FICHA TÉCNICA

BloxOne® Threat Defense Advanced

Fortaleça e otimize sua postura de segurança da base

A NECESSIDADE DE SEGURANÇA FUNDAMENTAL EM ESCALA

O modelo de segurança tradicional é inadequado no mundo atual das transformações digitais.

- O perímetro mudou, e seus usuários acessam diretamente os aplicativos baseados em nuvem de qualquer lugar.
- A IoT leva a uma explosão de dispositivos que não aceitam tecnologias tradicionais de endpoints para proteção.
- A maioria dos sistemas de segurança é complexa e não se expande facilmente até o nível necessário para proteger esses ambientes dinâmicos.

O que as organizações necessitam é de uma solução de segurança escalável, simples e automatizada que proteja toda a rede sem a necessidade de implantar ou gerenciar infraestrutura adicional.

O INFOBLOX FORNECE UMA PLATAFORMA ESCALÁVEL QUE MAXIMIZA SEU INVESTIMENTO EM DEFESA CONTRA AMEAÇAS EXISTENTE

O Infoblox BloxOne Threat Defense Advanced, solução abrangente de Detecção e Resposta de DNS (DNSDR), detecta atividades de ameaças que outras soluções deixam passar e interrompe ataques antes que ocorram, utilizando inteligência de ameaças de DNS pré-campanha para interromper a cadeia de suprimentos do agressor. As integrações e automações inteligentes do ecossistema reduzem o esforço manual, enquanto dados estatísticos exclusivos gerados por IA concentram os analistas no que é mais importante e apresentam insights que reduzem o MTTR, aumentam o ROI das ferramentas de segurança existentes e elevam a eficiência geral do SecOps.

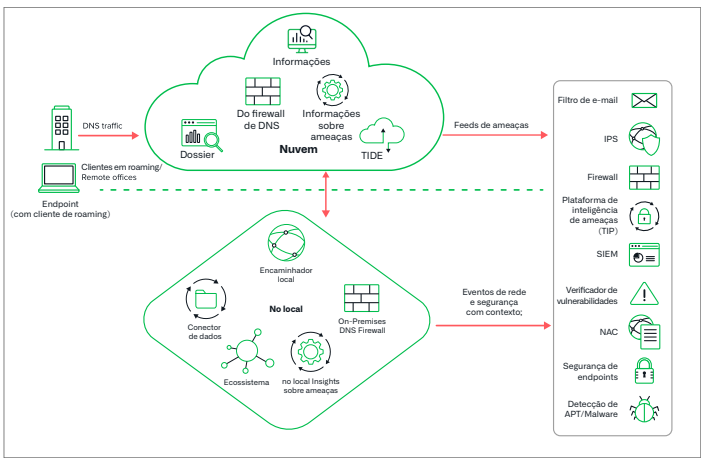


Figura 1: A arquitetura híbrido Infoblox permite proteção em qualquer lugar e implantação em qualquer lugar

PRINCIPAIS CAPACIDADES

- Detecta e bloqueia explorações, phishing, ransomware e outros malwares modernos que outras soluções perdem
- Proteja usuários e dispositivos, independentemente da plataforma ou do sistema operacional, na camada DNS, incluindo BYOD, IoT e ICS
- Descubra aplicativos de alto risco e gerencie seu Shadow IT, Insider, Compliance e outros riscos
- Evite técnicas de exfiltração de dados com aprendizado de máquina/análise de IA, incluindo exfiltração de dados baseada em DNS, DGA e DNSMessenger
- Restringir o acesso do usuário a conteúdo da web inapropriado ou indesejado e rastrear atividades
- Proteja sua marca com o Lookalike Domain Monitoring para suas propriedades mais valiosas da Internet
- Triplique a velocidade das investigações e simplifique as atividades de resposta e caça a ameaças
- Aumente a visibilidade: Obtenha visibilidade precisa “e um rico contexto de rede”, integrando-se aos metadados de ativos do IPAM para otimizar a compreensão e a correlação de eventos
- O SOC Insights permite que você inicie investigações e respostas sobre as ameaças mais importantes e reduza o MTTR com o AI-Driven Insights

MAXIMIZE A EFICIÊNCIA DO CENTRO DE OPERAÇÕES DE SEGURANÇA

Reduzir o tempo de resposta a incidentes

- Bloqueie automaticamente atividades maliciosas e fornecer os dados de ameaça ao restante do seu ecossistema de segurança para investigação, quarentena e correção.
- Otimize sua solução SOAR usando dados de inteligência de ameaças e rede contextual e integrações de ecossistema Infoblox (um facilitador crítico do SOAR), reduzindo o tempo de resposta às ameaças e o OPEX
- Use os recursos do Infoblox SOC Insights para saber quais eventos são mais importantes com a análise baseada em IA que vai além de simples painéis com classificação de risco de malware

Unifique a política de segurança com a portabilidade Intel contra ameaças

- Reúna e gerencie dados de inteligência de ameaças de fontes internas e externas e distribua para os sistemas de segurança existentes
- Reduza o custo dos feeds de ameaças e melhore a eficácia das informações sobre ameaças em toda a pilha de segurança

Investigação e caça de ameaças mais rápidas

- Inicie a investigação e a resposta sobre as ameaças mais importantes e reduza o MTTR com insights gerados por IA que vão além de simples painéis classificados como risco de malware
- Torna sua equipe de analistas de ameaças três vezes mais produtiva capacitando analistas de segurança com investigação automatizada de ameaças, insights sobre ameaças relacionadas e perspectivas de pesquisa adicionais de fontes cibernéticas especializadas para tomar decisões rápidas e precisas sobre ameaças

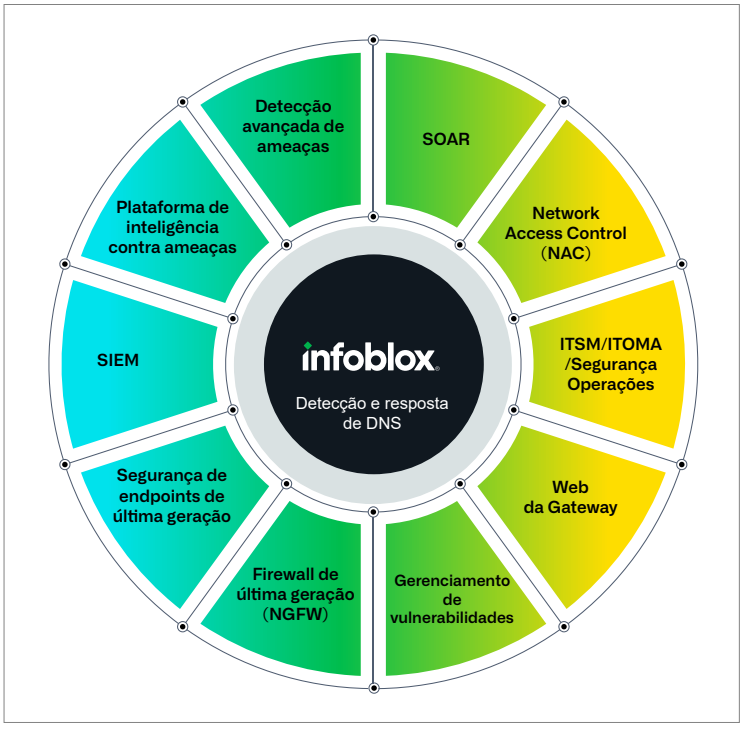
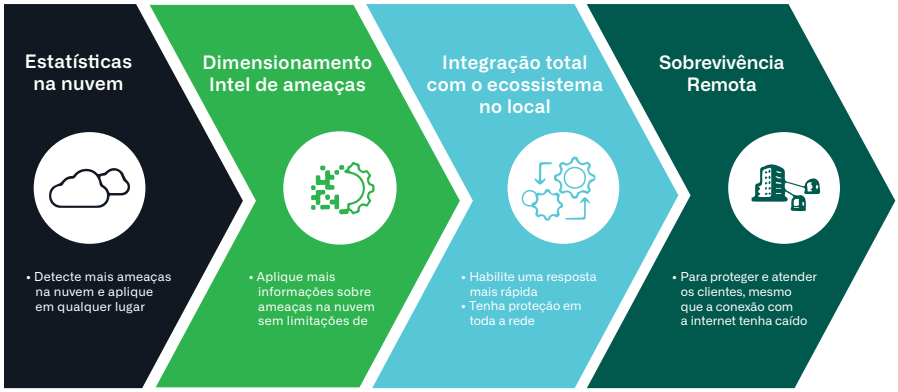


Figura 2: A BloxOne Threat Defense se integra a todo o ecossistema de segurança cibernética

> *"Atualmente, há um excesso de ransomware, spyware e adware provenientes de links abertos por usuários da Internet. A solução de segurança em nuvem Infoblox ajuda a bloquear os usuários de redirecionamentos que os levam a sites perigosos, evita que as máquinas sejam infectadas e mantém os usuários mais seguros".*
>
> **Senior System Administrator and Network Engineer, City University of Seattle**

A ABORDAGEM HÍBRIDA PROTEGE ONDE QUER QUE VOCÊ IMPLEMENTE



Funções analíticas na nuvem

- Aproveite os recursos de processamento superiores da nuvem para detectar uma variedade mais ampla de ameaças, incluindo exfiltração de dados, algoritmo de geração de domínios (DGA), fluxo rápido, malware sem arquivo, DGA de dicionário e outros, utilizando análises baseadas em aprendizado de máquina
- Detecte ameaças na nuvem e aplique em qualquer lugar para proteger sede, datacenter, escritórios remotos ou dispositivos de roaming

Dimensionamento de inteligência de ameaças

- Aplique informações abrangentes da pesquisa do Infoblox e de provedores terceirizados para aplicar políticas no local ou na nuvem e distribua-as automaticamente para o restante da infraestrutura de segurança
- Aplique mais inteligência de ameaças na nuvem sem grandes investimentos em mais appliances de segurança para cada site

Integrações poderosas com seu ecossistema de segurança

- Habilita a integração completa com o Infoblox local e tecnologias de segurança de terceiros, possibilitando a correção em toda a rede e melhorando o ROI dessas tecnologias

Capacidade de sobrevivência/resiliência remota

- Se houver alguma interrupção na sua conectividade com a Internet, o Infoblox local poderá continuar a proteger a rede

Para saber mais sobre como o BloxOne Threat Defense protege seus dados e infraestrutura, acesse: https://www.infoblox.com/products/bloxone-threat-defense

O ROI DO INFOBLOX SECURITY

Libera dispositivos de segurança sobrecarregados

- Reduz a carga sobre os dispositivos de segurança sobrecarregados, como firewalls, IPS e proxies da Web, utilizando seus servidores DNS já disponíveis como primeira linha de defesa
- **Redução de até 60 vezes no tráfego** enviado para NGFWs*

Melhore o ROI dos investimentos existentes

- Aproveite melhor produtos complementares/adjacentes com compartilhamento bidirecional de informações sobre ameaças e invasores
- Se enviar dados DNS para o SIEM, reduza o custo das soluções SIEM enviando somente dados DNS suspeitos para essas plataformas

Automação

- Reduza o custo do toque/erro humano usando automação
- Supere a falta de recursos qualificados - 60% menos demanda de sua equipe para implementar (configurar em poucas horas e não em meses) e operar, tanto em termos de habilidade quanto em custo
- Torne seus analistas de ameaças três vezes mais produtivos com um console único e fácil de usar para receber informações detalhadas sobre ameaças

**Com base em dados de clientes reais*

infoblox.

O Infoblox une rede e segurança para oferecer desempenho e proteção incomparáveis. Reconhecida por empresas presentes na lista Fortune 100 e por inovadores emergentes, fornecemos visibilidade e controle em tempo real sobre quem e o que se conecta à sua rede, para que sua organização opere com maior velocidade e detecte ameaças mais cedo.

Sede corporativa
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Versão: 20240122v1