互联网安全系统 Internet Security Systems (ISS)

以智慧维护安全，以安全保障智慧

安全漏洞、黑客侵袭、人为错误，病毒干扰，信息泄漏，混合威胁……

种种来自内部、外部的问题，使企业的信息安全难以得到有效保障，在网络、IT系统广泛应用的今天，这是每个企业都面临的挑战！

IBM的智慧应对

IBM ISS致力于帮助企业摆脱险恶IT环境、评估安全风险并提供适合企业安全需求的前瞻信息安全解决方案，以缓解和抗击来自互联网及各种来源的信息安全威胁。IBM信息安全服务提供从端到端信息安全产品、风险评估、体系设计、项目实施、专业培训到顶级托管服务的全面信息安全解决方案。IBM全方位的专业信息安全保障能力和经验可以帮助企业确保信息系统的整体安全，在推行新的业务计划同时，有效管理和降低各个层面的安全风险。

ISS概述

IBM ISS帮助企业评估风险、确定关键的信息资产，设计并部署安全防护解决方案。此外，作为产品应用的保障，根据企业组织安全信息资源的不同，IBM ISS提供了24×7全天候的监控与管理服务，并且开展教育与培训工作。IBM ISS作为各类型组织最可信赖的信息安全产品与服务提供商，服务全球超过11,000家客户，是全球领先的前瞻IT安全解决方案提供商。

IBM ISS的独到技术源于其专业的研发实力。X-Force研发团队针对检测到的全球范围的趋势性威胁和正在发生的攻击情况，在威胁发生前即提供“早期警报”，揭示主要的软件缺陷，研发防护工具，并将其研究成果以最快的速度向市场发布，向用户提供前瞻性防护。X-Force研发团队是在全球入侵防护、漏洞扫描及评估等信息安全领域上极具权威性的组织。所有IBM ISS产品都基于X-Force研发小组的精心打造！

IBM ISS端到端信息安全产品

IBM ISS的ESP（Enterprise Security Platform）企业安全平台可以为用户提供企业级安全的完整解决方案。该平台可以保护企业的整体基础设施，从网关、核心网络、主机，一直到远程终端，实现真正的前瞻性防护。Proventia系列产品的所有防护功能，都通过SiteProtector进行集中管理，这使得企业能够通过一个中央系统控制、监控Proventia系列产品，并对这些产品做出分析。这样就大幅度降低了企业的成本，节约了企业宝贵的时间与资源。

- **IBM Proventia统一安全管理平台：**
  SiteProtector集中式管理系统统一了网络、服务器和桌面保护产品与应用的安全管理和分析，极大减轻了IT人员的管理负担。客户可以从中央位置以最少的人力和运作成本来控制、监视并分析其安全防护状况。这一能力也使其可以很方便的实现大型企业范围内的安全配置。

- **IBM Proventia企业扫描器：**
  IBM Proventia企业扫描器是新一代安全漏洞管理系统，采用久负盛名的ISS扫描评估引擎作为核心，结合强大的工业标准硬件平台，提供服务器、桌面电脑、操作系统、路由器/交换机、防火墙以及应用程序已存在弱点的评估和完善的修复管理，从而确定系统的潜在风险。

- **IBM Proventia网络入侵防护系统：**
  IBM Proventia网络入侵防护系统精确地检测和阻断各种网络威胁——在它们影响企业信息资产之前将其阻截。通过串接式配置并以线速运行，可以实时阻断黑客入侵、拒绝服务攻击、恶意代码、SQL（Structured Query Language，结

构化查询语言）注入攻击、XSS（Cross Site Scripting）跨站脚本攻击和各类基于漏洞的混合威胁。

- **IBM Proventia主机入侵防护系统：**

  IBM Proventia主机入侵防护系统通过分析安全事件、主机日志以及进出主机的网络数据流量来提供实时的综合主机入侵保护，精确阻断恶意攻击，支持各类主流操作系统。可为法规遵从提供支持，满足有关可能损害服务器和敏感数据的恶意威胁的安全性法规要求。

- **IBM Proventia多功能安全网关：**

  IBM Proventia多功能安全网关整合全球领先的入侵检测和防护系统、防火墙、虚拟专用网、网关防毒、违规网页内容过滤和反垃圾邮件，谍件防护等多种功能，为企业提供高性价比的整合式边界安全防护。

- **IBM Proventia邮件安全网关：**
  - 保护邮件用户免受垃圾邮件的困扰；
  - 正确识别并阻止各种零日攻击；
  - 邮件内容过滤定制；
  - 邮件病毒防护。

- **IBM Proventia终端安全控制系统：**
  - 系统保护功能，防护已知和未知的威胁攻击；
  - 系统安全维护和配置管理；
  - 帮助确保遵从性并简化管理；
  - 提供终端数据泄漏防护。

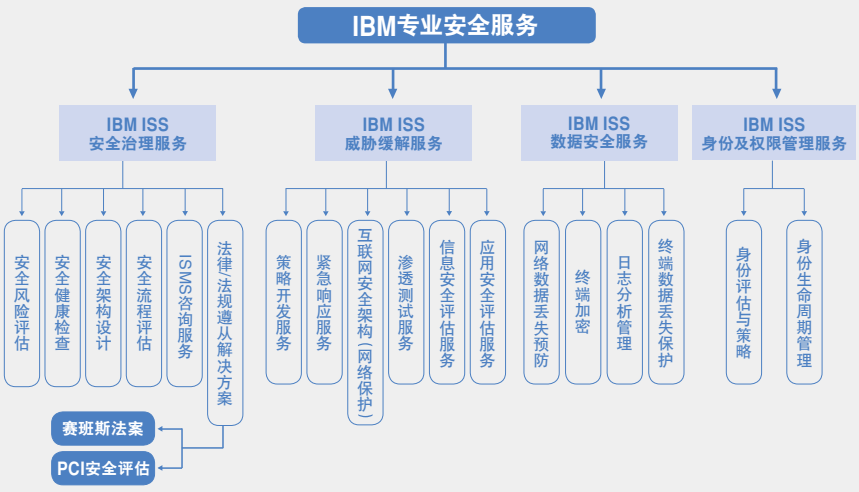
IBM专业安全服务

IBM ISS专业安全服务为您提供专业的安全咨询、安全评估以及全面的信息安全解决方案，以专业化的技术、顶尖的工具、世界一流的安全知识库以及值得信赖的IBM ISS顾问团队，帮助各种规模的组织降低风险、符合法规遵从、保持业务连续性、保护关键业务资产、缓解网络威胁、实现组织的安全目标。IBM ISS团队的安全专家使用专用的工具集、最新的威胁智能和先进的对策，帮助组织建立有效的安全计划，保护并增强业务运营。

IBM ISS专业安全服务的服务要点：

- 提供专家咨询，支持风险管理和法规遵从；
- 评估当前的安全状态，帮助客户保护关键业务资产；
- 推动经济，快捷且有效地实现信息安全目标。

IBM ISS专业安全服务产品线



注：PCI—— Payment Card Industry支付卡产业

智慧引领未来

IBM管理安全服务

IBM管理安全服务可以提供基础设施、知识资源和随需专业能力，帮助各组织保护自己的系统。

远离互联网攻击——实现所有这些功能的成本仅是常见内部安全资源成本的几分之一。

IBM ISS管理安全服务的服务要点：

- 为您的IT资产提供7×24的可信赖的监控和安全管理；
- 最大化利用已有的IT安全投资；
- 全球领先的SOC（System on Chip，系统级芯片）平台，有助于提高安全性；
- 基于最新技术的，满足您的灵活需求；
- 使用内置的安全智能，使您始终能够提前避免威胁；
- 帮助节约最高达55%的安全成本，并满足法规遵从需求。

IBM ISS管理安全服务产品：

- IBM针对网络的安全保障服务；
- IBM针对服务器的安全保障服务；
- IBM针对桌面的安全保障服务；
- IBM防火墙管理服务；
- IBM入侵检测/防御系统管理服务；
- IBM漏洞管理服务；
- IBM邮件安全管理服务；
- IBM Web安全管理服务；
- IBM安全日志管理服务；
- IBM安全预警服务。

客户收益

通过将安全运营负担转移至IBM ISS，组织可以获得具有领先的安全工具、技能、流程和专业能力优势。在系统正常运行时间和性能方面实现改进，并减少技术和资源的资金投入。而且，由于从日常安全监控和管理工作中解放出来，各组织还能够将内部IT资源重新分配到更具有战略意义的活动中，从而提高生产力。

经典案例

案例一：

某大型电力公司需进行网络改造

挑战：

此项目是北京2008奥运会保障工程的一部分，因此意义重大。客户固有网络存在以下问题：

- 下联节点多，各地分公司网络结构多样、复杂，存在安全风险及隐患；
- 缺少专业的安全评估工具和入侵防护设备；
- 已有其它厂商桌面防毒软件不能提供个人的入侵防护能力。

解决方案:

- Proventia IPS（GX）—— ISS千兆、百兆IPS产品，在线连接方式，提供实时防护；

- RealSecure Desktop Protection——个人防火墙、入侵防护；
- Proventia SiteProtector——Enterprise Version，提供全面、实时安全管理平台，并提供安全事件相关性分析、专业报告生成。

结果：

- 得到世界级的安全产品，增强系统防护能力。通过在线升级，虚拟补丁等服务机制享受ISS X-Force所有的研究成果，实现真正的前瞻性防护；
- 通过培训、学习，安全运维人员的认识、水平得到提高，能做到系统、准确地制定安全防范策略、及时采取防范措施，并能及时掌握网络受到的攻击情况和提供的相应的防范效果；
- 个人终端用户的被黑客攻击事件基本杜绝，并不需要频繁升级，减少运维人员工作量。

通过培训、学习，安全运维人员的认识、水平得到提高，能做到系统、准确地制定安全防范策略、及时采取防范措施。并能及时掌握网络受到的攻击情况和提供的相应的防范效果。

案例二：

在某重点大学新建校区的校园网入口处部署防火墙作为内部的安全防御系统

挑战：

自从该校区网络中心机房建成投入使用后，为校园网提供了高带宽、高可用性的网络环境。随着网络应用的不断普及，越来越多的应用系统依赖于校园网运行，但随之而来的网络安全事件也频频发生。自2006年9月以来，校内多个部门的服务器发生了被黑客入侵、篡改主页、发布不良信息等事件，造成了一定的负面影响，同时也受到所在市公安局网监处和网络警察支队的高度关注。

解决方案：

- Proventia GX6116入侵防护系统；
- Proventia GX5208入侵防护系统；
- Proventia SiteProtector统一安全管理平台。

结果：

在入侵防护系统部署后前期发现了大量的攻击行为包括注入攻击、RPC（Remote Procedure Call，远程过程调用）攻击、DNS（Domain Name System，域名系统）攻击及DDOS（Distribution Denial of service,分布式拒绝服务）攻击，但是IBM ISS IPS成功阻挡了这些攻击行为，经过3个月左右的时间，攻击行为明显减少，校园网及服务器也没有遭受任何攻击。