HOJA DE DATOS

Infoblox Threat Defense™ Advanced

El DNS protector, basado en inteligencia de amenazas predictiva, lo protege todo y en todo lugar antes de que se produzca el impacto

EL DNS ES EL PRIMER PUNTO DE PREVENCIÓN DE TODOS LOS CIBERATAQUES

El DNS es el primer punto de detección y prevención de todos los ciberataques. Ya se trate de un correo electrónico de phishing, un mensaje de smishing o una vulnerabilidad explotada, casi todos los ataques generan una consulta al DNS sobre un dominio malicioso. Como resultado, el DNS proporciona un punto de visibilidad y control potente y centralizado para proteger a toda la empresa, incluidos los usuarios, los dispositivos, el IoT/TO y las cargas de trabajo, ya sea in situ, en la nube o en el perímetro.

Como primer paso de cualquier comunicación, detectar y bloquear la actividad de amenazas en la capa del DNS ayuda a detener el tráfico malicioso antes de que llegue a herramientas subyacentes y active alertas. Al correlacionar los datos del DNS con el contexto de los dispositivos y activos, los equipos de NetOps y SecOps obtienen una visibilidad más profunda de lo que ocurre en sus entornos, lo que mejora tanto la eficiencia operativa como la postura de seguridad.

LAS SOLUCIONES TRADICIONALES DE «DETECCIÓN Y RESPUESTA» YA NO SON EFICACES

Los actores de amenazas utilizan cada vez más la IA para lanzar campañas más prolíficas, sofisticadas y sigilosas. Generan software malicioso de un solo uso, diseñado de forma específica para que las herramientas tradicionales de «detección y respuesta» —aquellas que esperan ver una infección de «paciente cero»— resulten ineficaces. Cada ataque se convierte en un escenario de «paciente cero» en el que no existe ninguna firma o conducta reconocida. Las herramientas de «detección y respuesta» a menudo actúan demasiado tarde en la cadena de eliminación y no logran evitar daños. Por lo tanto, se precisa un enfoque preventivo diferente, uno que detenga las amenazas antes de que entren en el entorno o se desplacen lateralmente. Así no solo se bloquean los ataques en una fase temprana, sino que también se reduce la carga de las herramientas tradicionales de «detección y respuesta».

El DNS funciona como un punto de control ascendente que ofrece a los equipos de seguridad una oportunidad proactiva para detectar y bloquear las amenazas antes de que lleguen a los usuarios, las cargas de trabajo o los endpoints.

SEGURIDAD PREVENTIVA CON EL DNS

Infoblox Threat Defense™ Advanced ofrece un **enfoque preventivo** único para la detección de amenazas, que no se basa en el «paciente cero», sino que utiliza una combinación de **inteligencia predictiva** sobre amenazas que bloquea la infraestructura de los actores maliciosos antes de que se conviertan en armas, y análisis algorítmicos/basados en el aprendizaje automático de las consultas al DNS en las redes de los clientes para ofrecer protección antes de que se produzca el impacto. Mediante la rápida identificación de los activos involucrados en incidentes de seguridad, las integraciones del ecosistema y los espacios de trabajo intuitivos, permite una detección y una respuesta más rápidas y un mayor retorno de la inversión (ROI) de las soluciones de seguridad existentes.

DATOS Y CIFRAS

- Supervisa **204 000** clústeres de actores de amenazas en tiempo real, cifra que sigue creciendo
- Reduce la tasa de falsos positivos al **0,0002 %**
- Bloquea **el 82 %** de las amenazas antes de la primera consulta
- Ofrece protección **68,4** días antes de un ataque de media
- Bloquea **5 veces más** dominios de alto y medio riesgo que las herramientas que solo buscan detectar conductas maliciosas conocidas
- Ahorra una media de **500 horas de trabajo de los analistas del SOC** al mes*
- Ayuda a ahorrar **400 000 $** en productividad al año*
- Reduce decenas de miles de alertas a unas pocas*

La encuesta SANS 2025 SOC reveló que siete de las diez principales barreras que impiden la plena utilización del SOC tienen que ver con las alertas, la integración de herramientas y la falta de aptitudes.

*Basado en datos reales de clientes.

BLOQUEE LAS AMENAZAS ANTES DE QUE SE PRODUZCA EL IMPACTO

Infoblox Threat Defense aplica inteligencia predictiva sobre amenazas al DNS con análisis algorítmico/de aprendizaje automático sobre el tráfico del DNS en tiempo real para bloquear la actividad de las amenazas antes de que afecten a su red, con lo que a menudo detectan amenazas que otras herramientas ignoran. Al detener las amenazas en la capa del DNS, Infoblox también ayuda a reducir el volumen de alertas y la carga de trabajo de las herramientas de seguridad subyacentes; los clientes comunican una reducción de hasta el 50 % en las alertas de los firewalls de próxima generación (NGFW) y los sistemas de detección y respuesta de endpoints (EDR).

> *"Un DNS seguro podría reducir las posibilidades de éxito del 92 % de los ataques que intentan desplegar software malicioso en una red determinada."*
>
> **Anne Neuberger,**
> **Responsable de Ciberseguridad Dirección,**
> **Agencia de Seguridad Nacional (NSA)**

Capacidad clave	Descripción	Infoblox Threat Defense	NGFW	SASE	EDR
Sistema de resolución seguro a nivel empresarial y registro de consultas al DNS	Utiliza datos de consulta al DNS para identificar y descartar dominios	●	◑	◑	◑
Monitorización completa de la conducta en el DNS	Supervisa todos los tipos de registros DNS para detectar actividad maliciosa	●	●	◔	○
Detección y desactivación de dominios similares/ doppleganger	Mitiga la superficie de ataque de los dominios similares/doppleganger	●	○	◑	○
Protección del DNS de día cero	Identifica nuevos o emergentes dominios para su organización que podrían suponer una amenaza	●	◑	◑	○
Detección de tunelización de DNS basada en el comportamiento	Detecta túneles del DNS utilizados para la exfiltración/infiltración de datos, comunicaciones C2, etc.	●	◑	◑	○
Protección proactiva frente a dominios sospechosos y de alto riesgo	Identifica y bloquea de forma preventiva los dominios sospechosos que probablemente se utilicen en futuras campañas maliciosas	●	◑	◑	◑
Enriquecimiento automático y nativo del contexto	Correlaciona el contexto de la red sin necesidad de clientes ni de usar sumideros (usuario, dispositivo, IP de origen, ubicación, dirección MAC, red de área local virtual)	●	◑	◑	◑
Detección y desactivación proactiva de los sistemas de distribución de amenazas (TDS)	Identifica la infraestructura de TDS de los actores de amenazas, no solo los dominios individuales, para hacer frente a los actores de amenazas que alternan numerosos dominios para evitar ser detectados	●	◔	○	○

Figura 1. Capacidades exclusivas de Threat Defense que otras herramientas no pueden abordar por completo

CARACTERÍSTICAS PRINCIPALES DE THREAT DEFENSE

- **"Protección antes del impacto" Monitor.** Permite a los CISO y a los equipos de seguridad ejecutar su estrategia de seguridad preventiva e informar con confianza a la junta directiva con métricas claras y cuantificables sobre las amenazas neutralizadas antes del impacto, obteniendo ventajas críticas de tiempo y reduciendo la carga en el centro de operaciones de seguridad (SOC).
- **Detección de activos e integración de inventario.** Identificación rápida de los activos implicados en incidentes de seguridad para obtener una evaluación y una respuesta más rápidas a los incidentes.
- **Espacio de trabajo de seguridad.** Interfaz de usuario simplificada e intuitiva que permite a los equipos de seguridad comprender lo que sucede en su entorno y sugerir formas de reducir los riesgos de seguridad.
- **Modo de detección.** Para obtener una fácil implementación y prueba de concepto, sin cambiar la infraestructura de red o de TI existente.

POTENCIE LA SEGURIDAD PREVENTIVA CON INTELIGENCIA PREDICTIVA

Infoblox es el principal creador de inteligencia sobre amenazas original basada en el DNS. La empresa adopta un enfoque preventivo — no solo defensivo — al utilizar sus conocimientos para rastrear la infraestructura de los actores de amenazas a medida que estos la construyen e interrumpir la ciberdelincuencia en origen, a menudo incluso antes de que se lance el ataque.

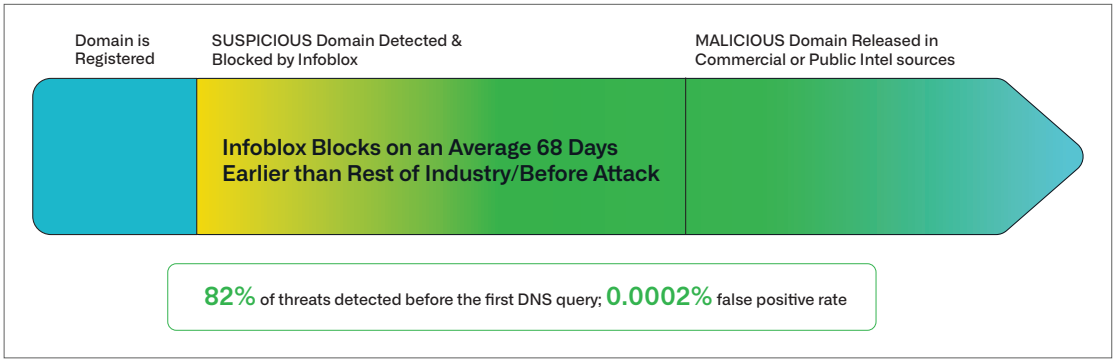

Figura 2. Infoblox Threat Intelligence puede proteger contra las amenazas antes que el resto del sector de la seguridad

Cómo crea Infoblox inteligencia original sobre las amenazas al DNS

Expertos en el DNS: Infoblox detecta los actores de amenazas que se esconden en el DNS porque sabe dónde buscar. A partir de dominios sospechosos o de alto riesgo, el equipo une los puntos hasta identificar la infraestructura del atacante y rastrearla a medida que evoluciona y surgen nuevas amenazas, antes de que otros las identifiquen.

Conocimientos sobre amenazas: Infoblox comprende cómo operan los actores maliciosos y cómo se manifiestan amenazas como el software malicioso, el ransomware, el phishing y los exploits basados en el DNS. Esos conocimientos sustentan sistemas predictivos que detectan dominios similares, actividad de mando y control (C2) del DNS, algoritmos de generación de dominios registrados (RDGA) y otras conductas sospechosas.

Ciencia de datos: Infoblox aplica el aprendizaje automático y la ciencia de datos avanzada a grandes volúmenes de datos de consultas al DNS, lo que permite obtener protección casi en tiempo real contra la exfiltración de datos, los algoritmos de generación de dominios (DGA) y una amplia gama de amenazas evasivas.

TRABAJE DE FORMA MÁS INTELIGENTE CON SOC INSIGHTS

Con el paquete adicional SOC Insights, Infoblox Threat Defense ofrece un alivio significativo al SOC, desde la fatiga por alertas y el agotamiento de los analistas hasta las largas tareas de investigación y respuesta.

- Ayude a los analistas a saber qué es lo más importante mediante análisis impulsados por IA que destilan cientos de miles de alertas hasta reducirlas a un puñado de información valiosa.
- Automatice el registro, la inteligencia sobre amenazas y otras recopilaciones y correlaciones de datos para que los analistas puedan acelerar la investigación y la respuesta.
- Acelere la respuesta a incidentes con la detección de activos y la integración de inventarios, que ayudan a los analistas a identificar más rápidamente los dispositivos afectados.

Figura 3. Infoblox Threat Intel compartió datos sorprendentes de investigación sobre el riesgo creciente de los dominios similares

EXPORTE REGISTROS DEL DNS DE ALTO VALOR A ESCALA

Infoblox facilita enviar datos de eventos y consultas al DNS de alta fidelidad a su SIEM, SOAR o «data lake» para obtener una visibilidad centralizada y una correlación de amenazas más rápida.

- Filtre y reenvíe solo los eventos del DNS de alto valor para reducir los costes de alimentación del SIEM y el ruido de alertas.
- Transmita registros del DNS ampliados en tiempo real mediante Cloud Data Connector de Infoblox.
- Mejore la detección y la respuesta en todo su ecosistema proporcionándole a cada herramienta el contexto que necesita.
- Comparta datos fácilmente con otras herramientas mediante integraciones bidireccionales certificadas, que mejoran la detección, la clasificación y la respuesta de extremo a extremo.

INVESTIGUE MÁS RÁPIDO CON DOSSIER

Dossier equipa a los analistas con una potente herramienta de investigación unificada para validar amenazas, tomar indicadores de compromiso (IOC) como base y acelerar las investigaciones, sin necesidad de pasar de una plataforma a otra.

- Consolide la inteligencia de amenazas interna, de Infoblox y de terceros en una interfaz intuitiva.
- Investigue rápidamente los IOC y descubra las amenazas relacionadas con la ampliación incorporada y el análisis de enlaces.
- Reduzca el tiempo de investigación hasta en un 67 %, al eliminar la recopilación manual de datos y los cambios de contexto.

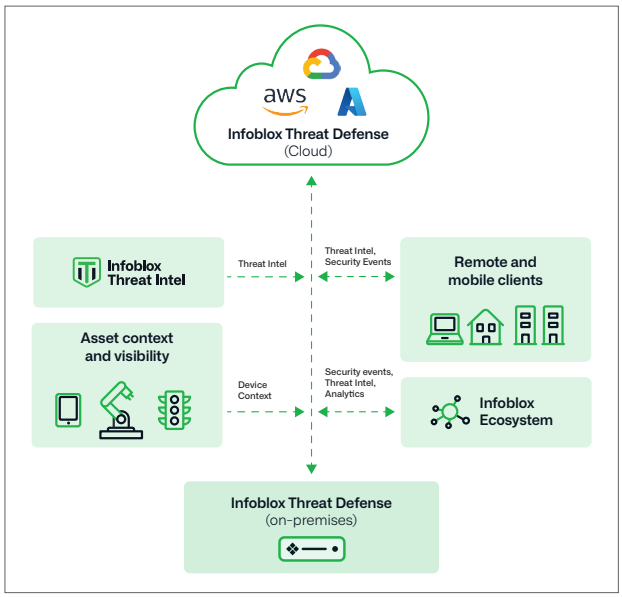

Figura 4. La arquitectura híbrida de Infoblox permite la protección en todas partes y el despliegue en cualquier lugar para contrarrestar el panorama de amenazas actual mediado por la IA.

PROTEJA SU MARCA FRENTE A LOS ENGAÑOS DIRIGIDOS

Infoblox ofrece dos capacidades integradas — monitorización de dominios similares y servicios de mitigación de dominios—, que ayudan a proteger su marca, a sus clientes y a sus empleados de los ciberataques basados en engaños. Juntas, le proporcionan visibilidad de las amenazas emergentes y la capacidad de tomar medidas rápidas y eficaces contra los dominios maliciosos antes de que afecten a su empresa.

Supervisión de dominios similares

Anticípese a los ataques de suplantación de identidad que explotan su marca o la de terceros de confianza.

- Detecte los dominios registrados para suplantar a su empresa, cadena de suministro o propiedades orientadas al cliente.
- Identifique los dominios utilizados en campañas de phishing y fraude que tienen a sus empleados o clientes como objetivo.
- Supervise los dominios de alta prioridad para detectar cambios en la postura de riesgo y reciba alertas en tiempo real.

Servicios de mitigación de dominios

Valide y neutralice rápidamente los dominios maliciosos que están activos en la red.

- Confirme y documente la actividad maliciosa mediante la validación de incidentes guiada por humanos y la elaboración de informes resumidos.
- Coordínese con los ISP, los proveedores de alojamiento y las agencias reguladoras de todo el mundo para lograr una desactivación rápida, a menudo en 24 horas.
- Supervise las amenazas mitigadas durante 30 días después de la desactivación para detectar y eliminar los intentos de reactivación sin coste adicional.
- Aborde una amplia gama de tipos de amenazas, incluyendo phishing, alojamiento de software malicioso, infraestructura C2 y datos robados.

Para obtener más información sobre cómo Infoblox Threat Defense protege sus datos e infraestructura, visite https://www.infoblox.com/es/products/threat-defense/.

Sede corporativa
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054 (EE. UU.)

+1.408.986.4000
www.infoblox.com/es

Versión: 20250121v1