infoblox.

솔루션 참고 사항

민첩하고 복원력이 높은 인프라 구축

오늘날과 같이 빠르게 변화하고 경쟁이 치열한 비즈니스 환경에서는 민첩성과 혁신이 기업의 성공을 좌우합니다. 기술이 계속 발전함에 따라 현대 네트워크는 최신 기술을 활용하여 혁신에 발맞추고 새로운 애플리케이션과 서비스를 효율적으로 배포하며 변화하는 시장 수요에 대응하는 데 필요한 유연성을 제공하여 적응력을 갖춰야 합니다.

현대화의 속도는 끊임없다

Gartner 보고서에 따르면 2026년까지 최소 50%의 온프레미스 애플리케이션이 SaaS 관리 플랫폼(SMP) 도구와 통합되도록 현대화될 것이며, 이는 2021년의 20%에서 증가한 수치입니다. 디지털화로 인해 네트워크는 더욱 역동적이고 지속적으로 변화하고 있습니다. 원격 근무, 멀티 클라우드 확장, 새로운 사이버 보안 요구, 새로운 기술 세트의 필요성 등 다양한 요인으로 인해 현대화 속도가 빨라지고 있습니다.

중요 레거시 네트워크 서비스의 단점

네트워크 인프라는 방화벽, 라우터, 스위치, Wifi 장치, 도메인 네임 서버, DHCP 서버 등 다양한 구성 요소로 이루어져 있습니다. 대부분의 중요한 인프라 요소는 이미 최신 하드웨어 또는 소프트웨어 버전으로 업그레이드되었습니다. 도메인 네임 서버 및 DHCP 서버의 경우는 어떨까요? 여전히 레거시 핵심 네트워크 서비스를 이용하고 있으신가요? 프리웨어, 자체 제작 또는 서로 다른 시스템 등 레거시 네트워크 서비스에 의존하는 것은 디지털 여정의 큰 장애물이 되고 있습니다.

- **레거시 시스템은 단절되어 있습니다**. 수동 관리는 비용이 많이 들고 다운타임과 가동 중단의 위험이 큽니다.
- **레거시 시스템은 느립니다**. 네트워크는 디지털화 또는 M&A를 위한 전략적 이니셔티브의 일환으로 새로운 아이디어와 기술을 채택할 수 있도록 민첩해야 합니다.
- **레거시 시스템은 노출됩니다**. 보안 갭과 상황 인식 부족으로 인해 위협에 대한 대응이 비효율적이고 느립니다.

DNS와 DHCP는 모든 네트워크에 필수적이며, 여전히 기본 서비스를 활용하고 있다면 네트워크가 대규모 중단에 직면할 수 있습니다.

현대화의 핵심 동인: 앞으로의 방향

조직은 끊임없이 증가하는 규제 환경, 리소스 제약, 끊임없이 진화하는 위협, 보안성 영역의 기술 격차 등의 문제를 해결하기 위해 네트워크를 현대화하고 있습니다. 100% 가동 시간을 제공하고, 새로운 아이디어를 수용하며, 기존 보안 스택을 개선하기 위해 지속적으로 다운타임을 줄이고, 오버헤드를 관리하며, 보안 침해를 최소화해야 합니다. 따라서 DNS, DHCP, IP 주소 관리(총칭하여 “DDI”)를 비롯한 중요한 네트워크 운영에 대한 접근 방식을 재고해야 합니다. 네트워크 현대화를 위한 핵심 동인은 다음과 같습니다.

운영 간소화: 프리웨어를 전용 도구로 교체하세요

무료는 무료가 아닙니다. 초기 자본 비용은 저렴해 보일 수 있지만, 무료 또는 저렴한 DDI 도구를 사용하면 발생하는 운영 비용이 이점을 능가할 것입니다. Microsoft나 오픈 소스 도구와 같은 프리웨어 솔루션은 시스템 제한과 고급 기능의 부족으로 인해 성장에 맞춰 확장할 수 없습니다. 이러한 기능에는 보다 높은 가용성 지원, 사용하지 않는 가상 머신의 발견, 정책 기반 유효성 검사 등이 포함됩니다. Microsoft 인프라는 지속적인 패치 업데이트로 인해 중단 및 다운타임이 발생하기 쉬우며, Azure AD로의 전환이 필요할 수 있습니다. 분산된 사이트를 수동으로 관리하면 효율성이 떨어지고 간접비가 증가합니다.

가장 좋은 방법은 미션 크리티컬 운영을 간소화하고 효율화하기 위해 **특별히 제작된 도구**를 활용하는 것입니다. 이러한 도구는 글로벌화를 위해 구축되었으며 다양한 인프라와 원격 위치로 원활하게 확장하여 운영 작업을 줄일 수 있습니다. 자동화, 검색 및 중앙 집중식 네트워크 가시성을 제공하여 관리를 간소화하고 유지관리를 최적화하며 시간을 단축합니다. 다운타임 없는 업그레이드를 제공하고 대규모 고가용성을 제공하여 다운타임을 줄입니다.

혁신 가속화: 분산된 시스템 대신 단일 중앙 집중식 도구 사용

대부분의 기업은 2~4개의 DNS 솔루션을 사용하므로 중요한 서비스를 관리하고 문제에 더 빠르게 대응하기가 어렵습니다. 조직과 정보의 분산으로 인해 지연과 오류가 발생하는 경우가 많습니다. 여러 클라우드 제공업체의 상이한 명명 규칙과 운영 모델로 인해 잘못된 구성과 다운타임이 발생합니다. 네트워크 전반에 걸친 가시성의 단편화는 문제 해결 및 감사에 소요되는 시간을 증가시킵니다.

조직은 혁신을 가속화하고 멀티 클라우드 확장, 인수 합병 등과 같은 비즈니스 이니셔티브를 실현할 수 있는 효율적이고 효과적인 솔루션을 찾아야 합니다. **중앙 집중식 도구**에 투자하면 자동화, 단일 DNS 명명 규칙, 온프레미스 및 클라우드 네트워크 전반의 가시성을 통해 이러한 목표를 달성할 수 있습니다. 서로 다른 시스템을 혼합하여 사용하는 대신, 중앙 집중식 도구를 사용하면 비즈니스 요구에 더 빠르게 적응하고 비효율성을 줄일 수 있습니다. 이는 정책 제어 및 일관성, 신속한 문제 해결, 향상된 협업을 제공하고, 잘못된 구성 및 오류를 제거하며, 감사 및 규정 준수 위험과 운영 비용을 절감합니다.

브랜드 무결성 보호: DNS를 활용하여 조기에 위협 탐지

멀웨어, 랜섬웨어, 유사 도메인, 데이터 유출, 피싱 등 끊임없이 진화하는 위협 환경은 브랜드 아이덴티티와 데이터 보호에 큰 위험 요소입니다. 기존 시장 솔루션은 DNS를 간과하고 공격을 선제하지 못하기 때문에 상당한 보안 갭이 존재합니다. 지난해에만 해커들은 대규모 피싱 공격에서 약 42,000개의 사칭 도메인을 사용했습니다. 또한 사일로화된 시스템, 기술 부족, 수동 관리, 상황 인식 부족으로 인해 SecOps의 비효율성과 응답 시간 지연이 발생합니다.

위협을 조기에 탐지하면 위험을 줄이고 보안 갭을 줄일 수 있습니다. 대부분의 사이버 공격이 DNS에 의존하기 때문에 **DNS 기반 위협 헌팅**을 활용하면 위협을 조기에 탐지하고 차단할 수 있습니다. DNS를 1차 방어선으로 사용하면 데이터 유출, 도메인 생성 알고리즘, 사칭 공격으로부터 모든 IoT/OT 디바이스를 보호하고 보안을 유지할 수 있습니다. 또한 조사 시간을 줄이고, 문제 해결을 자동화하며, 취약성 위험을 사전에 평가하여 SecOps 효율성을 개선합니다.

민첩하고 복원력이 높은 인프라를 위한 INFOBLOX 솔루션

가시성, 자동화 및 제어

Infoblox는 조직에 네트워크에 연결하는 사람과 사물에 대한 탁월한 가시성, 자동화 및 제어 기능을 제공합니다. Infoblox는 번거롭고 의무적인 유지보수를 제거하여 비용이 많이 드는 다운타임을 크게 줄이고, 노동 집약적인 운영 작업을 자동화하며, 네트워크 자산 재고 관리와 관련된 부담을 줄여줍니다. Infoblox 솔루션은 보안성을 염두에 두고 구축되어 상황 인식이 향상되어 잘못된 경고를 줄이고 효율성을 개선합니다. Infoblox는 다음을 제공합니다.

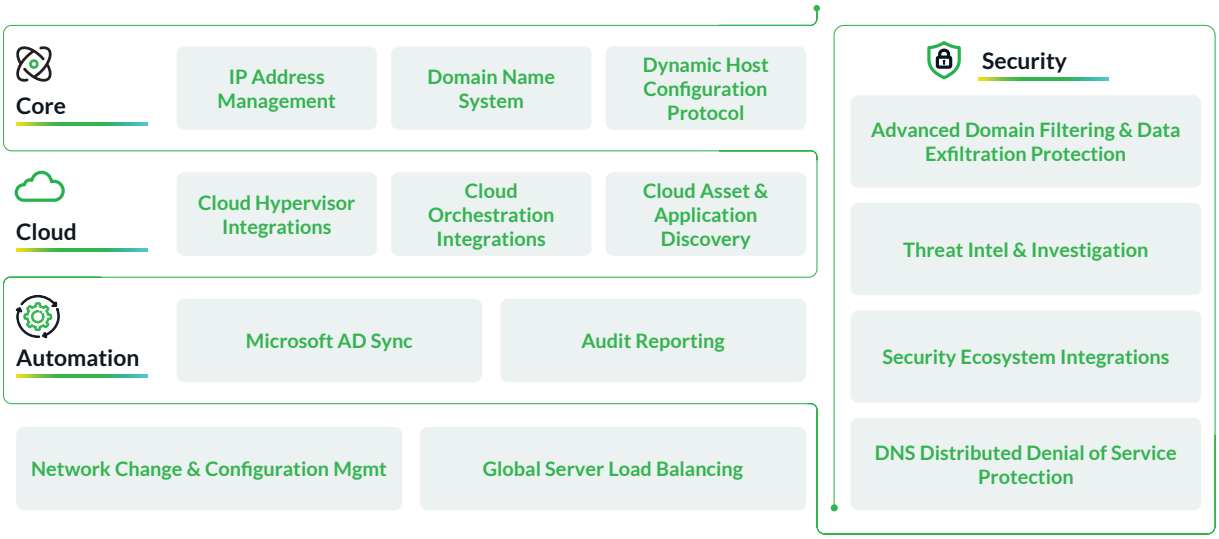

그림 1: Infoblox 솔루션

결론

현대화는 디지털 혁신을 주도합니다. 네트워크에 적합한 솔루션을 선택하면 지속적인 현대화를 추진할 수 있습니다. 중요한 네트워크 서비스를 관리하는 기존의 접근 방식은 신속한 혁신, 변화하는 비즈니스 요구 사항에 대한 적응, 경쟁력 유지에 방해가 됩니다. Infoblox가 제공하는 가시성, 자동화 및 제어 기능을 활용하여 비즈니스 성장에 필요한 속도로 네트워크를 현대화할 수 있습니다.

infoblox.

Infoblox는 네트워킹과 보안을 통합하여 비교할 수 없는 성능과 보호를 제공합니다. 포춘지 선정 100대 기업과 신생 혁신 기업에서 신뢰를 받으며, 사용자의 디바이스에 대한 실시간 가시성과 제어 기능을 제공하여 조직 내부에서 발생하는 위협을 조기에 차단할 수 있습니다.

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

+1.408.986.4000
www.infoblox.com

버전: 20230803v1