IBM Global Services

统一通信协作平台的安全解决方案

李明

IBM ISS 技术经理

IBM Internet Security Systems

Ahead of the threat.™

李明 – ISS 产品经理

- 现职与经历
  - IBM ISS 产品经理
  - ISS China 高级技术顾问
- 工作经验
  - 信息安全解决方案设计
  - 产品管理
  - 项目管理
- 参与的部分重要项目
  - 中国移动总部互联网紧急响应项目
  - 北京移动IDC安全项目
  - 江苏移动BOSS安全项目
  - 广东联通网管与安全项目
  - 广发银行服务器安全项目
  - 中石化ERP安全项目
  - 中远集团网络中心安全项目
  - 中国邮政综合网安全防范系统

交流内容

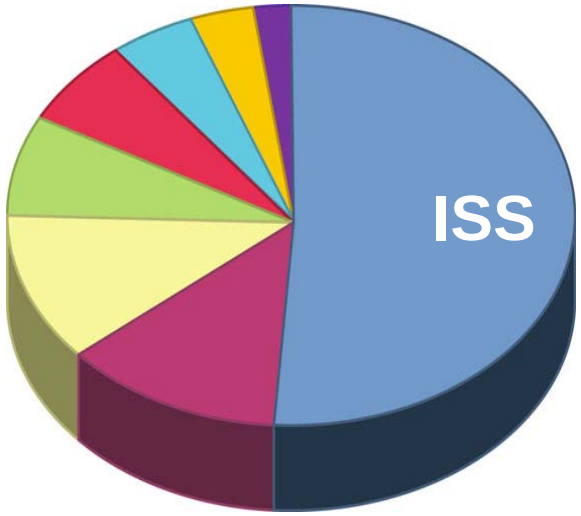
- IBM ISS简介
- 通信平台面临的安全威胁
- ISS统一通信安全平台（Unified Messaging Security）
- 问题与讨论

IBM ISS介绍

- 全球顶级的独立**IT**安全供应商
- 成立于 **1994**
- 总部位于 **Atlanta, USA**
- **1998 IPO – NASDAQ: ISSX**
- 在 **27** 个国家有 **1,200** 名雇员
- 全球 **11,000** 企业用户
- 全球顶级的安全智库
- 全球顶级的托管防护服务（**MSS**）供应商
- **2005** 年收入近**3.3**亿美元
- **2006**年底，**IBM**收购**ISS**

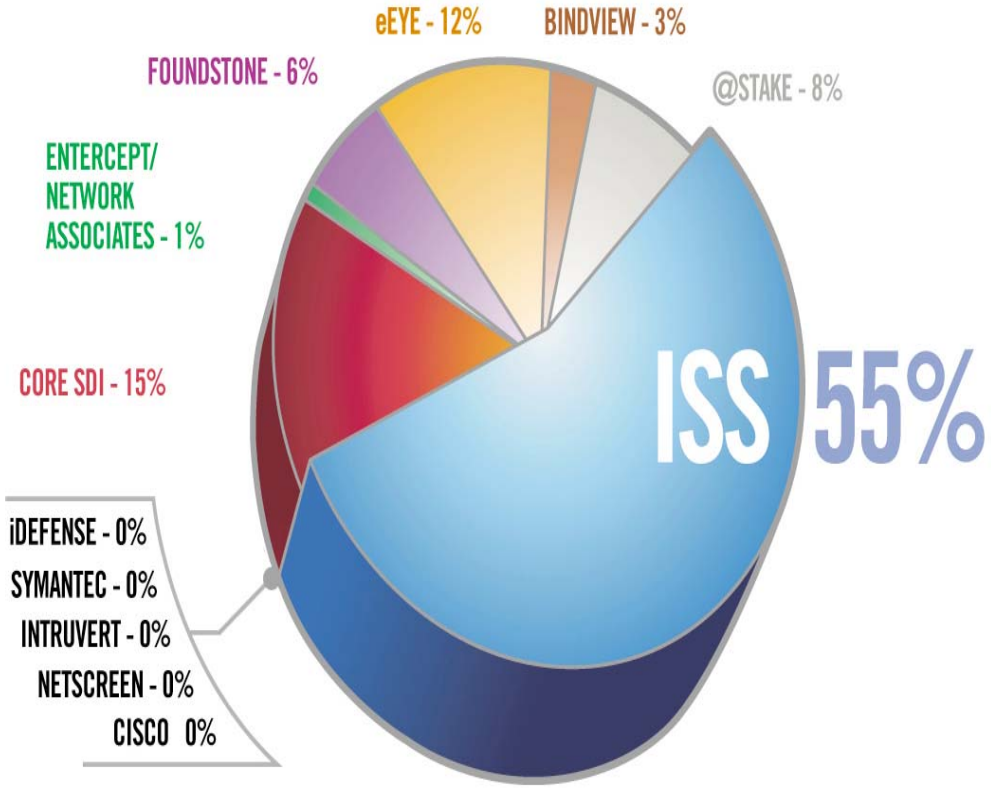
ISS 最了解互联网的风险

Figure 1: High Risk Vulnerabilities ('98 – 05)



Source: Frost & Sullivan (April 2005)

FROST & SULLIVAN



高风险漏洞来源:
Frost & Sullivan 2006, Internet

ISS 产品线

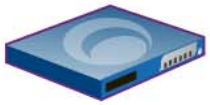
proventia management
SiteProtector™

Unified Enterprise Security
Console for all products

Enterprise Protection Products
(Appliances and Agents)

proventia network
Internet Scanner

proventia network
Enterprise Scanner



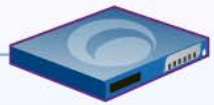
All based upon the
ISS protection platform

proventia network
Protection Agent

Proventia Mail Filter,MS3004
Complete antispam and mail filtering solution for inbound and outbound e-mail

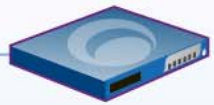
Proventia Web Filter
Web filtering solution to block unwanted Web content from network

proventia network
Protection Appliances

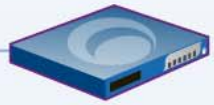


Proventia Network MFS
MX5010, MX3006, MX1004,M50,M30,M10
"All-in-One" Protection Appliance
- *IDS/IPS*
- *FW / VPN*
- *AntiVirus (signature & behavioral)*
- *AntiSpam*
- *Web Filter*
- *Spyware*

proventia network
Protection Appliances



Proventia ADS Series –
"Anomaly/Behavioral" Protection and Network Visibility Appliances



Proventia Network IPS
Preemptive Security for Enterprise Networks
GX4002, GX4004, GX5008, GX5108
G400, G2000,GX 6008,GX 6116

proventia server
Protection Agent

Proventia Server
"All-in-One" Protection Agent
RealSecure Server Sensor
Host IDS

proventia desktop
Protection Agent

Proventia Desktop
"All-in-One" Protection Agent
- *Firewall*
- *Virus Prevention System*
- *Intrusion Prevention*
- *VPN Enforcer*
- *Buffer Overflow Protection*

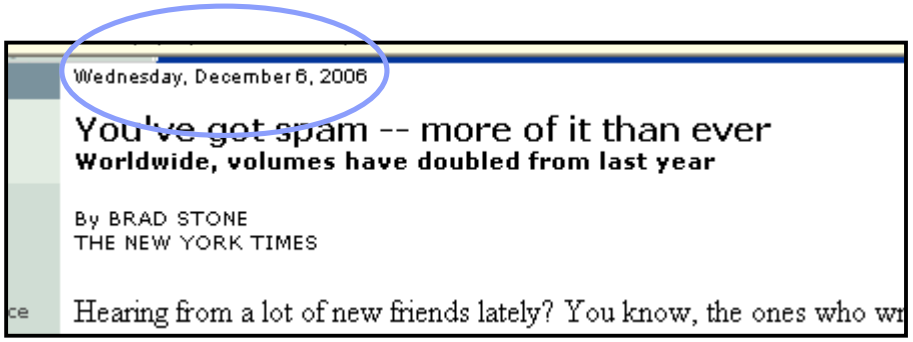
业界奖项

交流内容

- IBM ISS简介
- 通信平台面临的安全威胁
- ISS统一通信安全平台（Unified Messaging Security）
- 问题与讨论

今天通信平台面临的安全问题

- 垃圾邮件变成黑客工具 – 界线渐渐模糊
- 基于图像的垃圾邮件 – 传统过滤器无法捕捉
- 目标攻击指向个人信息 – 鱼叉式网络钓鱼攻击



http://seattlepi.nwsource.com/business/294837_spam06.html

关于邮件安全的一些数字

- 70%到80%的邮件是垃圾邮件
- 2 ~ 6%的邮件中包含病毒或者钓鱼攻击
- 恶意代码
  - 66% 的公司收到过附件带病毒的邮件
  - 恶意邮件病毒所需的传播时间从数小时降到几分钟
- 合规性
  - 30%的公司员工曾经将敏感信息主动或者错手发出到公司外部

垃圾邮件和钓鱼趋势

IBM ISS X-Force 2006 趋势分析报告

- 公司是钓鱼攻击的最大目标对象，占所有钓鱼邮件的 **71.37%**
- 一半以上的**55.78** 钓鱼攻击都把假冒网站建在美国
- **90%**以上的垃圾邮件都使用**HTML**邮件内容

截至2006年，超过40%的垃圾邮件是基于图像的垃圾邮件。

最常见的垃圾邮件标题

Subject line	Quota
Re: hi	1.47%
Canadian online drugstore	0.77%
<empty subject line>	0.68%
Re: VIhAGRA	0.57%
Re:	0.46%
Re: VkAGRA	0.46%
Re: new	0.38%
Re: 482	0.31%
hello	0.30%
Re: VIpAGRA	0.28%

威胁面前如何抉择…?

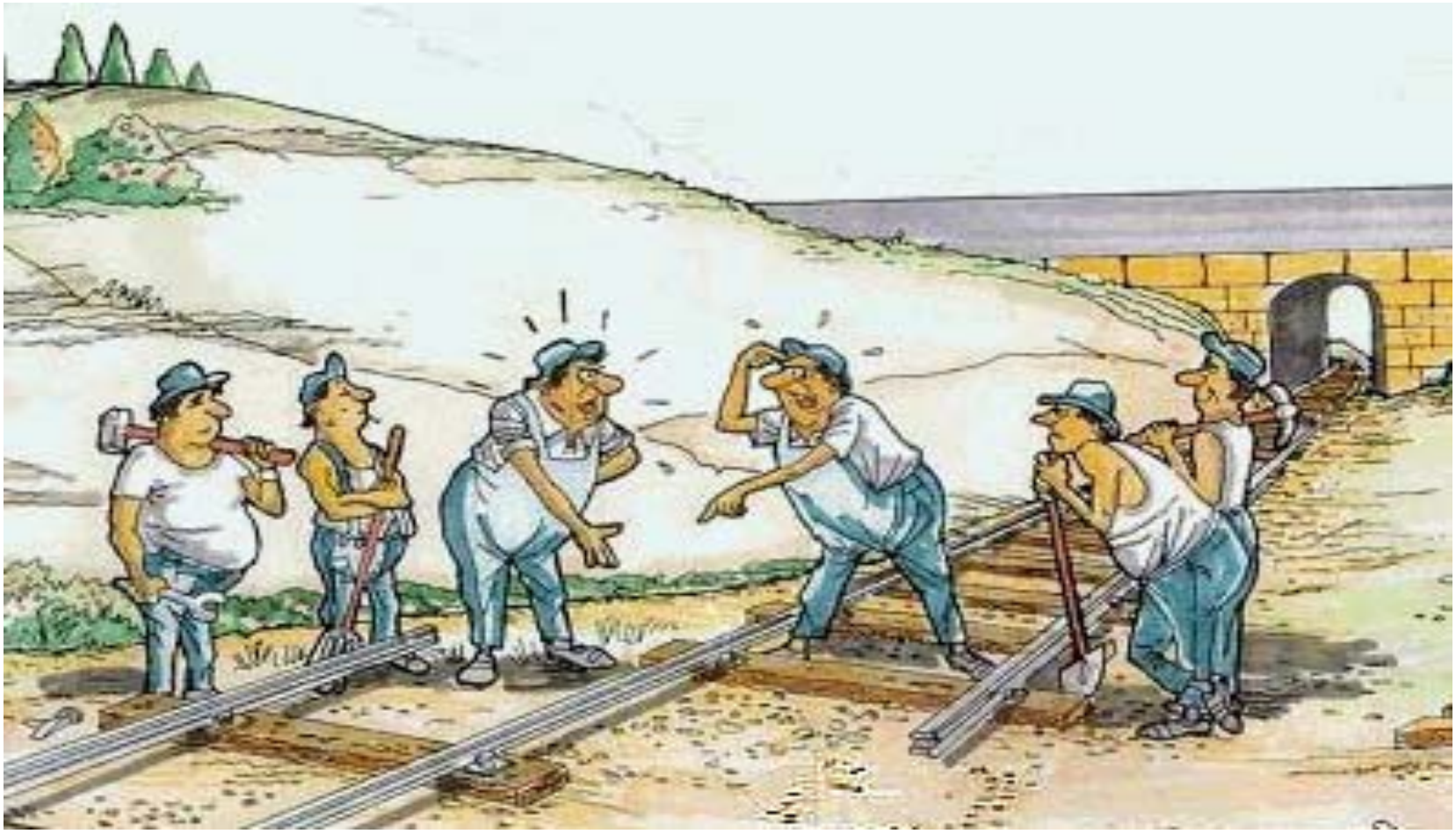
- “公司应该特别注意通信安全产品的体系架构和机制，如何能够有效而精确的阻断攻击并且过滤不必要的邮件，同时保证尽可能少的管理投入。主要需要考虑的功能有入侵防护、防毒和邮件过滤。”

  Gartner/30 June 2005/ID Number: G00129519

- IDC认为通信威胁管理、邮件服务器防毒、防垃圾邮件、出站内容合规性是统一通信安全解决方案的必要组件。

  IDC/SCM Market/3/06

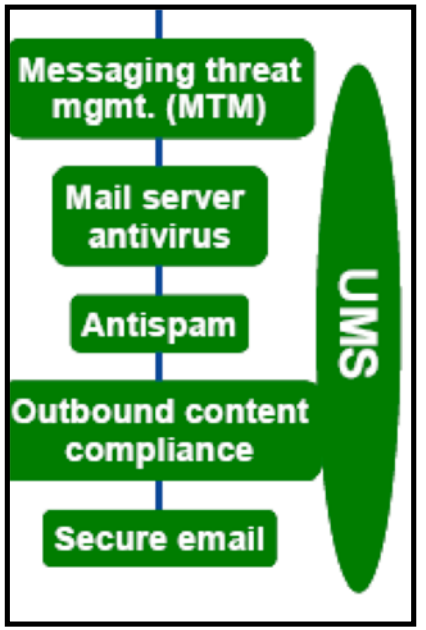
如果欠缺某些环节, 真正的安全体系就无法建立



交流内容

- IBM ISS简介
- 通信平台面临的安全威胁
- **ISS统一通信安全平台（Unified Messaging Security）**
- 问题与讨论

ISS 统一通信安全平台 – Proventia Mail



Proventia™ Mail 设备可以为邮件系统提供全面的安全防护，包括病毒防护、垃圾邮件过滤和攻击防护。保障企业邮件系统正常工作。

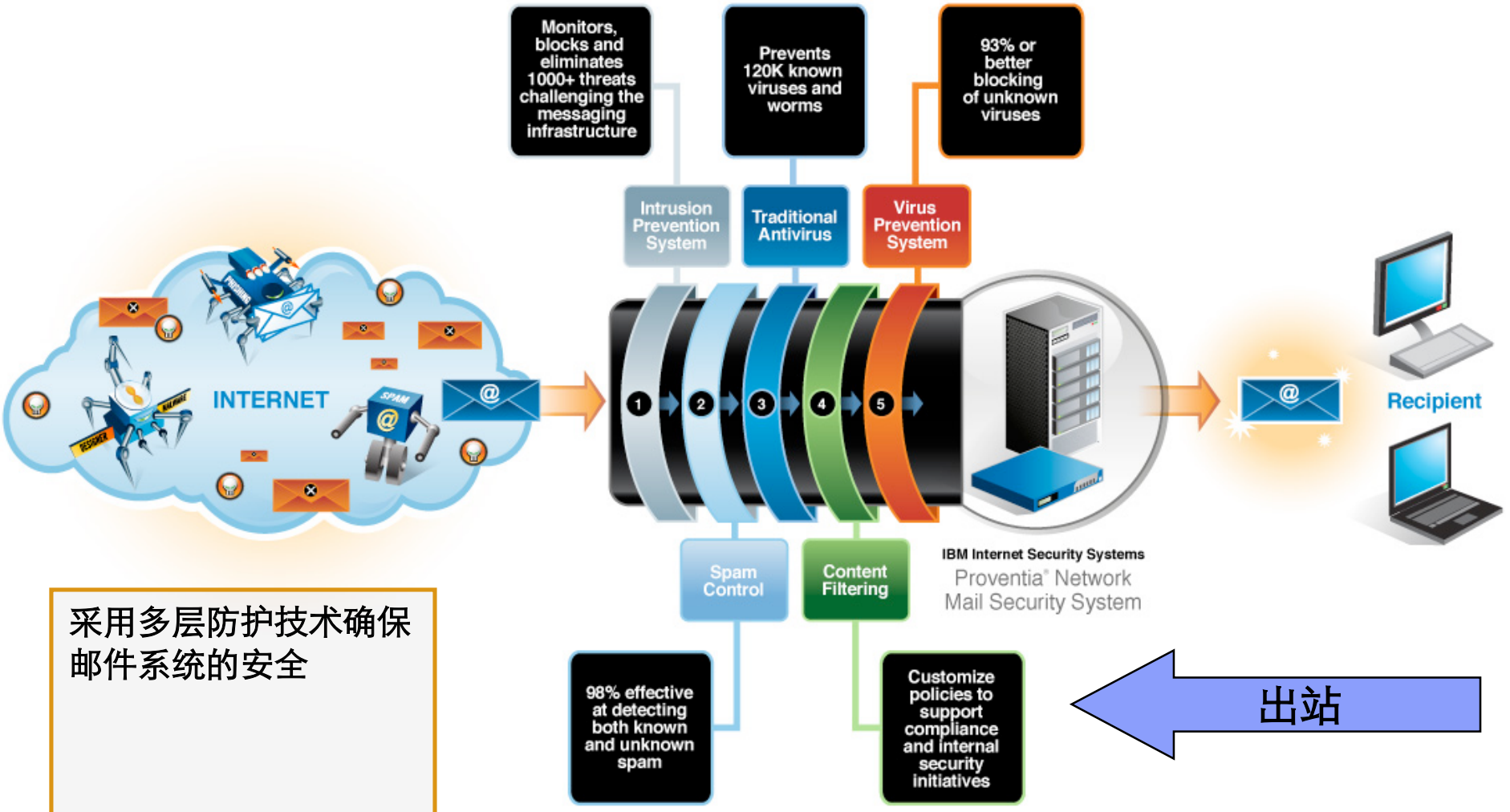
邮件安全挑战和解决方案

安全挑战	Proventia 解决方案
•保障企业的机密信息和电子邮件通信	•使用定制策略过滤进出内容，如信用卡/身份证号等敏感信息
•防止终端用户被垃圾邮件堵塞	•垃圾邮件检测率超过 98%,自动升级以应对新的垃圾邮件散发技术，包括基于图像的垃圾邮件。
•保护邮件系统免受病毒和其他网络攻击侵害	•零天VPS（Virus Prevention System）+集成的入侵防护技术

每一层防护功能抵御不同的风险

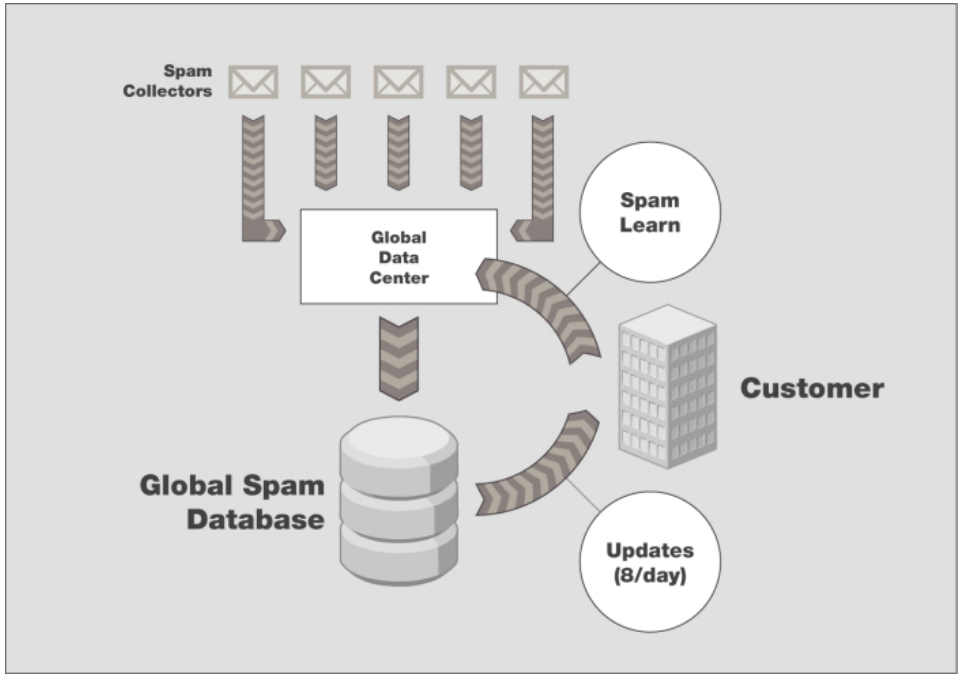
垃圾邮件过滤	o 检测已知的新类型的垃圾邮件，包括图像垃圾邮件和钓鱼邮件。具备强大的可定制的分析模块 o 减少网络宕机时间并提供员工工作效率
内容过滤	o 扫描邮件的内容，例如附件类型、信用卡号、身份证号或其他违反规定的内容 o 保护公司的信息机密性，避免知识产权损失，保护公司形象
病毒防护系统（VPS）	o 实时检测和阻断未公开的零天病毒，而无需病毒定义码更新 o 确保邮件系统免受病毒和其他攻击的侵害
特征码防毒技术	o 消灭已知的病毒，作为VPS的补充 o 确保邮件系统免受病毒和其他攻击的侵害
入侵防护系统	o 帮助保护邮件服务器免受各种攻击侵扰，例如拒绝服务攻击、 目录攻击和缓冲区溢出攻击 o 确保邮件系统免受病毒和其他攻击的侵害

Proventia Mail 如何工作



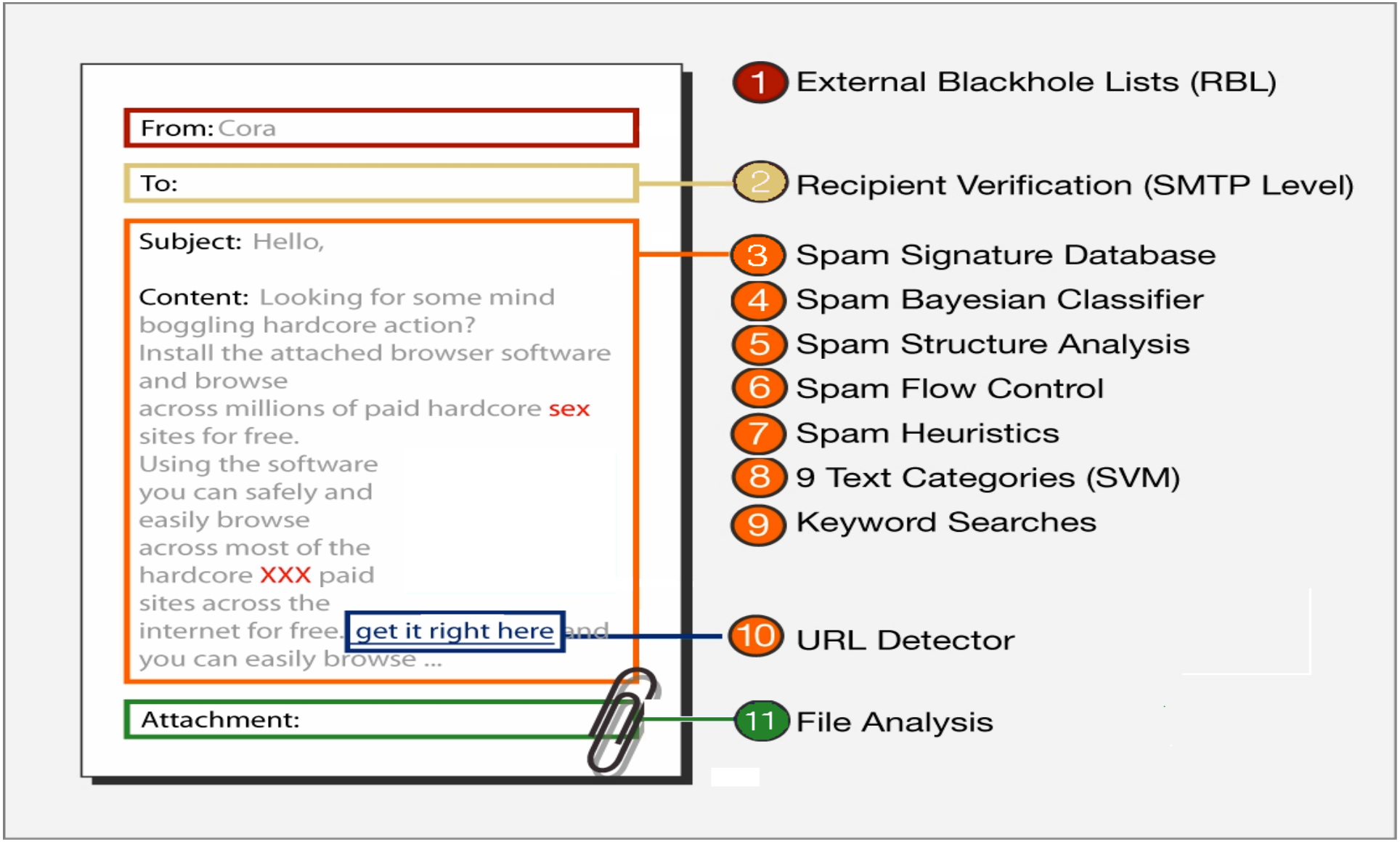
采用多层防护技术确保邮件系统的安全

全球垃圾邮件数据库和垃圾邮件学习功能

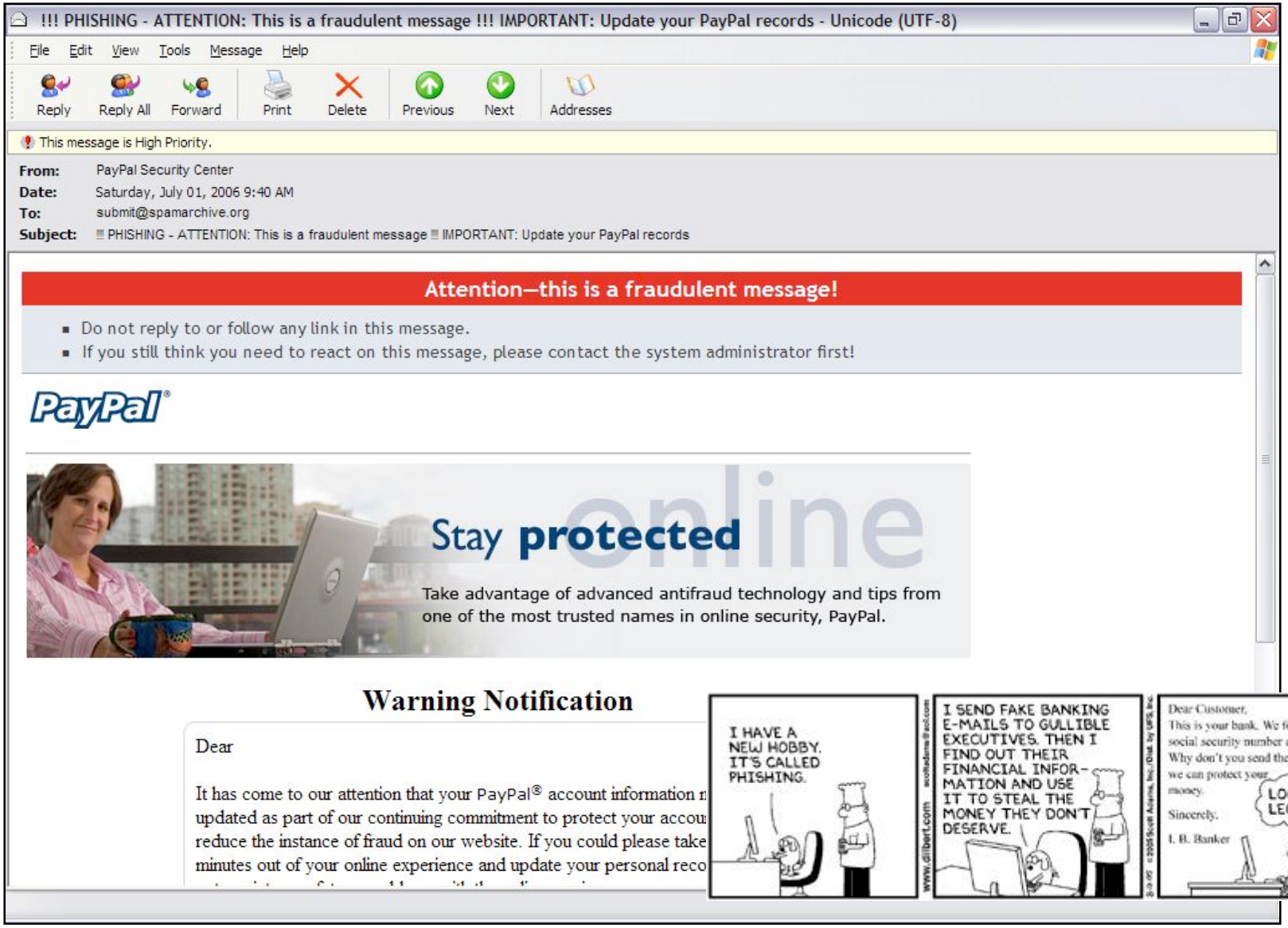


- 更新频率每天8次
- 62种分类
- 500个机器爬虫收集图像、文字和链接信息
- 每天分析70,000 垃圾邮件
- 数据库中包括42,000,000特征
- 每月分析图像和网页150,000,000
- 总共分析的页面和图像5.9 billion (约 1/5 Google的数据库)

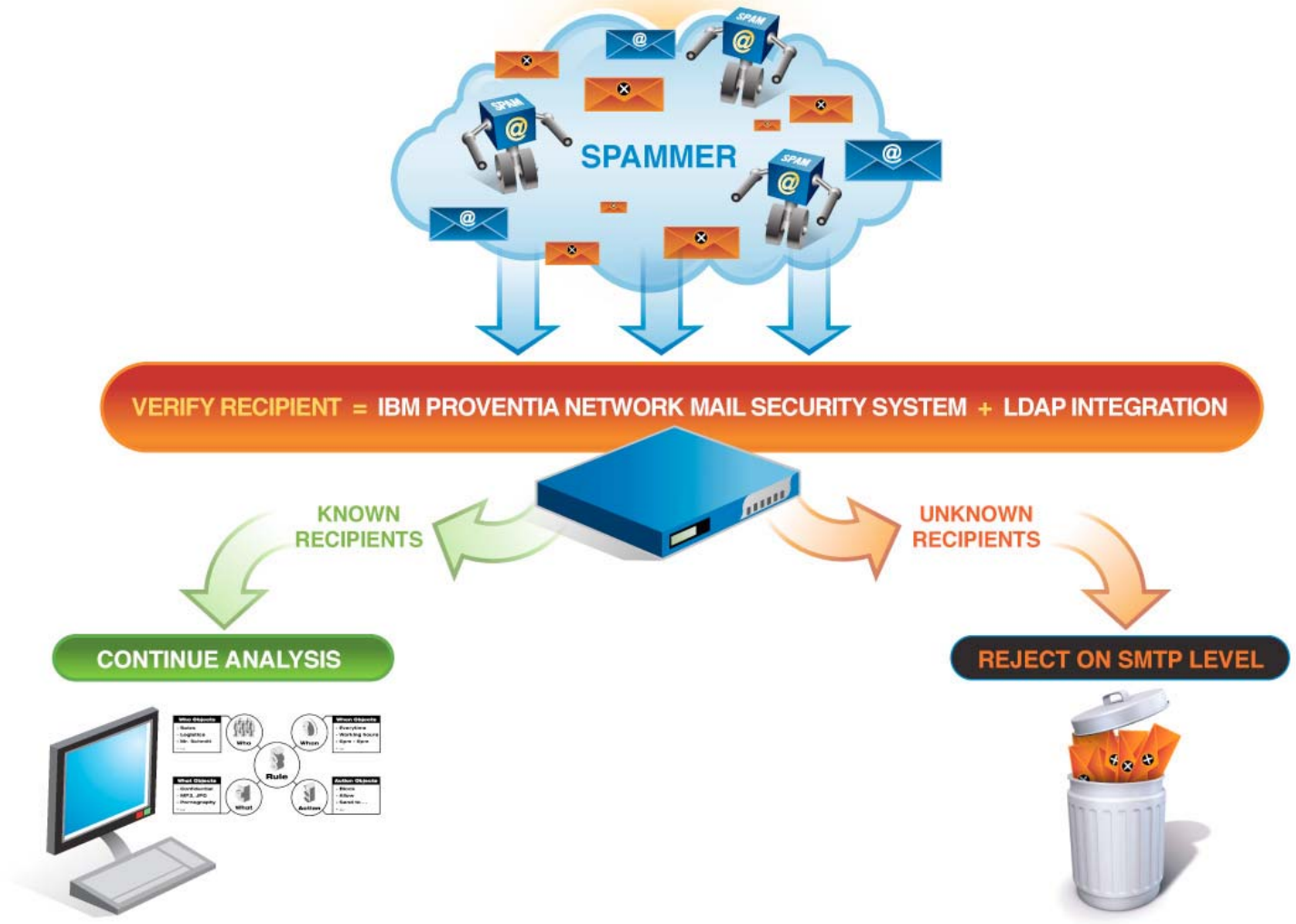
10个步骤的分析过程


From: Cora
To:
Subject: Hello,
Content: Looking for some mind boggling hardcore action? Install the attached browser software and browse across millions of paid hardcore sex sites for free. Using the software you can safely and easily browse across most of the hardcore XXX paid sites across the internet for free. get it right here and you can easily browse ...
Attachment:
1 External Blackhole Lists (RBL)
2 Recipient Verification (SMTP Level)
3 Spam Signature Database
4 Spam Bayesian Classifier
5 Spam Structure Analysis
6 Spam Flow Control
7 Spam Heuristics
8 9 Text Categories (SVM)
9 Keyword Searches
10 URL Detector
11 File Analysis

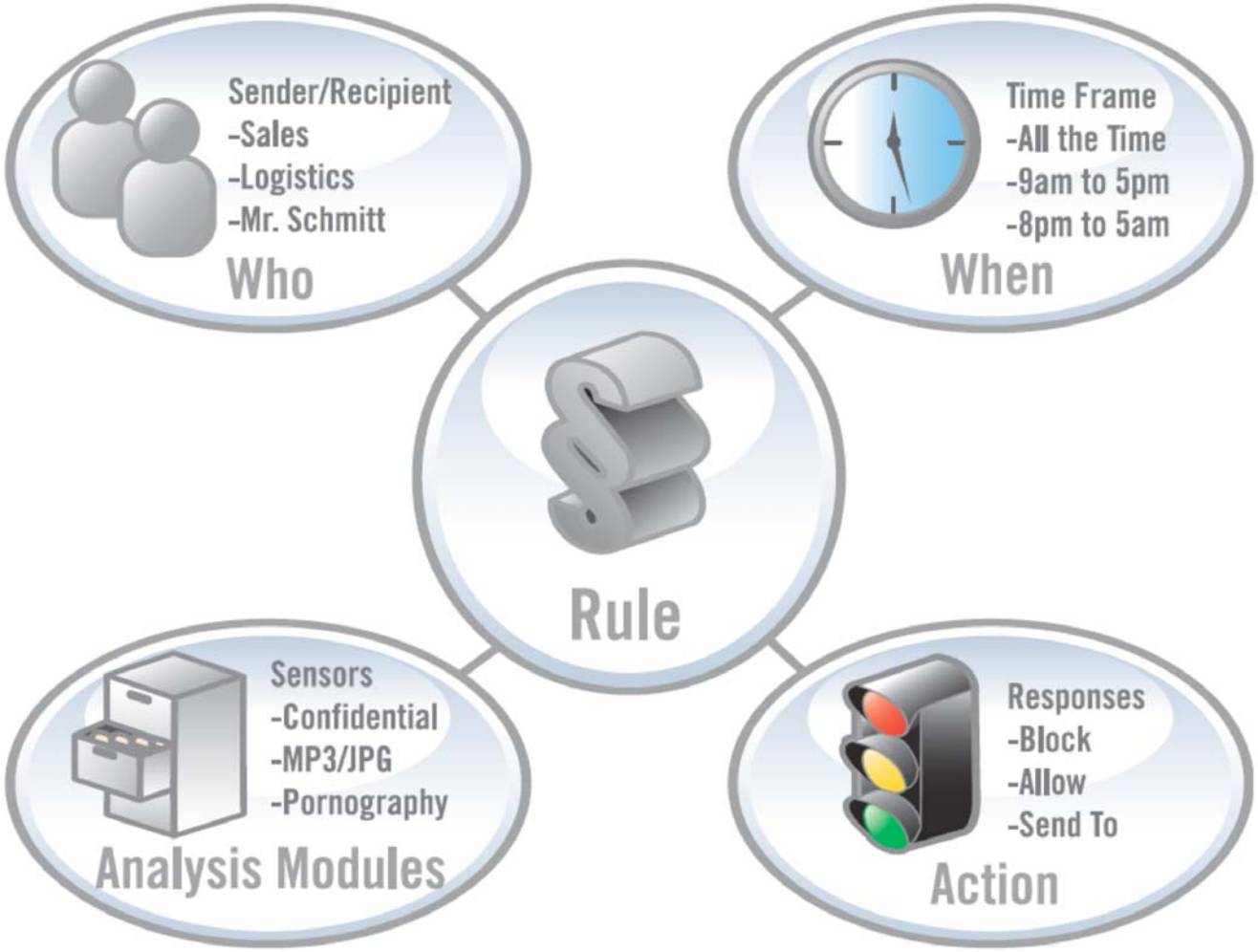
钓鱼防护



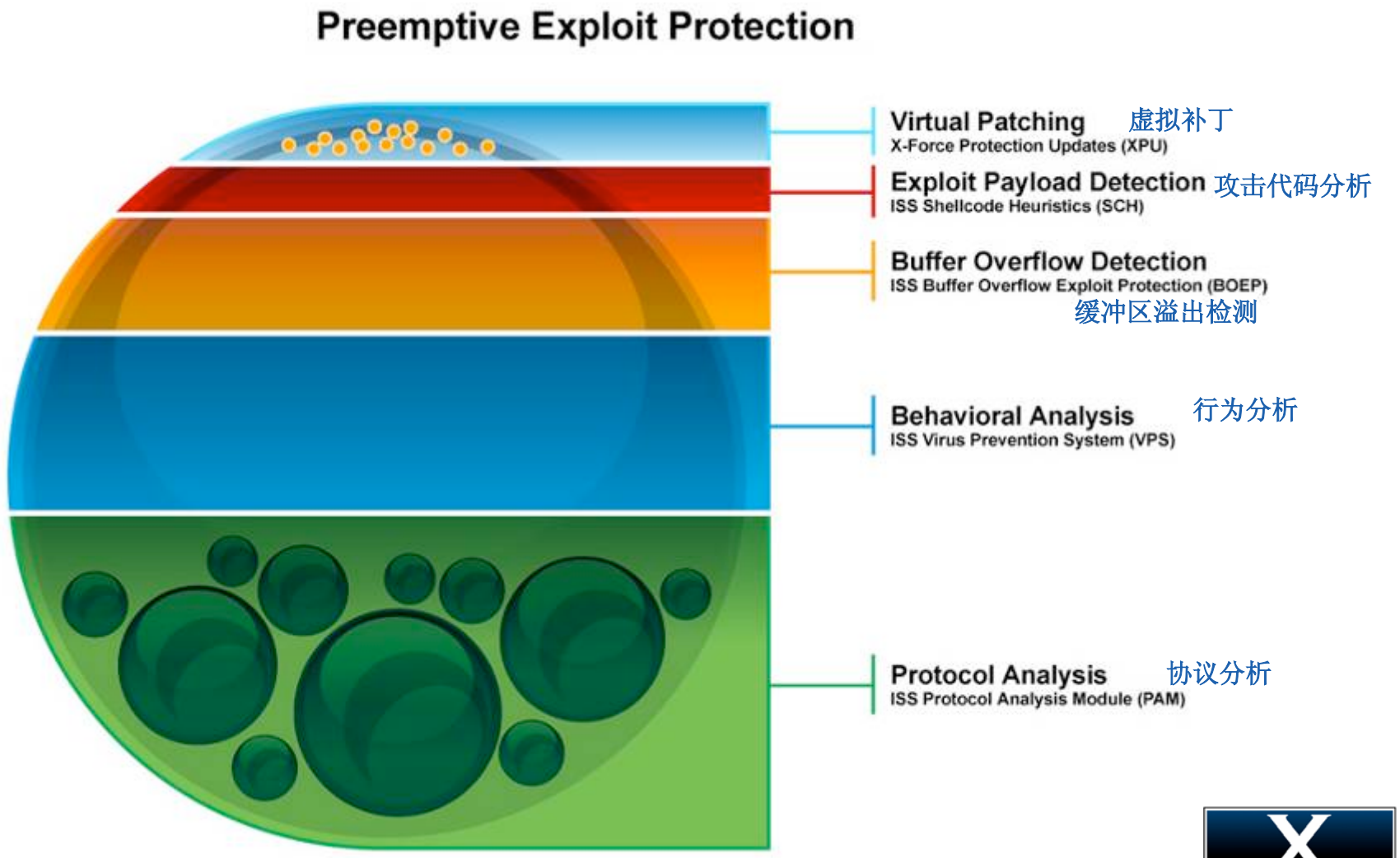
收件人验证



细颗粒度的策略控制



X-Force提供多样的检测和防护技术



强大的攻击防护功能

协议分析模块 **(PAM)**

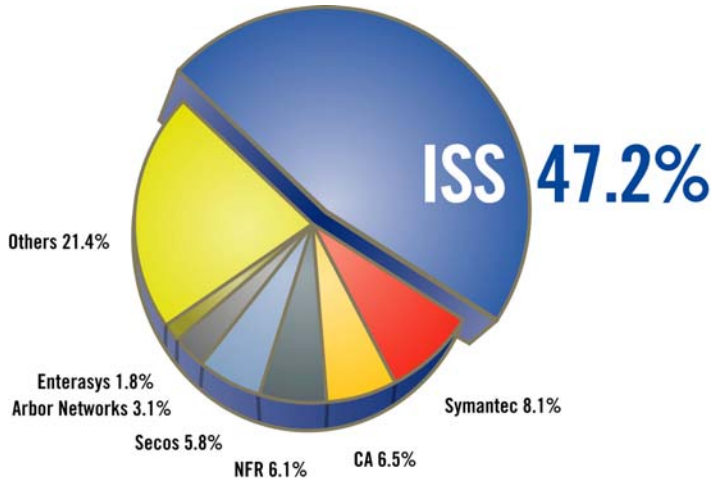
虚拟补丁

基于漏洞的防护

防护**2,500+**攻击手法

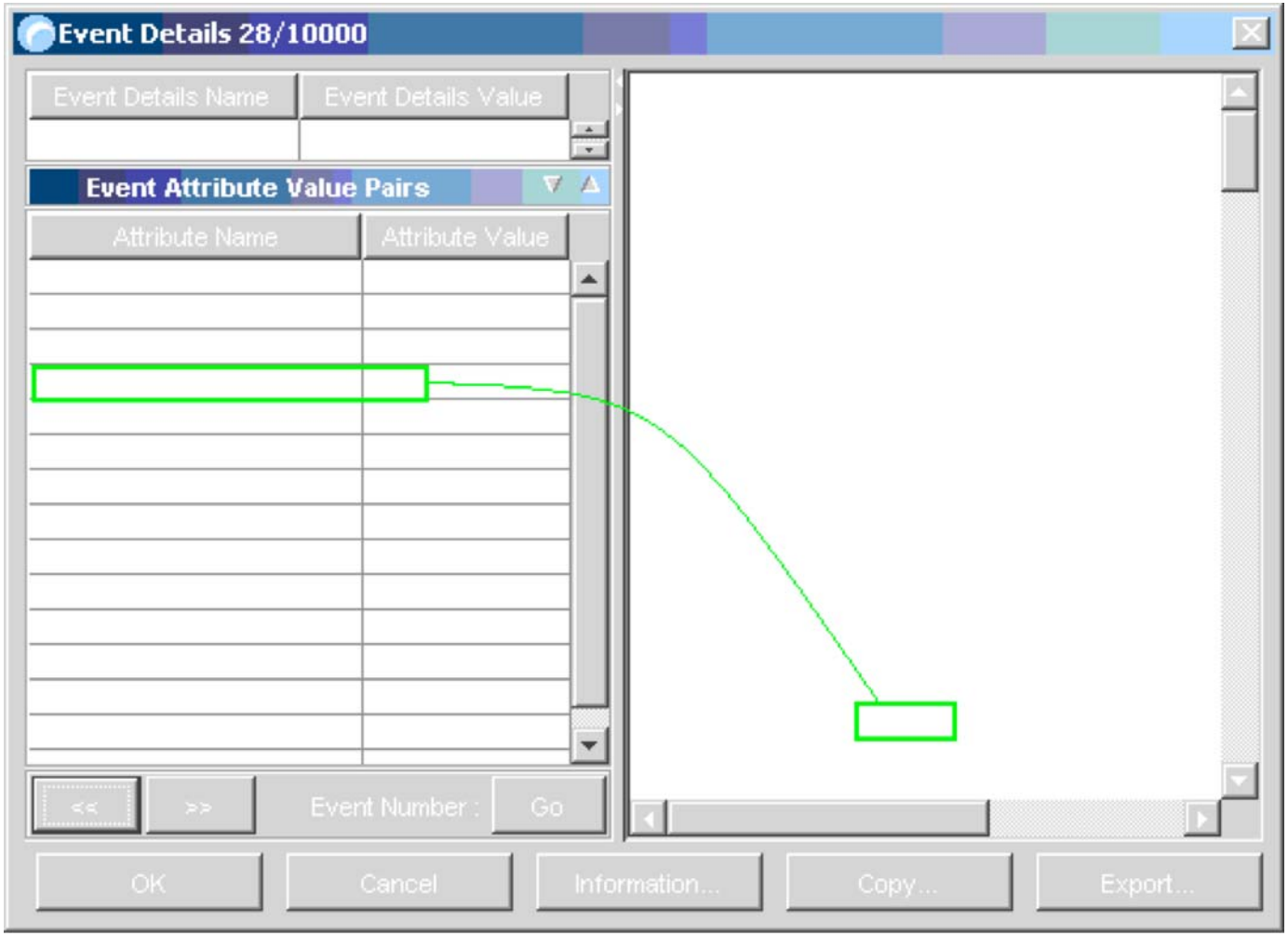
协议分析

超过**150**种协议



ISS 基于漏洞的防护的示例

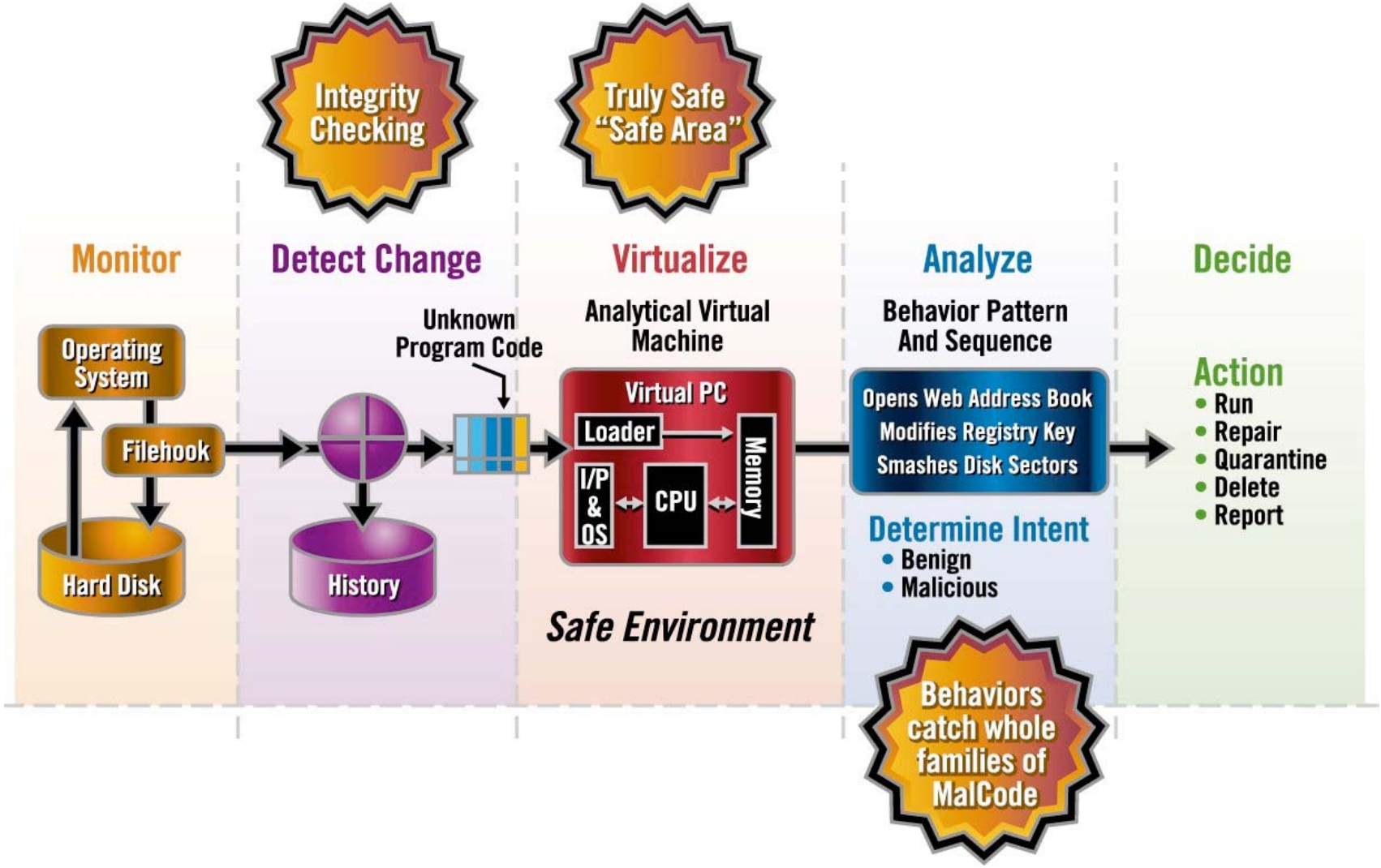
- 分析并理解会话
- 找出非法参数
- 检测缓冲溢出尝试
- 一次捕获所有变种



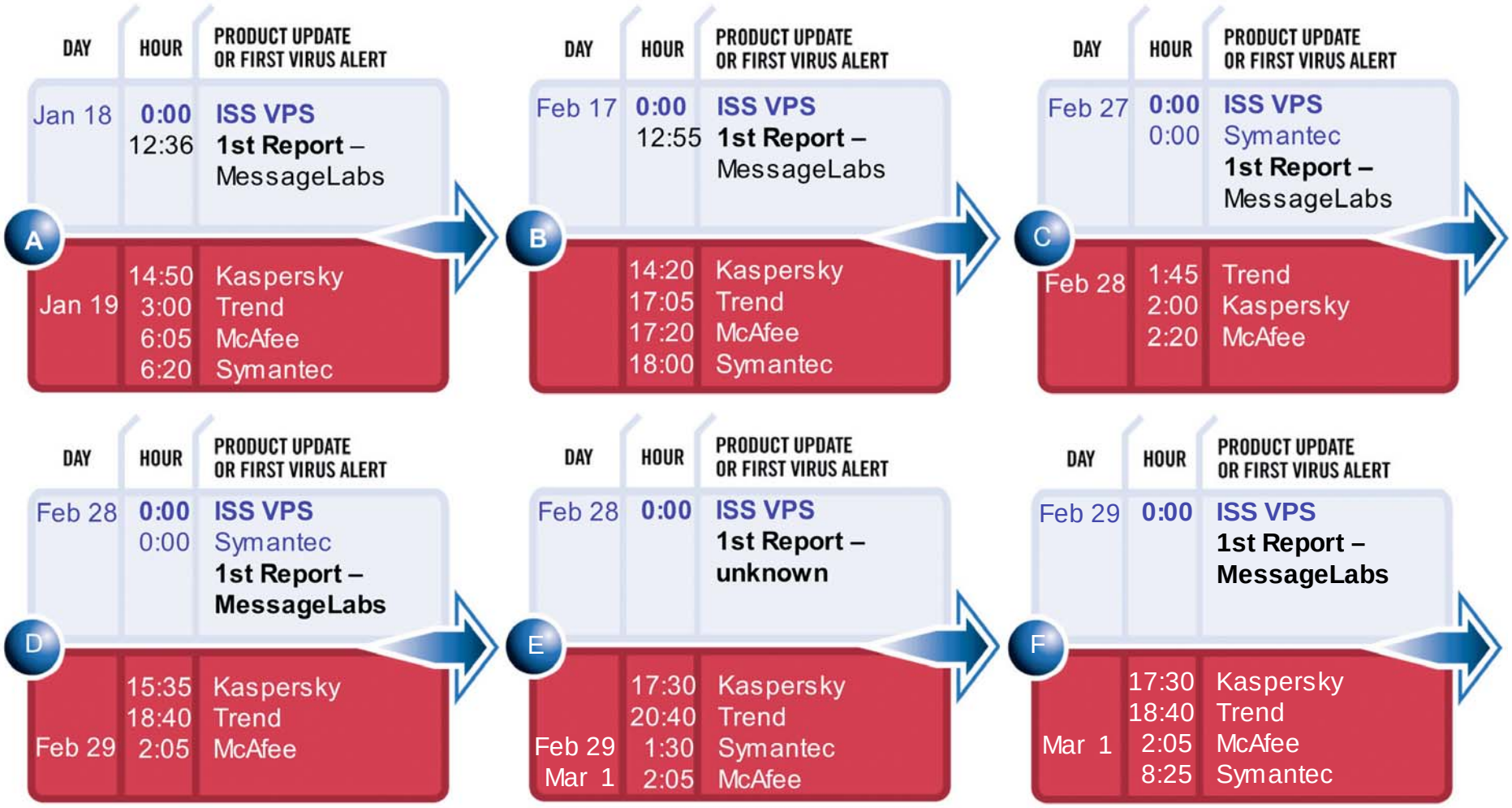
ISS病毒防专利技术

- 通过专利的行为分析阻止全面的蠕虫，病毒和其他恶意程序。
- 在恶意应用程序运行前阻断它
  - 在安全环境上运行
  - 环境复制 Windows API, CPU, memory等等.
  - 通过替代路径分析程序，然后得出结论
- 恶意应用程序用的技术越多（更多的感染向量），更容易检测
- 和传统的防病毒应用程序协同工作

ISS VPS 技术架构概述

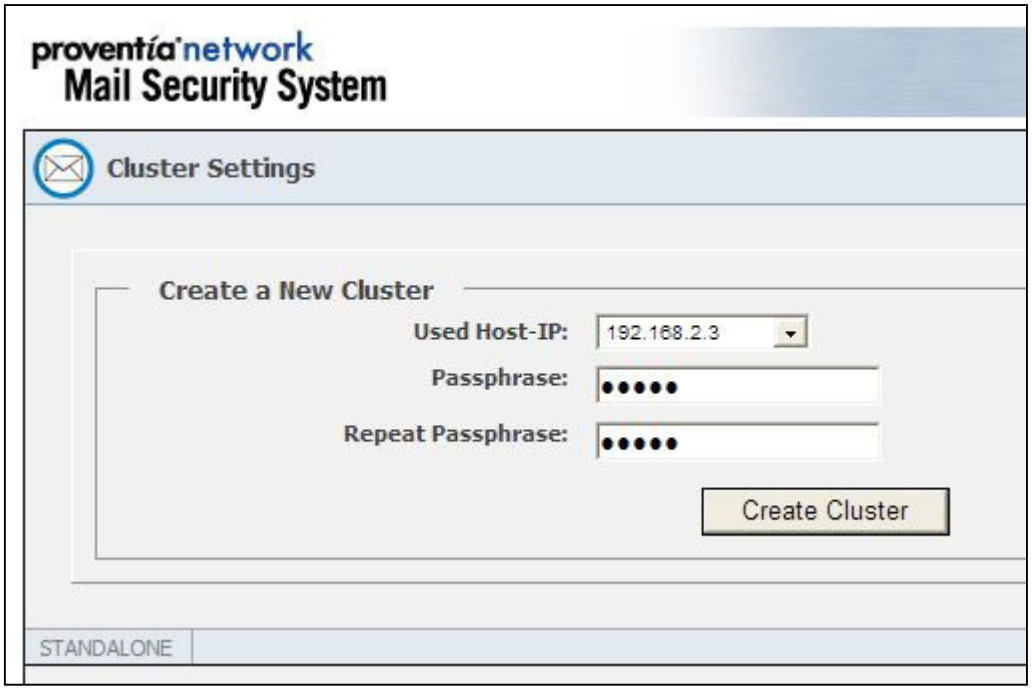


病毒变种和响应时间



Data Sources (GMT +1):
ISS—ISS VPS and MessageLabs first reports (days)
AV-Test.org—Other vendor response times (not

方便的管理



- 基于**Web**的管理
- **SiteProtector**集中进行管理 **Management**
- **Cluster/HA**

ISS统一通信安全平台的强大功能

- 深层防御：强大的病毒防护、垃圾邮件过滤和攻击防护功能
- 垃圾邮件过滤 **>98%**、误报**<0.01%**，处理能力 **36,000 mail/hour**
- 两种机制的病毒防护**(**传统防毒和 **VPS)**
- 强大的垃圾邮件过滤**/**内容过滤引擎
- 由**IBM X-Force** 机构研发

谢谢