Cisco Security Product training

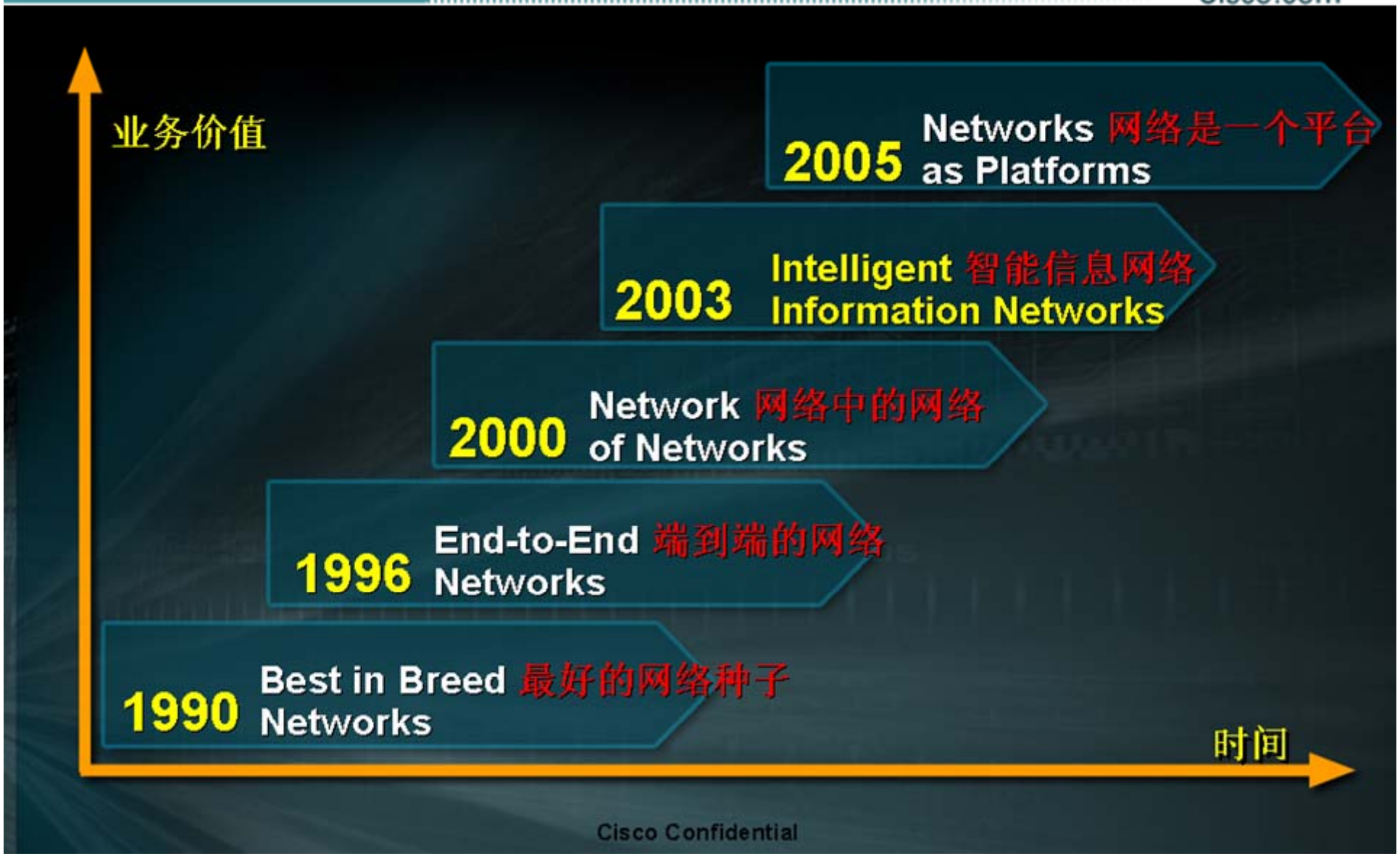
© 2003 Cisco Systems, Inc. All rights reserved.

目录

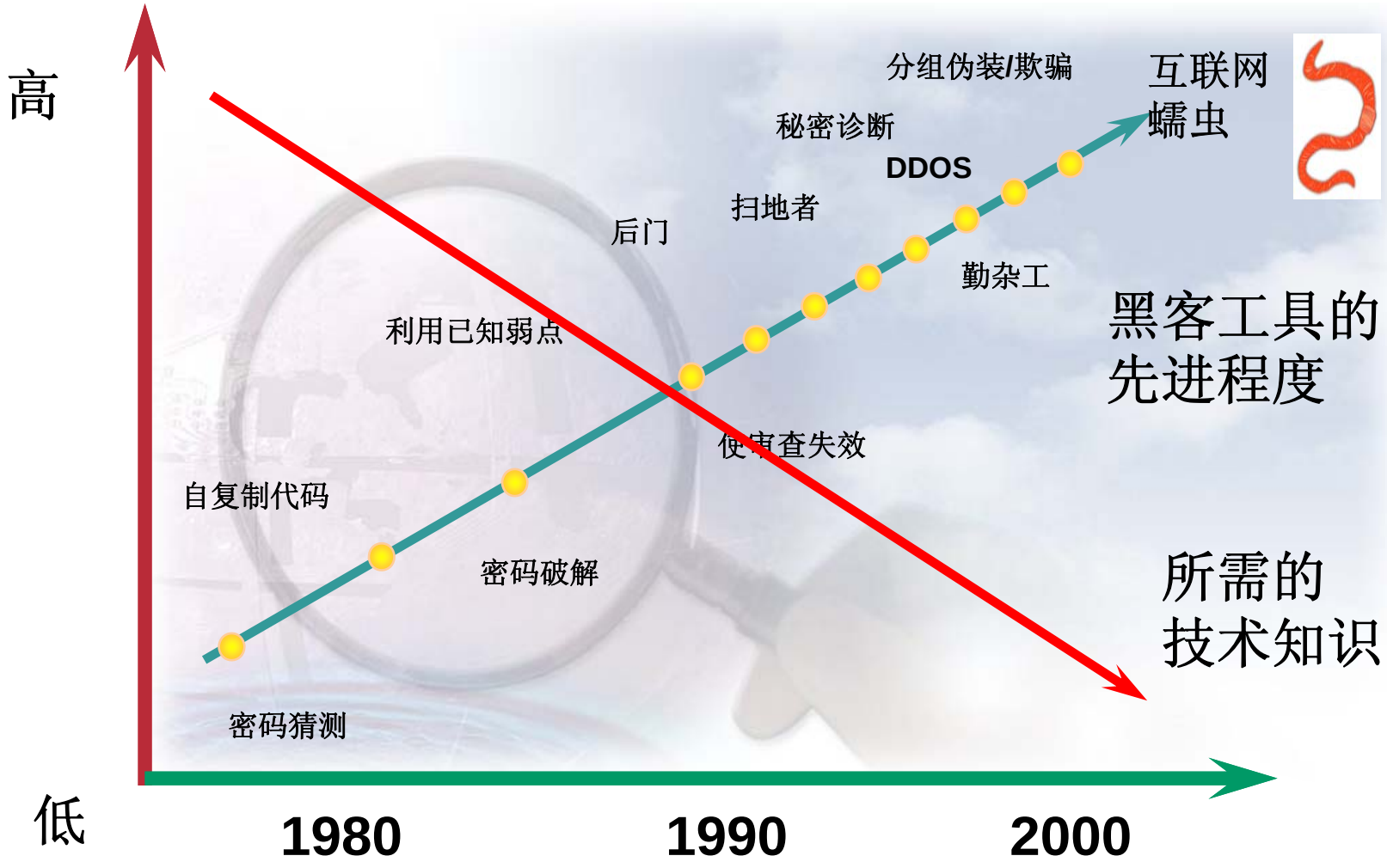
- 为什么网络需要安全
- 为什么选择思科的安全解决方案
- 受访者通常关心的问题
- 我们希望从受访者得到哪些信息

© 2003 Cisco Systems, Inc. All rights reserved.

所有的一切运行在和所有的一切包含在网络中
Everything On AND Everything In



蠕虫病毒的威胁能力：更危险，更易于使用



© 2003 Cisco Systems, Inc. All rights reserved.

当今信息安全的变化

Slammer蠕虫成为新的里程碑－对传统安全技术的震撼

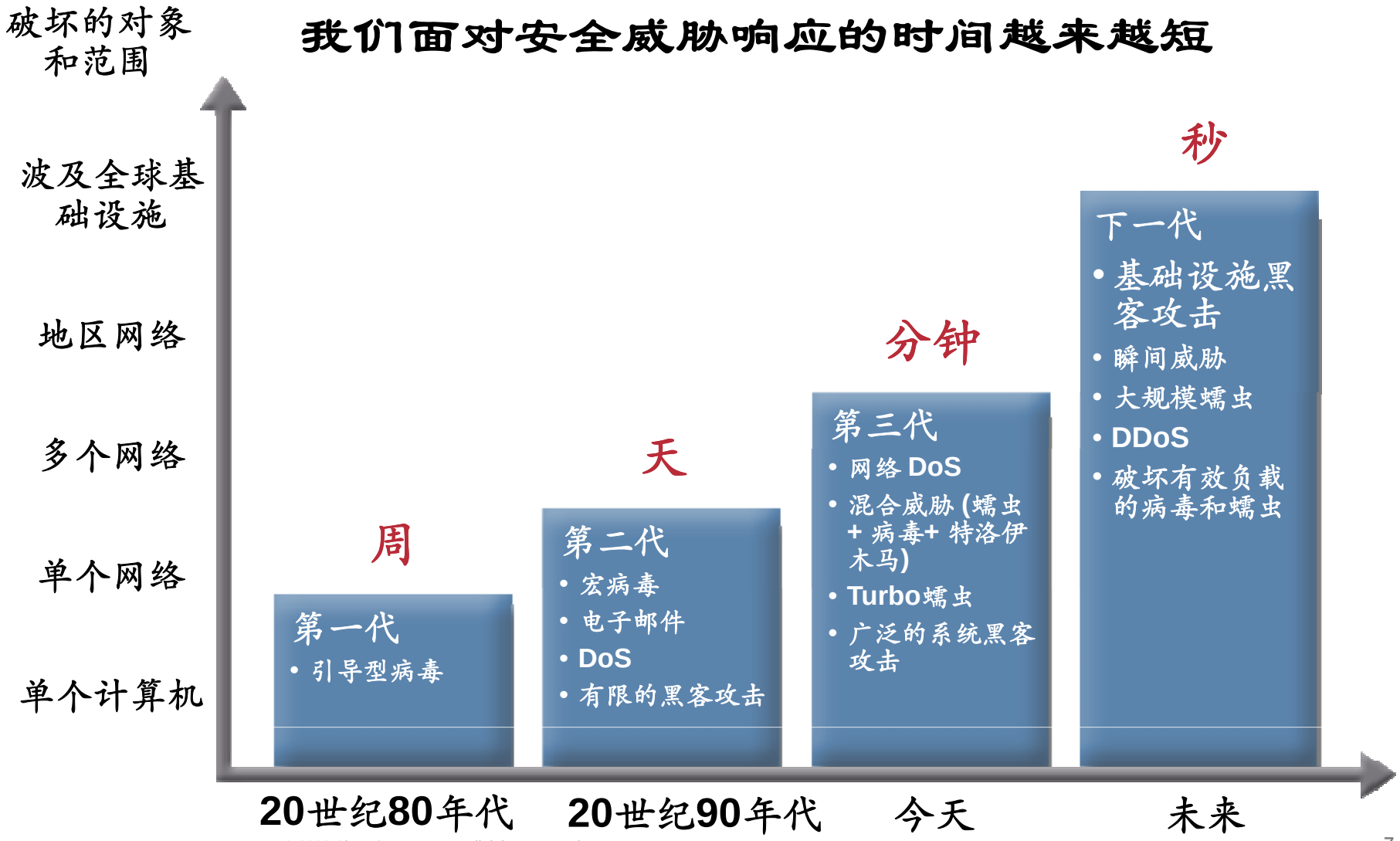
著名的互联网蠕虫事件

病毒名称	产生时间	造成损失
莫里斯蠕虫	1988年	6000多台计算机停机，直接经济损失达9600万美元!
美丽杀手	1999年	政府部门和一些大公司紧急关闭了网络服务器，经济损失超过12亿美元!
爱虫病毒	2000年5月	众多用户电脑被感染，损失超过100亿美元以上
红色代码	2001年7月	网络瘫痪，直接经济损失超过26亿美元
求职信	2001年12月	大量病毒邮件堵塞服务器，损失达数百亿美元
Sql蠕虫王	2003年1月	网络大面积瘫痪，银行自动提款机运做中断，直接经济损失超过26亿美元

© 2003 Cisco Systems, Inc. All rights reserved.

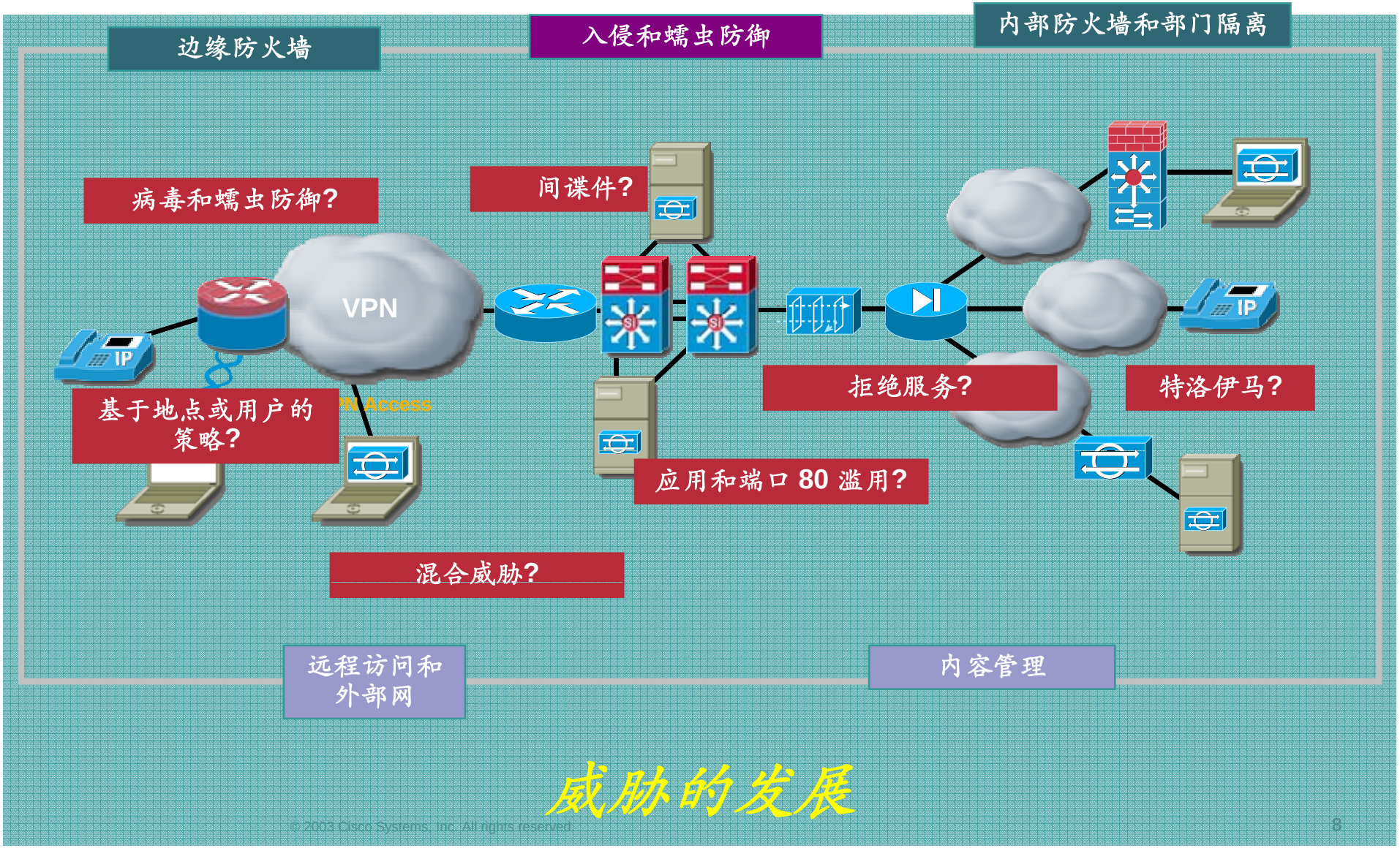
当今网络攻击的特征及变化

我们面对安全威胁响应的时间越来越短



© 2003 Cisco Systems, Inc. All rights reserved.

其他新的安全挑战



威胁的发展

© 2003 Cisco Systems, Inc. All rights reserved.

安全网络的新定义

- 没有100%的安全，威胁永远存在，关键在于采取的措施
- 安全的网络是：威胁出现，及时发现，及时响应，在网络失控之前，采用各种有效手段将安全威胁控制在可控范围内

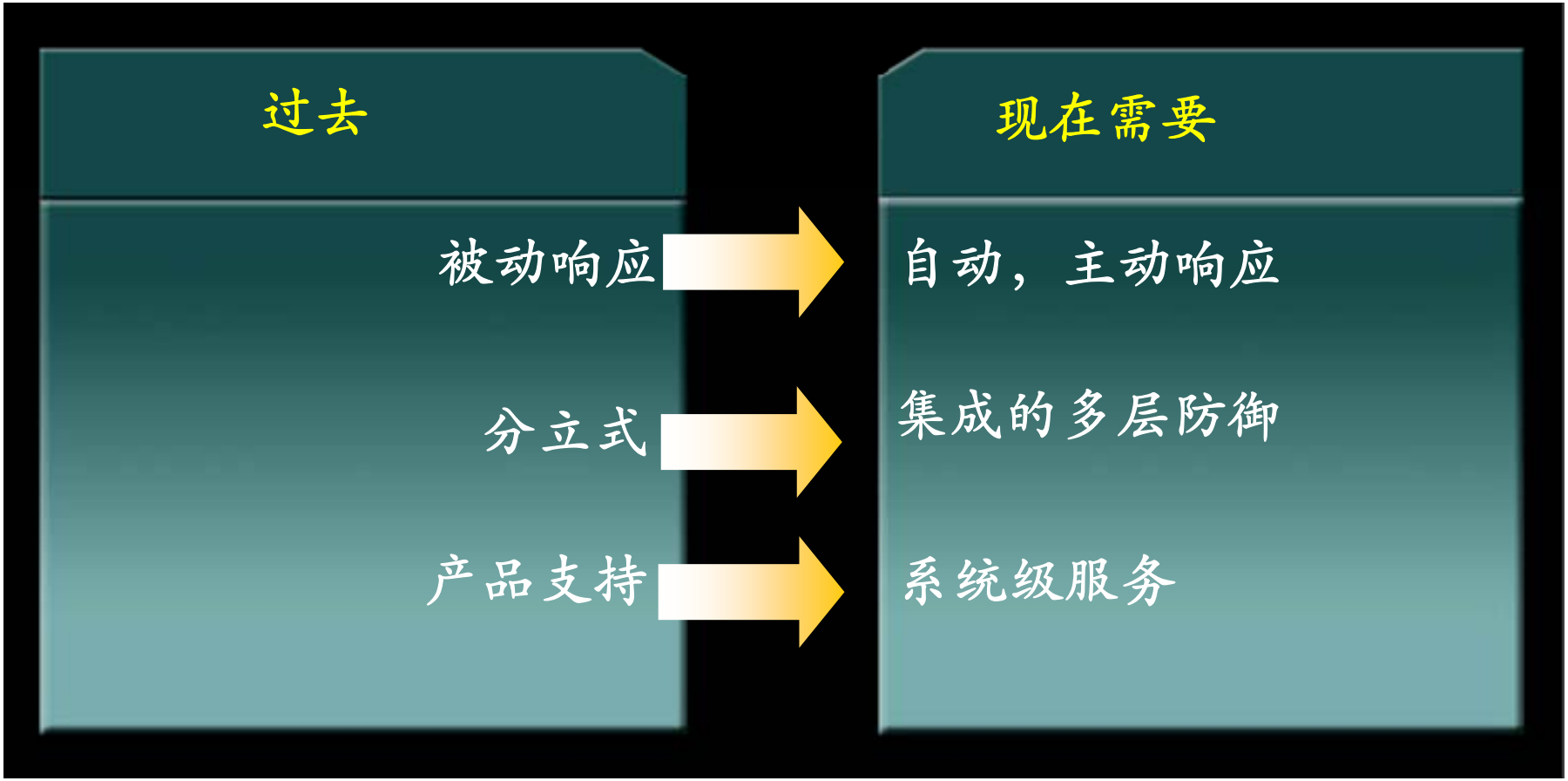
© 2003 Cisco Systems, Inc. All rights reserved.

目录

- 为什么网络需要安全
- 为什么选择思科的安全解决方案
- 受访者通常关心的问题
- 我们希望从受访者得到哪些信息

© 2003 Cisco Systems, Inc. All rights reserved.

如何应对当今网络攻击的变化



协作式的系统方法，自我防御系统

© 2003 Cisco Systems, Inc. All rights reserved.

思科安全战略的演进

可信网络
自防御网络
• 完全可信赖
• 可追溯的网络
• 安全预知
• 主动防御
• 自我恢复
• 快速响应
• 智能管理
集成化安全
• 集成化安全
路由器
交换机
装置
终端
• 防火墙 + VPN + IDS
• 集成化管理软件
• 改进的高级服务
全面集成的安全方案
深度防护
• 多种技术
• 多个位置
• 多种设备
• 没有或很少集成
单点的产品
• 安全装置
• 增强的路由器安全
• 单独的管理软件
基本的安全
• 基本的路由器安全
• 命令行界面
1990s
2000
2002
2003
2004…
将来…

思科自防御网络战略(Cisco Defending Network)

© 2003 Cisco Systems, Inc. All rights reserved.

思科SDN的发展

SDN 第三阶段 “自适应威胁防御”

- 安全服务和网络智能间相互了解和配合
- 提高安全服务有效性，实现主动响应
- 整合服务，提高运营效率
- 应用识别和检测，用于安全应用的供应/优化

SDN 第二阶段 “协作式安全系统”

- 安全成为网络级系统：终端 + 网络 + 策略
- 多项服务和设备协作，以有效管理抵御攻击
- NAC, IBNS, SWAN

SDN 第一阶段 “集成化安全”

- 使每个网络组件成为一个防御点
  路由器，交换机，设施，终端
- 安全连接 (V3PN, DMVPN), 威胁防御, 信任和身份识别
- 网络平台保护

© 2003 Cisco Systems, Inc. All rights reserved.

自适应威胁防御的运作流程

访问控制，分组检测

应用智能，内容检测，病毒防御

身份识别，虚拟化，QoS 划分，流量可视性

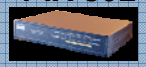
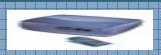
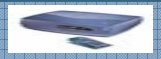
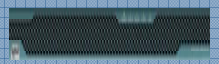
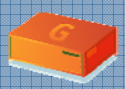
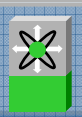
应用检测，使用实施，
Web控制
应用安全

恶意件/内容防御，异常检测
Anti-X防御

流量/接入控制，主动响应
抑制和控制

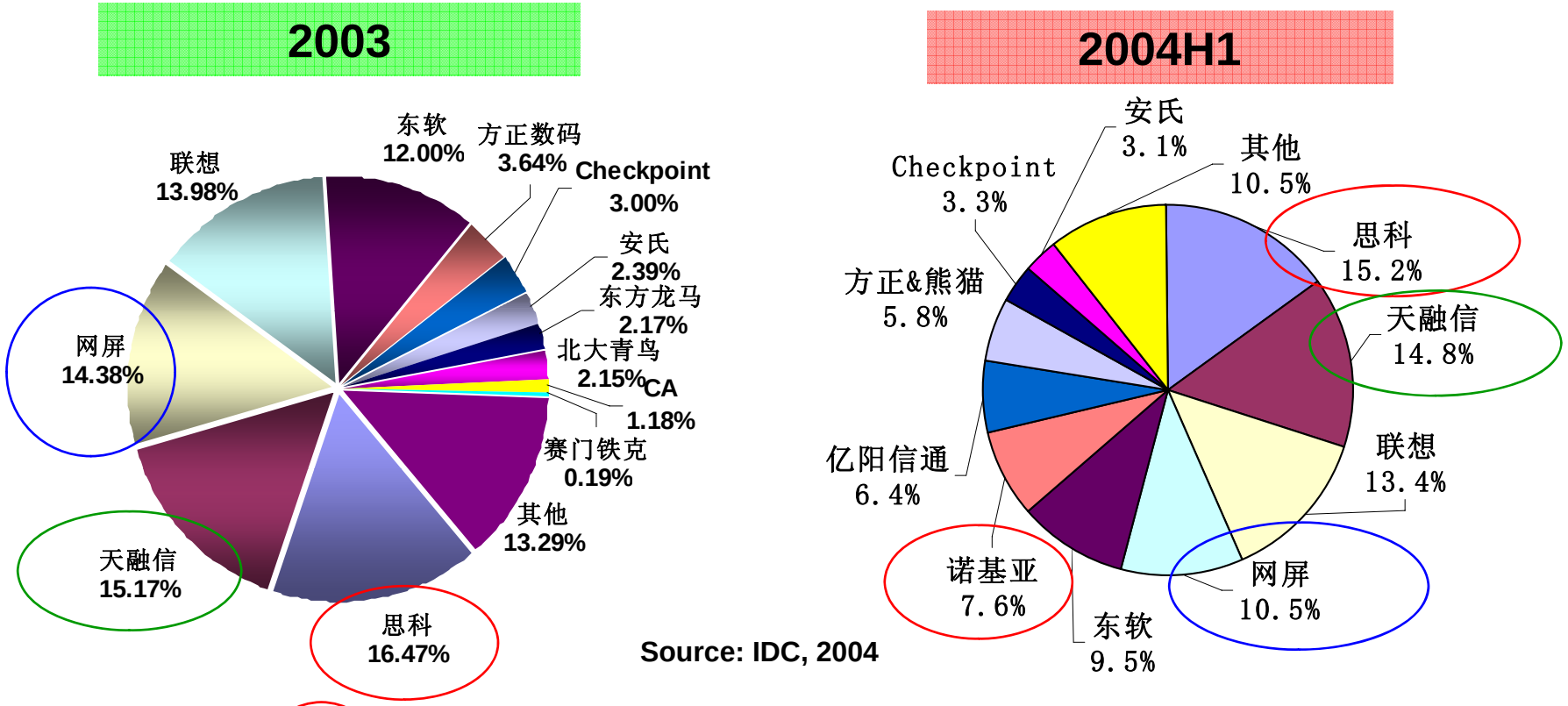
© 2003 Cisco Systems, Inc. All rights reserved.

思科自防御安全产品系列

思科防火墙系列	PIX 501  PIX 506E PIX 515E PIX 525 PIX 535 NP结构高端防火墙 800 1800  2800  3800 3700 7xxx
思科VPN系列	800 1800 2800 3800 3700 7xxx CAT6K ASA 5500
思科IDS/IPS安全入侵检测防护	CAT6K入侵检测 网络入侵检测 IOS 入侵防护 防火墙入侵检测 CSA入侵防护  ASA 5500
思科安全管理体系	ISC安全业务管理 VMS安全设备管理 CSA主机安全防护管理 ACS安全身份认证及审计 CWSIM安全信心管理 Protego安全威胁消除
专业的安全防护	 专业预防DDoS攻击技术 业务控制网关  网络存储安全保护技术
网络业务安全	数据平面安全 管理平面安全 业务平面安全 控制平面安全 基础网络安全最佳实践
安全顾问服务	SPA安全状态评估 SNR安全网络优化设计

© 2003 Cisco Sys[illegible]eserved.

防火墙/VPN市场占有率(US$M)，2004H1



Source: IDC, 2004

排名	1	2	3	4	5	6	7	8	9	10
厂商	思科	天融信	联想	网屏	东软	诺基亚	亿阳信通	方正&熊猫	Checkpoin	安氏
规模	7.4	7.2	6.5	5.1	4.6	3.7	3.1	2.8	1.6	1.5

© 2003 Cisco Systems, Inc. All rights reserved.

在这个市场有哪些主要竞争对手？

- **Netscreen**
- **Check Point**
- **Fortinet**
- **TopSec (**天融信）
- **DC (**联想）
- 亿洋信通

© 2003 Cisco Systems, Inc. All rights reserved.

小结：

- 思科是业界唯一一个有完整安全解决理念和解决方案的公司；
- 思科是唯一一个能提供全线产品的公司；
- 思科在国际、国内安全市场的占有率第一；
- 国内的公司也开始提出了类似于**SDN**的解决理念，但是明显是在追随或**COPY Cisco SDN**的理念；

© 2003 Cisco Systems, Inc. All rights reserved.

目录

- 为什么网络需要安全
- 为什么选择思科的安全解决方案
- 受访者通常关心的问题
- 我们希望从受访者得到哪些信息

© 2003 Cisco Systems, Inc. All rights reserved.

哪儿可以得到相关资料？

Cisco.com

- 思科网站

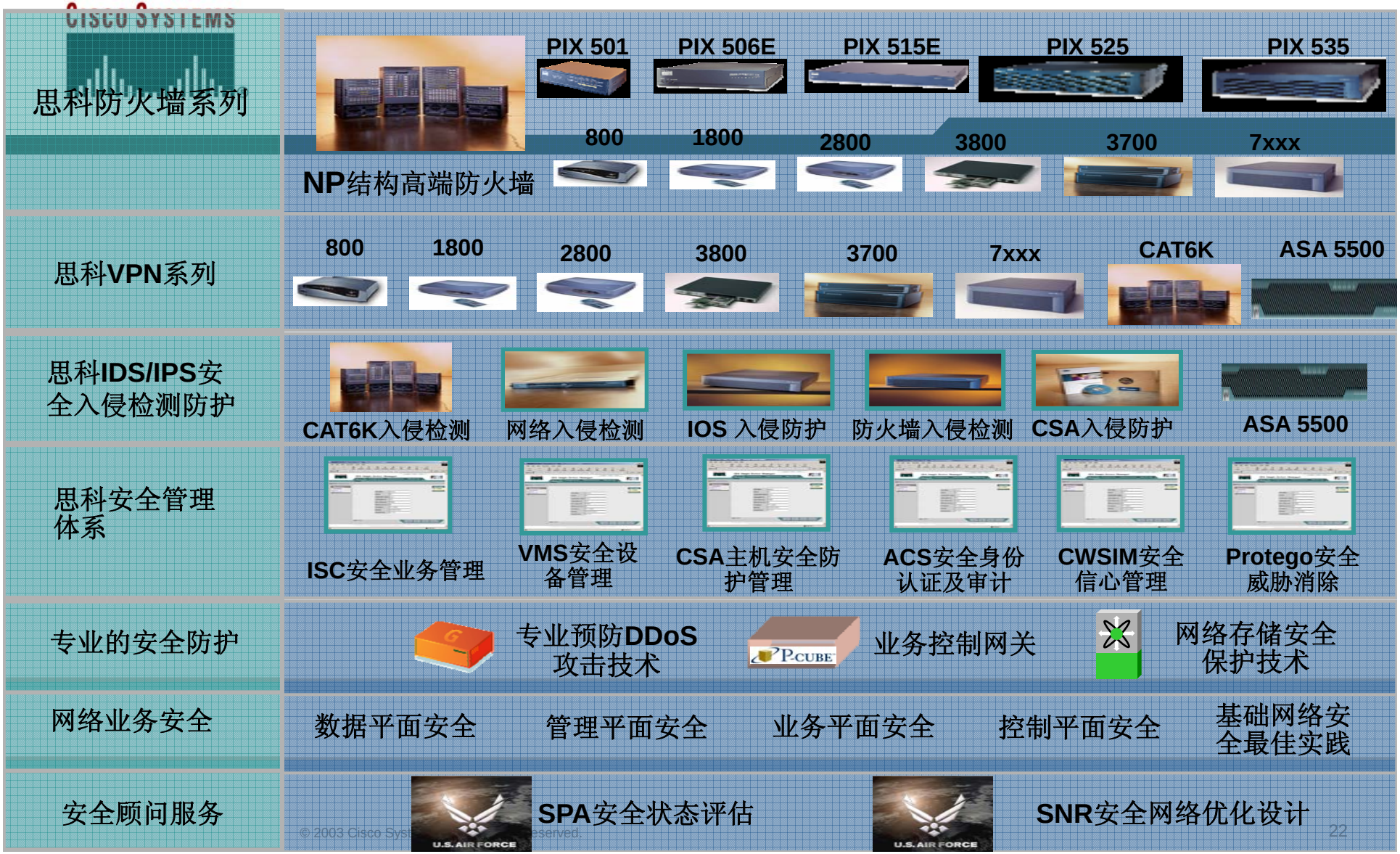
http://www.cisco.com/security/ （英文网站）

http://www.cisco.com/cn/power/security/ （中文网站）

- 思科销售人员（行业和区域）
- 思科代理商

© 2003 Cisco Systems, Inc. All rights reserved.

思科有哪些安全产品?



© 2003 Cisco Sys[illegible]eserved.

受访者问题：价格怎么样？

- 思科有用众多产品，从高端一直到中低端。有固定配置的，也有模块化配置的，所以价格是根据所要选择的产品和产品的配置而变化的；
- 对于安全产品不能只看单独的产品或者价格，重要的是看是否能提供整体解决方案。只有安全产品相互配合才能实现“自动响应、多层防御、系统级服务”。现在不能“头痛医头，脚痛医脚”
- 告诫客户：关键的业务都开始或已经转移到网络上。安全不再是可有可无的。任何一个安全问题都可造成业务的停顿，财务上的损失；

© 2003 Cisco Systems, Inc. All rights reserved.

受访者问题：如果我已有其他家的安全产品该怎么办？

- 先要确定客户已有什么安全产品？防火墙？**IDS?**
- 如果用户只把防火墙、**IDS**部署在网络边缘。可建议他们按照**SDN**第一阶段开始实施网络安全，在重要的地方部署防火墙、**IDS/IPS**，在路由器和交换机上实施安全特性；
- 如果他们在网络各处部署了防火墙、**IDS/IPS**，则建议用户开始考虑**SDN**的第二阶段**----**端点安全性，使用**NAC, CSA**等提高端点安全级别的软件；
- 或者直接进入第三阶段，提高网络对入侵威胁响应能力**----**自适应威胁防御；

© 2003 Cisco Systems, Inc. All rights reserved.

受访者问题：其它技术问题？

- 资金有限，网络的哪些部分应该首先实施部署安全产品和技术？
- 安全产品和技术的实施，是不是要对已有IP网络架构进行调整？
- 思科的防火墙和IDS与其他家有什么不同？
- 有其他安全产品时候，想实现SDN，应该怎么做？

…… ……

针对上述问题如何回答：

1) 告诉受访者访问思科网站和联系思科销售人员

2) 同时强调安全问题已经和IP网络不可分割，安全已成为IP网络的基础，思科不仅是IP网络设备的领先厂商，而且也是安全技术厂商，技术上和实施经验上都高于其它厂商。也只有思科才能将路由交换技术和安全进行完美的结合

© 2003 Cisco Systems, Inc. All rights reserved.

目录

- 为什么网络需要安全
- 为什么选择思科的安全解决方案
- 受访者通常关心的问题
- 我们希望从受访者得到哪些信息

© 2003 Cisco Systems, Inc. All rights reserved.

企业背景信息

- 受访者企业来自什么行业？（跨国企业、银行、政府、运营商等）
- 受访者在企业中的角色，是否有决策权或影响决策的能力**(BDM/TDM)**
- 受访企业安全系统归什么部门管理，与网络部门的关系？
- 对关键业务部门和数据如何进行保护的，是否只靠数据库的密码？
- 企业在近几年是否有过因蠕虫病毒的传播而造成业务的停顿？
- 企业因为业务扩展是否使得网络逐渐由封闭走向开放？他们有没有考虑过开放网络的安全问题？
- 由于笔记本计算机的增多，企业的移动性开始增多，企业是否开始考虑网络内部的安全性？
- 企业现有是否部署了安全产品：采用什么品牌的系统？使用了多少年？是否有更换或扩容需求？若有，具体时间如何？预算多少？
- 企业部署安全产品从哪里开始？是只部署在中心？还是网络的各个点？

© 2003 Cisco Systems, Inc. All rights reserved.

客户分类（从对SDN了解程度而言）

- 没听说过
- 听说过，但觉得像天方夜谭
- 听说过，觉得不错，但不知道怎么实现

© 2003 Cisco Systems, Inc. All rights reserved.

客户分类（从产生Leads可能性而言）

- 是否有近期更换或购买的需求？
- 客户想在哪些地方开始部署安全产品？
- 客户是否想对蠕虫病毒进行有效地控制？
- 客户是否想对内部员工网上的活动进行控制，尤其是防止合法员工去做非法的事情

© 2003 Cisco Systems, Inc. All rights reserved.

© 2003 Cisco Systems, Inc. All rights reserved.