

# Infoblox Threat Defense™ Business Cloud

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

### PROTÉJASE ANTES DE QUE HAYA IMPACTO CON LA SEGURIDAD ESENCIAL DEL DNS

Proteger la infraestructura, los datos y los usuarios es más difícil que nunca. Los modelos de seguridad tradicionales, que actúan en respuesta, son incapaces de seguir el ritmo. Las amenazas de hoy son más rápidas e inteligentes, y están diseñadas para eludir las defensas convencionales.

- Los ataques mediados por IA — como los dominios similares, el smishing, la elusión de la autenticación multifactor (MFA) y el phishing dirigido — evolucionan demasiado rápido para que las herramientas heredadas los detengan.
- El perímetro ha desaparecido. Ahora los usuarios se conectan desde cualquier lugar directamente a las aplicaciones en la nube, lo que deja huecos que las herramientas tradicionales no están diseñadas para abordar.
- Las SD-WAN y las sucursales suelen conectarse a internet directamente, sin pasar por puntos de inspección centralizados.
- IoT y los dispositivos no administrados crean puntos ciegos que la seguridad de endpoints no puede proteger por sí sola.
- La mayoría de las herramientas antiguas se basan en la detección de software malicioso conocido o en el filtrado de contenido: enfoques reactivos demasiado lentos para frenar a los atacantes actuales.

Para mantenerse a la vanguardia, las organizaciones necesitan **protección escalable y preventiva en la capa del DNS**. Infoblox ofrece una seguridad del DNS esencial, que identifica y bloquea las amenazas antes de que lleguen a los endpoints, cargas de trabajo en la nube o sucursales. Gracias a su visibilidad inigualable, su inteligencia predictiva y una integración perfecta en la pila de seguridad más amplia, Infoblox contribuye a reducir el ruido de las alertas, simplificar las operaciones y prevenir los ataques antes de que causen daños.

### SEGURIDAD DEL DNS PROTECTOR A GRAN ESCALA

A medida que las redes modernas se expanden a lo largo y ancho de centros de datos, redes SD-WAN, servicios en la nube e infraestructura de IoT, mantener una cobertura de seguridad uniforme se vuelve más complejo, aunque es más necesario que nunca.

Infoblox Threat Defense™ Business Cloud ofrece seguridad del DNS escalable y nativa de la nube que fortalece su postura desde la base, ya que protege su entorno actual y evoluciona con las iniciativas digitales sin añadir carga operativa. Ya se trate de proteger el DNS local, hacer extensiva la visibilidad a las sucursales distribuidas o dar soporte a usuarios remotos, Infoblox mantiene bajo control la capa del DNS donde lo necesite.

### PRESTACIONES CLAVE

- Anticípese a las amenazas modernas bloqueando ransomware, phishing, exploits y software malicioso mediante inteligencia de amenazas en tiempo real.
- Evite la exfiltración de datos con análisis y aprendizaje automático, detenga la tunelización del DNS, los algoritmos de generación de dominios (DGA), DNSMessenger y la actividad de flujo rápido.
- Proteja todos los dispositivos, dentro o fuera de la red, gestionados o no gestionados (BYOD, IoT, TO) en la capa del DNS.
- Aplique políticas de contenido con filtrado web y controles de acceso basados en el usuario.
- Proteja su marca con la [monitorización de dominios similares](#), que detecta y permite eliminar suplantaciones mediante dominios maliciosos.
- Investigue hasta tres veces más rápido con la telemetría del DNS enriquecida y el contexto de amenazas.
- Mejore la visibilidad por medio de correlacionar la actividad del DNS con los metadatos de la administración de direcciones IP (IPAM) para dar respuesta a los incidentes de forma más rápida y precisa.
- Priorice y responda más rápido a las amenazas críticas gracias a [SOC Insights](#) y el respaldo de la investigación impulsada por IA.
- Integre todo su ecosistema, compartiendo automáticamente registros e inteligencia de amenazas con SIEM, SOAR, firewalls de próxima generación (NGFW), IPS, endpoints y otras herramientas de seguridad.

A través de la inteligencia de amenazas en tiempo real, la visibilidad unificada y la integración con herramientas SOAR y SIEM, los equipos de seguridad pueden detectar, priorizar y responder más rápidamente. Así se reduce el tiempo de resolución, se mejora el rendimiento de la pila de seguridad existente y se abarata el coste total de la defensa contra amenazas empresariales.

Infoblox Threat Defense Business Cloud, que actúa desde la nube, puede ampliarse cómodamente para adaptarse a las cambiantes necesidades de los clientes, sin añadir complejidad operativa. A medida que crecen las demandas en los usuarios, los sitios y las cargas de trabajo, la seguridad se expande automáticamente.

## VENTAJAS DEL MODELO SAAS DE INFOBLOX

Infoblox Threat Defense Business Cloud es una solución de software como servicio (SaaS) que aporta capacidades de seguridad de última generación a su infraestructura local existente. La solución, basada en la nube y escalable de manera elástica, permite:

- Mejora inmediata de la postura de seguridad de una empresa
- Cobertura de seguridad fácil para todos los dispositivos, en cualquier lugar
- Menor carga para el equipo de TI

**“Hoy en día, existe una sobrecarga de ransomware, spyware y adware que llega a través de enlaces abiertos por usuarios de internet. La solución de seguridad en la nube de Infoblox ayuda a bloquear redirecciones hacia sitios maliciosos, evita la infección de dispositivos y protege a los usuarios de forma proactiva.”**

**Administrador sénior de sistemas e ingeniero de red,  
City University of Seattle**

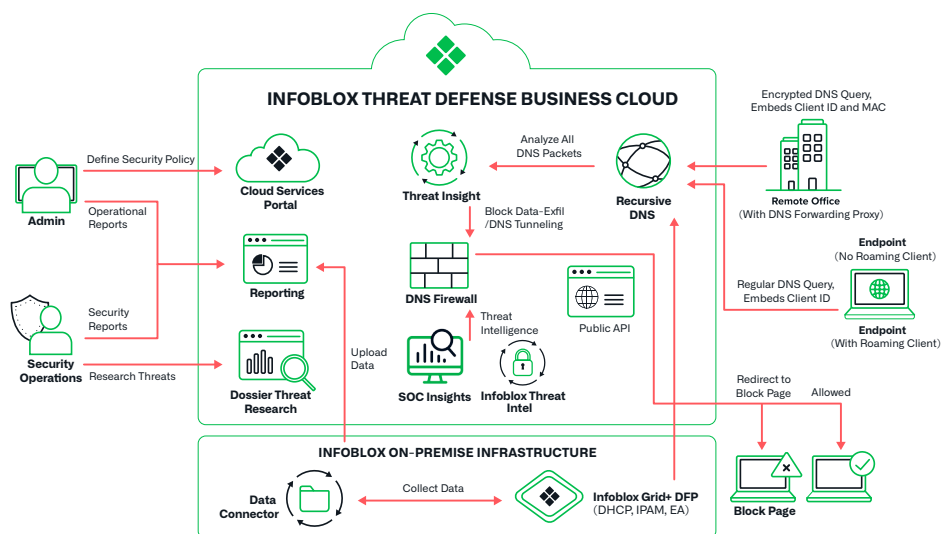


Figura 1. Escenario del flujo de trabajo para Infoblox Threat Defense Business Cloud

## PROXY DE REENVÍO DEL DNS

Para entornos en los que no es posible instalar un agente de endpoint — como IoT, impresoras o sistemas heredados—, Infoblox proporciona un proxy de reenvío del DNS (DFP), que mantiene la visibilidad a nivel del dispositivo y garantiza la aplicación de las políticas.

Este dispositivo virtual liviano incrusta la IP del cliente original en las consultas al DNS antes de reenviarlas a la nube de Infoblox. Así se obtiene una atribución precisa de la fuente, protección contra amenazas y una aplicación uniforme de las políticas, sin necesidad de agentes locales.

El proxy, integrado con Infoblox NIOS 8.3 y superior, permite a los clientes existentes activar la seguridad del DNS basada en la nube sin necesidad de infraestructura in situ adicional ni de implementaciones de software.

Infoblox Endpoint Agent proporciona protección segura de la capa del DNS para dispositivos itinerantes, lo que garantiza visibilidad y control aun cuando los usuarios trabajan fuera de la red.

Este agente liviano puede instalarse en portátiles o estaciones de trabajo para asegurar la visibilidad y la aplicación de políticas, incluso cuando los dispositivos están fuera de la red corporativa.

- Redirige a la nube de Infoblox las consultas al DNS con fines de inspección y aplicación de políticas.
- Cifra el tráfico y etiqueta cada consulta con la identidad del dispositivo y el contexto del usuario.
- Permite la atribución a nivel de usuario para investigar y documentar incidentes.
- Cambia automáticamente al modo de elusión cuando el dispositivo está en una red corporativa protegida.

Junto con el proxy de reenvío de DNS, el agente de endpoints ofrece a las organizaciones una cobertura total de usuarios, dispositivos y entornos, sin brechas de visibilidad ni protección.

## INTEGRADO

### Disponibilidad

Infoblox Threat Defense Business Cloud ofrece un 99,999% de tiempo de actividad del DNS (mantenimiento excluido), con suministro global de Anycast, copias de seguridad diarias y monitorización 24 horas.

### Seguridad

Todas las consultas al DNS y los datos almacenados se cifran en tránsito y en reposo. Los controles de acceso admiten restricciones por rol, IP y ubicación.

### Privacidad

Infoblox sigue las mejores prácticas de seguridad: aplica parches, análisis de código y pruebas de penetración periódicamente. Los datos de los clientes se separan lógicamente, se autentican mediante claves de API únicas y nunca se comparten con terceros.

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



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 (EE. UU.)

+1.408.986.4000  
[www.infoblox.com/es](https://www.infoblox.com/es)