백서 – **2018년 3월**

디지털 워크스페이스 전반의 포괄적인 보안 접근 방식

vmware®

목차

직원들이 원하는 애플리케이션을 언제 어디서나 모든 기기에서 바로 액세스할 수 있도록 하여 직원들의 역량을 강화하는 기업에서는 개인 및 조직 수준에서 측정 가능한 의사결정, 생산성 및 효율성 개선을 통해 다양한 이점을 누릴 수 있습니다.[1]

소개

기존 워크스페이스에 비해 디지털 워크스페이스를 이용하는 직원들의 생산성이 더 높고 기업에서도 더 높은 성과를 달성할 수 있다고 새롭게 확인된 비즈니스 이점으로 인해 모든 기기에 애플리케이션을 안전하게 제공하면서 유사한 수준의 이점을 달성하는 방법에 대한 기업의 관심이 높아졌습니다. 기업에서는 기존의 업무 경계가 사라져도 보안을 저하시키지 않으면서 Forbes Insights의 *디지털 인력의 영향(Impact of the Digital Workforce)* 연구에서 언급한 이점을 달성할 수 있기를 원합니다.

사라지는 업무 경계에 직면하는 기업

전 세계의 IT 팀은 점점 증가하고 심각해지는 보안 위협과 씨름하고 있습니다. 많은 경우 맬웨어 침투로 인한 운영 중단의 결과로 커다란 비용이 발생했습니다. 예를 들어, 수백만 명을 공략하기 위해 Microsoft Windows의 취약점을 활용한 WannaCry 사이버 공격은 랜섬웨어 수수료를 요구하며 150여 국가에 있는 컴퓨터를 볼모로 잡았습니다. 미국에서는 데이터 침해 사고 건수가 2017년에 최고치를 경신했습니다.[2]

오늘날 조직의 경계와 업무의 경계가 확장됨에 따라 사이버 범죄 기회가 늘어나고 있습니다. 제로데이 공격과 중간자(MITM) 공격이 좋은 예입니다. 제로데이 공격은 개발자가 버그에 대해 처음 알게 된 날에 또는 그 이전에 악용이 발생한 데서 그 이름이 유래했으며, 중간자(MITM) 공격은 공격자가 공개 키 메시지 교환에 개입하여 적극적으로 엿들은 후 요청된 키를 본인의 키로 바꾸어 메시지를 재전송하는 도청의 형태를 취합니다. 이를 통해 실제로 쌍방이 인지하지 못한 상태에서 두 사용자 간의 통신을 장악하고 모니터링하고 변조할 수 있습니다.[3] 심지어 한발 앞서 대응하기 위해 최선을 다하고 있는 기업들도 소셜 엔지니어링 및 프로그래밍 전문 지식, 봇 및 랜섬웨어 공격을 이용한 발전된 형태의 피싱 기법에 빈번하게 노출됩니다.

위협 퇴치 및 엔터프라이즈 데이터 보호

인텔리전스 기반 플랫폼을 통해 위협을 차단, 감지, 해결하여 변화하는 디지털 워크스페이스를 보호하기 위한 더 나은 접근 방법이 필요합니다. 이러한 방법을 사용하면 기존의 경계를 넘어 동적인 사이버 위협이 확산되고 새로운 취약점을 공략하도록 진화하는 상황에 맞게 디지털 워크스페이스 전략이 확장되고 발전하므로 기업에서 중요 데이터를 보다 효과적으로 보호할 수 있습니다.

본 백서에서는 오늘날의 경계 없는 환경에서 포괄적이며 예측 방식의 새로운 보안 접근 방식에 대해 설명합니다. 또한 변화하는 디지털 워크스페이스 보호의 중요성과 기업이 에코시스템의 구성 요소 간에 신뢰의 프레임워크를 도입해야 할 필요성에 대해 강조합니다. 뿐만 아니라 IT 조직에서 수집된 자료를 통해 통찰력을 확보하고 이를 바탕으로 위협을 차단하고 공격 확산을 방지하는 것과 관련된 올바른 결정을 내리는 데 필요한 8가지의 핵심적인 차단, 감지, 해결 기능에 대해서도 소개합니다.

---

1 Forbes Insights. "The High-Performance Digital Culture: Empowerment, Trust, and the New Equilibrium Between the Employee and IT", 2017년 10월

2 Identity Theft Resource Center. "2017 Annual Data Breach Year-End Review."

3 Technopedia. "Zero-Day Threat", 2018년

"2018년 모빌리티 및 디지털 워크스페이스 투자의 최우선 과제는 보안입니다."

– CCS INSIGHTS

보안 – 오늘날의 디지털 워크스페이스 전략에 대한 가장 큰 장애물

오늘날에는 어디서나 업무를 수행할 수 있습니다. 직원들은 사무실뿐만 아니라 집, 카페, 심지어 멀리 떨어진 곳에서도 다양한 네트워크를 통해 수많은 개인 및 기업 Endpoint에서 정보와 애플리케이션에 액세스할 수 있습니다. IT 팀은 언제 어디서나 원하는 기기를 사용하여 업무를 수행하고자 하는 직원들의 요구 사항을 인지하여 중요한 기업 데이터를 보호하면서 직원이 원하는 바를 수용하기 위해 바쁘게 움직이고 있습니다.

그러나 기존의 보안 솔루션으로는 이러한 요구 사항을 충족하기가 어렵습니다. IT 팀은 대충 짜집기된 복잡한 레거시 보안 기술을 통해 빠르게 변화하는 최종 사용자의 요구 사항을 충족하려고 시도하고 있습니다. 이 가운데 일부 기술은 보호를 의도하지 않은 대상까지 안전하게 보호하기 위해 구축됩니다. 시간이 지나면서 IT 팀에서 다양한 솔루션을 확보하게 됨에 따라 많은 기술이 서로 통신하지 못하게 되므로 잠재적인 공격 가능성이 늘어납니다. 기업의 성공을 위해서는 직원 만족도가 중요하지만 IT 책임자는 2018년 모빌리티 및 디지털 워크스페이스 투자의 최우선 과제가 보안이라고 보고합니다.[4]

최근 CCS Insights에서 실시한 설문조사에서 거의 절반(47%) 가량의 IT 구매자가 향후 12개월 동안 디지털 워크스페이스를 위해 가장 우선시하고 있는 투자 영역이 네트워크 보안이라고 답했고 그 다음으로 42%가 서비스 보안, 27%가 애플리케이션 보안이라고 답했습니다. 이러한 투자를 통해 워크로드 이동 시 데이터와 애플리케이션을 더 안전하게 보호할 수 있습니다. 그러나 보안 솔루션의 사일로는 복잡성을 증가시키고 오류를 발생시킬 여지를 남깁니다. 예를 들어, 네트워크 방화벽 기능으로 한 시스템에 대한 침입 시도를 저지하기는 했지만, 이로 인해 여러 시스템에서 횡방향 트래픽이 감염되고 있었다는 사실을 수개월 동안 인지하지 못했다면 기업에 큰 피해가 발생할 수 있습니다. 신뢰의 프레임워크를 기반으로 보안 솔루션의 사일로를 연결하는 접근 방식을 이용하면 보안 차단, 감지, 해결이 지속적으로 수행되므로 IT는 우선 순위를 지정할 필요가 없습니다.

기업에서는 직원들의 디지털 워크스페이스에 대해 보안을 최신 상태로 유지하는 접근 방식을 통해 시스템과 데이터를 공략하며 끊임없이 발전하는 사이버 위협에 보다 효과적으로 대응할 수 있습니다. 이 모델에서는 직원, 애플리케이션, Endpoint, 네트워크 등 엔드유저컴퓨팅 에코시스템을 보호하는 구성 요소 간에 신뢰를 구축하여 인증을 기반으로 승인된 액세스만 허용해야 합니다.
포괄적이고 통합된 신뢰의 프레임워크를 통해 데이터를 보호할 수 있고 통찰력과 자동화된 인텔리전스를 바탕으로 지속적인 감지 및 문제 해결을 수행하여 리스크를 최소화할 수 있습니다.

4 CCS Insights Survey, "IT Buyer Survey", 2017년 9월

새로운 보안 요구 사항

- 8가지의 핵심적인 차단, 감지, 해결 기능을 도입하여 조직을 보호해야 합니다.
- 프레임워크를 사용하여 에코시스템을 보호하는 구성 요소 간에 신뢰를 구축하여 통합된 뷰를 확보해야 합니다.
- 환경으로부터 통찰력을 얻어 예측 방식의 자동화된 의사 결정을 내려 디지털 워크스페이스를 보호하고 리스크를 지속적으로 완화해야 합니다.

변화하는 디지털 워크스페이스에서 포괄적인 보안을 구현하기 위한 3단계

IT 조직은 최종 사용자 환경을 보호하기 위한 포괄적인 엔터프라이즈급 접근 방식이 필요합니다. 이 모델은 보안 기술 사일로를 함께 연결하여 Endpoint, 애플리케이션, 직원, 네트워크 전반에 대한 보안을 포괄합니다. 최상의 결과를 얻기 위해 IT는 이러한 단계를 고려하여 변화하는 디지털 워크스페이스를 전략적으로 보호해야 합니다.

1단계: 위협 차단, 감지, 해결

사이버 위협은 발전해 왔습니다. 기존에는 무단으로 시스템에 침입했다가 바로 나가는 방식으로 자신의 IT 기량을 발휘해 친구들에게 강력한 인상을 주려는 학생들과 같이 장난스러운 해킹 활동에 그치는 경우도 있었지만 지금은 거의가 악의적인 의도를 가진 해커입니다. 사이버 범죄를 차단하기 위해서는 악의적 행위를 추적하는 동시에 정상 상태를 적용하는 포괄적인 대응이 필요합니다.

차단

수많은 기업, 특히 금융 서비스 기업이나 의료 서비스 기업과 같은 규제 대상 기업에서는 중요도가 높은 데이터의 백엔드 스토리지에 대한 규정 준수 요건을 충족하기 위해 노력하고 있습니다. 그러나 오늘날 고객 관리자는 고객과의 회의 동안 모바일 기기에서 중요 데이터에 액세스할 수 있으며 실수로 태블릿을 택시에 놓고 내려서 중요 데이터가 도난당할 수 있습니다. 이렇게 고객 정보가 분실되거나 손상되면 브랜드 및 재무에 부정적인 영향을 미칠 가능성이 매우 높습니다.

데이터 및 애플리케이션에 대해 소비자 수준의 간편하고 원활한 액세스를 제공해도 기업에 큰 리스크를 야기하지 않아야 합니다. 따라서 기업 수준의 보안 기능은 직원들의 디지털 워크스페이스를 보호하는 것부터 시작해야 합니다. IT는 직원들에게 의심스러운 링크를 클릭하지 않도록 교육하고 데이터 손실을 방지하기 위한 정책을 배포하여 맬웨어가 환경에 진입하지 못하게 해야 합니다. 또한 기업에서 직원부터 애플리케이션, 기기, 네트워크에 이르는 모든 자산에 대한 완벽한 가시성을 확보하게 되면 취약점을 식별하고 내외부 위협으로부터 환경을 보호할 수 있습니다. 액세스 제어, 중요 데이터 분류, 기기 사용 제한과 같은 정책의 구현을 비롯한 다양한 보호 조치를 완벽하게 구현하고 정기적으로 애플리케이션에 패치를 적용해야만 안심하고 감지 단계로 나아가기 위한 준비를 할 수 있습니다. 차단은 중요하지만 이와 동일하게 효과적인 감지 방법이 없으면 IT는 가장 중요한 문제를 해결하고 있는지조차 알지 못하게 됩니다.

감지

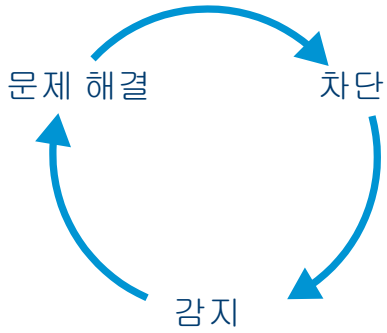
사라지는 경계, 내부자 위협, 점차 지능적으로 변하는 사이버 범죄로 인해 보안 관련 대화가 "만약 보안이 발생한다면"에서 "보안이 발생할 때"로 변모했습니다. 따라서 기업에서는 자산을 보호하는 것에서 벗어나 자격 증명 손상부터 패치가 적용되지 않은 취약점 악용까지 침입이 언제 발생하는지 감지하는 방법을 모색해야 합니다. IT 팀은 활동 중인 위협이 기업에 더 심각한 손상을 가하기 전에 이를 파악하여 해소할 수 있어야 합니다. 또한 감지는 경고로 인한 피로도를 야기하지 않는 방식으로 구현해야 합니다.

디지털 워크스페이스에 위협이 발생하면 준비된 기업에서는 지속적인 적응형 모니터링을 통해 이를 감지할 수 있으므로 IT 운영 및 보안 팀에서는 모바일 및 데스크톱 Endpoint와 애플리케이션에 대한 위협을 알아낼 수 있습니다. 자동화되고 지속적인 모니터링과 누가 어디서 어떤 네트워크를 통해 어떤 정보에 어떻게 액세스하는지에 대해 알림을 받을 수 있으므로 IT는 제어 능력을 유지할 수 있습니다. 그런 다음 IT는 마지막으로 알려진 정상 상태, 로깅 및 인텔리전스를 분석에 활용하여 차이점을 파악할 수 있고 이러한 통찰력을 가지고 다음에 수행할 조치를 현명하게 결정할 수 있습니다.

문제 해결

디지털 비즈니스는 빠르게 변화하므로 대부분의 경우 수작업으로 문제를 해결해야 하는 기존의 보안 솔루션이 무용지물이 되고 있습니다. 오늘날의 기업은 악의적인 침입 및 예상치 못한 운영 중단에 직면할 때 빠른 대응이 필요합니다. 대응에 지체하는 경우 더 큰 침해가 발생할 수 있습니다. VMware 내부 연구에 따르면 기업 고객 1/10이 대부분 또는 모든 Endpoint에 영향을 주는 Windows 패치 적용을 완료하는 데 1년 이상 걸리는 것으로 나타났습니다. 이는 사이버 보안 범죄자들에게 악용 방법을 개발하는 시간을 벌어주는 결과를 낳습니다.

IT 팀은 환경에 대한 통찰력을 활용하여 근본 원인을 바탕으로 정책을 사전에 정의하고 대응 및 복구를 신속하게 자동화하여 최상의 결과를 도출해야 합니다. 자동화를 통해 IT는 애플리케이션 또는 클라우드 서비스에 대한 액세스를 격리, 일시 중단 또는 차단할 수 있습니다. 대부분의 준비된 기업에서는 위협이 감지되면 비정상적인 동작을 감지하고 중요 데이터에 대한 액세스를 차단하는 자동화된 정책을 시작할 수 있는 엔진을 통해 문제 해결을 자동화하는 효과적인 솔루션을 갖추고 있습니다.



에코시스템의 구성 요소 간에 신뢰를 구축할 수 있는 전략적 프레임워크와 이러한 구성 요소를 보호하는 솔루션을 선택하는 기업이 중요한 기업 자산을 완벽하게 보호할 수 있고 감지 및 문제 해결 시간을 단축할 수 있습니다.

2단계: 차단, 감지, 해결 기능

다음 8가지 핵심 기능을 통해 기업은 최적화되고 포괄적인 디지털 워크스페이스 보안을 구현할 수 있습니다.

단일 개방형 플랫폼 접근 방식	단일 개방형 플랫폼을 통해 IT는 기기 및 애플리케이션의 규정 준수 적용을 간소화하고 리스크를 줄일 수 있습니다. 기업에서는 액세스, 기기 및 애플리케이션 관리 기능을 분석 및 인텔리전스와 통합하여 복잡하고 비용이 많이 드는 기존의 보안 솔루션 사일로를 고유하게 연결하는 단일 개방형 플랫폼을 도입해야 합니다. 인텔리전스 서비스가 지원되는 단일 플랫폼을 통해 워크스페이스 데이터를 집계하고 상관관계를 분석하며 권장 사항을 제안하여 통합형 통찰력과 자동화 기능을 제공할 수 있습니다. 이러한 접근 방식을 사용하는 기업은 직원, 애플리케이션, Endpoint, 네트워크를 한 곳에서 파악할 수 있게 됩니다. 이 플랫폼 접근 방식은 기업 에코시스템의 구성 요소 간에 신뢰를 구축하는 API 통신 네트워크를 기반으로 구축해야 합니다. 디지털 워크스페이스 전반에서 신뢰가 구축된 경우 상호 연결된 최소 권한 시스템을 통해 직원의 보안을 상시 유지할 수 있으므로 이는 중요한 문제입니다.
DLP(데이터 손실 방지) 정책	DLP 정책은 기업에서 데이터가 데이터 센터 내부에 있든 외부에 있든 관계없이 데이터를 보호하는 데 유용한 방법입니다. IT 팀은 원격으로 기기를 잠금 설정하거나 초기화할 수 있어야 합니다. 즉, 기기를 분실하거나 도난당한 경우 해당 기기를 찾아서 운영 체제(OS) 버전, 마지막 업데이트, 위치 등의 실시간 기기 정보를 획득할 수 있어야 합니다. Virtual Desktop Infrastructure(VDI)를 활용하여 데스크톱 및 애플리케이션을 중앙 집중화하면 분실되거나 도난당한 기기의 데이터 손실을 줄일 수 있습니다. 또한 기업은 Endpoint 전반에서 DLP 제어를 제공하는 기본 OS를 사용하여 애플리케이션별로 보안 정책을 적용하고 관리할 수 있어야 하고 e-메일 첨부 파일 제어, 자르기/복사/붙여넣기 제한, 동적 워터마크 등을 통해 컨텐츠 전반에서 데이터 손실을 방지할 수 있어야 합니다. SDK(소프트웨어 개발 키트)를 사용해 기업의 컨텐츠를 삭제할 수 있는 사용자의 기능을 제어하고 제한하는 것이 필요합니다. 정책 및 규정 준수 엔진을 이용하면 고급 DLP에 대한 규정 준수를 자동화할 수 있습니다. 고급 보안 정책에는 루팅 또는 탈옥된 기기로부터의 보호, 차단 및 허용 애플리케이션 목록, 애플리케이션의 실행 위치 제한, 지오펜싱, 네트워크 구성, 익스포트 및 스크린샷 차단, 외부 SD 카드나 원격 클라우드 백업 솔루션으로 기업 정보의 백업 또는 저장이 포함됩니다.
상황별 정책	상황별 정책을 사용하여 최종 사용자의 조건부 액세스를 설정하고 적용하면 승인된 사용자에게만 중요 정보 및 리소스에 대한 액세스 권한을 부여할 수 있습니다. 승인된 사용자만 특정 정보 및 리소스를 이용할 수 있도록 기업은 역할, 부서, 승인 수준 등을 기준으로 조건부 액세스를 설정할 수 있어야 합니다. 정책 시행을 액세스 및 기기 관리와 통합하여 IT는 데이터, 애플리케이션 또는 기기에 대한 사용자 권한을 제한할 수 있습니다. 이 기술은 모바일 애플리케이션에 대한 조건부 액세스를 적용하고 규정을 준수하는 애플리케이션만 내부 시스템에 액세스할 수 있도록 보장하는 데도 사용할 수 있습니다.

애플리케이션 보호	애플리케이션 수준에서 DLP 정책을 적용하여 기업은 데이터를 더 안전하게 보호하는 보다 세분화된 액세스 정책을 만드는 데 한 걸음 더 나아갈 수 있습니다. 디지털 워크스페이스에는 애플리케이션 수준에서 동일한 기능을 제공하는 DLP 정책(앞의 두 번째 기능에서 설명)이 포함되어 있어야 합니다. BYO(Bring Your Own) 기기와 기업 기기 모두 모바일 애플리케이션 관리를 통한 프로비저닝 및 액세스 제어가 가능하므로 사실상 ID에 의해 정의된 정책을 통해 애플리케이션을 래핑할 수 있습니다. 마찬가지로 승인되지 않은 클라우드 서비스와 승인된 클라우드 서비스에서의 액세스 및 활동 관리를 비롯한 클라우드 데이터 손실 방지는 위협으로부터 데이터를 더 안전하게 보호합니다. iOS, Android, macOS, Windows 10을 비롯한 주요 OS 전반에서 전체 기기 VPN, 애플리케이션별 VPN, SDK 기반 프록시 게이트웨이 통신이 지원되므로 IT는 애플리케이션 연결을 보호하기에 적합한 솔루션을 자유롭게 선택할 수 있습니다. 또한 생산성 애플리케이션(예: e-메일, 문서 관리 등)은 다음과 같은 DLP 및 RMS(권한 관리 서비스) 기능을 제공해야 합니다. • IRM(정보 권한 관리) 보안 e-메일 • PKI가 통합된 S/MIME • e-메일 분류 • 중요 정보 또는 개인 식별 정보(PII) 정책 • 첨부 파일 암호화 • 인쇄, 조회, 로밍을 위한 액세스 정책 • 문서 만료 • 워터마크
액세스 관리	기업은 여러 인증 단계를 통해 사용자 ID를 확인하거나 많은 애플리케이션에 대해 한꺼번에 사용자 ID를 확인하여 데이터 보호를 강화합니다. 끊임없이 증가하는 애플리케이션, 기기, 클라우드 서비스에 대해 개별 정책을 적용해야 하는 점점 복잡해지는 작업을 없애기 위해 기업에서는 최종 사용자의 ID를 사용하여 보안 매개 변수를 지정할 수 있어야 합니다. 원터치 싱글 사인온(SSO)을 이용하면 사용자가 여러 번 로그인하느라 번거롭게 시간을 낭비하지 않고도 데스크톱, 모바일, 클라우드 애플리케이션에 액세스할 수 있습니다. SSO를 통해 많은 애플리케이션에 대해 사용자 ID를 한번에 확인할 수 있으므로 애플리케이션 카탈로그에서 선택한 Endpoint에서 웹, 모바일, SaaS, 기존 애플리케이션에 다양하게 액세스할 수 있도록 디지털 워크스페이스별로 하나의 키를 제공하게 됩니다. 다단계 인증(MFA)을 통해 사용자와 시스템 구성 요소의 ID는 암호 입력을 비롯한 여러 인증 단계를 거쳐야 하며 요청한 액세스 또는 기능의 리스크에 맞게 보안이 강화됩니다.
암호화	암호화는 데이터가 전송 및 수신될 때 의도하지 않은 수신자가 볼 수 없도록 차단하여 중요 데이터를 보호합니다. 중요한 비즈니스 프로세스에서 데이터를 저장 또는 전송할 때 모든 데이터를 암호화하는 것이 가장 좋습니다. 데이터 침해가 발생하여 중요한 파일이 도난당해도 공격자가 암호화로 인해 데이터를 읽을 수 없어야 합니다. 전송 중인 데이터와 미사용 데이터의 경우에는 AES-256비트 암호화와 같은 AES(Advanced Encryption Standard)를 활용하는 것이 중요합니다. 기기 플랫폼과 기업 시스템 간의 가교 역할을 하는 IT는 터널 또는 애플리케이션별 VPN을 사용하여 규정을 준수하는 기기의 개별 애플리케이션에서 고유 인증을 사용하여 도달해야 하는 백엔드 시스템까지의 트래픽을 인증하고 암호화할 수 있습니다.

마이크로 세분화	기업에서는 네트워크 전반의 마이크로 세분화를 통해 더욱 적극적으로 위협에 대응하고 리스크를 줄이며 보안 태세를 강화할 수 있습니다. 마이크로 세분화는 다음과 같은 기능을 통합하여 제공합니다. • 워크로드별로 세분화된 분산 상태 저장 방화벽 및 ALG(애플리케이션 수준 게이트웨이)를 통해 데이터 센터 경계 내의 공격 면적 감소 • 가상 데스크톱, 가상 애플리케이션 호스트를 비롯한 가상 머신에 대한 객체 기반 정책 애플리케이션에 대해 보안 그룹 사용을 활성화하여 세분화된 애플리케이션 수준 제어 생성 • 기반 네트워크 하드웨어에 관계없이 랙 또는 데이터 센터를 포괄할 수 있는 논리적 네트워크 오버레이 기반의 격리 및 세분화를 통해 여러 데이터 센터 보안 정책의 중앙 관리 지원 전체 IT 환경은 훨씬 용이하게 관리할 수 있도록 작은 부분으로 나누어 보호하고 한 부분이 손상될 경우 피해를 억제할 수 있도록 해야 합니다. 애플리케이션에서 데이터 센터의 특정 워크로드로의 횡방향 트래픽을 격리하면 비즈니스에 심각한 피해를 주려는 맬웨어/바이러스의 공격 벡터가 대폭 감소합니다.
분석	기업에서는 애플리케이션 배포 및 사용에 대한 실행 가능한 통찰력을 바탕으로 보안 태세를 개선합니다. 애플리케이션 배포, 사용, 기기 보안 및 최종 사용자 환경 세부 정보가 통합되면 IT에서 디지털 워크스페이스 환경의 성능과 보안을 더 잘 이해할 수 있습니다. 자동화된 조치와 함께 기본 제공되는 인텔리전스 서비스를 사용하면 계획을 더 빠르게 세울 수 있고 보안이 강화되며 최종 사용자 환경이 개선됩니다. 또한 오늘날의 경계 없는 환경에서 보안 리스크를 지속적으로 모니터링하고 신속하게 대응하여 리스크를 완화합니다. 의사결정 엔진과 함께 인텔리전스 서비스를 이용하면 정보의 상관관계를 분석하여 위협을 감지하고 액세스 정책을 통해 문제 해결을 자동화할 수 있습니다.

3단계: 신뢰하는 파트너가 모든 위치에 보안 적용

보안 위협은 공략 대상과 정교함뿐 아니라 발생 빈도와 비용 모두 증가하고 있으므로 신뢰하는 보안 파트너 벤더가 통합된 단일 플랫폼을 이용하면 위협을 효과적으로 차단, 감지, 해결할 수 있습니다. 중요한 정보를 보호하도록 고안된 기존의 독립 실행형 보안 툴은 IT에 대한 가시성이 제한되므로 환경 전반에서 종종 솔루션 사일로가 생성됩니다. 이러한 임시 방편의 접근 방식은 조직에 부정적인 영향을 주며 복잡성으로 인한 높은 비용과 수작업을 요구하여 디지털 워크스페이스를 보호하기 어렵게 만듭니다.

성장하고 변화하는 디지털 워크스페이스를 보호하는 구성 요소 간에 신뢰를 구축해야 포괄적인 보안을 구현할 수 있습니다. 이상적인 접근 방식은 검증된 디지털 워크스페이스 플랫폼에 구축된 API를 활용하는 신뢰의 프레임워크를 이용하는 것입니다. 이러한 API를 활용하면 보안 솔루션으로 구성된 풍부한 에코시스템에서 플랫폼과 통신하고 궁극적으로 시스템 관리자가 원하는 통합 뷰를 제공하여 보안 및 관리를 간소화할 수 있습니다.

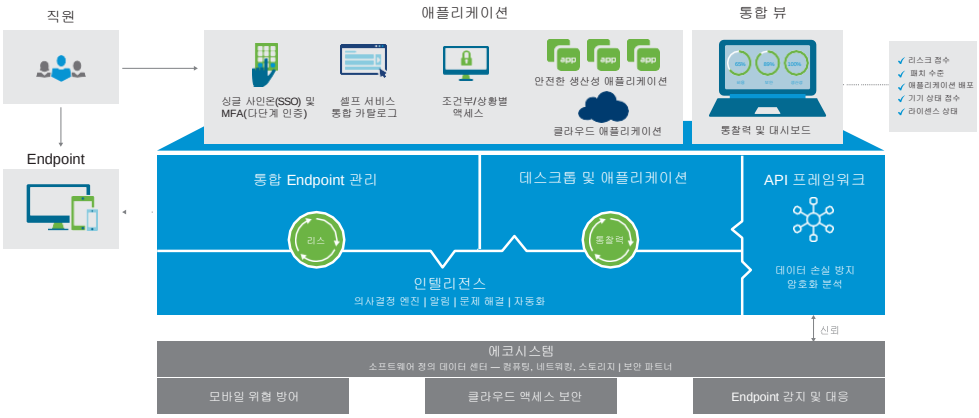
강력한 디지털 워크스페이스 전략에는 다음과 같은 영역에서 공격을 막고 리스크를 완화하는 데 주력하는 신뢰하는 보안 솔루션으로 구성된 개방형 에코시스템이 포함됩니다.

- OS 보안 결함 가시성
- 기기 상태 평가
- 기기 복구
- 액세스 관리 및 제어
- 정책 설정
- 바이러스 검사
- 패치 적용
- 재해 복구
- 규정 준수 모니터링

VMware의 기존 디지털 워크스페이스 보안 혁신 방안

사이버 보안 툴과 관련하여 상당한 혁신이 진행 중이지만 시장에 출시된 툴의 수와 다양성만 놓고 봤을 때 IT 책임자는 디지털 워크스페이스 보안에 대한 모범 사례 접근 방식이 나올 때까지 기다려야 합니다. 오늘날 기업에서는 VMware로 전환하면 프레임워크를 통해 보안을 간소화하여 변화하는 위협 환경 전반에서 공격에 대응할 수 있습니다.

VMware® Workspace ONE™ Trust Network™는 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 디지털 워크스페이스 플랫폼인 Workspace ONE의 통찰력을 신뢰하는 보안 파트너 솔루션과 통합하여 디지털 워크스페이스에서 예측 방식의 자동화된 보안을 제공합니다.



차단, 감지, 해결

VMware의 접근 방식을 통해 IT 운영 및 보안 팀에서는 NIST 사이버 보안 프레임워크와 같은 프레임워크를 사용하여 보안 기능을 Workspace ONE Trust Network 접근 방식에서 제공하는 기능에 간단하게 매핑하여 사이버 보안 리스크를 관리할 수 있습니다.

- 보안 기능은 머신 러닝을 사용하여 맬웨어를 인식하고, 네트워크를 마이크로 세분화하여 발전된 형태의 지속적 위협(APT)을 차단하며, 기업의 클라우드 기반 애플리케이션에서 데이터 외부 유출을 방지하는 등의 방식으로 디지털 워크스페이스를 보호하는 데서부터 시작됩니다.
- 디지털 워크스페이스에 위협이 발생하면 VMware 보안 기능이 모바일 및 데스크톱 Endpoint와 애플리케이션 전반에서 지속적인 적응형 모니터링을 통해 이를 감지합니다.
- 그런 다음 이러한 접근 방식은 강력한 의사결정 엔진을 사용하여 문제 해결을 자동화합니다. 예를 들어 비정상적인 동작에 근거하여 트로이 목마 또는 MITM 공격이 감지되면 기업 데이터에 대한 액세스를 차단하는 자동화된 정책이 시작됩니다.

액세스, 기기, 애플리케이션 관리와 분석의 통합

Workspace ONE Trust Network는 액세스, 기기, 애플리케이션 관리를 비롯해 Workspace ONE의 디지털 워크스페이스 핵심 기능을 Workspace ONE 인텔리전스를 기반으로 하는 분석과 통합하여 기존 보안 솔루션의 사일로를 고유하게 연결합니다. Workspace ONE 인텔리전스 서비스를 통해 워크스페이스 데이터를 집계하고 상관관계를 분석하며 권장 사항을 제안하여 통합형 통찰력과 자동화 기능을 제공할 수 있습니다. VMware는 Workspace ONE Trust Network 기능을 Workspace ONE 인텔리전스 서비스와 통합하여 기업에서 오늘날의 경계 없는 환경에서 보안 리스크를 지속적으로 모니터링하고 리스크 완화를 위해 신속하게 대응할 수 있도록 지원합니다.

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 에코시스템 활용

디지털 워크스페이스 전반에서 포괄적인 보안을 구현하기 위해서는 성장하고 변화하는 디지털 워크스페이스를 보호하는 구성 요소 간에 신뢰를 구축해야 합니다. VMware는 Workspace ONE 플랫폼에 구축된 API를 활용하여 신뢰의 프레임워크를 제공하는 Workspace ONE Trust Network를 통해 이를 가능하게 합니다. 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 VMware 고객은 기존 투자를 활용해 지속적인 모니터링 및 리스크 분석을 크게 개선하여 더 빠른 응답 시간을 제공할 수 있습니다. 따라서 추세와 패턴을 기반으로 구축에 따라 확장 가능한 예측 방식의 보안 전략을 실현할 수 있습니다.

VMware 고객은 기존 투자를 활용해 지속적인 모니터링 및 리스크 분석을 크게 개선하여 더 빠른 응답 시간을 제공할 수 있습니다. 따라서 추세와 패턴을 기반으로 구축에 따라 확장 가능한 예측 방식의 보안 전략을 실현할 수 있습니다.

업무의 경계가 없어지고 있으므로 기업에서 새로운 디지털 워크스페이스 보안 접근 방식을 도입해야 합니다. 에코시스템의 구성 요소 간에 신뢰를 구축하는 프레임워크는 새로운 직원, 새로운 애플리케이션, 새로운 기기, 새로운 네트워크를 수용합니다. 디지털 엔터프라이즈는 리스크를 완화하고 브랜드를 보호하며 비용을 줄이고 대응력을 높이고 모든 기기에서 소비자 수준의 편리한 환경을 제공하면서 빠르게 나아갈 수 있기를 원하므로 이러한 프레임워크는 발전을 위한 초석이 됩니다.

차단, 감지, 해결: 8가지 필수 기능

vmware Workspace ONE™ Trust Network	
기능	**중요한 이유**
단일 개방형 플랫폼 접근 방식	플랫폼, 애플리케이션, 사용자 프로필 전반에서 기술 사일로를 제거하여 규정 준수 적용을 간소화하고 리스크를 줄입니다.
DLP(데이터 손실 방지) 정책	기기 지우기, 원격 잠금 설정, 애플리케이션별 보안 정책을 통해 위치에 관계없이 데이터를 보호합니다.
상황별 정책	조건부 액세스 정책 시행을 통해 승인된 사용자에게만 중요 정보 및 리소스에 대한 액세스 권한을 부여합니다.
애플리케이션 보호	애플리케이션 수준에서 DLP 정책을 통해 누가 어떤 리소스에 액세스하는지 제어하여 정보를 보호합니다.
액세스 관리	여러 인증 단계를 통해 사용자 ID를 확인하거나 싱글 사인온(SSO)을 통해 많은 애플리케이션에 대해 한꺼번에 사용자 ID를 확인하여 데이터 보호를 강화합니다.
암호화	데이터가 전송 및 수신될 때 의도하지 않은 수신자가 볼 수 없도록 차단하여 중요 데이터를 보호합니다.
마이크로 세분화	워크로드와 트래픽을 분리하여 공격 범위를 축소합니다.
분석	실행 가능한 통찰력, 애플리케이션 분석 및 자동화를 바탕으로 보안 태세 및 규정 준수를 개선합니다.

자세한 정보

직원들에게 디지털 워크스페이스를 제공하면 직원과 기업 모두에 이익이 됩니다. 생산성과 효율성 측면에서 IT 보안 문제가 장애물이 되어서는 안 됩니다. Workspace ONE Trust Network 접근 방식은 동적인 사이버 위협이 증가하고 기존의 경계를 넘어서 새로운 취약점을 공략하도록 변화하는 추세에 맞춰 디지털 워크스페이스 전략을 확장하고 발전시키므로 기업에서 중요 데이터를 보호하기 위한 포괄적인 보안을 실현하기 위해 필요로 하는 기능을 제공합니다. 액세스, 기기, 애플리케이션 관리를 분석과 통합하고 에코시스템 전반에서 신뢰의 프레임워크를 활용하며 수집된 데이터에서 통찰력을 얻어 올바른 보안 결정을 내리는 방식으로 디지털 워크스페이스를 보호합니다.

Workspace ONE Trust Network에 대한 자세한 내용은 www.vmware.com/kr/products/workspace-one/security를 참조하십시오.

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