



准确防御最多种类的安全威胁

IronPort 防垃圾邮件技术

概览

随着安全威胁的制造者不断采用更先进更狡猾的技术手段以求渗透进企业现有的安全防护系统，当今的电子邮件安全威胁已经不再只是原来那些让人讨厌的垃圾邮件那么简单了。

IronPort 防垃圾邮件™解决方案将传统防垃圾技术的优势和 IronPort 突破性的上下文敏感的垃圾检测技术相结合，彻底消除了各种已知的和新兴的恶意邮件对企业网络的安全威胁。

功能特点

强大的企业网络外层防护系统

基于信誉的过滤 — IronPort首创的技术 提供一个针对垃圾邮件的强大的外层防护。

IronPort信誉过滤器™具有无与伦比的检测效果，在连接层就可以准确地将多达80%的垃圾邮件阻挡在企业网络之外。IronPort®系列设备同样拥有一个独一无二的邮件速率限制功能，可以智能化地延缓企业邮件系统接收来自可疑邮件发送人的邮件的速度，这极大降低了垃圾邮件的危害和误报及漏网的风险。

基于邮件上下文的评分确保了高准确性

IronPort防垃圾邮件技术 使用的是业界最具技术创新的方式来进行邮件安全威胁的检测。除了要评估邮件发送人的信誉之外，IronPort独有的邮件上下文自适应扫描引擎™ (CASE)还要对邮

件完整的上下文进行检查，包括

- 邮件内容
- 邮件构造和组织的方式
- 邮件发送者的信誉值

在对CASE分值和邮件发送人的信誉进行综合分析后，所得出的最终结果将比传统垃圾邮件过滤技术更加准确。

IronPort的Web信誉技术 会观测并分析一个Web站点的行为和数据流量模式以评估该站点的可信赖度。IronPort的CASE技术将判定邮件体中任何一个URL的信誉度，这样对邮件的分析就会得出更准确的结果。有了这些技术的支持，IronPort就能即时保护所有IronPort防垃圾邮件技术的客户时刻远离任何垃圾邮件、病毒、钓鱼攻击和间谍软件等安全隐患的威胁。



功能特点 (接上)

自动升级功能和全面完善的保护

自动、及时和安全的规则升级机制 免除了后续的手动规则调整和维护。IronPort 的升级服务将确保 IronPort 设备总是运行在最新的引擎上，能够及时截获所有最新出现的邮件安全威胁。

简单方便的配置系统 管理员可以轻松地对服务进行全局配置，也可以利用 IronPort 的强大的邮件安全管理器™来设置特定于用户和组的安全策略。

终极用户可直接访问 IronPort 垃圾邮件隔离区以检查和管理所有受到隔离的邮件，也能重新定期发送给他们的邮件摘要。一个强大的用于微软 Outlook 的垃圾邮件报告插件让用户能够将任何漏网的垃圾邮件直接发送到 IronPort 的安全威胁操作中心进行二次评估。

实时监控和集中式报告

邮件流监视器™ 实时提供关于都是谁正在向企业发送邮件的完整视图，并能迅速提醒管理员注意可疑邮件流以便立即采取行动。

邮件流中心™ 让您能够迅速找到任何一封曾经流经企业邮件系统的邮件的当前状态。有了这个集中式报告工具，管理员和客户支持人员就可以很快地解答诸如“我的邮件到底出了什么问题？”等此类用户的询问。

快速、准确的邮件检测

IronPort 的 24x7 全天候运行的威胁操作中心(TOC) 使用各种技术手段和设备设施以确保 TOC 的高效用。TOC 中的分析人员能够使用 32 种以上的语言进行交流，手中握有强大的工具来维护巨量的邮件信息、管理关于最新邮件趋势的知识库以及实时发布规则升级，确保新的邮件安全威胁在刚刚兴起的时候就会被封阻，同时还要对用户的报告和反馈进行细致彻底的校验。



Jan Mak, IronPort 安全威胁操作中心 (TOC) 的主管

产品优势

防御最多种类的邮件安全威胁 IronPort防垃圾邮件解决方案可以对付所有已知的安全威胁，包括垃圾邮件、钓鱼攻击、僵尸网络攻击以及那些难以检测的小量且流行时间很短的邮件安全威胁如“419”等。此外，IronPort防垃圾邮件技术也能识别各种新兴的混合式安全威胁，比如那些通过内嵌有害URL或者附带可执行病毒文件等手段传播有害内容的垃圾邮件攻击等等。

具有最高的准确性 IronPort解决方案之所以具有高准确性和高效用，其幕后的关键就是IronPort SenderBase®所提供的巨量数据。SenderBase是全球第一个同时也是最大最准确的邮件流量监视网络。除了最优秀的技术之外，IronPort防垃圾解决方案的背后也有着各学科专家小组的支持，包括邮件安全、机器学习和人类基因科学等等。作为预防性安全威胁检测技术的领导者，IronPort的安全专家不断进行技术创新以保证总是领先于各种新兴的安全威胁一步。IronPort防垃圾解决方案和IronPort的威胁操作中心紧密集成，确保了最高级别的准确性和响应能力。

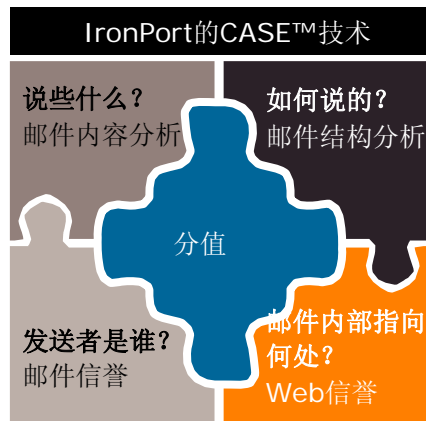
简单易用，实现“零管理” IronPort 的自动、及时和安全的规则升级机制免除了后续的手动规则调整和维护。时间上的节省，再加上完善的报表，为管理员提供了关于企业邮件流的强大的细节视图。

以全球信息为后盾的解决方案 除了特定于当地的内容敏感的邮件威胁检测技术之外，IronPort 防垃圾解决方案同样也有着来自全球各地的内容丰富的 SMTP 和 HTTP 数据的大力支持，这些数据由美洲、欧洲和亚洲的 10 万多个 ISP、大学和企业机构所贡献。

拥有业界领先的性能 IronPort 的垃圾邮件过滤技术在处理现实邮件流时具有业界领先的性能，这是因为 IronPort 信誉过滤器技术可以将邮件流带宽消耗降低多达 80%，通过减少需要处理的邮件量极大提高了系统的效率。另外，IronPort 的 CASE 技术独特的一点是能够在扫描一封邮件的期间同时进行多种评估，避免了不必要的计算开销。

图表一 IRONPORT 防垃圾邮件技术的优点：世界领先的检测效果

IronPort 的 CASE 技术使用先进的机器学习技术来模拟人类在评估邮件安全性时所使用的逻辑。一个人类分析师，还有 CASE 技术，在检查邮件时会问这四个基本问题：



- * 经过优化有效防御混合式安全威胁
- * 拥有业界领先的检测效果
 - 完整的上下文分析将误报率和漏网率降至最低
 - 10 万多家 ISP、大学和企业为 IronPort 贡献宝贵的数据
 - 24x7 全天候运行的威胁操作中心
- * 全球化解决方案
 - 特定于内容的，种类丰富的邮件属性
 - 一个全球 SenderBase 网络



概要

全新的防垃圾邮件解决方案

随着邮件安全威胁愈演愈烈，以及安全威胁的制造者不断采用更先进更狡猾的技术手段以求渗透进企业现有的安全防护系统，一个能为企业提供最安全的保护的多层垃圾防御系统是必不可少的。IronPort 防垃圾邮件解决方案结合了传统技术的优势和 IronPort 革命性的上下文敏感的检测技术，能够过滤那些即使是内嵌在邮件体中的 URL，彻底消除了各种已知和新兴的恶意邮件对企业网络的安全威胁。

联系我们

开始了解IRONPORT

IronPort的销售代表，渠道合作伙伴和技术支持工程师随时准备着协助您评估IronPort的产品将如何帮您把邮件系统变得更加安全可靠和易于管理。如果您认为您的企业可以从IronPort业界领先的产品中受益，请打电话到650-989-6530询问，或者访问我们的网站www.ironport.com/leader



IronPort系统有限公司

北京市朝阳区西大望路3号蓝堡写字楼北区2908室, 100026
电话 +8610-51660876 传真 +8610-51660876-800
上海市淮海中路93号大上海时代广场办公楼26楼, 200021
电话 +8621-51176322 传真 +8621-51777991
电子信箱 cn-info@ironport.com 网站 www.ironport.com/cn

IronPort 系统有限公司是业界领先的电子邮件安全产品提供商，其客户不但包括众多中小型企业，还包括许多位列全球2000强的大型企业。IronPort 为那些面临着管理、保护和发展其至关重要的邮件系统等艰巨任务的企业提供高性能的、易于使用的和技术创新的一流产品。

2005年IronPort系统有限公司版权所有。IronPort和SenderBase是IronPort系统有限公司的注册商标。AsyncOS，上下文自适应扫描引擎(CASE)，邮件安全管理器，IronPort防垃圾邮件，IronPort C系列设备，邮件流中心，邮件流监视器，信誉过滤器，Web信誉跟踪，病毒爆发过滤器和虚拟网关是IronPort系统有限公司的商标。所有其他商标是它们相应所有者的财产。产品规格届时如有变更将不做另行通知。