

消除电子邮件风险： 高级邮件保护七大技术

目录

摘要报告	3
引言	3
入站威胁：垃圾邮件已今非昔比	3
全球垃圾邮件量以及垃圾邮件占有所有邮件的比例呈现持续增长态势	4
犯罪因素越来越多	4
威胁阴云笼罩电子邮件	4
出站威胁：敏感数据外泄	6
电子邮件安全现状：可规避风险持续存在	7
安全与成本节省：二者可以兼得	7
成本节省	7
效率提升	8
增强安全，降低成本	9
新型解决方案	10
总结	10
STAMP — 迈克菲高级邮件保护七大技术	10
基于信誉的多协议防护	10
全局信息与局部情况相结合	11
完整内容检测（包括结构化和非结构化）	11
通过集成策略实施强大的加密以及其他合规措施	12
集成的入站和出站防护	13
混合型解决方案架构	13
企业级可扩展性、稳定性、管理便利性和强大的报告功能	13
总结	14
迈克菲电子邮件安全产品	14
McAfee Email Gateway	14
TrustedSource	15
迈克菲混合型交付架构	15
结论与未来举措	15
尾注	16

摘要报告

电子邮件是当今主要的业务沟通媒介。正因为如此，它成为了黑客、垃圾邮件制造者、恶意软件拥有者垂涎的目标，同时也为粗心或不怀好意的内部人员泄露公司机密信息创造了条件。立法者已经意识到了企业电子邮件安全的重要性，并制定了各类针对电子邮件安全的规则以及与隐私和知识产权保护及归档相关的法规。2008年9月，迈克菲委托 IDC 的分析人员进行了电子邮件安全状况调查¹，范围涵盖北美地区员工人数超过 500 的企业。鉴于我们所面临的威胁和挑战，调查结果令人不安。调查表明，面对当前电子邮件的安全现状，有人居安思危，有人毫不在意。而同时解决方案性能虽达到次优状态，却仍有大量待完善之处。

本文将审视当今的电子邮件威胁、企业防御的现状以及应对日益增加的威胁的计划。最为重要的是，我们将给出针对企业电子邮件安全的技术蓝图 — STAMP（迈克菲的高级邮件保护七大技术）。

引言

与以往相比，如今的电子邮件威胁更加危险。在入站威胁方面，由以牟取不义之财为目的的不法分子策划的混合电子邮件和 Web 攻击越发猖獗。垃圾邮件已经不再是为了强卖，而是意在窃取。攻击越来越有针对性而且行动迅速。犯罪分子更加变本加厉、更加有组织，也更加狡猾。有组织的僵尸网络大军既能够在全球发起攻击，又能迅速地回归到休眠状态。有害负载的不断变化以逃避基于签名的防护，并且更常见的是通过嵌入式 Web 链接而非直接文件附件来传播。每一封渗透过网络外圈的恶意电子邮件都比以往更具风险性。

在出站威胁方面，电子邮件成为敏感和机密信息外泄的主要途径。企业中的人员可访问的信息越来越多，每个人都能够访问电子邮件和 Web。再加上合同工、咨询人员和短期工作人员的临时工作特性，势必导致数据泄露的风险持续加大。由此所导致的业务丢失、罚款、法律诉讼以及品牌受损带来的潜在成本更是难以估计。

而同时，IT 安全专业人员面临的因经济不确定性、业务问题以及不断变化的业务优先级（例如，绿色计算和外包完全业务往往被排在后面）所产生的预算和成本压力也不可小觑。

由迈克菲组织的 IDC 调查揭示了令北美地区企业中负责电子邮件安全管理的 IT 专业人士感到放心和不安的问题。近 60% 的被调查者表示，与最佳实践相比，他们实现了较为优化的入站电子邮件安全保护，只有 3% 的被调查者表示对入站电子邮件安全保护不满意。几乎 90% 的被调查者表示，非常担心通过电子邮件导致的数据泄露，只有不到三分之一的被调查者企业实施了相关解决方案。这种不作为部分原因应归结为缺乏有效的评估可用解决方案的框架，因此，无法选择到既功能强大又经济高效的解决方案。

根据客户体验、IDC 白皮书、由 TrustedSource™（迈克菲全球多协议信誉系统）收集的数据以及第三方资源，本文将概述当今的电子邮件威胁并阐述大多数现有电子邮件安全解决方案难以提供充分的安全保护的原因。然后，我们会提出一个解决方案框架 — 迈克菲的高级邮件保护七大技术（STAMP）。

入站威胁：垃圾邮件已今非昔比

垃圾邮件几乎与 Internet 相生相伴。早在 1978 年，APARANET 用户就收到过未经请求的营销邮件。这些邮件又迅速演化为 USENET 和 MUDder 邮件。^{2,3} 上世纪九十年代中期，垃圾邮件主要是未经请求的邮件，至 2005 年，每天的垃圾邮件量超过了 500 亿。⁴ 自 2005 年起，迈克菲的 TrustedSource 研究团队一直对垃圾邮件量的变化进行跟踪，结果表明垃圾邮件量激增的趋势没有减缓的迹象（参见图 1）。现在，平均每天的垃圾邮件量超过 1590 亿 — 占全球电子邮件量的 80% 以上。

全球垃圾邮件量以及垃圾邮件占所有邮件的比例呈现持续增长态势

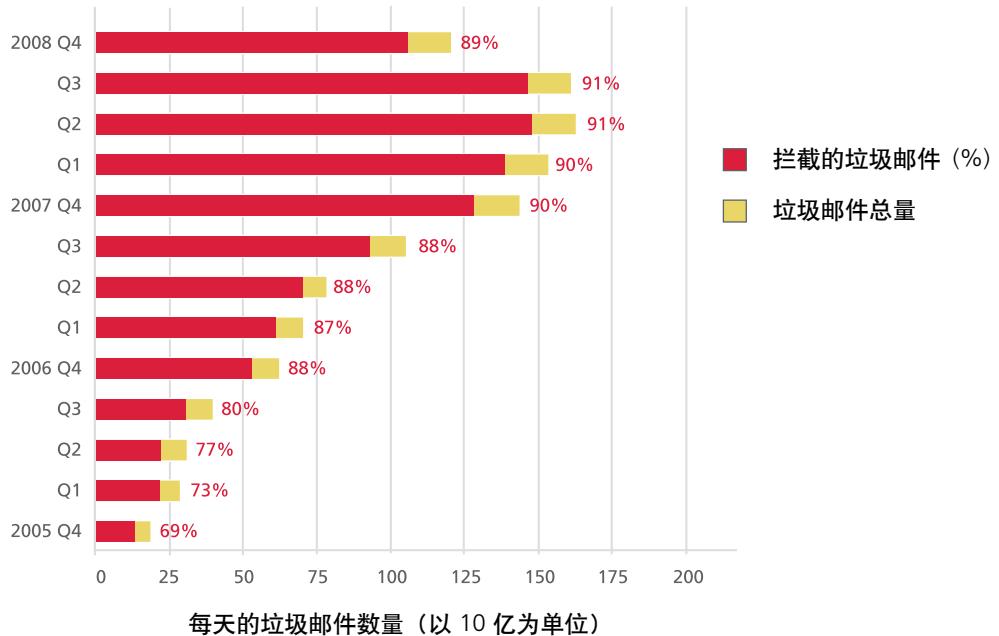


图 1：垃圾邮件不断增长。（信息来源：McAfee TrustedSource.org）

垃圾邮件已进入网络犯罪领域

如果当今的垃圾邮件仅仅是在量上有所增加，那么它们还不构成威胁或者说还是“良性的”。尽管这些“不请自来”的电子邮件耗费了带宽，降低了效率，然而真正的威胁在于当今垃圾邮件制造者的动机和狡猾程度。垃圾邮件制造者已不再仅仅是一些寻找商机的商人，受经济利益驱使的有组织犯罪人员已开始加入这一行列。表 1 显示了垃圾邮件今昔对比情况。迈克菲预计，如今 20% 的垃圾邮件或者自身携带恶意软件攻击或者包含指向恶意软件攻击的链接。

	平稳期 (1995 年至 2007 年)	爆发期 (2007 —)
有效负载	嵌入	链接
动机	营销和欺诈	窃取信息和资源
组织结构	个人或小组	有组织的犯罪网络
基于签名的防护的成效	高	低
主要伎俩	以量为主	以量为主和社会工程

表 1：垃圾邮件今昔对比

威胁阴云笼罩电子邮件

也许没有一个例子比臭名昭著的 Storm 僵尸网络能够更好地说明当今垃圾邮件威胁的严重性。包括迈克菲在内的许多公司都对 Storm 进行过深入研究（要了解有关 Storm 的全面分析，请参阅迈克菲的白皮书：*Storm: The First Comprehensive Solution for Internet Fraud.*）

Storm 僵尸网络最初是作为一系列电子邮件出现的，这些电子邮件引诱用户点击一个嵌入式可执行文件，该文件以一段席卷欧洲的风暴的视频为幌子。如果用户点击了该可执行文件，其计算机就会成为一个僵尸 (bot)。一段时间内，Storm 持续以指向一些突发事件的链接为诱饵来嵌入恶意文件。参见图 2 示例。

白皮书 消除电子邮件风险：高级邮件保护七大技术



图 2：一封早期的 Storm 垃圾邮件

虽然这可能看似粗制滥造，但 Storm 的制造者们很快改变了伎俩，利用社会工程来引诱用户。图 3 显示了一个“更精致”的示例。

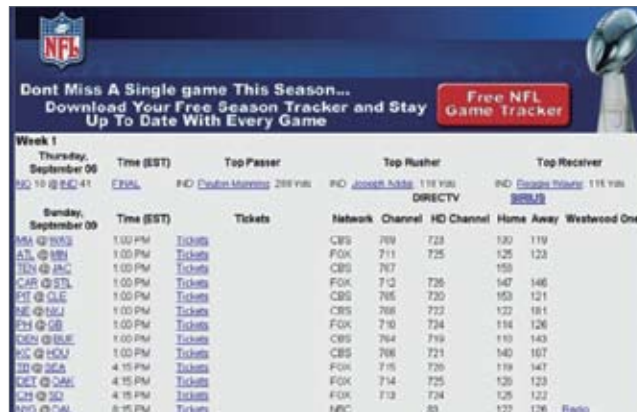


图 3：后面出现的 Storm 垃圾邮件更煞费苦心，也更狡猾。

据预计，在其高峰期，Storm 僵尸网络的节点数量曾达到 1000 万。随着一些漏洞被修补，有些人认为 Storm 威胁的时代结束了。另外一些人则预期 Storm 将卷土重来或者被更新的僵尸网络大军（例如，Nugache）取代。⁵ 实际上，Storm 在 2008 年 7 月借助一封有关“Amero”货币取代美元的电子邮件“重现江湖”。⁶ 无论如何，Storm 为我们提供了了解这一新出现的犯罪威胁的目的和伎俩的有效途径。在许多方面堪称是开创性的，其中包括⁷

- **网络隐蔽性** — Storm 使用高级网络技术来隐藏发送方身份
- **弹性** — Storm 率先采用了分布式 P2P 命令和控制以及其他技术来阻止研究人员的关闭尝试。
- **耐性** — Storm 并非是一种不间断攻击，在谋划下一场“完美风暴”之前，它会有一段相当长的静默期。
- **多途径感染机制** — Storm 采用混合型 Web 和电子邮件攻击充实了传统的基于电子邮件的病毒攻击方式。
- **社会工程** — Storm 不断创新新的社会工程攻击。
- **变形** — Storm 的恶意软件不断变形以规避基于签名的防护。
- **自防护** — Storm 率先使用了自动防御性的自防护机制，能够启动分布式拒绝服务 (DDoS) 攻击来防范分析僵尸网络的研究人员。
- **垃圾邮件创新** — Storm 拥有一系列垃圾邮件方面的创新，包括基于 PDF 和 Excel 的垃圾邮件。

白皮书 消除电子邮件风险：高级邮件保护七大技术

Storm 现象证明了新的混合电子邮件和 Web 垃圾邮件威胁的复杂性和狡猾性

- **桌面隐蔽性** — Storm 采用新的技术来避免导致受感染计算机明显的性能下降。
- **模块化** — Storm 攻击组件是模块化的和分段化的。

Storm 凸显了新的混合电子邮件和 Web 垃圾邮件威胁的复杂性和狡猾性。它揭示了当今垃圾邮件发送者如何在传统防御下规避检测、继续求生的现状，也暗示了垃圾邮件如何从“不痛不痒”一步步发展成为恶劣的犯罪行为。虽然 Web 2.0 威胁的非电子邮件部分吸引了大量关注，但 Storm 事件充分说明 IT 安全保卫战始于有效的垃圾邮件防护，同时也将终于此。因此在当今这个时代，即使投以重金购买电子邮件安全解决方案依然无法抵挡垃圾邮件数量的疯涨，依然不能让 IT 安全管理员高枕无忧，这就不足为奇了。

出站威胁：敏感数据外泄

数据泄露已成为近年来的热门话题。工业、政府部门和新兴组织等领域都频频经历数据泄露和安全事件，包括 2006 年美国共和党全国委员会不慎将捐赠者姓名和社会保障号电邮给了《美国太阳报》的记者这一引起巨大轰动的事件。最近的一个事件是 2008 年 7 月，加州消费者事务部的一名离职员工将 5000 份个人文件发送到了她自己的 Yahoo! 帐户中，其中包括员工姓名和社会保障号。

企业员工、合同工以及其他内部人员对机密信息的访问越来越多，这些信息很容易通过电子邮件和 Web 通讯措施泄露。而且很多工作人员习惯使用电子邮件作为存档系统，他们借助电子邮件文件夹在邮件服务器上保留重要文件。新的报告显示，保护敏感数据的难度越来越高⁸。

- 2008 年 1 月至 10 月中旬，共发生 263 起严重隐私泄漏事件
- 据 FTC 估计，每年有多达 900 万的美国人的身份信息遭窃
- 2005 年 1 月以来，有超过 2.44 亿的美国居民数据记录由于安全事件而遭到泄露

2008 年初，IDC 曾预测：“大多数泄露事件可能具备一定的偶然性，但我们认为由拥有高科技手段的犯罪组织所精心策划的攻击会呈现上涨趋势。”⁹ Verizon 发起的一项为期五年的调查研究¹⁰（如图 4）显示，个人身份识别信息 (PII) 尤其是支付卡数据，已成为数据安全事件中首当其冲的“受害者”。

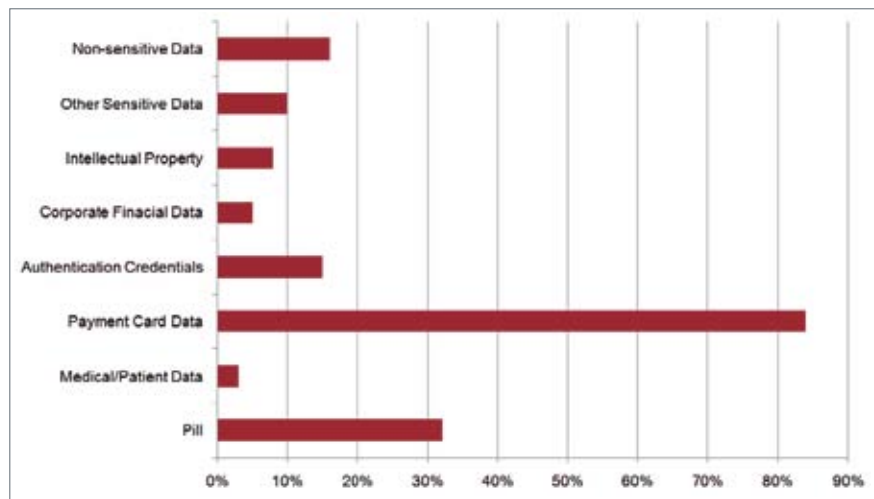


图 4：针对个人和支付数据的数据威胁。（信息来源：Verizon 2008 数据威胁调查报告）

白皮书 消除电子邮件风险：高级邮件保护七大技术

电子邮件安全现状：可规避风险持续存在

面对日益增加和严重的入站和出站威胁，企业电子邮件安全应如何应对？IDC 研究结果证实了先前的预期。调查发现：

- 绝大多数 IT 人士都在高度关注主要的入站电子邮件攻击类别：
 - » 内嵌了恶意链接的电子邮件 (83%)
 - » 包含恶意附件的电子邮件 (86%)
 - » 基于电子邮件的网络钓鱼诈骗 (83%)
 - » 基于邮件的僵尸网络传播 (74%)
 - » 垃圾邮件 (78 %)
 - » 与电子邮件相关的数据泄露 (77%)
- 许多参与调查的人士反映在过去一年里遇到多起电子邮件安全事件
- 虽然电子邮件安全已引起广泛关注，并且安全事件频发，但仍有 60% 以上的调查对象表示其垃圾邮件检测率只有 95% 甚至更低，仅仅 11% 的调查对象的检测率达到了 99% 这一当今行业最高统一标准
- 奇怪的是，在垃圾邮件检测率低于 95% 水平的那 60% 调查对象中，只有 3% 表示对现有解决方案不满
- 很多调查对象表示曾遭遇过通过电子邮件偶然或有意泄露敏感和专有信息的事件
- 虽然有近 80% 的受访企业十分顾虑电子邮件信息泄露问题，但只有 28% 部署了 DLP 解决方案
- 79% 的调查对象承认，一款能够实现入站和出站电子邮件安全的集成解决方案可以降低许可、支持和管理成本，但有很多企业仍在使用单点解决方案

企业期望如此之低原因有二。其一，他们认为这并不能经济高效地带来更佳的结果；其二，他们尚未认识到这样做的优势所在。如果我们假设有 11% 各种规模的企业可以实现 99% 以上的效率，那么每个人都可以做到。这样是否值得呢？一项简易 ROI 模型给出了肯定的答案。

安全与成本节省：二者可以兼得

表 2 中所示的模型展示了部署一流解决方案后带来的两项成本节省和一项效率提升，将企业入站安全效率提高至 99.5%，连接层拦截捕获率^{12, 13} 提升到 80% 甚至更高。

成本节省

第一条控制成本的途径是减少恶意软件感染和相关的清除。据迈克菲估计，有大约 40% 的垃圾邮件包含恶意软件或恶意软件链接。业内直接和间接清除成本预计每次感染超过 10000 美元。结合这些数据以及通常的恶意软件捕获率及用户行为，可以计算出入站垃圾邮件检测效率的提升所能节省的恶意软件清除成本。

第二条途径则是降低存档和带宽费用。通过信誉和收件人验证这类连接层技术拦截消息后，消息发送者就无法与电子邮件服务器建立连接。这就大幅节省了带宽使用，避免了存储垃圾邮件长达七年¹⁴的高昂代价，因为无用的电子邮件再也无法进入。采用了连接控制技术的解决方案能够拦截 80% 甚至更多的恶意电子邮件，而 IDC 研究数字显示只有 13% 的受访企业达到了这一水平，并且有 41% 尚未部署这项技术。

效率提升

ROI 模型还表明，通过减少花在打开、识别和删除垃圾邮件上的时间，可以有效提升用户的工作效率。表 2（第 9 页）显示，对于一家目前整体垃圾邮件拦截率为 95%、连接层捕获率为 60% 的 1000 人的组织来说，部署一款更有成效的解决方案每年可以节省成本 270700 美元。按照每年每个用户 30 美元的成本计算，这样一款解决方案的总 ROI 在 1800% 以上。

白皮书 消除电子邮件风险：高级邮件保护七大技术

增强安全，降低成本

关于企业的假设	
每个企业用户每天收到的“正常”电子邮件的平均数	50
用户从网关外部收到的“正常”电子邮件的比例	20%
现有解决方案的垃圾邮件过滤准确率	95%
现有解决方案的连接层拦截率	50%
企业内的用户数	1000
每年全面负担的平均用户成本	\$100,000
现有解决方案下每年每个用户的成本	\$15
关于行业的假设	
全球范围内“恶意”电子邮件的比例（涵盖整个 Internet）	80%
一流解决方案的垃圾邮件过滤准确率	99.5%
一流解决方案的连接层拦截率	80.0%
包含恶意软件或恶意软件链接的垃圾邮件比例	20%
每次恶意软件感染的清除成本	\$100,000
用户花在打开、处理和删除垃圾邮件上的时间（单位：秒）	30
每传送 20KB 消息花费的存档成本	\$0.005
每传送 20KB 消息花费的带宽成本	\$0.005
一流解决方案下每年每个用户的成本	\$30.00
计算	
每个用户每天收到的来自网关外的“正常”电子邮件数	10
每天收到的来自网关外的“正常”电子邮件总数	10,000
网关外试图向企业内部发送的总电子邮件数	50,000
每天试图发送的垃圾邮件总数	40,000
现有解决方案下每天发送的垃圾邮件总数（95% 的垃圾邮件过滤准确率）	2,000
一流解决方案下每天发送的垃圾邮件总数（99.5% 的垃圾邮件过滤准确率）	200
通过一流解决方案每天在连接层拦截的额外垃圾邮件数	12,000
一流解决方案下每天无法发送到用户的垃圾邮件数	1,800
一流解决方案下每天无法发送到用户的含恶意软件的垃圾邮件数	360
一流解决方案下每天避免的恶意软件感染	2.0
每打开一封垃圾邮件带来的效率损失	\$0.40
增加的解决方案总成本（按现有解决方案 15000 美元、一流解决方案 30000 美元计）	\$15,000
硬性成本节省	
节省的恶意软件清除成本	\$52,000
连接层降低的带宽和存档成本	\$31,200
总计硬性成本节省	\$83,200
硬性成本 ROI	
效率增益	\$187,500
总成本节省（硬性成本节省+效率增益）	\$270,700
总 ROI	
	1,805%

表 2：针对拥有 1000 名员工的企业的 ROI 模型。

企业在部署全新且更有效的解决方案后，还能获得额外的好处。除了入站安全保护方面的回报。企业还能有效降低出站数据泄露的风险，节省管理成本，并通过厂商整合提高管理灵活性。

新型解决方案

调查对象还透露，部署全新的交付模式也是他们发展计划的一部分。超过三分之一的调查对象计划在明年部署虚拟安全设备。超过半数的认为，一款混合型解决方案（综合托管解决方案和现场设备）可以更好地抵御入站和出站电子邮件威胁。有趣的是，只有 11% 的人认为只部署托管解决方案才是最佳途径。无论是出于绿色计算的承诺还是迫于成本压力，企业都要寻求改善电子邮件安全解决方案的交付效率。在降低成本、提升效率的同时，企业必须确保维持或改善整体安全状况。

总结

即使面临当今并不可观的经济状况，企业高管们依然正确认识到电子邮件安全的重要性，并愿意投资于新的解决方案。96% 的调查对象表示，企业高级管理层十分清楚电子邮件安全的重要意义，有近 60% 预计会增加电子邮件安全解决方案方面的投资。

总的来说，虽然目前成本和风险状况并不乐观，但企业仍对次优的入站安全现状表示满意，并且没有广泛部署足够的出站安全措施。他们部署了过多的解决方案，现在有机会对提供商进行整合。最后，他们计划大力应用全新的解决方案。

草率的进行解决方案替代和整合并非明智之举，企业必须首先清楚解决方案之间的差距 — 具备次优性能且管理成本更高的解决方案 VS 高度集成、有效且易于管理的全面解决方案。迈克菲综合分析了其中的差距，并提出了实现高级邮件保护的七大技术。本文重点剖析了这些技术。迈克菲建议企业在考虑新的电子邮件安全解决方案时应根据自身提供相应功能的能力进行评估。

STAMP — 迈克菲高级邮件保护七大技术

电子邮件安全技术已日趋成熟。许多基本功能 — 如能够抵御入侵、拒绝服务 (DOS) 攻击和目录收集攻击 (DHA) 的安全消息传输代理 (MTA) 都已广为人们所熟悉。但是，我们从上述内容中了解到，当今许多解决方案并不能有效地拦截形形色色的威胁，或者很好地与业务环境兼容。为了经济高效地保护企业免于各种入站和出站电子邮件风险，电子邮件安全解决方案必须具备以下功能：

- 基于信誉的多协议防护
- 全局信息与局部情况相结合
- 完整内容检测（包括结构化和非结构化）
- 通过集成策略实施强大的加密以及其他合规措施
- 集成的入站和出站防护
- 综合解决方案架构
- 企业级扩展能力、稳定性、管理便利性和强大的报告功能

本文接下来的部分将详细介绍这些功能。

基于信誉的多协议防护

与评价财务行为（借款数、延迟付款、贷款拖欠等）的信用分数一样，信誉服务会根据 Internet 实体的网络行为（是否曾一次发送过数百万封邮件、是否与已知钓鱼网站有关联、是否存在恶意软件等）为其评定一个分数。这些分数有助于安全管理员确定是否允许与这些实体之间建立连接。

许多信誉服务都有一个重大缺陷，就是只能评估 IP 地址。多数情况下，这种评估只限于表面。有些服务仅提供 +10 - -10 的分数范围，这样管理员就没有足够的信息来判断解决方案如何得到这一分数。能否想象在申请抵押贷款时只得到了 +8 的信用分数却没有任何解释是什么情形？

真正成熟和先进的信誉服务应能够对多种类型的 Internet 实体进行评分，然后通过关联构成形成详细、精确的图像。在您评估信誉服务时，应该重点关注提供了多种因素并且附有说明的评分。有些情况下，负分可能是根据与您特定的环境无关的条件评出的。

全局信息与局部情况相结合

虽然关于 Internet 世界的信息十分有用，但有些信息可能并不是您需要的。这就是成熟的安全解决方案能将全局信息与局部情况相结合的原因。举例来说，有些组织会将电子新闻稿视为垃圾邮件，而其他组织可能制定了更为灵活的策略，允许他们的用户接收电子新闻稿。有些会阻止带有公共 Web 域（Hotmail、Gmail、Yahoo、AOL 等）的电子邮件，有些则允许这些流量。

最佳的深度防护策略是综合全局和局部标准部署有效且可定制的电子邮件安全解决方案。有效的使用将使垃圾邮件的拦截更轻松。仅仅基于全球信誉服务就能拦截 80% 以上的垃圾邮件，而基于局部信息还能阻止额外的 19.5% 的垃圾邮件。合适的组合有助于企业将整体垃圾邮件拦截率轻松提高到 99.5% 甚至更高。

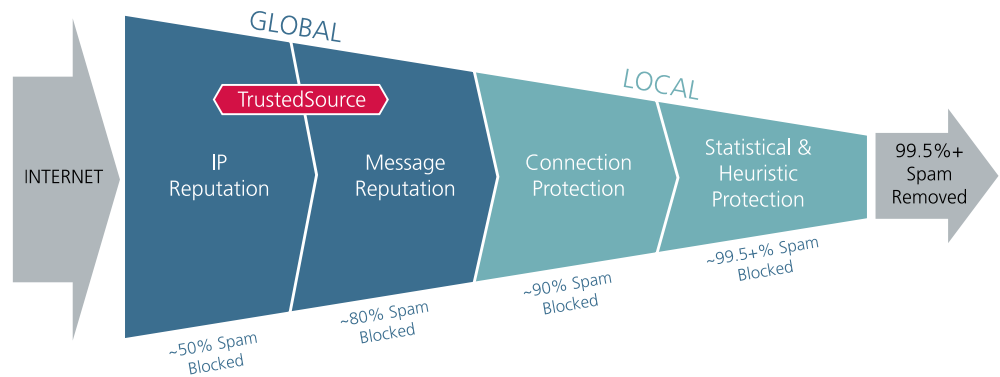


图 5：全局信息与局部情况相结合实现了超过 99% 的垃圾邮件拦截率。

完整内容检测（包括结构化和非结构化）

数据泄露是当今企业面临的最大的安全问题之一。如何保护知识产权以及监管数据成为广泛关注的话题。但相关的支持技术却是极其复杂。由于大多数面向移动数据的安全产品只能执行关键字匹配，因此对于垃圾邮件发送者来说，使用一些肉眼可以看到而计算机无法识别的内容取代关键字以达到掩饰目的是十分轻松的。举例来说，Viagra 一词可以通过多种方式隐藏：

- \ / i a g r a
- V1agra
- Vi@gr@
- Y agra
- V/i/a/g/r/a
- Vi?agr?

白皮书 消除电子邮件风险：高级邮件保护七大技术

上面是六种可能的变形。实际上，这个六个字母组成的单词可以采用超过 600,426,974,379,824,381,952 种方法表示¹⁵。

结构化数据（比如社会保障号或信用卡号）遵循可预测的模式，而非结构化数据则可以是任何内容。有效的解决方案可以提供我们所依赖的相同深度防护逻辑，在结构化和非结构化数据于企业内外转移时予以识别。HIPAA、PCI DSS 等许多法规支持关键字匹配，所以一款有效的解决方案应能针对所有的美国主要现行法规及其定期更新提供丰富的字典库。此外，企业应促成先进技术之间的协同工作，在各种敏感数据离开企业前提前识别。这些技术包括：

- **指纹识别** — 通过独一无二的方式识别敏感性文档，从而对部分或整个文档进行跟踪
- **高级词法分析** — 仔细检查单词、词组、间断性单词以及紧邻的多个单词，从而检测匹配的内容，即使包含误拼写单词、改变顺序的句子和段落或者大范围单词替代也无妨
- **类似文档归类** — 检查邮件内容或附件，并将其与已识别为应保护文档的已知文档进行比较。
- **高级内容分析** — 搜索一些措辞的组合，这些措辞用在一起时会违反策略，而单独使用时则不会

通过集成策略实施强大的加密以及其他合规措施

SOX、HIPAA、PCI DSS 等法规要求，敏感性信息在企业内外移动时必须进行加密。最佳也是最可靠的实施加密的位置是网关。这可以避免由于人为疏忽导致企业蒙受不合规的风险。

有两种基本的加密方式是可以选择的，具体取决于内容和通讯手段的性质：

- **网关-网关** — 在企业网关之间进行传输时对邮件进行加密
- **网关-用户** — 为发送给不具备加密/解密功能的用户的邮件进行加密

有效的电子邮件安全解决方案应同时支持两种加密方式，并可以让用户根据策略灵活地选择。灵活的解决方案要提供如下面向网关-网关加密的选项：

- **SSL/TLS** — 使用 SSL/TLS（安全套接层/传输层安全）创建通向收件人服务器或客户端的安全“隧道”
- **S/MIME** — 使用 S/MIME（安全/多用途网际邮件扩充协议）加密邮件并安全发送
- **OpenPGP** — 使用 PGP（可靠加密）加密邮件并安全发送

网关-用户加密选项应包括：

- **电子邮件推送** — 将加密的邮件发送给用户，并提示用于解密邮件的密码
- **电子邮件存放** — 将加密的邮件存放于安全的 Web 邮箱中，供用户使用密码检索
- 得到业内高度认可的桌面和网关加密解决方案

通过识别传输中的敏感内容并应用基于策略的加密，可以让您实现全面的出站数据保护，如下图所示。

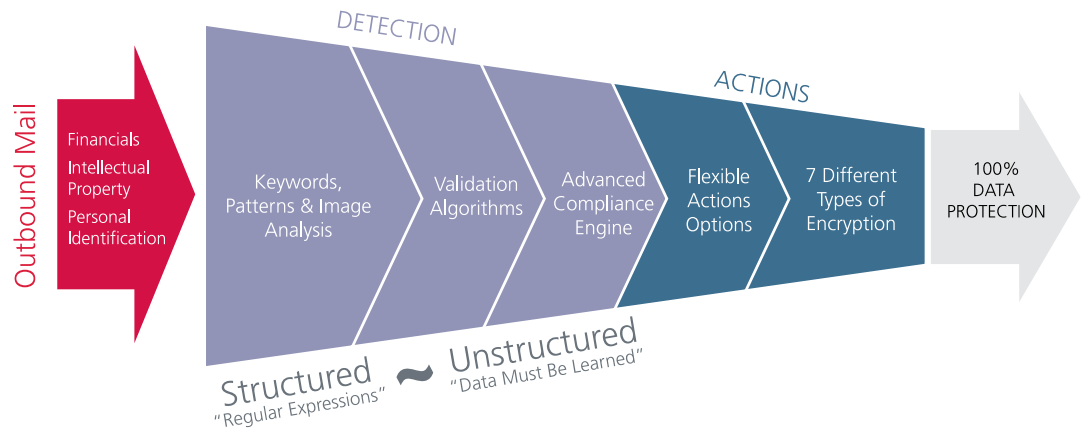


图 6：通过综合检测和加密功能有效防止数据泄露。

集成的入站和出站防护

如果是使用单点产品来保护入站和出站的电子邮件，则会使电子邮件安全管理过于复杂。全面的解决方案则能够通过一款易于部署和管理的产品提供集成的入站和出站防护。

混合型解决方案架构

混合型解决方案架构是指一项涵盖技术和业务的架构，能够在托管、虚拟和设备平台上提供灵活、可靠的交付、便携性以及安全服务组合。它能够让 IT 安全人员有效地抵御当今新出现的以及不断变化的威胁，同时充分利用所有三项交付平台的优势。混合型解决方案架构应基于六大设计理念构建：

- 集成软硬件以及虚拟化和托管服务交付平台的可用性
- 完全便携性和主动性安全服务
- 可组合：支持服务部署，可以在交付平台间实现服务“分割”
- 统一服务和定价
- 统一策略定义和管理
- 统一报告

企业级可扩展性、稳定性、管理便利性和强大的报告功能

如果无法轻松高效地管理，那么即使是最好的技术也无法解决任何问题。有效的电子邮件安全解决方案应该能让电子邮件管理员在不影响安全或合规要求的前提下提供投资回报和投资保护，并能够通过丰富的报告和取证功能证明安全性或合规性。解决方案必须可以：

1. 轻松地实施和维护
2. 随着企业需求的变化和业务拓展进行升级
3. 提供极高的可用性和稳定性
4. 自动保证效率，而无需管理
5. 提供现成可用的丰富记录和报告功能

白皮书 消除电子邮件风险：高级邮件保护七大技术

总结

综合使用这七大技术可以有效抵御形形色色的威胁和攻击。下表简要介绍了这七项技术以及其各自的优势。

七大高级技术的优势

技术	优势	避免的威胁类型
基于信誉的多协议防护	<ul style="list-style-type: none">零日威胁防护减少带宽使用减少不必要的归档成本避免购置额外电子邮件服务器的必要降低垃圾邮件带来的影响	<ul style="list-style-type: none">恶意软件网络钓鱼诈骗病毒木马间谍软件未知攻击
全局信息与局部情况相结合	<ul style="list-style-type: none">超过 99.5% 的拦截率零日威胁防护高效的系统处理第一时间拦截威胁	<ul style="list-style-type: none">包含混合威胁的垃圾邮件有害附件非法内容违反策略的行为拒绝服务攻击
完整内容检测（包括结构化和非结构化）	<ul style="list-style-type: none">提前拦截有意图的数据泄露提前避免无意中的误用，避免数据泄露指导用户遵循正确的策略和使用方式自动通知安全和合规主管	<ul style="list-style-type: none">数据泄露违反策略的行为非法内容（入站和出站）有意图混淆受保护数据的行为无意中的数据误用
通过集成解决方案实施强大的加密以及其他合规措施	<ul style="list-style-type: none">强制实施合规措施，即使在员工忘记或不知晓的情况下降低遭窃的风险	<ul style="list-style-type: none">敏感数据在传输过程中遭窃违反策略的行为违反法规的行为
集成的入站和出站防护	<ul style="list-style-type: none">提高运营和管理效率，降低成本集成报告	
综合解决方案架构	<ul style="list-style-type: none">提高业务灵活性实现资源和成本利用最优化避免网站遭受风险，即使没有专业的安全知识也无妨符合环保计划的要求	
企业级可扩展性、稳定性、管理便利性和强大的报告功能	<ul style="list-style-type: none">成本效益提升 ROI强大的合规报告功能	

迈克菲电子邮件安全产品

McAfee Email Gateway

McAfee Email Gateway (原产品名为 *IronMail*) 提供了全面的电子邮件保护功能。集成的入站和出站防护不但可以避免电子邮件携带的威胁和数据泄露，而且能让电子邮件管理员轻松实施管理。McAfee Email Gateway 综合了网络局部信息和 TrustedSource 全局信息，垃圾邮件检测率高达 99% 以上，可以全面防御入站威胁和恶意软件。在合规和数据泄露防护方面，这款产品拥有高级合规功能和最尖端的扫描技术，能够在检测敏感信息的同时，提供最详细、最灵活的管理措施（包括六种不同的加密技术）。而且这款集成的解决方案还支持集中管理，可以通过一个具备企业级报告和记录功能的控制台覆盖所有入站和出站的 Internet 电子邮件。

白皮书 消除电子邮件风险：高级邮件保护七大技术

全面的入站防护可以充分提高用户效率和服务正常运行时间。

- 高于 99% 的垃圾邮件检测率
- 实时零日威胁防护
- 抵御大量垃圾邮件涌入
- 拒绝服务攻击防护

全面的出站防护可以避免信息通过电子邮件泄露，而且不会影响业务运营

- 全面的数据丢失防护 (DLP)：隐私信息和知识产权内容检测和数据泄露防御
- 基于策略的电子邮件加密

全面的管理灵活性可以让您提供最佳的电子邮件保护，并证明其安全性

- 可以根据您的业务需求配置入站和出站策略
- 灵活的部署架构
- 丰富的报告和信息显示板

TrustedSource

McAfee TrustedSource™ 全局多协议信誉服务是同类服务中的“先锋”。它能够评估数千种不同标准，并提供了范围在 -180 至 +180 的信誉分数，辅以相关的说明。管理员可以根据自己的需求精确调整。同时，这项服务还可以评估多种类型的 Internet 实体，并在评分前对分析进行关联。TrustedSource 会为以下各项内容评定分数：

- 发件人
- 邮件正文
- 图像
- 附件
- URL
- 域
- 恶意软件

迈克菲混合型交付架构

虽然很多厂商宣称其解决方案支持多种平台，但只有迈克菲能够在托管、虚拟和设备平台上提供灵活、可靠的交付、便携性以及安全服务组合。

有关迈克菲综合交付架构的更多信息，请参考白皮书“*迈克菲混合型交付架构：IT 执行概要 (The McAfee Hybrid Delivery Architecture: An IT Executive Overview)*”。

结论与未来举措

当今有大量的企业在使用次优的电子邮件安全解决方案。这类解决方案在一定程度上可能增加攻击的成功率以及数据泄露的风险，并且会导致企业无法通过合规审核甚至增加成本负担。企业必须定期更新电子邮件安全解决方案才能确保安全、灵活和经济高效。迈克菲建议，企业在升级到新一代电子邮件保护时可重点关注七大核心 STAMP 功能。McAfee Email Gateway (IronMail) 产品系列（受 TrustedSource 支持）就涵盖了这七大核心技术。它提供了一款全面的客户解决方案，可以有效抵御当今各种企业电子邮件威胁、漏洞和风险。

有关 McAfee STAMP、McAfee Email Gateway 及其他迈克菲解决方案的更多信息，请访问 www.mcafee.com/cn。

如要了解贵企业的全局电子邮件和 Web 信誉，可以试用一下我们的免费信誉报告服务——域状况检查 (Domain Health Check)：www.securecomputing.com/dhc/。

白皮书 消除电子邮件风险：高级邮件保护七大技术

尾注

1. Securing Email Against Today's Threats: A Wake-Up Call on the Benefits of Comprehensive Messaging Security, IDC 文档号 214837, 2008 年 10 月
2. http://en.wikipedia.org/wiki/Bronze_Soldier_of_Tallinn
3. <http://www.templetons.com/brad/spamterm.html>
4. http://en.wikipedia.org/wiki/Bronze_Soldier_of_Tallinn
5. 有关针对 Storm 未来的争议和不同见解, 请访问: http://en.wikipedia.org/wiki/Bronze_Soldier_of_Tallinn
6. <http://www.offensivecomputing.net/?q=node/799>
7. Storm: The First Comprehensive Solution for Internet Fraud, www.mcafee.com
8. 来源: <http://www.privacyrights.org/index.htm> 和联邦贸易委员会
9. Worldwide Security 2008 Top 10 Predictions: Security's Troublesome Twins, Crime, and Compliance, Ride the Web to Drive 2008 Trends, IDC 文档号 210400, 2008 年 1 月
10. Verizon 2008 数据安全事件调查报告
11. Securing Email Against Today's Threats: A Wake-Up Call on the Benefits of Comprehensive Messaging Security, IDC 文档号 214837, 2008 年 10 月
12. 请参见 Money: Monetary Savings on Network Edge – Year after Year, <http://www.securecomputing.com/pdf/MGS-Monetary-download.pdf>
13. 连接层拦截技术指的是通过分析原始内容（如邮件标题和收件人）在连接层进行操作
14. “Web 2.0 威胁防御的七项设计要求”白皮书, <http://www.securecomputing.com/SWAT/>
15. 来源: <http://cockeyed.com/lessons/viagra/viagra.html>



McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee、迈克菲和/或此处提及的其他标志是 McAfee, Inc. 和/或其分支机构在美国和/或其他国家/地区的注册商标或商标。本文提及的所有其他注册和未注册商标都是其各自所有者的专有财产。© 2009 McAfee, Inc. 保留所有权利。
项目代号: 5390wp_stamp_mail_0109_fnl

迈克菲（上海）软件有限公司

北京市朝阳门外大街 16 号中国人寿大厦 1709 室 邮编: 100020 电话: (8610) 85722000 传真: (8610) 86752299
上海市卢湾区湖滨路 222 号 1 号楼 企业天地 1101 室 邮编: 200021 电话: (8621) 23080699 传真: (8621) 63406606
广州市天河区体育东路 118 号财富广场西塔 15 楼 106 室 邮编: 510620 电话: (8620) 38860668 传真: (8620) 38860638
迈克菲销售热线: 800-810-0369