PREDECIR.
PREVENIR.
PREVALECER.

CONTRA ATAQUES
SOFISTICADOS Y
POTENCIADOS POR IA
CON EL PODER DEL DNS

infoblox®

ÍNDICE

EL PROBLEMA CON UN ENFOQUE REACTIVO DE "DETECTAR Y RESPONDER"

Los métodos tradicionales se están volviendo demasiado lentos, arriesgados e ineficaces.

El enfoque heredado relativo a la cadena de eliminación está en vías de extinción. Se basaba en una estrategia de "infección del paciente cero", en la que otra organización servía como primer objetivo, también conocido como "paciente cero", para aprender más sobre el comportamiento del malware y luego aplicar esos conocimientos a la organización propia.

Sin embargo, ese modelo ya no es válido. Los actores de amenazas actuales crean malware a medida para cada sector, empresa e incluso empleado, lo que aumenta exponencialmente las posibilidades de que el paciente cero sea usted.

El tiempo medio de irrupción de un actor de amenazas, es decir, el tiempo que tarda un adversario en desplazarse lateralmente por una red una vez obtenido el acceso inicial, se ha reducido a apenas 48 minutos[1] . Esto significa que las organizaciones disponen de un margen de tiempo muy breve para detectar, investigar y remediar un ataque antes de que se propague por la red.

TIEMPO MEDIO DE IRRUPCIÓN DE UN ACTOR DE AMENAZAS

Compromiso inicial
El actor de amenazas obtiene acceso a la red

48 minutos
Tiempo medio que tarda en desplazarse lateralmente por la red

Impacto de los actores de amenazas

LOS ACTORES DE AMENAZAS ESTÁN GANANDO UNA VENTAJA INJUSTA

Pese a que las organizaciones invierten más de 200.000 millones de dólares al año en soluciones de ciberseguridad[2], las brechas como el ransomware siguen dando fruto, lo que pone de manifiesto las graves deficiencias de los enfoques actuales.

Puesto que los actores de amenazas utilizan nuevas herramientas para lanzar ataques más frecuentes, sofisticados y sigilosos, las soluciones de seguridad reactivas ya no son suficientes. El malware de un solo uso generado por IA está ahora tan bien diseñado que cada ataque se convierte en un "día cero", y no existe ninguna firma ni conducta conocida para detectarlo.

CÓMO UTILIZAN LA IA LOS ACTORES DE AMENAZAS

La capacidad de la IA para procesar grandes volúmenes de datos y aprender de los patrones permite a los ciberdelincuentes desarrollar estrategias de ataque más avanzadas y específicas.

Ingeniería social impulsada por IA
Un método destacado es la ingeniería social impulsada por IA, en la que los atacantes crean correos electrónicos de phishing y llamadas de phishing de voz (vishing) muy convincentes, que a menudo parecen provenir de personas de confianza, lo que facilita engañar a las víctimas para que revelen información confidencial o concedan acceso a sistemas seguros.

Desarrollo de software malicioso impulsado por IA
Además, la IA acelera el desarrollo de código malicioso, lo que reduce el tiempo necesario para crear ransomware sofisticado capaz de evadir las medidas de seguridad tradicionales. Esta capacidad debilita la barrera de entrada y permite a hackers menos experimentados lanzar ataques de ransomware eficaces.

Reducción de la barrera de entrada al cibercrimen
Por último, la IA está haciendo que el cibercrimen sea más accesible. mediante herramientas basadas en IA que lo automatizan todo, desde la generación de kits de phishing hasta el envío del software malicioso, incluso los atacantes con pocos conocimientos pueden ahora ejecutar campañas creíbles y dañinas. Este aumento del cibercrimen "como servicio" — impulsado por la IA— da lugar a ataques más frecuentes, variados y difíciles de predecir en todos los sectores.

TENDENCIAS CLAVE EN EL PANORAMA DE LOS CIBERATAQUES

Herramientas como ChatGPT y FraudGPT permiten a atacantes novatos crear correos electrónicos de phishing avanzados y malware sofisticado y dirigido, que elude las defensas tradicionales.

Los ataques de ransomware aumentaron un 132% en el primer trimestre de 2025 en comparación con el cuarto trimestre de 2024, apoyados en la ingeniería social basada en el engaño y la IA para obtener acceso inicial a las redes[3].

Cada segundo, hay 11 víctimas de ataques de malware en todo el mundo, lo que supone 340 millones de víctimas al año, cifra que seguirá creciendo exponencialmente[4].

La explotación de vulnerabilidades aumentó un 34%, debido a amenazas impulsadas por la IA[5].

El 78% de los responsables de seguridad de la información encuestados afirmaron que las amenazas impulsadas por la IA tenían un impacto significativo en su organización[6].

El 61% de las organizaciones observaron un aumento de los ataques “deepfake” en 2024[7].

El número de dominios de nivel superior (TLD) se ha multiplicado (hace 30 años había 7; ahora hay más de 1500), lo que facilita a los actores la creación de dominios similares mediante la IA[8]

EL PAPEL DE LOS SISTEMAS DE DISTRIBUCIÓN DEL TRÁFICO EN LOS ATAQUES MODERNOS

Los actores de amenazas han adoptado sistemas de distribución de tráfico (TDS) para potenciar sus actividades maliciosas. Al igual que Google AdSense permite a los sitios web monetizar su tráfico dirigiendo a los usuarios hacia los anuncios pertinentes, los ciberdelincuentes utilizan TDS maliciosos para canalizar a los usuarios hacia sitios fraudulentos, a menudo a través de sitios web secuestrados o anuncios engañosos. Las cadenas de redireccionamiento se crean para ocultar la infraestructura del atacante, haciéndola casi invisible para las herramientas de seguridad tradicionales. Es un método sigiloso, escalable y, lamentablemente, muy rentable para los actores maliciosos.

- La tecnología publicitaria maliciosa utiliza TDS y, en su mayoría, distribuye malware para robar información, que es la causa principal de las violaciones de datos en las empresas.
- Vane Viper, una campaña a gran escala de CAPTCHA falsos que utiliza TDS para distribuir Lumma Stealer, cuenta con una enorme infraestructura de más de 10.000 dominios. En el 4.º trimestre de 2024, generó 1 millón de impresiones publicitarias al día a través de más de 3.000 sitios web de anunciantes.

SALVAGUARDE SU ORGANIZACIÓN CON EL DNS PROTECTOR

La seguridad preventiva es un enfoque avanzado que se centra en anticipar, predecir y detener las ciberamenazas antes de que puedan causar daños.

Gartner define la ciberseguridad preventiva como: “Un enfoque proactivo destinado a prevenir, interrumpir o disuadir los ciberataques para que no alcancen sus objetivos”. Dado el uso cada vez mayor de la IA generativa en los ciberataques por parte de los actores maliciosos, las tecnologías de ciberseguridad preventiva desempeñan un papel crucial en la mejora de la defensa de las organizaciones contra el malware habilitado por IA, las vulnerabilidades de día cero, el ransomware y otras amenazas asociadas. A menudo, estas amenazas no pueden mitigarse de forma eficaz únicamente con las herramientas y los enfoques tradicionales de “detección y respuesta”.

Las organizaciones pueden utilizar el DNS para proteger todo su entorno —infraestructura local, cargas de trabajo en la nube, usuarios remotos y dispositivos IoT/TO— frente a ataques sofisticados y modernos.

Un enfoque de DNS protector es preventivo, porque no depende del paciente cero. Utiliza una combinación de inteligencia predictiva sobre amenazas que bloquea la infraestructura de los actores maliciosos antes de que se conviertan en armas, y un análisis algorítmico/basado en ML de las consultas al DNS en las redes de los clientes para proporcionar protección antes del impacto.

INTELIGENCIA PREDICTIVA DE AMENAZAS:

Lleva un seguimiento de las actividades previas al ataque e identifica la infraestructura de los actores maliciosos antes de que se convierta en arma, en lugar de perseguir variantes de malware y dominios concretos.

Aprovecha la telemetría del DNS y el aprendizaje automático para identificar dominios de alto riesgo y bloquear las amenazas antes de que lleguen a las redes.

Detecta y bloquea los TDS, que se utilizan para redirigir dinámicamente a los usuarios a sitios de phishing, kits de explotación o cargas útiles de malware.

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

El Instituto Nacional de Estándares y Tecnología (NIST) norteamericano ha reconocido la importancia del DNS en la ciberseguridad y ha incluido las directrices de DNS protector en su documento oficial, NIST SP 800-81. La guía destaca el papel del DNS como capa fundamental de ciberdefensa y afirma que, al integrar el DNS protector en las infraestructuras de seguridad existentes, las organizaciones pueden mejorar su capacidad para detectar y bloquear las amenazas antes que los sistemas de seguridad tradicionales.

> “Los servidores del DNS pueden proporcionar información significativa sobre las conexiones y los flujos de datos de los endpoints y, a menudo, prevenir incidentes de seguridad antes que otros sistemas”
>
> (**NIST**).

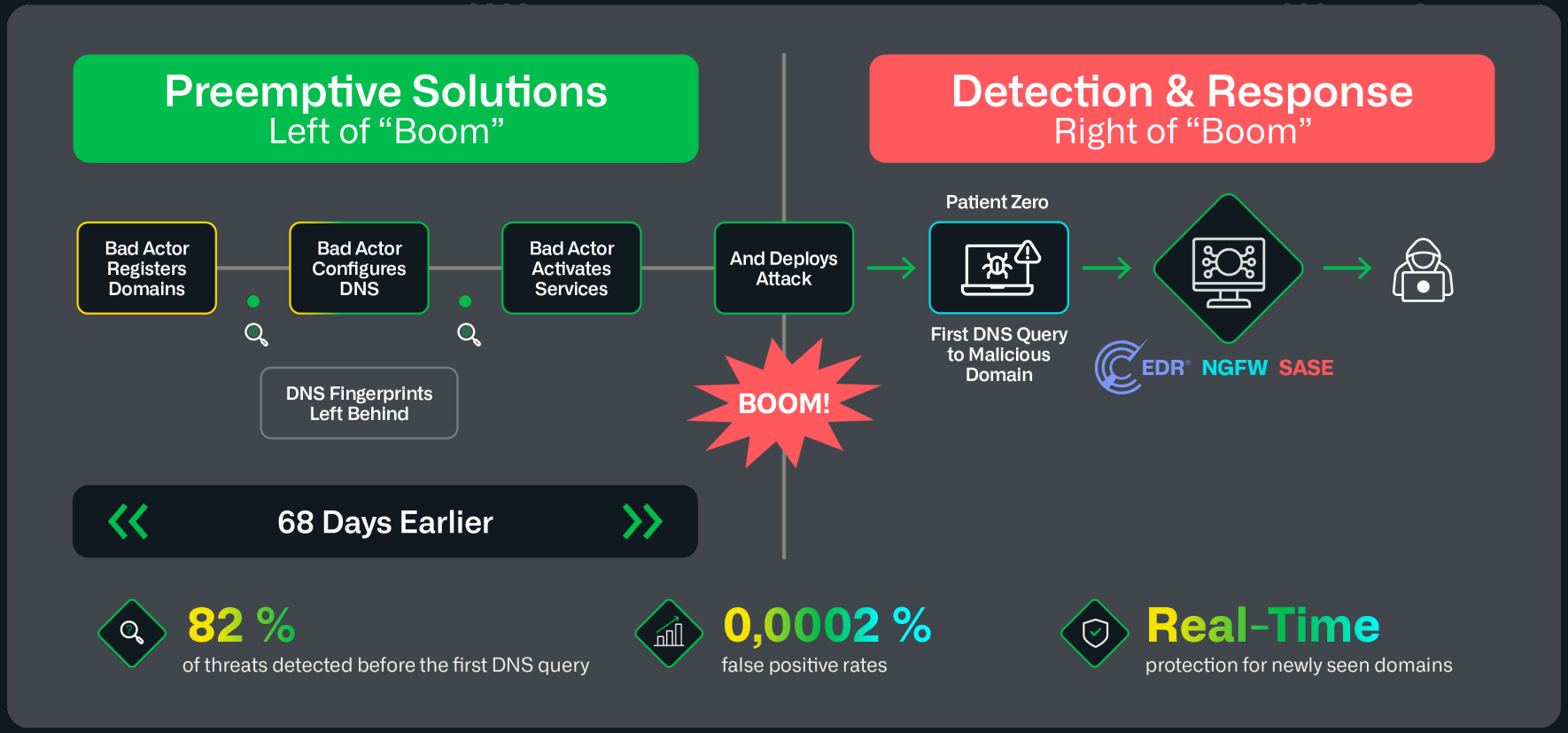
La oferta de DNS protector de Infoblox, Infoblox Threat Defense™, líder del sector, presenta muchas ventajas con respecto a las medidas de seguridad reactivas:

- Ofrece protección **antes del impacto** y en el momento en que se intenta la comunicación.
- Como **resolutor del DNS**—es decir, un servidor o software que convierte nombres de dominio legibles por humanos en direcciones IP legibles por máquinas—, Infoblox **ve todas las conexiones al DNS** de cada dispositivo (incluidos los dispositivos de usuario final, IoT/TO), independientemente de si se encuentran detrás de un firewall o no, y de si hay un **agente SASE o no.**
- Supervisa **204.000 clústeres** de actores de amenazas en tiempo real o grupos de actividades de ciberataques relacionados.
- **Bloquea 5 veces más dominios de alto y medio riesgo** que otras herramientas de seguridad que buscan comportamientos maliciosos conocidos.
- Bloquea una media de **68,4 días antes** que el resto del sector.
- **Detecta el 82% de las amenazas basadas en dominios** antes de la primera consulta al DNS.
- Tiene una **tasa de falsos positivos del 0,0002%**.
- Identifica y bloquea **el uso no autorizado de la IA** basándose en la actividad del DNS.
- Ayuda a reducir la exposición a **registros del DNS descolgados** y dominios similares.
- **Reduce la carga en un 50%** en otras herramientas de seguridad, como firewalls y sistemas de gestión de información y eventos de seguridad (SIEM), al filtrar **el tráfico malicioso** antes de que llegue a esos sistemas.
- Fácil **atribución de usuarios y dispositivos**, y priorización de amenazas con información sobre los activos.

INFOBLOX THREAT DEFENSE

SE HAN DESCUBIERTO Y MONITORIZADO 204.000 (y sumando) clústeres y cárteles casi en tiempo real

>100 perfiles de actores de amenazas nombrados



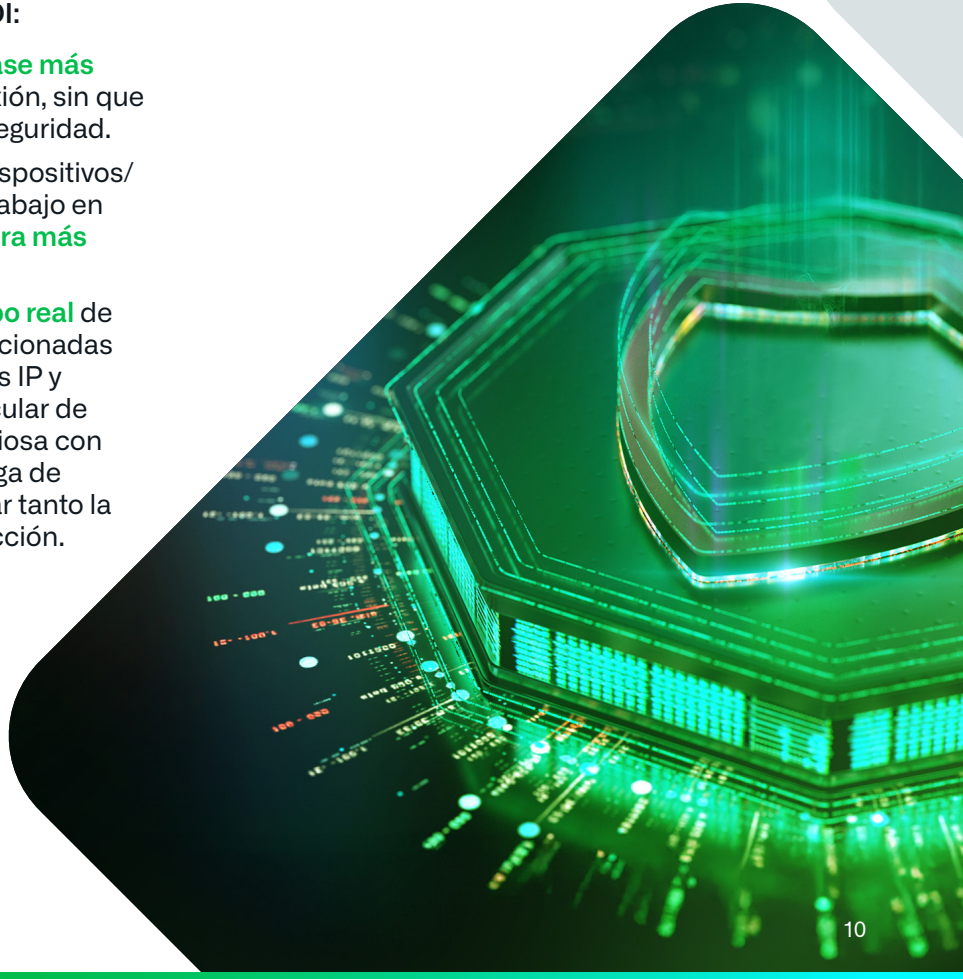
EL PODER DE UNA PLATAFORMA DDI PROTECTORA

El DNS protector funciona mejor cuando el DNS ya está gestionado, es decir, en una plataforma DDI. Infoblox es el único proveedor que cuenta con una plataforma DDI protectora integrada, lo que facilita activar una protección gestionada por un equipo central, responsable de todas las cuestiones relativas al DNS.

De este modo, se simplifican enormemente las operaciones y la resolución de problemas, en comparación con lo que requiere habilitar el DNS protector en firewalls de próxima generación (NGFW) o soluciones Secure Access Service Edge (SASE). Con Infoblox como resolutor del DNS, las organizaciones se benefician de una única plataforma unificada que supervisa los datos de las consultas al DNS de la empresa en busca de amenazas, evalúa el riesgo cuando un nuevo dominio entra en los resolutores de Infoblox y lo bloquea de forma proactiva en línea según sea necesario para evitar que se produzcan incidentes

Otras razones por las que conviene usar un DNS protector en una plataforma DDI:

- **Bloquea la amenaza en la fase más temprana,** antes de la conexión, sin que llegue al resto de la pila de seguridad.
- Protege a los usuarios, los dispositivos/IoT/TO/ICS y las cargas de trabajo en la nube mediante la **cobertura más amplia disponible.**
- **Visibilidad nativa y en tiempo real** de las consultas al DNS correlacionadas con la gestión de direcciones IP y DHCP, lo que le permite vincular de inmediato la actividad maliciosa con un usuario, dispositivo o carga de trabajo específicos y acelerar tanto la investigación como la corrección.



BENEFICIOS EMPRESARIALES

- Reducción del riesgo de violaciones de datos.
- Ahorro medio de 500 horas en analistas del SOC al mes y 400.000 dólares en productividad al año.
- Retorno de la inversión del 243%, con un periodo de amortización inferior a seis meses.
- Reducción del 50% del número de alertas generadas por otras herramientas de seguridad, lo que reduce los costes operativos.

CASOS PRÁCTICOS DE CLIENTES

Los clientes de Infoblox han implementado con éxito las soluciones de Infoblox para diversos casos de uso:

Protección proactiva contra el ransomware

Una cadena de restaurantes informales decidió adoptar un enfoque más proactivo para mejorar su postura de seguridad general mediante la implementación del DNS protector, tras varios incidentes de ransomware de gran repercusión. También deseaba obtener visibilidad sobre el 100% del tráfico del DNS para supervisar las amenazas.

Prevención de la exfiltración de datos a través del DNS

Una importante compañía de seguros médicos remedió las brechas en la tunelización del DNS que se identificaron durante una prueba de penetración interna del equipo rojo, que no pudo bloquearse con las soluciones NGFW y SASE existentes.

Zero Trust

Una empresa de transportes utilizó una combinación de acceso remoto basado en el DNS y detección de amenazas junto con soluciones para endpoints —como la detección y respuesta de endpoints (EDR) y la gestión de dispositivos móviles (MDM)— para crear una estrategia de usuarios y dispositivos de confianza cero a fin de proteger "a todo el mundo, en todo lugar y en todo momento".

infoblox®

ROMPA LA CADENA DE ATAQUE ANTES DE QUE COMIENCE. NO SEA EL PACIENTE CERO; REDUZCA A CERO LAS AMENAZAS.

Para obtener más información, visite la página de Infoblox Threat Defense en http://www.infoblox.com/es/products/threat-defense/.

1. *CrowdStrike 2025 Global Threat Report: Beware the Enterprising Adversary*, Myers, Adam, CrowdStrike Blog, 27 de febrero de 2025.
2. *Day 19: Analyzing DNS Logs — Detection Use Cases and How to Spot Malicious Activity*, Infosec Ninja, 7 de mayo de 2025
3. *Massive Surge In Ransomware Attacks—AI And 2FA Bypass In Crosshairs*, Winder, Davey, Forbes, 25 de marzo de 2025.
4. *ITRC Annual Data Breach Report*, Identity Theft Resource Center, enero de 2025.
5. *Verizon 2025 DBIR Report*
6. *Top 40 AI Cybersecurity Statistics*, Fox, Jacob, Cobalt, 10 de octubre de 2024.
7. *Speedy threat actors improving their lateral movement*, Hurley, Billy, IT Brew, 4 de marzo de 2025.
8. ICANN—En 2012, la ICANN (Corporación de Internet para la Asignación de Nombres y Números) lanzó un programa de ampliación de dominios de primer nivel, que permite a las organizaciones solicitar dominios de primer nivel personalizados.