NOTAS DE LA SOLUCIÓN

CREAR UNA INFRAESTRUCTURA ÁGIL Y RESILIENTE

En el panorama empresarial actual, competitivo y en permanente cambio, la agilidad y la innovación son fundamentales para el éxito empresarial. A medida que evoluciona la tecnología, las redes modernas deben poder adaptarse y seguir el ritmo de la innovación aprovechando los últimos avances que permitan implementar de forma eficiente nuevas aplicaciones y servicios, y ofrecer la flexibilidad necesaria para responder a las cambiantes demandas del mercado.

EL RITMO DE LA MODERNIZACIÓN ES IMPLACABLE

Según un informe de Gartner, de aquí a 2026, al menos el 50 % de las aplicaciones in situ se modernizarán para integrarse con herramientas de plataforma de gestión SaaS (SMP), frente al 20 % existente en 2021. Con la digitalización, las redes se vuelven más dinámicas y cambian constantemente. Diversos factores, como el trabajo remoto, la expansión multinube, las nuevas exigencias en materia de ciberseguridad y la necesidad de nuevas competencias, contribuyen a acelerar la modernización.

DEFICIENCIAS DE LOS SERVICIOS CRÍTICOS DE RED HEREDADOS

La infraestructura de red consta de muchos componentes: cortafuegos, enrutadores, conmutadores, dispositivos Wi-Fi, servidores de nombres de dominio, servidores DHCP y otros. La mayoría de los elementos de las infraestructuras críticas ya se han actualizado a versiones modernas de hardware o software. ¿Qué pasa con los servidores de nombres de dominio y los servidores DHCP? ¿Sus servicios de red centrales siguen siendo heredados? Depender de servicios de red obsoletos —software libre, sistemas caseros o dispares— supone un enorme obstáculo para la transición digital.

- **Los sistemas heredados están desarticulados**: la gestión manual es costosa y conlleva un alto riesgo de tiempo de inactividad y caídas del servicio.
- **Los sistemas heredados son lentos**: las redes deben ser ágiles para adoptar nuevas ideas y tecnologías como parte de iniciativas estratégicas de digitalización o fusiones y adquisiciones.
- **Los sistemas heredados están expuestos**: las brechas de seguridad y la falta de conciencia contextual resultan en una corrección ineficaz y tardía de las amenazas.

El DNS y el DHCP son fundamentales para todas las redes, y si todavía utiliza servicios nativos, su red está expuesta a interrupciones masivas.

IMPULSORES CLAVE DE LA MODERNIZACIÓN: EL CAMINO A SEGUIR

Las organizaciones modernizan sus redes para hacer frente a los retos que plantean un alcance normativo cada vez mayor, las limitaciones de recursos, amenazas en constante evolución y el desconocimiento en el ámbito de la seguridad. Deben reducir constantemente el tiempo de inactividad, acotar los costes y minimizar las brechas de seguridad para ofrecer un tiempo de actividad del 100 %, adoptar nuevas ideas y mejorar la pila de seguridad existente. Esto exige replantearse los enfoques de las operaciones críticas de la red, incluida la gestión de DNS, DHCP y direcciones IP (en conjunto, «DDI»). Estos son los factores clave para modernizar su red.

OPTIMICE LAS OPERACIONES: REEMPLACE EL FREEWARE CON HERRAMIENTAS DISEÑADAS PARA UN PROPÓSITO ESPECÍFICO

Libre no significa gratuito. Aunque los gastos de capital iniciales pueden parecer menores, los gastos operativos en los que incurrirá al utilizar herramientas DDI libres o de bajo coste superarán las ventajas. Las soluciones freeware, como Microsoft o las herramientas de código abierto, no pueden adaptarse al crecimiento debido a las limitaciones del sistema y a la falta de funciones avanzadas para ofrecer una alta disponibilidad, la detección de máquinas virtuales no utilizadas, validaciones basadas en políticas, etc. Las infraestructuras de Microsoft son propensas a sufrir interrupciones y tiempo de inactividad, ya sea debido a las constantes actualizaciones de parches o a la necesidad de migrar a Azure AD. La gestión manual de sitios distribuidos incrementa la ineficiencia y aumenta los costes.

El mejor enfoque es aprovechar **herramientas diseñadas específicamente** para simplificar y optimizar las operaciones críticas. Estas herramientas están diseñadas para la globalización y le permiten reducir las tareas operativas, al expandirse sin problemas a diversas infraestructuras y ubicaciones remotas. Simplifican la gestión, optimizan el mantenimiento y reducen el tiempo, puesto que proporcionan automatización, detección y visibilidad centralizada de la red. Proporcionan actualizaciones sin tiempo de inactividad, que se reduce al mínimo gracias a una alta disponibilidad a escala.

ACELERE LAS INNOVACIONES: USE UNA ÚNICA HERRAMIENTA CENTRALIZADA EN LUGAR DE SISTEMAS DISPARES

La mayoría de las empresas utilizan entre dos y cuatro soluciones de DNS, lo que dificulta la gestión de servicios críticos y responder rápidamente a los problemas. Los silos organizativos e informativos a menudo provocan retrasos y errores. Las diferentes convenciones de nomenclatura y modelos operativos de los distintos proveedores de nube dan lugar a configuraciones incorrectas y a tiempo de inactividad. La visibilidad fragmentada de las redes aumenta el tiempo necesario para la resolución de problemas y la auditoría.

Las organizaciones deben encontrar una solución eficiente y eficaz para acelerar las innovaciones y habilitar iniciativas empresariales como la expansión multinube, las fusiones y adquisiciones, etc. Invertir en una **herramienta centralizada** le permitirá alcanzar estos objetivos mediante la automatización, una misma convención de nomenclatura para el DNS y visibilidad en las redes locales y la nube. En lugar de utilizar una combinación de sistemas dispares, podrá adaptarse más rápidamente a las necesidades empresariales y reducir las ineficiencias mediante una herramienta centralizada que proporciona control y coherencia de las políticas, permite una resolución de problemas más rápida y una mejor colaboración, elimina las configuraciones incorrectas y los errores, y reduce los riesgos de auditoría y cumplimiento normativo, así como los costes operativos.

PROTEJA LA INTEGRIDAD DE LA MARCA: APROVECHE EL DNS PARA DETECTAR AMENAZAS DE FORMA TEMPRANA

Los ámbitos en constante evolución del panorama de las amenazas —como el malware, el ransomware, los dominios similares, la exfiltración de datos y el phishing— suponen enormes riesgos para la identidad de la marca y la protección de datos. Existe una importante brecha de seguridad, ya que las soluciones existentes en el mercado ignoran el DNS y no logran anticiparse a los ataques. Solo en el último año, los hackers utilizaron casi 42.000 dominios impostores en un ataque masivo de phishing. Además, los sistemas aislados y dispares, la falta de personal cualificado, la gestión manual y el desconocimiento del contexto dan lugar a ineficiencias en las operaciones de seguridad y a retrasos en los tiempos de respuesta.

La detección temprana de las amenazas reduce el riesgo y cierra la brecha de seguridad. Aplicar la **búsqueda de amenazas basada en el DNS** permite detectar y bloquear las amenazas más temprano, ya que la mayoría de los ciberataques se basan en el DNS. El uso del DNS como primera línea de defensa protege contra la exfiltración de datos, los algoritmos de generación de dominios y los impostores, y protege todos los dispositivos IoT/TO. Además, mejora la eficiencia de SecOps, ya que reduce el tiempo de investigación, automatiza la corrección y evalúa con carácter proactivo los riesgos de vulnerabilidad.

SOLUCIONES DE INFOBLOX PARA UNA INFRAESTRUCTURA ÁGIL Y RESILIENTE

Visibilidad, automatización y control

Infoblox ofrece a las organizaciones una visibilidad, automatización y control sin precedentes sobre quién y qué se conecta a su red. Infoblox reduce significativamente el costoso tiempo de inactividad al eliminar el mantenimiento engorroso y obligatorio, automatiza las tareas operativas que requieren mucha mano de obra y reduce la carga asociada a la gestión del inventario de activos de red. Las soluciones de Infoblox están diseñadas con la seguridad en mente, reduciendo las alertas falsas mediante un mayor conocimiento contextual y mejorando la eficiencia. Infoblox proporciona:

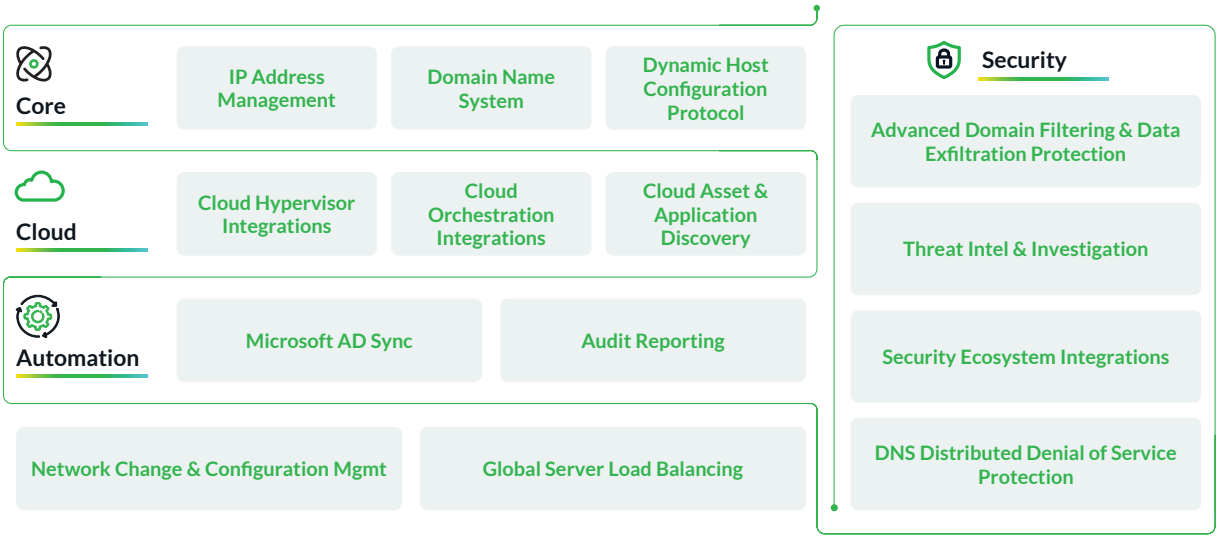

Figura 1: Soluciones de Infoblox

CONCLUSIÓN

La modernización impulsa la transformación digital. Elegir la solución adecuada para su red impulsa la modernización continua. Los enfoques heredados para gestionar servicios de red críticos dificultarán su capacidad para innovar rápidamente, adaptarse a las demandas empresariales cambiantes y mantener la competitividad. Aproveche la visibilidad, la automatización y el control que ofrece Infoblox para modernizar su red a la velocidad que sea necesaria y adecuada para el crecimiento de su empresa.

infoblox.

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

Versión: 20230803v1