Hoja de datos

BloxOne® Threat Defense Advanced

Fortalezca y optimice su postura de seguridad desde la base

LA NECESIDAD DE UNA SEGURIDAD FUNDAMENTAL A ESCALA

El modelo de seguridad tradicional no es adecuado en el mundo actual de transformaciones digitales.

- El perímetro ha cambiado y los usuarios acceden directamente a las aplicaciones basadas en la nube desde cualquier lugar.
- El IoT conduce a una explosión de dispositivos que no aceptan tecnologías tradicionales de puntos finales para su protección.
- La mayoría de los sistemas de seguridad son complejos y no se escalan fácilmente al nivel necesario para proteger estos entornos dinámicos.

Lo que las organizaciones necesitan es una solución de seguridad escalable, sencilla y automatizada que proteja toda la red sin necesidad de implementar o gestionar infraestructuras adicionales.

2MAXIMIZA SU INVERSIÓN EN DEFENSA CONTRA AMENAZAS EXISTENTE

Infoblox BloxOne Threat Defense Advanced, una solución integral de detección y respuesta DNS (DNSDR), detecta la actividad de amenazas que otras soluciones pasan por alto y detiene los ataques antes de que se produzcan con inteligencia de amenazas DNS previamente detectada para interrumpir las cadenas de suministro de atacantes. Las integraciones inteligentes del ecosistema y la automatización reducen el esfuerzo manual, mientras que los análisis con IA centran a los analistas en lo que más importa y proporcionan información que reduce el MTTR, aumenta el ROI de las herramientas de seguridad existentes y eleva la eficiencia general de SecOps.

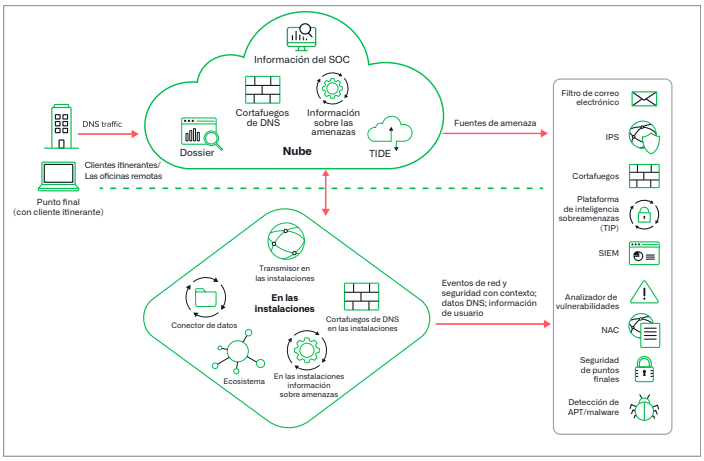


Figura 1: La arquitectura híbrida de Infoblox permite la protección en todas partes y el despliegue en cualquier sitio

PRESTACIONES CLAVE

- Detecte y bloquee exploits, phishing, ransomware y otros programas maliciosos modernos que otras soluciones pasan por alto
- Proteja a los usuarios y dispositivos, independientemente de la plataforma o el sistema operativo, en la capa DNS, incluyendo BYOD, IoT e ICS
- Descubra aplicaciones de alto riesgo y gestione su Shadow IT, Insider, Compliance y otros riesgos
- Evite las técnicas de exfiltración de datos con el aprendizaje automático/análisis de IA, incluyendo la exfiltración de datos basada en DNS, DGA y DNSMessenger
- Restrinja el acceso de los usuarios a contenidos web inapropiados o no deseados y realice un seguimiento de la actividad
- Proteja su marca con la monitorización de dominios similares para sus propiedades de Internet más valiosas
- Acelere las investigaciones el triple y optimice las actividades de respuesta a amenazas y búsqueda de amenazas
- Mejore la visibilidad: obtenga visibilidad precisa “y contexto de red enriquecido” mediante la integración con metadatos de activos IPAM para una comprensión y correlación óptimas de los eventos
- SOC Insights le permite comenzar a investigar y responder a las amenazas más importantes, así como reducir el MTTR con información basada en IA

MAXIMICE LA EFICACIA DEL CENTRO DE OPERACIONES DE SEGURIDAD

Reduzca el tiempo de respuesta a incidentes

- Bloquee automáticamente la actividad maliciosa y proporcione los datos de amenazas al resto de su ecosistema de seguridad para su investigación, cuarentena y corrección
- Optimice su solución SOAR utilizando datos contextuales de inteligencia sobre amenazas y redes, e integraciones de ecosistema Infoblox (un facilitador crítico de SOAR): reduzca el tiempo de respuesta a amenazas y OPEX
- Utilice las funciones de Infoblox SOC Insights para saber qué eventos son más importantes con los análisis basados en la IA que van más allá de los simples paneles de control clasificados por el riesgo de software malicioso

Unifique la política de seguridad con la portabilidad de la inteligencia de amenazas

- Recopile y gestione datos de inteligencia sobre amenazas de fuentes internas y externas y distribúyalos a sistemas de seguridad existentes
- Reduzca el coste de las fuentes de amenazas al tiempo que mejora la eficacia de la información sobre amenazas en toda la pila de seguridad

Investigación y búsqueda de amenazas más rápidas

- Inicie la investigación y la respuesta sobre las amenazas más importantes y reduzca el MTTR con información basada en IA que va más allá de los simples paneles clasificados por riesgo de software malicioso
- Hace que su equipo de analistas de amenazas **sea 3 veces más productivo** al capacitar a analistas de seguridad con investigación automatizada de amenazas, información sobre amenazas relacionadas y perspectivas de investigación adicionales de fuentes cibernéticas expertas para tomar decisiones rápidas y precisas

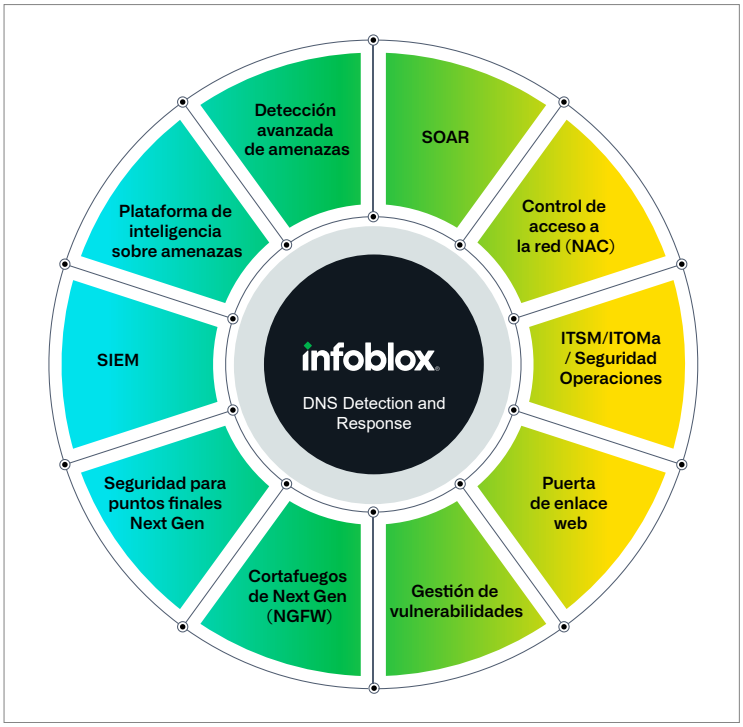
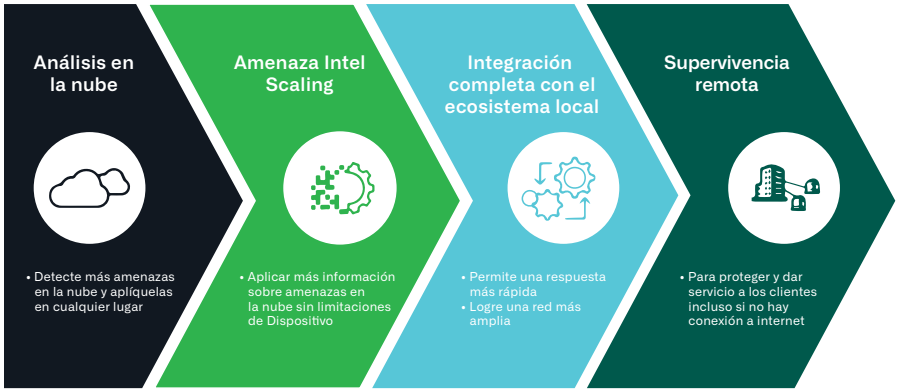


Figura 2: BloxOne Threat Defense se integra con todo el ecosistema de ciberseguridad

> *"En los tiempos que corren hay demasiado ransomware, spyware y adware que llegan a través de enlaces abiertos por usuarios de Internet. La solución de seguridad en la nube de Infoblox ayuda a bloquear las redirecciones que llevan a los usuarios a sitios maliciosos, evita que las máquinas se infecten y mantiene a los usuarios más seguros".*
>
> **Administrador sénior del sistema e ingeniero de redes, City University of Seattle**

EL ENFOQUE HÍBRIDO PROTEGE DONDEQUIERA QUE SE IMPLEMENTE



Análisis en la nube

- Aproveche las mayores capacidades de procesamiento de la nube para detectar una mayor gama de amenazas, incluida la exfiltración de datos, algoritmo de generación de dominios (DGA), flujo rápido, software malicioso sin archivos y mucho más utilizando análisis basados en aprendizaje automático
- Detecte amenazas en la nube y aplíquelas en cualquier lugar para proteger la sede central, el centro de datos, las oficinas remotas o los dispositivos móviles

Escalado de inteligencia de amenazas

- Aplique inteligencia completa de investigación de Infoblox y proveedores externos para aplicar políticas en las instalaciones o en la nube, y distribuirla automáticamente al resto de la infraestructura de seguridad
- Aplique más inteligencia sobre amenazas en la nube sin grandes inversiones en más dispositivos de seguridad para cada sitio

Potentes integraciones con su ecosistema de seguridad

- Permite una integración completa con las tecnologías de seguridad de Infoblox y de terceros en las instalaciones, lo que hace posible la reparación en toda la red y mejora el ROI de esas tecnologías

Supervivencia/resiliencia remota

- Si alguna vez hay una interrupción en la conectividad a Internet, Infoblox en las instalaciones puede seguir protegiendo la red

Para obtener más información sobre las formas en que BloxOne Threat Defense protege sus datos e infraestructura, visite: https://www.infoblox.com/products/bloxone-threat-defense

EL ROI DE LA SEGURIDAD DE INFOBLOX

Descargue los dispositivos de seguridad sobrecargados

- Reduzca la carga de los saturados dispositivos de seguridad perimetral, como cortafuegos, IPS y proxies web, utilizando sus servidores DNS ya disponibles como primera línea de defensa
- **Hasta 60 veces menos tráfico** enviado a NGFWs*

Mejore el ROI de las inversiones existentes

- Obtenga más valor de productos complementarios/adyacentes compartiendo bidireccionalmente información sobre amenazas y atacantes
- Si envía datos DNS a SIEM, reduzca el coste de las soluciones SIEM enviando solo datos sospechosos a estas plataformas

Automatización

- Reduzca el coste del contacto/error humano mediante la automatización
- Supere la falta de recursos cualificados - un 60 % menos de exigencia a su equipo para implementar (configurar en horas en lugar de meses) y operar tanto por habilidades como por coste
- Haga que sus analistas de amenazas sean tres veces más productivos con una consola única y fácil de usar para obtener una profunda inteligencia de amenazas

**Basado en datos reales de clientes*

infoblox.

Infoblox une redes y seguridad para ofrecer un rendimiento y una protección inigualables. Con la confianza de empresas Fortune 100 e innovadores emergentes, proporcionamos visibilidad y control en tiempo real sobre quién y qué se conecta a su red, para que su organización funcione más rápido y detenga antes las amenazas.

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

+1.408.986.4000
www.infoblox.com

Versión: 20240122v1