VMware NSX for Horizon

요약 정보

VMware NSX™ for Horizon®은 빠르고 간편한 VDI 네트워킹을 제공합니다. IT 관리자가 시간이 많이 소요되는 네트워크 프로비저닝 없이 몇 초 만에 동적으로 가상 데스크톱에 적용되는 정책을 설정할 수 있습니다. 데이터 센터에서 데스크톱과 애플리케이션으로 보안 정책을 확장하는 이 연합 솔루션은 또한 업계 최고의 보안 솔루션을 통합할 수 있는 확장 가능한 플랫폼을 제공합니다.

이점

- 데이터 센터에서 다른 워크로드와 함께 관리되는 가상 데스크톱의 보안 향상
- 논리적 그룹화, 역할 또는 태그를 바탕으로 사용자에 대한 네트워킹 및 보안 정책의 관리를 간소화하고 가속화
- 기반 인프라에 관계없이 가상 머신에 따라 데스크톱이 생성되는 즉시 자동으로 정책 적용
- 바이러스 백신, 맬웨어, 침입 방지 및 차세대 보안 서비스를 위한 업계 최고의 솔루션 통합

가상 데스크톱 및 애플리케이션을 위한 네트워킹 및 보안: 빠르고 간편하며 확장 가능

많은 기업이 데스크톱 및 애플리케이션 가상화를 구현하여 클라이언트 컴퓨팅 보안을 개선하고 더 높은 수준의 엔터프라이즈 이동성을 제공하고 있습니다. 데스크톱 및 애플리케이션을 중앙 집중화하여 사용하지 않는 데이터를 보호하고 무단 애플리케이션 액세스를 방지하며 더욱 효율적인 방식으로 이미지의 패치 적용, 유지 관리 및 업그레이드를 제공합니다.

그러나 데스크톱 및 애플리케이션 가상화로 데이터 센터 방화벽 내부에 수백 또는 수천 대의 데스크톱이 배치됨에 따라 새로운 보안 문제를 야기할 수 있습니다. 이러한 데스크톱은 다른 사용자 및 미션 크리티컬 워크로드와 인접해 있으므로 맬웨어 및 기타 공격으로 인한 위험도 크게 증가합니다. 데스크톱에서 서버로 공격이 확산될 수 있으므로 데이터 센터 내 공격 면적이 더 넓어지게 됩니다. 이 "횡방향" 공격 시나리오는 오늘날 수많은 고객, 특히 엄격한 보안 및 규정 준수 의무가 있는 고객에게 영향을 미치고 있는 일반적인 공격 방법입니다.

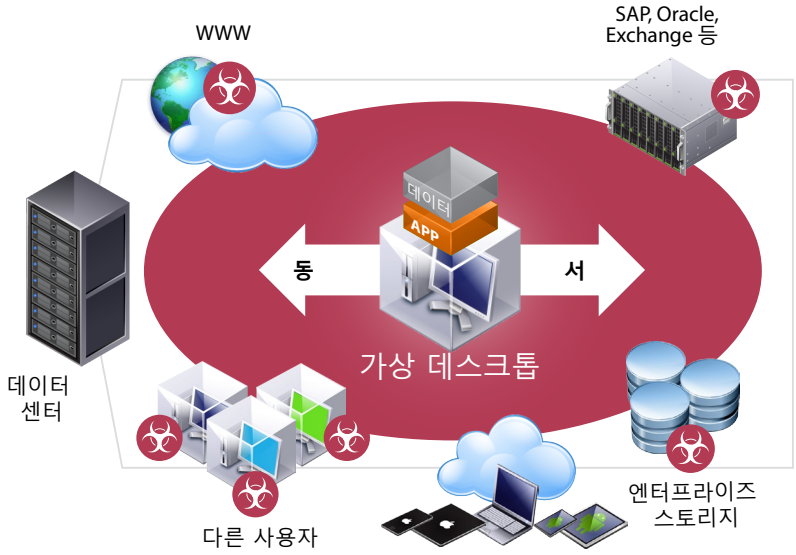

그림 1: 데이터 센터 내 횡방향 보안 문제

사용자와 워크로드 중심의 네트워킹 및 보안 정책을 관리하려는 조직은 또한 기본적으로 하드웨어 중심 아키텍처에 많은 투자가 필요하므로 자본 비용이 많이 소요되며 운영이 복잡하고 동적 비즈니스 환경에 맞게 빠르게 적응할 수 없습니다.

VMware NSX for Horizon

VMware NSX for Horizon은 효율적으로 데이터 센터 내 횡방향 트래픽을 보호하는 동시에 IT에서 빠르고 간편하게 네트워킹 및 보안 정책을 관리할 수 있도록 보장합니다. 이러한 정책은 인프라, 기기 및 위치에 관계없이 최종 사용자의 가상 데스크톱과 애플리케이션에 동적으로 적용됩니다.

그림 2: NSX for Horizon은 빠르고 간편하며 확장 가능한 VDI 네트워킹 및 보안 제공

이 솔루션은 기업에 빠르고 간편한 VDI 네트워킹과 보안을 제공합니다. IT 관리자가 시간이 많이 소요되는 네트워크 프로비저닝 없이 몇 초 만에 동적으로 가상 데스크톱에 적용되는 정책을 설정할 수 있습니다.

데이터 센터에서 데스크톱 및 애플리케이션으로 보안 정책을 확장하는 이 솔루션은 또한 업계 최고의 보안 파트너사로 구성된 VMware 에코시스템과 통합할 수 있는 확장 가능한 플랫폼을 제공하므로 고객이 전체 데스크톱을 보호하기 위한 우수한 방어막을 구현할 수 있습니다.

작동 방식

VMware NSX for Horizon은 관리자가 정책을 중앙 집중식으로 정의할 수 있어 데스크톱 가상화 보안을 개선하고 횡방향 공격을 방지할 수 있습니다. 또한 이 정책을 모든 vSphere 호스트 내 하이퍼바이저 계층에 배포하여 각 가상 데스크톱이 생성되는 즉시 자동으로 해당 데스크톱에 적용합니다. 가상 데스크톱 및 데이터 센터 내 인접 워크로드를 보호하기 위해 VMware NSX는 "마이크로 세분화"를 구현하여 각 데스크톱에 자체 경계 방어 수단을 제공합니다. 이 "완제품으로 패키지화된 보안"은 VMware NSX 분산 가상 방화벽 기능을 사용하여 각 가상 머신의 송수신 트래픽을 추적하고 데스크톱과 인접 워크로드 간 무단 액세스를 차단합니다. 한 호스트에서 다른 호스트 또는 다른 데이터 센터로 가상 데스크톱이 이동해도 자동으로 해당 정책이 계속 적용됩니다.

특징 및 이점

VMware NSX for Horizon으로 빠르고 간편하게 VDI 네트워킹에서 인프라와 기기, 위치에 관계없이 동적으로 최종 사용자에게 보안 정책을 적용할 수 있습니다.

빠르고 간편한 VDI 네트워킹

관리자는 VMware NSX for Horizon을 사용하여 몇 번의 클릭만으로 간편하게 모든 가상 데스크톱에 대해 보안 정책을 생성, 변경 및 관리할 수 있습니다. 신속하게 사용자 그룹에 보안 정책을 매핑하여 가상 데스크톱의 온보딩 기간을 단축할 수 있습니다. 관리자는 가상화된 네트워크 기능을 구축할 수 있는 기능(스위칭, 라우팅, 방화벽, 로드 밸런싱 등)을 사용하여 복잡한 VLAN, ACL 또는 하드웨어 구성을 수행할 필요 없이 VDI용 가상 네트워크를 구축할 수 있습니다.

최종 사용자와 데스크톱에 동적으로 적용되는 자동화된 정책

관리자는 기반 네트워크 인프라에 관계없이 역할, 논리적 그룹화, 데스크톱 운영 체제 등을 바탕으로 사용자에게 매핑되는 네트워크 보안 서비스를 사용하여 최종 사용자의 컴퓨팅 환경에 맞게 동적으로 적응하는 정책을 설정할 수 있습니다. 중앙 집중식으로 관리되는 이 정책은 각 데스크톱이 생성되는 즉시 데스크톱 가상 머신에 자동으로 적용되므로 기업은 데이터 센터 간 영구적으로 가상 데스크톱에 적용되는 보안을 믿고 안심하고 확장할 수 있습니다.

고급 보안을 위한 플랫폼

VMware NSX는 이미 구축되어 있는 보안 파트너사의 에코시스템에서 제공하는 동급 최고의 기능을 통합할 수 있는 확장 가능한 플랫폼을 제공합니다. 서비스를 동적으로 추가하여 데이터 센터에서 데스크톱과 애플리케이션으로 가상 데스크톱 보안을 확장할 수 있습니다. 이 에코시스템에는 Trend Micro, Intel Security, Palo Alto Networks 등의 파트너사가 포함되며, 바이러스 백신, 맬웨어, 침입 방지 및 차세대 보안 서비스를 사용하여 운영 체제, 브라우저, e-메일 등을 보호하는 솔루션을 제공합니다.

자세한 정보

VMware의 웹 사이트와 트위터에서 Horizon 및 VMware NSX에 대한 자세한 내용을 참조하십시오.

VMware Horizon 참고 자료

웹: http://www.vmware.com/kr/products/horizon-view

블로그: http://blogs.vmware.com/euc/

트위터: @VMwareHorizon

VMware NSX 참고 자료

웹: http://www.vmware.com/kr/products/nsx/

블로그: http://blogs.vmware.com/networkvirtualization/

트위터: @VMwareNSX

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, 13층(삼성동, 아셈타워) (우) 135-798 전화: (02) 3016-6500 e-메일: vmware_kr@vmware.com
Copyright © 2015 VMware, Inc. All rights reserved. 이 제품은 미국 및 국제 저작권과 지적 재산권에 관한 법률의 보호를 받습니다. VMware 제품은 여러 건의 특허 보호 대상이며 일부는 특허 출원 중입니다. 자세한 내용은 웹 사이트(http://www.vmware.com/kr/support/patents)를 참조하시기 바랍니다. VMware는 미국 및/또는 기타 관할 지역에서 VMware, Inc.의 등록 상표 또는 상표입니다. 이 문서에 언급된 기타 명칭과 표시는 모두 해당 소유권자의 상표입니다. Item No: VMW-SB-NSXNETWKSECUR-A4-20150401-WEB