VMware NSX Data Center

비즈니스 속도에 맞게 IT가 대응할 수 있도록 지원

"기술은 놀라운 속도로 빠르게 발전하고 있으며 기회를 선점하는 조직만이 커다란 보상을 얻을 수 있습니다."

BART VAN ARK 박사
THE CONFERENCE BOARD의
총괄 부사장 겸 수석 경제학자 및 전략 책임자

VMware NSX® Data Center는 네트워킹에 대한 소프트웨어 정의 접근 방식인 가상 클라우드 네트워크를 구현하여 데이터 센터, 클라우드, 애플리케이션 프레임워크 전반으로 확장할 수 있는 네트워크 가상화 및 보안 플랫폼입니다. NSX Data Center를 사용하면 네트워킹 및 보안 기능이 가상 머신(VM)에서 컨테이너, 베어메탈까지 실행 위치에 관계없이 애플리케이션에 더 가까이 배치됩니다. 가상 머신의 운영 모델과 마찬가지로 기반 하드웨어에 관계없이 네트워크를 프로비저닝하고 관리할 수 있습니다. NSX Data Center는 소프트웨어로 전체 네트워크 모델을 재현하며 단순한 네트워크에서 복잡한 멀티 Tier 네트워크까지 어떤 네트워크 토폴로지라도 몇 초 내에 생성하고 프로비저닝할 수 있습니다. 사용자는 NSX를 통해 제공되는 서비스 또는 차세대 방화벽에서 성능 관리 솔루션에 이르는 타사 통합 기능의 광범위한 에코시스템을 통해 제공되는 서비스의 조합을 통해 요구 사항이 다양한 여러 가상 네트워크를 생성함으로써 기본적으로 더 민첩하고 안전한 환경을 구축할 수 있습니다. 그런 다음 이러한 서비스를 클라우드 내 또는 클라우드 간 다양한 Endpoint로 확장할 수 있습니다.

서로 상충되는 요구 사항으로 인한 절충

속도와 대응력, 강력한 보안, 애플리케이션의 고가용성은 모두 IT 조직이 추진해야 하는 매우 중요한 우선 과제들입니다. 오늘날의 조직은 강력한 애플리케이션 인프라가 매우 중요하며 따라서 혁신 및 성공적인 디지털 트랜스포메이션을 위한 기본 토대로서 IT의 중요성 또한 갈수록 더 커지고 있습니다. 그러나 급격한 변화와 이에 따른 IT에 대한 기대치 변경으로 인해 각 과제들의 우선 순위가 계속 바뀌면서 실제로 이러한 과제를 구현하는 과정에서 종종 절충이 필요하게 되었습니다.

IT는 각 이해관계자들의 다양한 요구 사항을 충족하는 과정에서 종종 IT 우선 과제들이 서로 상충되는 상황에 처하고 있습니다. 예를 들어 보안과 관련된 복잡하고 엄격한 규제에 따라 애플리케이션을 보호하기 위해 애플리케이션의 신속한 배포를 포기해야 하는 경우가 많습니다. 환경 전반의 애플리케이션 가용성에 대해서도 이와 유사한 문제가 종종 발생하여 IT와 다른 조직의 입장이 충돌하곤 합니다.

이러한 끊임없는 상충은 결과적으로 IT에 큰 영향을 미칩니다. 실제로 이로 인해 여러 업무 영역에서 심각한 결함이 발생하고 있습니다. 조직은 신속하게 요구 사항을 충족할 수 없으며, 데이터 센터 및 클라우드 환경 전반에 취약점이 존재하고 전반적인 대응력이 부족합니다.

인프라의 최대 잠재력 활용

대부분의 조직은 데이터 센터의 컴퓨팅 구성 요소를 이미 가상화했습니다. 또한 많은 조직이 스토리지 가상화를 결정했으며 70% 이상의 조직이 소프트웨어 정의 스토리지를 이미 도입했거나 도입할 계획입니다.

하드웨어에서 소프트웨어로의 이러한 기능 추상화를 통해 조직은 애플리케이션 구성 요소를 신속하게 프로비저닝하고 데이터 센터 간에 가상 시스템을 이동하고 주요 프로세스를 자동화할 수 있었습니다.

주요 이점

세분화된 보안 - 워크로드 수준에서 마이크로 세분화된 보안 정책을 사용하여 환경에서 보안 위협의 횡방향 확산을 방지

속도 및 대응력 - 며칠씩 걸리던 네트워크 프로비저닝 시간이 몇 초로 단축되고 자동화를 통해 운영 효율성 향상

일관된 운영 - 데이터 센터 및 퍼블릭 및 프라이빗 클라우드, 애플리케이션 프레임워크 간 물리적 네트워크 토폴로지와 독립적으로 네트워킹 및 보안 정책을 일관되게 관리

그러나 안타깝게도 이러한 여러 이점이 진화 속도가 느린 데이터 센터 구성 요소로 인해 여전히 제대로 발휘되지 못하고 있으며, 보편적인 가상화가 아직 이루어지지 않고 있는 데이터 센터 인프라의 한 요소인 네트워크에는 이러한 이점이 적용되지 않고 있습니다. 네트워킹 가상화 없이는 Software-Defined Data Center의 모든 가치를 실현할 수 없습니다.

하드웨어 기반의 네트워크 아키텍처를 보유한 조직은 가상화된 네트워킹을 배포하는 조직의 속도, 대응력, 보안을 따라잡을 수 없습니다. 조직의 상태는 네트워크의 상태에 좌우되고 있습니다.

데이터 센터 네트워킹에 대한 근본적으로 새로운 접근 방식, 즉 더 이상 속도와 보안, 그리고 보안과 대응력 간의 절충이 필요하지 않은 접근 방식이 필요합니다. IT가 이러한 절충 없이 성과를 낼 수 있도록 하려면 조직의 잠재력을 최대한 발휘하지 못하게 하는 원인인 데이터 센터 규칙을 새로 작성해야 합니다. 이제 수많은 조직이 깨달았듯이 네트워크 가상화가 바로 그 새로운 접근 방식입니다.

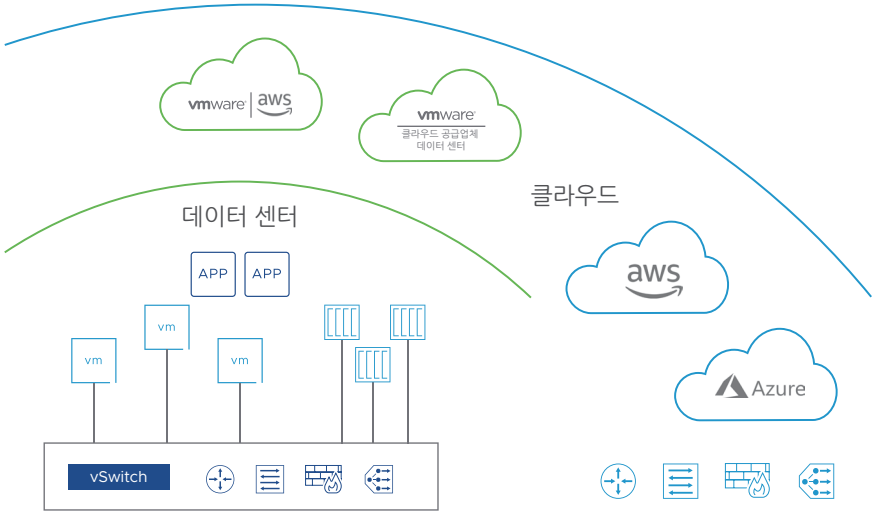

그림 1: NSX Data Center를 통한 일관된 네트워킹 및 보안

IT는 네트워크 가상화를 통해 네트워크 및 보안 서비스를 데이터 센터 가상화 계층으로 이동하여 현재 가상 머신을 실행할 때와 동일한 간편성과 속도로 전체 애플리케이션 환경을 생성, 스냅샷 생성, 저장, 이동, 삭제 및 복원할 수 있습니다. NSX Data Center는 이기종 환경 및 애플리케이션 프레임워크 전반에 걸쳐 공통 네트워킹 및 보안 정책을 확장함으로써 데이터 센터, 프라이빗 및 퍼블릭 클라우드, 기존 애플리케이션 및 컨테이너화된 새로운 클라우드 네이티브 애플리케이션에 대해 이러한 이점을 실현할 수 있도록 합니다. 그 결과 운영 및 재정적인 이유로 이전에는 불가능했던 수준의 보안과 효율성을 실현할 수 있습니다.

VMware NSX는 Software-Defined Data Center를 위한 네트워크 가상화 플랫폼이며 멀티 클라우드 환경을 확장합니다. 스위칭, 라우팅 및 방화벽과 같이 이전에는 네트워크 하드웨어에 내장되어 있었던 기능을 소프트웨어로 추상화합니다.

NSX를 통해 IT는 조직의 혁신을 이끄는 견인차 역할을 하며 다양한 이해관계자의 요청을 서로 상충되거나 상호 배타적으로 간주하지 않고 동시에 모두 수용할 수 있습니다. 이제 IT는 새로운 차원의 보안을 제공할 뿐만 아니라 비즈니스 속도에 맞게 이러한 보안을 제공할 수 있습니다.

주요 기능

분산 상태 저장 방화벽 - 하이퍼바이저 커널에 내장된 Layer 7까지의 상태 저장 방화벽 기능을 클라우드 네이티브, 기본 퍼블릭 클라우드 및 베어메탈 호스트에 바로 통합하여 전체 환경에 분산 제공

상황 인식 마이크로 세분화 - 보안 그룹 및 정책을 동적으로 생성한 후 다양한 특성 및 Layer 7 애플리케이션 정보를 기반으로 자동 업데이트하여 적응형 마이크로 세분화 정책 제공

클라우드 관리 – vRealize Suite, OpenStack 등과 기본적으로 통합되며 Terraform Provider, Ansible Module 및 PowerShell과의 통합을 완벽하게 지원

타사 통합 - 주요 타사 벤더의 에코시스템을 통해 보안 및 고급 네트워킹 서비스 개선

클라우드 네이티브 지원 - 컨테이너 네트워크 가시성을 통해 컨테이너 플랫폼, 가상 머신 및 베어메탈 호스트에 엔터프라이즈급 고급 네트워킹 및 보안 지원

NSX Intelligence™ – 새 툴 또는 에이전트 배포 없이 애플리케이션 세분화 정책을 검색, 분석 및 시행하는 데 걸리는 시간을 단축하고 인프라에 내장된 고유한 보안 기능을 통해 보안 작업 간소화

보안 내재화

NSX Data Center는 네트워크 통신에서부터 개별 워크로드의 프로세스 수준 동작에 이르기까지 애플리케이션의 구성에 대한 고유한 가시성을 활용할 수 있으며, 이는 제품이 애플리케이션의 구축 기반이 되는 하이퍼바이저 및 기타 네이티브 제어 지점에 내장되어 있기에 가능한 일입니다. 이러한 가시성을 통해 애플리케이션의 보안 태세에 따라 네트워크 보안 정책이 자동으로 생성됩니다. 따라서 IT/정보 보안 및 애플리케이션 개발 팀이 보안 검토 주기에 소비하는 시간이 줄어듭니다.

또한 여러 데이터 센터 및 하이브리드 클라우드 환경 전반에 걸쳐 보안 정책을 확장 및 시행할 수 있으며, 가상 머신, 컨테이너 및 베어메탈 서버를 기반으로 구축된 애플리케이션에 대한 범용 제어가 가능합니다. 또한 NSX Data Center는 차세대 방화벽, 침입 방지 시스템(IPS)/침입 탐지 시스템(IDS) 솔루션, 바이러스 백신 툴과 같은 타사 보안 서비스에 대한 가시성과 제어를 확장하여 효율성을 높입니다.

NSX Data Center는 애플리케이션 개발 수명주기에 대한 추가 기능 프로세스의 사후 대응 방식에서 수명주기에 통합되어 자동화된 단계의 사전 예방적인 방식으로 보안을 전환합니다. 새로 프로비저닝되는 워크로드는 보안 정책을 자동으로 상속하여 수명주기 동안 유지합니다. 더 이상 사용되지 않는 워크로드의 보안 정책에 대해 시간이 지남에 따라 증가한 정책을 줄여 관리를 간소화합니다.

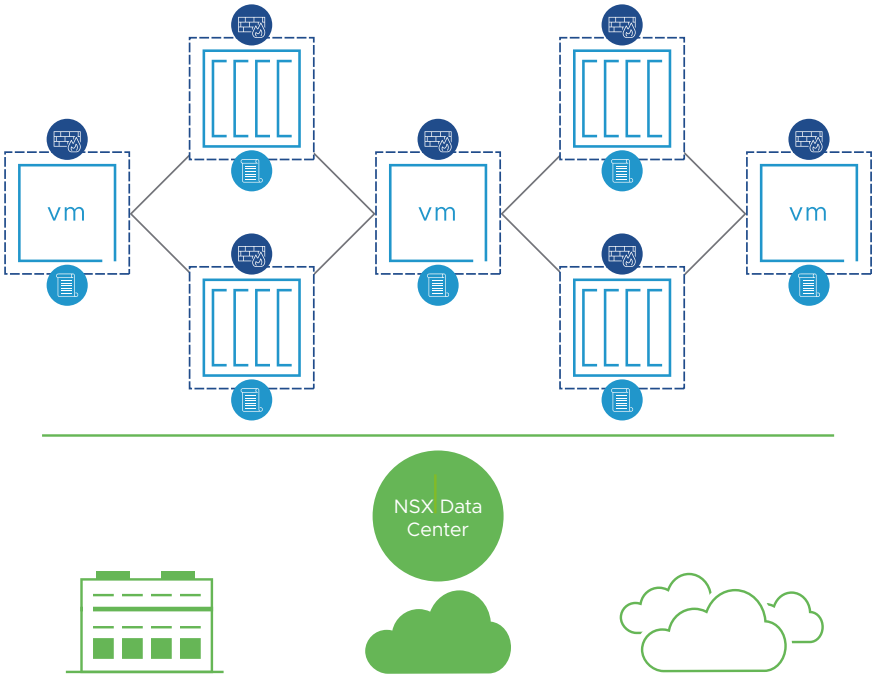

그림 2: 데이터 센터의 가장 세분화된 수준에서 보안 적용

자동화

조직이 확장되는 속도가 점점 더 가속화됨에 따라 가상화된 네트워킹과 보안을 자동화하여 서비스 및 애플리케이션을 비즈니스 속도로 생성하고 배포할 수 있습니다. 자동화를 통해 오류가 발생하기 쉬운 수동 네트워크 프로비저닝 작업을 제거함으로써 애플리케이션 배포 속도가 크게 향상됩니다.

NSX Data Center와 함께 클라우드 관리 소프트웨어(예: VMware vRealize® Automation Cloud™)를 사용하면 중앙 제어 창에서 네트워킹 및 보안 인프라와 애플리케이션의 프로비저닝과 배포, 운영, 폐기를 관리할 수 있습니다. 네트워킹 및 보안 수명주기를 프로세스에 통합함으로써 VMware는 모든 인프라 운영을 자동화하고 애플리케이션 수명주기에서 네트워킹 및 보안에 의한 병목 현상을 제거합니다.

기존(가상 머신 기반) 및 새로운(컨테이너 기반) 애플리케이션에 대해 공통 네트워킹 및 보안 정책을 확장함으로써 두 프레임워크의 네트워킹 및 보안을 자동화할 수 있습니다. 또한 온프레미스 데이터 센터, 프라이빗 클라우드 및 퍼블릭 클라우드에 대해 애플리케이션의 배포와 이동, 폐기를 자동화할 수 있습니다.

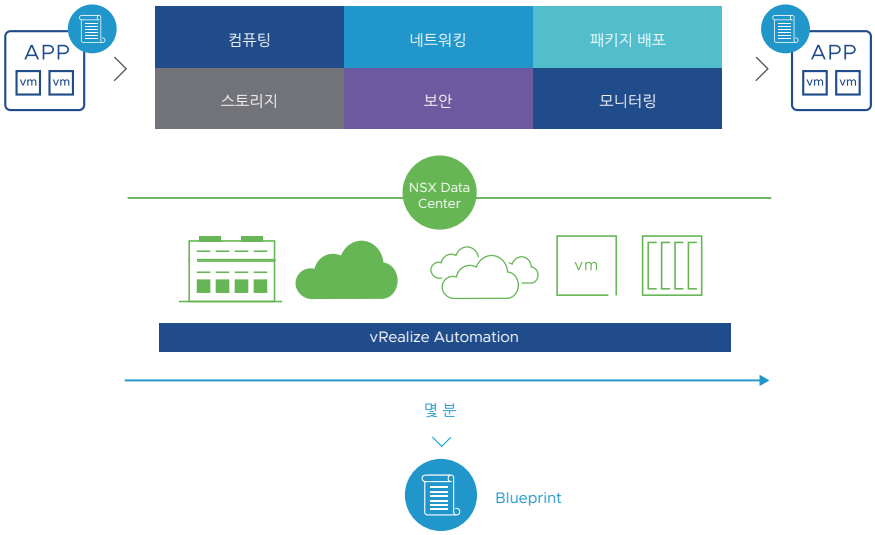

그림 3: 자동화된 네트워킹 및 보안을 통한 신속하고 반복 가능한 배포

멀티 클라우드 네트워킹

NSX Data Center 및 NSX Cloud는 사이트 전체에 걸쳐 통합된 네트워킹 및 보안 모델을 제공하므로 수동 네트워크 구성을 제거하고 네트워크 자동화를 통해 높은 운영 효율성을 달성합니다. 개별 워크로드의 수명주기 동안 네트워크 및 보안 정책이 계속 유지되므로 하이브리드 및 멀티 클라우드 환경에서 정책과 관리를 간소화합니다.

이는 또한 조직이 애플리케이션 다운타임을 발생시키지 않거나 최소화하면서 가상 머신 또는 전체 데이터 센터를 한 위치에서 다른 위치로 마이그레이션하도록 지원합니다. 그 결과 조직은 계획된 마이그레이션 및 예상치 못한 운영 중단이 발생했을 때 신속하게 복구할 수 있습니다. 이기종 환경을 포괄하는 네트워크 및 보안을 통해 조직은 다양한 물리적 데이터 센터의 리소스를 활용하여 단일 프라이빗 클라우드로 운영할 수도 있습니다. 액티브-액티브 데이터 센터를 사용하는 이러한 형태의 리소스 풀링을 멀티 데이터 센터 풀링 또는 메트로 풀링이라고 합니다.

이러한 기능들을 통해 안전하고 원활한 애플리케이션 모빌리티를 제공하여 클라우드 또는 물리적 사이트 간에 쉽게 마이그레이션할 수 있도록 합니다. NSX Data Center 및 NSX Cloud는 IT 조직이 인프라에서 사용하는 것과 동일한 가상화된 네트워크 및 보안 플랫폼을 클라우드 또는 다른 사이트로 확장하여 관리자의 개입이 적은 신속한 마이그레이션 프로세스를 제공합니다.

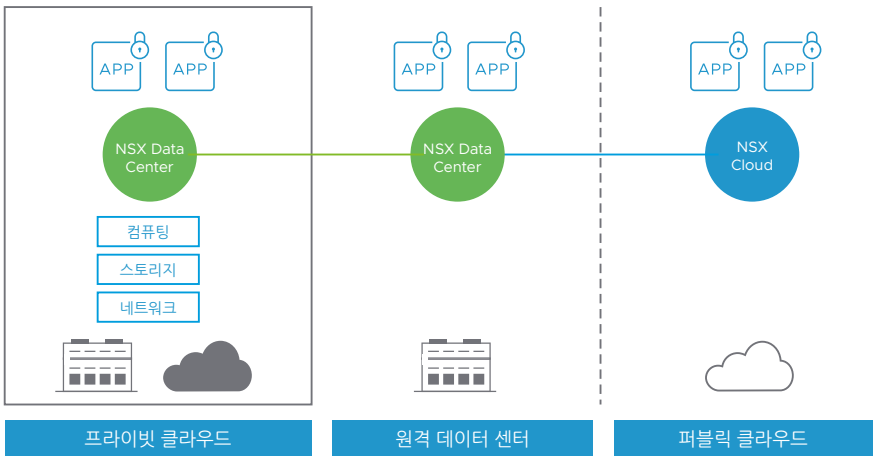

그림 4: 운영 중단으로 인한 영향을 줄이면서 사이트 및 클라우드 간 일관된 네트워킹 및 보안 제공

클라우드 네이티브

VMware NSX Data Center는 새로운 애플리케이션 플랫폼과 통합되어 완벽하게 소프트웨어로 수행되고 API 기반 인프라의 코드화 방식으로 사용 가능한 네트워킹 및 보안 기능(예: 로드 밸런싱, 방화벽, 스위칭 및 라우팅)을 제공합니다.

컨테이너 및 마이크로 서비스 아키텍처를 기반으로 하는 애플리케이션이 점차 증가함에 따라 이러한 새로운 애플리케이션을 개별 워크로드에 연결하고 보호할 수 있어야 합니다. NSX Data Center는 L3 네트워킹 기능을 포함하여 컨테이너 및 마이크로 서비스를 다른 워크로드 또는 Endpoint와 같이 1급 객체로 처리합니다. 기본적으로 컨테이너 간 네트워킹은 물론 개별 컨테이너 수준까지 마이크로 세분화를 제공하여 프로비저닝, 변경, 이동 및 폐기될 때 워크로드와 함께 유지되는 정책을 통해 마이크로 서비스에 대한 마이크로 세분화를 가능하게 합니다.

NSX Data Center는 여러 애플리케이션 및 컨테이너 조정 플랫폼, 하이퍼바이저 및 퍼블릭 클라우드 환경과 통합됩니다. 또한 다양한 애플리케이션 플랫폼을 통합하여 새로운 애플리케이션 개발 시 고유의 민첩한 네트워킹 및 보안을 제공합니다.

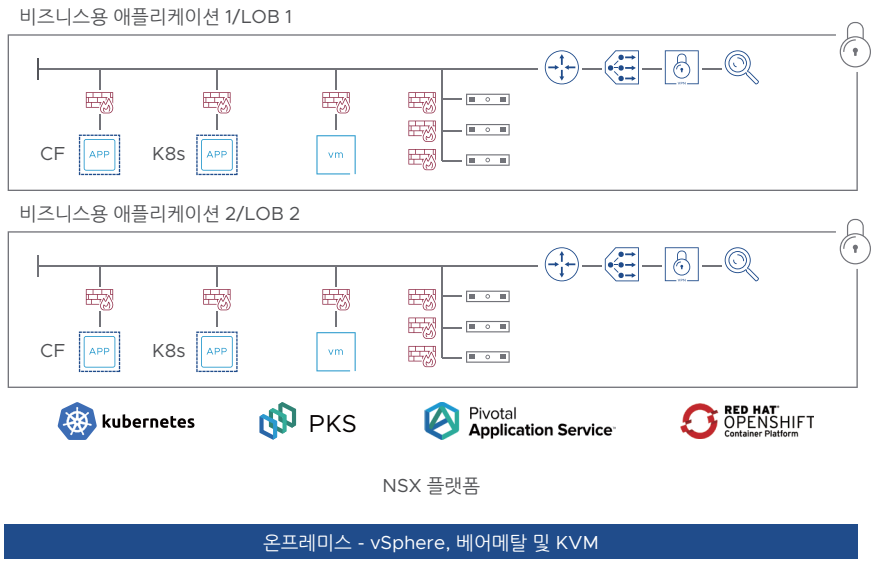

그림 5: 애플리케이션 프레임워크, 플랫폼, 사이트 및 클라우드 전반에 걸쳐 컨테이너화된 워크로드에 고급 네트워킹 및 보안 제공

자세한 정보
자세한 내용은 *https://vmware.com/kr/products/nsx.html*을 참조하십시오.

VMware NSX Intelligence

NSX Intelligence NSX Data Center 내에 기본적으로 내장된 분산 분석 엔진입니다. 이를 통해 NSX Service-Defined Firewall을 사용하여 마이크로 세분화 운영 프로세스를 획기적으로 간소화하고, 자동화할 수 있는 지속적인 데이터 센터 가시성을 확보할 수 있습니다. 이는 모든 가상 머신의 인벤토리를 구성하고, 모든 트래픽 흐름을 기록하고, 상세한 애플리케이션 종속성 맵을 시각화하는 것에서 시작됩니다. NSX Intelligence는 vRealize Network Insight™와의 긴밀한 통합을 통해 그룹화를 강화하고 모든 기존 인벤토리 메타데이터, 구성 관리 데이터베이스(CMDB) 태그 또는 애플리케이션 모델을 수집합니다.

정책을 만드는 것은 간단합니다. 시스템은 방화벽에 대한 애플리케이션 그룹 및 세분화 정책을 자동으로 권장합니다. NSX Intelligence UI는 NSX Manager™에 포함되어 있어 정책에 대해 반복할 수 있는 원활한 워크플로우를 제공합니다. 변경 사항은 토폴로지 맵에 즉시 반영되므로 즉각적인 시각적 피드백을 제공하고 새 정책을 신속하게 확인할 수 있습니다.

오늘날의 비즈니스 가치 가속화 및 미래를 위한 기반 구축

NSX Data Center를 구축한 조직은 NSX Data Center가 IT 조직의 성공을 좌우하며 데이터 센터 인프라 및 멀티 클라우드 전략의 기본 요소로 빠르게 자리잡고 있다는 점을 확인했습니다. 현재, 수많은 NSX Data Center 고객이 조직의 가치 실현 기간을 단축하며 기존 하드웨어 기반 네트워크로는 불가능한 방식으로 가장 중요하고 민감한 애플리케이션의 일부를 빠르고 민첩하며 안전한 가상 네트워크에서 제공하고 있습니다.

이러한 네트워킹 및 보안의 혁신을 통해 NSX Data Center 고객은 상당한 이점을 즉시 실현할 수 있었으며, 이전에 업무의 대부분을 차지했던 시간이 많이 걸리고 번거로운 작업으로부터 해방되었습니다. 그 결과 이들 조직은 조직의 미래 및 IT가 이러한 비전을 지원하는 데 필요한 기능을 계획함에 있어 더욱 발전된 조직의 전략을 고려할 수 있게 되었습니다.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
서울시 강남구 영동대로 517 아셈타워 13층 (우) 06164 e-메일: vmware_kr@vmware.com

Item No: 332553aq-so-launch-nsx-t-2-5-A4 8/19