HOJA DE DATOS

Infoblox para grupos de seguridad de las telecomunicaciones

Mejore la resiliencia y la eficacia de la seguridad e impulse la eficiencia de SecOps

EL DESAFÍO

Las redes de los proveedores de servicios de comunicaciones (CSP) actuales evolucionan hacia nubes de telecomunicaciones que abarcan redes privadas, públicas e híbridas, expandiendo los dominios operativos a través de las redes RAN, de cable y centrales, nubes privadas y públicas y ubicaciones perimetrales de acceso múltiple. Al trasladar la computación y el almacenamiento al perímetro para habilitar nuevos tipos de procesamiento y prestación de servicios en miles de nuevos sitios, aumenta drásticamente el potencial de sufrir amenazas de seguridad, tanto de aplicaciones de terceros como de atacantes externos. Los operadores almacenan extensas cantidades de datos personales y son responsables de la estabilidad de sus servicios de comunicación. El despliegue generalizado de dispositivos fuera del centro de datos también deja expuestos un número creciente de puntos de acceso y crea una superficie de ataque masiva, que los atacantes pueden explotar. Una violación de datos o un fallo en el servicio como consecuencia de un ciberataque puede causar graves daños financieros y de reputación o afectar a los clientes, lo que representa un golpe sustancial para cualquier empresa en un mercado altamente competitivo.

Con más recursos desplegados en el extremo más alejado, los equipos de TI y seguridad de los operadores deben gestionar un número significativamente mayor de pods, máquinas virtuales (a veces cientos a la vez y, potencialmente, miles de contenedores) en entornos físicos, virtuales y en la nube. Los dispositivos sin parches pueden convertirse en puntos de compromiso. Y aunque la protección de los endpoints con capacidades de detección y respuesta es imprescindible, los equipos de seguridad, ya de por sí sobrecargados, deben reconocer los signos de un ataque sin importar las circunstancias en una red en constante evolución y crecimiento. Los CSP necesitan soluciones de ciberseguridad maduras que amplíen su visibilidad para identificar las amenazas modernas, acortar las investigaciones y acelerar la respuesta eficaz ante incidentes.

LA SOLUCIÓN

Las soluciones de Infoblox para proveedores de servicios permiten las conexiones IP cruciales entre sus suscriptores y su mundo digital. Unificamos DNS, DHCP y la gestión de direcciones IP (DDI) para automatizar la visibilidad, la escalabilidad y la gestión de la red. Nuestras soluciones contribuyen a reducir los tiempos de respuesta a incidentes en dos tercios, al permitir que todos los componentes principales de su pila de seguridad —incluidos los sistemas de seguridad, orquestación, automatización y respuesta (SOAR)— respondan rápidamente a los eventos de seguridad antes de que causen daños. También ayudamos a los proveedores a minimizar las interrupciones comerciales causadas por ataques DDoS y otros riesgos y ataques basados en el DNS.

PRESTACIONES CLAVE

Reforzar la protección de seguridad
Detecte y bloquee los exploits e intentos de phishing, ransomware y software malicioso moderno que otras soluciones pasan por alto.

Aumentar la visibilidad
Obtenga una visibilidad precisa y un contexto de red enriquecido mediante la integración con metadatos de activos de gestión de direcciones IP, para lograr una comprensión y correlación óptimas de los eventos.

Acelerar la respuesta a los incidentes
Reduzca el tiempo de corrección, al correlacionar automáticamente la inteligencia sobre eventos, redes y amenazas de decenas de fuentes para acortar el tiempo de investigación hasta en dos tercios.

Mejorar el retorno de su inversión en seguridad
Obtenga el máximo valor con el mínimo esfuerzo gracias a unas defensas más sólidas y una mayor eficiencia en las operaciones de seguridad, y aproveche mejor sus plataformas SIEM y SOAR, y las demás herramientas de seguridad.

Infoblox reduce el coste total de su protección contra amenazas por medio de disminuir la carga de las defensas perimetrales. Nuestras soluciones permiten a los equipos de seguridad obtener más valor de las soluciones de terceros existentes, a través del intercambio bidireccional y en tiempo real de información sobre eventos de seguridad, así como mediante automatizaciones que reducen los costes asociados con el esfuerzo manual y el error humano. Los analistas de seguridad pueden obtener una visión integral de la inteligencia de amenazas asociada con un evento y reducir el tiempo de investigación de amenazas hasta en dos tercios.

BENEFICIOS CLAVE

Detener las amenazas que otras defensas no detectan

Una mejor inteligencia sobre amenazas hace que todas las herramientas de seguridad resulten más eficaces. BloxOne® Threat Defense recopila, selecciona y agrega información sobre amenazas de Infoblox, sus otras herramientas comerciales y fuentes gubernamentales y de terceros. La selección de Infoblox Cyber Intelligence Unit (CIU) impulsa la precisión, al tiempo que minimiza los falsos positivos y le permite personalizar la combinación según sus necesidades. A continuación, se puede compartir un «superfeed» normalizado en todo el paquete de seguridad, lo que aumenta la eficacia de cada defensa.

Bloquear el software malicioso y la fuga de datos

BloxOne Threat Defense opera a nivel del DNS para detectar amenazas que otras soluciones pasan por alto y detiene los ataques antes en el ciclo de vida de la amenaza. Bloquee el acceso a sitios maliciosos, las comunicaciones de mando y control (C&C), el robo de datos basado en el DNS y otras actividades maliciosas, aprovechando threat intel de múltiples fuentes y la potente IA/ML.

Minimizar las interrupciones empresariales

El DNS es fundamental para todas las organizaciones porque proporciona conectividad de red crítica. Si su DNS cae, su empresa se para. Los ataques DDoS exitosos pueden costarle a una organización cientos de miles de dólares en ingresos mensuales perdidos. Advanced DNS Protection (ADP) de Infoblox le protege eficazmente de la gama más amplia de ataques DDoS del DNS, manteniendo el tiempo de actividad del servicio para su empresa.

Acelerar la investigación y la corrección

Los analistas necesitan tener acceso a información fiable sobre amenazas y otros datos contextuales sobre un evento para acelerar las respuestas. Con Dossier™ como parte de BloxOne Threat Defense, los analistas obtienen una vista única de la inteligencia sobre amenazas asociada a un evento. El acceso rápido a inteligencia específica de eventos permite acelerar las investigaciones de amenazas hasta en dos tercios.

Mejorar las herramientas SIEM, SOAR y más

Al contar con gran cantidad de herramientas de defensa, los equipos de ciberseguridad pueden verse abrumados por la necesidad de gestionar manualmente decenas de herramientas de seguridad y responder a cientos o miles de alertas cada día. Ecosystem Exchange de Infoblox ofrece un conjunto de integraciones altamente interconectadas que permiten a los equipos de seguridad eliminar silos, optimizar sus soluciones SIEM y SOAR y mejorar el ROI de todo su ecosistema de ciberseguridad.

Reducir la sobrecarga de seguridad
Aproveche la inteligencia de eventos y amenazas, así como los análisis basados en IA/ML sobre el DNS, para disfrutar de protección escalable contra el software malicioso moderno y las amenazas del DNS.

Minimizar las interrupciones de la red
Mantenga la integridad del DNS y detenga los ataques DDoS externos e internos contra el DNS que pueden dejar su red fuera de servicio.

Aliviar las cargas de SecOps mediante la automatización

BloxOne Threat Defense incluye muchas funciones que le permiten aprovechar la inteligencia sobre amenazas, la información de eventos y otros datos de forma más inteligente. La automatización elimina los gastos generales de gestión y hace que las tareas de investigación y respuesta de SecOps sean más eficientes. Aligere la carga de dispositivos de seguridad perimetral saturados, como cortafuegos, IPS y proxies web, utilizando como primera línea de defensa los servidores del DNS que ya tiene disponibles.

Simplificar y optimizar la gestión de cambios y configuración de la red

Las raíces de muchos problemas de red pueden rastrearse hasta detectar un cambio: errores cometidos al modificar manualmente los dispositivos, configuraciones deficientes que causan problemas posteriormente y el debilitamiento de políticas de seguridad críticas y de la protección de la red. Infoblox NetMRI es una solución de gestión de cambios y configuraciones de red que automatiza flujos de trabajo rutinarios, como el aprovisionamiento de dispositivos y las operaciones de seguridad, lo que permite un cumplimiento más estricto y una respuesta más rápida a los incidentes.

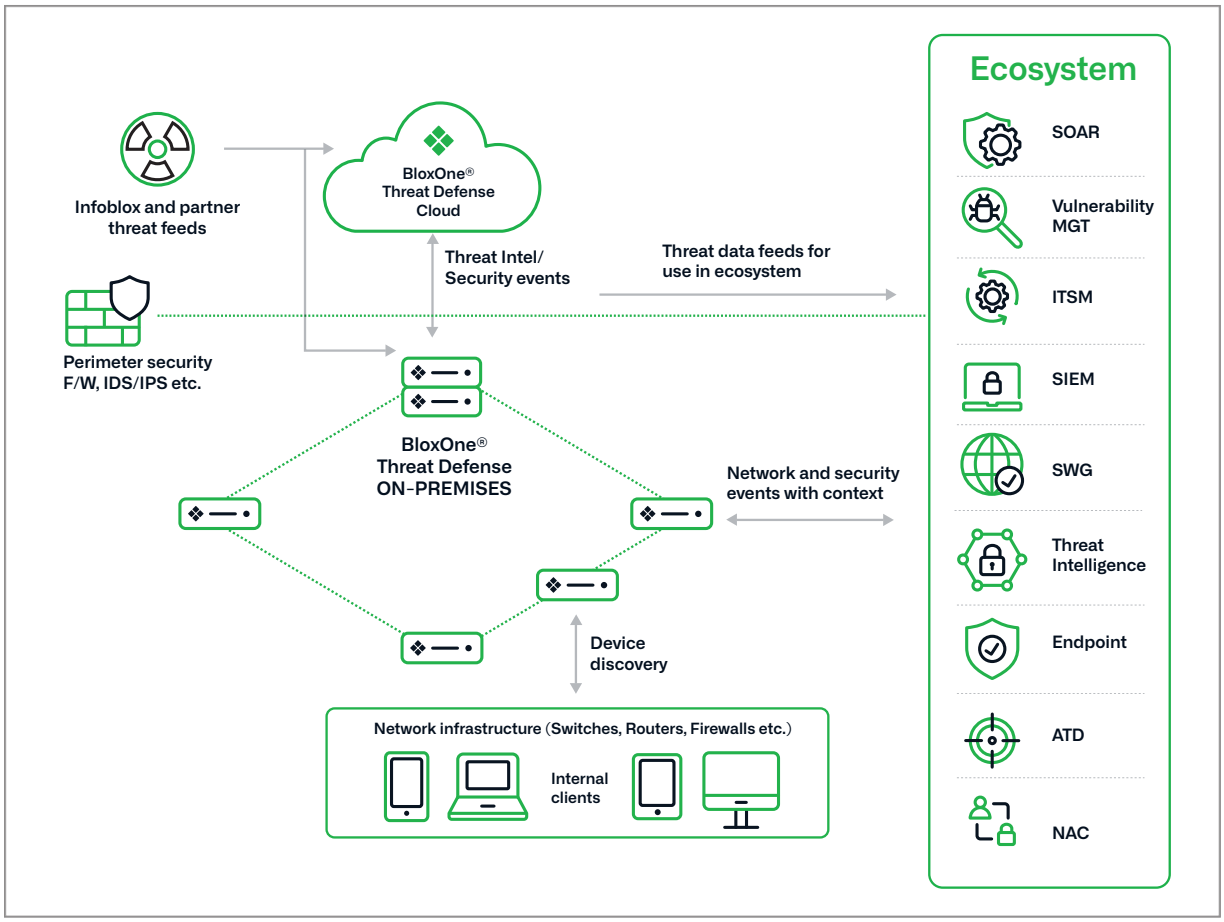

Figura 1: Infoblox refuerza y optimiza las redes de los proveedores de servicios de comunicación

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

+1.408.986.4000
www.infoblox.com/es

Versión: 20240521v1