infoblox

ESTUDIO DE CASO

La plataforma de datos SIEM líder amplía la fiabilidad, la visibilidad y la seguridad globales en redes híbridas con Infoblox

RESUMEN

Esta empresa estadounidense produce programas informáticos para buscar, supervisar y analizar datos generados por máquinas a través de una interfaz de estilo web.

Sus soluciones, incluida una de las principales herramientas de gestión de eventos e información de seguridad (SIEM) del mercado, ayudan a capturar, indexar y correlacionar datos en tiempo real en un repositorio de búsqueda a partir del cual puede generar alertas, paneles, informes y visualizaciones. La empresa utiliza datos de máquinas para identificar patrones de datos con el fin de proporcionar métricas, diagnosticar problemas y aportar inteligencia a las operaciones empresariales. Como cliente de Infoblox y socio OEM desde 2015, la compañía recientemente necesitó actualizar y expandir su plataforma DNS, DHCP e IPAM (DDI) para respaldar las operaciones globales y mejorar su postura de seguridad. Eligió la solución BloxOne® Threat Defense Advanced integrada en DDI de Infoblox para proteger su infraestructura, sus datos y sus usuarios del malware, el ransomware y la exfiltración de datos DNS.

SITUACIÓN

Fiabilidad y expansión global

En 2015, la compañía reemplazó su plataforma Microsoft DNS y DHCP con Infoblox DDI para mejorar el tiempo de actividad y la confiabilidad de la red. En el proceso, la empresa se convirtió en el proveedor de tecnología OEM para la herramienta de búsqueda y visualización de datos de Infoblox, Infoblox Reporting and Analytics. En 2021, sin embargo, había llegado el momento de renovar la red técnica. El equipo de TI de la compañía consideró brevemente EfficientIP, pero con la sólida reputación de Infoblox y su historial de confiabilidad, la compañía renovó su asociación con Infoblox y comenzó a construir sus 21 regiones en todo el mundo. La expansión a la nube formaba parte de una iniciativa de modernización y una hoja de ruta, pero la principal prioridad de la empresa era mejorar los servicios de red centrales. El equipo de TI quería una IPAM autorizada, visibilidad de un solo plano de control, gestión unificada, reducción de herramientas de red superfluas y gastos generales, flujos de trabajo simplificados y escalabilidad rápida. En consecuencia, continuó ampliando sus servicios con Infoblox basándose en la premisa de que “la confianza se gana con esfuerzo y se pierde fácilmente”.

“Se ha dicho que ‘la confianza se gana con esfuerzo y se rompe con facilidad’. Afortunadamente, Infoblox proporciona una DDI segura y fiable de categoría mundial que podemos confiar. Es nuestra plataforma preferida para la coherencia de la red global, la visibilidad del plano de control único y nos proporciona la escalabilidad que necesitamos para dar servicio a nuestras regiones globales en expansión. BloxOne Threat Defense con sus integraciones de ecosistemas, Dossier y Threat Insight es fácil de implementar y usar. Nos protege a nosotros, nuestros datos, infraestructuras y usuarios del malware, el ransomware, las amenazas de exfiltración de datos y los malos actores a los que nos enfrentamos a diario.”

Jefe de equipo de TI

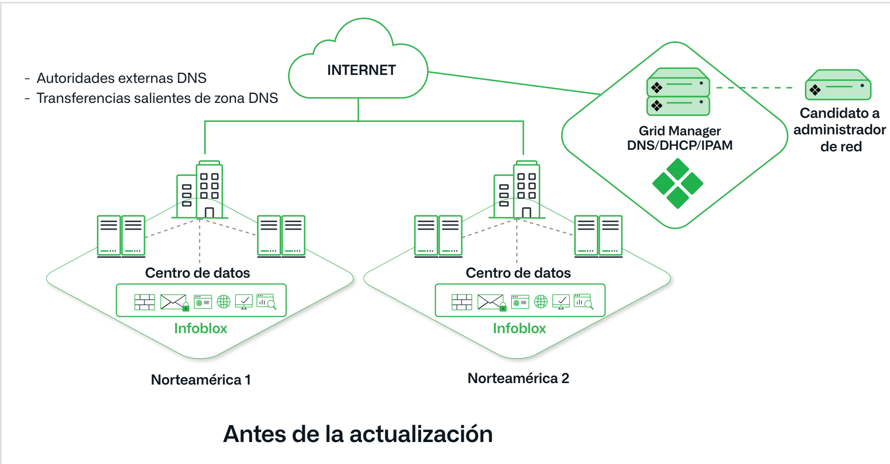

Figura 1: Arquitectura de red antes de modernizar con Infoblox

DESAFÍO

Actualización de los servicios para ampliar la fiabilidad, la visibilidad y la seguridad en todo el mundo

Con Infoblox, la empresa no sufrió ningún conflicto importante en la red, interrupciones o eventos de seguridad, lo que le permitió centrarse en la actualización de su tecnología de sistema operativo de identidad de red DDI para ampliar la visibilidad, la seguridad y el tiempo de actividad de la red a otros sitios de todo el mundo. Especificaba gestión centralizada, gestión de direcciones IP de nivel empresarial (IPAM) y conmutación por error de DHCP para una disponibilidad del servicio “siempre activa”. La empresa también requería un DNS autoritativo interno y un servicio de DNS recursivo seguro para las consultas salientes. Si bien la automatización no era una prioridad principal, el equipo de TI se centró en eliminar las herramientas superfluas, el mantenimiento y los gastos generales. Sin embargo, también priorizaron la visibilidad bajo demanda para auditoría histórica y cumplimiento, métricas de utilización y rendimiento, alertas de seguridad de DNS y planificación de capacidad.

Dadas las crecientes amenazas de seguridad, la empresa priorizó el endurecimiento de su postura de seguridad. Decidió que la seguridad integrada en DDI era la solución adecuada para proteger su infraestructura, datos, socios y usuarios contra el comando y control, el ransomware, el malware, el algoritmo de generación de dominios (DGA), el flujo rápido, DNS Messenger y la exfiltración de datos a través de DNS. Tanto los requisitos de red como los de seguridad requerían una transición de su implementación existente (véase la Figura 1) a una arquitectura DDI modernizada de nivel empresarial (véase la Figura 2).

SOLUCIÓN

Modernización, visibilidad, seguridad y escalabilidad de la red

Con un personal de TI muy pequeño, la empresa necesitaba simplicidad y “establecer y olvidar” fiabilidad. La plataforma DDI de nivel empresarial de Infoblox incluía una combinación de hardware y dispositivos virtuales reforzados con seguridad para ver y administrar mejor su red. Implementaron un Grid Manager y un Grid Manager Candidate, que incluía IPAM totalmente gestionado y DNS autoritativo interno en un miembro de HA para una

PERFIL DEL CLIENTE:

- Esta empresa de software, una compañía global con más de 7500 empleados, 850 patentes y disponibilidad en 21 regiones de todo el mundo, ofrece una plataforma de datos abierta y extensible que admite datos compartidos en cualquier entorno. Esto significa que todos los equipos de la organización pueden obtener visibilidad contextual de la red de extremo a extremo para cada interacción y proceso empresarial.

SITUACIÓN:

- La empresa buscaba mejorar la fiabilidad de su infraestructura aumentando la redundancia y añadiendo DNS Security para integrarlo con su oferta SIEM, garantizando el tiempo de actividad y la disponibilidad de las aplicaciones.

DESAFÍO:

- Los responsables de la toma de decisiones de TI se dieron cuenta de que necesitaban ampliar los servicios de red principales para obtener visibilidad, fiabilidad, gestión y escalabilidad de un solo plano de control para servir a sus usuarios finales en todo el mundo.

INICIATIVAS:

- Actualice a una solución DDI modernizada y escalable con visibilidad integral de la red gestionada a través de un único plano de control
- Garantice un tiempo de actividad continuo, alta disponibilidad y redundancia incluso durante la migración de red
- Habilite IPAM empresarial, DNS interno y externo, conmutación por error de DHCP e informes
- Acceda a los datos de la red bajo demanda para la auditoría o el cumplimiento, el rendimiento y los eventos de amenazas y el análisis predictivo
- Implemente soluciones integradas de seguridad y ecosistema de DDI para proteger a los socios, las filiales y los usuarios finales de los ataques de malware y ciberseguridad

visibilidad óptima. El diseño de la red especificaba unidades dedicadas para las consultas DNS entrantes de Internet. Las consultas DNS salientes (caché DNS DMZ) se reenviaron a la nube para la resolución de direcciones IP geolocales. Además, el protocolo de conmutación por error DHCP permitió la redundancia del sitio mientras que los miembros de HA ofrecían la máxima disponibilidad del servicio, especialmente para los despliegues de VoIP en toda su red global.

Se añadió Cloud Network Automation de Infoblox para visibilidad, gestión y control en servicios de nube pública de AWS. También se ha añadido DNS Traffic Control (DTC) para la gestión del tráfico de red, el tiempo de actividad de las aplicaciones, la facilidad de implantación de nuevos servicios y la integración de API.

Como era de esperar, la empresa también era una gran usuaria de Infoblox Reporting and Analytics. Esta solución fue útil para las alertas, los cuadros de mando y los informes para una visibilidad de la red a petición, una visión de la red y una mejora del tiempo de respuesta. En lugar de estar enterrados en su red, los ricos metadatos DDI de la empresa eran visibles, accesibles y útiles para búsquedas, análisis predictivos y visualizaciones gráficas para puntos finales, rendimiento, análisis forenses de seguridad, registro de acceso y auditoría y cumplimiento para admitir visibilidad y tiempo de actividad coherentes.

Aunque la empresa contaba con Cisco Umbrella para la seguridad, prefería la idea de utilizar DNS tanto como primera capa de defensa como para enriquecer sus otros conjuntos de herramientas. La solución de seguridad de Infoblox era simple: comenzar con DNS, agregar y correlacionar inteligencia sobre amenazas, bloquear a los malos actores y, al hacerlo, eliminar la carga de otras herramientas críticas. En consecuencia, el equipo de TI de la empresa seleccionó la solución de Infoblox. BloxOne Threat Defense Advanced (Figura 2) local y gestionado en la nube para obtener una protección actualizada contra amenazas como ransomware, DGA, DNS Messenger y exfiltración de datos a través de DNS. BloxOne Threat Defense actúa como Un solucionador general en la nube para la resolución geolocal para proteger a los usuarios y eliminar el malware. La solución también ofrecía capacidades de seguridad probadas en el mercado y en el tiempo que llenaban un vacío de seguridad que faltaba para asegurar el DNS, mejorar las alertas y proteger a los socios comerciales y a los usuarios. Al departamento de TI le gustó su administración rápida y sencilla, los datos

RESULTADOS:

- Establezca seguridad desde la red utilizando DDI seguro y de nivel empresarial
- Garantice la redundancia de la base de datos, la resiliencia de la red y el tiempo de actividad confiable
- Integre con las capacidades de seguridad existentes mientras fortalece la postura de seguridad en todo el sistema

SOLUCIONES INFOBLOX

- NIOS DDI con conmutación por error
- Automatización de redes en la nube
- Control de tráfico DNS
- Informes y análisis
- BloxOne® Threat Defense Advanced
- Integración de ecosistemas
- Dossier
- Información sobre amenazas
- Dispositivos de informes virtuales Infoblox 2225 HA, 1425, v1425, Security Hardened, BITDA y v5005

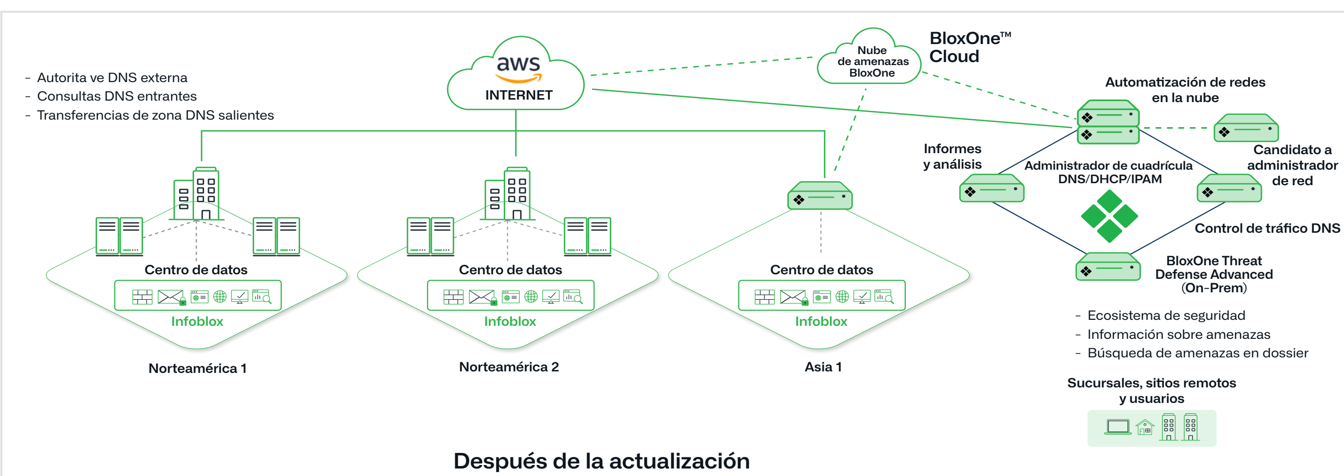

Figura 2: Arquitectura posterior a la actualización con DDI modernizada, incluidos los informes y BloxOne Threat Defense

contextuales de IPAM combinados con la defensa frente a amenazas y la integración DDI de Infoblox. La empresa también añadió Dossier y DNS Threat Insight con sus sofisticados algoritmos y aprendizaje automático para escanear constantemente la red en busca de exfiltración de datos DNS y detener toda transmisión de datos DNS no autorizada.

RESULTADOS

Los servicios de red modernizados ofrecen fiabilidad, visibilidad, seguridad y escalabilidad global

Con su actualización de Infoblox, la compañía está mejor posicionada para cumplir su promesa de proporcionar confiabilidad, calidad, servicio personalizado y soporte sin precedentes para los clientes de software globales. Ahora cuenta con visibilidad total de la red, disponibilidad continua de las aplicaciones, tiempo de actividad y redundancia, junto con un DNS empresarial coherente para los usuarios locales, externos y conectados en cualquier lugar. Además, la modernización de la DDI ayuda a preparar las inversiones en TI para el futuro, ya que la empresa planifica su migración a la nube. El acceso a los datos bajo demanda mejora la visibilidad y la gestión de la red y acelera la toma de decisiones y la respuesta de la red, especialmente para un equipo de TI pequeño.

Desde el punto de vista de la seguridad, BloxOne Threat Defense Advanced con Threat Insight es fácil de configurar y usar y ofrece los metadatos integrados en DDI y la flexibilidad necesarios para una seguridad de primer nivel contra los malos actores y las amenazas de seguridad diarias.

Las soluciones de seguridad de Infoblox refuerzan las capacidades de seguridad de la empresa y la ayudan a ofrecer una respuesta de seguridad sólida, no solo para proteger la infraestructura, los datos y los trabajadores remotos, sino también para proporcionar la confianza necesaria para potenciar la expansión de nuevos proveedores, socios y usuarios remotos. BloxOne Threat Defense Advanced con Dossier y Threat Insight permite una rápida detección, investigación, respuesta y reparación contra ransomware, malware y exfiltración de datos. Estas herramientas e integraciones de seguridad intensifican la protección de la red contra amenazas de seguridad cada vez más frecuentes y complejas en toda la red nacional de sucursales de la empresa. Al crear seguridad desde la red, la empresa puede aprovechar sus metadatos DDI para obtener una visibilidad contextual profunda y conocimientos para mejorar el control, la eficiencia de la seguridad, reducir los costos de seguridad y hacer que las herramientas de seguridad sean más efectivas. Utilizando las fiables y modernizadas plataformas de red y seguridad de Infoblox, la empresa puede continuar con sus décadas de compromiso en la potenciación de la visibilidad de los datos para aplicaciones de seguridad y SIEM en el futuro.

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

+1.408.986.4000
www.infoblox.com