# Symantec安全专题规划与解决方案汇总

# 目录

# 企业安全建设的发展趋势

## 传统的思路和模式

**以边界、安全域为主的“传统防护思路”**

**被动的、防御型的技术手段**

**应对型的安全建设模式**

### 防护重点

逐渐转向针对：

- **数据内容**
- **应用**
- **用户身份**
- **行为**

的安全防护。

### 安全治理观念

1.加强主动防御的**合规管理工作**。

2. 加强安全**监控综合分析**；

3. 通过安全指标为衡量手段，推进安全治理、衡量安全建设绩效。

### 高效安全管理需求

通过工具化、自动化的安全手段，应对不断扩张的IT资产的管理，有效落实安全管理要求

# 来自最佳实践的企业安全建设框架：

- **以合规管理推动安全治理常态化**
  - 以风险和企业策略为驱动
  - 以自动化的风险与合规管理为手段
  - 不断治理和改善安全状态
  - 应对不断变化的挑战

- **以身份管理确保可信的访问**
  - 人是IT系统使用的主体
  - 身份的标识与认证确保主体的安全


- **以“信息”风险管理为核心**
  - 信息的安全更针对数据的内容
  - 信息是IT系统的核心与重点

- **增强基础设施管理**
  - 标准化、流程化、自动化
  - 更加高效、安全的IT运行管理
  - 更加安全的基础设施环境

- **提供良好的基础设施保护**
  - 提供安全保护良好的基础设施

    包括：网络/终端/服务器/存储/数据/应用

# 最佳实践安全框架中的安全技术要点



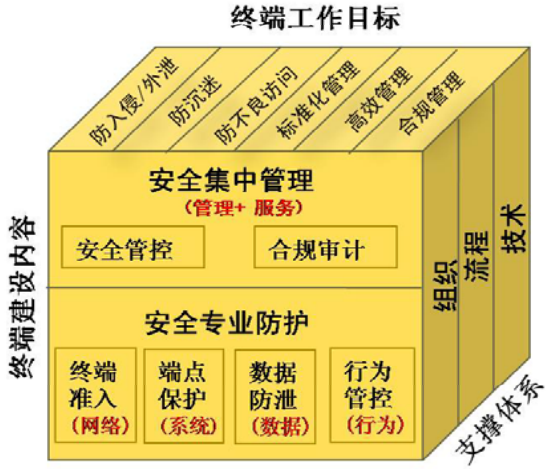



# 目录

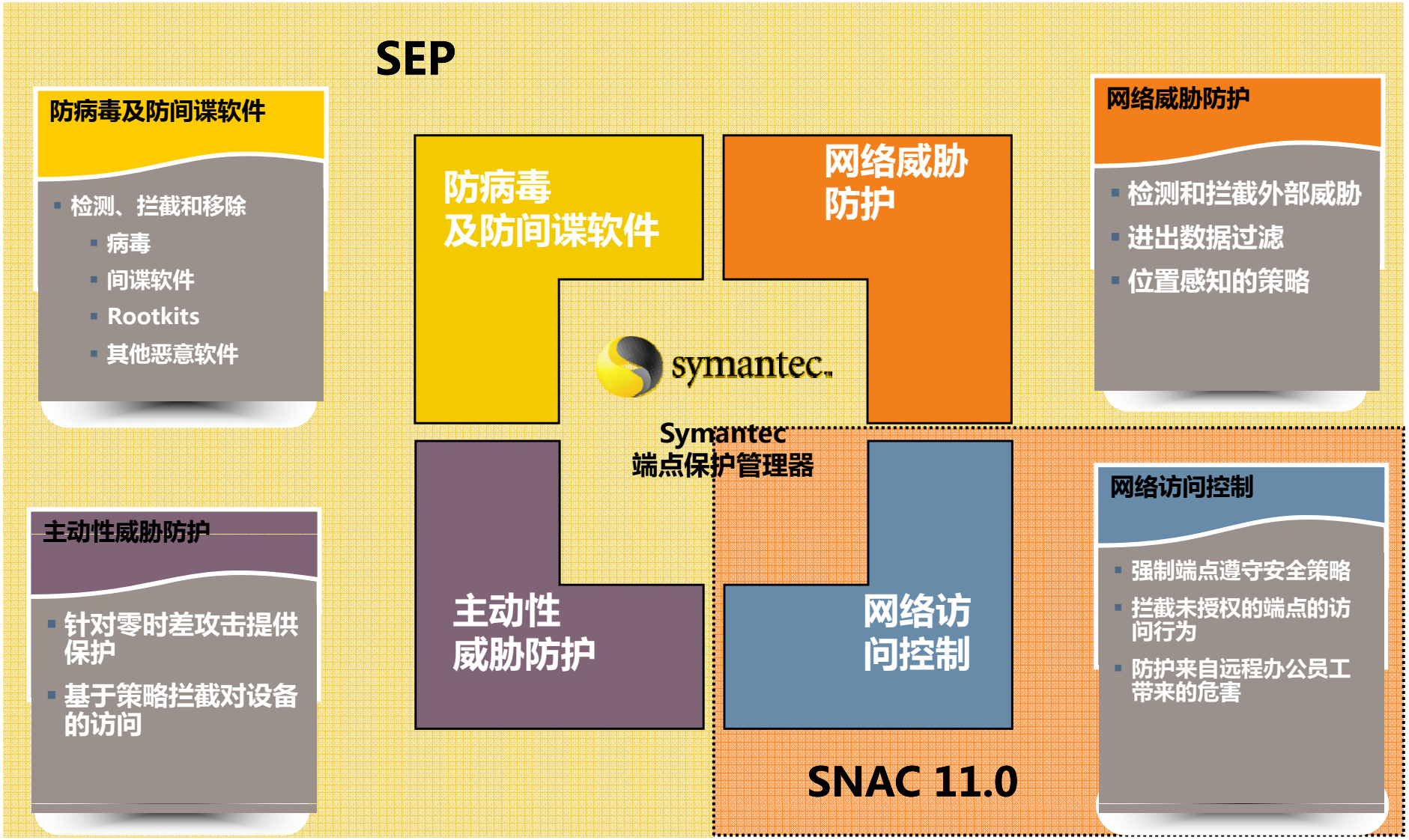
1. 安全框架最佳实践
2. 赛门铁克专题性安全解决方案

# 专题1：终端安全全面解决方案

# 终端安全规划与建设内容




# Symantec 终端安全防护（SEP）—专业防护1



# Symantec端点防护的虚拟 Insight 功能

### Virtual Image Exception
### 虚拟镜像排除

- 针对通过克隆部署的虚拟机
- 扫描时排除所有文件
- 极大降低扫描的性能开销

### Shared Insight Cache
### 缓存服务器

- 同样的文件只扫描一次
- 同时支持物理与虚拟环境

### Virtual Client Tagging
### 虚拟客户端标示

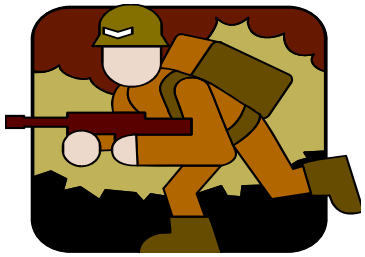
- 识别虚拟机
- 创建虚拟机的特殊策略
- 支持虚拟机的搜索

### Offline Scanning
### 虚拟机离线扫描

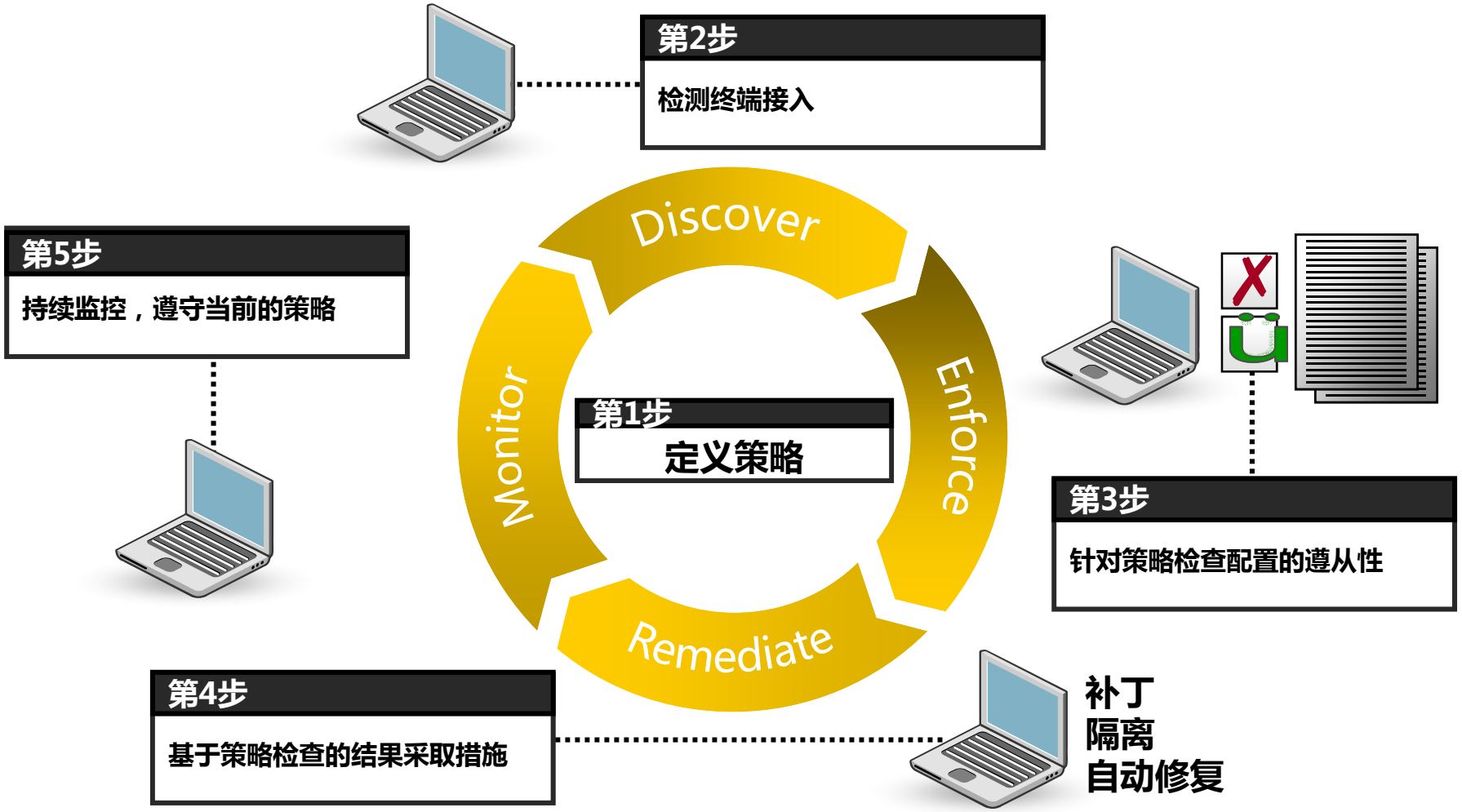
- 支持所有主流的虚拟环境
- 分散扫描的时间

# Symantec DLP 终端敏感数据外传拦截—专业防护2

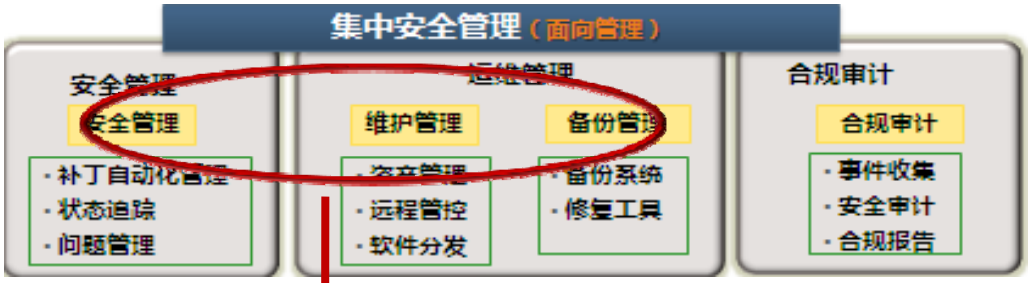

# Symantec WEB网关纵深防御（SWG）—专业防护3

| | | |
|---|---|---|
| 事前预防 |  | URL过滤<br>应用程序控制 |
| 事中拦截 |  | 病毒过滤<br>间谍软件过滤<br>数据防泄露 |
| 事后纠正 |  | 防僵尸网络 |

# Symantec网络准入控制（ SNAC ） - 专业防护4

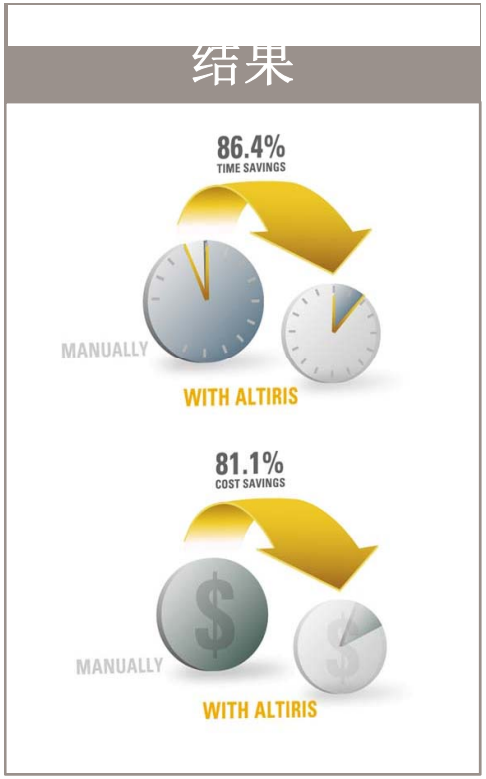


# Symantec Altiris 客户端管理套件（CMS）—集中管控



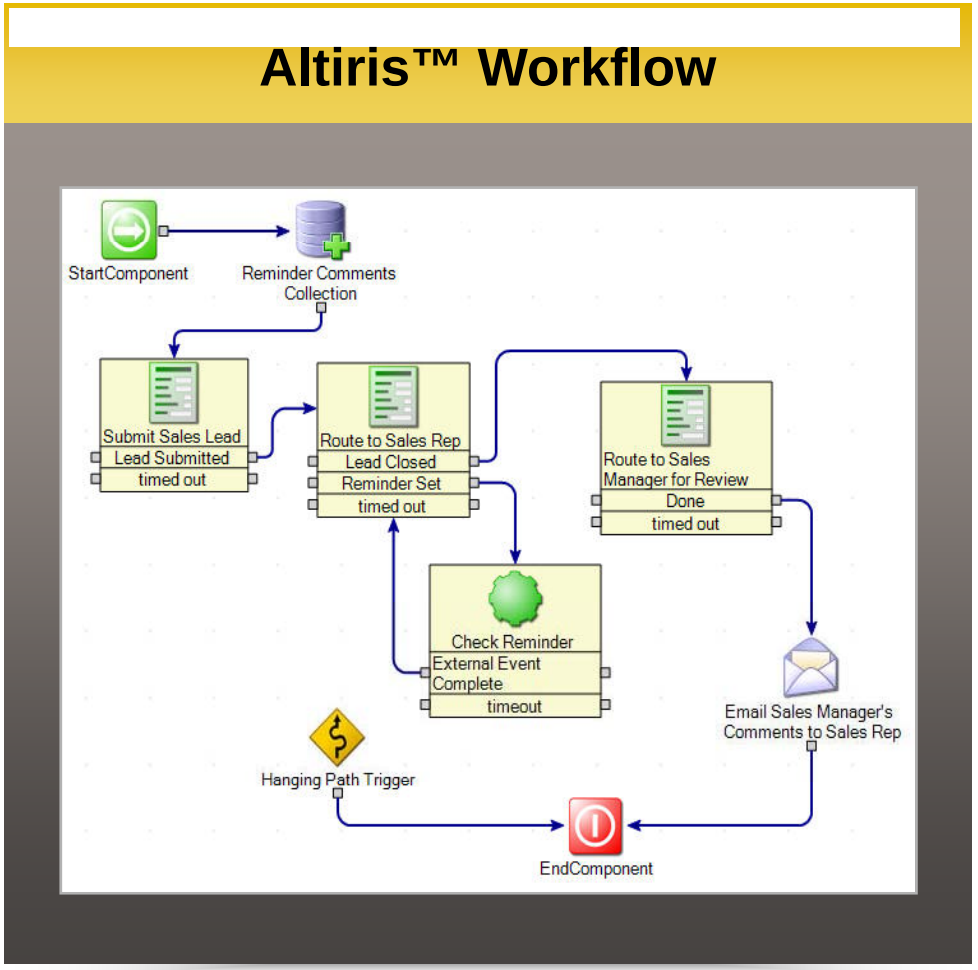



Altiris™
Client Management Suite

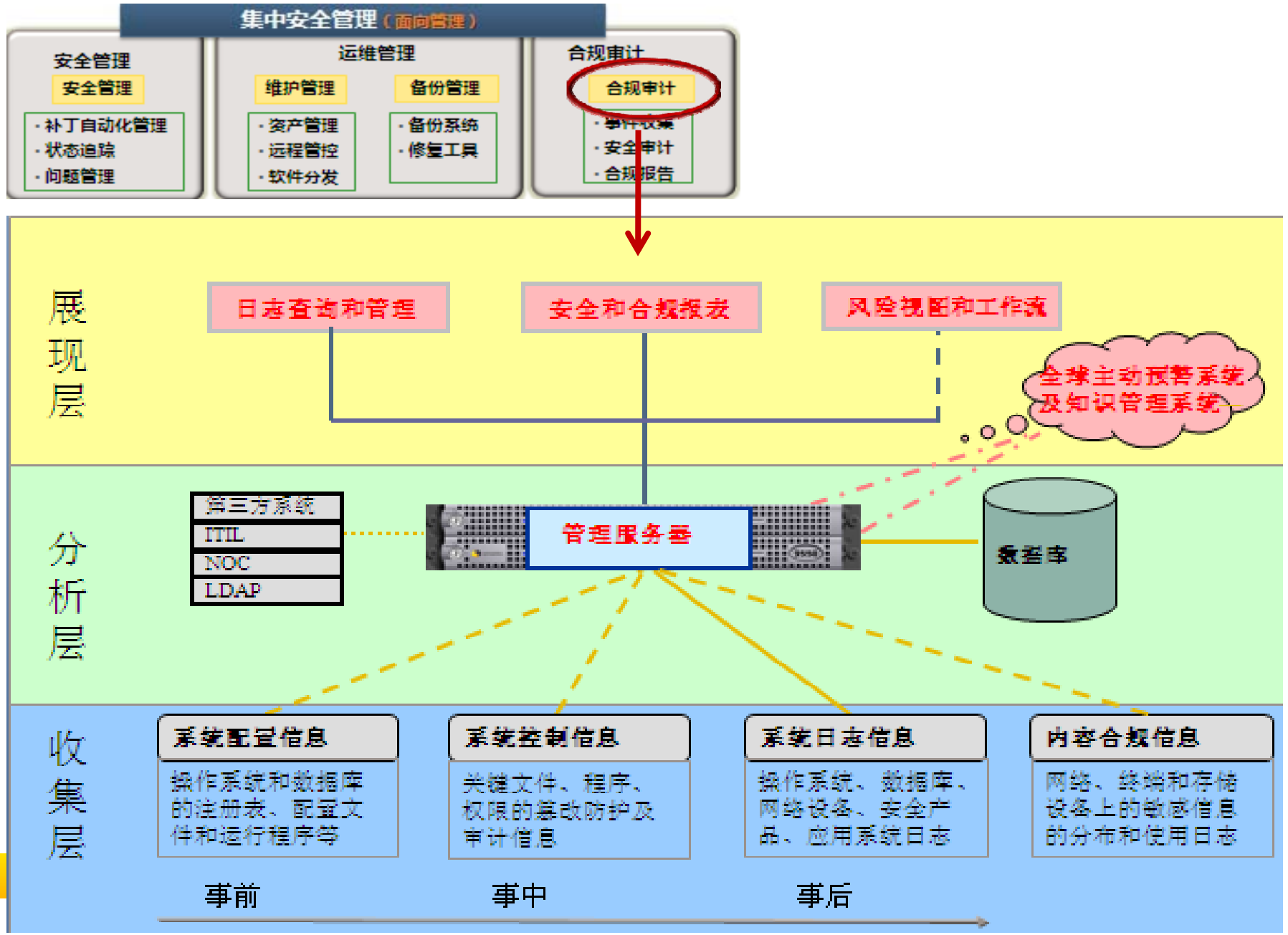


# 完全自动化的处理流程

- 任务管理器自动化
  - 集成的部署和迁移任务
  - 条件逻辑
  - 包含所有功能
- Altiris™ Workflow Solution
  - 及时协调人员和系统之间的交互
  - 使用电子邮件、网页、移动设备
  - 处理日常审批和跟进工作
  - 根据要求提供更好的服务；效率更高的 IT 资源
  - 自助服务类别的基础

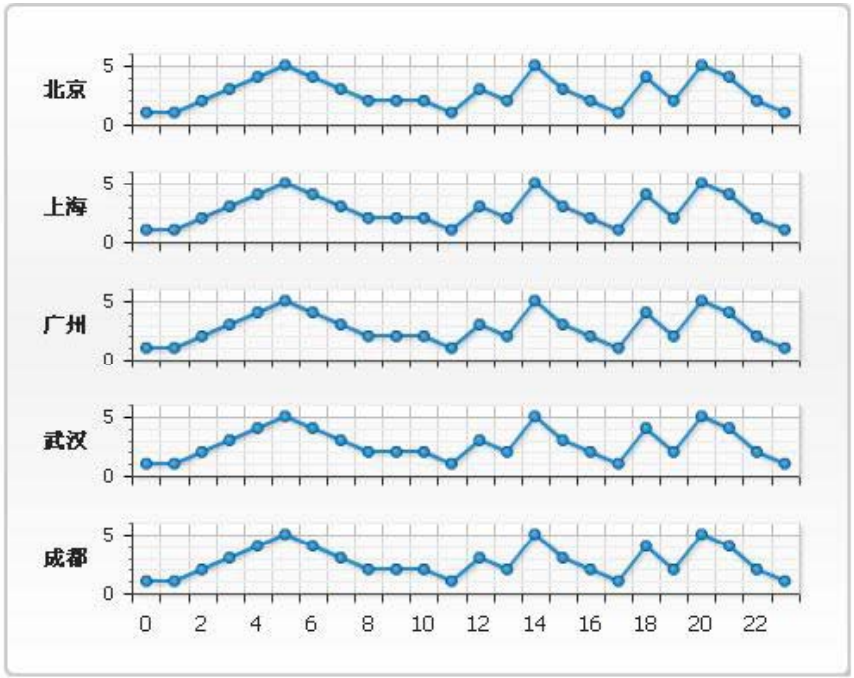


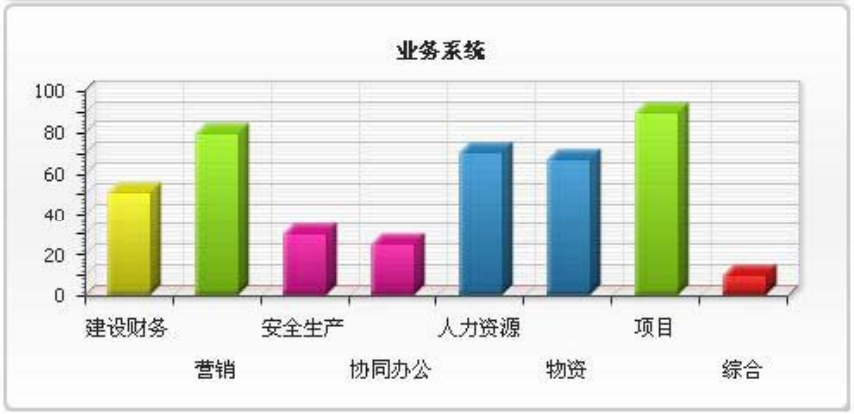
# Symantec 安全合规审计与报表系统（SIM）—集中管控

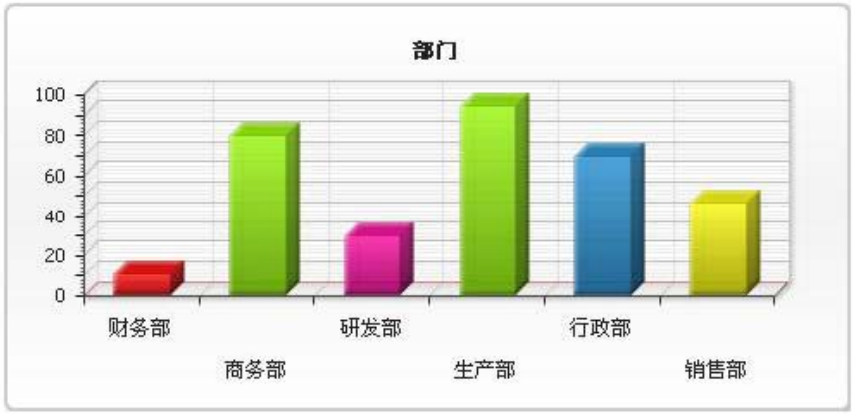


# KPI视图展现


安全地图
北京
上海
成都
武汉
广州
日期
2009-01-06
播放间隔
10秒


北京
上海
广州
武汉
成都
5
0
0 2 4 6 8 10 12 14 16 18 20 22


业务系统
100
80
60
40
20
0
建设财务
营销
安全生产
协同办公
人力资源
物资
项目
综合


部门
100
80
60
40
20
0
财务部
商务部
研发部
生产部
行政部
销售部

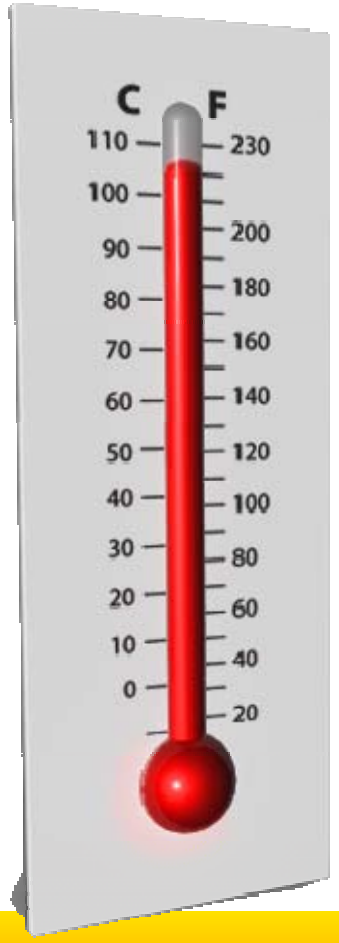
# 专题2：服务器安全全面解决方案

# 服务器安全的规划与重点建设内容

- 系统防护
  - 事前安全配置与漏洞检查
  - 事中安全监控与防护
  - 事后安全审计
- 服务器管理
  - 运维管理
  - 安全管理
- 信息防护
  - 信息在服务器上的安全存放（加密）
  - 信息异常分布的扫描与弥补（隔离/转移）
- 合规管理
  - 归档与电子发现

# 服务器系统层安全的焦点

*1+* 种操作系统*10+* 台服务器*100+* 次系统变更*1000+* 次访问…




| | |
|---|---|
| 事前 | 服务器是否有安全风险和配置缺陷，符合数据中心的安全要求吗？ |
| 事中 | 当违规操作或者恶意入侵正在发生，能及时发现并有效预警吗？ |
| 事后 | 损害发生后，能够审计分析出问题并有效取证吗？ |

# Symantec服务器系统防护解决方案—系统防护

ESM + CCS VM SCSP SIM

**事先评估** **事中监控** **事后审计**

**法规**

SOX
PCI-DSS
ISO27001
等级保护
...

**配置**

密码
服务
文件
审计
...

**漏洞**

RPC
补丁
web
端口
...

**安全锁定**

限制网络连接
锁定配置文件
锁定用户权限
...

**监控预警**

系统监控
文件监控
日志监控
...


**识别风险并开发相应的策略**

**监控并预警问题**

**证明有效性并判定趋势**

# Symantec 服务器三重防护功能—系统防护

## SSIM收集并关联分析系统日志

**事件收集和存储能力**

- 收集ESM/SCSP以及100多种操作系统、防火墙、IDS、路由和交换设备的日志
- 支持海量日志存储，并进行加密、压缩、HASH处理确保可以作为取证证据

**强大的关联分析能力**

- 跨产品日志关联分析
- 强大的查询报告能力
- 内置各种法规遵从模版

## ESM发现配置缺陷和安全漏洞

**配置检查**

- 注册表
- 配置文件
- 密码
- …

**漏洞扫描**

- 服务器漏洞
- 补丁安装检查
- 网络设备漏洞
- …

## SCSP实时阻止入侵和违规操作

**安全防护**

- 零日攻击
- 系统加固
- 非法入侵
- …

**检查违规操作**

- 用户变动
- 文件变动
- 权限变动
- …

# Symantec Altiris 服务器管理套件（SMS）—服务器管理

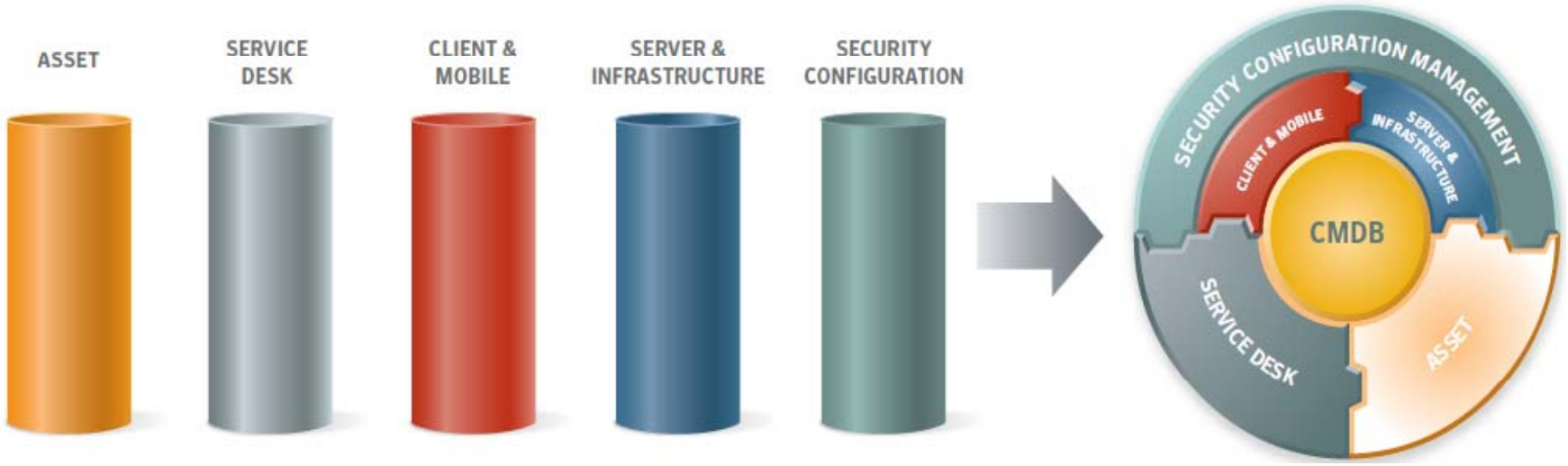
四大基础模块


其他可选插件

- Backup and Recovery
- Advanced Configuration Management
- Endpoint Protection
- Audit and Compliance

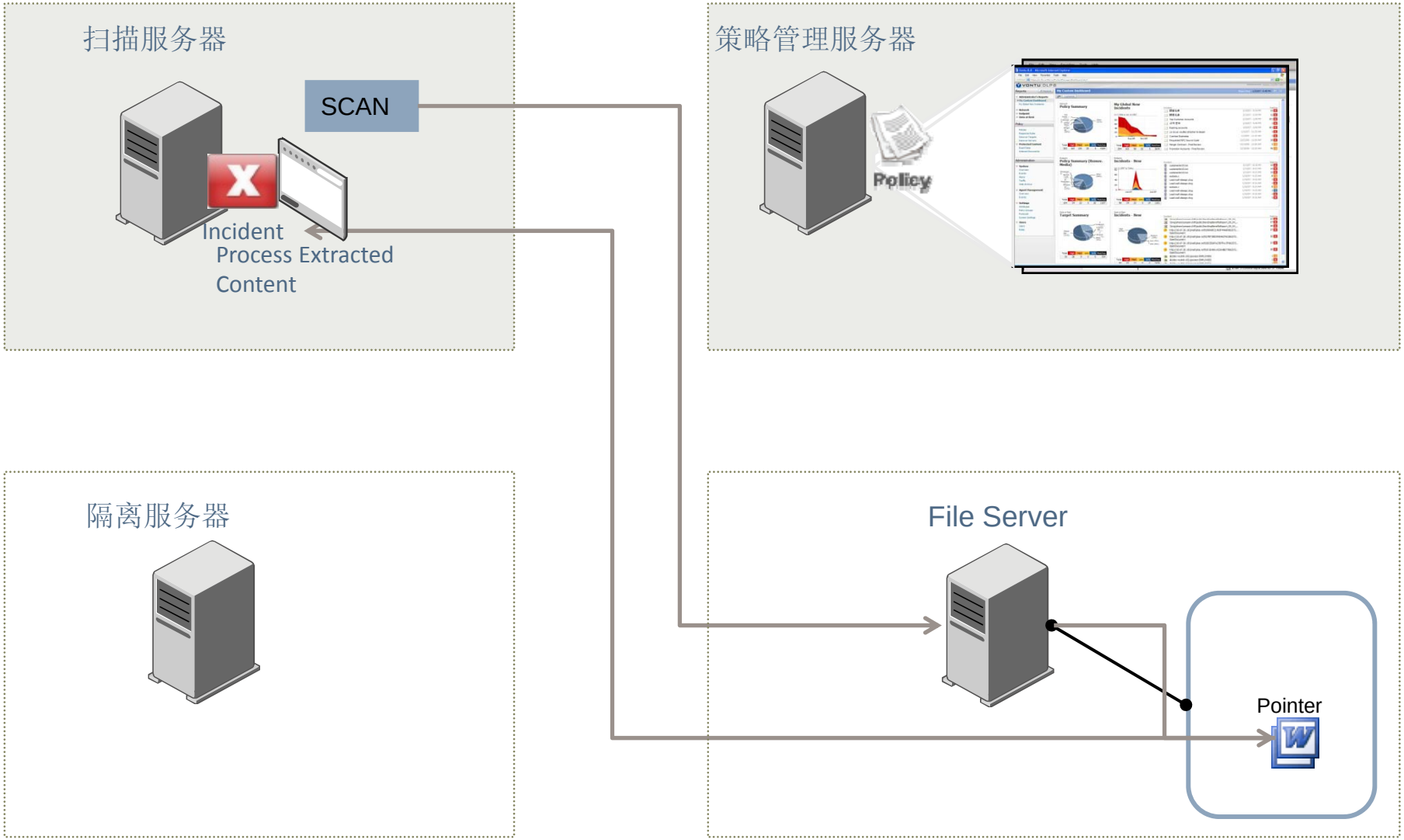
- 统一的控制台集中管理服务器硬软件
- 服务器可视化
- 可裸机部署硬件设置、镜像和脚本化安装 **Windows*** 以及 **Linux***
- 在**Windows and Linux**环境中可一对多进行补丁管理
- 基于角色和区域的安全管理特性
- 管理刀片,虚拟机， 机架和塔式服务器
- 具有实时仪表板和分发向导的直观管理界面.

# Altiris IT资产标准化管理整体方案




- 遵循ITIL的服务过程管理，加强IT的支持和交付
- 通过对ITIL的全面支持，加强IT内控
- 从而达到法规遵从的要求

# 服务器敏感信息排查与隔离—信息安全



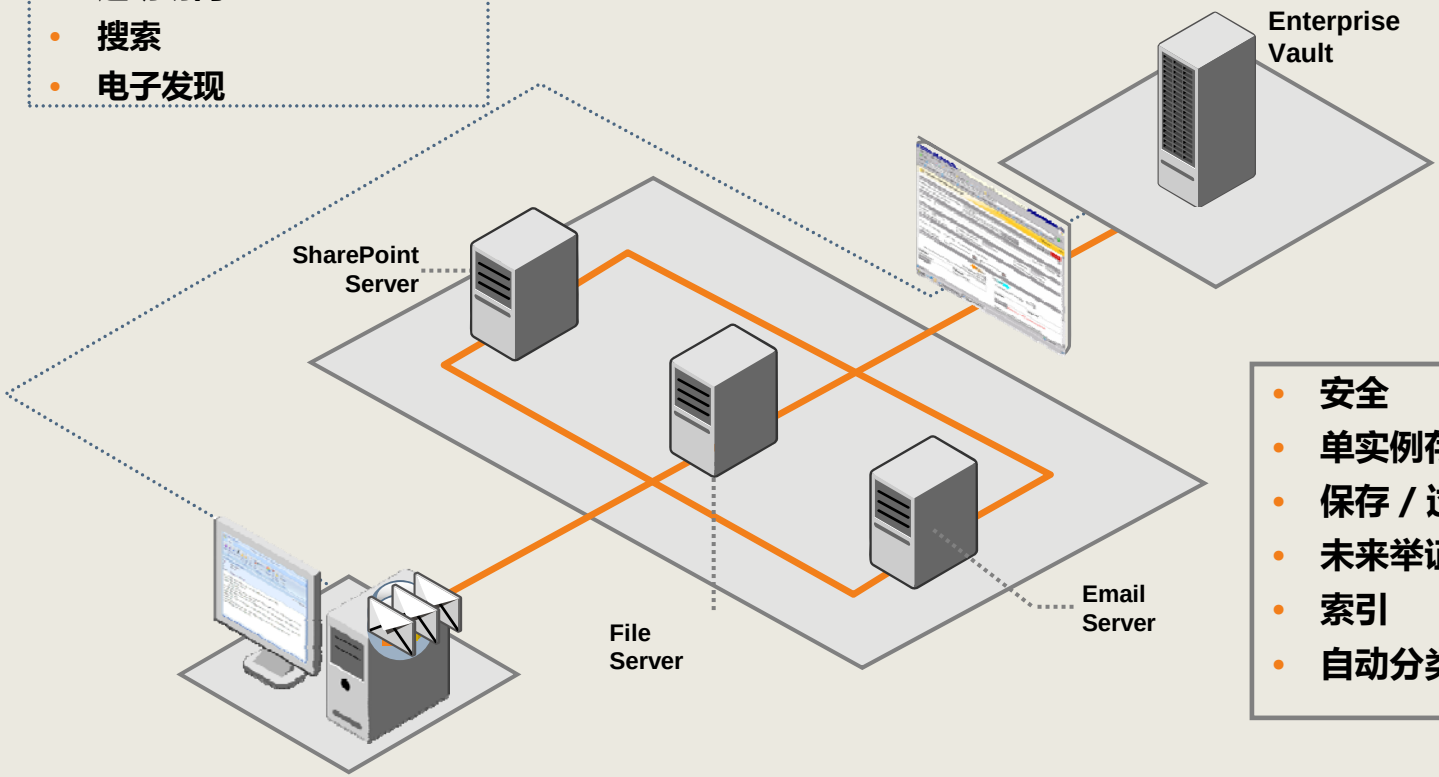
# 归档需求的产生（SOX法案为例）—合规管理

- 第903节：邮件及电传欺诈的刑事责任的规定
- 邮件系统中包含大量影响公司业务和财务信息的重要数据
- 在美国上市的公司需要对邮件进行归档保存并保证能被快速查询到

## Symantec EV（Enterprise Vault）解决方案

# Symantec Enterprise Vault—合规管理

- 透明访问
- 搜索
- 电子发现



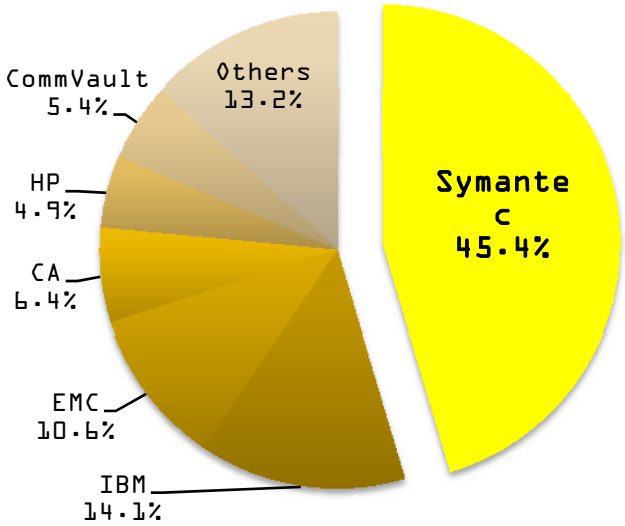

- 安全
- 单实例存储
- 保存 / 过期
- 未来举证
- 索引
- 自动分类

**成本更低** **更快** **更可靠**

# 专题3：数据保护与高可用解决方案

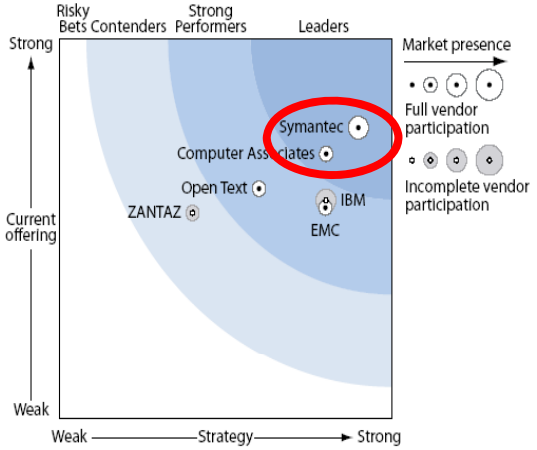
# NetBackup: 备份软件的领导者

## Gartner: #1
## Data Protection Market Share

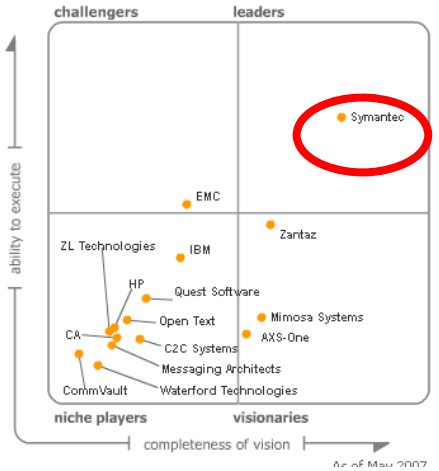



**Worldwide Backup / Recovery Market Share for 2007 (Published July 2008)**

## Forrester: Leading Archiving Vision




## Gartner: Leading Archiving Vision




**Gartner Archiving Magic uadrant, 200 7**

## Gartner: #1 Data Protection Vision

Gartner Data Protection Vision (Published April 2008)

| | RATING | | | | |
|---|---|---|---|---|---|
| | Strong Negative | Caution | Promising | Positive | Strong Positive |
| Atempo | | x | | | |
| BakBone Software | | x | | | |
| CA | | | x | | |
| CommVault | | | | x | |
| EMC | | | x | | |
| HP | | | x | | |
| IBM | | | x | | |
| Symantec | | | | x | |
| Syncsort | | | x | | |

# 系统高可用性—集群整合

## 大多数“传统”集群

- 2节点主/备
- 2节点主/主
- 专用备机（N：1）

## 赛门铁克“高级”集群

- 漫游备机（N + 1）
- 无备机（N：N）
- 支持所有操作系统集群，实现统一管理

# 《信息系统灾难恢复规范》

6级-数据零丢失和远程集群支持

5级-实时数据传输及完整设备支持

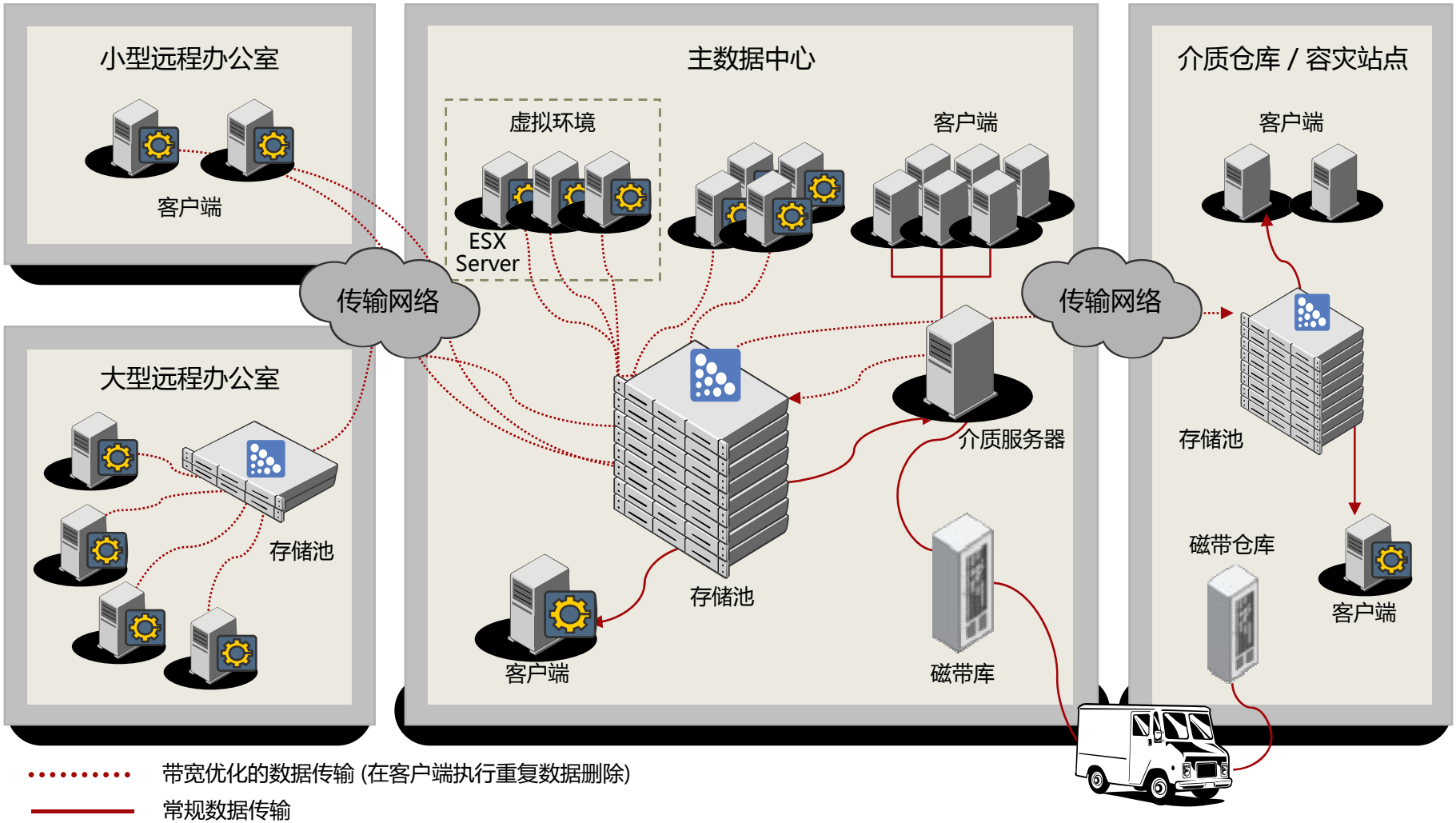
4级-电子传输及完整设备支持

3级-电子传输和部分设备支持

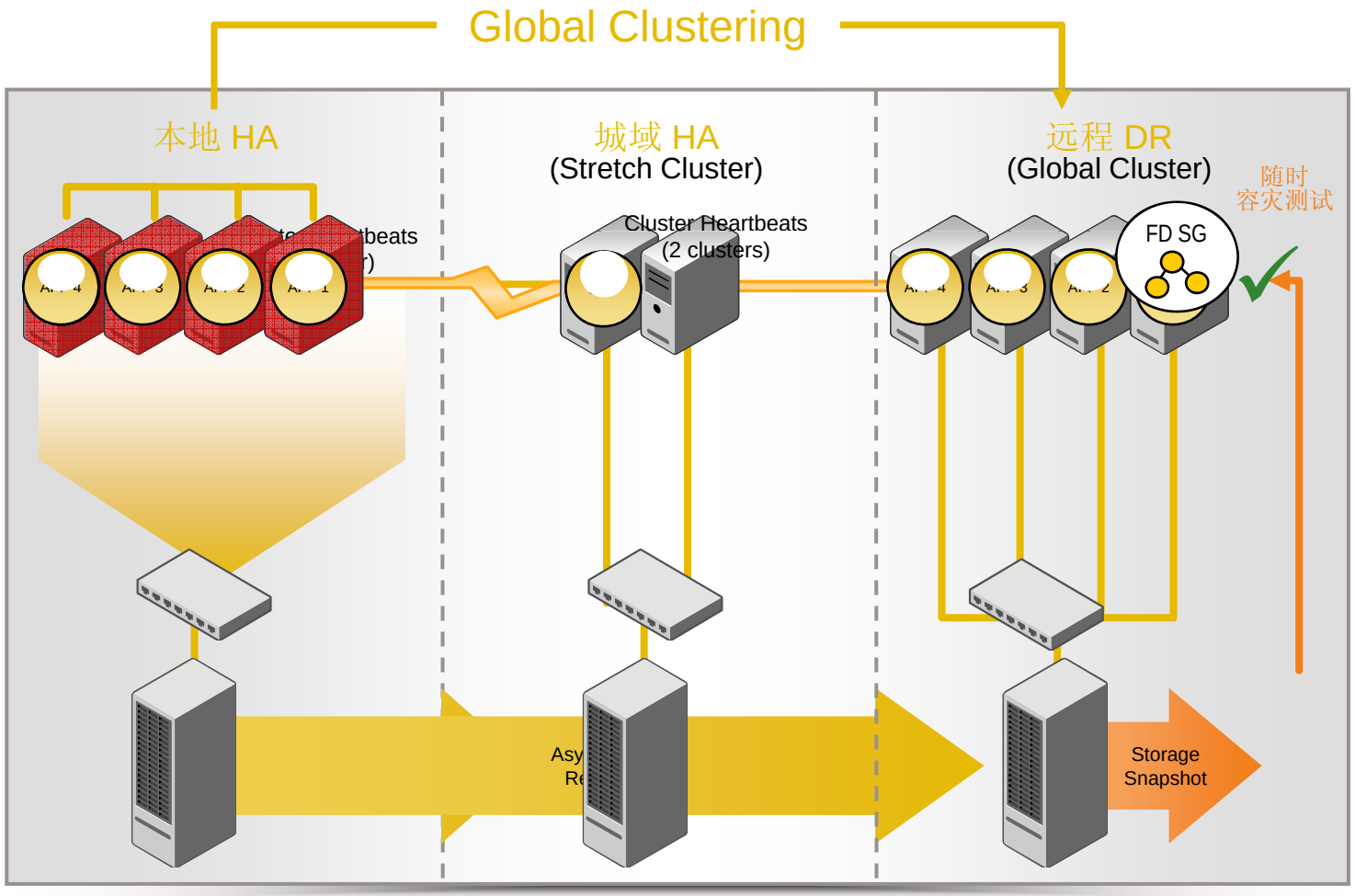
2级-备用场地支持

1级-基本支持

# 国标1234级容灾解决方案

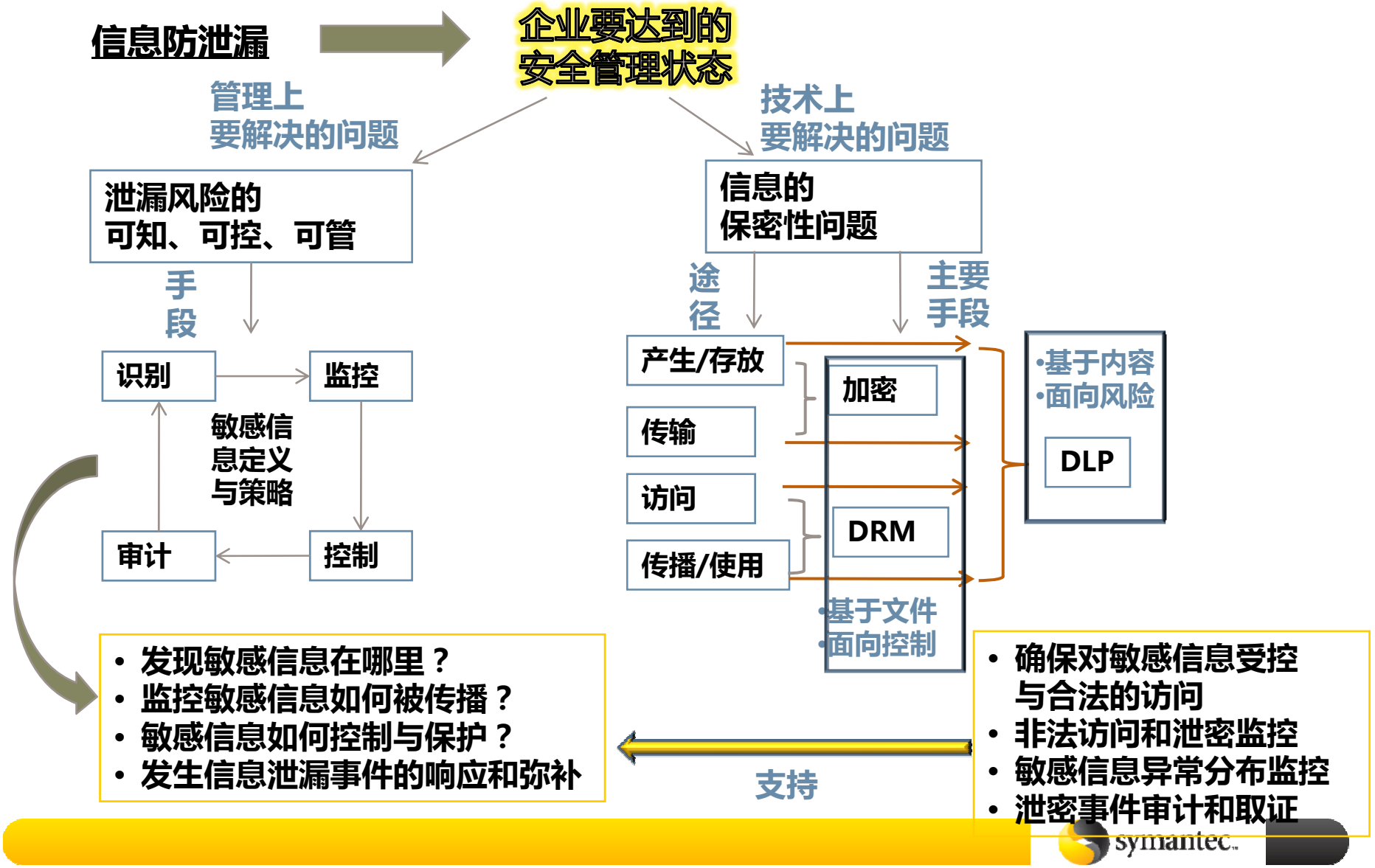


# 国标56级容灾解决方案



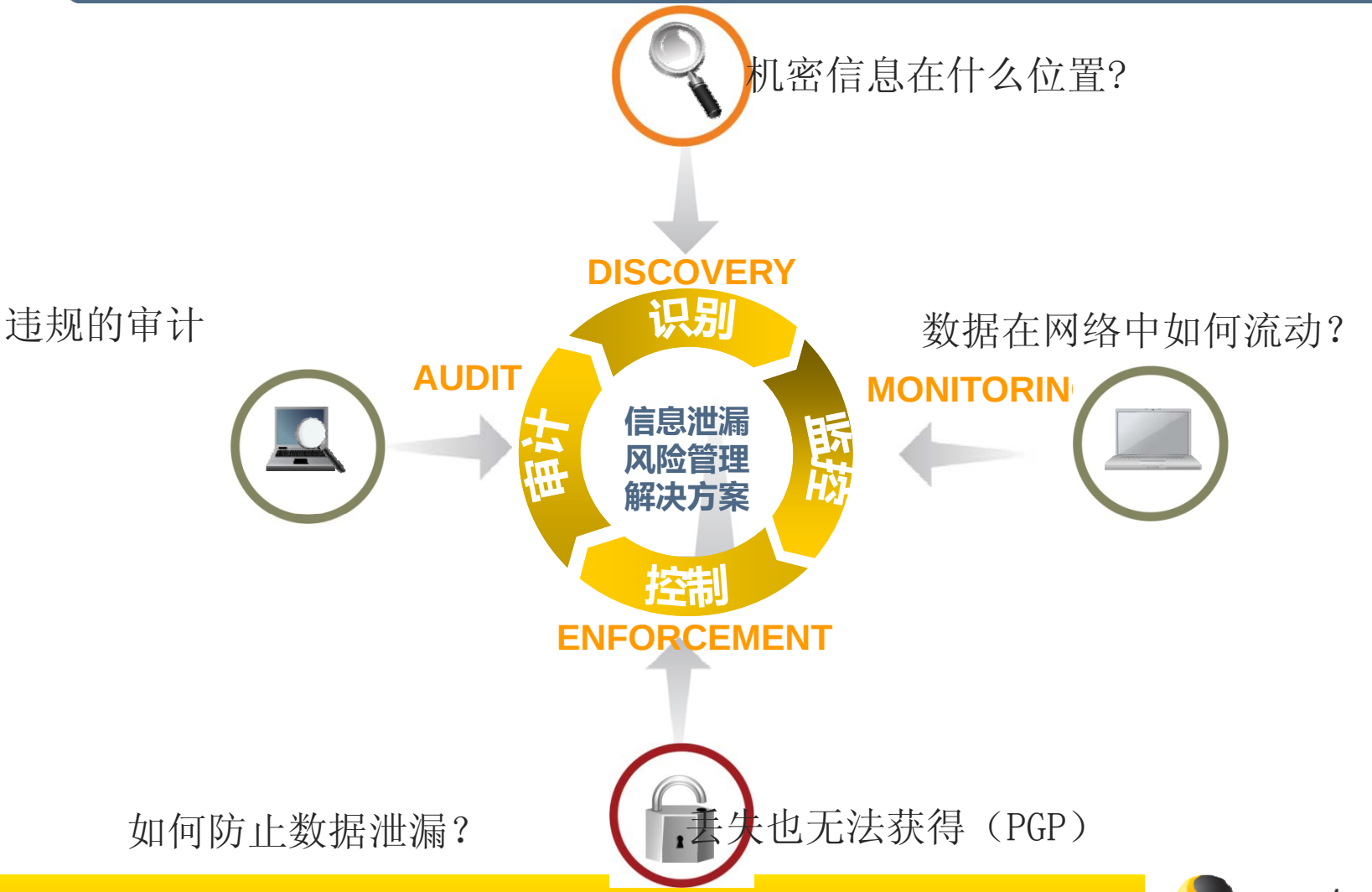
# 专题4：信息防泄漏解决方案

# 对信息防泄漏工作的理解

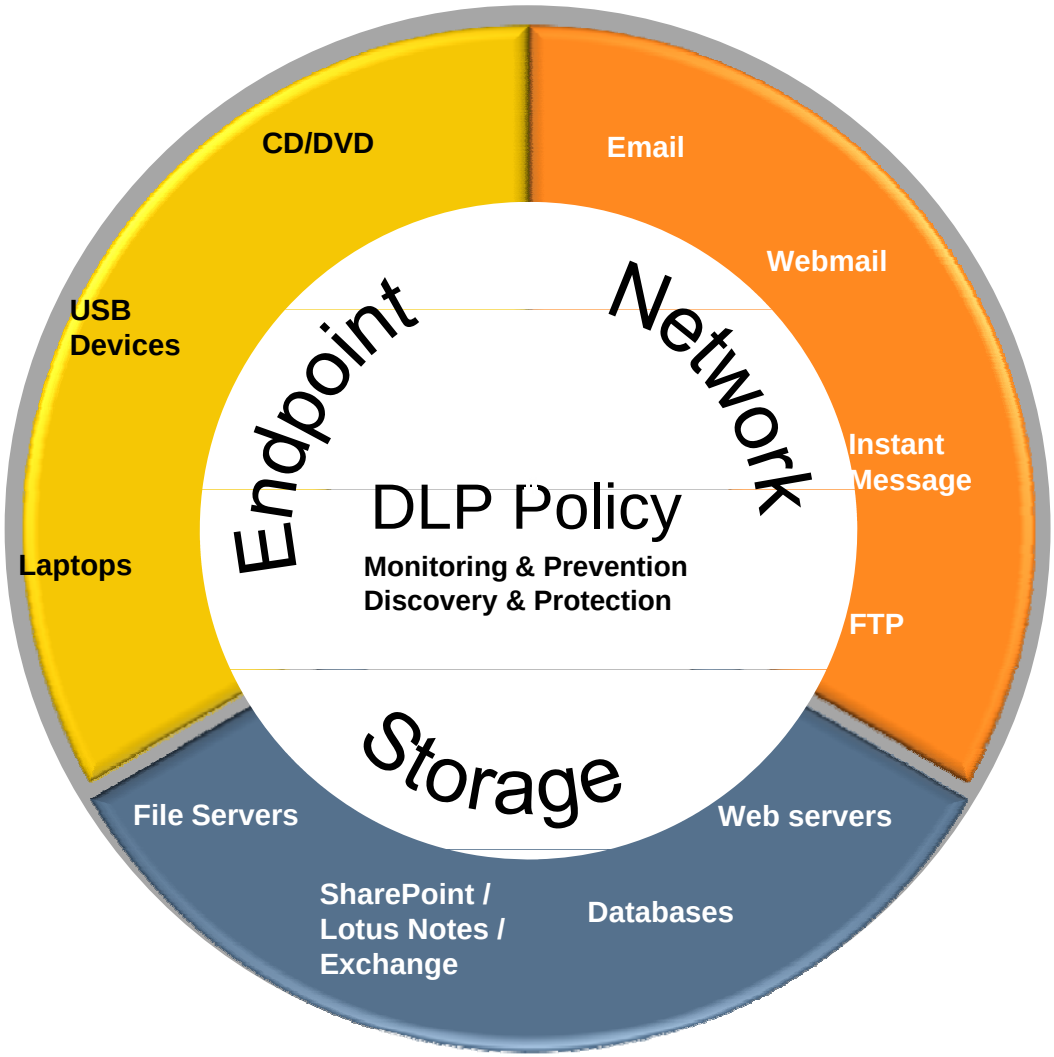


# Symantec防信息泄露解决方案

## DATA LOSS PREVENTION (DLP) + PGP

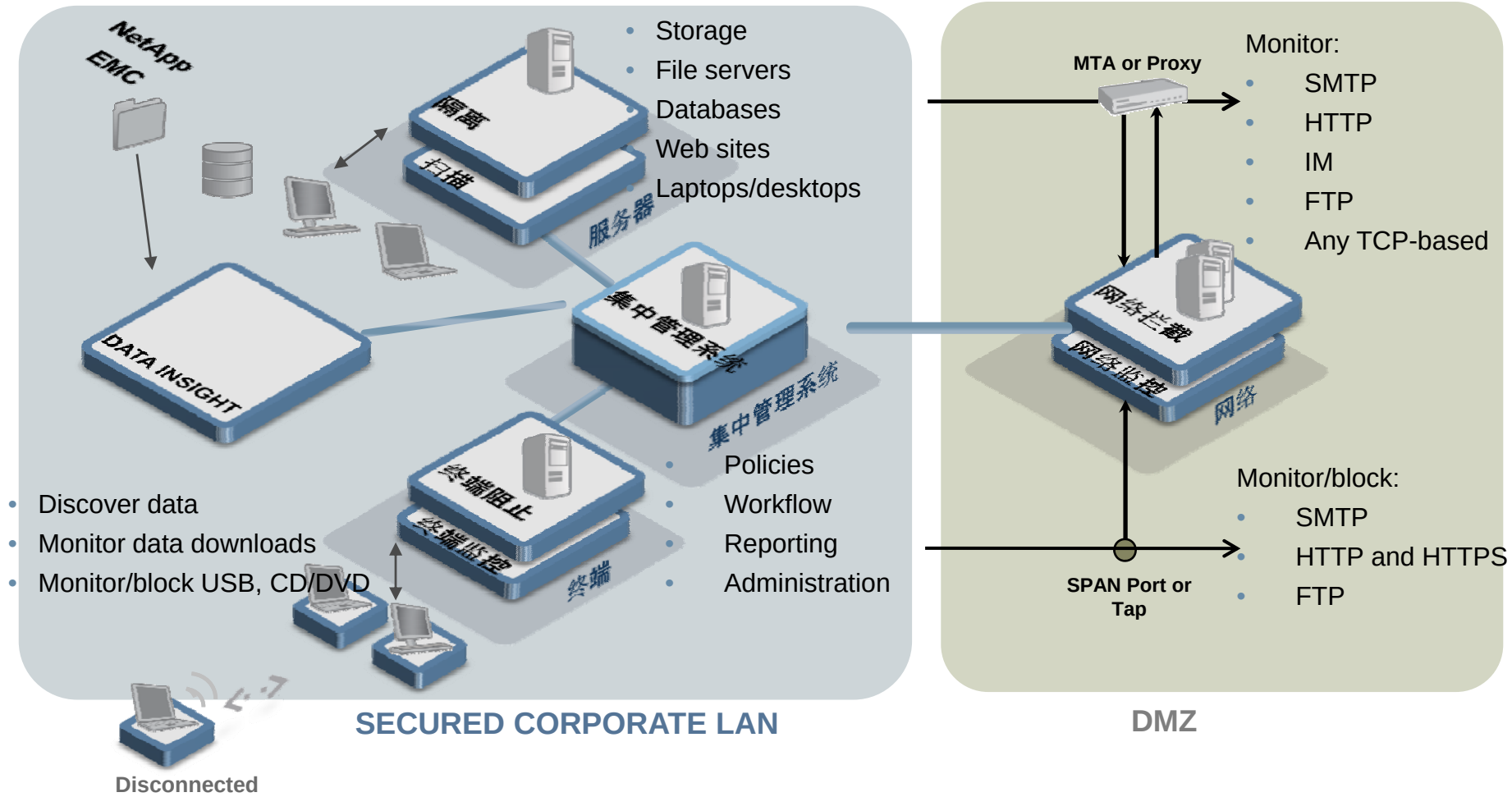


# Symantec DLP对威胁的覆盖

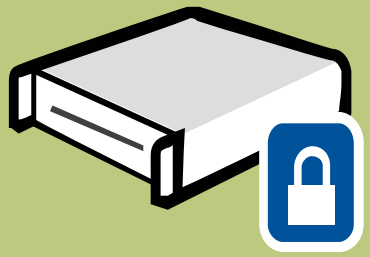


# Symantec DLP 系统架构

服务器（存储）+终端+网络“三位一体”，统一策略



# 完整的加密保护——PGP



**Universal Server™**

Central Management of
Encryption Applications

**整盘加密**
- Laptop & Disk Security

**移动设备加密**
- USB Device & Media Encryption

**邮件加密——桌面**
- Email, File, Disk, & IM Encryption

**邮件加密——网关**
- User-transparent, Gateway Email Encryption

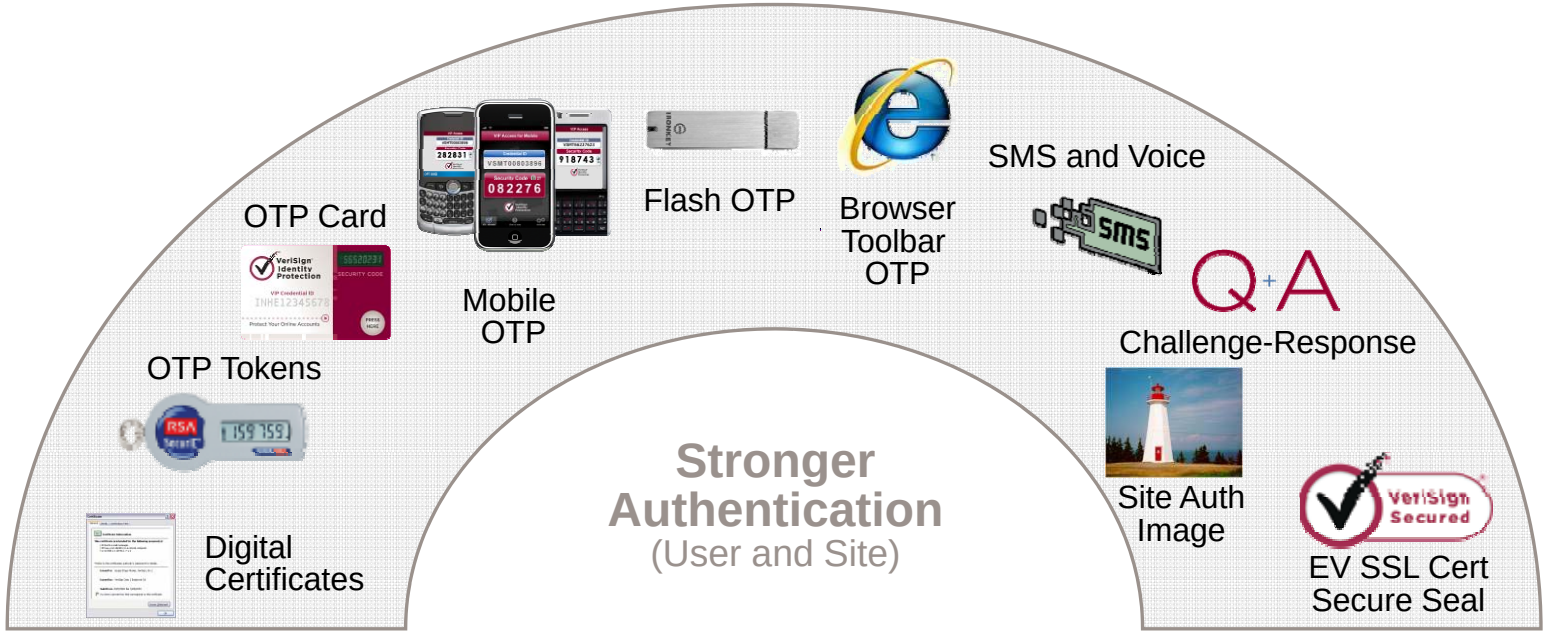
**智能手机解决方案**
- PGP® Mobile
- PGP® Support Package for BlackBerry®

**传输加密—— Command Line**
- Secure FTP/Batch & Backups

**共享文件加密——NetShare**
- Shared Server Storage Security

# 专题5：身份认证解决方案

# 赛门铁克强认证解决方案

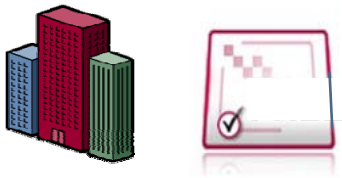



**VIP Fraud Detection and Risk Analysis Service**

**VeriSign® Identity Protection Network**
(fraud intelligence and shared authentication)

# 用户认证和管理产品系列

## Public Key Infrastructure

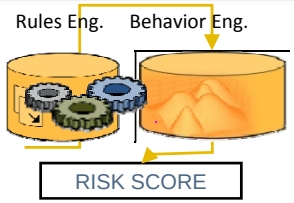


PKI service issues certificates for strong authentication, encryption and digital signing

## VeriSign Identity Protection


Shared cloud-based two-factor authentication solution offering multiple credential choices

## Fraud Detection Service




Risk-Based authentication and software-based fraud detection

### Government

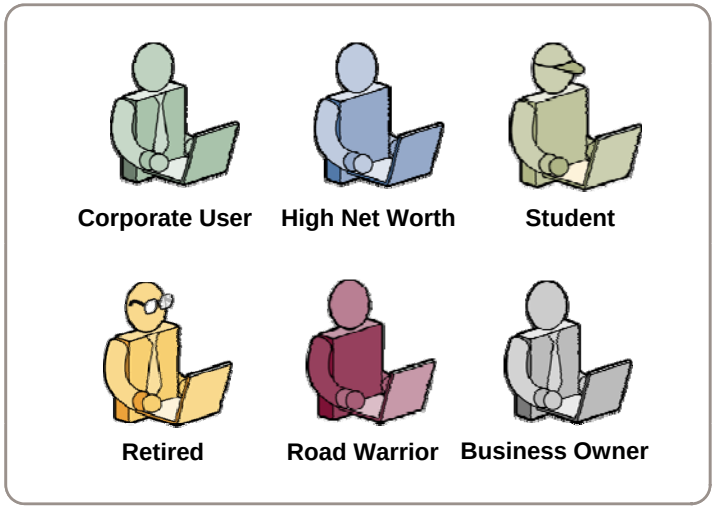
### eCommerce

### Enterprise


### Financial Services

# 在线欺诈检测服务器的概念

用户总是有各种类型




... 黑客的位置飘忽不定

以用户为核心的身份认证和欺诈检测

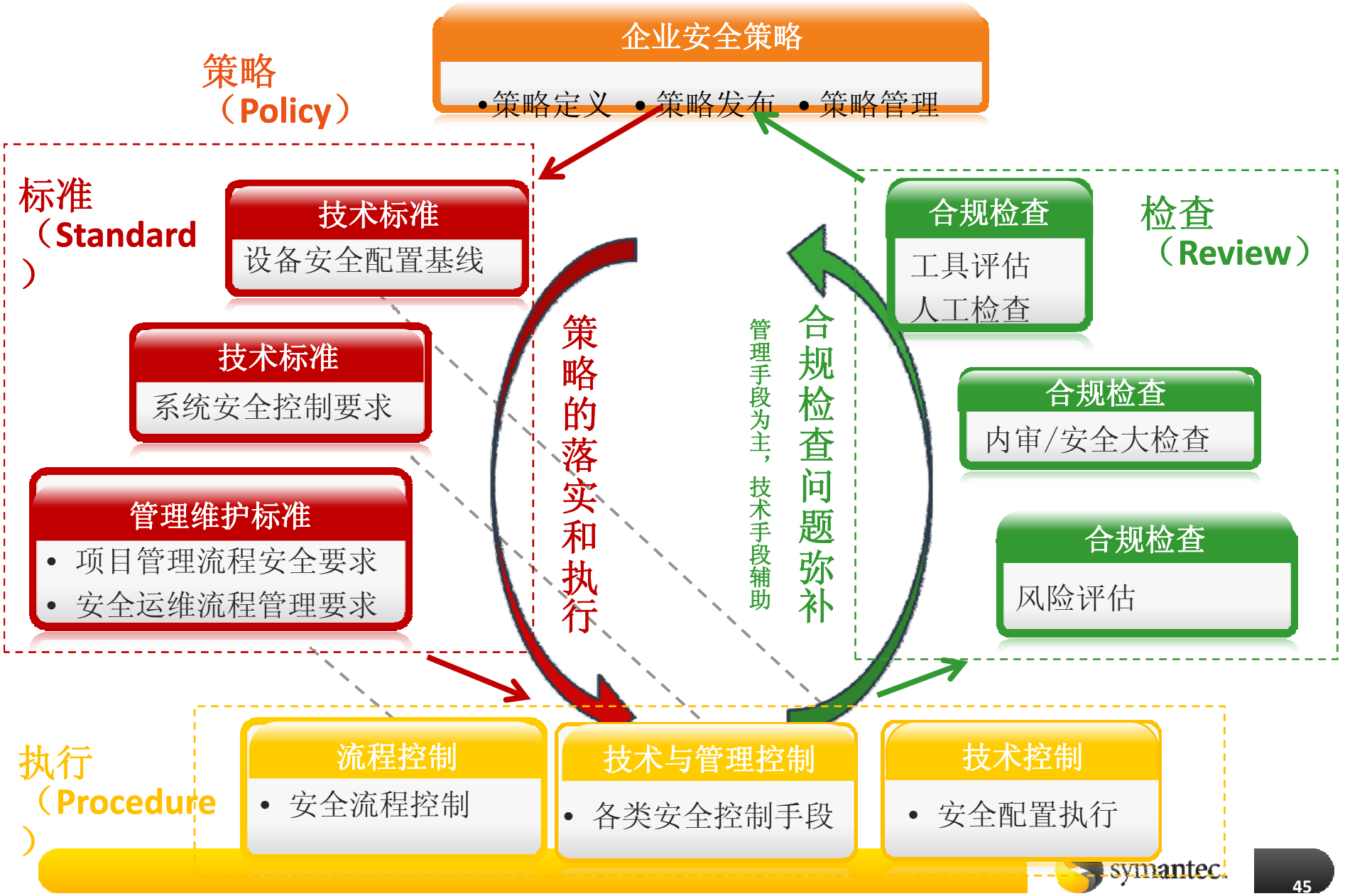
- 对大多数用户是不可见的
- 非侵入式 (不需要安装任何软件在客户端)
- 了解每一个用户独特性
- 学习用户的行为习惯

智能和异常检测

- 学习和适应每一个用户独特行为
- 强制性策略阻止攻击人和欺诈者
- 第一时间阻止新型攻击
- 赛门铁克针对在线攻击独特的视角

# 专题6：法规遵从解决方案

# 企业当前的合规管理的状态



# 合规管理问题和挑战

## 规定规范众多

- 国际：ISO 27001、COBIT、SOX……
- 国内：等保
- 企业：IT运维方面、系统和设备方面（安全基线）、安全子系统方面

## 内外检查审计多

- 对外检查多内外部审计，向多方报告
- 对内覆盖部门多，管理复杂

## 合规及执行状况的可知度（迷惑）

- 管理员：1台unix主机到底应该符合哪些规？做好哪些事情就可以适多个规范？
- 主管和领导：不同策略和标准的实际符合度？

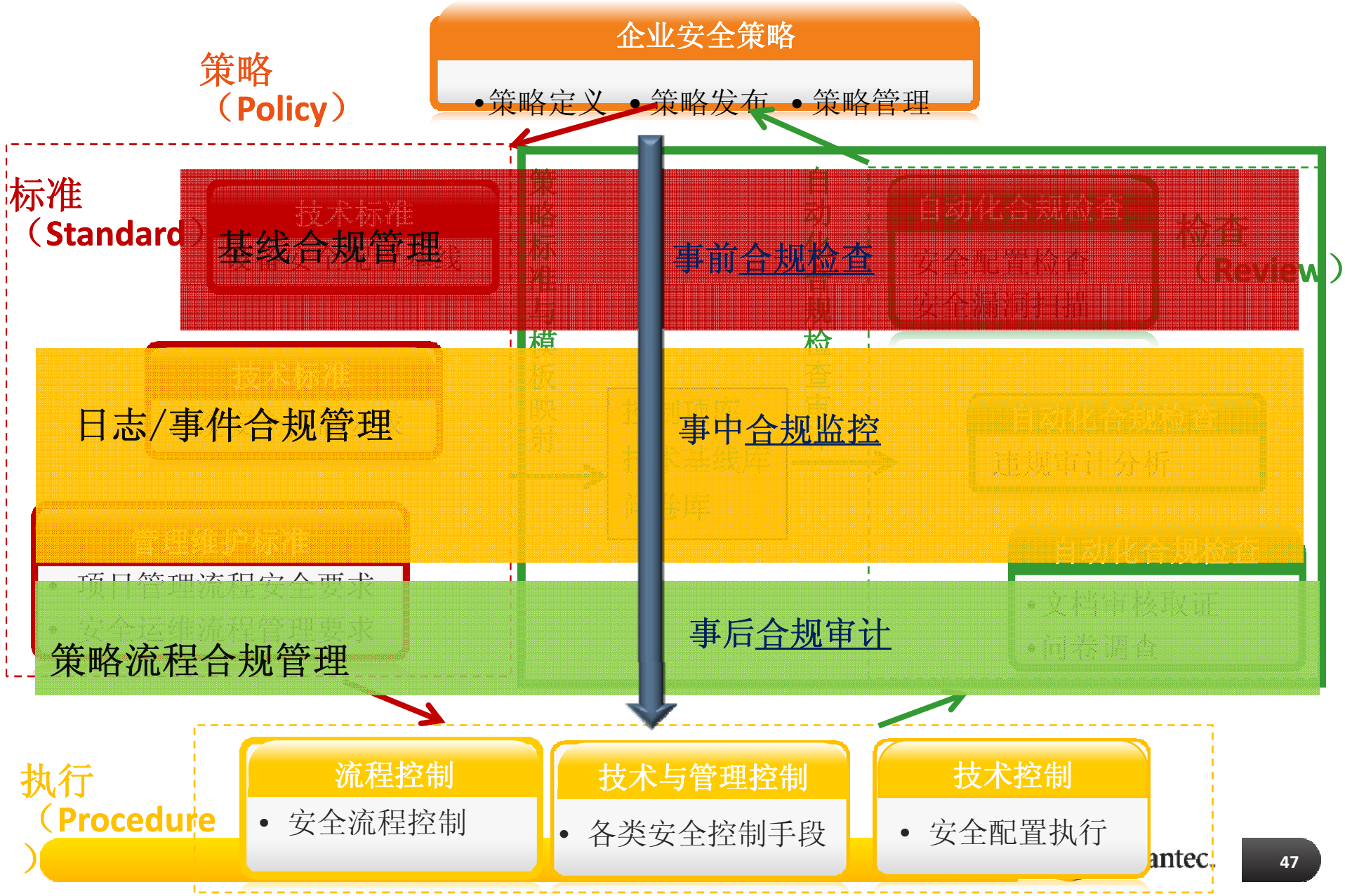
## 安全和遵从成本高

- 应对检查的手动评估或提供证据
- 控制目标重叠导致工作量和成本的增加

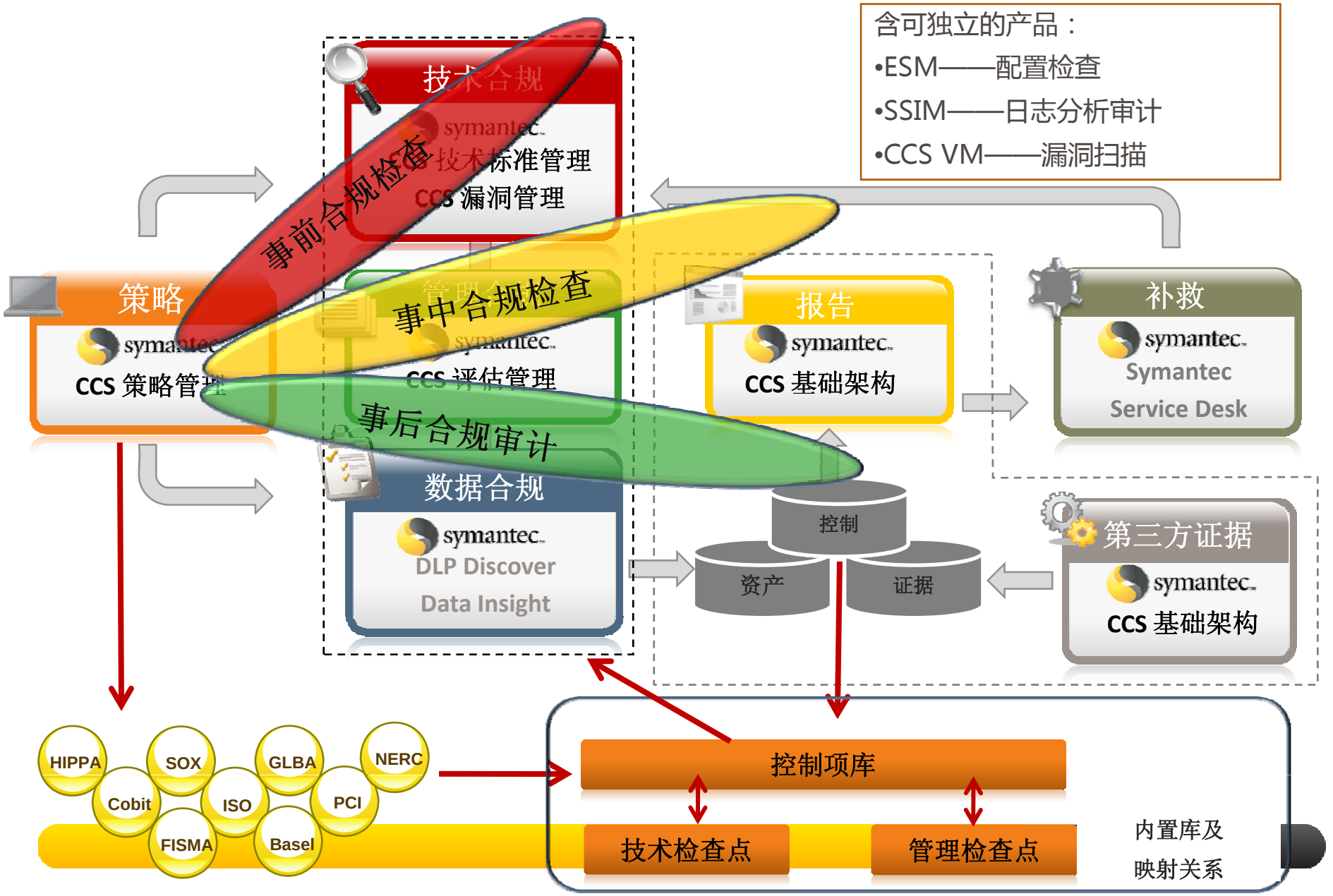
**核心问题：**

1. 缺少统一的合规管理视图
2. 缺少一体化的合规要求标准
3. 缺少一体化的平台支撑和自动化的手段

# 自动化的合规管理形态


企业安全策略
•策略定义 •策略发布 •策略管理
策略
（Policy）
标准
（Standard）
基线合规管理
事前合规检查
检查
（Review）
日志/事件合规管理
事中合规监控
策略流程合规管理
事后合规审计
执行
（Procedure
）
流程控制
• 安全流程控制
技术与管理控制
• 各类安全控制手段
技术控制
• 安全配置执行

# Symantec提供全面集成式的 合规管理解决方案



# Symantec解决方案助力企业安全建设

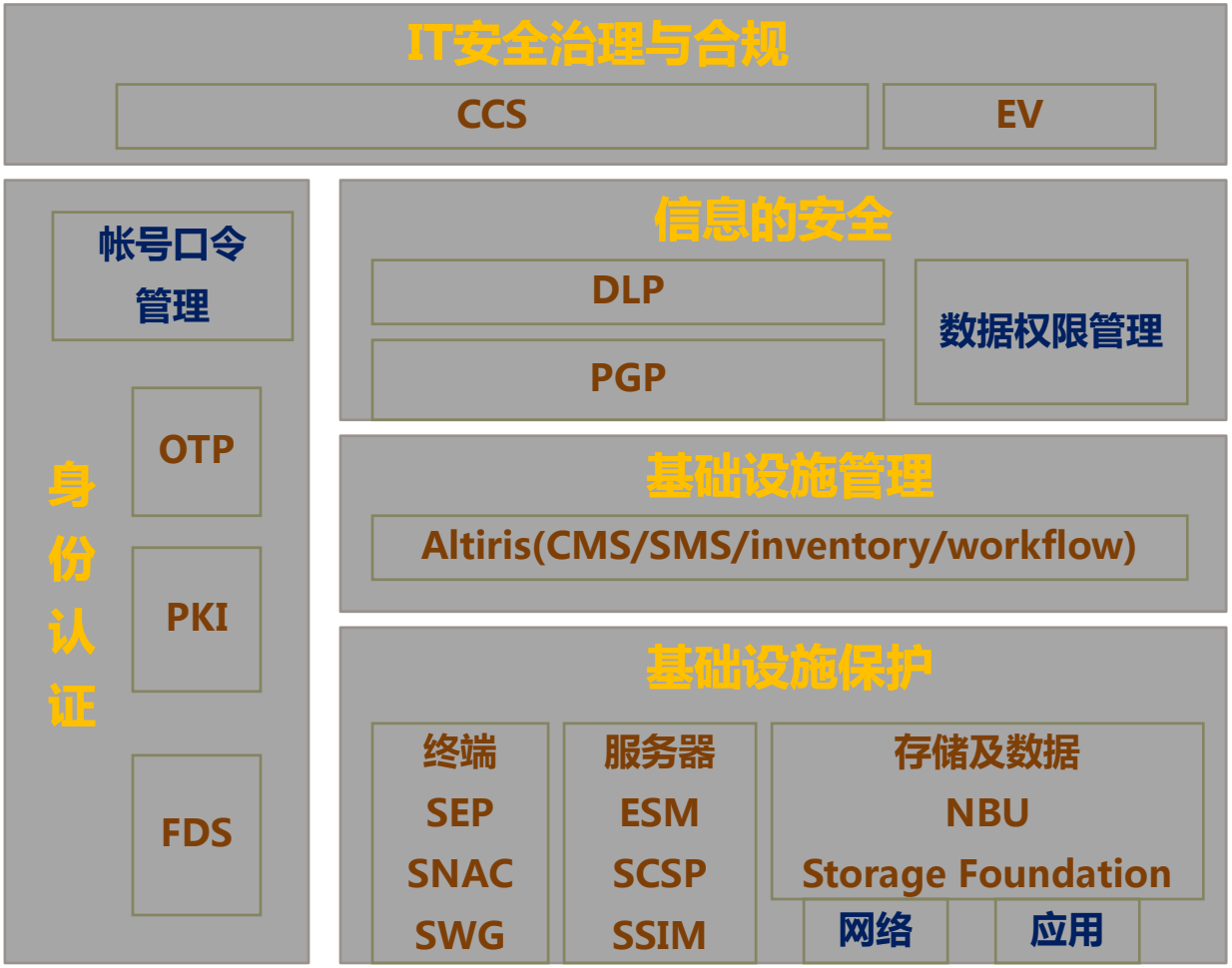
# Thank you!

梁洋洋

Yangyang_liang@symantec.com

18618345220

# 安全框架各层次的建设内容重点


IT安全治理与合规
CCS
EV
帐号口令管理
身份认证
OTP
PKI
FDS
信息的安全
DLP
PGP
数据权限管理
基础设施管理
Altiris(CMS/SMS/inventory/workflow)
基础设施保护
终端
SEP
SNAC
SWG
服务器
ESM
SCSP
SSIM
存储及数据
NBU
Storage Foundation
网络
应用