



NSFOCUS

THE 10TH ANNIVERSARY OF NSFOCUS

绿盟科技十年誌庆

浅谈云计算安全威胁和防护要点



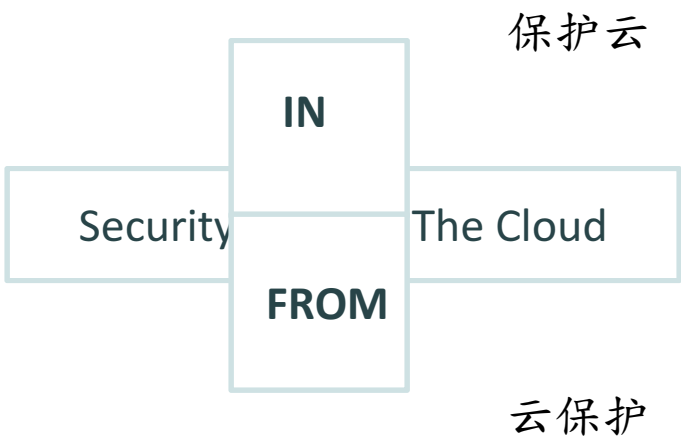
赵粮
2010年4月22日

北京鸿翔大厦

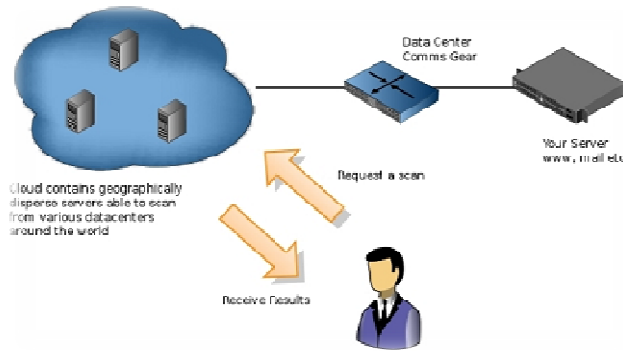
云计算为运营商带来充满想象的蓝海



按需的自服务
 宽带接入
 虚拟池化的资源
 快速弹性架构
 可测量的服务



身份账号, 访问控制
 防拒绝服务
 漏洞扫描 补丁
 审计



AV@Cloud
 IAM@Cloud
 VA@Cloud
 Log&Audit@Cloud

NIST Definition of Cloud Computing v15, <http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>

现代领先的运营商已经将产品线从单纯的话音、接入、电路等资源类供应扩展到IT的各个方面，例如：

- 应用管理
- 数据媒体应用
- 移动应用视频会议
- IT产品批发
- **网络安全**
- **云计算**
- 等等

网络安全和云计算已经成为运营商手中的重武器



at&t

Protect yourself from DDoS attacks
Don't wait until it's too late

- ▶ View Video
- ▶ Read the White Paper
- ▶ Read the Product Brief

The banner features a shield with a globe inside, surrounded by purple lines representing network connections.

Overview Description/Diagram Features Benefits Related Services

Send to a colleague

Telecom Companies: The Cloud Clock is Ticking! -- Gartner

http://blogs.gartner.com/daryl_plummer/2009/03/03/telecom-companies-the-cloud-clock-is-ticking/

Cloud computing

How cloud computing can help your business thrive.



More about BT's cloud computing services



Bringing it all together



Provided by BT



Provided by BT



Provided by BT



Provided by BT



Provided by BT



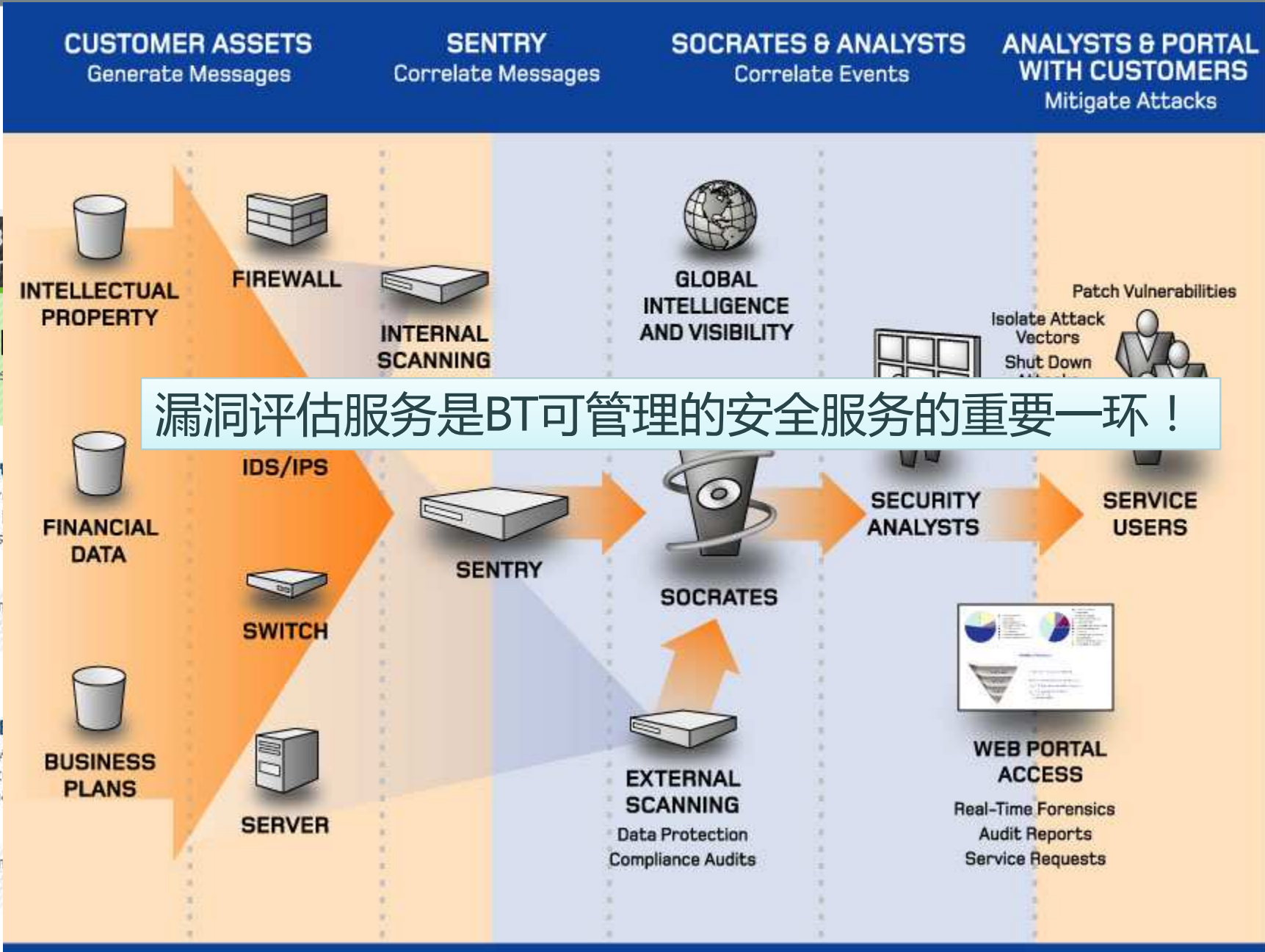
Provided by BT

Cloud computing is an Internet-based way of working where users access

云服务SaaS和网络安全服务是BT综合信息服务提供商的关键产品



Try all our business applications for FREE

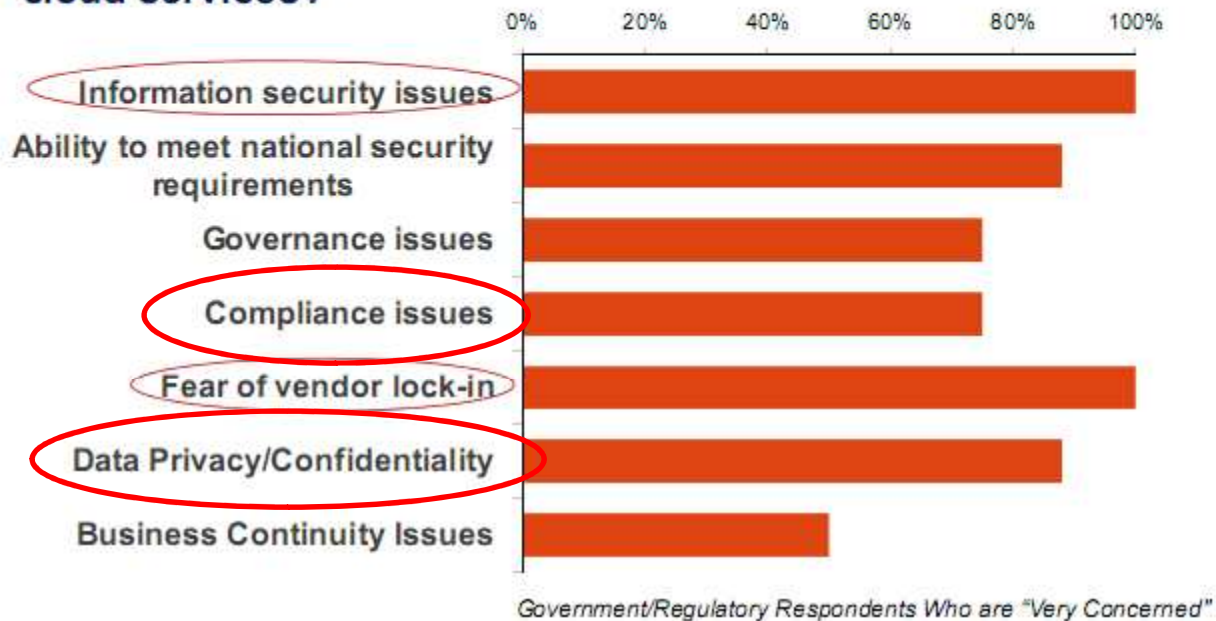


- Threat #1: Abuse and Nefarious Use of Cloud Computing
云计算的滥用、恶用、拒绝服务攻击
- Threat #2: Insecure Interfaces and APIs
不安全的接口和API
- Threat #3: Malicious Insiders
恶意的内部员工
- Threat #4: Shared Technology Issues
共享技术产生的问题
- Threat #5: Data Loss or Leakage
数据泄漏
- Threat #6: Account or Service Hijacking
账号和服务劫持
- Threat #7: Unknown Risk Profile
未知的风险场景



帮助建立
用户的信心、消除
用户的顾虑是云计算安全的重要目标

Q: How concerned are you about the following issues related to cloud services?



Source: World Economic Forum/Accenture survey, Fall 2009

2010年12月17日发布2.1版, 3月29日中文版完成

- D1: 云计算架构框架
- D2: IT治理和企业风险管理
- D3: 法律和电子发现
- D4: 合规性和审计
- D5: 信息生命周期管理
- D6: 可携带性和可交互性
- D7: 传统安全、业务连续性和灾难恢复
- D8: 数据中心运行
- D9: 事件响应、通告和补救
- D10: 应用安全
- D11: 加密和密钥管理
- D12: 身份和访问管理
- D13: 虚拟化

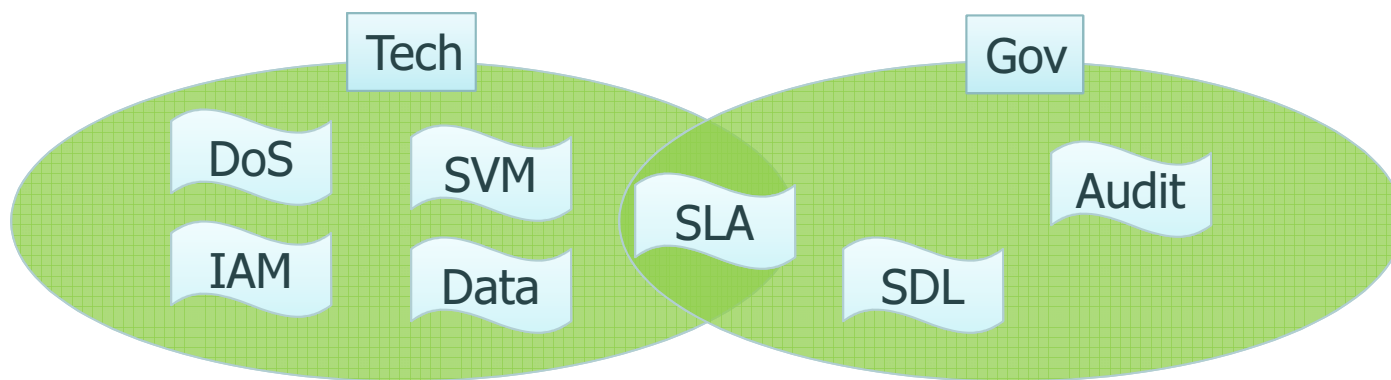


Table: Security Assessment Matrix for SAAS, PAAS, and IAAS

	SAAS		PAAS		IAAS	
	Provider	Customer	Provider	Customer	Provider	Customer
Physical Security	X		X		X	
Environmental Protection	X		X		X	
Capacity Management	X		X		X	X
Metering	X		X		X	
Billing	X		X		X	
Change Management	X		X	X	X	X
Incident Management	X	X	X	X	X	X
Vulnerability Management	X		X	X	X	X
Patch Management	X		X	X	X	X
Security Management	X		X		X	X
Security Monitoring	X		X	X	X	X
Storage Security	X		X		X	
Data Handling	X		X		X	
Decommissioning and Disposal	X		X		X	
Media Disposal	X		X		X	
Disaster Recovery and Business Continuity	X	X		X	X	X
Service Level Reporting	X	X	X	X	X	X
Supply Chain Security	X		X	X	X	X
Technology Refresh Cycles	X		X	X(Software)	X	X
Asset Management	X		X	X(Software Licenses)	X	X
Visitor Management	X		X		X	
Staff Vetting	X		X	X	X	X

SAMPLE

- [DoS]对抗各种形式的拒绝服务攻击的能力 - D7/D8/D9
- [SLA]清晰、细化、合同化的安全SLA - D2/D7/D8
- [IAM]完备的身份和访问控制管理 - D12/D13
- [SVM]全面及时的漏洞扫描和修补 - D4/D10/D13
- [Data]透明和明确定义的数据安全 - D5/D6/D11
- [Audit]完备的电子证据和审计系统 - D3/D4
- [SDL]应用生命周期的安全和供应商安全管理 - D10/D11



- 1 七个安全推荐主要从用户的采购角度来阐述，也可以为云服务商的安全建设提供参考
- 2 七个安全推荐与CSA云安全指南一致，但与七大威胁并无一一对应关系
- 3 七个建议之间没有明显的优先级顺序
- 4 该推荐还在开发中……



Thank you.

