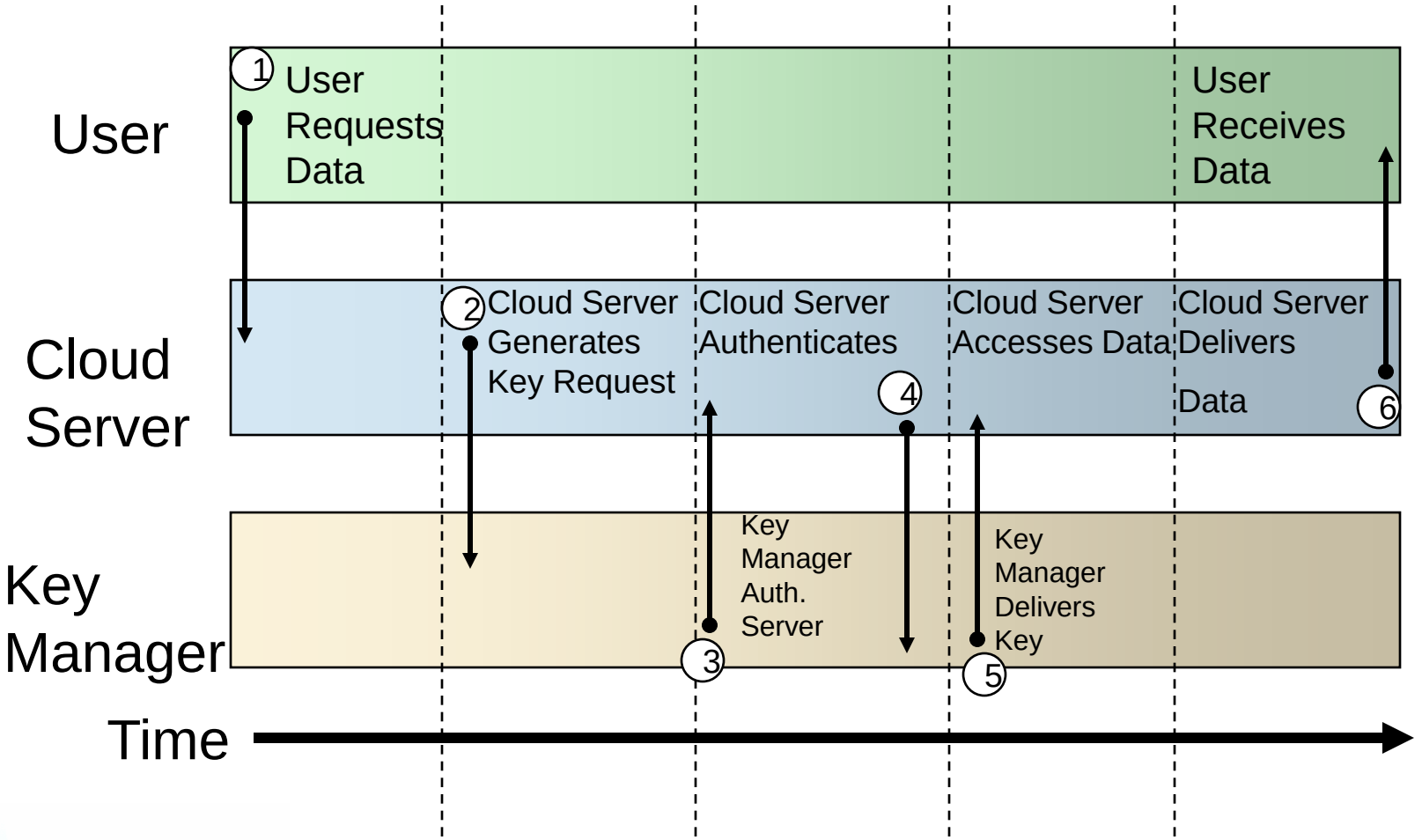
Identity Management Recommendations, C

IAM Area	Challenge	Recommendation
Authorization Management	• Establishing standard authorization model for multiple cloud providers • Passing authorization information between cloud providers • Enforcing and monitoring enforcement of authorization	• Identity authoritative sources of user and policy information • Determine privacy policies for type of data • Establish mechanism to transfer policy information from policy administration point (PAP) to policy decision point (PDP) • Establish mechanism to transfer policy information from policy information point (PIP) to PDP • Establish mechanism to request policy decision from PDP • Establish policy enforcement point (PEP) to enforce policy • Implement logging of all authorization management actions

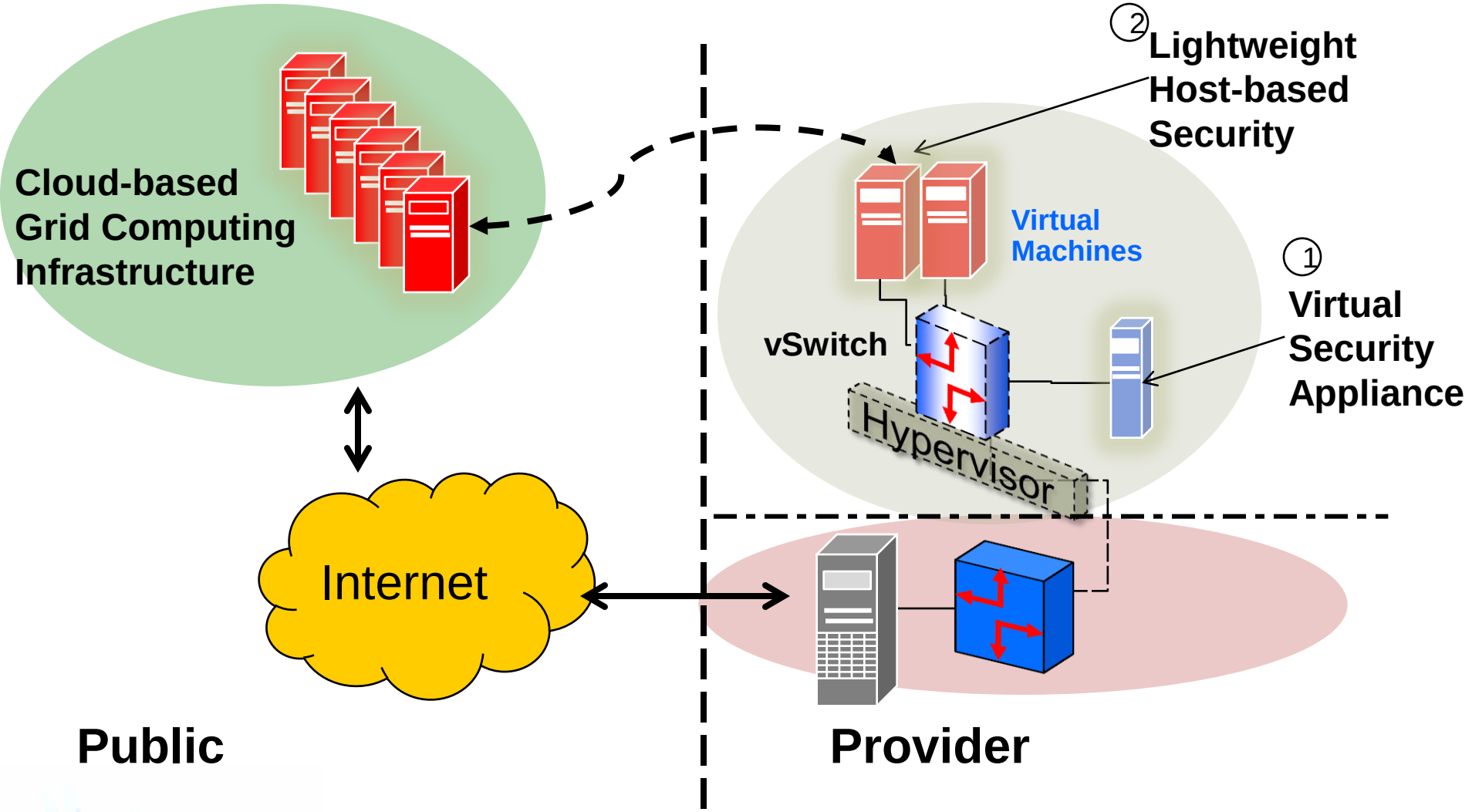
Emerging Approaches to Cloud Security Data Centric



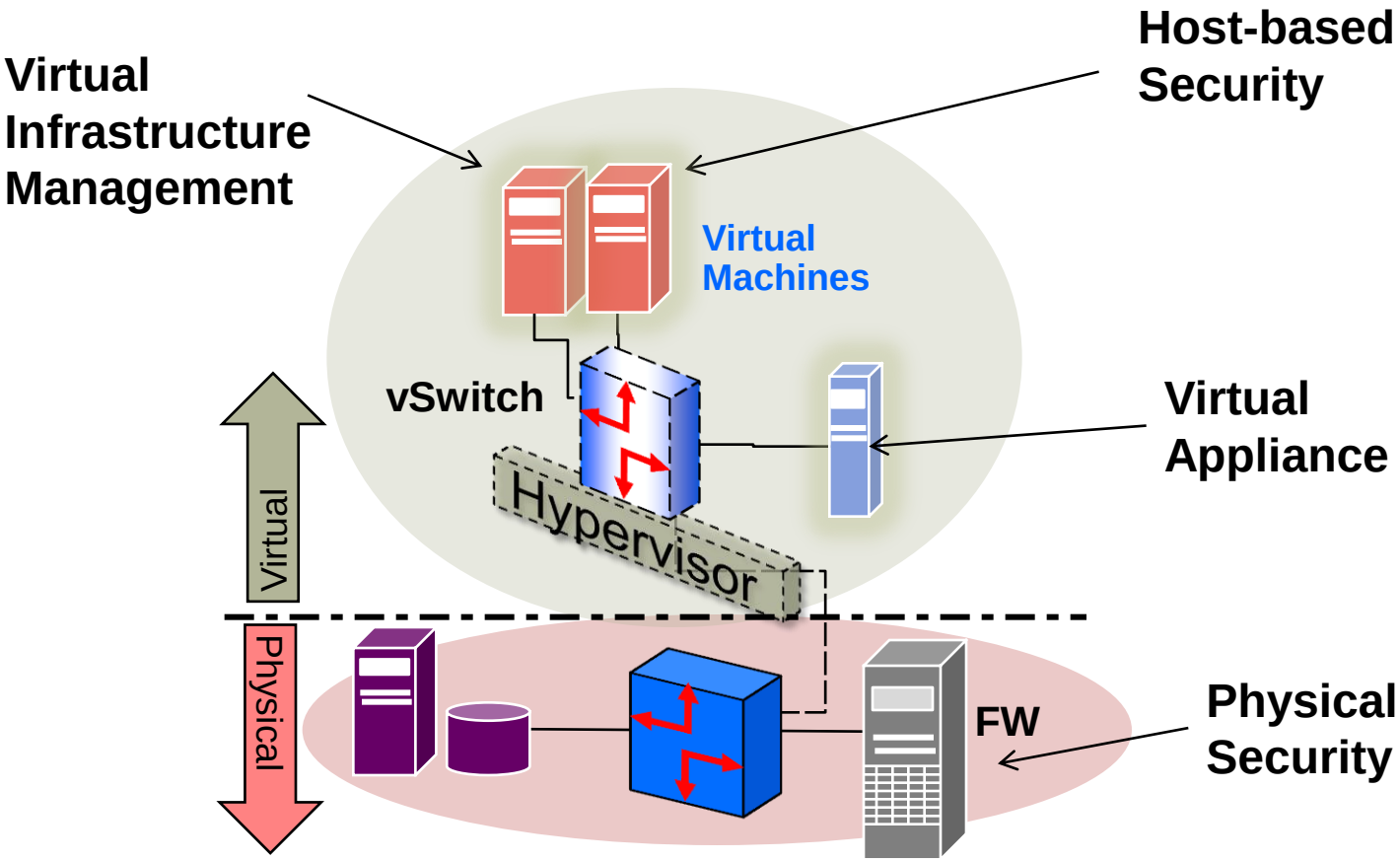
Emerging Approaches to Cloud Security Data Centric Continued



Emerging Approaches to Cloud Security
Infrastructure Centric



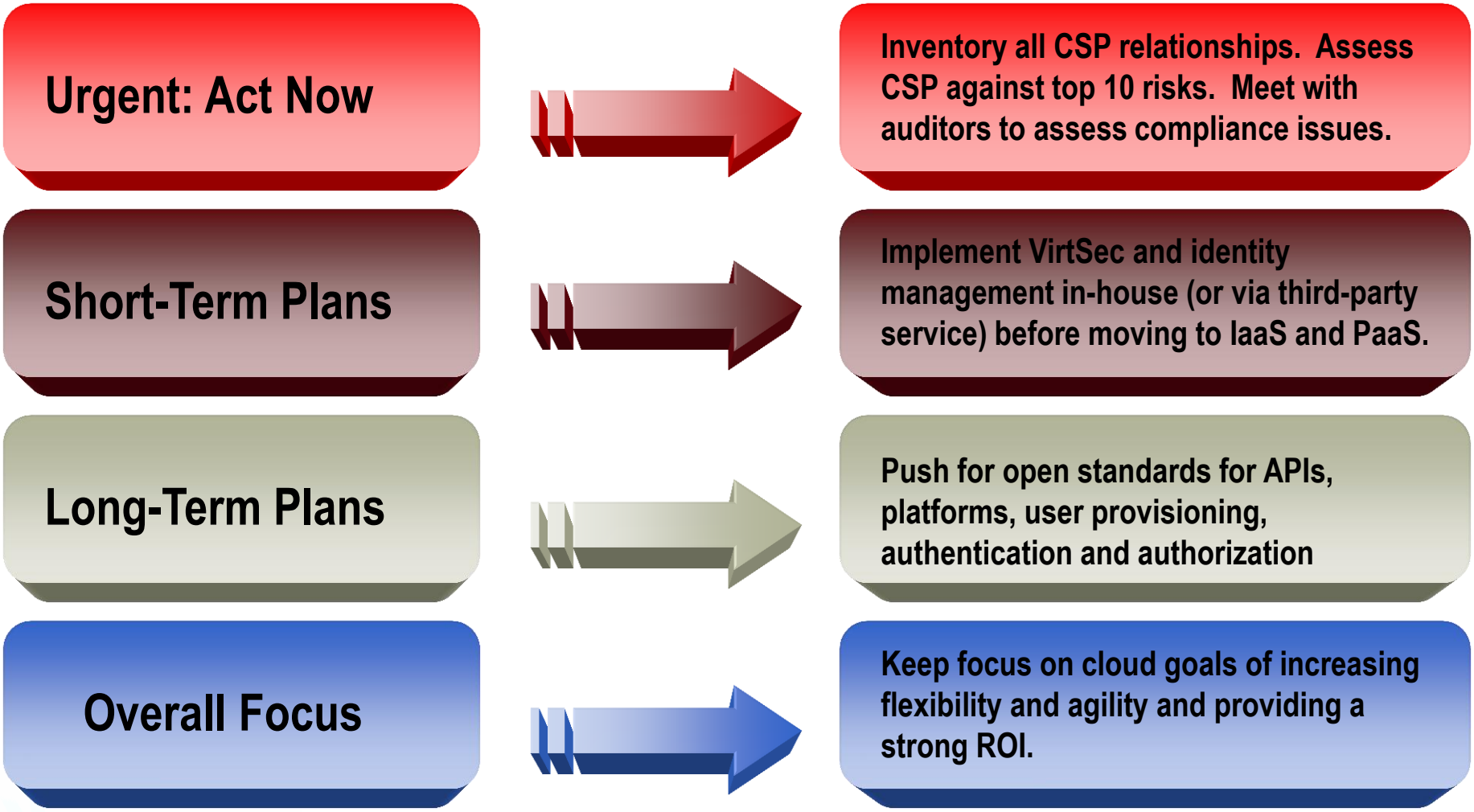
Virtualization Security Contact Points



Summary

- A risk-based approach is the only way to assess a cloud computing deployment decision
  - Most offerings are currently too risky for sensitive data
- Establish detective and preventive controls specific to each cloud deployment model:
  - SaaS - Browser patching, endpoint security, access reports
  - PaaS – Browser patching, hardening, endpoint security, access reports and vulnerability scanning
  - IaaS – VPN, configuration and patch management, host IDS/IPS, VirtSec appliance, access reports, vulnerability scanning, logging & event management
- Identity management is a key area of preventive control focus for all service models
  - This starts internally

Conclusion: What Should You Be Doing?



Thank You

Ted Ritter, CISSP
Senior Research Analyst
www.nemertes.com