OGREN group

Eric Ogren
92 Robert Road
Stow, MA 01775
m: 978•618•9240
eric@ogrengroup.com

虚拟补丁修复：行之有效的成本节省策略

Ogren Group 专题报告
2011 年 12 月

执行摘要

由于传统的劳动密集型 IT 补丁修复流程不能足够快地修补漏洞，因此安全主管正在打破僵局，转为使用虚拟补丁修复来保护服务器和桌面免受新的网络威胁。虚拟补丁修复提供了一种行之有效的策略，可在漏洞公布的几小时内提供及时的防护，比传统的补丁修复提前了几周甚至几个月。此外，利用虚拟补丁修复策略，安全主管还可通过减少补丁修复和软件维护频率来实现显著的成本节省。

与漏洞攻击速度相比，应用永久软件补丁和升级程序的传统方式费时费力且对应用程序具有很强的入侵性。在漏洞公布后，攻击在一天之后就会遍地开花；自动攻击带来的大多数损害发生在消息发布后的前 15 天内，而 80% 的攻击出现在 60 天内。即使专注于维护合规的服务器和桌面配置，普通组织仍需 30 多天才能修复标准操作系统和应用程序，而修复复杂的业务应用程序则需几个月甚至几年时间。

虚拟补丁修复使用基于主机的过滤器来检测和清理网络流量，*在恶意软件危及易受攻击的目标之前，在不中断应用程序和业务运营的情况下，高效地修正或阻止有可能会攻击漏洞的应用程序输入流*。Ogren Group 调查发现，将虚拟补丁修复整合到漏洞管理流程的组织可以实现显著的成本节省：

- **通过快速消除服务器和桌面中的关键漏洞，有效避免泄露事件发生。**虚拟补丁修复可在漏洞公布的几小时内快速提供及时保护，防止已知漏洞受到攻击。
- **可以根据 IT 时间表有序进行补丁程序维护。**安全团队以受控方式调查、测试和部署传统的补丁程序，减少令人忧虑的补丁事件的发生率。IT 可以通过延长标准补丁修复周期之间的间隔来节省资源。
- **通过延长旧有系统的寿命来推迟升级成本。**许多组织都有不再具有补丁程序或升级支持的旧有应用程序或操作系统。虚拟补丁修复可让 IT 延长旧有应用程序的寿命，从而推迟重新设计或升级的成本。
- **为虚拟化环境提供具有成本效益的安全性。**组织正在采用虚拟化应用程序，以实现行之有效的成本节省并提高安全性。驻留在服务器上或各虚拟机内的虚拟补丁修复可保护虚拟化环境免受虚拟机创建后发现的漏洞攻击。

本专题报告受趋势科技委托完成，主要强调了趋势科技服务器深度安全防护系统和防毒墙网络版产品中基于主机的虚拟补丁修复带来的安全性和运营成本节省。本报告中的信息来自 Ogren Group 对全球组织企业安全官的调查和访谈。

虚拟补丁修复

虚拟补丁修复是一种基于主机的安全功能，可在通过补丁管理和软件维护等程序应用永久修正之前，保护应用程序和端点免受漏洞威胁。其工作原理不是修改可执行程序（结果会造成质量保证和软件资产管理方面的复杂性），*而是针对网络流，检测入站流量并保护应用程序免受攻击，尽管尚未对漏洞进行永久补丁修复*。虚拟补丁修复增强了组织的补丁修复流程，从而大大减轻了整个补丁修复流程的工作负荷：

- **无需更改应用程序或桌面环境，即可在网络数据路径中轻松应用。**虚拟补丁修复不需要修改应用程序或操作系统，从而减轻了测试和部署补丁程序以及有时从不良补丁程序进行恢复的开销负担。
- **减少使用网络防火墙和路由器规则来避免补丁修复的诱因。**许多安全团队都很注意调整防火墙或路由器规则，以避免应用软件补丁程序，这可能会不必要地阻止流向其他应用程序的合法流量，并可能导致网络中出现不良的维护副作用。
- **维持生产应用程序以实现更佳的运行时间和 SLA 性能。**通过虚拟补丁修复，无需预设非工作时间的停机，即可保护关键应用程序免受漏洞威胁。

虚拟补丁修复可加快补丁修复时间，使关键应用程序和端点始终保持合规性。安全和 IT 团队需要更短的软件补丁修复周期和更少的软件维护修复工作来降低运营成本。此外，对于由于较高的工程成本或长期停机风险而使补丁修复失去吸引力的旧有应用程序来说，虚拟补丁修复是唯一实用的防护方法。

对新漏洞快速做出反应

安全领域最令入注目和使用最广泛的指标之一是从供应商公布漏洞到 IT 在受影响的系统中部署补丁程序所经过的时间。尽管安全团队无法控制攻击何时通过网络到达，但 IT 可以控制攻击者攻击公司基础架构内未经补丁修复的漏洞所需要的时间。在许多情况下，调查、测试和将补丁程序部署到操作系统可能需要 30 天或更多时间，对于应用程序来说，通常需要更久。虚拟补丁修复可在几天内（通常是在几小时内）自动提供补丁程序，从而缩短服务器和桌面暴露于漏洞威胁的时间。虚拟补丁修复所带来的成本节省可以由企业安全团队来证明：

- **降低因为受攻击的漏洞而需要公开披露管制数据丢失的风险。**由于漏洞暴露情况得以快速缓解，因此丢失管制数据的风险以及由此导致的成本高昂的公开披露费用大大降低。
- **减少临时紧急补丁修复或软件修正的需求。**虚拟补丁修复为 IT 以有序方式安排永久补丁修复和软件修正争取了时间。减少了在紧急应用高优先级补丁程序或快速工程修正源代码上花费的资源。
- **服务水平协议和应用程序运行时间均得以增强。**虚拟补丁修复无需应用程序停机即可对漏洞进行补丁修复，从而可以自动保护应用程序和桌面环境的安全。

延长旧有应用程序和平台的寿命

许多组织都有一些关键业务应用程序在不再具有操作系统供应商支持或被视为太脆弱而无法进行补丁修复的操作系统平台上执行。由于种种原因（例如，未从工程角度优先考虑较新的创收应用程序、应用程序长期停机的风险，或之前已付费的应用程序重建成本过高），旧有应用程序可能无法轻易升级到较新的操作系统版本。虚拟补丁修复为 IT 提供了一种替代选择，通过为业务减少合规性、安全性和运营成本问题，延长旧有操作系统平台上应用程序的寿命。

- **虚拟补丁修复可消除对旧有操作系统的高昂支持合同的需要**。例如，Windows 2000 的支持合同起价为每季度 $50,000，而 Oracle 为 Solaris 8 制定了按补丁付费的计划。
- **推迟应用程序更换投资。**虚拟补丁修复可以延长不受支持操作系统上的应用程序的寿命，从而推迟对服务器、操作系统使用授权和应用程序软件升级的新投资。
- **IT 可以通过定制虚拟补丁程序，保护内部开发的应用程序。**与重新设计应用程序软件相比，在网络数据流中部署虚拟补丁程序更加容易。虚拟补丁修复可让组织通过为旧有应用程序应用定制开发的虚拟补丁程序来节省工程费用。
- **虚拟补丁修复可能是旧有应用程序漏洞防护的唯一实用方式。**旧有应用程序或生产系统（例如，基于 Oracle 数据库的应用程序或系统）可能对入侵性软件补丁程序太过敏感，但可以通过虚拟补丁修复进一步进行保护，以免受到攻击。

趋势科技虚拟补丁修复

趋势科技针对服务器和最终用户端点推出的旗舰安全解决方案分别是趋势科技服务器深度安全防护系统和防毒墙网络版，可在企业网络内提供及时的虚拟补丁修复。趋势科技的虚拟补丁修复解决方案可在整个补丁修复流程中（从通知可用补丁程序、识别受影响的应用程序，到最大程度地减少需要应用虚拟补丁程序的点）为 IT 人员节省时间和精力：

- **整合了有关已公布漏洞和可用虚拟补丁程序的通知。**趋势科技虚拟补丁修复利用与主要基础架构软件供应商和行业组织（例如 CERT、SANS、Bugtraq、VulnWatch、PacketStorm 和 Securiteam）的关系，使安全团队不断收到漏洞防护和补丁程序可用性的通知。
- **自动发现应用程序和漏洞。**趋势科技虚拟补丁修复会检测到应用程序的存在，并评估应用程序是否存在漏洞，以便为 IT 提供优先级不同的建议。
- **一个虚拟补丁修复实例可以保护多台虚拟机。**对于虚拟化数据中心应用程序，作为一台虚拟设备部署的趋势科技虚拟补丁修复通过自动保护服务器上所有虚拟机的应用程序漏洞，为 IT 人员节省时间和精力。或者，虚拟补丁修复可在每台虚拟机上单独执行和管理。

趋势科技为组织提供了适用于服务器和端点的完整虚拟补丁修复覆盖范围，作为趋势科技服务器深度安全防护系统产品内的一个模块，以及防毒墙网络版端点保护产品的一个入侵防御防火墙插件。这样，企业安全团队便能通过一致的管理和报告界面，将虚拟补丁修复部署到组织内的服务器和桌面。

趋势科技服务器深度安全防护系统通过一个集中管理的解决方案，为在独立、虚拟和基于云的环境中运行的系统提供基于软件的集成安全，该解决方案包括：

- 深度数据包检查（IDS/IPS、Web 应用程序保护和应用程序控制）
- 防恶意软件
- 双向状态防火墙
- 完整性监控
- 日志检查

企业环境中的防毒墙网络版用户可通过入侵防御防火墙插件获得虚拟补丁修复的优势，证明了一个易于管理的解决方案应具有以下特性：

- 针对操作系统和某些常见应用程序的虚拟补丁修复
- 可接受使用安全策略，可阻止来自特定应用程序（例如，来自社交媒体站点）的流量
- 针对远程和移动企业端点的防火墙防护
- 从网络流量中移除受感染的数据
- 根据端点的位置自动调整安全配置
- 集中管理和报告

Ogren Group 调查还发现，组织不仅将趋势科技的虚拟补丁修复集成到安全流程中，而且这些安全流程还在不断发展，以利用虚拟补丁修复带来的成本节省优势。对 IT 来说，虚拟补丁修复的成熟以及有效的成本节省可让安全团队使用重要的增强功能为业务提供保护，包括：

- **与漏洞管理流程集成，以实现自动化防护。**自动化是降低合规服务器和桌面维护成本的关键。趋势科技已将虚拟补丁修复与领先的漏洞管理供应商集成，以实现服务器和桌面发现、评估和防护的自动化。
- **与虚拟化流程集成，以高效保护虚拟化应用程序和虚拟桌面基础架构。**大型企业已部署趋势科技的创新方法，即在一台同时包含虚拟补丁修复软件的服务器上利用一个防恶意软件虚拟设备。趋势科技的虚拟设备不需要将代理捆绑到各台虚拟机，从而可以增强性能，保持虚拟机的密度，并自动保护无法以其他方式轻松进行补丁修复的虚拟机。
- **与基于云的安全系统集成，以具有成本效益的方式保护服务器和桌面。**趋势科技利用其云安全智能防护网络，将最新的虚拟补丁程序高效馈送到趋势科技服务器深度安全防护系统和防毒墙网络版。

结论和建议

为了降低运营成本，高效满足合规性要求，并灵活地为企业提供新服务，IT 组织正在不断发展其基础架构。Ogren Group 相信，趋势科技的趋势科技服务器深度安全防护系统和防毒墙网络版所提供的虚拟补丁修复是经过检验的能够大幅节省成本的杰出范例，带来了显著的安全优势：

- **反应快速，可缓解关键服务器和桌面暴露于新漏洞威胁的情况。**虚拟补丁修复可及时提供漏洞防护，而无需进行应用程序修改，从而缩短了测试和部署关键补丁程序所需的时间。
- **可以根据 IT 时间表有序进行补丁程序维护（降低了维护频率）。**安全团队以受控方式调查、测试和部署传统的补丁程序，减少了补丁程序部署周期。
- **延长旧有应用程序的寿命。**虚拟补丁修复可移除较旧操作系统（例如 Windows 2000 和 Solaris 8）上已付费应用程序中的漏洞，从而避免费用高昂的支持合同。
- **减少与紧急补丁修复和软件修复操作相关的业务中断及相应成本。**趋势科技自动提供的虚拟补丁修复可让 IT 按照计划的工作日程表对高优先级的漏洞进行补丁修复和软件修正。

Ogren Group 建议企业利用虚拟补丁修复所带来的成本节省优势。尤其是，虚拟补丁修复服务可为 IT 节省时间和金钱，同时还可增强数据中心应用程序的安全性。Ogren Group 相信，对于需要更快进行漏洞防护和补丁修复以确保业务安全性和合规性的安全团队来说，趋势科技通过趋势科技服务器深度安全防护系统和防毒墙网络版代理提供的虚拟补丁修复应在其决选名单中。

虚拟补丁修复成本节省工作表

利用虚拟补丁修复可降低安全风险，同时降低运营成本。根据所选策略不同，各组织的预期成本节省也会有所不同。此工作表可帮助您逐条列举组织使用虚拟补丁修复可节省的成本。

优化补丁修复流程的运营效率

虚拟补丁修复安全的首要任务是保护业务免受恶意代码及管制数据和知识产权遭窃的威胁。虚拟补丁修复过滤器可在几小时内部署完成，从而可在应用永久补丁程序或软件修复之前保护应用程序。

$_____	降低紧急带外补丁修复的年度成本	考虑到 IT 劳动力的成本增加，将测试和应用补丁程序所需的时间也计算在内。
$_____	降低紧急软件修复的年度成本	对于某些应用程序，这包括外包费用或内部计费。
$_____	降低标准补丁修复周期的频率	通过虚拟补丁修复提供的防护，您可以延长标准补丁修复周期之间的间隔，从而使 IT 人员有更多时间专注于其他活动，并减少停机时间。
$_____	增加应用程序运行时间所带来的成本节省	通过虚拟补丁修复，应用程序可以一直保持运行状态，从而增加运行时间，进而提高收入或改进 SLA。
$_____	降低发生泄露事件的风险	缩短漏洞暴露时间，从而降低管制数据丢失几率并防止发生泄露事件。

$_____	降低补丁程序还原的成本	补丁程序对应用程序和操作系统具有入侵性。补丁程序破坏了生产环境下的系统而不得不移除的情况并不少见。
$_____	降低发现可用补丁程序的成本	趋势科技服务器深度安全防护系统虚拟补丁修复会自动监控供应商公告和漏洞来源（包括 CERT、SANS、Bugtraq 和 VulnWatch），为 IT 提供补丁程序的全面通知。
$_____	节省补丁程序适用性调查工作	趋势科技服务器深度安全防护系统虚拟补丁修复会自动识别应用程序及其补丁程序级别。而且，虚拟补丁修复还可减少在防火墙和路由器规则中部署补丁程序应急措施的诱因。
$_____	保护“不可触碰的”应用程序	由于停机成本或风险原因，应用程序可能被视为不能进行补丁修复，例如 Oracle 数据库服务器。

延长旧有平台和应用程序的寿命

旧有应用程序（特别是在 Windows 2000、Oracle 10.1、Red Hat 3 和 Solaris 8 操作系统上运行的应用程序）保持合规性的成本非常高。虚拟补丁修复可通过延长其使用寿命来提高旧有应用程序的投资回报。

$_____	降低旧有平台支持合同的年度成本	供应商可能按补丁程序收费，或对支持停用软件要求费用补偿。
$_____	降低迁移旧有应用程序的成本	延长应用程序的寿命可以推迟在服务器、平台软件和应用程序工程上的投资。
$_____	降低旧有应用程序的持续工程费用	通过虚拟补丁修复，应用程序可以一直保持运行状态，从而使 IT 可以推迟永久软件修正。

虚拟数据中心、虚拟桌面基础架构以及保护面向云的应用程序系统等 IT 举措都是具有战略意义的决策，可以带来长期的成本节省优势。趋势科技服务器深度安全防护系统和防毒墙网络版虚拟补丁修复可及时快速地抑制新漏洞的暴露，并延长旧有应用程序的寿命，从而带来直接的成本节省。此工作表将帮助 IT 分析虚拟补丁修复为其组织带来的影响。