思科邮件安全图像分析：防止网络传播暴露图像

挑战

全球 80% 的业务通信都通过邮件来实现，因此，邮件成为了各种规模组织的主要通信方式。[1] 然而，邮件在提供各种业务优势的同时还带来了重大风险，这些风险来自有意使用或以性骚扰形式使用的邮件。

员工通过企业邮件系统发送和接收性暴露内容是一种十分严重的问题和安全威胁。如果不予以制止，此类邮件便会损坏公司文化，进而让工作环境变得不友善，从而使企业承担法律责任。

“如果连续广泛地散播色情内容和侮辱性评论，可能会让工作环境变得不友善。”

– 美国平等就业机会委员会

保护员工免遭性骚扰是大多数雇主应承担的法律义务。雇主应对员工的行为负法律责任，并且可能会面临不利的经济后果。为了避免承担责任，雇主必须证实其采取了一切合理步骤来防止工作环境变得不友善。

至少，雇主应该制定邮件可接受的使用策略，并且对该策略进行有效**实施**、**监控**和**传达**。但是，只有书面策略是不够的。未通过沟通、教育和强制方式实施的策略在解除义务方面几乎起不到任何作用。

*“有效的预防计划应包括明确反对性骚扰的**策略**并且定期明确地向员工**传达**该策略同时还能有效**实施**该策略。”*

– 美国平等就业机会委员会

对于雇主来说，意识不到骚扰的发生实质上不是防御。忽略该问题会带来各种影响，除了损坏公司底线外，如果涉及非法图像，甚至可能会发展到雇主遭到刑事控告。通过主动采取措施来监控和实施策略并就策略对员工加以教育，雇主可以大大减轻以下风险：

- 对公司声誉和品牌的损坏
- 让工作环境变得不友善
- 降低工作效率
- 性骚扰诉讼
- 刑事诉讼

[1] 来源：Radicati，2011 年

解决方案

思科® 邮件安全图像分析解决方案可过滤性暴露图像附件，并且经过许可可以用于屡获殊荣的思科 X 系列和 C 系列邮件安全设备或思科云邮件安全服务。该技术允许雇主执行以下操作，因此可协助企业证实其履行了审慎职责：

- **标识**包含高风险图像附件的邮件
- **监控**滥用邮件系统的用户
- **教育**用户遵守公司邮件使用政策
- **实施**该策略是符合需要的

图 1. 思科邮件安全图像分析使用 12 个不同的检测层来标识传入邮件和传出邮件的暴露内容。

功能

通过思科邮件安全图像分析，可以对邮件图像策略的识别、监控、教育和实施进行控制。

确定

多层检测引擎。思科邮件安全图像分析使用 12 种不同的检测方法来识别通过邮件网关传输的大量合法企业图像中隐藏的暴露图像。

第一代图像分析技术过分依赖不精确的“肤色”分析技术。普遍抱怨此类解决方案的误报率高。思科邮件安全图像分析已将该要素归入较复杂的决策流程的次要部分，可以提供精确的检测，并且误报率非常低。

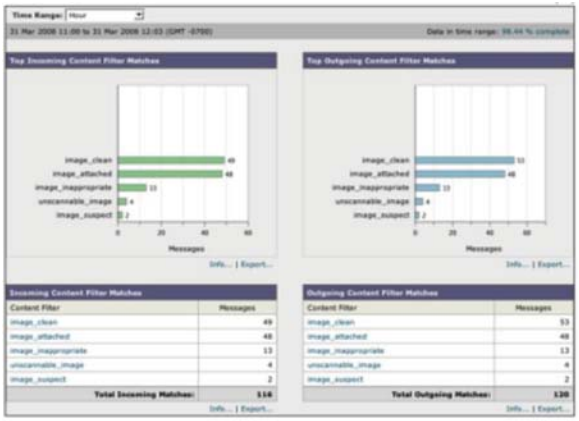
嵌入式图像扫描。思科邮件安全图像分析可以检测以下类型的附件和嵌入式文件：JPEG、BMP、PNG、TIFF、GIF、TGA 和 PCX。如果图像嵌入在另一个文件中，思科的内容扫描引擎可提取该文件。内容扫描引擎可以从超过 400 种文件中提取图像，包括 Word、Excel、和 PowerPoint 文档。

可调节的灵敏度。管理员可以利用灵敏度设置来调节引擎的主动性，从而满足其独特需求。

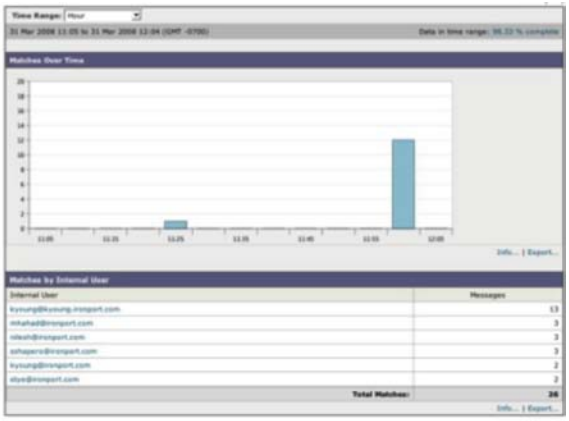
监控

管理报告。许多网络管理员承认他们不知道是否有不适当的图像内容在网络上传播以及何时传播。借助思科邮件安全图像分析，管理员可以生成管理报告，从而了解传入邮件流量和传出邮件流量中是否存在任何滥用情况。根据过滤器匹配项，管理员可以使用现有的报告功能来创建 PDF 和 CSV 格式且易于使用的报告。这些报告可以“按需”生成，也可以安排自动生成并分发给人力资源等其他部门。

图 2. 内容过滤器报告显示特定用户在传入和传出邮件中捕获的不当或可疑图像。



管理员可以通过思科邮件安全图像分析了解入站邮件内容和出站邮件内容。



第一时间关注策略过滤器上匹配率最高的用户。

教育

邮件通知。通过思科邮件安全图像分析，管理员可以选择在用户违反策略时向用户发送自定义邮件通知。这些通知可确保公司可接受的使用策略定期且明确地传达给用户，并且可充当禁止用户将来滥用的强大工具。

实施

策略集成。思科邮件安全图像分析与邮件和内容过滤器相集成，可以基于策略按收件人或发件人进行过滤。现有的过滤基础设施支持根据一个过滤器匹配项来合并多种操作。例如，如果引擎检测到邮件中有暴露图像，可以执行多种操作（隔离或去除附件，在图像上标记公司策略消息等）。

好处

放心。很多公司对通过公司邮件系统交换的图像类型的了解很有限。思科邮件安全图像分析可以让公司放心，因为其邮件系统符合规定并且使用正确。

规避法律责任。如果涉及恶劣的工作环境，美国最高法院判决雇主需要对员工的行为负责。根据美国平等就业机会委员会 收集的数据，每起指控雇主的性骚扰判决成本超过 250,000 美元。即使美国雇主成功赢得此类诉讼，诉讼费也达到平均 100,000 美元左右。但是，根据法院判决和法律规定，如果雇主尽力避免并及时纠正任何骚扰行为，则雇主可以不承担法律责任。思科邮件安全图像分析提供了各种检测、报告和策略实施功能，可以帮助雇主在上述情况下为自己辩护。

“2010 财年，EEOC 在雇主赔偿方面创下了 4.04 亿美元的记录。”

– 美国平等就业机会委员会

维护品牌形象。企业花费重金树立品牌形象，并在全球范围打造这一形象。金融、政府和医疗机构需要树立保守、安全和专业的形象。对大型零售商而言，树立家一样亲和友善的形象非常重要。负面报道对这些精心打造的形象的损害非常严重，可能成为媒体的笑柄并因而损失收入。借助思科邮件安全图像分析，雇主可以持续监控公司邮件传送并采取必要的补救措施，主动防范此类威胁。

保护员工。公司需要采取主动措施来保护员工免受其不当行为的影响，同时保护公司文化免受不当邮件内容带来的负面影响。思科邮件安全图像分析为公司提供了各种有效工具，使其可以在威胁在组织内广泛传播前主动将威胁消除。

提高工作效率。通过主动管理工作场所中的暴露图像内容，可以鼓励所有人员遵守相关规定，并保证工作环境安全，使员工在工作时间不沉溺于非工作相关的活动，从而积极提高工作效率。

国际法律和法规

以下行为可能被视为性骚扰：显示色情内容或者通过邮件传播污秽材料。– 英国平等和人权委员会

性骚扰可以用许多不同的形式呈现，其中可能包括发送性暴露邮件。
– 澳大利亚人权委员会

如果您在工作场所看到性侵犯照片，表明您可能已受到性骚扰。
– 新西兰人权委员会

总结

在公司网络中分发色情和不当图像，表示雇主面临着严重的业务风险。识别采取冒犯行为的用户以及实施公司策略是一些非常重要的措施，可以保护组织避免因此类犯罪而承担法律责任并降低品牌认知度。思科邮件安全图像分析是一种易于使用的解决方案，可以在暴露内容进入或离开组织前对其进行检测和控制。

更多详情

思科通过全球销售团队和经销商网络提供“先试后买”计划。思科邮件安全图像分析和思科邮件安全提供 30 天免费试用版，可以让管理层全面了解公司邮件系统中的任何滥用情况。有关详细信息，请访问 http://www.cisco.com/go/emailsecurity。

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。地址、电话号码和传真号码均列在思科网站 **www.cisco.com/go/offices** 中。

美国印刷 C22-719504-00 10/12