VMware vShield App with Data Security

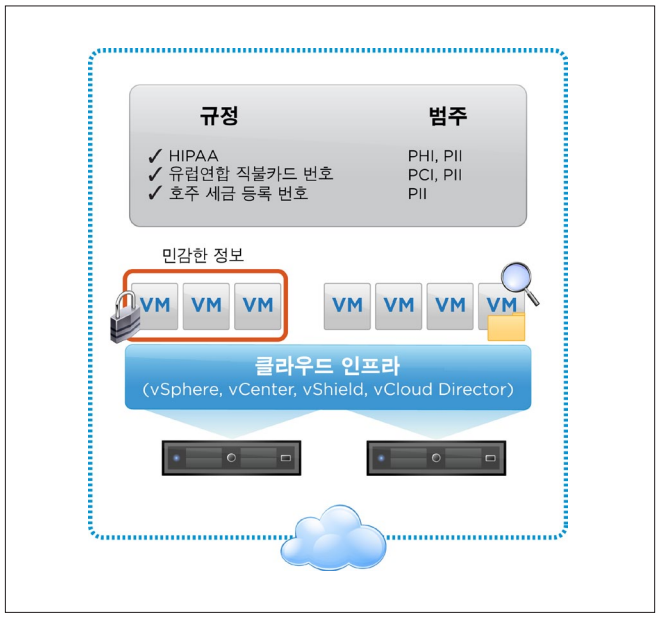
네트워크 기반의 각종 공격으로부터 애플리케이션을 보호하고 민감한 데이터 검색

요약 정보

VMware vShield 가상화 보안 제품군 중 하나인 VMware vShield™ App with Data Security는 네트워크 기반의 각종 공격으로부터 가상 데이터 센터의 애플리케이션과 데이터를 보호합니다. 따라서 조직은 가상 머신 간의 네트워크 커뮤니케이션을 확실하게 파악하고 제어할 수 있습니다. 또한 이 제품은 가상화된 워크로드 내부에서 신용카드 정보와 같은 민감한 데이터를 검색하는 기능을 제공하고 규정(예: PCI-DSS) 위반 사항을 보고하므로 IT 조직은 해당되는 전 세계 모든 규정에 대한 준수 상태를 신속하게 평가할 수 있습니다. 여기에 바이러스 백신 파일 검색을 오프로드하는 VMware vShield Endpoint도 포함되므로 바이러스 백신 "과부하"를 최소화합니다.

주요 장점

- 가상 머신 간의 네트워크 커뮤니케이션을 더욱 확실하게 파악 및 제어
- 가상 머신에 저장된 민감한 데이터를 더욱 확실하게 파악하여 규정 미준수의 위험 감소
- 보안 그룹을 구분하기 위해 전용 하드웨어 및 VLAN이 필요 없음
- 강력한 보안을 유지하고 동시에 하드웨어 리소스 활용률도 최적화
- 모든 가상 머신 네트워크 활동에 대한 포괄적인 로깅을 통해 간편하게 규정 준수



vShield App with Data Security는 보안 그룹을 사용하여 세분화된 정책 적용을 수행합니다.

vShield App with Data Security 개요

vShield App with Data Security는 애플리케이션을 인식하는 하이퍼바이저 기반의 가상 데이터 센터용 방화벽 솔루션으로, 가상 머신 컨테이너에 상주하는 구조화되지 않은 데이터 파일에 저장된 신용카드 정보와 같이 민감한 데이터를 동적으로 검색합니다. 따라서 관리자는 데이터 센터, 클러스터 또는 리소스 풀에서 민감한 데이터가 존재하는지 여부를 검색할 수 있어 규정 준수 감사를 충족할 수 있습니다.

이 제품은 VMware vSphere®에 직접 연결하여 네트워크 기반의 각종 내부 위협으로부터 안전하게 보호하고 기업 보안 환경 내에서 정책 위반의 가능성을 줄여 줍니다. 이를 지원하기 위해 이 제품은 소스/대상 IP 주소에 기반한 연결 제어 및 심층 패킷 조사와 더불어 애플리케이션 인식 방화벽을 사용합니다.

또한 IT 부서에서 비즈니스별 보안 그룹을 신속하게 생성할 수 있도록 지원하여 정책 제어를 간소화하며, 이 제품의 플로우 모니터링 제어 기능을 통해 IT 부서는 가상 머신 네트워크 트래픽을 분석하고 보안 그룹 정책을 동적으로 적용할 수 있습니다. 관리자는 VMware vCenter Server™에 매끄럽게 통합되어 가상 데이터 센터의 보안 관리 통합을 촉진하는 vShield Manager 콘솔을 통해 중앙에서 vShield App with Data Security를 관리할 수 있습니다.

이 제품은 vLAN과 같은 기존 제어와 하드웨어에 대한 의존성을 없애주므로 하드웨어와 정책을 계속 추가할 필요가 없어 비용 효율이 뛰어나며 물리적 보안의 한계를 극복합니다.

vShield App with Data Security의 작동 방식

이 제품은 민감한 데이터 검색 정책을 관리할 수 있는 관리자 콘솔을 제공합니다. 관리자는 대상 가상 머신 컨테이너(데이터 센터, 클러스터, 리소스 풀 등) 전체에 검색할 관련 규정을 선택하여 정책을 생성합니다. 이때 파일은 파일 확장자, 크기 또는 수정한 날짜를 기준으로 필터링될 수 있습니다. 도출된 검색 결과에는 선택한 규정을 준수하지 않는 데이터 센터, 클러스터, 가상 머신 및 파일 이름을 식별하는 정보가 포함됩니다. 마지막으로 관리자는 REST(Representational State Transfer) API를 사용하여 이같이 규정을 준수하지 않는 파일을 올바르게 수정합니다.

vShield App는 각 vSphere 호스트에 설치되어 해당 호스트의 모든 네트워크 트래픽은 물론, 물리적 NIC(Network Interface Card)를 절대 통과하지 않는 패킷에 대해서도 제어 및 모니터링을 제공합니다. 이 제품은 애플리케이션 구축에 관한 정적인 가정 또는 물리적 경계 대신 관리자가 정의한 비즈니스별 정의 그룹에 기반하여 정책을 생성 및 적용합니다.

또한 vCenter Server를 활용하는 중앙 집중식 인터페이스를 제공하여 가상 데이터 센터 내의 여러 vSphere 호스트에 이러한 정책을 일관적으로 적용할 수 있도록 합니다.

vShield App with Data Security의 기능

- **가상화된 호스트에 대한 데이터 규정 준수 감사 충족** – 관리자는 REST API를 통해 직접 또는 프로그래밍 방식으로 검색을 수행하여 선택한 정책에 대한 준수 여부를 검증합니다.
- **제공된 템플릿** 중에서 선택하여 검색을 수행할 가상화된 특정 리소스에 적용되는 정책을 구성할 수 있습니다.
- **민감한 정보에 대한 검색 결과 데이터**는 규정을 준수하지 않는 가상 머신을 파악하고 차단하는 데 사용할 수 있습니다.
- **애플리케이션을 인식하는 보호 제공** – 가상 NIC를 통과하는 모든 트래픽에 대한 세분화된 정책을 정의하고 적용하여 내부 가상 데이터 센터 트래픽을 훨씬 심층적으로 파악할 수 있으며 동시에 물리적 방화벽으로 우회할 필요가 없습니다.
- **변경 인식 보호 기능 유지** – 가상 머신을 호스트 간에 마이그레이션할 때에도 방화벽 보호 기능을 지속적으로 작동시켜 네트워크 토폴로지의 변경이 애플리케이션 보안에 영향을 미치지 않도록 합니다.
- **효율적인 동적 정책 관리** – 시간이 지나면서 계속 변화하는 비즈니스 요구 사항을 충족할 수 있도록 관리자에게 내부 방화벽 정책에 대한 정의 및 재정의와 관련된 풍부한 컨텍스트를 제공합니다.
- **봇넷 위험 감소** – 보안 관리자는 신뢰할 수 있는 애플리케이션으로 포트를 동적으로 할당하여 봇넷 및 기타 공격으로부터 안전하게 보호할 수 있습니다.
- **공유 리소스에 대한 보안 허용** – 보안 관리자는 vSphere 호스트상의 공유 서비스(예: 스토리지, 백업)에 대한 액세스를 IP 주소에 따라 제한할 수 있습니다.
- **IT 규정 준수 촉진** – 기업이 내부 정책과 외부 규정 요구 사항의 준수를 입증하기 위해 로깅 및 감사 제어를 사용하여 가상 머신 네트워크 보안을 더욱 심층적으로 파악하고 제어합니다.

주요 특징

민감한 정보 검색

- 정책 기반 콘솔로 관리자가 규정 준수 검색에 사용할 규정을 선택할 수 있습니다.
- 조직은 PII(Personally Identifiable Information), PCI-DSS 카드 소지자 정보, PHI(Protected Health Information), 기타 전 세계(북미, EMEA, 아시아 태평양) 규정을 포함한 80여 개의 규정 템플릿에서 원하는 템플릿을 선택할 수 있습니다.
- 결과 보고서로 선택한 규정을 준수하지 않는 데이터가 포함된 리소스를 파악할 수 있습니다.
- REST API 또는 운영자 콘솔을 사용하여 기능을 프로그래밍할 수 있습니다.
- 감염된 가상 머신은 VMware vCenter Configuration Manager를 통해 차단 및 해결됩니다.

방화벽

- 하이퍼바이저 수준의 방화벽은 하이퍼바이저 검사를 통해 가상 NIC 수준에서 적용되는 인바운드/아웃바운드 연결 제어를 제공하는 방식으로 멀티 홈 가상 머신을 지원합니다.
- 계층 2 방화벽(투명 방화벽이라고도 함)은 암호 스니핑, DHCP 스누핑, ARP(Address Resolution Protocol) 스푸핑, 감염 공격 등의 다양한 유형의 공격으로부터 보호합니다. 또한 SNMP 트래픽에 대한 완벽한 격리 기능도 제공합니다.
- 네트워크, 애플리케이션 포트, 프로토콜 유형(TCP, UDP) 또는 애플리케이션 유형에 따라 보호를 적용할 수 있습니다.
- 가상 머신을 마이그레이션과 동시에 동적으로 보호합니다.
- IP 기반의 상태 방화벽과 애플리케이션 계층 게이트웨이는 Oracle, Sun RPC(Remote Procedure Call), Microsoft RPC, LDAP, SMTP 등의 광범위한 프로토콜을 지원합니다. 또한 이 게이트웨이는 필요한 세션(포트)만을 열어 보안을 강화합니다. 지원되는 프로토콜의 전체 목록은 VMware vShield 관리 가이드를 참조하십시오.

플로우 모니터링

- 관리자는 가상 머신 간의 네트워크 활동을 관찰하여 방화벽 정책을 정의/재정의하고, 봇넷을 파악하고, 애플리케이션 트래픽(애플리케이션, 세션 및 바이트) 상세 보고를 통해 비즈니스 프로세스를 강화할 수 있습니다.

보안 그룹

- 관리자는 가상 NIC를 기준으로 모든 가상 머신에 대한 비즈니스별 그룹을 정의할 수 있습니다.

정책 관리

- vShield Manager는 제품 기능을 제어하는 다양한 기능을 제공하며, 이 중 상당수의 기능은 vCenter Server 인터페이스를 통해서도 액세스할 수 있습니다.
- 관리자는 보안 그룹, vCenter Server 그룹화 및 TCP-5 튜플(소스 IP, 대상 IP, 소스 포트, 대상 포트 및 프로토콜)에 대한 정책을 적용할 수 있습니다.
- REST API를 통해 관리 및 정책 적용을 위한 프로그래밍 가능한 인터페이스를 제공합니다.
- 이 제품은 엔터프라이즈 보안 관리 툴과의 통합을 지원합니다.

IP 주소 지정

- 프로비저닝을 단순화하기 위해 동일한 IP 주소를 여러 테넌트 영역에 사용하는 등 유연하게 IP 주소를 지정할 수 있습니다.

로깅 및 감사

- 업계 표준 syslog 형식을 기반으로 로깅을 수행합니다.
- REST API와 vShield Manager로 로깅 및 감사 툴에 액세스합니다.
- 관리자는 규칙 수준에서 방화벽의 로깅 설정/해제를 정의할 수 있습니다.

지원되는 릴리스

vSphere 환경에 지원되는 릴리스에 대한 자세한 내용은 http://www.vmware.com/products를 참조하십시오.

관련 제품

vShield 보안 제품군에는 경계 보안을 제공하는 VMware vShield Edge, 강화된 엔드포인트 보안과 성능을 제공하는 VMware vShield Endpoint, vShield Manager 그리고 이 모든 제품이 포함된 vShield Bundle이 있습니다.

추가 정보

자세한 정보를 찾거나 VMware 제품을 구입하려면 1-877-4-VMWARE(한국 지사 (02) 6001-3890)로 전화하거나 http://www.vmware.com/products를 방문하거나 인증된 재판매자를 온라인으로 검색하십시오. 제품 규격 및 시스템 요구 사항에 대한 자세한 내용은 VMware vShield 관리 가이드 (http://www.vmware.com/pdf/vshield_41_admin.pdf)를 참조하십시오.

vShield 제품에 대한 자세한 내용은 http://www.vmware.com/products에서 확인하십시오.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
VMware, Inc. 서울시 강남구 삼성동 159-1번지 아셈타워 37층 (우) 135-798 전화: (02) 6001-3890 e-메일: korea-sales@vmware.com