建立主动安全防护体系

郭训平
中国区技术部经理 赛门铁克公司

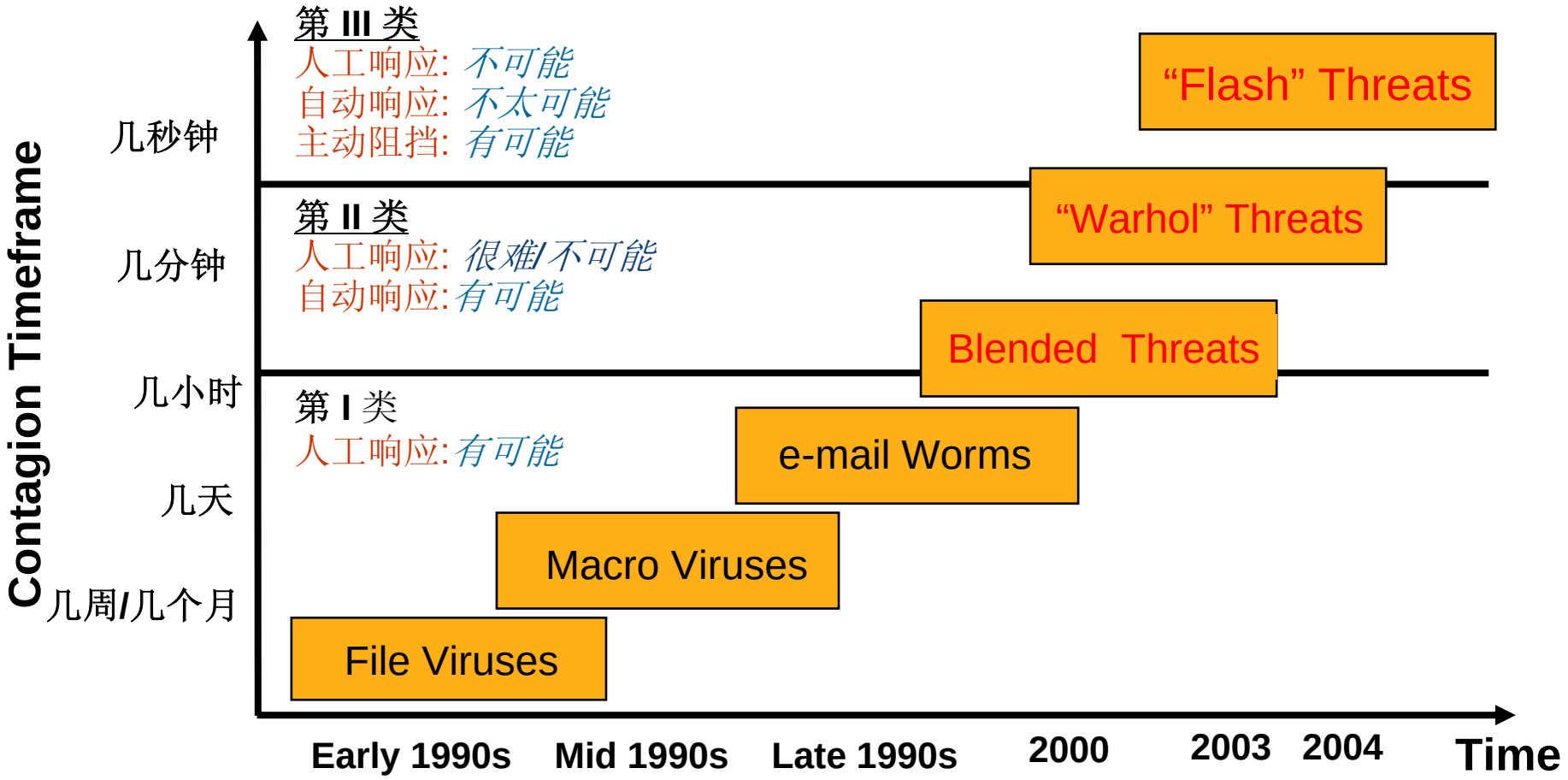
议题

1. 安全威胁分析
2. 安全建设面临的挑战
3. 两种安全响应模型
   - 反应式安全响应模型
   - 主动安全响应模型
4. 建立主动性信息安全体系
5. 总结

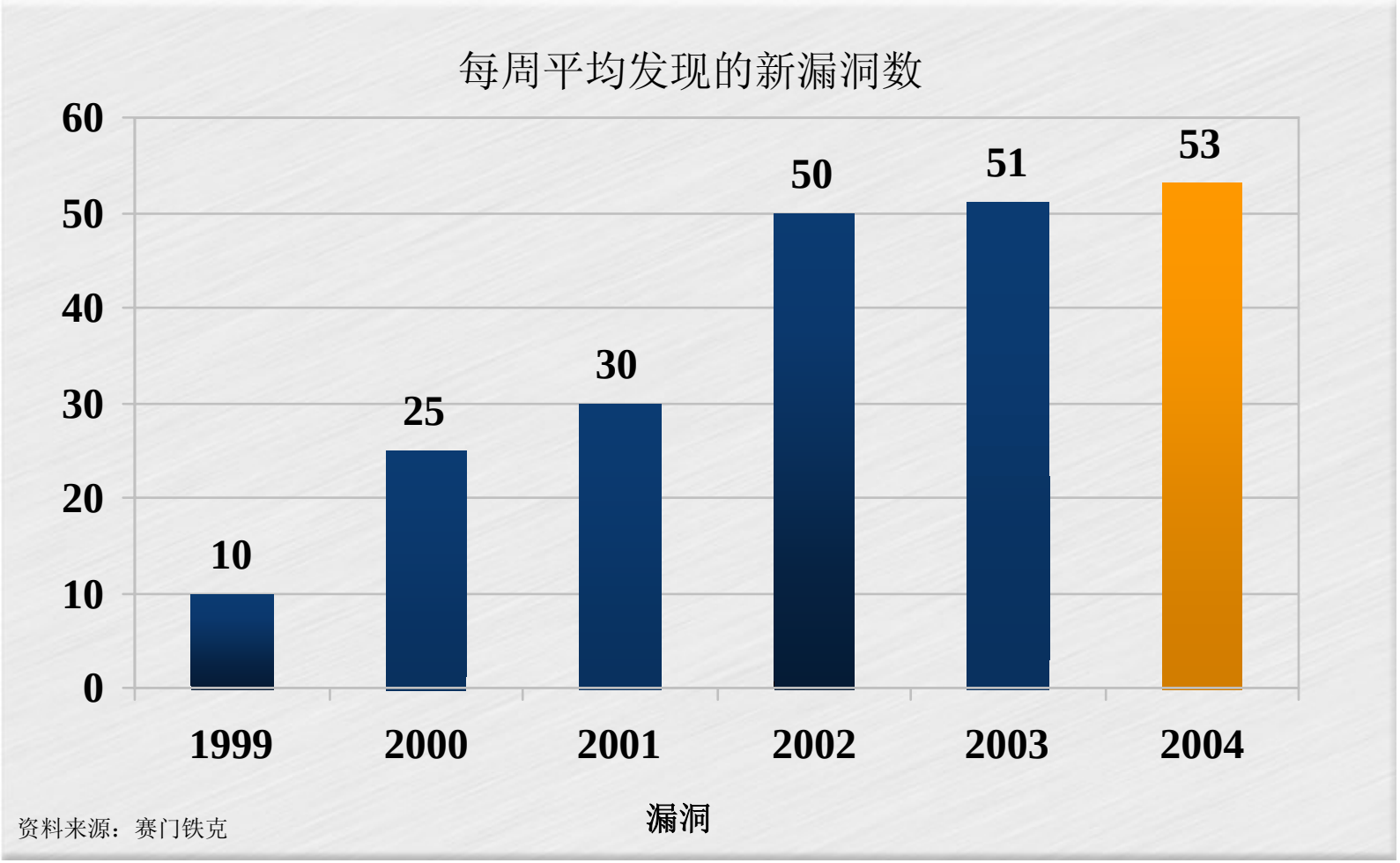
议题

1. 安全威胁分析
2. 安全建设面临的挑战
3. 两种安全响应模型
   - 反应式安全响应模型
   - 主动安全响应模型
4. 建立主动性信息安全体系
5. 总结

威胁的现状和趋势


第 III 类
人工响应: 不可能
自动响应: 不太可能
主动阻挡: 有可能
第 II 类
人工响应: 很难/不可能
自动响应: 有可能
第 I 类
人工响应: 有可能
Contagion Timeframe
几秒钟
几分钟
几小时
几天
几周/几个月
"Flash" Threats
"Warhol" Threats
Blended Threats
e-mail Worms
Macro Viruses
File Viruses
Early 1990s
Mid 1990s
Late 1990s
2000
2003
2004
Time

软件漏洞


每周平均发现的新漏洞数
60
50
40
30
20
10
0
10
25
30
50
51
53
1999
2000
2001
2002
2003
2004
漏洞
资料来源：赛门铁克

The Threat Landscape TODAY

- Zero Day Attacks.
- SpyWare/Adware.
- Scams & Phishing.
- Spam.
- Bots and Zombie networks.
- Blended Threats.
- Mass Mailers.
- Worms.

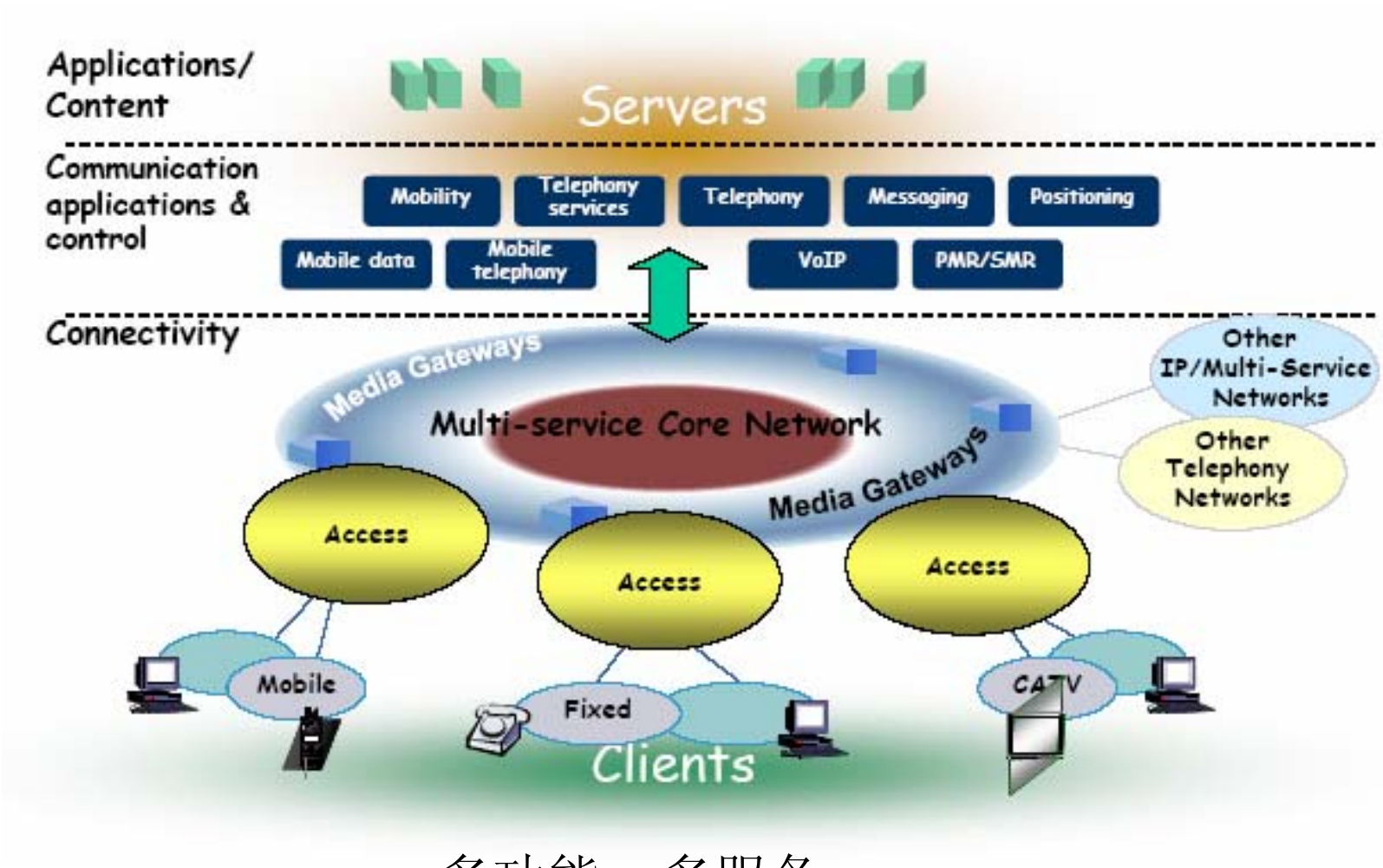
- Bots and Zombie networks.

Top bot-infected cities

Rank	City	Country	Percent of Asia Pacific bot infected computers
1	Beijing	China	21%
2	Taipei	Taiwan	20%
3	Seoul	South Korea	17%
4	Guangzhou	China	8%
5	Hong Kong	Hong Kong (SAR)	6%
6	Hangzhou	China	4%
7	Ningbo	China	2%
8	Singapore	Singapore	1%
9	Makati	Philippines	1%
10	Wuhan	China	1%

Table 3. Top bot-infected cities for the Asia Pacific region

网络结构和应用模式的变化……



多功能、多服务……

议题

1. 安全威胁分析
2. **安全建设面临的挑战**
3. 两种安全响应模型
   - 反应式安全响应模型
   - 主动安全响应模型
4. 建立主动性信息安全体系
5. 总结

目前信息安全建设所面临的挑战

被动应付多于主动防御

不了解真正的安全风险

注重结果不重视过程

安全技术管理水平不高

缺乏有效而统一的标准

用户管理和资源访问的控制较弱

安全组织不健全和安全意识不强

议题

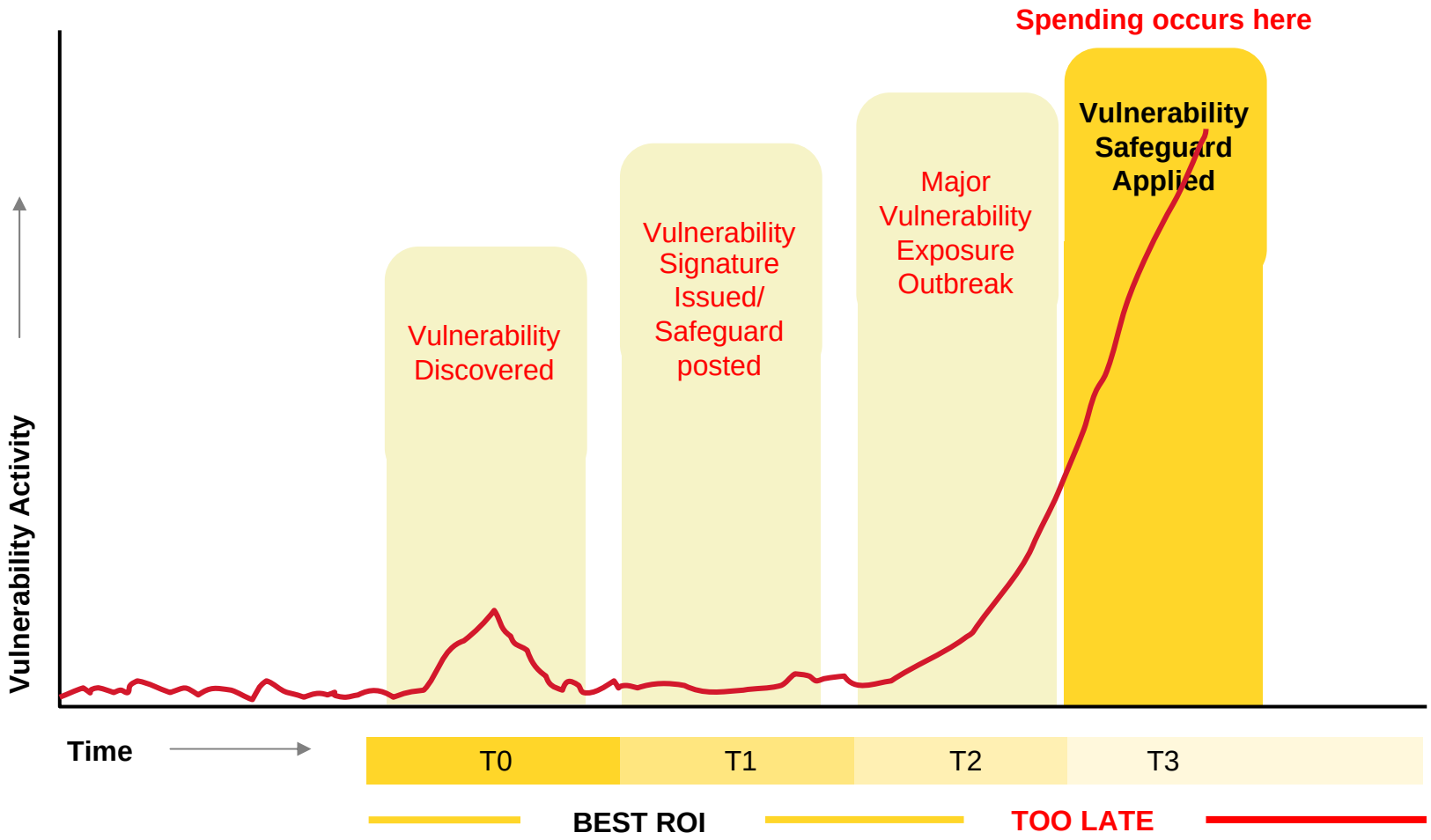
1. 安全威胁分析
2. 安全建设面临的挑战
3. 两种安全响应模型
   - 反应式安全响应模型
   - 主动安全响应模型
4. 建立主动性信息安全体系
5. 总结

两种安全响应模型

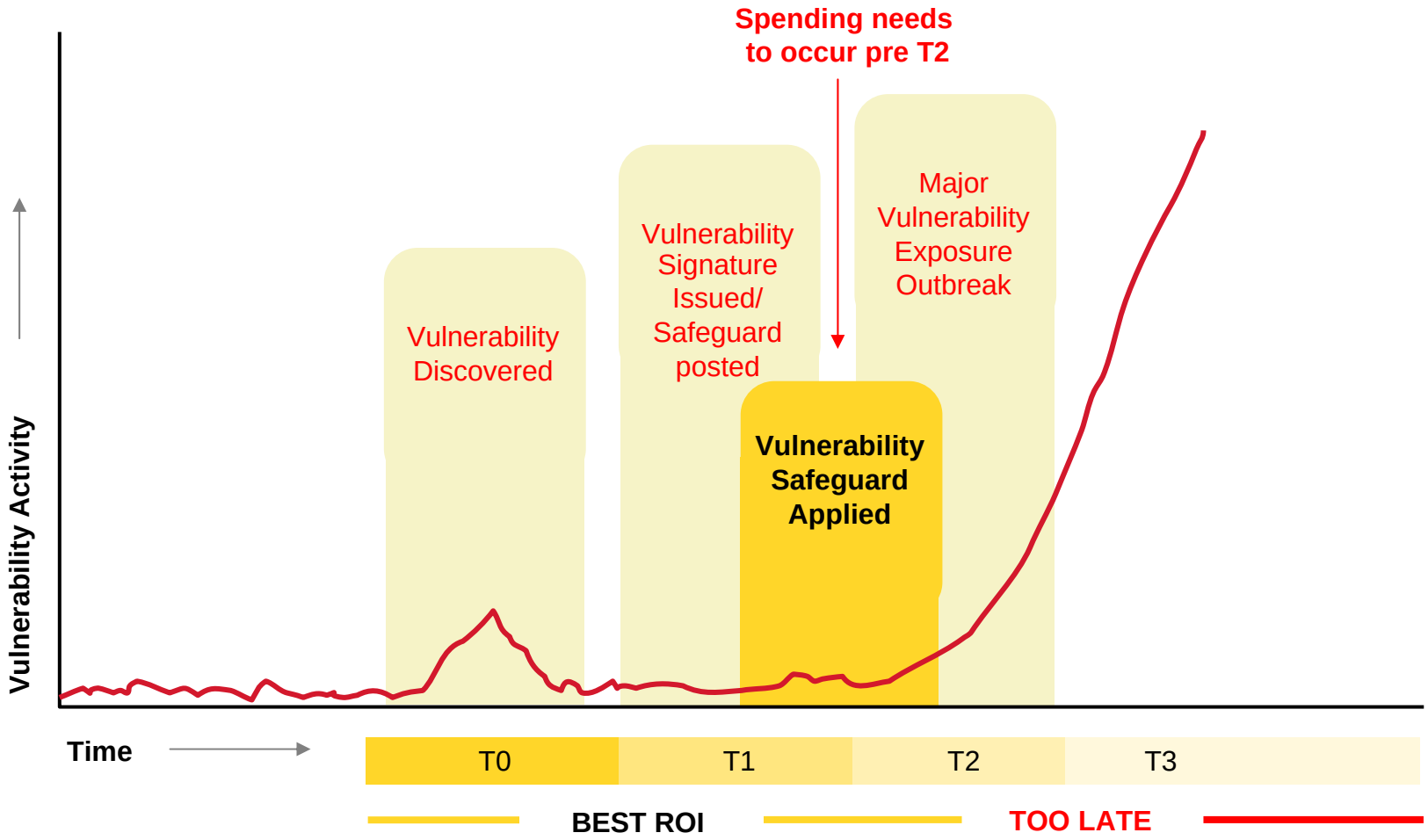
1. **响应式安全防护模型**：基于特定威胁的特征，目前绝大多数安全产品均基于这种技术
- 通过名字识别攻击
- 根据需要进行响应
- 减轻损失
- 事后恢复

2. **主动式安全防护模型**：以识别和阻挡未知威胁为主导思想
- 早期预警技术
- 有效的补丁管理
- 主动识别和阻挡技术

Common Approach Today: A Reactive Security Model



The Way Forward:
A Proactive Security Model



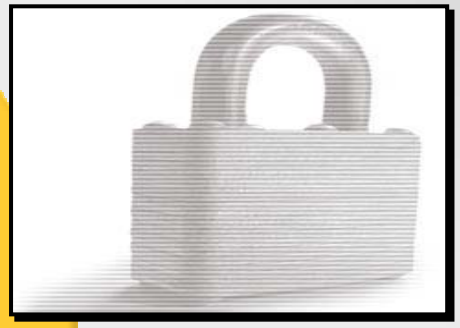
议题

1. 安全威胁分析
2. 安全建设面临的挑战
3. 两种安全响应模型
   - 反应式安全响应模型
   - 主动安全响应模型
4. **建立主动性信息安全体系**
5. 总结

信息安全发展趋势－主动信息安全体系

对即将来临的威胁预先进行警报和风险分析

通过集成方案和单点技术在客户端、网关和服务器上采取防护措施



安全策略符合、安全标准流程管理
安全事件管理、安全教育、安全外包

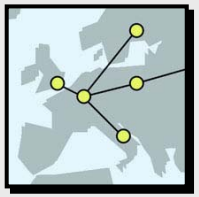
在受攻击前做好预防工作，在受到攻击后减轻损害程度。**7x24**病毒和漏洞升级支持

业务担忧与“警报”机制

业务担忧

更多的威胁和漏洞

攻击导致的损失越来越大



全球、一周七天、一天 24 小时全天候的连接

需要专业的安全指导

预警

咨询和评估

预期结果

- 增强洞察力以便更准确的预计和量化风险
- 拉近安全意识和行动之间的距离
- 简化运作并加强控制

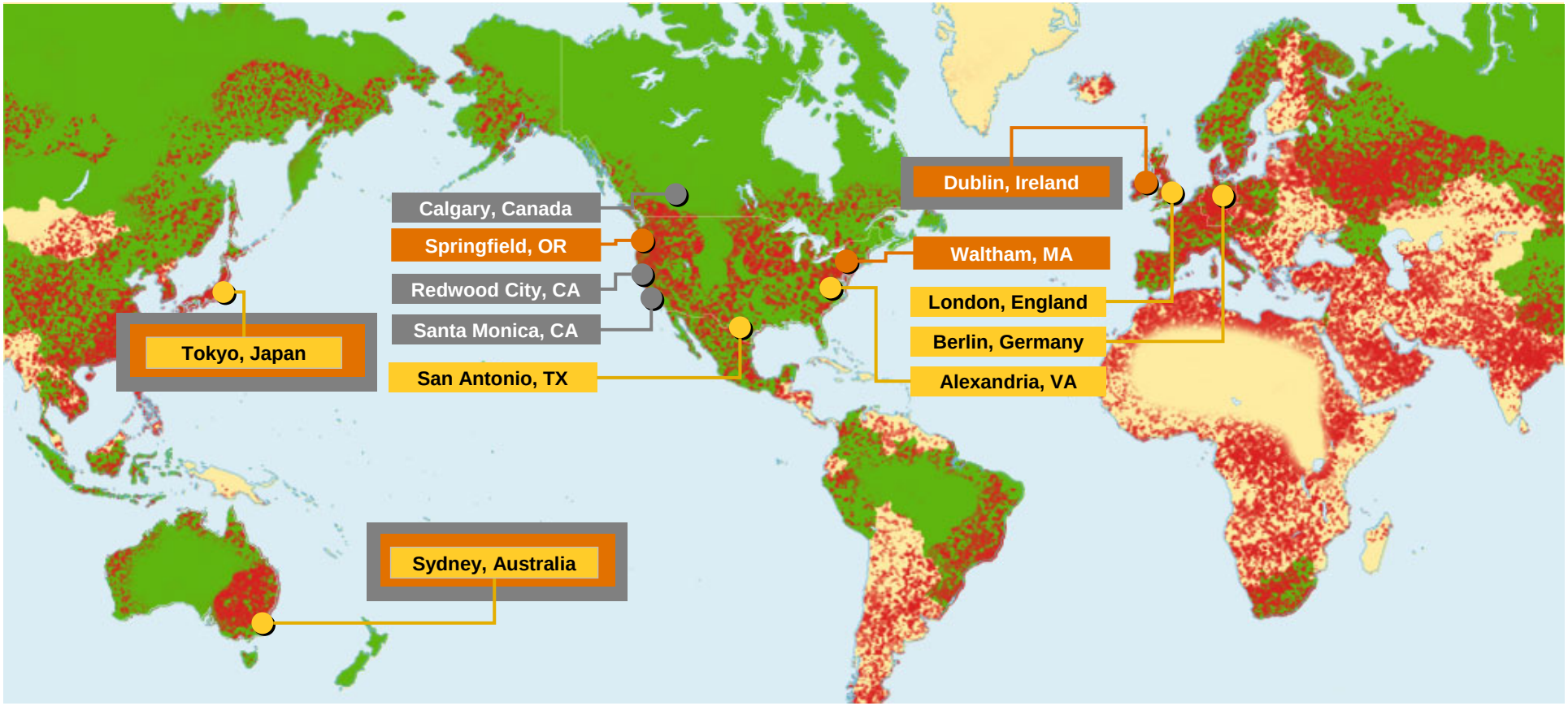
Early Warning of Global Threats

- Risk reduction
  - Maintain highest possible uptime
  - Advance notification of attacks that may impact your organization
  - Decision support
- Reduce time spent tracking and responding to new security threats
  - Timely notifications with expert recommendations
  - Single reliable source
- Increase productivity, optimize prioritization of resources

Global Central Nervous System for Threats

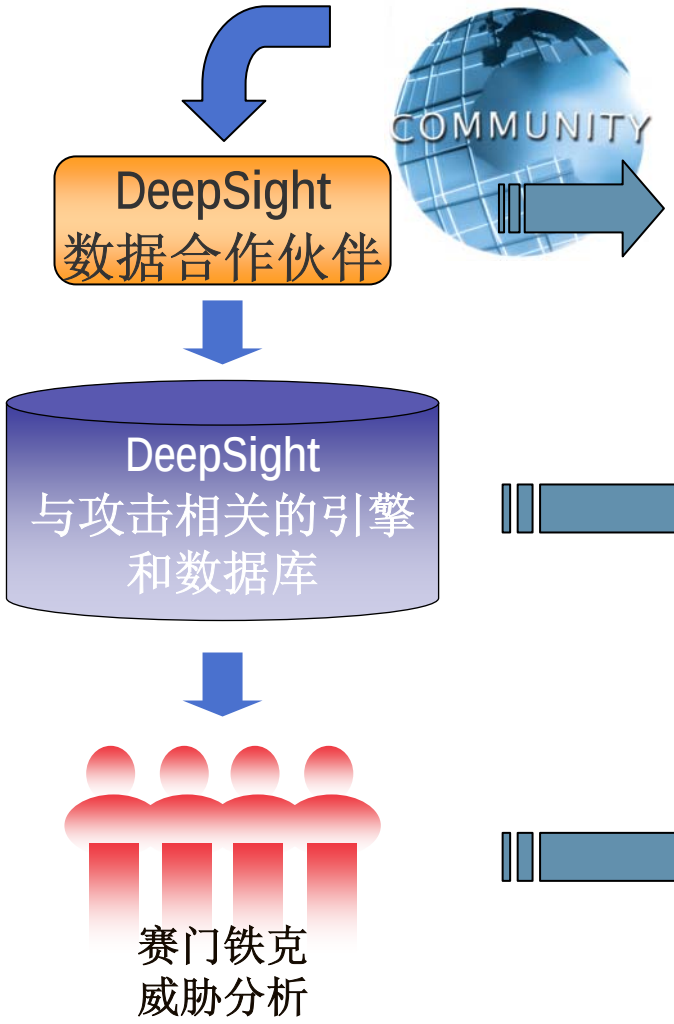
Symantec SOCs + **Symantec Monitored Countries** + **Symantec Support** + **20,000 Registered Sensors in 180 Countries** + **Symantec Security Response Labs**

Over 20,000 Managed Security Devices + 120 Million Symantec Systems Worldwide



DeepSight 威胁管理系统

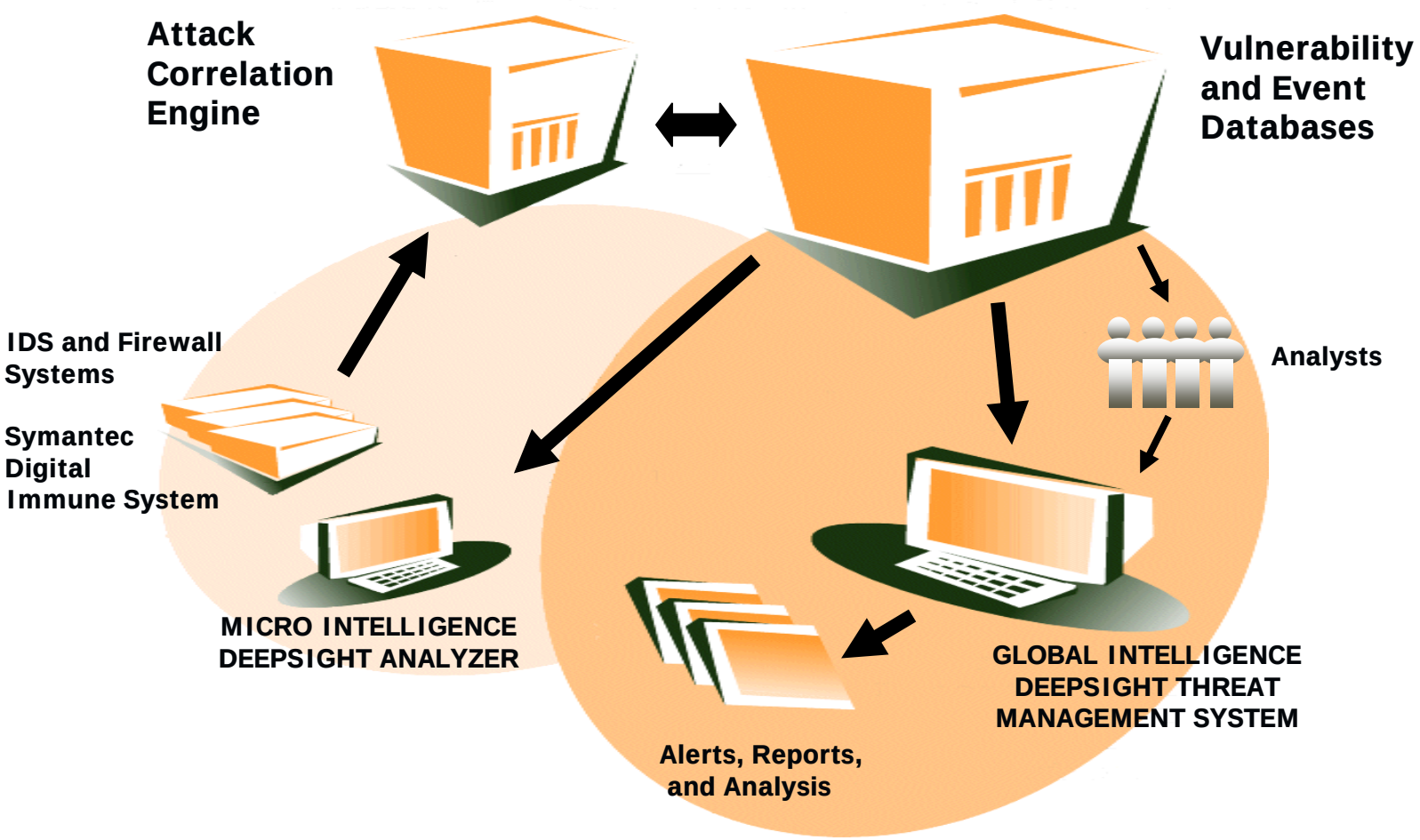
结构概览



- 在全球超过170个国家注册超过 15,000 个合作伙伴 上载IDS信息
- 超过 13 亿个事件
- 超过 12,000 独特攻击
- 几乎 74 亿个攻击者
- 深层的专家分析和调查

DeepSight Threat Management System

Architecture



安全预警系统:

- 精确地告诉他们问题是什么
- 精确地告诉他们问题在哪里
- 精确地告诉他们如何解决这些问题及限制这些危害
- 把上述这些情况及时地告诉他们

What Symantec Early Warning Systems Can Do For You

- Maintain Business Continuity
  - Advance notification of attacks that could impact your organization
  - Make more informed decisions and respond quicker
  - Maintain highest possible uptime
- Improve Business Efficiency
  - Reduced time spent tracking new security threats
  - Actionable information
  - Resource prioritization and productivity
- Achieve Business Results
  - Brand Reputation
  - Gain Competitive Advantage
  - Maintain stakeholder value

业务担忧与“防护”机制

业务担忧

更多危险的混合型威胁

有限的 IT和运营资源

需要尽可能的增大信息可用性

日益增长的管理要求

防火墙
VPNs
防病毒
防垃圾邮件
入侵防护

备份/恢复
软件管理

安全实施服务

托管安全服务

预期结果

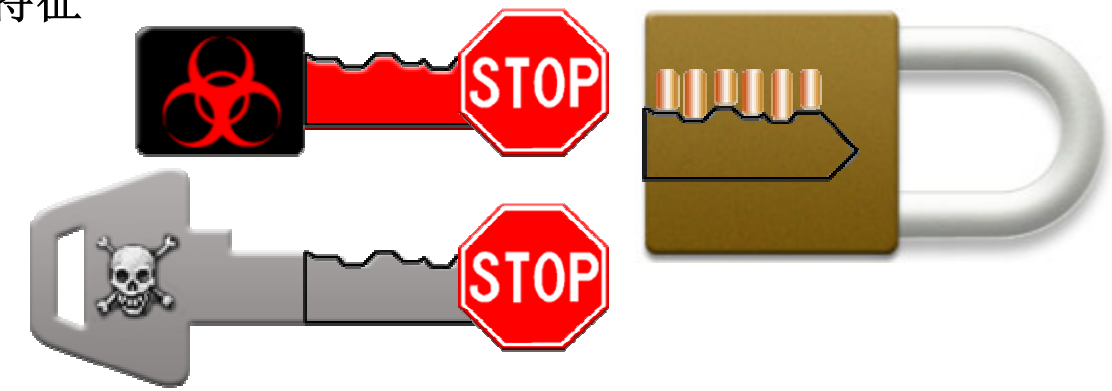
- 降低运营风险
- 通过集中的自动化流程来简化运营
- 有效地防御损害并快速恢复

主动防护技术举例： 一般漏洞利用阻截

思想：

正如只有形状正确的钥匙才能打开锁一样，只有“形状”正确的蠕虫才能利用漏洞进行攻击。

步骤 1：总结新漏洞的“形状”特征



步骤 2：以该形状作为特征，扫描网络流量并阻截与其匹配的任何数据

立即阻截所有的新蠕虫，无需特定的特征。

集成的安全防护解决方

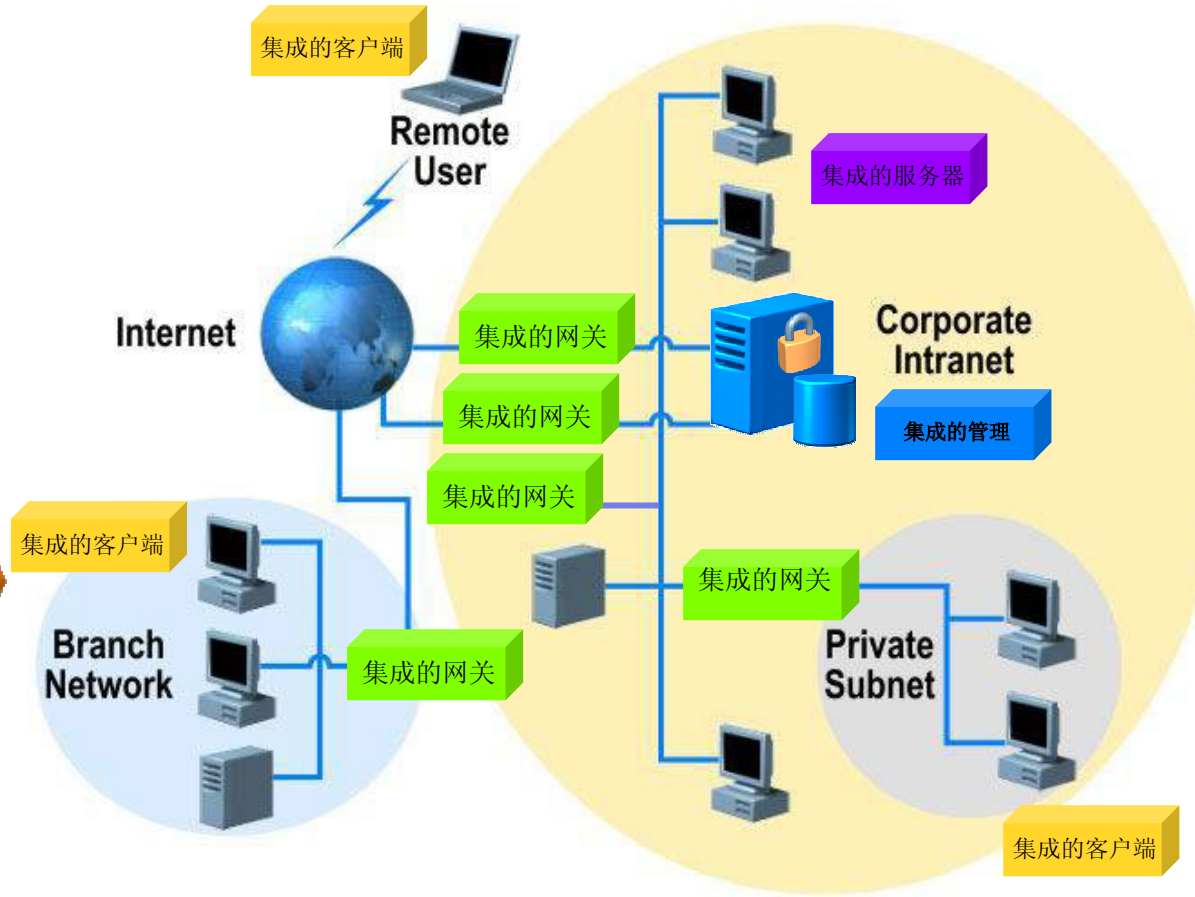
效果：
- 减少安全的复杂性
- 全面的防护
- 降低总体的总拥有成本

集成的客户端

集成的网关

集成的管理

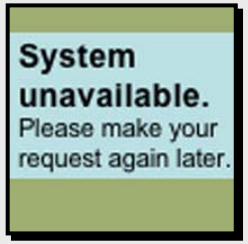
集成的服务器



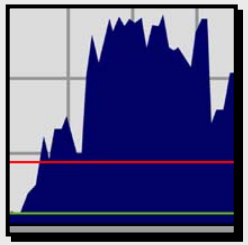
业务担忧与“响应”机制

业务担忧

对于被动性响应来说，攻击发生得太快



出于保护目的而使关键系统脱机的代价



在高通信量攻击发生期间维持运营的能力

响应定义和特征

事故分析
修补管理

客户支持

寻求补救措施

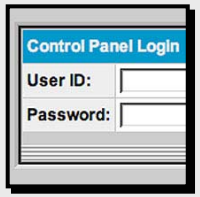
预期结果

- 轻松快速的部署新安全措施
- 在攻击发生前主动响应威胁
- 在攻击发生前、发生时和发生后都不中断业务运营
- 有效防御损害并快速恢复
- 通过集中的自动修补来减少漏洞

业务担忧与“管理”机制

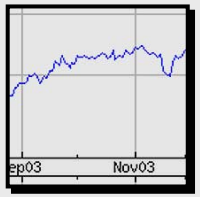
业务担忧

IT 和业务目标更紧密的结合在一起



影响安全的业务实践

防护措施具有适当降低风险的能力



漏洞对公司、股东和客户的影响

安全管理

托管安全服务

教育和咨询

预期结果

- 下列问题的答案：
  - 我们的安全状况如何？
  - 我们会在什么时候受到攻击？
  - 我们如何调整防御措施？
- 改进风险状况
- 快速、准确地识别事故
- 即时响应

议题

1. 安全威胁分析
2. 安全建设面临的挑战
3. 两种安全响应模型
   - 反应式安全响应模型
   - 主动安全响应模型
4. 建立主动性信息安全体系
5. 总结

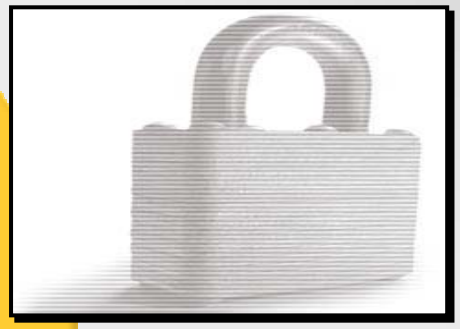
主动式信息安全体系

对即将来临的威胁预先进行警报和风险分析

警报

防护

通过集成方案和单点技术在客户端、网关和服务器上采取防护措施



多层次主动性

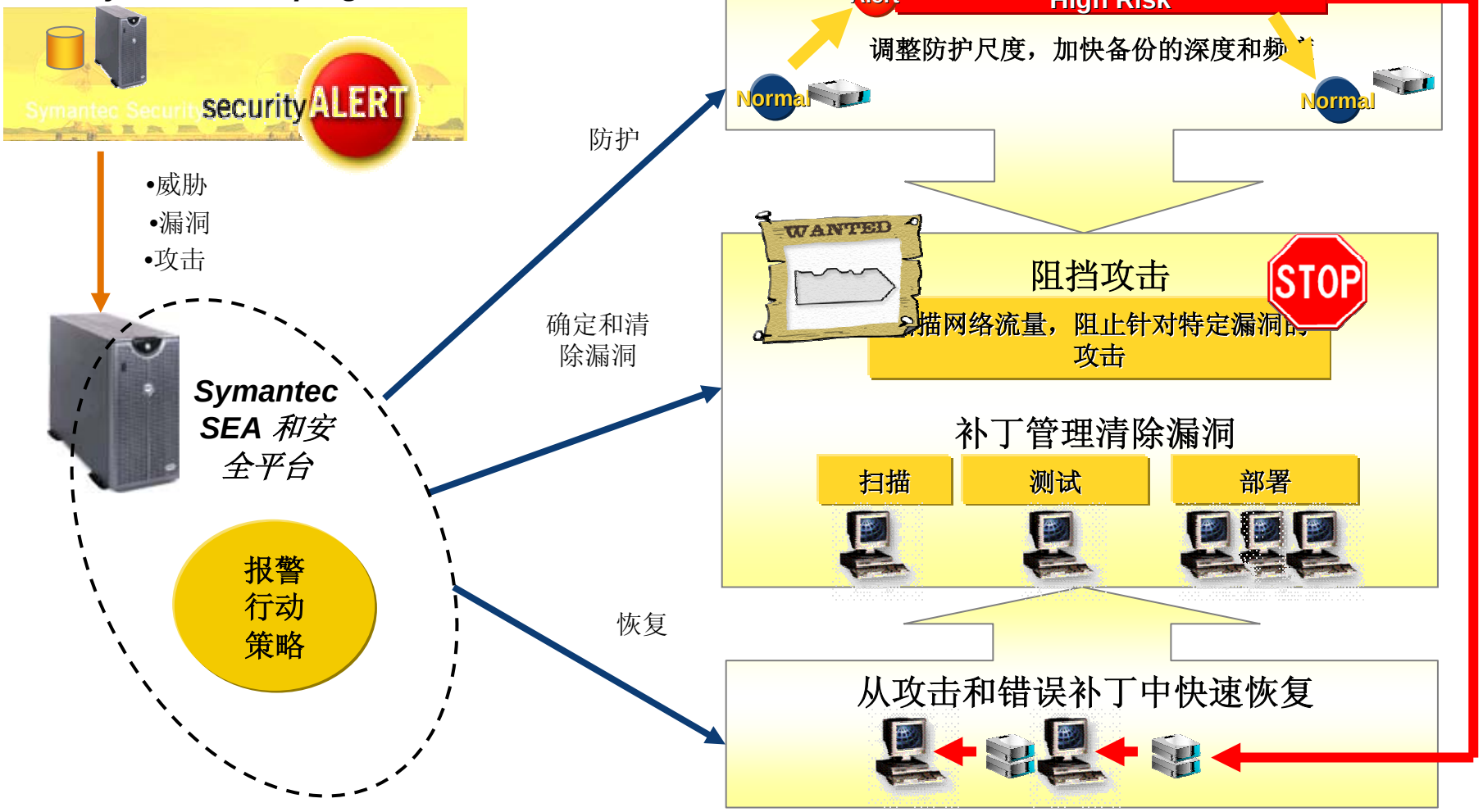
管理

响应

安全策略符合、安全标准流程管理
安全事件管理、安全教育、安全外包

在受攻击前做好预防工作，在受到攻击后减轻损害程度。**7x24**病毒和漏洞升级支持

集成威胁、安全、补丁管理和恢复



谢谢