VMware AppDefense로 애플리케이션을 가상화된 환경 및 클라우드 환경에서 보호

요약 정보

VMware AppDefense™는 가상화 환경에서 실행되는 애플리케이션을 보호하는 데이터 센터 Endpoint 보안 제품입니다. 위협을 사후 대응 방식으로 추적하는 기존 Endpoint 보안 솔루션과 달리, AppDefense는 애플리케이션이 의도된 상태(정상 상태)대로 작동하고 있는지 모니터링하고, 의도된 상태에서 벗어나 위협이 감지되는 경우 자동으로 대응하도록 설계되었습니다. 따라서 보안 운영의 효율성과 효과가 극대화되고 애플리케이션 보안 태세 검토 프로세스가 간소화됩니다.

핵심 요점

- 데이터 센터 Endpoint 보안 간소화
- SOC에서 더 효과적으로 위협 감지
- 문제 발생 시 자동 대응
- 애플리케이션 보안 검토 간소화

IT보안에 대한 전 세계 지출이 증가하고 있는 가운데, 조직이 데이터 침해의 피해를 입을 가능성이 1/4로 증가했습니다.[1] 시장에 나와 있는 수많은 보안 제품과 이를 구입하기 위한 막대한 예산에도 불구하고 데이터 보안은 전혀 개선되지 않고 있습니다. 이로 인해 최고 정보 보안 책임자(CISO)는 점점 역동적이고 분산된 IT 환경에 상주하는 애플리케이션과 데이터를 보호해야 하는 어려운 과제에 직면하고 있습니다. 점점 더 많은 조직이 최신 방식의 신속한 애플리케이션 개발 모델을 도입함에 따라, 비즈니스의 속도에 맞게 보안을 구현하는 일이 더욱 어려워지고 있으며, 보안은 종종 발전의 장애물로 간주되곤 합니다.

CISO와 해당 팀이 데이터와 애플리케이션을 보호하기 위해 노력하는 과정에서 직면하는 2가지의 주된 어려움은 다음과 같습니다.

감지되지 않은 위협 및 허위 경보

수많은 허위 경보를 생성하는 기존 Endpoint 보안 솔루션으로 인해, 보안 운영 팀은 존재하지도 않는 위협을 수작업으로 조사하느라 시간을 허비하곤 합니다. 그러나 이보다 더 큰 문제는 위협을 완전히 놓칠 수 있다는 것입니다.

빠르게 변화하는 동적 환경

기존 보안 솔루션은 최신 애플리케이션 개발 및 배포 속도를 수용하도록 설계되지 않았습니다. 즉, 새로운 애플리케이션의 출시 및 업그레이드 속도에 맞춰 보안 적용이 이루어지지 않고 있습니다.

가상화를 통한 보안 혁신

VMware AppDefense는 이러한 당면 과제를 모두 해결할 수 있는 독보적인 위치를 확보하고 있습니다. AppDefense는 데이터 센터 Endpoint 보안 솔루션 제품으로, 위협 감지 및 대응 기능이 애플리케이션 및 데이터가 상주하는 가상화 계층 내에 포함되어 있습니다. VMware vSphere®를 활용하는 AppDefense는 기존 Endpoint 보안 솔루션에 비해 다음과 같은 3가지 주요 이점을 제공합니다.

애플리케이션의 의도된 상태에 대한 신뢰할 만한 정보 – 정상 상태가 무엇인지 알아야 비정상 상태를 감지 가능

vSphere 하이퍼바이저 내부에서, AppDefense는 데이터 센터 Endpoint의 의도된 작동 방식을 제대로 이해하고 변경 사항을 가장 신속하게 파악합니다. 이 상황별 인텔리전스를 통해 적절한 변경 사항과 실제 위협을 정확하게 구분할 수 있습니다.

자동화되고 정확한 위협 대응 – 적시에 적절하게 대응

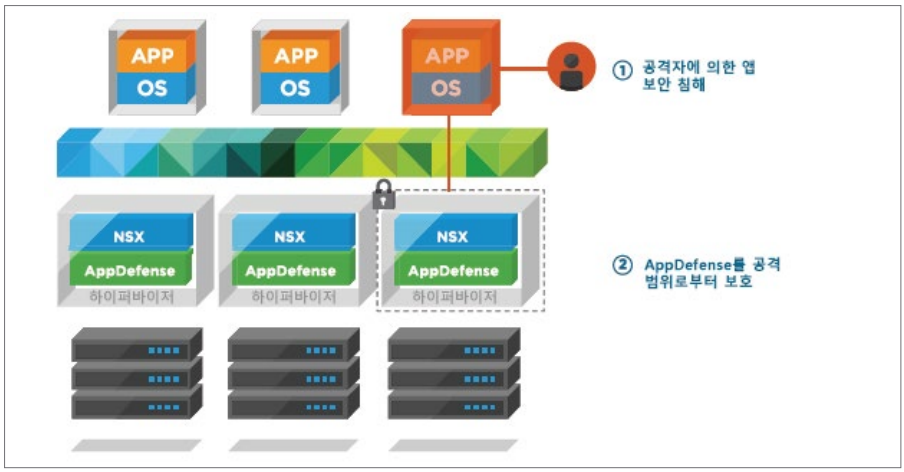
위협이 감지될 경우 AppDefense는 vSphere와 VMware NSX®를 트리거하여 수동 개입 없이 위협에 적절하게 대응할 수 있습니다. 예를 들어, AppDefense는 다음을 자동으로 수행합니다.

- 프로세스 통신 차단
- Endpoint 스냅샷을 통한 문제 분석
- Endpoint 일시 중단
- Endpoint 종료

vmware®

공격 범위로부터 분리 – AppDefense 자체 보호

대부분의 맬웨어 변종이 Endpoint에 도달했을 때 하는 첫 번째 행동은 바이러스 백신과 기타 에이전트 기반 Endpoint 보안 솔루션을 무력화하는 것입니다. 하이퍼바이저는 AppDefense를 운영할 수 있는 보호된 지점을 제공하므로 Endpoint가 손상되더라도 AppDefense 자체는 보호됩니다.



AppDefense의 효과

AppDefense는 조직의 보안 전략에 광범위한 영향을 미치는 핵심 보안 제품입니다.

SOC(보안 운영 센터)를 위한 애플리케이션 중심 알림

AppDefense는 많지는 않지만 신뢰성 있는 알림을 생성합니다. AppDefense가 생성하는 신뢰성 있는 알림은 자동화된 대응 기능과 함께 결합되어 보안 관리자가 노이즈 데이터 사이를 헤매고 존재하지 않는 위협을 조사하는 대신 자체 환경에서 위협을 포착하고 제거하는 데 집중할 수 있도록 합니다.

애플리케이션 보안 태세 검토 혁신

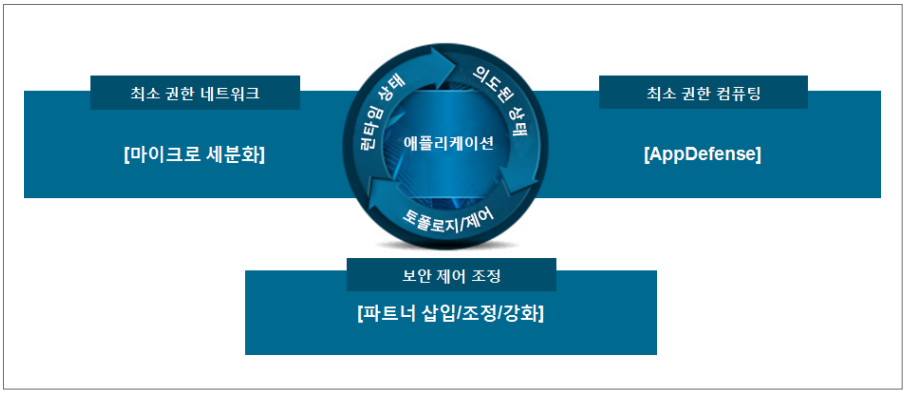
최신 애플리케이션 개발 영역에서 애플리케이션은 빠르게 출시되고, 변경되고, 폐기됩니다. 보안 팀이 새로운 애플리케이션의 존재를 파악할 때쯤이면 이미 변경되었을 가능성이 큽니다. AppDefense는 애플리케이션 팀과 보안 팀 간에 정보의 공통 출처를 생성하여 보안 검토 프로세스를 간소화합니다.

VMware를 통한 애플리케이션 중심 보안

VMware는 네트워크 가상화 플랫폼인 VMware NSX으로 데이터 센터 전반에 걸쳐 마이크로 세분화를 구현하여 네트워크 보안을 혁신했습니다. NSX는 방화벽과 같은 네트워크 및 보안 서비스를 하이퍼바이저에 직접 설계하여 네트워크에 대해 최소 권한 모델을 구현합니다. 따라서 네트워크 보안 팀이 환경 내에서 보안 위협의 수평적 확산을 방지할 수 있습니다.

자세한 정보

자세한 정보를 알아보거나 VMware AppDefense를 구매하려면 http://www.vmware.com/kr/appdefense를 방문하여 Hands-On Lab에서 제품을 테스트해 보십시오.



AppDefense는 인프라의 또 다른 핵심 영역에 위협 감지 및 대응 기능을 통합하여 데이터 센터 Endpoint에 최소 권한 모델을 구현합니다. 위협이 Endpoint에 침입하면 AppDefense는 즉시 위협을 감지하고 자동적으로 정밀한 대응을 취합니다. NSX와 AppDefense는 애플리케이션 인프라를 보호하는 강력한 솔루션을 제공하므로 해당 인프라에 상주하는 애플리케이션와 데이터도 보호합니다.

[1] Ponemon Institute, 2017년 6월 "2017 Cost of a Data Breach Study: Global Overview"

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: vmw53313-sb-securing-app-cloud-env-app-defense-ko-KR-a4-101