案例研究

CONCORD HOSPITAL

利用BigFix降低成本，提高安全性，并整合基础架构

客 户

Concord Hospital，美国新罕布什尔，http://www.concordhospital.org

所属行业

医疗保健

挑 战

- 需要将现有的反病毒(AV)管理进行整合
- 需要降低AV管理的直接和间接成本
- 现有解决方案存在潜在的终端性能问题

解决方案

BigFix Endpoint Protection帮助Concord Hospital进一步整合安全和管理基础架构，改善安全状态，并降低整体运营成本。

成 果

- 5~10分钟完成卸载和安装
- 迁移过程中无需求助帮助台，由于对AV端点影响大幅降低，工作站可用性评分从1分提高到6分(共10分)
- 试运行中发现20%的病毒感染率，并且在部署后成功修复
- 硬件更新频率将可以从2~3年增加到5年，从而大幅节省成本

"整合的功能越多，我们必须学习和管理的工具就越少，就能更多地将安全管理整合到日常工作流程中，并且需要更少的代理来服务终端。"

——Mark Starry

企业架构师兼安全主管

Concord Hospital

客户

Concord Hospital是一家位于美国新罕布什尔的地方性医疗中心，为新罕布什尔地区的人们提供综合的急性病治疗服务和医疗保健计划。

挑战

像大多数组织一样，Concord Hospital一直在设法在不增加工作人员的情况下扩展IT 服务和提高安全性。检查其主要IT职能后，我们发现反病毒管理占据太多时间和成本。此外，由于在扫描和签名文件更新期间台式电脑和笔记本电脑性能受到了显著影响，所以最终用户满意度较低。

解决方案概述

BigFix技术可以为Concord Hospital和Capital Region Health Care组织的4800个系统提供资产发现、软件许可管理和补丁管理功能。当他们需要重建反病毒软件的订阅(该产品已无法满足其需求)时，他们很自然地选择了BigFix和他们的合作伙伴Trend Micro，希望获得最新一代恶意软件防护功能、网站信誉评级服务和易管理性。

成果

自2004年安装BigFix以来，未发生过恶意软件疫情，补丁合规性从60% 提高到了93%，医院通过识别和删除未充分利用的软件实现了高达25%的软件许可成本节约。此外，现在还可以对管理EPHI的关键服务器和工作站实施和验证安全控制措施，从而促进了HIPAA合规性管理。

BigFix部署详细介绍

Concord Hospital将BigFix/Trend Micro Core Protection Module和Web Protection Module作为测试项目的一部分进行了实施。在一个小型实验室环境中初步测试后，很快进行了试运行，并在更多端点上进行了实验，结果发现了之前反病毒解决方案未发现的20% 的感染率。"我们获得了一次宝贵的经验——永远不要以为你可以百分之百相信你的反病毒解决方案。"高级网络工程师Mike Goodnow说。

因为Concord Hospital是BigFix的现有用户，部署Endpoint Protection时无需再部署其他软件或硬件。Concord开始对20个终端进行测试部署，并很快在整个企业内进行部署。

卸载和安装平均需要5~10分钟时间，所有的全面扫描均需要30~60分钟时间。实施过程几乎是觉察不到的——在部署的阶段没有一个用户打电话向帮助台求助，只有很少的用户发现旧的AV系统图标托盘已不存在了。

Concord Hospital发现用新的AV替换原有AV后，工作站性能得到了提升。用户调查显示，员工对于工作站可用性的评分从原来的1分提高到现在的6~7分(共10分)。原来，定义更新的发布和全手动扫描会使很多工作站(和部分服务器)的效率受到影响，现在已觉察不到任何影响。Concord甚至在用户没有意识到的情况下进行了多次手动扫描，并查看用户的反应——没有人畏缩。

Concord Hospital还实施了Web Protection Module(WPM)，这是一个云计算客户端解决方案，依据Trend Micro Smart Protection Network 来阻止用户访问恶意网站、阻止下载恶意软件并阻止端点通过 Internet 向收集站点静默地传输数据。他们本来只打算将该组件用于漫游笔记本电脑，但是，当部署Core Protection Module(CPM)的试行版时，他们发现工作站上，甚至是网关保护解决方案的若干层上也存在很多病毒和间谍软件感染。很多网关或边缘保护解决方案都依赖于定时的“定义”或“列表”，而WPM是持续更新的，并且几乎接近我们现在可以实现的实时保护。Goodnow说，“我们认为仅仅依赖边缘保护解决方案还不够，强有力的端点保护仍然是非常有价值的。因此，现在我们在所有工作站上有应用了Web Protection。此外，”Goodnow接着说，“Web Protection Module提供了很好的保护，但却几乎没有增加工作站或笔记本电脑的日常开支——而且到目前为止，我们没有发现任何误报。”

为什么选择BigFix?

Concord Hospital已准备使用BigFix进行补丁管理、配置合规性管理和一般终端管理。将 Trend Micro的反恶意软件、端点防火墙和网络访问控制(NAC)整合到同一基础架构中，使得Concord Hospital可以在降低总体成本和管理经费的同时提升端点安全保护。

展望未来

作为一家医疗服务供应商，Concord Hospital的漫游笔记本电脑与很多组织相比较少。但是，在所有人都迁移至由BigFix管理的Trend Micro反恶意软件后，该团队打算对这些设备上的端点防火墙以及网络访问控制的实施情况进行一个调查。尽管很多外围设备和基于网络的保护已经就位，Concord还是希望可以看到与实施Web Protection相似的结果，因为他们原本以为实施Web Protection的结果会与外围设备保护解决方案相似。

为了从整合中收获更多益处，Concord Hospital正在测试BigFix的操作系统部署，以便从单一的中央位置在整个网络中快速部署新的工作站和服务器。这可以节省时间和资金，实施一个标准且经过批准的映像，降低与不合规或不安全的配置相关的风险。"整合的功能越多，我们必须学习和管理的工具就越少，就能更多地将安全管理整合到日常工作流程中，并且需要更少的代理来服务端点。"企业架构师兼安全主管Mark Starry总结道。

BigFix:突破性技术，革命性经济

BigFix® 成立于1997年，是IBM收购的公司，也是一家全球领先的高性能企业系统和安全管理解决方案供应商，这些解决方案可以彻底变革IT组织用来管理其计算基础架构并保证架构安全的方法。基于直接将管理智能分配给计算设备本身的独特基础架构，BigFix比旧有管理软件更快、更准确和更具适应性。从系统生命周期管理、安全与漏洞管理到端点保护，BigFix解决方案可以跨大部分复杂全球网络将劳动密集型IT任务自动化，从而为组织节省大量时间、劳动力和资金。BigFix为数百万全球分布的计算设备提供实时可见性和控制。BigFix客户包括许多世界上最大、在每个行业最具名望的组织，这些行业包括金融服务、零售、教育、制造业和公共部门机构。关于更多信息，请登录网站www.bigfix.com。

20100829