联合 Infoblox 和 McAfee，加强安全保护

单一管理平台，对安全自动化、调整和响应的实时可见性，安全运营团队的效率更上一层

McAfee 和 Infoblox 合作提高整体可见性、提供全面保护，并加快威胁响应速度，让安全运营团队的工作效率更上一层。解决方案将可疑的 DNS 流量导向到 McAfee® Web Gateway Cloud Services，协助进行深层内容检查，包括恶意软件扫描和 SSL 检查。此外，通过在 ActiveTrust 和数据交换层 (DXL) 之间共享情报，组织可以连接安全工具的孤岛，提供跨解决方案的工作流程调整，及时有效地保护网络和 Web 绑定端点。

Infoblox 于 2017 年获得最创新的 McAfee 安全创新联盟合作伙伴称号。

McAfee 兼容解决方案

- Infoblox ActiveTrust
- Infoblox ActiveTrust Cloud
- Infoblox DDI
- McAfee Web Gateway
- McAfee Web Gateway Cloud Service
- McAfee Enterprise Security Manager
- 数据交换层
- McAfee® ePolicy Orchestrator®

联系我们

业务问题

尽管公司已经投资装置各种安全工具，但恶意软件还是能够侵入网络，窃取数据并绕过现有的安全基础设施。防火墙不会调查或过滤 DNS 流量，因此成为恶意行为者最常利用的漏洞。如今，91% 的恶意软件一旦突破了防线，就会利用 DNS 进行攻击。*SC Magazine* 最新调查显示，46% 的受访者说他们经历过基于 DNS 的数据泄露。

能够实时检测和响应 DNS 保护平台侦测到的网络事件和威胁，可以大大加快事件响应速度。但是，无法较易地获取网络数据，就难以基于事件脉络采取相应的行动。

此外，现今组织使用的各种安全工具运作时都各自孤立、互不联系。无法互为操作，不能共享威胁情报，组织就很难对日益频繁的攻击做出有效响应。

要克服上述挑战需要做到以下方面：

- 查看了解 DNS 流量
- 多管齐下检测威胁，修补 DNS 安全漏洞
- 集成 DNS 安全性与生态系统内的其他安全工具

有了 Infoblox 和 McAfee 的集成解决方案，就能在单一平台检视 DNS 和 Web 流量，堵上组织的 DNS 安全漏洞，Infoblox DNS、DHCP、IPAM、DDI 和 McAfee 产品之间的数据也能自动共享。不同的产品纳入集成解决方案后能互为操作，更能防御通过 DNS 流量发动的攻击，而且还可以简化代理分发的管理负担，实现自动化工作流程，快速修复 McAfee 管理的受感染端点，使安全运营团队达到更高一级的效率。

McAfee 和 Infoblox 联合解决方案：DNS 和网络安全、数据共享和调整

Infoblox 和 McAfee 的方案既可在客户所在处就地部署，也能在云端部署，或两者结合，保护遍布各地的设备和用户。

McAfee Web Gateway Cloud Service 与 Infoblox ActiveTrust Cloud 结合

如有数据经 DNS 而泄漏，或发生 DNS 与命令和控制服务器 (C&C) 及僵尸网络之间的通信，Infoblox ActiveTrust Cloud 均能检测并加以阻断。它会自动阻断访问不符合策略规定的内容，并与您的现有安全基础架构共享聚合威胁情报和感染指标 (IoC)，加快修复工作。解决方案参考本地 DDI 数据、借鉴丰富的网络事件脉络，能更清楚检视安全事件，更好地排出应对的优先顺序，并为混合部署实现统一的策略管理和报告。ActiveTrust Cloud 如作为一项交付服务，其特点在于容易配置和使用，无需投入专门的IT资源。它能保护各个地点和位置的设备 - 本地网络、漫游或远程办公室或分支机构办公室。

Infoblox ActiveTrust Cloud 和 McAfee Web Gateway Cloud Service 的集成统一了域阻断和 HTTP 安全，为共同客户提供更广泛的保护。功能包括：

- 对于 Infoblox ActiveTrust Cloud 所识别的可疑但未证实有恶意的连接，McAfee Web Gateway 会作更频密的网络流量检测，以对多个层次的连接尝试进行主动和自适应保护
- 通过利用 McAfee 和 Infoblox 威胁情报的综合功能，共享更广泛的威胁情报，带来更完善的保护
- 提高内容过滤技术，通过扫描可能违反 DLP 的上传操作来管理对云应用及其内容的访问

通过集成方案，就可更快地检测来自各个地点和位置受感染端点或可疑用户的恶意流量和数据泄漏。ActiveTrust Cloud 可自动转向 McAfee Web Gateway，确保企业数据得到实时保护。

此外，Infoblox ActiveTrust Cloud 还与高级 McAfee 端点管理控制台 McAfee ePolicy Orchestrator (McAfee ePO™) 软件集成，后者可以对端点计算机上运行的 ActiveTrust Endpoint Agent 进行集中分发、更新和管理，简化管理任务，从而让联合解决方案的工作流程更为高效顺畅。

集成 DXL 和 McAfee ePO 的 Infoblox DDI 与 ActiveTrust

Infoblox DDI 为设备和网络提供设备发现和单一数据源。网络如有变化，Infoblox DDI 都能得知，如新加入网络的设备、虚拟工作负载拆分，或 DNS 安全解决方案检测到恶意活动。

Infoblox DDI 和 ActiveTrust 使用出站 RESTful 应用程序编程接口 (API) 通过 DXL 发布安全和网络事件主题以及脉络。数据交换层 (DXL) 是整个 McAfee 产品组合及其技术合作伙伴生态系统的威胁情报共享结构。通过共享安全数据，SIEM、用户行为分析，漏洞扫描和移动管理解决方案等应用程序可以将高价值信息纳入其自己的事件脉络用于修复工作，形成严密的保护圈。DXL 主题订阅者可以在其解决方案中集成 DDI 网络更改和识别 DNS 威胁，并根据需要，触发对事件的响应。上述网络和安全事件也可以通过 DXL 引入到 McAfee ePO 管理中，从而实现修复和策略操作。

McAfee 和 Infoblox 联合解决方案参考架构

检测、自动化和调整

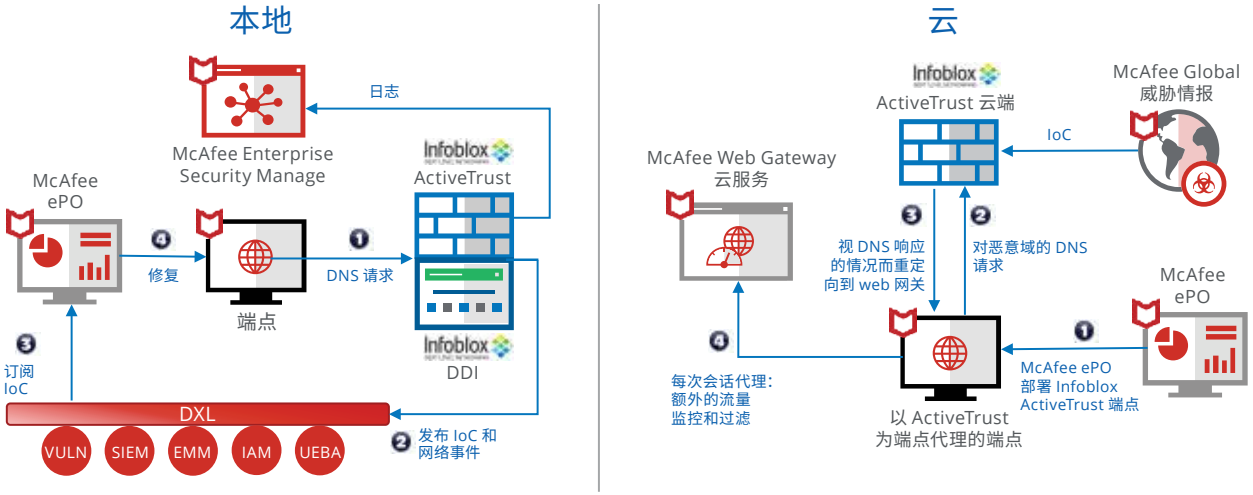

图 1. 解决方案参考架构显示了 Infoblox DDI、ActiveTrust 和 ActiveTrust Cloud 以及 McAfee 安全解决方案之间的集成关系。

集成 McAfee Enterprise Security Manager 的 Infoblox DDI 和 ActiveTrust

Infoblox 与 McAfee Enterprise Security Manager (SIEM) 解决方案共享网络事件和 DNS 安全事件和警报，以实现全面的威胁数据关联和检测。Infoblox 还共享有用的网络事件脉络和可操作的情报 (IP 地址、DHCP 指纹、租约记录等)，以协助评估风险并确定警报的优先级。因此，一旦发生真实风险事件，响应就会更加高效，让安全运营团队的工作效率更上一层。

关于 McAfee Web Gateway Cloud Service

McAfee Web Protection 采用安全网关技术来保护每个设备、用户和位置免受复杂威胁的侵害。

McAfee Web Protection 是结合部署在本地的 McAfee Web Gateway 和云交付 McAfee Web Gateway Cloud Service 的统合式解决方案。本地部署和云解决方案结合部署，就能借助单个控制台管理，且能实施同一个各地设备都适用的共享策略。

McAfee ePolicy Orchestrator 简介

端点管理控制台 McAfee ePolicy Orchestrator，是 McAfee 管理解决方案的基础。30,000 多名客户在超过 6000 万个节点上使用 McAfee ePO 软件来管理网络安全，简化和自动化合规流程，并提高安全管理活动的整体可见性。这套软件的架构可进行扩展且部署快速，又能配合企业系统优化，是目前最先进的安全管理软件。

数据交换层简介

数据交换层 (DXL) 通信结构连接多个供应商产品以及内部开发的解决方案，优化横跨上述方面的安全操作。企业可以实时且安全地获取新的访问数据，并和其他产品作轻量级即时交互。

McAfee Enterprise Security Manager 简介

McAfee Enterprise Security Manager 是 McAfee 旗下安全信息和事件管理 (SIEM) 解决方案系列产品的基础，所提供的功能、可操作的情报以及实时态势感知，不论速度或规模均符合安全组织在识别、了解和应对隐秘威胁方面所需；软件还附带内置的合规性框架，简化合规过程。

Infoblox ActiveTrust Cloud 简介

Infoblox ActiveTrust Cloud 属于 SaaS 解决方案，如有数据经 DNS 而泄露、或发生与恶意软件、命令和控制服务器之间的通信，方案均能加以阻断，还可自动阻断访问不符合规定的内容，并与您的现有安全基础架构共享情报和 IoC，促进调整、加快修复工作。解决方案采纳自动化而快速准确的威胁情报源、行为分析和机器学习，让用户更能应对威胁，甚至可以截获零日威胁。

Infoblox ActiveTrust 简介

本地 DNS 安全解决方案 Infoblox ActiveTrust，可以防止数据经 DNS 而泄露，或使用 DNS 与恶意软件进行 C&C 通信，还能汇总内外部威胁情报，将经过验证的威胁数据分发到客户的安全生态系统进行修复，并可迅速调查以识别事件脉络、排出威胁的优先级。

Infoblox DDI 简介

Infoblox 的安全云管理网络服务，引领着下一代 DDI 的发展。Infoblox 服务让云和混合系统的安全和自动化水平以及可靠性都再上一个台阶，为客户铺好单一网络管理平台的大道。Infoblox 是公认的行业领导者，市场占有率达 50%，服务 8,000 多名客户，其中包括《财富》500 强中的 350 家。请访问 www.infoblox.com 了解更多信息

McAfee
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com