数据表

ActiveTrust® Cloud 云服务

挑战和企业前景

大部分互联网通信都建立在 DNS 的基础之上。攻击者知道 DNS 通常不够安全，而且 DNS 仍然是数据泄露的主要载体。超过91%的恶意软件使用DNS与C&C服务器通信，封锁数据以勒索赎金（勒索软件）或窃取数据。现有安全控制（如防火墙和代理）很少关注 DNS 及相关威胁。

特点和优势

- 威胁洞察：使用分析与机器学习检测和阻止基于 DNS 的数据泄露、DGA、DNSMessenger 和快速通量
- DNS 防火墙/DNS 响应策略区 (RPZ)：干扰与 C&C 的恶意通信，防止恶意软件扩散
- 内容分类：限制和审核访问不良内容（例如社交媒体，成人内容和其他限制级内容）的活动
- 威胁情报数据交换 (TIDE)：收集和管理来自内部和外部的威胁情报，并将威胁情报数据分发给第三方安全系统，以迅速修复威胁所造成的破坏
- 档案整理工具轻松调查威胁：利用类似谷歌的威胁指标调查工具掌握即时威胁环境以及快速分析威胁，缩短攻击窗口
- 使用公共 API 或本地部署集成的生态系统通知：通过使用公共 API 或本地部署的 Infoblox 将安全事件数据提取到生态系统工具中，从而更快地应对威胁
- 云服务门户：借助统一管理、分析和报告的直观门户，无需 DNS 专业知识，就可以根据业务需求定制策略
- ActiveTrust Cloud 端点客户端：使用 SCCM或 McAfee ePO 等自动化解决方案部署轻量级代理，加快大规模部署工作
- DNS 转发代理：将 DNS 查询转发到 Infoblox Cloud，无需端点代理，嵌入客户端 IP；还集成了 NIOS 8.3+，无需安装其他软件
- 报告与分析：深入视察了解侵入行动和被入侵的设备，及其事件脉络详情
- 智能缓存：如果超时，则允许最终用户使用缓存条目连接到目标域
- 具有 EDNS 的递归 DNS 服务：通过高度可用的递归 DNS 服务获取本地的地理位置响应
- 精细的策略管理：能够为不同的用户群体应用不同的策略；设置策略优先级以自定义威胁源、内容类别过滤器的强制执行

当今环境多变，带来更多挑战 —— 劳动力的流动性越来越大、办公室位置分散以及物联网的采用率越来越高。81% 的流动知识工作者将自己的工作设备连接到免费的公共 WiFi 网络，引起安全问题。漫游用户不一定都开着 VPN，而是经常依赖未保护 DNS 安全的防病毒产品。

此外，当今的企业格局也在变化。组织越来越多地使用云服务，原因如下：

- 他们希望用较低的前期成本实现简单、快速、可靠、高价值的实施
- 他们不愿在内部部署/更改架构组件或管理更多的解决方案
- 他们缺乏管理本地基础设施的专用 IT 资源（特别是在远程/分支机构）
- 他们希望利用云的规模和扩展用例（任何地方的保护 - 本地和外部）。

解决方案：使用 ActiveTrust Cloud 随处保护设备

Infoblox ActiveTrust Cloud 云是订购服务，可阻止基于 DNS 的数据 泄露、阻止恶意软件与命令和控制服务器之间的通信、自动阻止访问不符合策略的内容，并与您的现有安全基础架构共享情报和 IoC，加快调整和修复。

该解决方案通过本地 DDI 数据利用丰富的网络环境实现更好的优先级排序，整合和分发存储的、及时且准确的威胁情报，并实现统一的策略管理和混合部署报告。

作为订购服务，无需专用 IT 资源即可轻松配置和使用，并可保护企业网络、漫游或远程办公室/分支机构的所有设备。

主要优势

预防其他系统无法检测到的基于 DNS 的数据泄露 ActiveTrust Cloud 使用独特的行为分析、机器学习和人工智能， 自动阻止数据通过 DNS 泄露。它还利用行为分析技术检测零日威胁，并将与 DGA、DNSMessenger 和快速通量相关联的域添加到响应策略区 (RPZ) 黑名单。

内容分类和策略执行

安全管理员可用 ActiveTrust Cloud 限制访问特定类型的内容（例如社交媒体、成人内容和其他受限类别），并审查组织中的内容活动。

集成到 DNS，尽早检测恶意软件，避免破坏

ActiveTrust Cloud 是一款集成至 DNS 的特定用途解决方案，用于恶意软件早期检测，无需在各处部署基础设施。该解决方案能够利用定期更新和保留的威胁情报，干扰设备与恶意互联网目标的通信，借此自动牵制和控制恶意软件。

利用云来扩展威胁检测，随地都能执行

ActiveTrust Cloud允许客户借助云规模执行大规模分析，并利用威胁情报来检测更多威胁。

更快的威胁调查

ActiveTrust Cloud支持威胁分析师和安全研究人员利用威胁的事件脉络和多个来源的信息轻松调查各种威胁，短短几分钟之内便可采取行动。这一优势能够大大缩短网络罪犯的攻击窗口。

统一的策略管理、分析和报告

如果将 ActiveTrust Cloud与本地 ActiveTrust Cloud 解决方案同时用于混合部署模型，管理员能够无缝管理策略，获得设备活动的完整生命周期视图并利用数据连接器虚拟实用程序获取包含本地 Infoblox Grid™ 数据的全面报告。

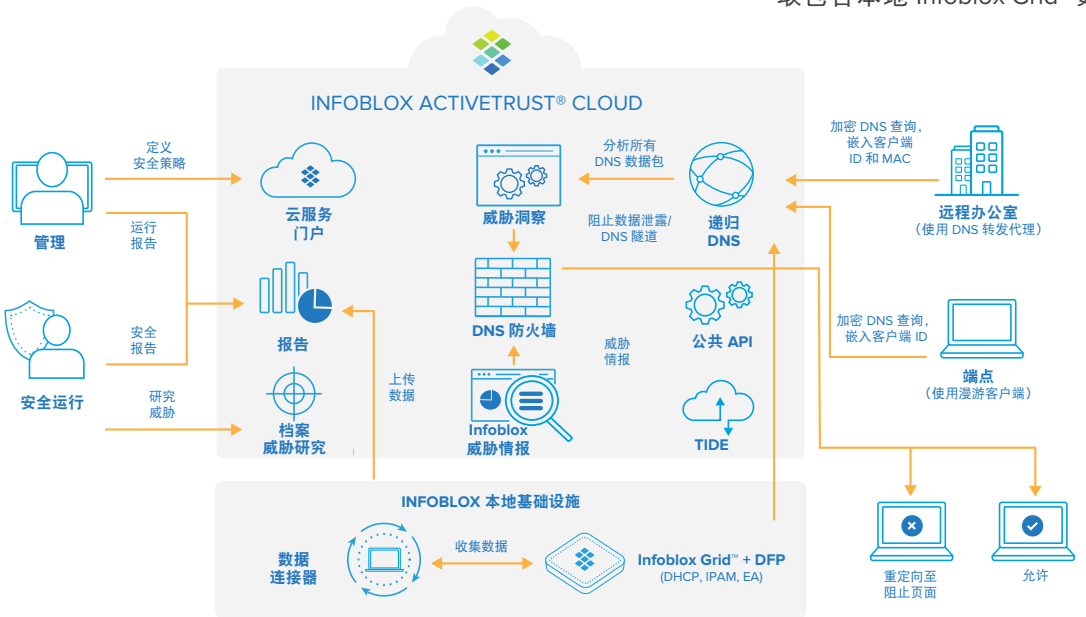

图 1：工作流场景

共享 + 威胁情报数据，加强安全防护

将来自所有源的威胁数据组合起来，使用脉络元数据选择相关子集，并利用正确的格式 (JSON，STIX，CSV，CEF 和 RPZ) 将数据分发给现有的安全生态系统，如 NGFW、Web 代理和 SIEM。安全状况和态势感知能力将能因此大大提高。

提高可见性以及丰富网络环境

ActiveTrust Cloud 通过利用本地数据连接器或 Infoblox 网格来获取 DHCP 指纹，包括 IP 地址、MAC 地址、设备类型、设备操作系统、DHCP 租赁历史等，从而帮助识别受感染的设备。凭借这种深入的可见性，管理员可以了解宝贵的网络环境资讯，从而优先处理需要修复的威胁。

利用公共 API 和本地生态系统集成加速修复

ActiveTrust Cloud 通过公共 API 或利用本地 Infoblox 基础架构轻松访问安全事件，从而加快对威胁的响应。事件数据可以发送到 SIEM，也可以发送到漏洞扫描程序、网络访问控制、端点修复等其他工具。

开始评估

可先试用，再决定是否订购，试用服务过程非常简单。请到以下网址申请 30 天免费全功能试用：http://www.infoblox.com/activetrustcloudsignup.

客户评价

“现在上网打开链接所接触的勒索软件、间谍软件和广告软件实在是太多了。 Infoblox 云服务安全解决方案能阻止用户被转到不良网站，防止设备感染，保护用户安全。”

— 西雅图市大学高级系统管理员和网络工程师

附录：

等级和附加功能

	ActiveTrust Cloud 标准版	ActiveTrust Cloud 增强版
递归 DNS 防火墙 (RPZ 区)	威胁情报源 标准版（6 个信誉数据集） 基础软件 • 反恶意软件 • 勒索软件 • Bogon • 自动指标共享 (AIS) 数据 (2)	威胁情报源 标准版 (6) + 高级版 (7) + SURBL (3) • 基础软件、反恶意软件、勒索软件、bogon, AIS (2) • 恶意软件 IP、bots IP、漏洞利用工具包 IP、恶意软件 DGA 主机名、Tor 出口节点 IP、US OFAC Sanctions IP、EECN IP • SURBL 多域、SURBL 新域、SURBL Multi Lite
内容分类	不含	限制访问云中令人反感的内容
档案 （威胁调查工具）	不含 （仅可通过云服务门户执行基础的威胁查询）	32,000 次查询/年
公共 API（用于生态系统） • 威胁 API • 自定义列表 API	不含	• 包括 - 通过云 API 取得 CEF 或 JSON 格式的安全事件 - 附上更详细的安全报告 • 能够通过 Cloud API 创建自定义威胁源
威胁洞察 （DNS 隧道/数据泄露，DNSMessenger，DGA，Inline DGA，Dictionary DGA，快速通量）	不含	包括基于机器学习的分析

TIDE Infoblox 威胁情报数据交换 (TIDE) 许可——支持在第三方安全解决方案中使用	不含	许可使用以下其中一项：（用于任何非 Infoblox 安全解决方案） • 主机名，或 • IP 地址，或 • URL
报告	基础型 - 所阻断的恶意软件、攻击次数	• 通过虚拟数据连接器实用程序集成本地网格报告 • 利用穿透报表提高可见性，精确识别用户和设备
ActiveTrust Cloud 端点（客户端代理 - 可以使用 SCCM 或 McAfee ePO 部署）	包含	包含
DNS 转发代理	包含	包含
具有地理位置响应的托管递归 DNS（使用 EDNS）	包含	包含

合作伙伴威胁情报

现在，以下市场合作伙伴数据馈送可应用于 ActiveTrust Cloud，以实现基于 DNS 的实施：

ThreatTrack BorderPatrol – BorderPatrol 站点列表是一个由域组成的“黑名单”，这些域涉及发布潜在的恶意软件和广告。

Farsight Newly Observed Domains – 提供增量防御层，以防止恶意软件数据窃取、品牌滥用和基于垃圾邮件的攻击，这些攻击源自或止于新启用的域。

Proofpoint 新兴威胁信誉主机名和动态 IP – 这些动态馈送可以识别可疑和恶意活动中涉及的 IP 和域，正如 Proofpoint's ET 实验室中直接观察到的一样。单独的 IP 地址和域列表。

注：您还可以从 Infoblox 购买这些合作伙伴的情报馈送，作为 ActiveTrust Cloud Plus 的一部分。

Infoblox ActiveTrust Cloud 端点

要使用 ActiveTrust 云服务，管理员可以在设备或工作站上安装漫游客户端 - ActiveTrust 端点。这个小型轻量级客户端代理：

- 将端点的 DNS 重定向至云中 Infoblox DNS
- 在 DNS 数据包中加密以及嵌入客户端身份
- 将登录用户的信息发送到 ActiveTrust 云进行报告
- 当处于由本地 ActiveTrust 提供保护的公司网络时，自动切换到旁路模式

ActiveTrust Cloud 端点可以安装在 Windows (7/8/10) 和 Mac OSX 10.10 – 10.12 上，并且可以使用 SCCM 或 McAfee ePO 等自动化解决方案进行大规模部署。

DNS 转发代理

如果安装端点代理不一定可取或可行（对特定 IoT 设备而言即是如此），则可以使用 DNS 转发代理。这种虚拟设备可将客户端 IP 嵌入到 DNS 查询，然后再转发到 Infoblox Cloud。与端点代理一样，类似的通信也经过加密，并且可以保持客户端可见性。DNS 转发代理也与 NIOS 8.3 及更高版本集成，Infoblox 客户无需在本地安装其他软件。

Infoblox 软件即服务优势

ActiveTrust Cloud 服务利用具有容器化架构，是先进的新一代平台。该解决方案能够随着用户基础和设备数量的增长而水平伸缩每一个组件以及处理请求。

该服务能够：

- 立即改善公司的安全态势
- 立即试用新一代功能
- 将 IT 开销降至最低

可用性（随时随地访问）

Infoblox 全天在线，随时随地都能使用，而且非常可靠，其服务涵盖时间可达到 DNS 基础设施运行时间的 99.999%（不包括定期维护）。Infoblox 能够动用遍布全球的数据中心，进行灾难恢复（任意广播）。Infoblox NOC 持续监测服务，而配置、策略以及用户数据每天都会进行备份。

安全和隐私

为了对您的数据以及您在访问服务时加以保护，Infoblox 采取以下做法：在传输期间加密 DNS 查询，加密所有数据库和已存数据，根据位置、IP 地址和角色限制访问，以及设置控制条件来管理数据移动。

Infoblox 也坚持执行最佳安全实践，如确保所有软件均已修补以及执行渗透测试、静态和动态代码分析。

数据隐私：Infoblox 软件即服务解决方案对客户数据作逻辑分离，且以唯一的 API 密钥来验证身份，借此保护客户数据的隐私。Infoblox 的客户数据一概不与任何第三方供应商分享。

Infoblox
NEXT LEVEL NETWORKING

Infoblox 安全的云服务管理网络服务，引领着下一代 DDI 的发展。Infoblox 服务让本地、云和混合网络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 53%，客户 8,000 多家，其中 350 家位列《财富》500 强。

北京办事处联系方式: 北京市朝阳区东四环中路56号, 远洋国际中心A座6-7楼（邮编: 100025）
电话: 86 010-6105 7675 | 邮箱: GCG@infoblox.com | www.infoblox.com