数据表

BloxOne® 高级威胁防御

从根本上加强和优化您的安全态势

大规模基础安全的需求

传统的安全模型已经不足以适应当今数字化转型的世界。

- 周边环境已经发生变化，您的用户可以从任何地方直接访问基于云的应用程序。
- 物联网导致不接受传统端点技术保护的设备激增。
- 大多数安全系统都很复杂，不容易扩展到保护这些动态环境所需的水平。

组织需要的是一个可扩展、简单且自动化的安全解决方案，以保护整个网络，而无需部署或管理额外的基础设施。

INFOBLOX 提供可扩展的平台，最大限度地利用您现有的威胁防御投资

Infoblox BloxOne 高级威胁防御是一款全面的 DNS 检测和响应 (DNSDR) 解决方案，可检测其他解决方案遗漏的威胁活动，并通过搜寻的活动前 DNS 威胁情报预防攻击，破坏攻击方的供应链。通过智能生态系统集成和自动化，减少了手动工作，而借助 Infoblox 独特的AI 驱动分析，分析师可以专注于最重要的问题，保证洞察分析报告可以缩短 MTTR，提高现有安全工具的投资回报率，提高整体 SecOps 效率。

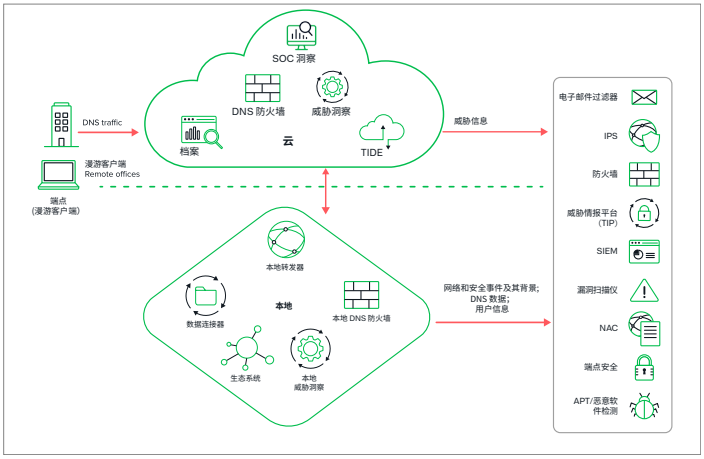


图 1: *Infoblox* 混合架构可实现随处保护和随地部署

主要功能

- 检测并阻止其他解决方案所忽略的漏洞、网络钓鱼、勒索软件和其他现代恶意软件
- 在 DNS 层保护用户和设备，无论平台或操作系统如何，包括 BYOD、物联网和 ICS
- 发现高风险应用程序，并管理影子 IT、内部人员、合规性和其他风险
- 通过机器学习/人工智能分析防止数据泄露技术，包括基于 DNS 的
- 数据泄露、DGA 和 DNSMessenger
- 限制用户访问不当或不需要的网络内容并跟踪活动
- 为您最有价值的互联网财产提供 Lookalike 域监控，保护您的品牌
- 将调查速度提高 3 倍，简化威胁响应和威胁搜寻活动
- 增强可视性：通过与 IPAM 资产元数据集成，获得精确的可视性“和丰富的网络上下文”，以实现最佳的事件理解和相关性
- 借助 SOC 洞察，可以通过 AI 驱动的洞察快速启动对最严重威胁的调查和响应，缩短 MTTR

最大限度地提高安全运营中心的效率

缩短事件响应时间

- 自动阻止恶意活动并向安全生态系统的其他部分提供威胁数据，以进行调查、隔离和修复
- 使用上下文网络和威胁情报数据以及 Infoblox 生态系统集成（SOAR 的关键推动因素）优化您的 SOAR 解决方案 - 缩短威胁响应时间，降低运营成本
- 借助 Infoblox SOC 洞察功能，通过 AI 驱动分析了解哪些事件最重要，而不仅仅是简单的恶意软件风险排名仪表板上显示的信息

将安全策略与威胁情报可移植性相统一

- 收集和管理来自内部和外部来源的威胁情报数据，并将其分发到现有安全系统
- 降低威胁信息反馈成本，同时提高整个安全堆栈中威胁情报的有效性

更快的威胁调查和搜寻

- 可以通过 AI 驱动的洞察（不仅仅是简单的恶意软件风险排名仪表板上显示的信息）快速启动对最严重威胁的调查和响应，缩短 MTTR
- 通过为安全分析师提供自动威胁调查、相关威胁洞察以及来自专家网络资源的其他研究观点，使您的威胁分析师团队的工作效率提高 3 倍，从而对威胁做出快速、准确的决策。

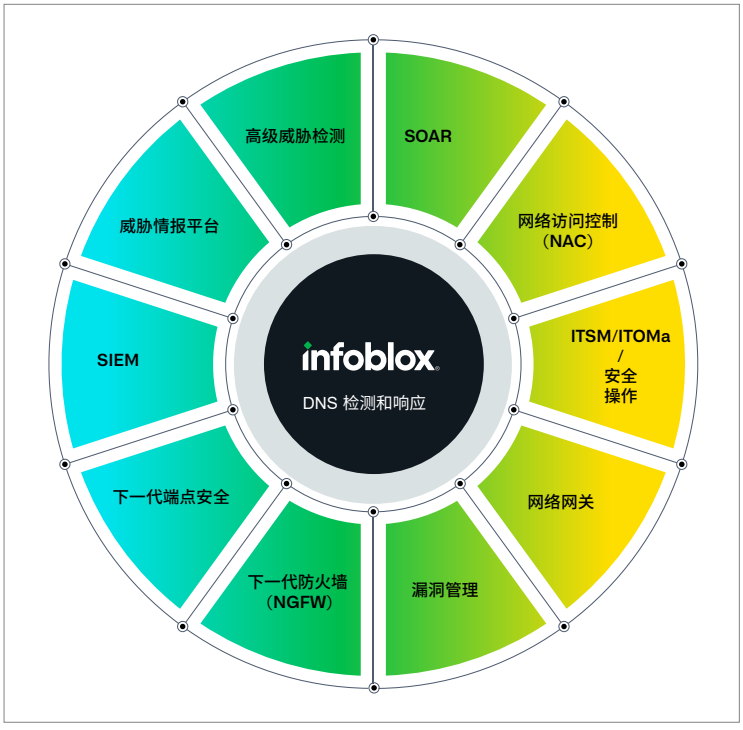
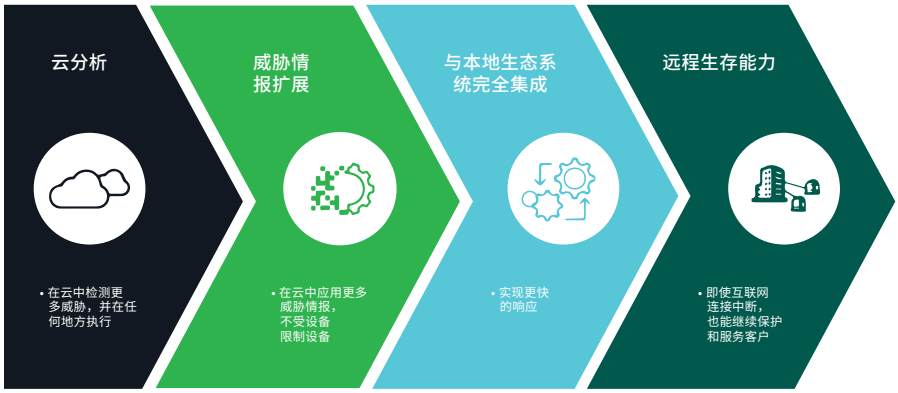


图 2: *BloxOne* 威胁防御与整个网络安全生态系统集成

> “当今时代，有太多的勒索软件、间谍软件和广告软件通过互联网用户打开的链接进入。*Infoblox* 云安全解决方案有助于阻止用户重定向到不良网站，防止机器受到感染，使用户更安全。”
>
> **西雅图城市大学高级系统管理员兼网络工程师**

无论您部署在何处，混合方法都能为您提供保护



云分析

- 利用云更强大的处理能力，使用基于机器学习的分析来检测更广泛的威胁，包括数据泄露、域生成算法 (DGA)、快速流量、无文件恶意软件、字典 DGA 等
- 检测云中的威胁并在任何地方强制执行，以保护总部、数据中心、远程办公室或漫游设备

威胁情报扩展

- 应用来自 Infoblox 研究和第三方提供商的全面情报，在本地或云中实施策略，并将其自动分发到安全基础设施的其余部分
- 无需为每个站点投资更多安全设备，即可在云中应用更多威胁情报

与安全生态系统的强大集成

- 可与本地 Infoblox 和第三方安全技术全面集成，实现全网络修复并提高这些技术的投资回报率

远程生存能力/复原能力

- 如果互联网连接中断，本地 Infoblox 可以继续保护网络

要详细了解 BloxOne 威胁防御如何保护您的数据和基础设施，请访问：
https://www.infoblox.com/products/bloxone-threat-defense

INFOBLOX SECURITY 的投资回报率

减轻设备安全压力

- 将已有的 DNS 服务器作为第一道防线，减轻防火墙、IPS 和网络代理服务器等外围安全设备的负担
- 发送至 NGFW 的流量最多可减少 60 倍*

提高现有投资的回报率

- 通过双向共享威胁和攻击者信息，从相邻/互补产品中获取更多价值
- 如果将 DNS 数据发送到 SIEM，则仅发送可疑的 DNS 数据到这些平台，以降低 SIEM 解决方案的成本

自动化

- 使用自动化降低人工接触/错误的成本
- 克服技能资源不足的问题- 在技能和成本方面，团队实施（配置只需数小时而非数月）和操作的需求降低 60%
- 通过易于使用的单一控制台来获取深度威胁情报，使威胁分析师的工作效率提高 3 倍

*基于真实的客户数据

infoblox.

Infoblox 将网络和安全融为一体，提供无与伦比的性能和保护。我们深受《财富》100 强公司和新兴创新者的信赖，提供对连接到您网络的人员和内容的实时可见性和控制，因此您的组织可以更快地运行并更早地阻止威胁。

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

+1.408.986.4000
www.infoblox.com

版本： 20240122v1