数据表

Infoblox Threat Defense ™高级版

由预测性威胁情报支持的保护性 DNS 在造成任何影响之前保护任何地方的一切

DNS 是所有网络攻击的最早预防点

DNS 是所有网络攻击的首个检测点和预防点。无论是从网络钓鱼电子邮件、网络钓鱼文本还是被利用的漏洞开始，几乎每一次攻击都会生成一个指向恶意域的 DNS 查询。因此，DNS 提供了一个强大的集中式可视性和控制点，以保护整个企业的安全，包括用户、设备、物联网/OT 和工作负载，无论是在本地、云端还是边缘。

作为任何通信的第一步，在 DNS 层检测和阻止威胁活动有助于在恶意流量到达下游工具并触发警报之前将其拦截。通过将 DNS 数据与设备和资产环境关联，NetOps 和 SecOps 团队可以更深入地了解其环境中的动态，从而提高运营效率和安全态势。

传统的“检测并响应”解决方案已不再有效

威胁行为者正越来越多地利用人工智能发起更多、更复杂且更隐蔽的活动。他们生成独特定制、一次性使用的恶意软件，使传统——依赖“零号病人”感染的那些——“检测与响应”工具失效。每一次攻击都变成没有特征码或已知行为可循的“零号病人”场景。“检测与响应”工具往往在攻击链的后段才发挥作用，无法阻止损害。因此，需要采取一种不同的先发制人的方法。这种方法能在威胁进入环境或横向移动之前将其阻止。这不仅能更早阻止攻击，还能减轻传统“检测和响应”工具的负担。

DNS 作为上游控制点，使安全团队能够更主动地在威胁到达用户、工作负载或终端之前就进行检测与阻止。

基于DNS 的预防性安全

Infoblox Threat Defense™ Advanced 提供了一种独特的 **先发制人的** 威胁检测方法。这种方法不依赖于“零号病人”。它结合了 **预测性威胁情报**在威胁行为者基础架构被武器化之前对其进行阻断，并通过对客户网络中 DNS 查询的算法/基于机器学习的分析，在造成影响之前提供防护。通过快速识别安全事件中涉及的资产、生态系统集成和直观的工作区，它可以实现更快的检测、更快的响应，并提升现有安全投入的投资回报率（ROI）。

事实与数据

- 监控 **204,000个** 实时威胁行为者集群，并且数量还在增加
- 将误报率降低至**0.0002%**
- 在首次查询前阻止了 **82%** 的威胁
- 平均提前 **68.4天**提供防护，在攻击发生前
- 拦截多达 **5** 倍的高风险/中等风险域名，与只查找已知恶意行为的工具相比
- 平均每月节省**500 个 SOC 分析师工时***
- 每年可助力节省 **40 万美元** 的生产力成本*
- 将数以万计的警报减少到少数几条*

SANS 2025 SOC 调查显示，阻碍充分利用 SOC 的十大障碍中有七个涉及警报、工具集成和技能短缺。

*基于真实客户数据。

在威胁产生影响之前阻止

Infoblox Threat Defense 将预测性 DNS 威胁情报与算法/机器学习分析应用于实时 DNS 流量，在威胁活动影响您的网络之前将其拦截，通常检测到其他工具无法检测到的威胁。通过在 DNS 层阻止威胁，Infoblox 还帮助减少警报量和下游安全工具的工作量，客户报告说，下一代防火墙 (NGFW) 和端点检测与响应 (EDR) 系统的警报减少了多达 50%。

“安全 DNS 可以降低 92% 的恶意软件攻击在特定网络上成功部署恶意软件的能力。”

Anne Neuberger，
网络安全总监局，
国家安全局 (NSA)

主要功能	描述	Infoblox Threat Defense	NGFW	SASE	EDR
企业级安全解析器和 DNS 查询日志	使用 DNS 查询数据来查找和判定恶意域名	●	◑	◑	◑
完整 DNS 行为监控	监控所有 DNS 记录类型以检测恶意活动	●	●	◔	○
相似/模拟域名的检测和删除	缓解相似/模拟域名的攻击面	●	○	◑	○
零日 DNS 保护	识别可能对您的组织构成威胁的新兴或新增域名	●	◑	◑	○
基于行为的 DNS 隧道检测	检测用于数据泄露/渗透、C2 通信等的 DNS 隧道。	●	◑	◑	○
主动保护可疑/高风险域名	预先识别并阻止可能在未来恶意活动中被利用的可疑域名	●	◑	◑	◑
自动丰富本地语境	无需客户端或 sinkholing（用户、设备、源 IP、位置、MAC 地址、VLAN）即可关联网络上下文。	●	◑	◑	◑
主动检测与破坏威胁分布系统 (TDS)	识别威胁行为者的 TDS 基础设施，而不仅仅是单个域名，以应对其通过频繁更换域名来规避检测的手段。	●	◔	○	○

图 1：其他工具无法完全覆盖的 Threat Defense 独有功能

THREAT DEFENSE的主要特点

- **“防护优先于影响”监控器。**使首席信息安全官（CISO）和安全团队能够执行其预防性安全策略，并以清晰、可量化的指标向董事会自信汇报在威胁造成影响已被消除的风险——从而赢得关键的时间优势，并减轻安全运营中心（SOC）的负担。
- **资产发现和库存集成。**快速识别安全事件中涉及的资产，以加快事件评估和响应速度。
- **安全工作区。**简洁直观的用户界面，使安全团队能够了解其环境中的动态，并提出降低安全风险的建议。
- **检测模式。**无需更改现有 IT 或网络基础设施即可轻松部署和概念验证。

借助预测性智能提供先发制人的安全

Infoblox 是原始 DNS 威胁情报的领先提供者。该公司采取先发制人而非单纯防御的方法，利用自身洞察在威胁行为者基础设施构建过程中进行追踪，并在源头打击网络犯罪，往往在攻击尚未发起之前就已将其破坏。

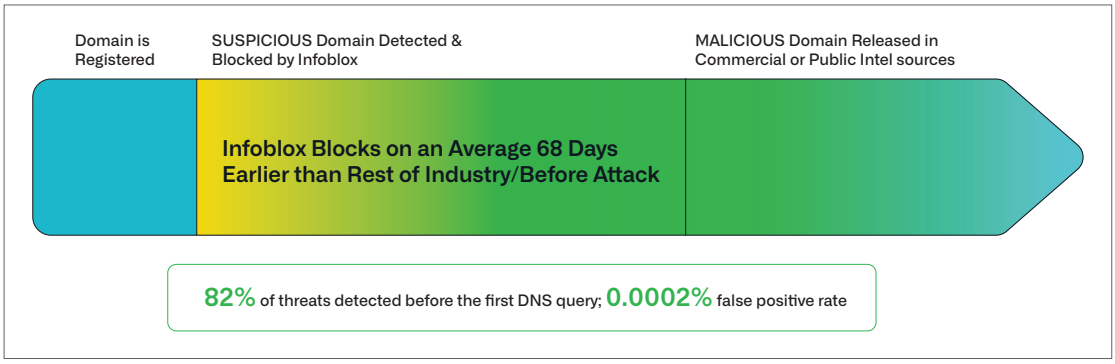

图 2：Infoblox threat intelligence对威胁的防御领先整个安全行业。

Infoblox 如何创建原始 DNS 威胁情报

DNS 专家：Infoblox 通过精准定位发现隐藏在 DNS 中的威胁行为者。从高风险或可疑域名开始，该团队将各个线索连接起来，以识别攻击者的基础架构，并随着其发展进行跟踪，令其浮出水面，领先于任何其他渠道。

威胁专业知识：Infoblox 深谙恶意行为者的运作方式以及恶意软件、勒索软件、网络钓鱼和基于 DNS 的漏洞等威胁的表现形式。凭借这些专业知识，Infoblox的预测系统能够检测相似域名、DNS 命令与控制 (C2) 活动、注册域名生成算法 (RDGAs) 和其他可疑行为。

数据科学：Infoblox 将机器学习和先进的数据科学应用于海量 DNS 查询数据，从而实现对数据外泄、域生成算法 (DGA) 和各种规避性威胁的接近实时的防护。

借助 SOC INSIGHTS 更高效地工作

从警报疲劳和分析师倦怠到冗长的调查和响应工作，Infoblox Threat Defense 搭配额外的 SOC Insights 套件，可大幅减轻 SOC 的负担。

- 借助人工智能驱动的分析，将成千上万的警报提炼为少量洞察，帮助分析人员聚焦最重要的内容。
- 自动化日志、威胁情报和其他数据的收集与关联，以便分析师能够迅速启动调查和响应。
- 通过资产发现和库存集成加快事件响应，帮助分析人员更快识别受影响的设备。

图 3：Infoblox Threat Intel 分享了令人惊讶的研究数据关于相似域名风险的升级

大规模导出高价值的 DNS 日志

Infoblox 使您可以轻松地将高保真 DNS 查询和事件数据发送到 SIEM、SOAR 或数据湖，以实现集中可视化和更快的威胁关联。

- 仅过滤和转发高价值的 DNS 事件，以降低 SIEM 的摄取成本和警报噪音。
- 使用 Infoblox 云数据连接器实时流式传输增强型 DNS 日志。
- 为每个工具提供所需的上下文，从而提升整个生态系统的检测和响应能力。
- 通过经过认证的双向集成，与其他工具无缝共享数据——改进端到端的检测、分流和响应。

使用 DOSSIER 加快调查速度

Dossier 为分析人员提供了强大的一体化研究工具，用于验证威胁、分析入侵迹象（IOC），并加快调查速度——无需在不同平台之间切换。

- 将内部、Infoblox 和第三方威胁情报整合到一个直观的界面中。
- 借助内置的丰富信息和链接分析功能，快速调查 IOC 并发现相关威胁。
- 通过消除手动数据收集和上下文切换，将调查时间缩短高达 67%。

保护您的品牌免受有针对性的欺诈

Infoblox 提供两种集成功能——相似域名监控和域名缓解服务——帮助保护您的品牌、客户和员工免受基于欺骗的网络攻击。它们共同令您洞察新出现的威胁，并能在恶意域名影响您的业务之前对其采取快速、有效的行动。

相似域名监控

抢先防范利用您的品牌或可信第三方进行的冒充攻击。

- 检测那些注册用于冒充您的公司、供应链或面向客户资产的域名。
- 识别用于针对员工或客户的网络钓鱼和欺诈活动的域名。
- 监控高优先级域的风险态势变化，并接收实时警报。

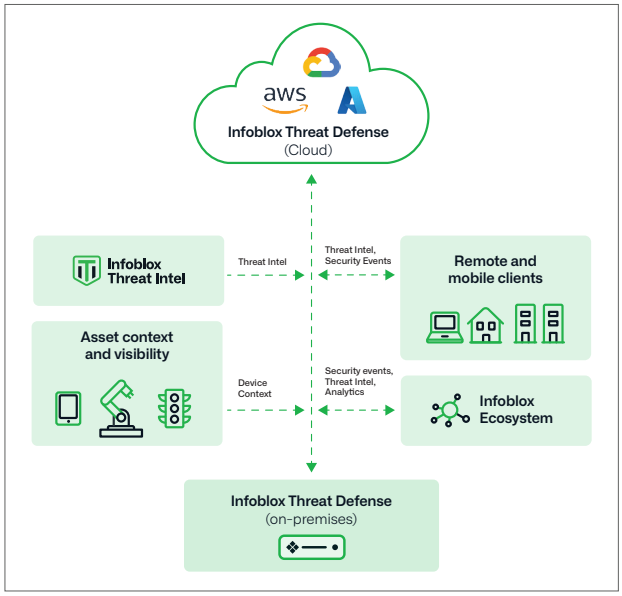

图 4：Infoblox 混合架构可实现全方位的保护和灵活部署，以应对当今由人工智能驱动的威胁形势。

域名缓解服务

快速验证并删除在真实环境中活跃的恶意域名。

- 通过人为主导的事件验证和汇总报告，确认并记录恶意活动。
- 与全球 ISP、托管服务提供商和监管机构协调，实现快速删除——通常在 24 小时内完成。
- 在移除威胁后的 30 天内持续监控已缓解的威胁，以检测并清除重新激活这一威胁的企图，且无需额外费用。
- 应对多种威胁类型，包括网络钓鱼、恶意软件托管、C2 基础设施和被盗数据。

如要详细了解 Infoblox Threat Defense 如何保护您的数据和基础设施，请访问
https://www.infoblox.com/products/threat-defense/.

公司总部
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

版本：20250121v1