RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

云安全服务实践

Security-as-a-Service in Action

郑林，CISSP

McAfee

RSA CONFERENCE CHINA 2012
RSA信息安全大会2012

专题会议主题：

专题会议分类：

关于演讲者

- 郑林  @McAfeeZhenglin）
  - 迈克菲（McAfee）公司中国区技术总监
  - 2001年，首个在中国发现CodeRed II（红色代码）蠕虫
  - 2006年，尝试提供在线委托式邮件安全服务
  - 2011年起，发起并负责建设了中国首批基于SaaS模式的端点安全、邮件安全、Web安全运营平台

议程

- 第一部分：攻防失衡导致的安全风险长尾
- 第二部分：风险到机会的转变
- 第三部分：云安全服务实践
- 第四部分：全球威胁智能感知——安全的方向

议程

- 第一部分：攻防失衡导致的安全风险长尾
  - 威胁和企业防御措施现状
- 第二部分：风险到机会的转变
  - 安全市场长尾
  - 云安全概念的误区
  - 云安全服务市场状况
- 第三部分：云安全服务实践
  - 中国云安全服务用户案例分享
  - 服务商的机会及案例分享
- 第四部分：全球威胁智能感知——安全的方向

第一部分：攻防失衡导致的安全风险长尾

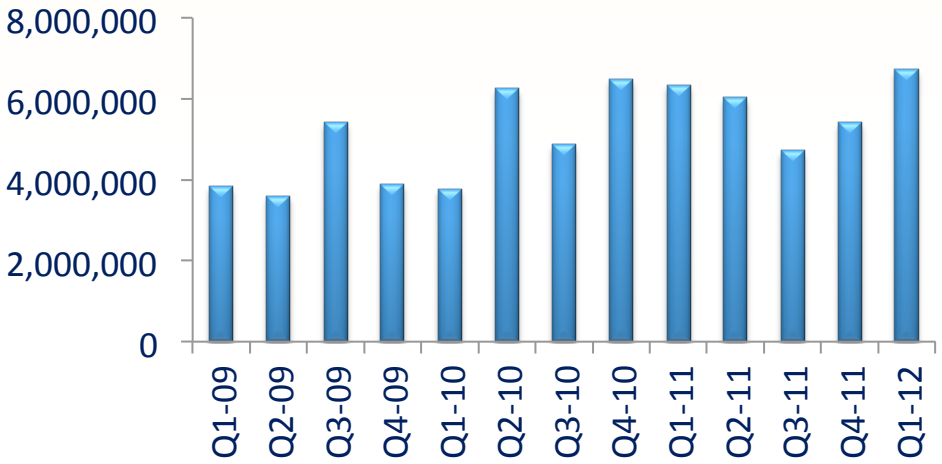
RSA CONFERENCE CHINA 2012
RSA信息安全大会2012

专题会议主题：

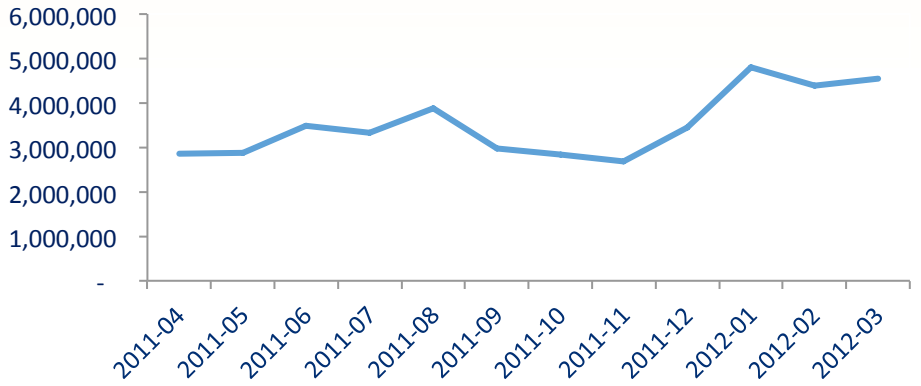
专题会议分类：

恶意代码和僵尸网络持续增长

每季度新增恶意代码样本数量



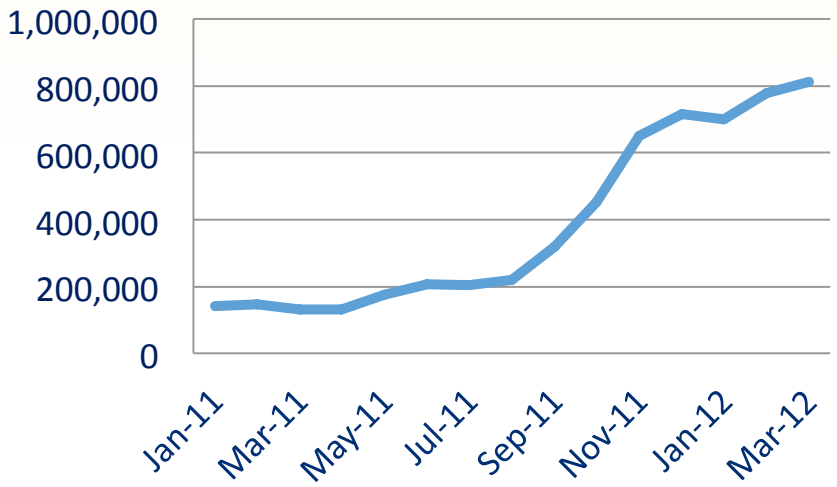
每月新增全球僵尸网络数量



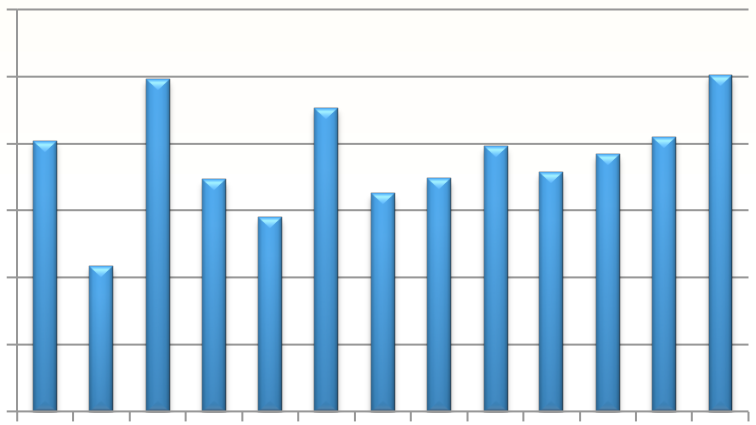
—— McAfee Labs

“挂马”网站和木马

活动的恶意URL数量

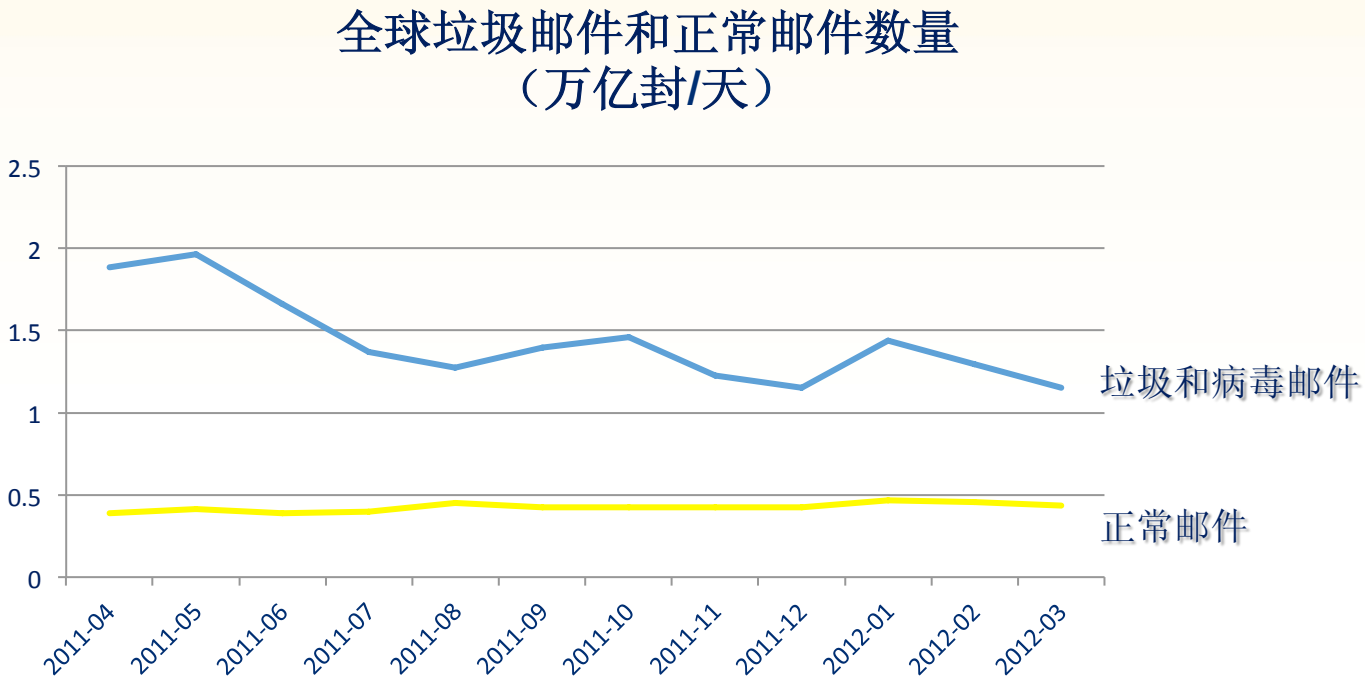


新增口令盗窃类木马样本数量



—— McAfee Labs

垃圾邮件



—— McAfee Labs

中国中小企业信息化

- 2010年末，全国工商登记中小企业1100万多家，个体工商户超过3400万个。
- 中小企业提供了80%以上的城镇就业岗位、提供了全国约65%的发明专利、75%以上的企业技术创新和80%以上的新产品开发。
- 中小企业应用信息技术开展研发、管理和生产控制的比例达到45%，利用电子商务开展采购、销售等业务的比例达到40%

“十二五”中小企业成长规划，工业和信息化部，2011

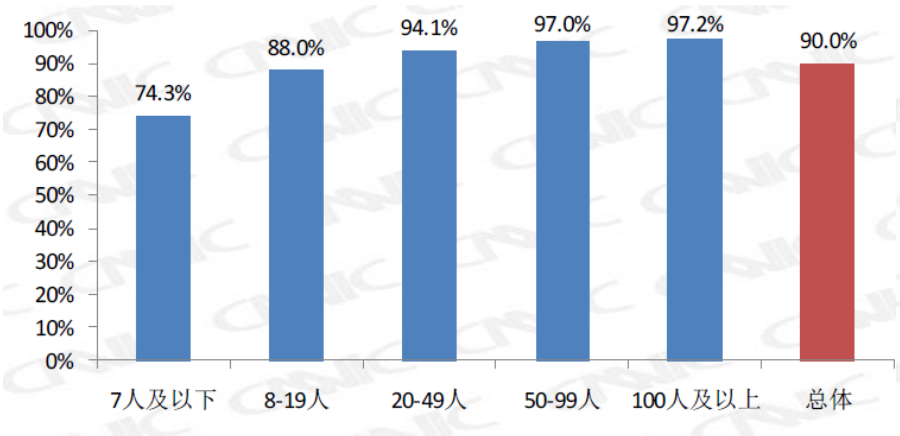


图 1　使用计算机的企业比例（按企业规模划分）

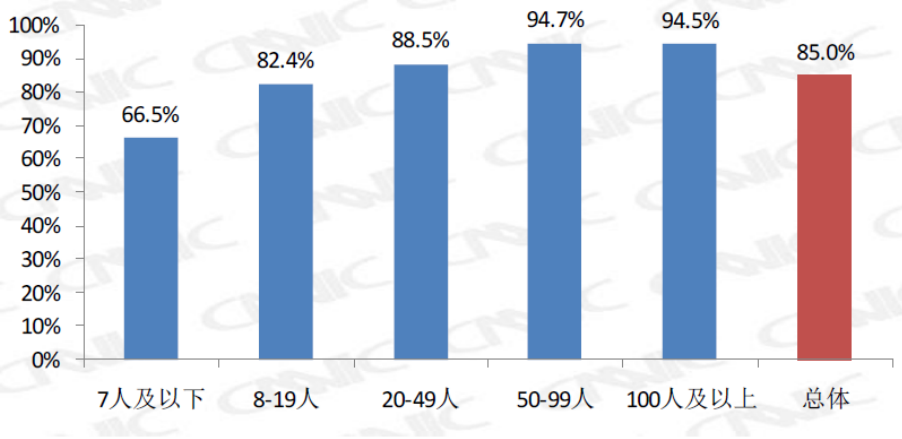
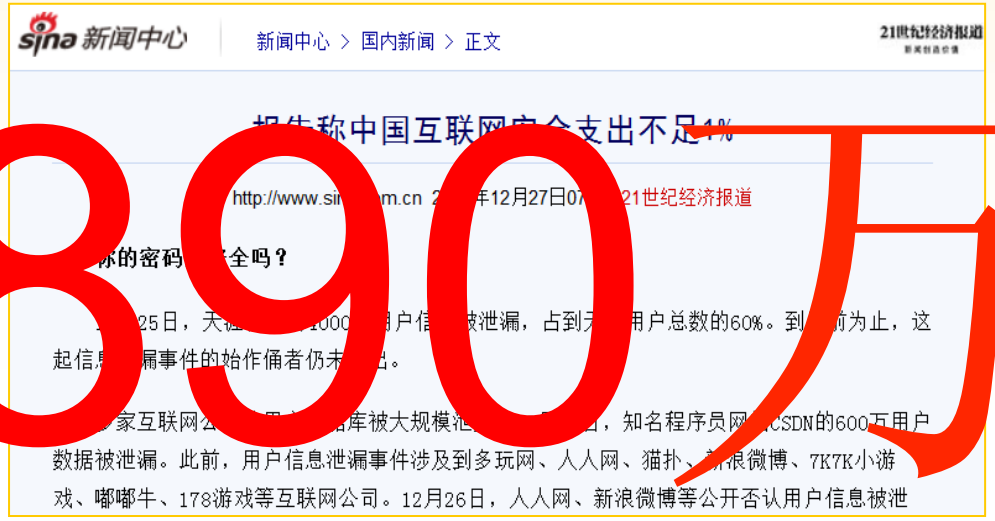


图 5　使用互联网办公的企业比例（按企业规模划分）

中国中小企业互联网应用调查报告，CNNIC, 2011

巨大的安全风险在累积



890万

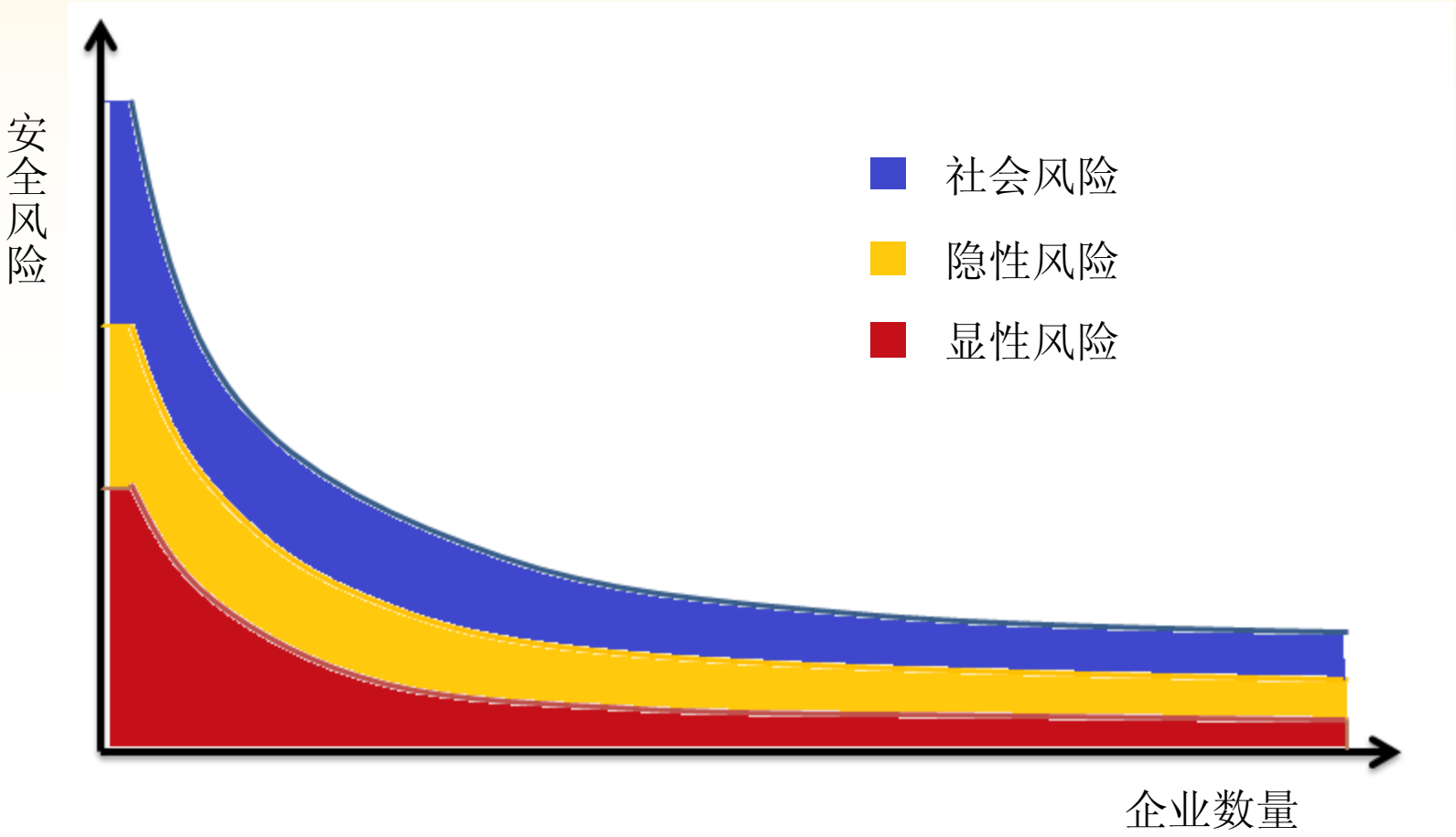
信息失窃
直接财务损失
声誉损失
影响工作效率

对合作伙伴的影响
未来业务损失

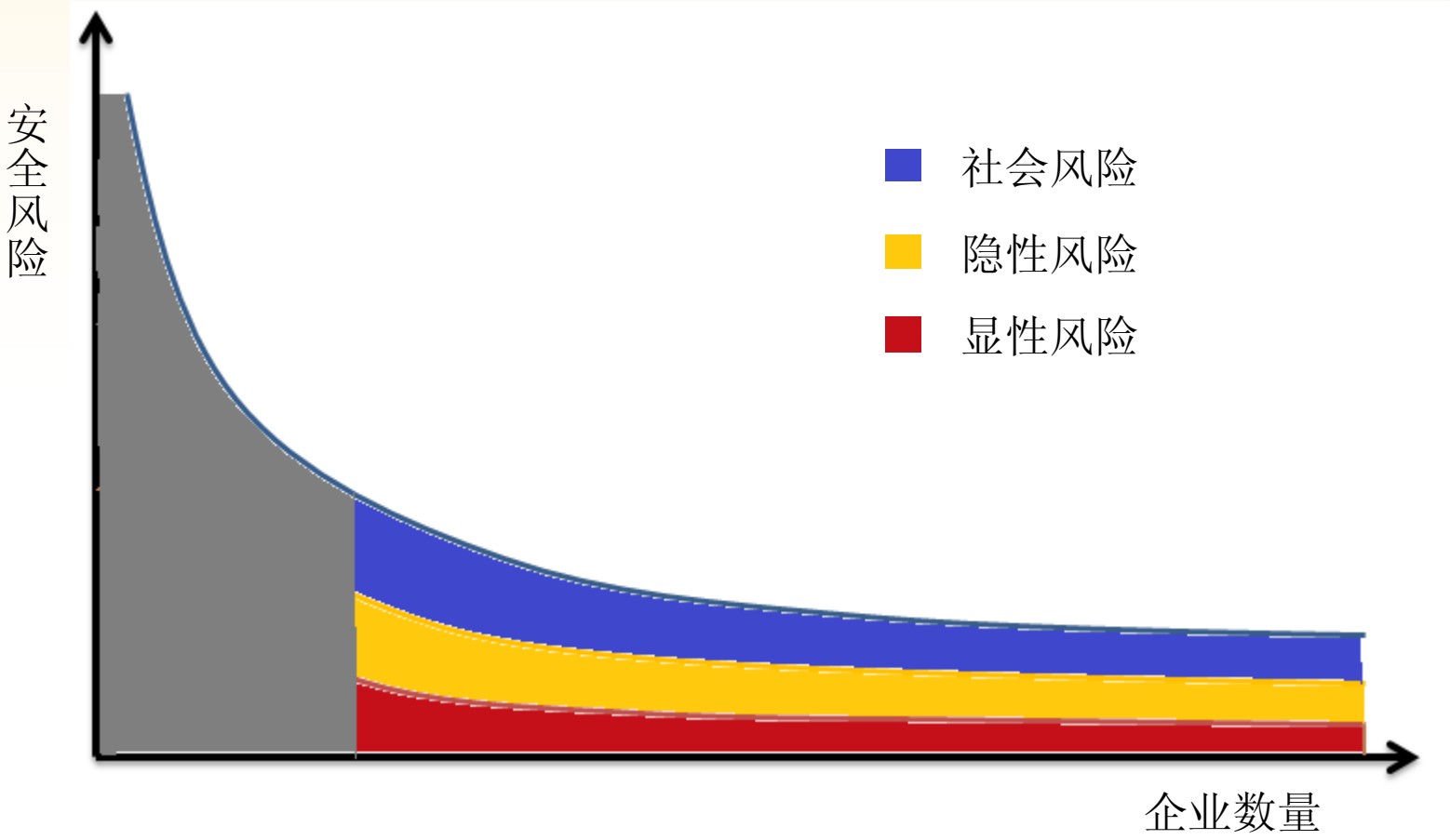
僵尸网络

——CNCERT

安全风险长尾的形成



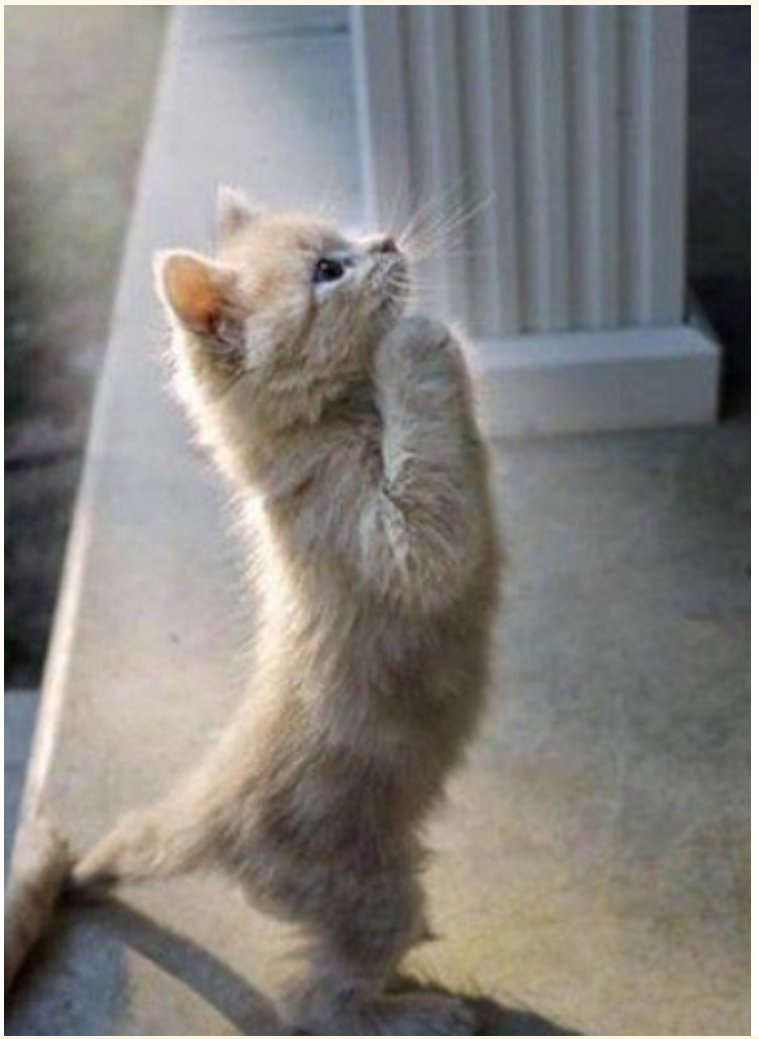
安全风险长尾的形成



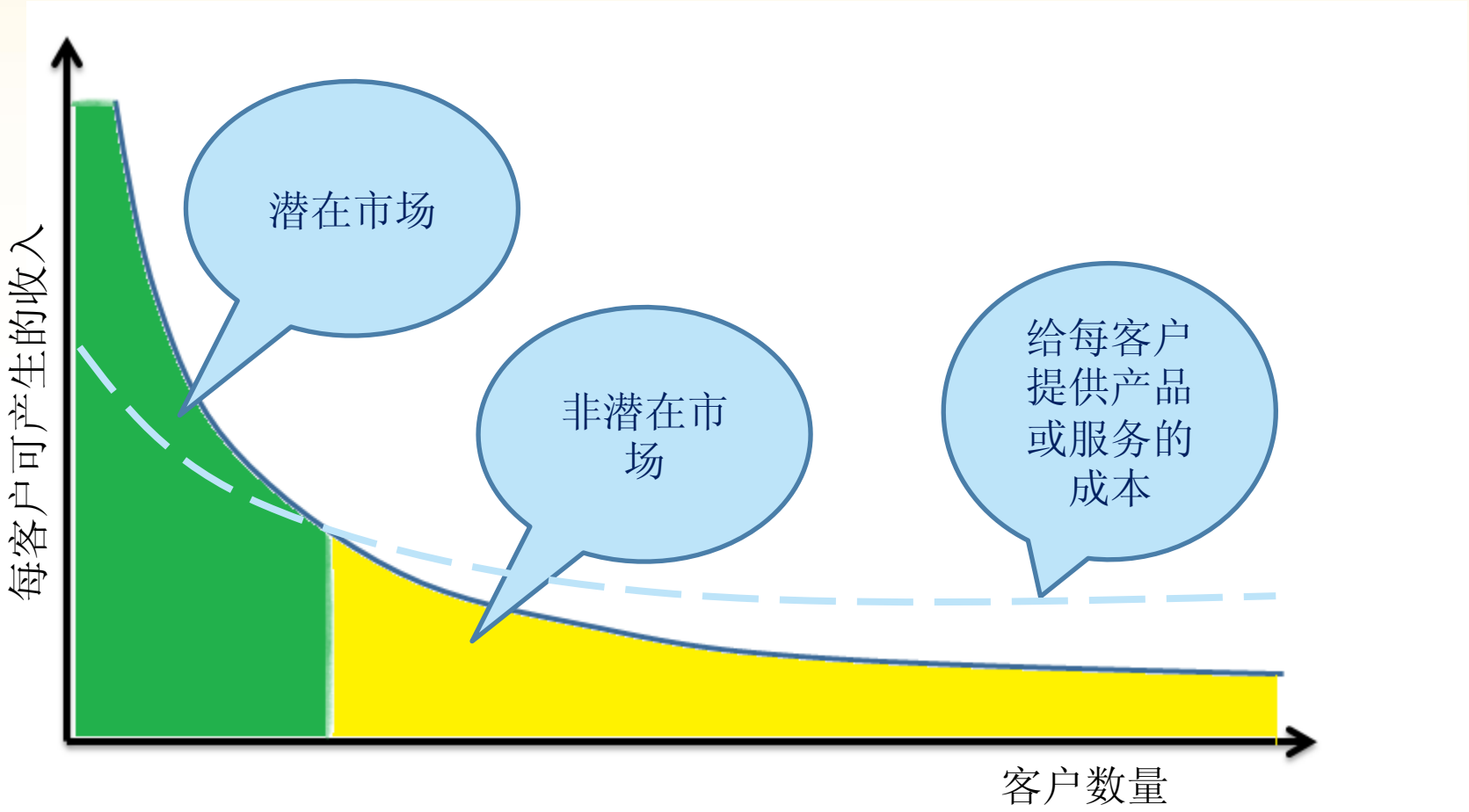
为什么中小企业无法实现有效的安全防护？——从中小企业的角度分析

RSA CONFERENCE CHINA 2012

- 专业人员
- 资本性支出
- 规模增长和灵活性
- 维护负担
- 时间



为什么中小企业无法实现有效的安全防护？——从集成商和服务商的角度分析



第二部分：风险到机会的转变

RSA CONFERENCE CHINA 2012
RSA信息安全大会2012

专题会议主题：

专题会议分类：

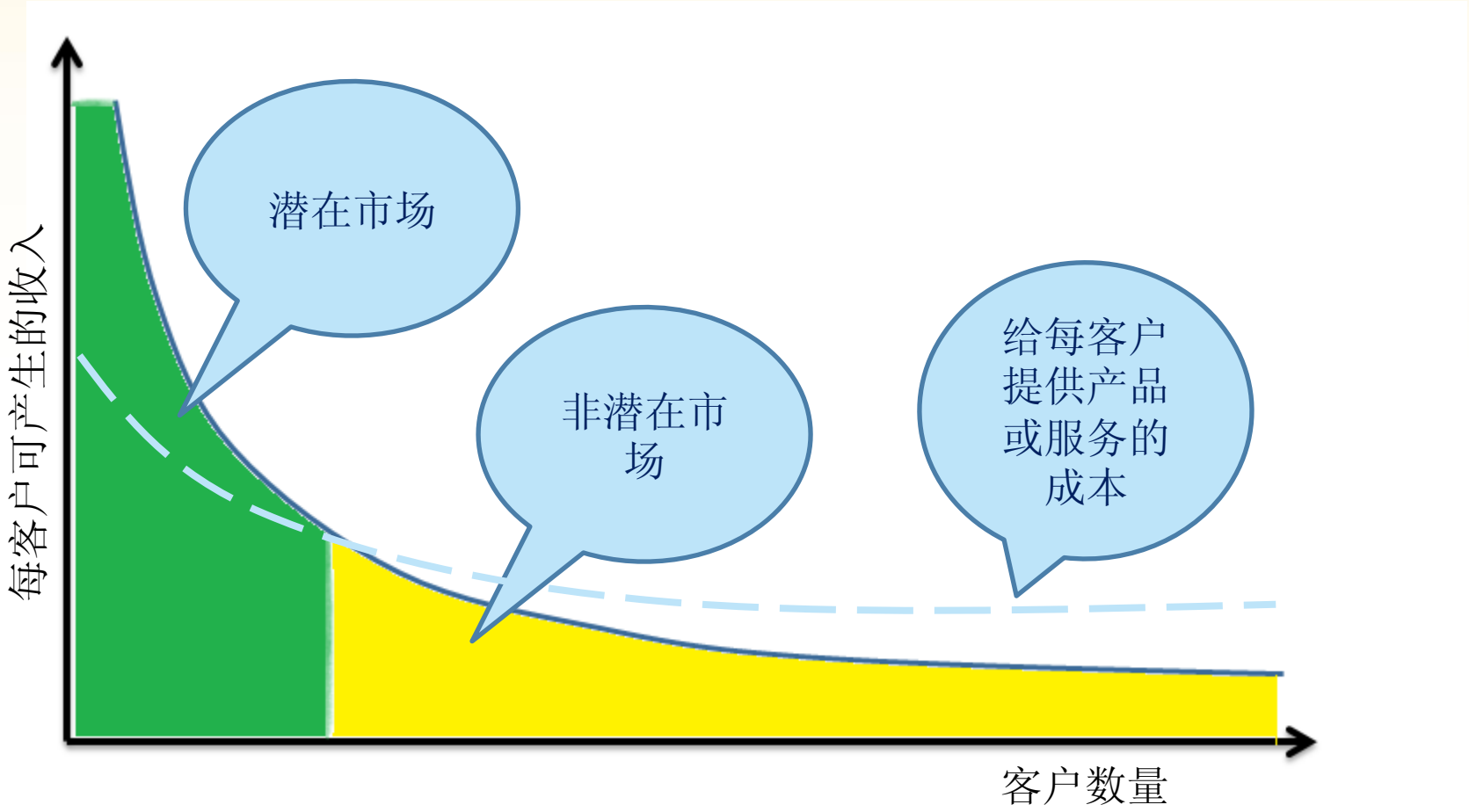
利用云实现风险到机会的转变——从用户角度分析

RSA CONFERENCE CHINA 2012

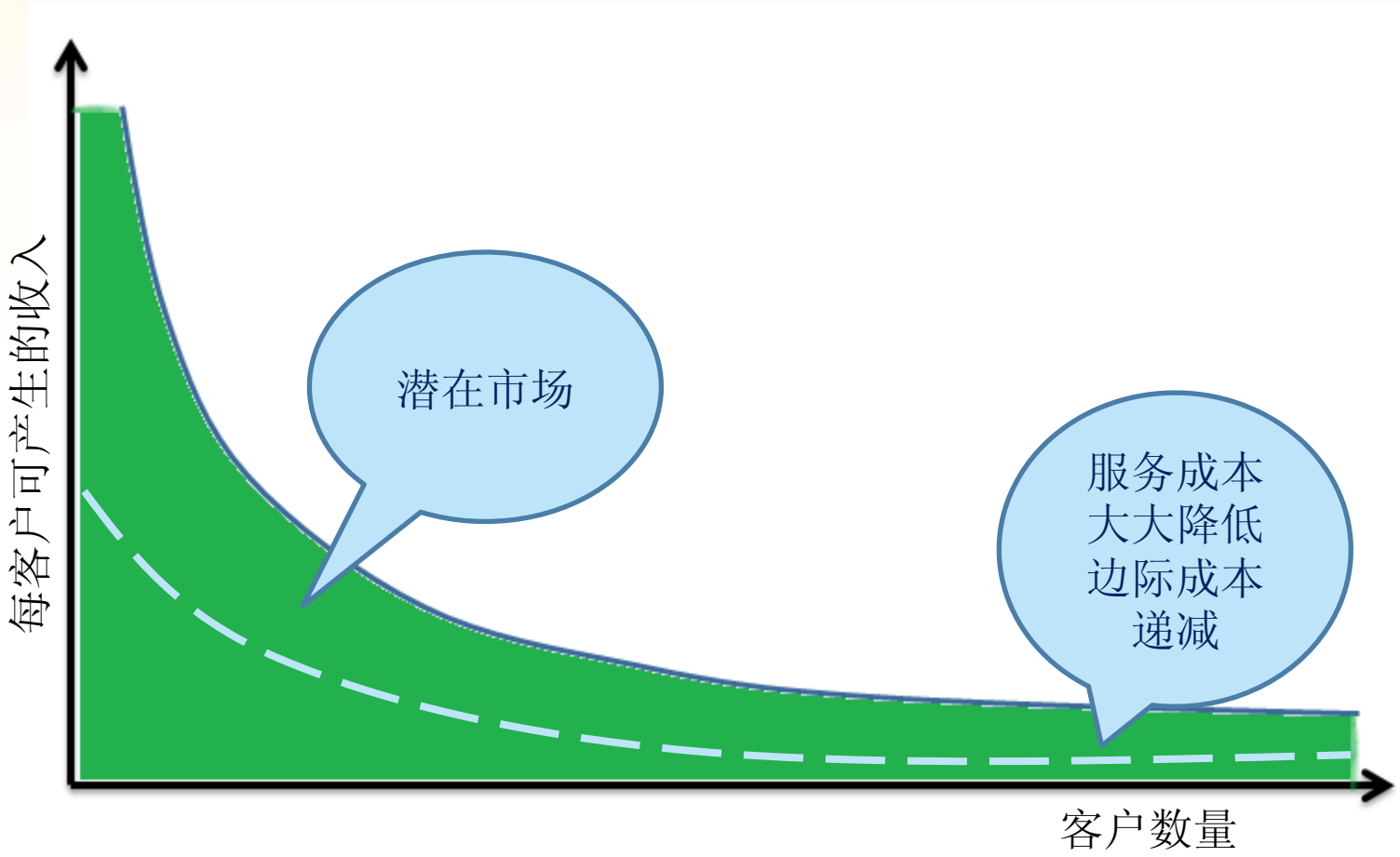
- 投资
  - 将一次性支出转化为分阶段支出；将资本性支出转化为运营性支出
- 灵活性
  - 在不确定的经济环境下，即时按需使用需要的保护
- 管理和使用
  - 不需要专职IT管理人员；在任何地方均可受到安全防护
- 升级和维护
  - 升级和维护大部分在服务商一侧进行

The Cloud Changing the Business Ecosystem (KPMG，2011)

利用云实现风险到机会的转变——从集成商和服务商角度分析



利用云实现风险到机会的转变——安全市场的长尾

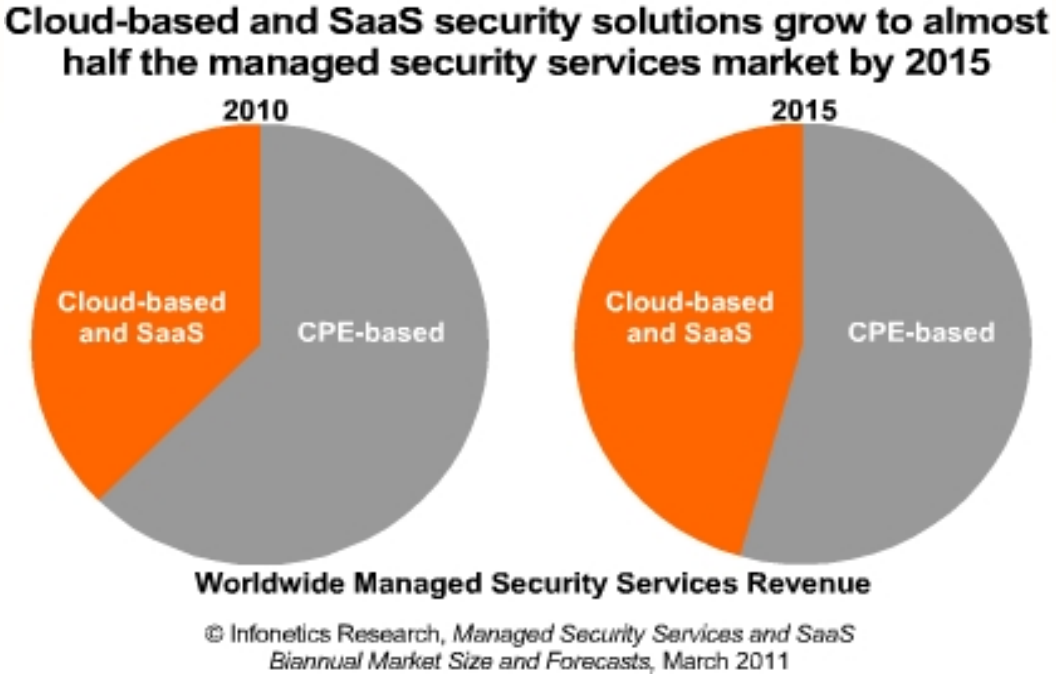


云安全概念的误区

- 云安全服务（Security as a Service, Security from the cloud ）
  - 如何利用云计算技术给用户提供安全服务
- 云计算安全（Cloud Computing Security, Security for the cloud）
  - 如何保护云计算环境本身的安全性
- 云安全智能（Cloud Security Intelligence, Security in the cloud）
  - 如何利用云的技术增强安全防护的技术能力

SaaS云安全服务市场规模

- Infonetics Research预计基于SaaS的云安全服务的市场到2015年达80亿美元，CAGR达23%。
- 基于SaaS的云安全服务在北美和欧洲目前已经广为接受，但是在全球其他地区有更大的增长潜力。



SaaS云安全服务市场规模

- 2015年，25%的企业会采用SaaS模式进行电子邮件和Web保护。（Gartner，2010）
- 在欧洲的各类企业中，采用SaaS模式进行电子邮件保护的已经达到了33.18%
  （MXIntelligence.net, 2012）

SaaS安全服务的类型

Domain	Types of services	market penetration
Security event monitoring	• Log monitoring, event correlation, and analysis • DDoS protection	15%–20%
Managed endpoints	• Managed desktop antimalware • Managed desktop data security • Managed desktop change/configuration control • Managed server HIDS • Managed server change/configuration control	10%–15%
Log management	• Log collection, retention, integrity/chain of custody, access/review auditing, and reporting	5%–10%
Threat intelligence	• Threat/malware/vulnerability intelligence and alert services • Internal and external vulnerability scans • Patching, upgrades, configuration enforcement, and change control	15%–20%
Vulnerability management	• Internal and external vulnerability scans • Patching, upgrades, configuration enforcement, and change control	10%–15%
Application security services	• Application penetration testing and vulnerability scans • Code analysis and review • Managed application firewalls	5%–10%
Incident response services	• Incident planning and response • Forensics and investigations	0%–5%
Content security	• Email monitoring and filtering • Email encryption • Email archiving • Web monitoring and filtering	25%–30%
Policy/compliance	• Regulatory compliance assessments • Policy compliance assessments • Third-party assessments • Security benchmarking	15%–20%
Managed devices (i.e., hosted and managed CPE security devices not just the logs of those devices)	• Managed/hosted network perimeter services • Managed/hosted application firewalls • Managed/hosted SIEM	10%–15%
Identity and access management	• Access administration • Two-factor authN • Federation	5%–10%

Forrester, 2010

第三部分：云安全服务实践

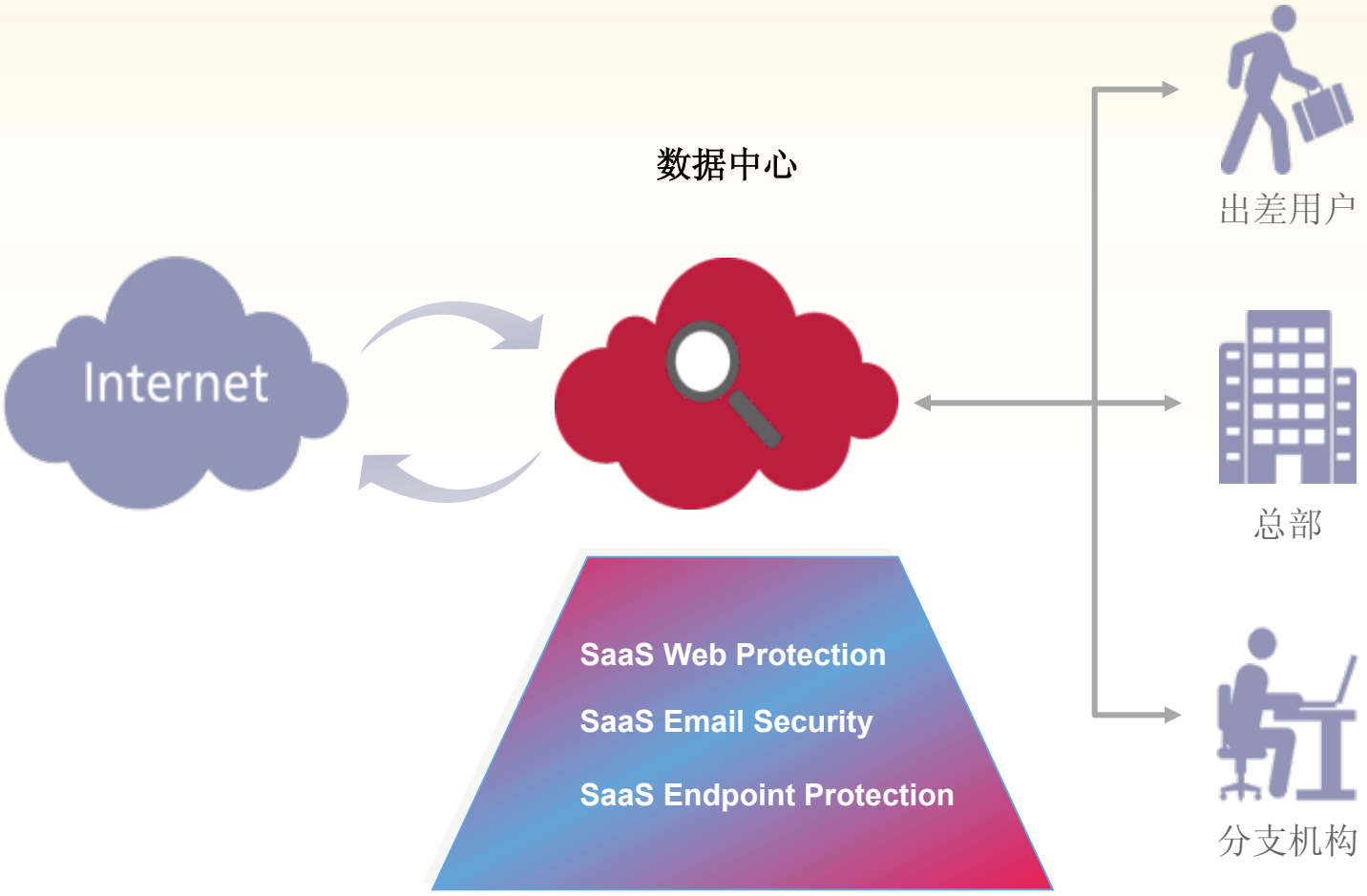
RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

专题会议主题：

专题会议分类：

云安全服务的平台和实现概要：以SaaS服务为例

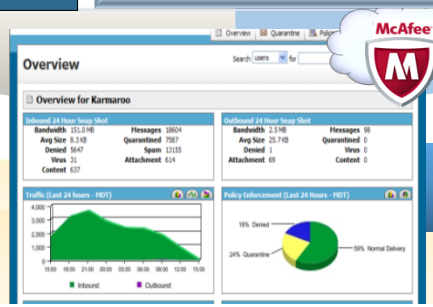
云安全服务的平台和实现概要：以SaaS服务为例



云安全服务的平台和实现概要：以SaaS服务为例

RSA CONFERENCE CHINA 2012

电子邮件保护	• 在云端实现对垃圾邮件、病毒和钓鱼邮件的过滤，减轻本地负担 • 外发邮件数据保护 • 当邮件服务器宕机时，提供最多至5天的邮件缓存
邮件持续性保护	• 提供邮件宕机保护服务，最多可以提供60天的邮件存储 • 基于Web的邮件访问 • 邮件服务器恢复后，实现智能的邮件同步
邮件加密和归档	• 保护机密的信息资产 • 双向的机密，支持移动设备 • 将邮件在云端归档和索引
端点计算机安全	• **防病毒和间谍软件** • **防火墙** • **上网安全保护** • **统一策略和报表**
http:// 上网安全保护	• 防止恶意代码感染PC • 提高网络利用率 • 限制访问包含不适当内容的站点



基于云的技术

McAfee
An Intel Company

RSA信息安全大会2012

云安全服务实践
——邮件云安全服务：某软件企业

RSA CONFERENCE CHINA 2012

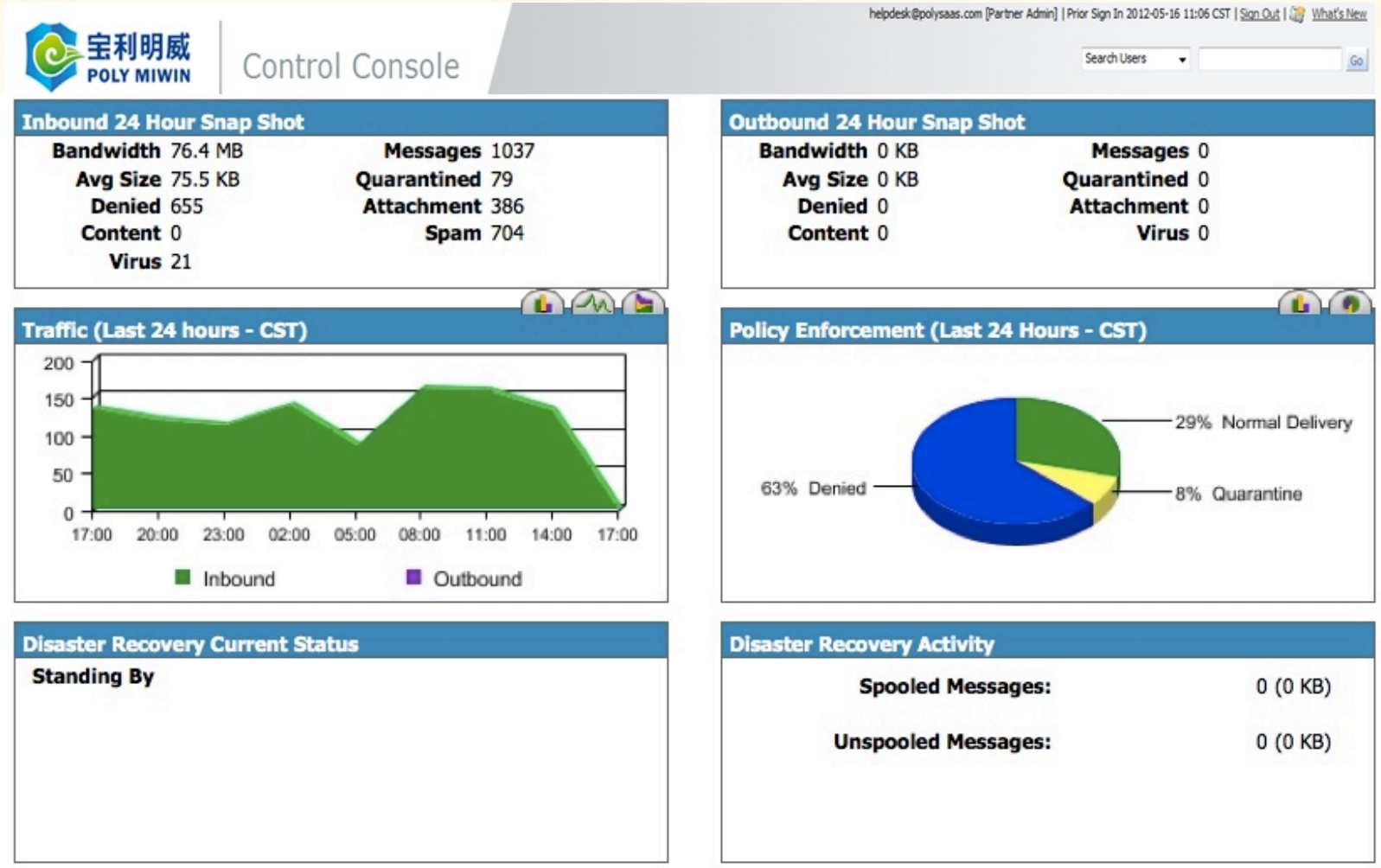
- 挑战
  - 尽管企业邮箱已经有一层过滤，但垃圾邮件和病毒邮件比例依然很高
  - 传统网关成本难以承受
  - 缺少有经验的网络管理员
- 采用邮件云安全的优势
  - 经济性：转换固定成本为运行成本，节省投资达80%
  - 易用性：易于部署，零硬件，零维护
  - 功能性：不仅能够完全替代硬件网关，还增加了邮件服务器宕机保护功能以及邮件归档功能

McAfee An Intel Company

宝利明威 POLY MIWIN

云安全服务实践
——邮件云安全服务：某软件企业

RSA CONFERENCE CHINA 2012



McAfee
An Intel Company

宝利明威
POLY MIWIN

云安全服务实践
——端点云安全服务：锐力体育

RSA CONFERENCE CHINA 2012

- 背景:
  - 上海锐力健身装备有限公司(以下简称“锐力体育”) 是Nike、Adidas的中国区总代，在全国有600多家店面，店面分布很广。
- 挑战
  - 许久以来，和其它连锁零售行业类似，锐力在安全软件的选型上陷入困境：动辄几百数千的门店，带来的是安全软件的部署、监控、管理的极为不便。无奈下，很多地方选择了个人版杀毒软件甚至让PC完全“裸奔”，整个公司陷入巨大的安全隐患之中。
- 锐力体育所有门店都已经完成了希望云安全杀毒软件的部署。

锐力体育全国系统部高级总监王歆：”希望云安全解决了长期困扰我的安全问题。”

云安全服务实践
——端点云安全服务：锐力体育

RSA CONFERENCE CHINA 2012

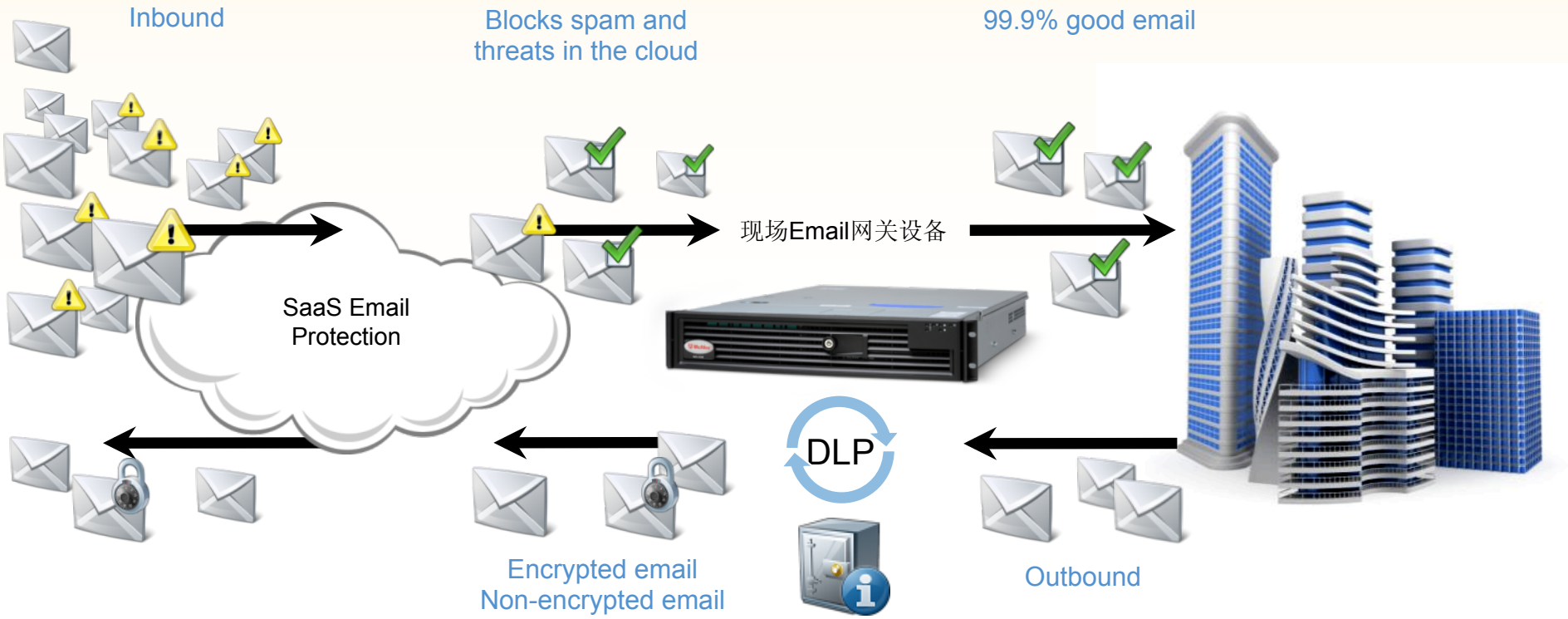
	部署传统企业版杀毒软件	部署希望云安全
所需条件	需在门店与总部之间搭建或租借VPN、DDN专线	独有的‘云’技术实现跨网管理
	购买防病毒服务器系统（硬件+操作系统+数据库）	部署免服务器
	购买防病毒软件授权	国内第一款完全免费的企业版杀毒软件
部署成本	昂贵	0

SaaS不仅仅只适用于中小型企业

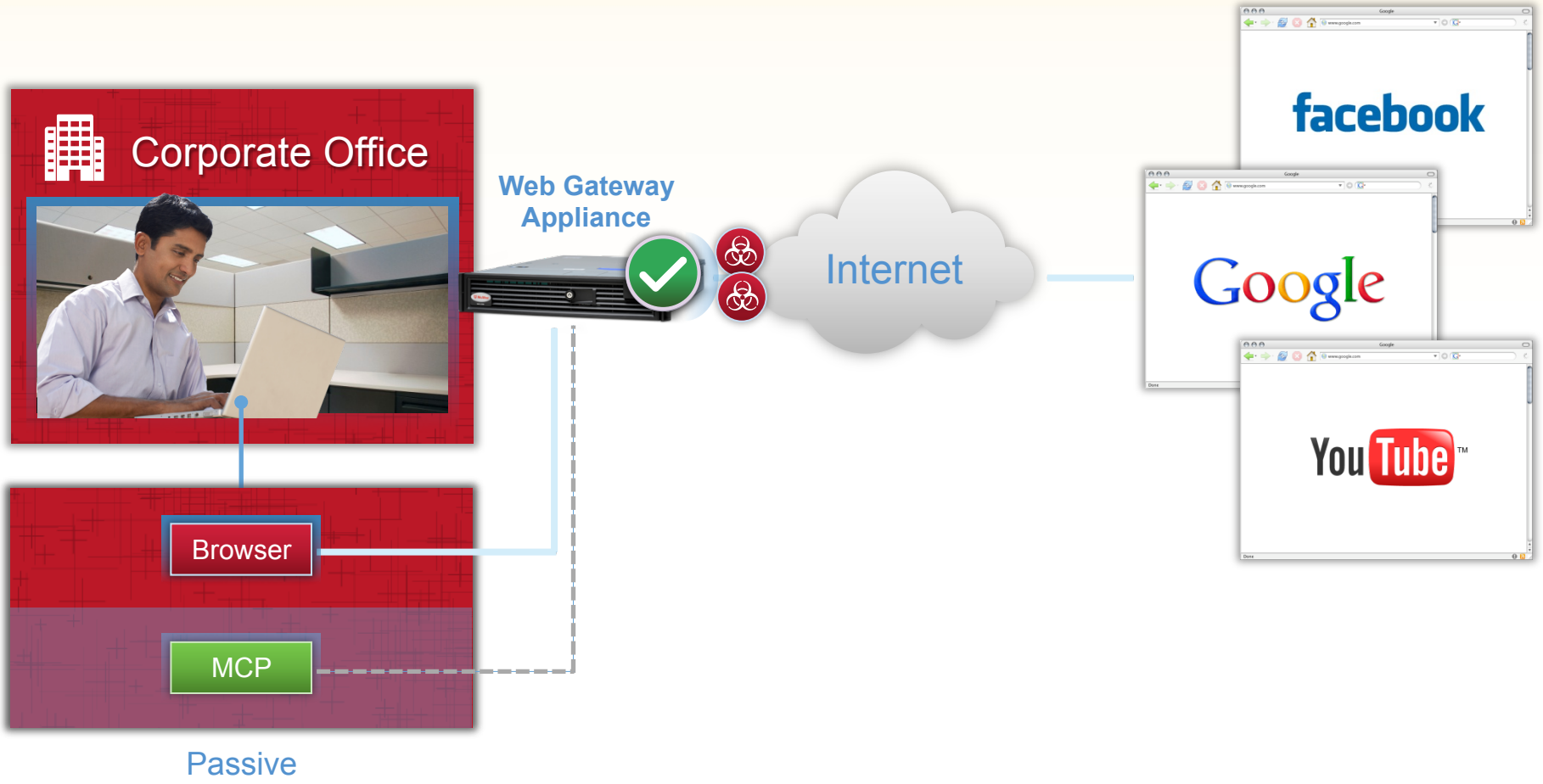
- 在北美，25%的企业已经在采用基于SaaS和传统设备模式结合的混合模式进行邮件安全防护。在超过一万人规模的企业中，这个比例达到了38%（IDC, 2010）
- 驱动因素：
  - 把事情交给最专业的人做：inbound 和Outbound
  - 更加灵活方便的安全架构：多分支机构；出差员工；隔离威胁
  - 更加全面的保护
  - 成本节约、绿色IT

利用SaaS优化安全架构：Lulzsec的故事

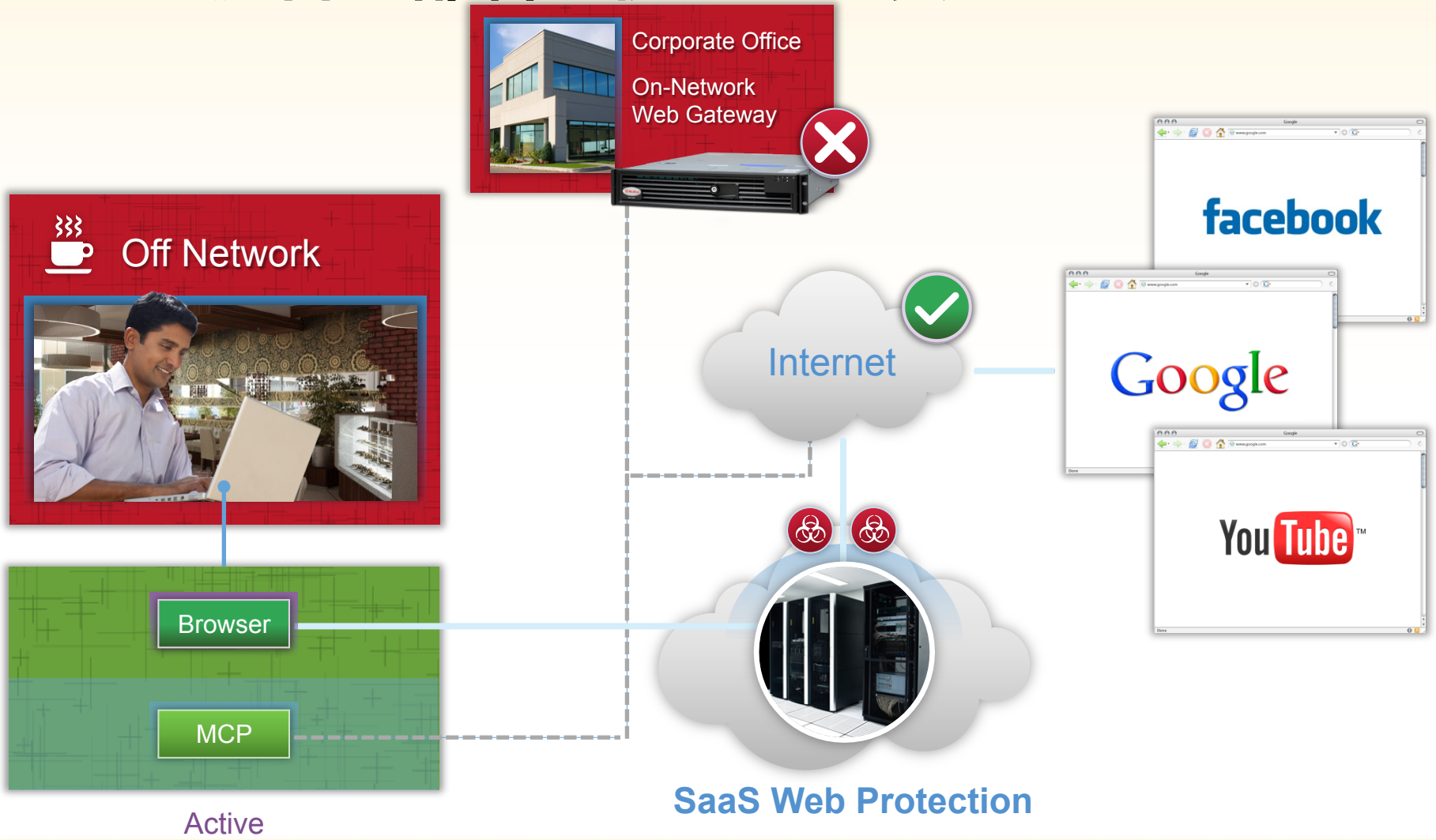
利用SaaS优化企业的安全架构 —— 混合型部署示例：邮件安全



利用SaaS优化企业的安全架构 —— 混合型部署示例：Web安全



利用SaaS优化企业的安全架构 —— 混合型部署示例：Web安全



电信运营商运营SaaS云安全服务案例——AT&T

With McAfee since 2004

- 主要目标
  - 提供多种服务的一站式服务合作伙伴
  - 支持复杂的、多样化的增值服务市场策略
- 目标客户
  - 中小企业、大型企业、政府、国际化市场
- 合作内容和模式
  - 邮件安全保护、邮件加密、邮件持续性、邮件归档
  - OEM模式

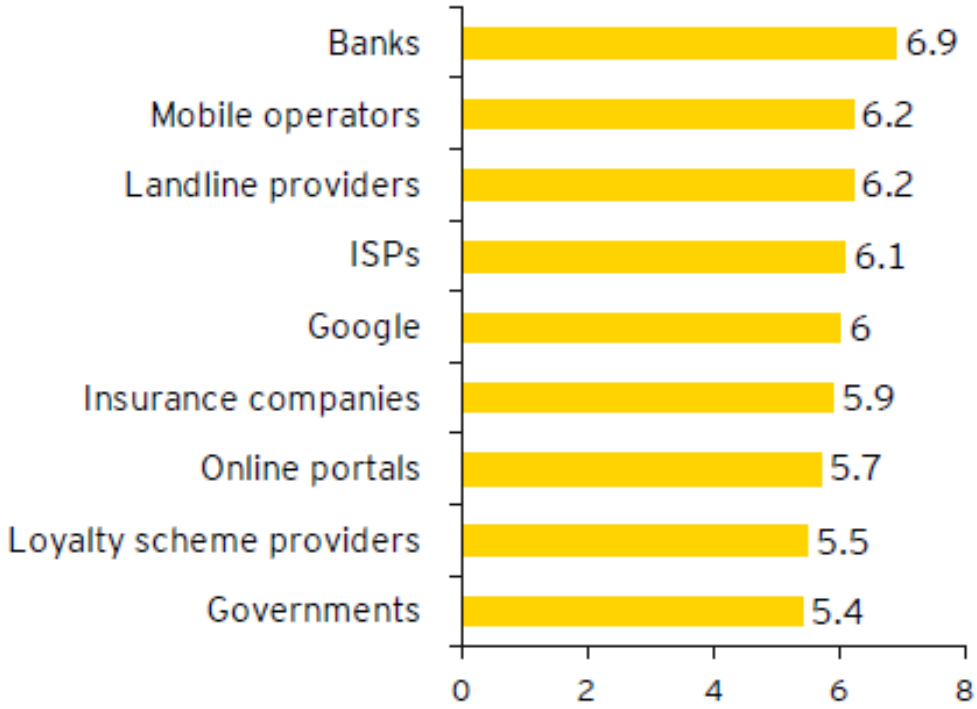
电信运营商具有提供安全服务的先天优势

- 电信运营商将通过进一步提供安全服务来为现有的电信基础架构服务提供进一步的增值。
- 电信运营商将改变安全服务市场的成本体系：
  - 基于现有庞大的客户群可以实现规模经济效应；
  - 基于网络的云计算基础架构投入已经提供了多租户、低成本的选择。
- 运营商掌控了客户的管道，并且充分的带宽资源是提供SaaS服务的先决条件之一。

—— Forrester, 2010.3

信任：云安全服务推进的关键问题

- 您认为能否信任下面的机构对数据保护和隐私性的保护？



源于：Nokia Siemens Networks Privacy Study 2009, sample of 9,200 mobile phone users between the ages of 16 and 65 from 14 countries including Germany, China, US, Argentina

第四部分：全球威胁智能感知——安全的方向

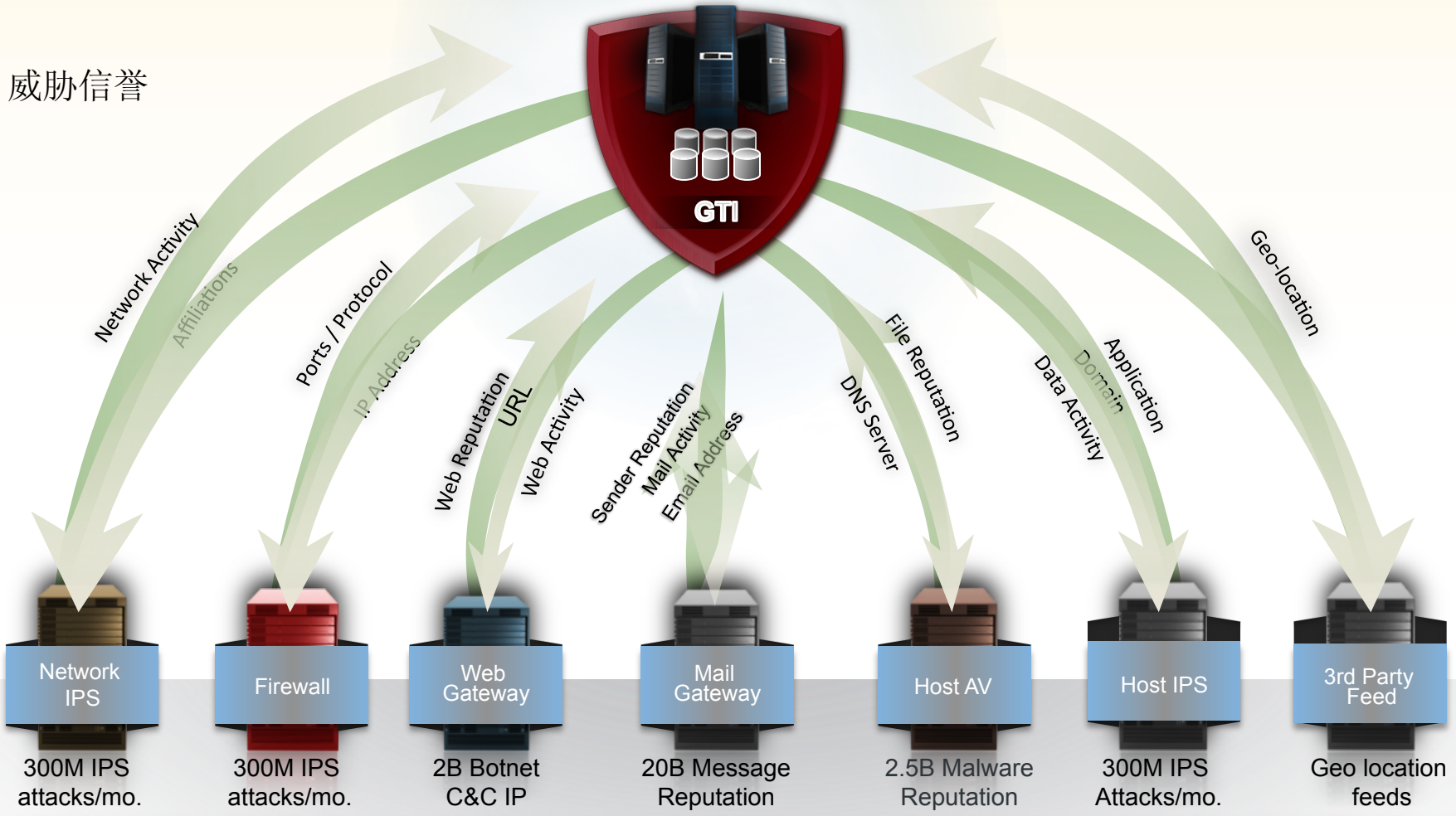
RSA CONFERENCE CHINA 2012
RSA信息安全大会2012

专题会议主题：

专题会议分类：

全球威胁智能感知——安全的方向

威胁信誉



McAfee An Intel Company

参考文献

- 云安全概念的误区
  - http://qing.weibo.com/mcafeezhenglin
- “十二五”中小企业成长规划
  - 工业与信息化产业部
- 中国中小企业互联网应用调查报告
  - CNNIC, 2011
- Hybrid Messaging Security Solutions: Enhanced Security and Business Flexibility
  - IDC, Feb. 2010
- Surviving Lulz: Behind the Scenes of LulzSec
  - Matthew Prince , RSA Conference 2012, San Francisco

谢谢

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012