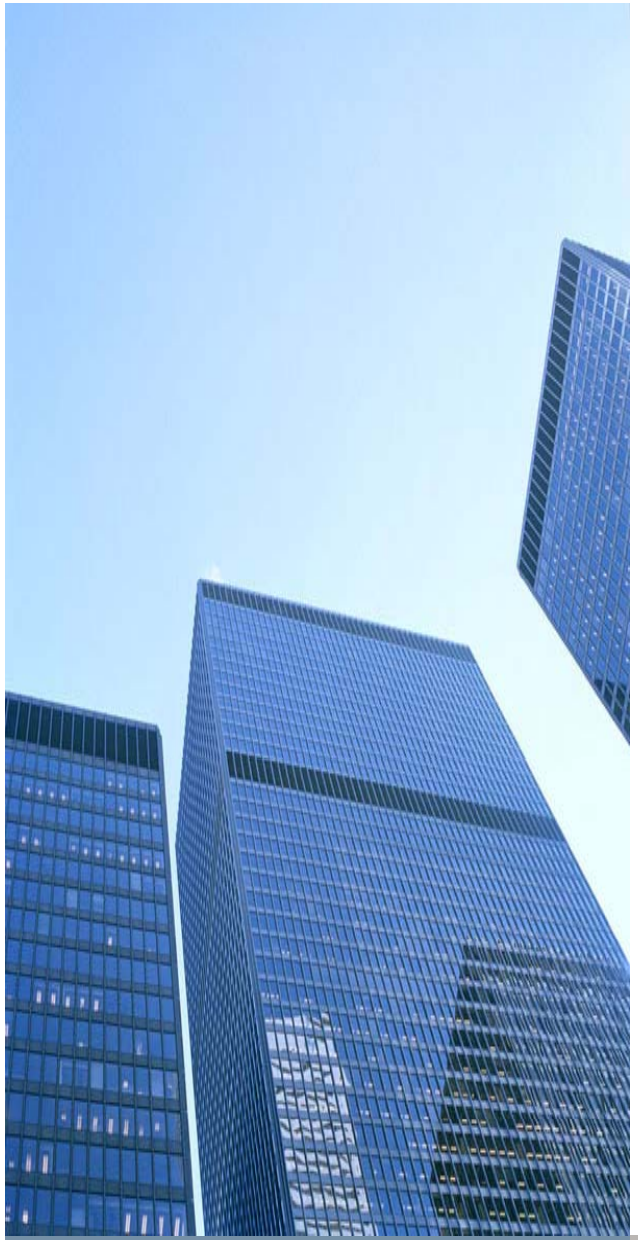
赛门铁克安全管理解决方案

Speaker Name

Mail Address

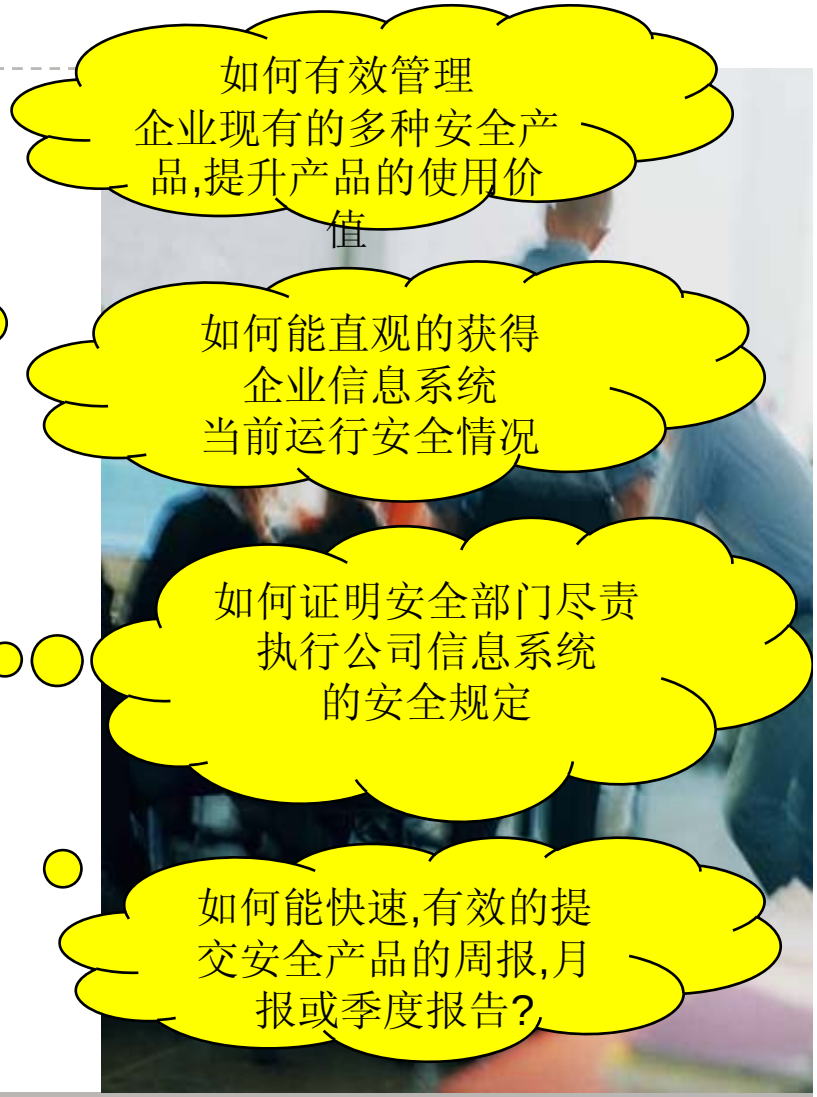


议程

1. 用户面临的的问题
2. 赛门铁克安全管理平台SSIM简介
3. 赛门铁克安全管理平台SSIM架构
4. 总结

用户在安全管理方面遇到的挑战:

- **复杂(CIO)**
  - 不断变换的信息安全威胁,需要采用新的防护技术进行拦截,但是如何实现跨平台,跨产品的统一集中管理
  - 如何证明企业在安全方面的投入产生了应有的回报
- **合规/执行企业安全策略(Security Manager)**
  - 缺少全面的报表统计工具
  - 缺少集中日志保存,存贮方案,在突发安全事件时,很难进行事后取证
  - 需要花费大量的人力,物力,完成外部审计
- **工作效率(IT/安全维护人员)**
  - 防火墙/IDS等安全产品的报警过多,没有时间查看
  - 无法区分安全产品的误报缺少安全专业知识,无法进行跨产品的事故分析
  - 不同的产品,不同的界面,不同的报表格式,需要一段时间来熟悉和管理

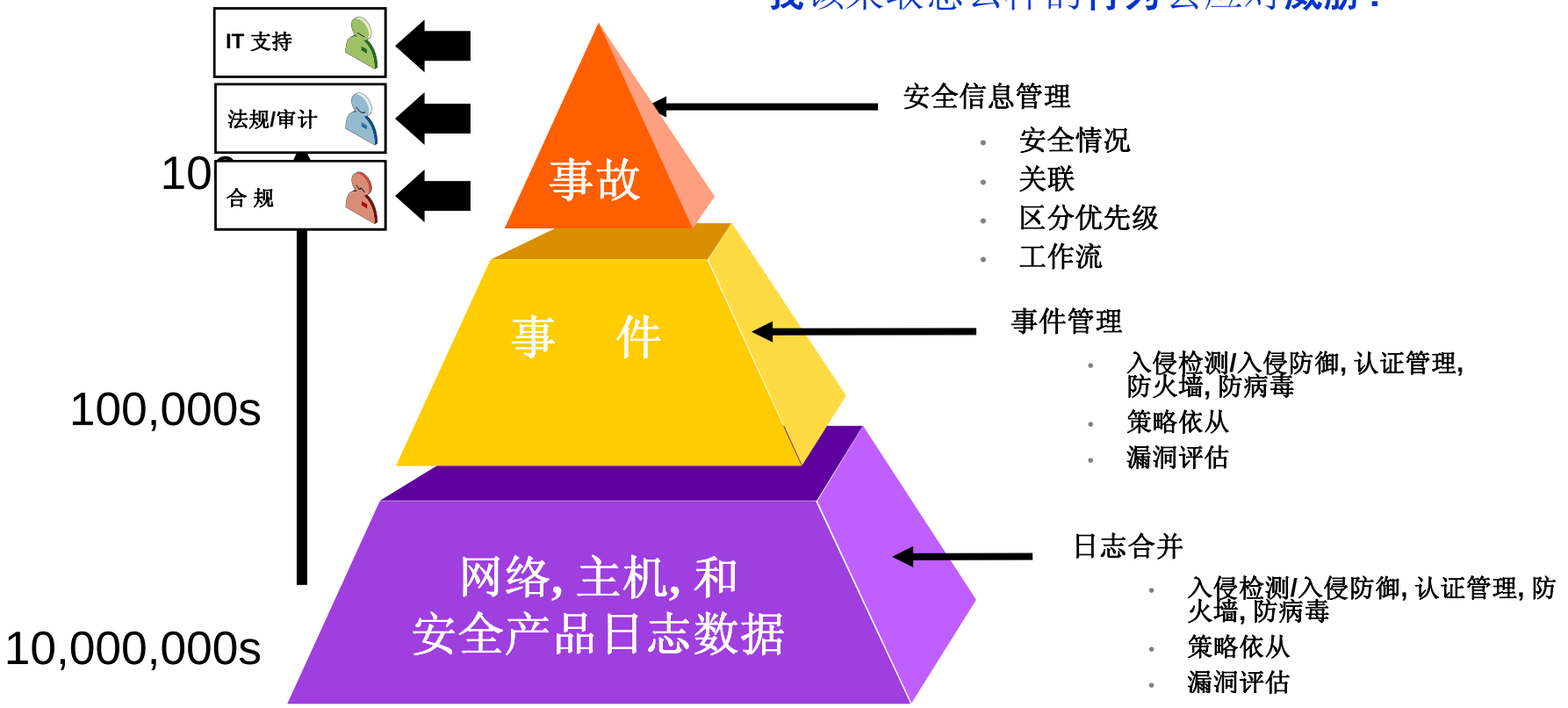


安全管理面临的挑战:

安全信息事件的过载

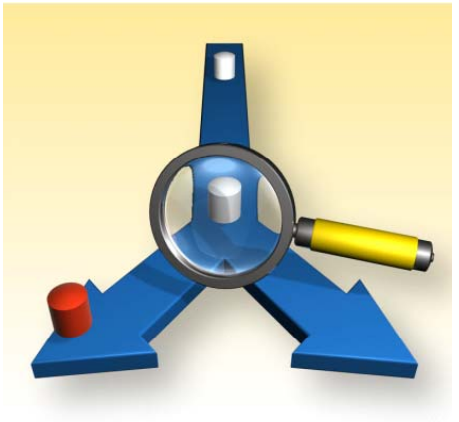
哪些**业务资产**在被**威胁**?

我该采取怎么样的**行为**去应对**威胁?**



某国内电信用户

- **应用/数据大集中 –** 所有应用集中在EDC集中管理,专门的安全管理小组
- **SOX 合规要求 – 不能有效监控用户行为,评估安全风险**
- 同时部署多家安全产品 - Symantec, CheckPoint, Cisco, Microsoft, 安氏…
- 安全信息的事件量
  - **23台防火墙:**
    - 11.7 GB/天 > 513 GB/月
  - **IDS:**
    - 1,600,000 事件/天 > 48,000,000 事件/月



- **通常每天**
  - 安全事故的统计
    - 防火墙和IDS及其它安全产品日志量为6,600,000 条记录
    - 真正与安全相关的有620 条报警
    - 急需用户解决的严重威胁有 2 个.

事件报警与安全威胁的比例: 3,300,000:1

赛门铁克安全管理解决方案

托管服务
监控与管理

解决专业人员和资源
的缺乏

解决经验和实施经验
的缺乏

构建和维护
咨询服务

Deepsight
早期预警和分析

解决安全知识和分析能力
的缺乏

解决技术和人员
的局限性

收集和关联
Security Information Manager

Symantec Security Information Manager

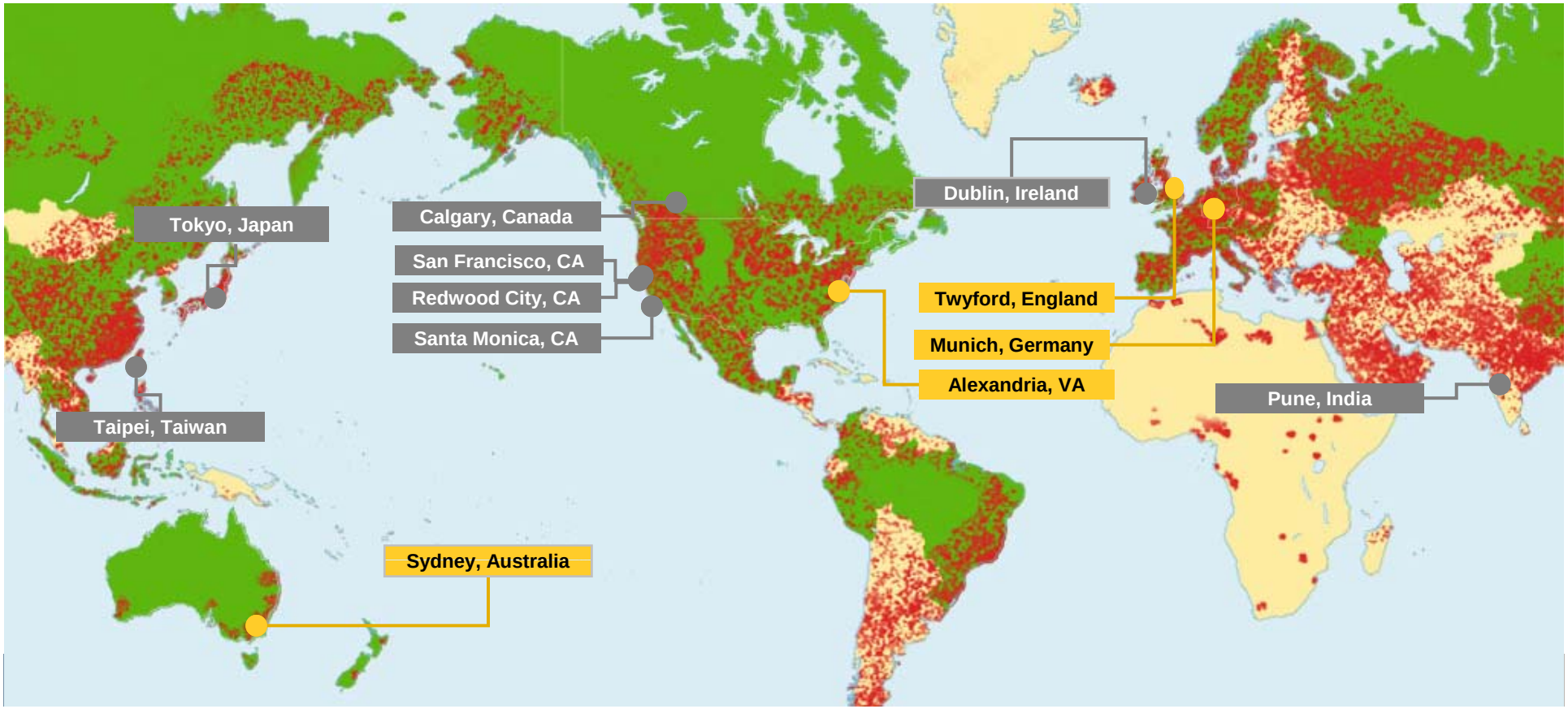
Introducing Symantec Security Information Manager

- Symantec™ Security Information Manager (SSIM) 是安全信息和事件管理的的统一平台,他能帮助用户:
  - 收集并分类安全日志
  - 识别并解决重大安全事件
  - 满足在安全监控和日志存贮方面的审计和合规需求
  - 衡量安全控制的有效性

SSIM 后台安全知识库 – 赛门铁克全球智能监控网络

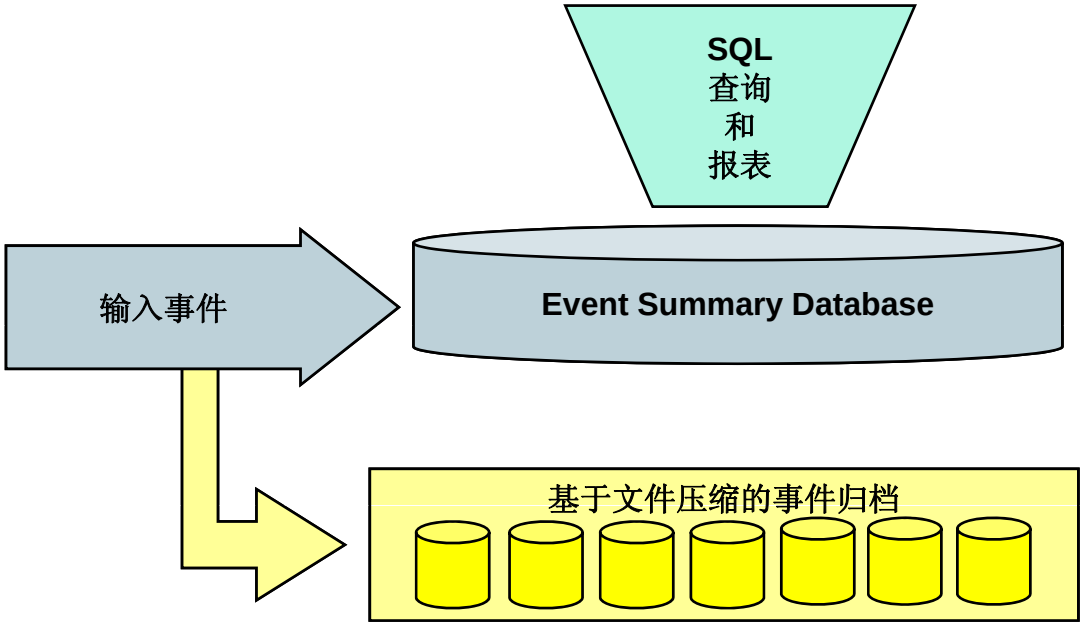
4 Symantec 安全运营中心 + 74 被监控国家 + 40,000+ Registered Sensors in 180+ Countries + 8 个安全响应中心

>6,200 Managed Security Devices + 120 Million Systems Worldwide + 30% of World's email Traffic + Advanced Honeypot Network



事件收集-集中保存事件信息

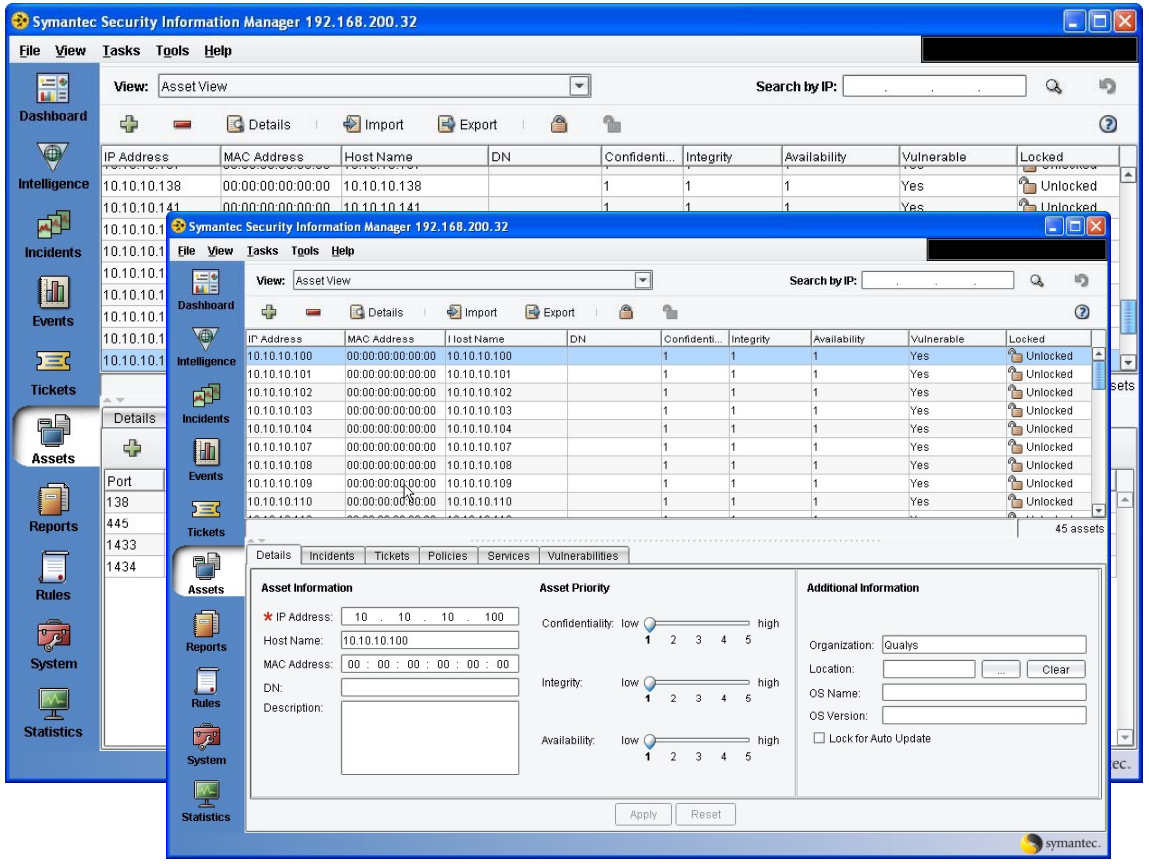
- **集中保存原始日志数据…**
  - 用于事后取证
  - 达到合规要求
- **支持长期日志保存需求**
  - 归档文件同时被压缩保存,压缩比率为50%-80%
  - 灵活的存贮选择 (内置存贮或SAN/NAS/DAS)
- **不再需要DBA**
  - 数据归档和备份更为方便,备份时间和复杂程序较数据库备份都有所减少
  - 归档文件可以用于在线恢复,规则测试和搜索
  - 不再需要数据库的日常维护



提升ROI并降低成本

优先级调整和资产管理

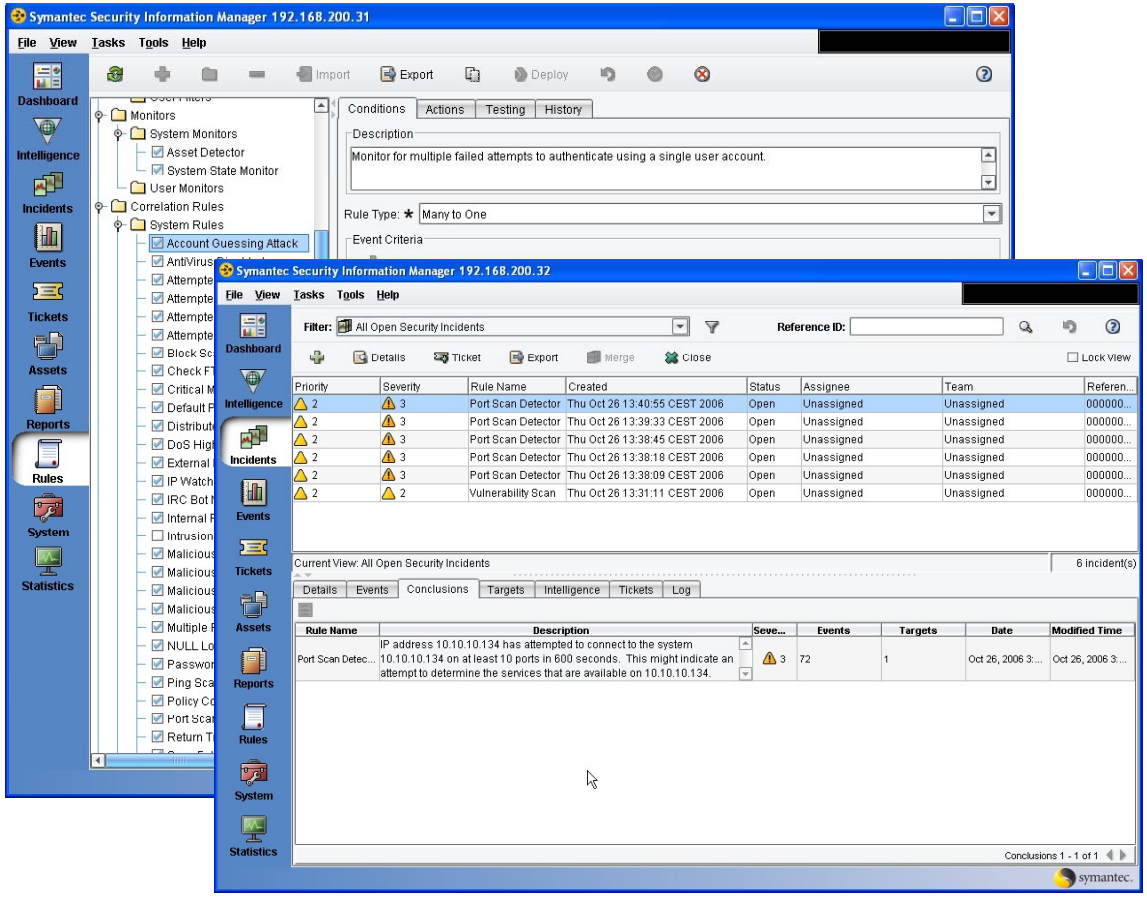
- **紧急安全事件优先级的自动提升或调低,基于:**
  - 业务依赖 (CIA values)
  - 相关的策略和法规要求
  - 开放的端口/服务
  - 漏洞状态
- **通过定制规则,适应用户要求:**
  - 灵活的规则编辑工具
  - 可以调整事件触发的阈值
- **减少误报**
  - 不必再为IDS发出目标地址为Unix主机的Windows RPC攻击报警而烦恼.



只关心发生在关键资产上的重要事件

威胁识别-通过事件关联和事件的规式化

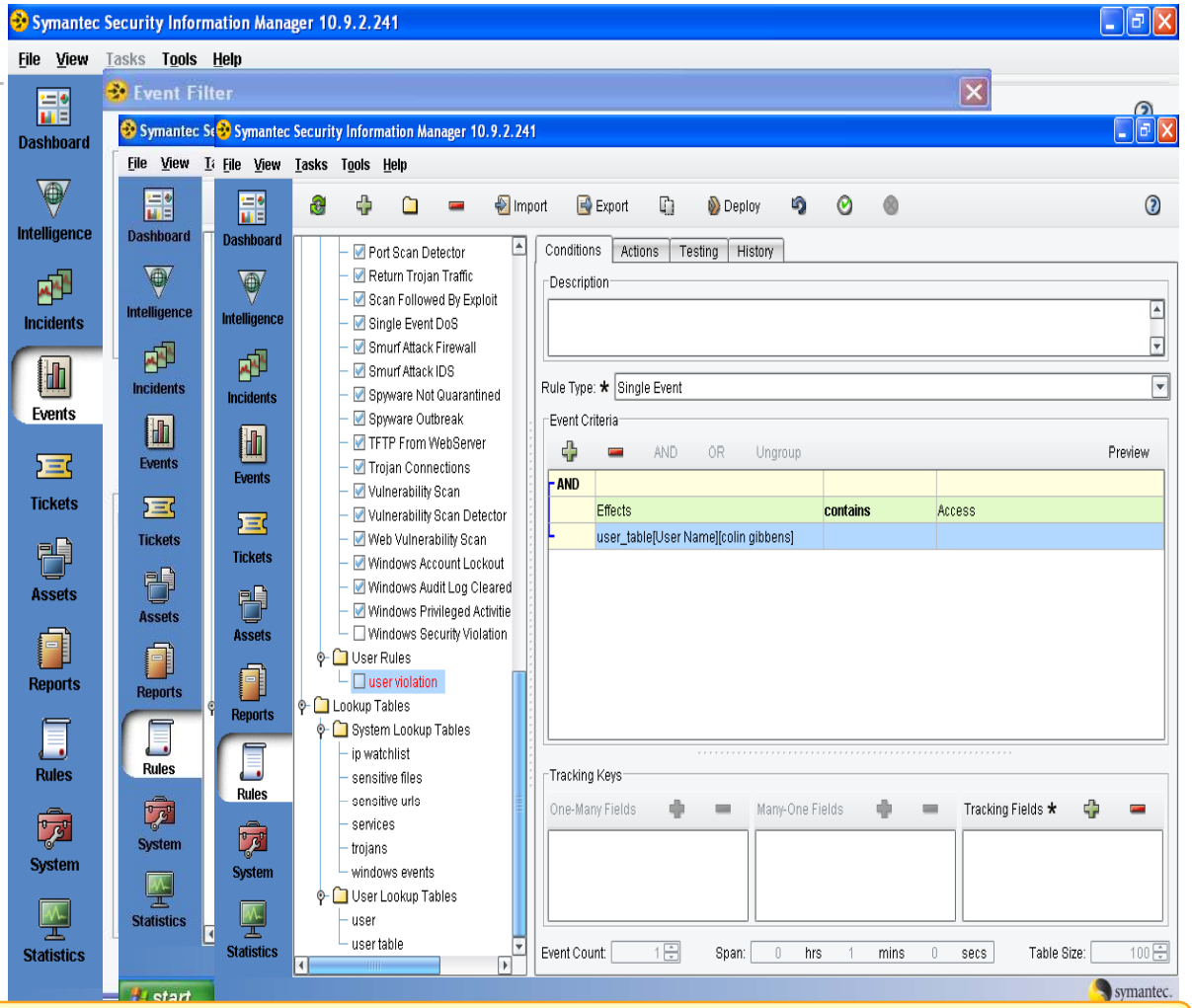
- **简单易用 –** 图形化的规则编辑器, 使得用户能灵活的定制和修修改规则
- **攻击方式统一 –** 事件类型自动分类,根据事件的效果,攻击方法,访问的资源自动匹配关联规则,不必针对新的攻击事件编写特定规则
- **内容监控 –** 监控IP地址和可疑URL访问,数据来源于赛门铁克安全预警服务和赛门铁克安全托管服务
- **提供四十余种默认关联规则 –** 监控蠕虫扩散,病毒,DoS和其它可疑攻击,不用定制,测试或部署任何自定义规则.



Find the needle in the haystack

用户行为的监控

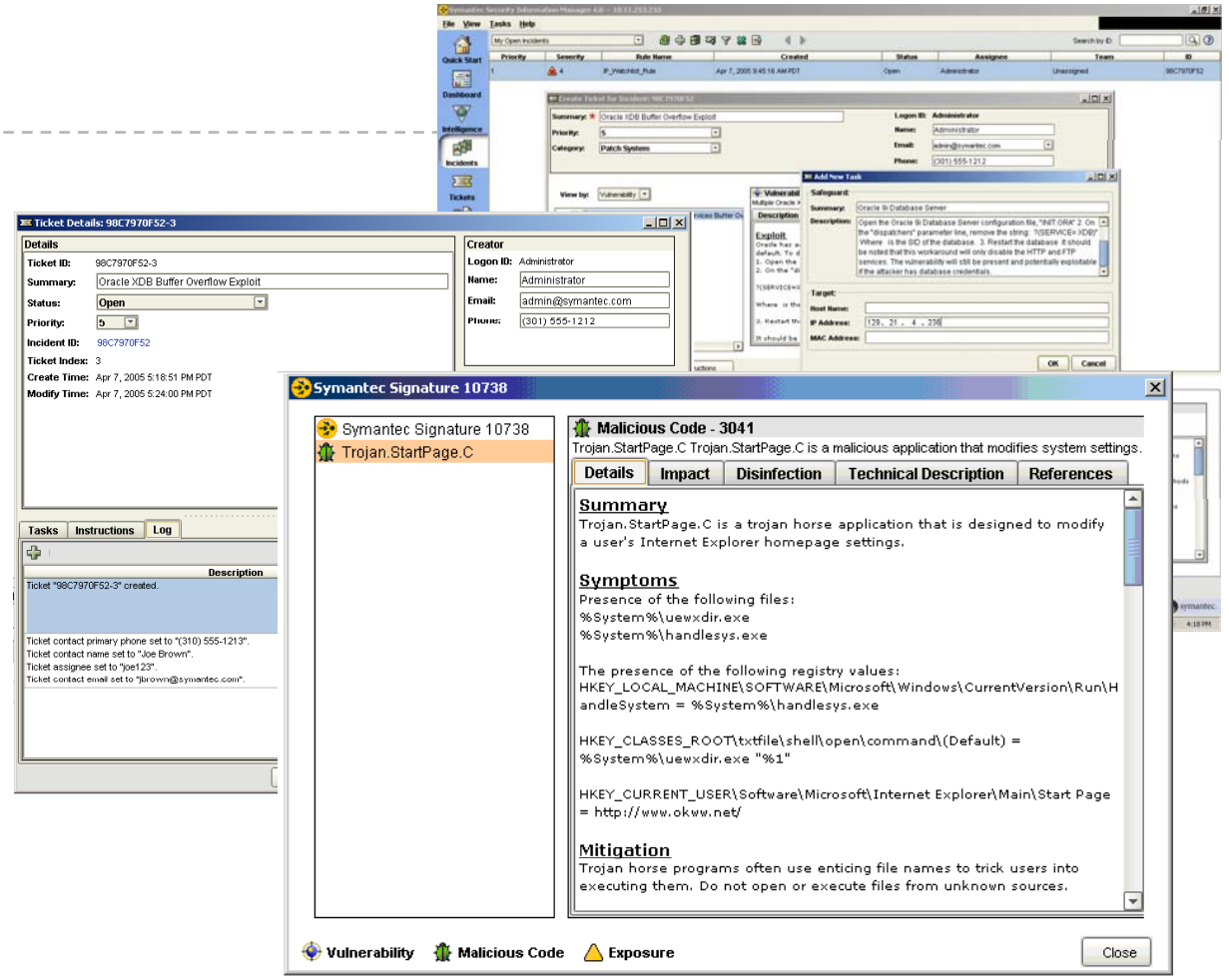
- **用户行为的搜索和查询：**
  - 从不同安全产品(VPN, OS, Firewall, IDS)收集的安全事件中追踪用户行为
  - 事件审计,从历史事件中，发行导常用户行为
- **针对用户行为的关联和提示:**
  - 定制用户表跟踪特定用户的行为
  - 创建特定规则针对特定的用户行为自动触发



发现并报告异常用户行为

工作流管理

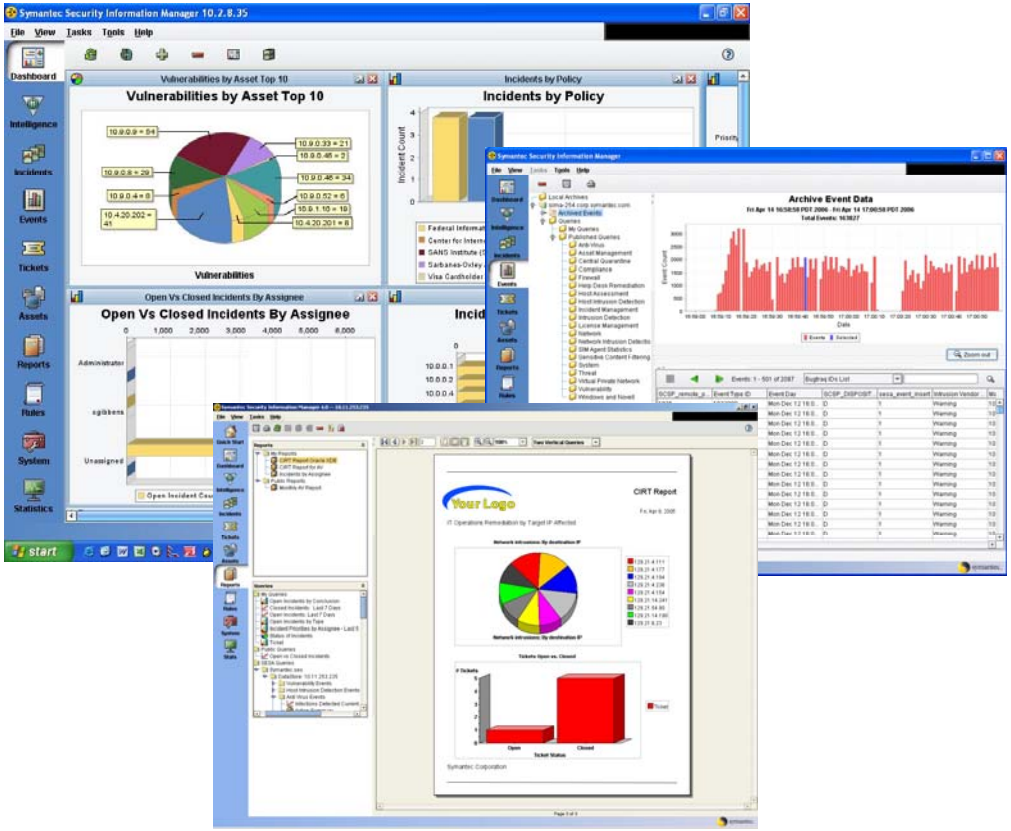
- 通过报警和工作流实现安全事件的响应
  - SSIM支持email, pager, 和 SNMP报警
  - 内建的工单管理也可与第三方的工单管理集成
  - 工单自动指定给特定的用户或工作组
- 为IT运维人员提供安全事件的解决方案
  - SSIM内建赛门铁克全球智能监控网络的知识库并在后台自动更新
- 实现制度化的知识普及
  - 针对特定安全事件的解决方案共享



消除安全与运维之间的间隙

可定制的报表

- 完成事后审计搜索
  - 简单快速的日志复查
  - 生成针对审计人员的报告
  - 自定义查询条件和内容
- 关键报告的自动生成
  - 定制用户登录的仪表板
  - 提供按照时间统计的趋势报表
  - 自动定时生成并分发报告
- **通过查询向导定制报表**
  - **导入用户Logo, 定制页眉/页脚 legends, etc.**
  - **生成多页或集成多种报表的报告**
  - **支持多种文件格的导出 (CSV, pdf, html, xml)**

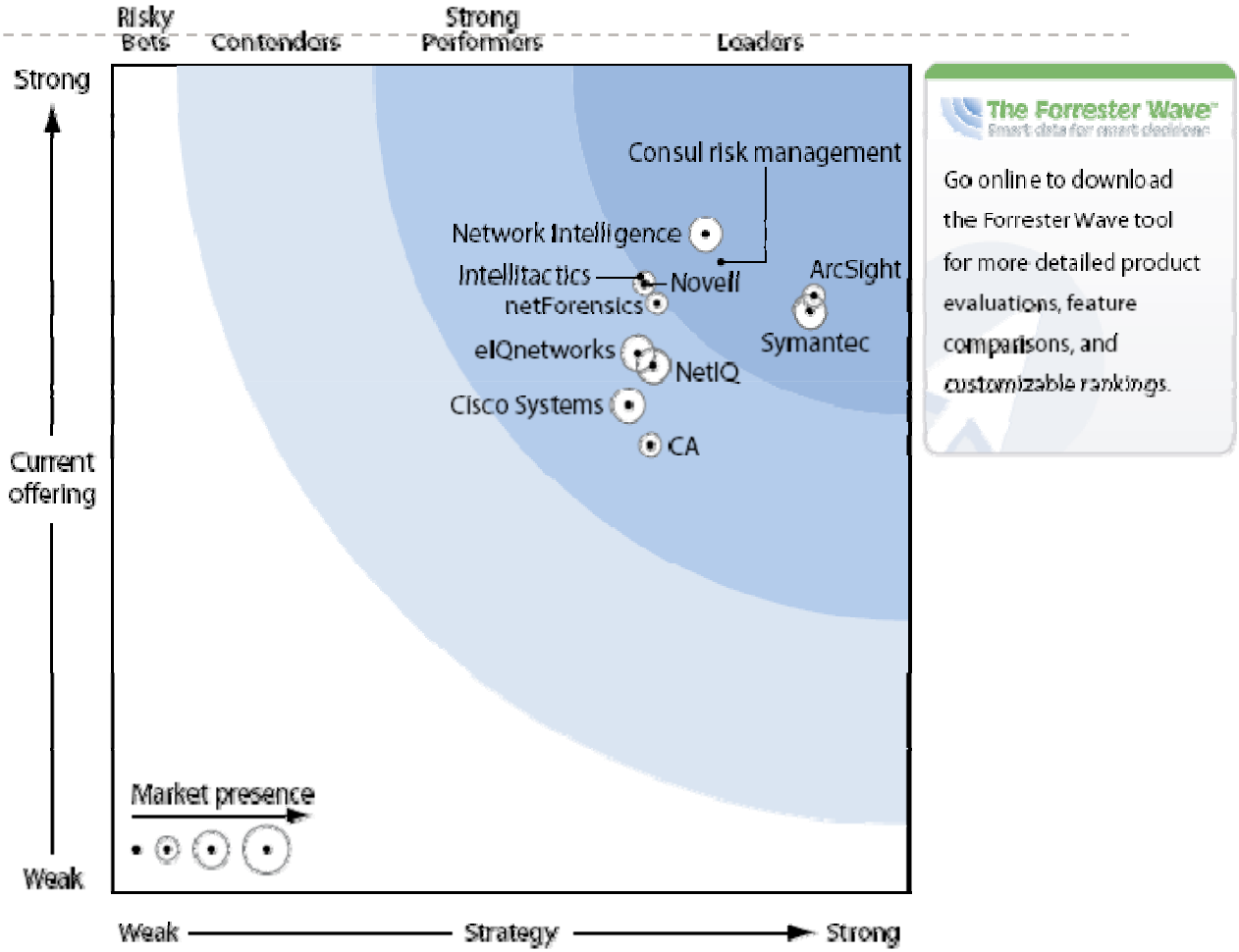


Measure and Report on Effectiveness

The SIM Wave

- **SSIM 4.5 is a Leader in the Forrester Wave**
- Report Quotes
  - SSIM is much improved this year with 4.5
  - SSIM is easier to deploy and configure
  - Improved data management capabilities make it easier to perform historical analysis

Figure 3 Forrester Wave™: Enterprise Security Information Management, Q4 '06



Source: Forrester Research, Inc.

Case Study | Fortune 50 Global Manufacturer

- **Driver:** *Compliance*
  - Compliance teams require proof of a incident response process with a focus on user & access control incident management
  - Needed a mechanism to tie together a broad solution of several Symantec products
- **Solution:** *Global SSIM Deployment*
  - 9 Appliance in 6 Locations across US, EMEA and JPAC
  - SSIM turns millions of events into a handful of incidents daily, processing 7000+ EPS
  - Professional Services delivered a tuned solution
- **Result**
  - Limited Security Analyst team addresses top concerns
  - Incident Response Process is fully documented and reports to auditors demonstrate due care

Large deployment driven by Compliance

Case Study | Novacoast

- **Monitors & correlates Symantec Network Security and Mail Security & dozen third party security devices**
- **Cost savings:**
  - SSIM savings: $53,000 per year
  - DeepSight savings: $41,000/year

"We used to spend seven hours a week doing a close analysis of bulletins about Internet attacks and vulnerabilities.

Now we spend maybe an hour a week. DeepSight is saving us $41,000 a year."

Adam Gray

Chief Technology Officer

Novacoast Inc.

SOLUTION AT A GLANCE

Business Drivers
- Maintain competitive edge by increasing network security, minimizing potential disruption
- Reduce total cost of ownership of security solutions

Technology Challenges
- Centralize and correlate data from multiplatform, multivendor security solutions
- Simplify and centralize security monitoring and reporting
- Reduce spam and reduce time spent administering antispam efforts

Solution
- Symantec network security and email security solution with correlated security event reporting

Symantec Products
- Symantec™ Network Security 7100
- Symantec™ Network Security 4.0
- Symantec™ Security Information Manager 9500
- Symantec™ Mail Security 8200

Technology Environment
- Applications: Sage BusinessWorks accounting software, JBoss Application Server, Novell GroupWise, and a number of home grown applications
- Server Platform: Dell 1750, 1850, and 2850 servers running SUSE Linux Enterprise Server (12 total) and Novell NetWare (3 total)
- Storage: Dell 6TB tape library

Symantec Services
- Symantec DeepSight™ Threat Management System
- Symantec Education Services

Event Collectors - Over 100 Supported Products (partial list)

Intrusion Detection/Prevention
Symantec Network Security (SNS)
Symantec HIDS
Symantec ITA
Snort
Symantec Sygate
Symantec Critical System Protection
Cisco IDS
Cisco Security Agents
TippingPoint NIPS
Enterasys Network Dragon
eEye Retina
JuniperIDP
ISS Siteprotector
McAfee Intrushield
SourceFire

Web servers, Filters and Proxies
Apache Web Server
IBM Websphere
Bluecoat Proxy
Microsoft ISA
Microsoft IIS
Sun One WebServer

Vulnerability/Policy Scanners
Symantec ESM
Symantec Bindview
Nessus
nCircle
Qualys QualysGuard
StillSecure VAM

Databases
Oracle Security Logs (9i & 10g)
MS SQL Server Logs

Firewalls
Symantec Gateway Security
Cisco PIX
Cisco FWSM
Nokia FW
Juniper NetScreen Firewall
Checkpoint Firewall-1
Nortel Contivity
Fortinet Fortigate
SunScreen
Microsoft Windows Firewall
Microsoft ISA

Operating systems
Microsoft Windows Event Log
Solaris OS Collector
Sun BSM
SUSE Linux
Debian Linux
RedHat Linux
IBM AIX
HP/UX
Tandem
SELinux
IPTables

Identifty Management
Microsoft Windows DHCP
Microsoft Operations Manager
Microsoft Active Directory
RSA SecurID
Cisco ACS

Routers, Switches and VPN
Cisco IOS
Juniper VPN
CyberGuard
Cisco VPN 3000 Concentrator

Enterprise AV Solutions
Symantec AntiVirus
Symantec Client Security
Symantec Mail Security for Exchange
Symantec Mail Security for Lotus Domino
Symantec Mail Security for SMTP
McAfee EPO
McAfee GroupShield
McAfee VirusScan
Trend Micro Control Manager (TMCM)
Trend Micro OfficeScan
Trend Server Protect Information Server
Trend Interscan Messaging Security Suite
Trend Scanmail for Exchange
Trend Scanmail for Notes
Trend Interscan Viruswall
Trend Interscan Web Security Suite

Other
Cisco Netflow
Fox Server Control
Blue Lance LT Auditor
PassGo UPM
Kiwi Syslog
Generic Syslog
Symantec Cyberwolf
Symantec Wholesecurity

Security Information Manager Architecture

赛门铁克SSIM产品硬件型号

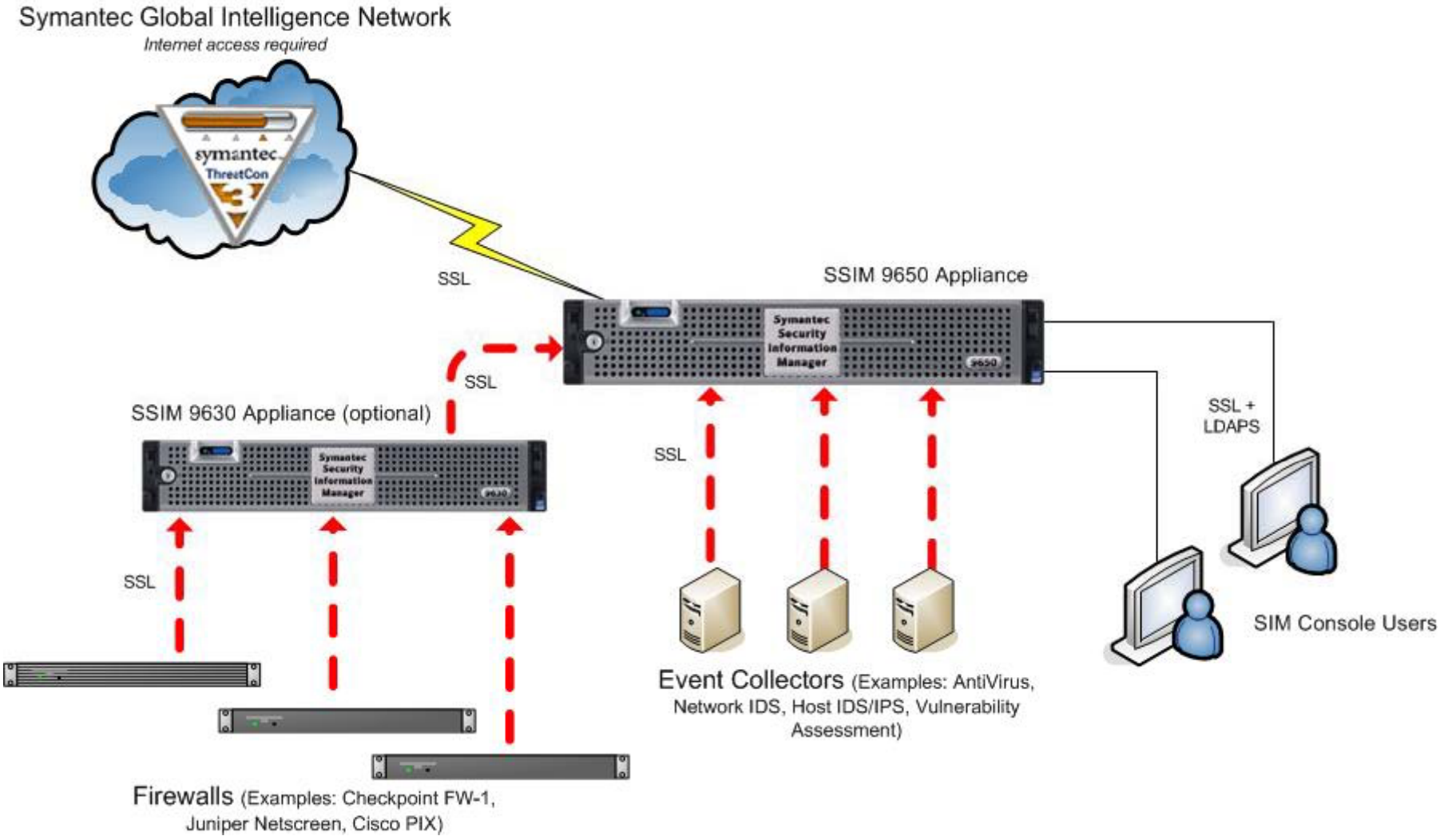
- 事件关联设备 9650
  - 满足用户事件规格化,过滤,合并,关联,存贮,监控和管理的要求

- 事件收集设备 9630
  - 可选型号,用于事件的规格化,过滤,合并防火墙,IDS和其它安全产品的事件信息

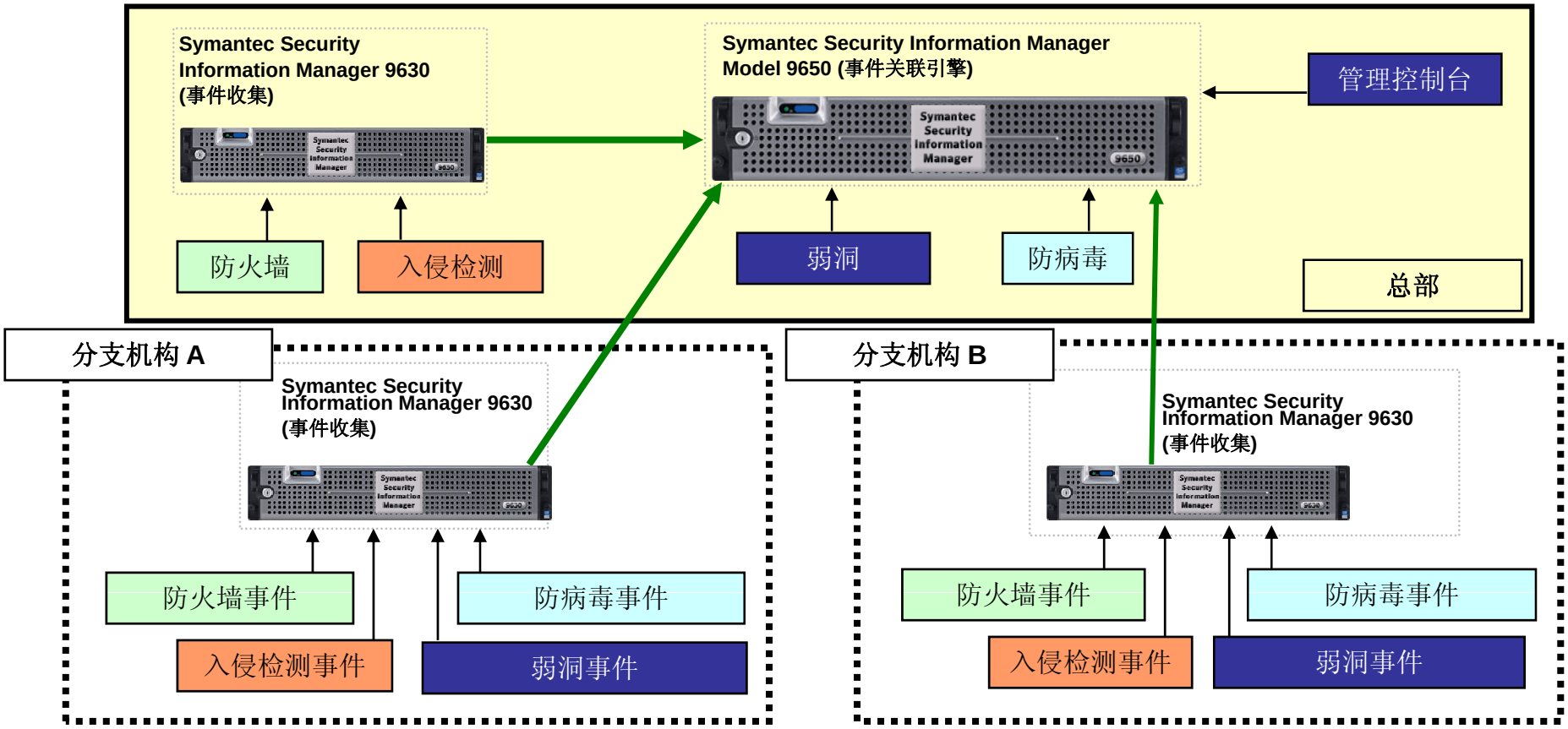
灵活的选择和简单的部署方式

- *两种设备都内置了针对 CheckPoint, Cisco PIX, Juniper NetScreen, SNORT, Unix Syslog 和通用 Syslog 事件收集器.*

Symantec Security Information Manager 部署方式

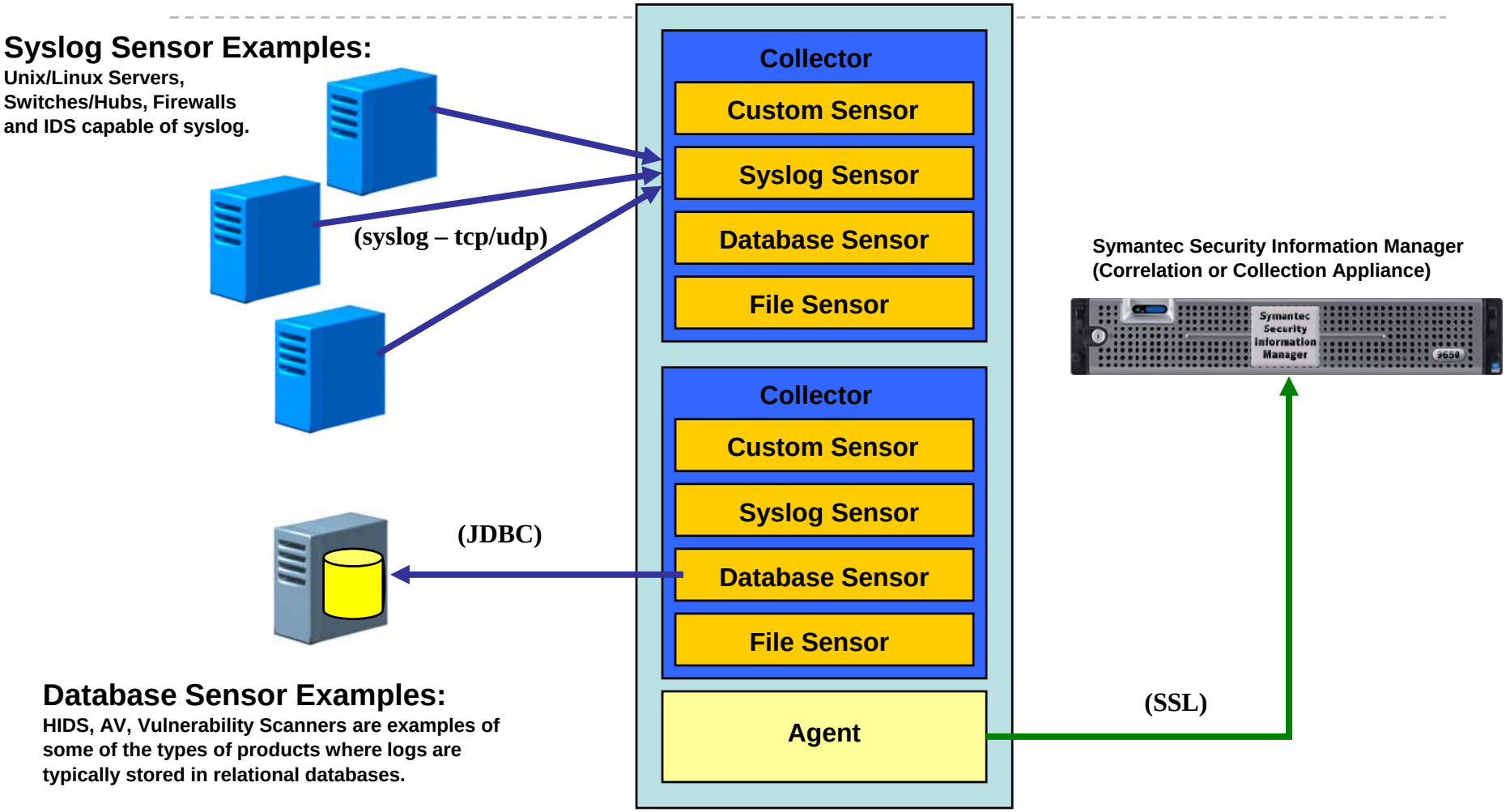


部署方案 2: 两级部署

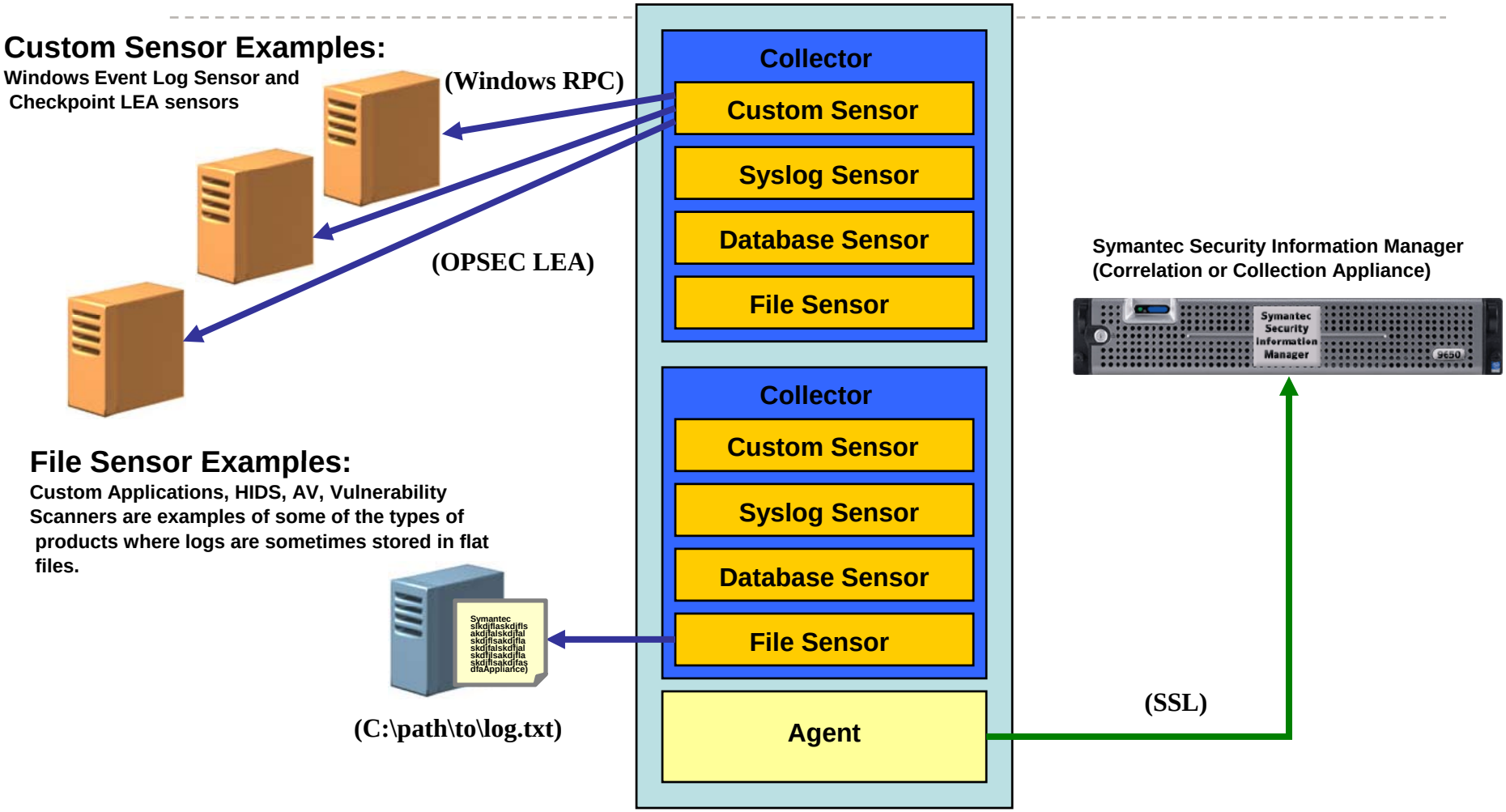


灵活的基于角色的访问控制和数据管理

Collector Architecture: Syslog and Database Sensor Examples



Collector Architecture: Custom and File Sensor Examples



Summary – Why Symantec?

- 全球最大的信息安全产品厂家,不仅提供完善的产品,还提供全面的相关服务.
- 灵活的部署方式,即插即用.
- 不光提供满足合规/审计要求的事件存储,还能智能关联,分析,发现新的安全威胁
- 集成赛门铁克全球安全监控网络的安全知识库并7x24持续更新

symantec.

Keep your business
Up, Running, and Growing,
No Matter What Happens.

Thank You!

Appendix

SSIM 4.5的新增功能

- 长期的日志和事件保存
  - 针对事件审计和合规要求提供长期日志保存的能力
  - 提供多种外部存贮设备选择 DAS, SAN, NAS and NetBackup certification
  - 提升了事件保存和查询的效率
- 增强的合规,风险和安全管理报表功能
  - 提供上百种通定义报表满足用户的报表要求，并提供工具由用户自行定制
  - 报表能自动的定义后台统计，并分发给指定人员
- 强化的企业部署管理能力
  - 细化的基于角色的访问权限控制
  - 通过新的事件存贮机制提供整体性能
  - 提供基于Web的API 接口用于安全访问和更新设备中的数据信息
    - 通过API发布资产,事故和工单信息或与第三方工单系统,资产管理或报警系统集成
- 提升风险识别能力
  - 通过定制规则发现异常行为
  - 通过赛门铁克全球智能监控网络，后台更新安全知识库

Key Benefits of AntiVirus Integration

- **Enhanced Threat and Virus mitigation content**
  - Provides AntiVirus administrators with the near real-time, vulnerability, outbreak, and safeguard information needed to minimize the risks and costs associated with malicious code
- **Workflow allows you to manage outbreaks**
  - Automates & bridges the gap between IT security, and AV Desktop administrators for faster remediation of threats
- **Proactive notification of virus and spyware infections and outbreaks**
  - Provides near real-time email, pager and SNMP based alerting
- **Monitoring for Expanded Threats with multiple attack vectors**
  - Correlates information from multiple AV and Client protection technologies to provide a threat based view of the customer's environment

安全管理工作流

识别 → 区分优先级 → 响应 → 复查