案例研究

DLP 和加密解决方案

在金融、政府、医疗和保险行业的部署

DLP 案例研究

DLP 解决方案在银行业得到证实的结果

1

客户背景

某家为本地小型银行提供 IT 服务的公司有两百个分布于各地的办公室，需要提供一种具成本效益的解决方案来过滤该银行传入邮件中的垃圾邮件和病毒，并保护出站邮件中的敏感数据。由于银行信息特别敏感，防数据丢失解决方案需要严格遵守银行业的相关法规。该公司面对的主要法规包括 SOX、PCI、PII，以及多部各州自行颁布的法规。

技术挑战

该公司需要能够为其客户提供可扩展、可靠而又具成本效益的系统，因此他们必须向所支持的银行提供强大的防数据丢失解决方案。此外，由于该公司为不同的银行提供支持服务，他们需要根据不同银行的具体情况对解决方案进行定制。同时，他们还必须确保银行能够出具针对相关严格法规的合规报告。他们面对的法规包括 SOX、PCI、PII，以及各州自行颁布的法规。

思科的优势

Cisco IronPort 可为公司提供综合性的邮件安全解决方案，不仅具有成本效益，还可扩展。

Cisco IronPort 与防数据丢失 (DLP) 技术领域的领先者 RSA 合作，提供了基于 Cisco IronPort 邮件安全设备的集成的防数据丢失解决方案。RSA DLP 解决方案包括 100 多个预定义策略，用于确保遵守美国和国际法规，因此可以十分容易地为不同公司进行解决方案定制。

由于此解决方案集成在 Cisco IronPort 解决方案内部，因此还可以轻松地根据防数据丢失策略运行报告，以确保银行在云端和设备中的双重合规性。管理员可以访问实时和计划的报告，按策略、严重程度和发件人排序查看主要的 DLP 邮件违规事件。此外，邮件跟踪功能还允许管理员搜索包含特定 DLP 违规的邮件。借助这两个跟踪系统，银行即可向外界证明其 DLP 解决方案的有效性。

建立受信任的关系

2

客户背景

该客户是一家资产规模达 75 亿美元的控股公司，在华盛顿特区和西弗吉尼亚州查尔斯顿设有两个总部，并在西弗吉尼亚、弗吉尼亚、华盛顿特区、马里兰及俄亥俄共计设有 113 家提供全面服务的银行办事处。该客户需要一个能够保证自身符合银行业相关法规的防数据丢失（DLP）和加密解决方案。

技术挑战

该客户目前已部署了 Cisco IronPort 邮件安全设备，但他们仍希望对市场中提供加密和 DLP 解决方案的领先供应商逐一进行考察。该公司寻求的是一款能够同时满足具体基础设施、功能和预算方面需求的最佳产品。

思科的优势

该公司在对多个解决方案进行考察后，清楚地认识到 Cisco IronPort 能够在尽量不影响现有基础设施的前提下对其进行扩展，同时提供最佳的解决方案。该客户目前已在网络中部署了 Cisco IronPort 邮件安全设备，因此可通过升级并启用相关功能的方式来添加加密和 DLP 解决方案。由于 RSA DLP策略以 100 多项预定义策略的形式部署，因此只需通过选择并应用正确的策略即可完成部署过程。客户目前对入站邮件安全解决方案感到十分满意，因此也倾向于部署相同可信品牌的出站安全解决方案。最后，Cisco IronPort 能与客户紧密协作，帮助设立可满足未来 DLP 需求的策略，这让他们十分满意。Cisco IronPort 不仅有最优秀、最易于使用的解决方案，而且是个专注的合作伙伴，因此客户最终选择了部署 Cisco IronPort 的邮件 DLP 解决方案。

扩大服务覆盖范围的同时降低成本

3

客户背景

该客户为包括县警察局在内的县级政府部门提供邮件支持服务。该客户需要为所有政府职员同时配备加密解决方案和防数据丢失（DLP）解决方案，以保护敏感政府数据的安全。

技术挑战

该客户寻求一种可同时满足加密和 DLP 需求并且价格适中的解决方案，同时希望将服务覆盖范围扩大到包含所有职员。客户目前使用 Zix 提供的加密解决方案，但由于其过高的成本和有限的部署范围，客户希望替换掉该解决方案。按现在的价格，该县只能承担为一小部分职员配备加密解决方案的成本，并且他们没有现成的 DLP 解决方案。

思科的优势

Cisco IronPort 可提供包含 DLP 和加密功能的综合解决方案，这让该客户十分高兴，因为他们成功部署过其他思科产品并且对使用体验非常满意。客户执行现场评估时，对 DLP 捕获率和报告功能印象深刻。Cisco IronPort 已经与 RSA 开展合作，RSA 提供的DLP 解决方案具有高捕获率和低误报率的特性。此外，Cisco IronPort 还提供 DLP 违规报告，让客户能够轻松跟踪并监管 DLP 活动。管理员可以访问实时和计划的报告，按策略、严重程度和发件人排序查看主要的 DLP 邮件违规事件。

客户不仅对捕获率和性能感到满意，也对优秀的成本结构大加赞赏。与竞争对手的产品相比，使用 Cisco IronPort 的加密和 DLP 解决方案可为客户节省大量成本。使用 Cisco IronPort 解决方案，客户能够以低于竞争对手的价格为其所有用户部署 DLP 和加密解决方案。

改善医疗行业的通信

客户背景

一家大型地区性医疗卫生组织设立了集成式的医疗服务和设施体系，提供高质量的医疗服务，包括急诊入院到住院治疗和高水平的手术，以及康复和家庭护理。客户需要实施加密和防数据丢失（DLP）解决方案来标识并保护敏感的个人健康信息（PHI）。

技术挑战

客户已于数年前在网络中部署了 Cisco IronPort 邮件安全设备，对入站邮件安全性感到十分满意。出于合规性考虑以及通过邮件发送病患健康信息的实践，客户发现了需要通过邮件加密和 DLP 解决方案来实施出站安全功能的其他需求。这一新技术可使医生安全地与同行、保险公司和病患通信。

思科的优势

客户对之前用于入站保护功能的 Cisco IronPort 邮件安全设施的实施过程无可挑剔。出于对思科品牌的信任，客户目前希望进一步采用思科的 DLP 和加密解决方案。

在对解决方案进行研究后，客户对于思科能够针对其需求提供如此完整而统一的邮件安全功能留下了深刻的印象。Cisco IronPort 出站邮件加密和防数据丢失解决方案得到了客户的独家认可，印证了业内对于此解决方案是适用于企业的最佳方案的评价。

公司还对 Cisco IronPort 与防数据丢失领域内的领先者 RSA 建立合作伙伴关系感到特别满意。凭借该功能提供的预定义模板以及较低的误报率，该解决方案得以进一步领先于其他竞争产品。借助运行于基础设施上的 Cisco IronPort DLP 解决方案，客户现在能够采用受保护且机密的方式与外部医生、保险公司以及病患轻松通信。

现在和未来均可轻松集成

客户背景

该公司是一家提供综合金融服务的公司，为个人、企业和机构投资者提供综合性的理财建议和服务。公司目前已部署了 Google Postini 邮件安全解决方案，但还需要采用防数据丢失（DLP）解决方案来满足合规性方面的要求。

技术挑战

客户需要最优秀的 DLP 解决方案，帮助其应对宾夕法尼亚州和马萨诸塞州颁布的特定法律的要求。客户还需要解决 GLBA、Sarbanes-Oxley、PCI、HIPAA 以及其他法规的一般合规性问题。最后，客户希望能够使用可与现有基础设施完全集成的解决方案来解决未来的合规性要求。

思科的优势

研究众多 DLP 解决方案时，客户对 RSA 的 DLP 与 Cisco IronPort 邮件安全设备的集成所带来的优异性能感到印象深刻。尽管客户最初并无意购买新的邮件安全解决方案，但他们发现购买 Cisco IronPort 邮件安全设备并将邮件安全和防数据丢失捆绑到单一设备可在未来极大地降低成本。他们认识到合并的解决方案不但能改善邮件的安全状况，还可在部署过程中节省大笔资金。Cisco IronPort 邮件安全设备可轻松集成到客户现有的基础设施，并且捆绑的 RSA DLP 功能提供了客户所需的最佳 DLP 解决方案。

客户对 Cisco IronPort 邮件 DLP 解决方案内置 100 多种预定义策略这一点感到尤其满意。这意味着当法规要求随时间变化时可轻松部署不同的策略。

寻找单一平台

6

客户背景

一家拥有 500 多名保户的大型人寿保险公司需要统一其邮件安全解决方案。公司希望与单一供应商合作，实施涵盖入站邮件安全和出站扫描、防数据丢失以及加密功能的解决方案。

技术挑战

公司寻求一种包括加密、防数据丢失和入站邮件安全功能的单一解决方案，并倾向与单一供应商合作。该公司特别强调防数据丢失解决方案能够确保公司实现其合规性要求。

思科的优势

客户考察若干不同解决方案之后，认为许多供应商可针对某一个问题提供优秀的解决方案，但很少有公司能够保证全部三个解决方案都具有优异的表现。由于 Cisco IronPort 邮件安全设备在邮件安全性、加密和防数据丢失方面的强大性能，客户最终选择了此解决方案。

Cisco IronPort 能够统一公司的邮件网关，赋予客户简单的部署和使用体验。由于防数据丢失是关键交付内容，客户选择部署集成了 RSA 邮件 DLP 解决方案的 Cisco IronPort 邮件安全设备。防数据丢失功能简单而且精准的部署过程为客户留下了深刻印象。只需点击一次按钮，公司的管理员即可启用各种预定义 RSA 邮件 DLP 策略，这些策略不仅可用于处理政府法规，例如针对美国的 HIPAA 和针对英国的数据保护法案，也能够应对非政府的行业规定，例如支付卡行业数据安全标准（PCI DSS）。

客户还高兴地发现此解决方案的误报率较低，而误报率问题在其他防数据丢失解决方案十分常见。RSA 邮件 DLP 的预定义策略由 RSA 的信息策略和分类研究团队使用经过专门优化的尖端内容分析技术创建，可消除误报并最大化捕获率。