VMware Workspace ONE Trust Network

변화하는 디지털 워크스페이스를 위한 보안

요약 정보

VMware Workspace ONE™ Trust Network™는 직원, 애플리케이션, Endpoint, 네트워크를 보호하기 위해 포괄적이고 최적화된 엔터프라이즈 보안 접근 방식을 제공합니다. 최신 위협을 차단, 감지, 해결하는 기능을 갖춘 Workspace ONE Trust Network는 파트너 솔루션이 통합된 풍부한 에코시스템을 통해 인텔리전스 기반 Workspace ONE 플랫폼에 내재된 보안 기능을 강화하여 디지털 워크스페이스 전반에서 리스크를 지속적으로 모니터링하고 리스크 완화를 위해 신속하게 대응합니다.

주요 이점

Workspace ONE Trust Network는 신뢰의 프레임워크와 인증을 통해 보안과 관리를 간소화합니다. Workspace ONE Trust Network는 IT에 다음과 같은 이점을 제공합니다.

- 통합 뷰를 제공하는 행동 기반 프레임워크를 통해 보안 솔루션 사일로 제거 및 디지털 워크스페이스 전반의 복잡성 감소
- 액세스, 기기, 애플리케이션의 보안 및 관리를 통찰력 및 자동화와 고유하게 통합하여 엔드유저컴퓨팅 에코시스템 전반의 리스크 완화
- 신뢰하는 개방형 파트너 에코시스템 활용 및 지속적인 기존 투자 활용을 통해 비용 절감

보안 – 오늘날의 디지털 워크스페이스 전략에 대한 가장 큰 장애물

디지털 워크스페이스는 직원 생산성을 5배[1] 향상시켜 직원들이 원하는 기기에서 애플리케이션 및 데이터에 간편하고 안전하게 액세스하도록 지원할 수 있습니다. 기업이 디지털 트랜스포메이션으로 전환함에 따라, 직원, 애플리케이션, Endpoint 및 네트워크로 구성된 디지털 워크스페이스 에코시스템은 BYOD 도입 및 IT 소비자화와 같은 일반적 추세에 따라 기존 경계를 초월하여 성장 및 발전하고 있습니다. 또한 기존 경계가 사라짐에 따라 제로데이 공격, 중간자(MiTM) 공격, 피싱, 봇, 랜섬웨어 같은 발전된 형태의 사이버 공격이 등장하고 있습니다.

모빌리티 및 디지털 워크스페이스 투자[2]의 최우선 과제가 보안임에도 불구하고, 기존의 보안 툴은 레거시 기능을 제공하는 보안 사일로에만 주력하여 IT에 제한된 가시성을 제공합니다. 이러한 임시 방편의 접근 방식은 복잡성으로 인한 높은 비용과 수작업을 요구하여 디지털 워크스페이스를 보호하기 어렵게 만듭니다. 결과적으로 보안은 오늘날의 디지털 워크스페이스 전략을 구현함에 있어 가장 큰 장애물이 되었습니다.

경계 없는 기업에 포괄적이며 예측 방식의 보안 제공

사용자 환경에 영향을 주지 않으면서 보안 요구 사항을 충족하려면 다음과 같은 새로운 요구 사항을 충족해야 합니다.

1. 기업에서는 프레임워크를 사용하여 에코시스템을 보호하는 구성 요소 간에 신뢰를 구축하여 통합된 뷰를 확보해야 합니다.
2. 기업은 환경으로부터 통찰력을 얻어 예측 방식의 자동화된 의사 결정을 내려 디지털 워크스페이스를 보호하고 리스크를 지속적으로 완화해야 합니다.

Workspace ONE Trust Network는 직원, 애플리케이션, Endpoint, 네트워크를 보호하기 위해 포괄적이고 최적화된 엔터프라이즈 보안 접근 방식을 제공합니다. Workspace ONE Trust Network는 신뢰의 프레임워크와 인증을 기반으로 하여 변화하는 디지털 워크스페이스 전반에서 위협을 차단, 감지, 해결하는 기능을 제공합니다. 디지털 워크스페이스 전반에서 신뢰가 구축된 경우 상호 연결된 최소 권한 시스템을 통해 직원의 보안을 상시 유지할 수 있습니다. 최신 사이버 위협과 관련된 리스크를 관리하기 위해 Workspace ONE Trust Network는 인텔리전스 기반 Workspace ONE 플랫폼의 통찰력을 신뢰할 수 있는 보안 파트너 솔루션과 통합하여 디지털 워크스페이스에서 예측 방식의 자동화된 보안을 제공합니다.

---

1 출처: https://www.vmware.com/radius/impact-digital-workforce/

2 2017년 12월 CCS Insights Mobile Technology Buyer Survey

차단, 감지 및 해결

중요한 것은 기업에 사이버 공격이 발생하는지 여부가 아니라 언제 발생하느냐입니다. 이를 예측할 수 있는 IT 운영 및 보안 팀에서는 NIST 사이버 보안 프레임워크와 같은 프레임워크를 사용하여 보안 기능을 Workspace ONE Trust Network에서 제공하는 기능에 간단하게 매핑하여 사이버 보안 리스크를 관리할 수 있습니다.

- 보안 기능은 머신 러닝을 사용하여 맬웨어를 방지하고, 기업의 클라우드 기반 애플리케이션에서 데이터 외부 유출을 방지하며, 네트워크를 마이크로 세분화하여 발전된 형태의 지속적 위협(APT)을 차단하는 등의 방식으로 디지털 워크스페이스를 보호하는 데서부터 시작됩니다.
- 디지털 워크스페이스에 위협이 발생하면 지속적인 적응형 모니터링을 통해 이를 감지할 수 있으므로 IT 운영 및 보안 팀에서는 모바일 및 데스크톱 Endpoint와 애플리케이션에 대한 위협을 알아낼 수 있습니다.
- 위협이 감지된 후 Workspace ONE Trust Network는 강력한 의사결정 엔진을 활용하여 문제 해결을 자동화할 수 있습니다. 비정상적인 동작에 근거하여 공격이 감지되면 기업 데이터에 대한 액세스를 차단하는 자동화된 정책을 시작할 수 있습니다.

액세스, 기기, 애플리케이션 보안 및 관리와 분석의 통합

Workspace ONE Trust Network는 액세스, 기기, 애플리케이션 보안 및 관리 등 인텔리전스 기반 Workspace ONE 플랫폼에 내재된 보안 기능을 분석과 통합하여 관리 보안 솔루션의 사일로를 고유하게 연결합니다. Workspace ONE 인텔리전스 서비스는 Workspace ONE 플랫폼에서 분석을 제공할 뿐만 아니라 워크스페이스 데이터를 집계하고 상관관계를 분석하며 권장 사항을 제안하여 통합형 통찰력과 자동화 기능을 제공합니다. 기업에서는 Workspace ONE Trust Network 기능을 인텔리전스 서비스와 통합하여 오늘날의 경계 없는 환경에서 보안 리스크를 지속적으로 모니터링하고 리스크 완화를 위해 신속하게 대응할 수 있습니다.

의사결정 엔진은 사용자 행동을 기반으로 네트워크 외부의 기업 데이터와 같은 정보의 상관관계를 분석하여 위협을 감지하고 액세스 정책을 통해 문제 해결을 자동화할 수 있습니다. 위협 데이터 및 세분화된 기기 규정 준수 상태에 대한 통합형 통찰력은 보안 문제를 실시간으로 파악하고 완화하여 디지털 워크스페이스에 대한 보안 검역을 강화할 수 있는 간편한 방법을 제공합니다. 의사결정 엔진을 통해 IT는 중요한 패치를 적용하여 취약한 Windows 10 Endpoint 문제 해결, 그룹 또는 개인 수준에서 애플리케이션 및 서비스에 대한 조건부 액세스 제어 설정과 같은 일반적인 작업을 자동화하고 최적화하는 규칙을 생성할 수 있습니다.

신뢰하는 파트너 솔루션으로 구성된 풍부한 에코시스템 활용

디지털 워크스페이스 전반에서 포괄적인 보안을 구현하기 위해서는 성장하고 변화하는 디지털 워크스페이스를 보호하는 구성 요소 간에 신뢰를 구축해야 합니다. Workspace ONE Trust Network는 Workspace ONE 플랫폼에 구축된 API를 활용하여 신뢰의 프레임워크를 제공합니다. 이러한 API를 활용하면 보안 솔루션으로 구성된 풍부한 에코시스템에서 Workspace ONE과 통신하고 궁극적으로 시스템 관리자가 원하는 통합 뷰를 제공하여 보안 및 관리를 간소화할 수 있습니다. 보안 솔루션 사일로를 연결하여 고객은 기존 투자를 활용해 지속적인 모니터링 및 리스크 분석을 크게 개선하여 더 빠른 응답 시간을 제공할 수 있습니다. 따라서 추세와 패턴을 기반으로 구축에 맞게 확장 가능한 예측 방식의 보안 전략을 실현할 수 있습니다.

자세한 정보

Workspace ONE Trust Network에 대한 자세한 정보: www.vmware.com/kr/products/workspace-one/security

무료 Hands-On Lab 체험해 보기: https://www.vmware.com/go/workspace-hol

VMware 제품에 대한 자세한 내용 또는 구입 방법

문의

vmware_kr@vmware.com

웹 사이트 방문

http://www.vmware.com/kr/products를 방문하거나 온라인으로 해당 지역의 공인 파트너사를 검색하십시오.

주요 기능

기업에서는 Workspace ONE Trust Network가 변화하는 사이버 위협 환경을 차단, 감지, 해결하기 위해 제공하는 중요한 보안 기능을 활용할 수 있습니다.

기능	설명
보안 솔루션을 연결하는 기본적인 디지털 워크스페이스 플랫폼	API를 활용하여 개방형 보안 에코시스템과 Workspace ONE 간에 통신하는 신뢰의 프레임워크를 통해 보안과 관리를 간소화합니다.
액세스 관리를 통해 비즈니스 간소화	IT가 모든 애플리케이션에 대해 애플리케이션 프로비저닝, 셀프 서비스 카탈로그, 다단계 인증 및 싱글 사인온(SSO)을 제공하도록 지원합니다.
상황별 정책을 통해 사용자 환경 및 보안 최적화	기기 규정 준수 상태, 사용자 인증 강도, 데이터 민감도, 사용자 위치 등을 기반으로 하는 조건부 액세스 정책을 통해 인증을 제어합니다.
DLP(데이터 손실 방지) 정책으로 정보 유출 방지	기기 수준의 암호화, 데이터 암호화, 하드웨어 보안 정책을 활성화합니다. 애플리케이션 블랙리스트, 기기 페어링, Wi-Fi 보안, TLS 시행 등의 정책을 구성합니다. 맬웨어, 위협, 악성 애플리케이션, 인메모리 공격 또는 탈옥 기기를 모니터링하고 원격 잠금, 기기 지우기, 액세스 차단 또는 맞춤형 기기 격리 제어를 사용하여 자동으로 문제를 해결합니다.
사용자 경험을 저하시키지 않으면서 애플리케이션 보호	VMware Boxer™, Browser™, Content Locker™와 같은 VMware의 안전한 생산성 애플리케이션을 통해 보안 제어를 활용합니다. 기타 모든 애플리케이션과 클라우드 서비스에 대해 위협을 감지하고 문제 해결을 자동화합니다.
미사용 데이터 및 전송 중인 데이터 암호화	VMware Tunnel을 통해 기기의 애플리케이션에서 데이터 센터로 이동하는 트래픽을 인증하고 암호화합니다. AES 256비트 암호화를 통해 미사용 및 전송 중인 애플리케이션 데이터를 보호합니다.
마이크로 세분화를 통한 네트워크 전반의 보안 자동화	VMware NSX®에서 제공하는 마이크로 세분화 기능을 사용하여 데이터 센터의 공격 면적을 최소화하고 네트워크 전반에서 보안을 자동화합니다.
통합형 통찰력 및 자동화를 통해 예측 방식의 보안 제공	Workspace ONE 인텔리전스에서 제공하는 위협 데이터 및 세분화된 기기 규정 준수 상태에 대한 통합형 통찰력을 통해 보안 문제를 실시간으로 파악하고 완화합니다.

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: 130019wf-vmw-fy19q1 euc launch-trust network-ds-a4-106 3/18