VMware vShield Bundle

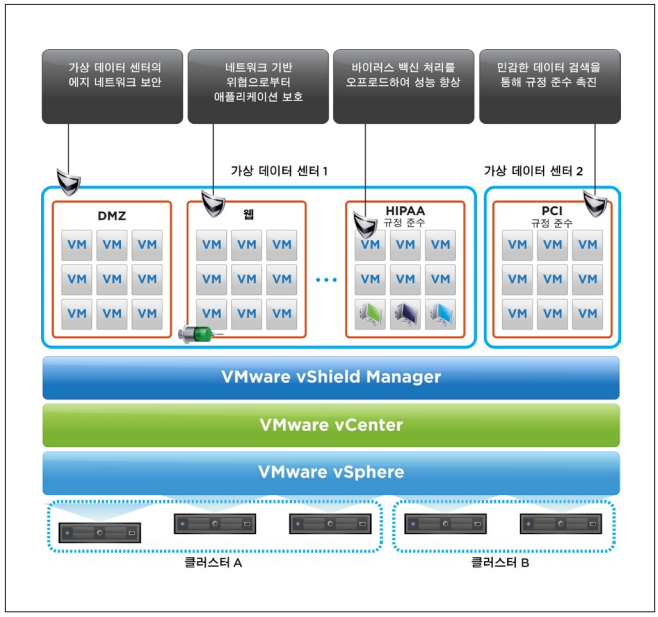
신뢰할 수 있는 클라우드 인프라를 위한 기반

요약 정보

VMware vShield™ Bundle은 신뢰할 수 있는 클라우드 인프라를 위한 기반입니다. vShield Bundle은 네트워크 에지, 애플리케이션, 데이터, 엔드포인트 등 모든 수준의 가상 데이터 센터와 클라우드 환경을 보호하는 비용 효율적이고 적응력이 뛰어난 통합 보호 서비스 및 관리를 제공합니다. vShield Bundle은 VMware vSphere®, VMware vCenter™ Server 및 VMware vCloud™ Director와 연동됩니다.

주요 장점

- 네트워크 에지, 애플리케이션, 데이터, 엔드포인트 등 모든 수준의 가상 데이터 센터와 클라우드 환경 보호
- 비용과 복잡성 감소
- 구축 시 에이전트가 필요 없어 바이러스 백신과 맬웨어 방지 "과부하" 해소
- 민감한 데이터 검색을 통해 규정 미준수 위험 및 명성 손상 감소
- 맞춤형 신뢰 영역으로 공통적인 보안 정책 및 액세스 요구 사항을 가진 애플리케이션과 데이터를 그룹화



VMware vShield는 보안 그룹을 사용하여 세분화된 정책 적용을 수행합니다.

VMware vShield Bundle 기능에 대한 개요

vShield Bundle은 가상화된 데이터 센터에 물리적 보안보다 더욱 뛰어난 보안을 제공합니다. 이 번들은 네 가지 vShield 제품의 고급 기능을 모두 포함하고 있으며, 이를 통해 네트워크 에지에서 애플리케이션 및 데이터 그리고 엔드포인트에 이르는 다양한 가상 데이터 센터와 클라우드 환경을 보호하는 비용 효율적이고 적응력이 뛰어난 통합 보호 서비스 및 관리를 제공합니다.

네트워크 에지

vShield Bundle은 가상 데이터 센터 경계 영역을 보호하는 에지 네트워크 보안 솔루션과 함께 네트워크 보호 게이트웨이 서비스 및 웹 로드 밸런싱과 같은 필수적인 보안 기능을 제공하여 성능과 가용성을 보장합니다. 이 솔루션은 VMware vSphere로 직접 연결할 수 있으며 탁월한 유연성을 제공하기 위해 Fault Tolerance, 고가용성 등의 기본 제공 기능을 활용합니다.

또한 vShield Bundle은 VMware vCloud Director와 연동되어 멀티 테넌트 클라우드 인프라 내의 가상 데이터 센터에 대한 안전한 프로비저닝을 자동화 및 가속화합니다. 동시에, 보안 및 가상 인프라 관리자의 업무를 구분하여 인증된 리소스에게만 액세스를 허용합니다.

가상 어플라이언스로 구축되는 vShield Bundle은 방화벽, VPN(Virtual Private Network), 웹 로드 밸런싱 장치, NAT(네트워크 주소 변환), DHCP(Dynamic Host Configuration Protocol) 서비스와 같은 네트워크 보안 게이트웨이 기능을 제공하여 소스 및 대상 IP 주소에 대한 패킷 헤더를 모니터링합니다. 또한 정책에 따라 연결을 거부 또는 허용하고, VPN 세션을 실행 또는 종료하며, 네트워크 주소 변환을 수행하고, 소스-대상 포트와 프로토콜 유형([TCP](Transmission Control Protocol) 또는 [UDP](User Datagram Protocol))별로 데이터를 검사할 수 있습니다.

애플리케이션 및 데이터

vShield Bundle은 가상 데이터 센터를 위한 하이퍼바이저 기반의 애플리케이션 인식 방화벽 솔루션을 제공합니다. 또한 가상 머신 컨테이너에 상주하는 구조화되지 않은 데이터 파일에 저장된 신용카드 정보와 같이 민감한 데이터를 동적으로 검색할 수 있습니다. 따라서 관리자는 데이터 센터, 클러스터 또는 리소스 풀에서 민감한 데이터가 존재하는지 여부를 검색할 수 있어 규정 준수 감사를 충족할 수 있습니다.

이 제품은 vSphere에 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 관리자가 비즈니스별 보안 그룹을 신속하게 생성할 수 있도록 하여 정책 제어를 간소화합니다. vShield Bundle은 애플리케이션 구축에 관한 정적인 가정 또는 물리적 경계 대신, 관리자가 정의한 비즈니스별 정의 그룹에 기반하여 정책을 생성 및 적용합니다. 여기에는 가상 머신 네트워크 트래픽을 분석하고 보안 그룹 정책을 동적으로 적용하는 플로우 모니터링이 포함됩니다.

vShield Bundle은 민감한 데이터 검색 정책을 관리할 수 있는 관리자 콘솔을 제공합니다. "정책"은 대상 가상 머신 컨테이너(데이터 센터, 클러스터, 리소스 풀 등) 전체에 검색할 관련 규정을 선택하여 생성됩니다. 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.

엔드포인트

엔드포인트 솔루션은 혁신적인 아키텍처 방식을 사용하여 바이러스 백신, 민감한 데이터 검색 및 VMware 파트너가 제공하는 vSphere 및 VMware View™ 환경용 기타 엔드포인트 보안 기능을 최적화합니다.

vShield Bundle은 바이러스 백신 구축을 위해 바이러스 백신 검색 활동을 저장된 바이러스 백신 파일 서명과 검색 엔진을 제공하는 보안 가상 어플라이언스로 오프로드하여 성능을 향상시킵니다. 바이러스 백신 및 맬웨어 방지 기능을 지원하기 위해 이 아키텍처는 가상 머신 내 소프트웨어 에이전트의 설치 공간을 줄여 시스템 리소스에 여유를 주고 성능을 개선하며 바이러스 백신의 "과부하"(예정된 검색 및 서명 업데이트를 수행하는 동안 리소스에 너무 많은 부하가 발생)를 방지합니다. 보안 가상 어플라이언스는 오프라인 상태가 되지 않으므로 바이러스 백신 서명을 지속적으로 업데이트할 수 있어 결과적으로 호스트의 가상 머신이 중단 없이 지속적으로 보호됩니다. 새로운 가상 머신 또한 최신 바이러스 백신 서명으로 즉시 보호됩니다. 특히 vShield Bundle을 사용하는 가상 인프라 관리자는 각 가상 머신에 관리해야 할 바이러스 백신 에이전트가 없어 업무량이 대폭 줄어듭니다. 대신 관리자는 파트너의 관리 콘솔을 사용하여 보안 가상 어플라이언스를 관리할 수 있습니다. 이 방식을 사용하면 각 가상 머신에 대해 업데이트를 자주 수행할 필요가 없습니다.

vShield Bundle은 vSphere의 강력하고 안전한 하이퍼바이저 자체 검사 기능을 활용하는, 강력하고 부정 조작이 불가능한 보안 가상 어플라이언스(VMware 파트너에서 제공)로 더욱 향상된 보안 기능을 제공함으로써 바이러스 백신과 맬웨어 방지 서비스 자체의 취약성을 개선합니다.

vShield Bundle은 또한 VMware 파트너에게 파일, 메모리 및 프로세스 검색을 구축할 수 있는 인터페이스를 제공합니다. 이 아키텍처는 한 보안 가상 어플라이언스에서는 민감한 데이터를 검색하고 또 다른 보안 가상 어플라이언스에서는 바이러스 백신 솔루션을 검색하는 등 여러 보안 솔루션을 동시에 지원합니다.

조직은 바이러스 백신 및 맬웨어 방지 서비스에 대한 상세 활동 로깅을 통해 규정 준수를 입증하고 감사 요구 사항을 만족할 수 있습니다.

관리

관리자는 함께 포함된 관리 콘솔인 vShield Manager를 통해 vShield Bundle을 중앙 집중식으로 관리합니다. vShield Manager는 VMware vCenter Server와 긴밀하게 통합되어 가상 데이터 센터에 대한 통합 보안 관리를 보조합니다.

vShield Bundle의 기능

vShield Bundle은 모든 수준에서의 클라우드 환경과 가상 데이터 센터를 보호하는 보안 서비스 및 관리를 제공하기 위해 구축됩니다.

네트워크 에지

vShield Bundle은 다음을 위한 필수 기능을 제공하는 포괄적인 에지 네트워크 게이트웨이 보안 솔루션을 제공합니다.

- **에지 보안 하드웨어 통합** – 기존의 vSphere 리소스를 사용하여 에지 보안 서비스를 프로비저닝하기 때문에 vSphere 호스트 간에 "에어 갭"을 적용하기 위해 별도의 특수 하드웨어 장치가 필요하지 않습니다.
- **가상 데이터 센터 경계를 신속하고 안전하게 프로비저닝** – 하드웨어에 독립적인 보안 논리적 경계("에지")를 가상 데이터 센터 환경 주위로 간단하게 생성하여 멀티 테넌트 IT 인프라 내의 공유 네트워크 리소스를 더욱 쉽게 활용할 수 있습니다.
- **공유 네트워크상의 데이터에 대한 완벽한 보안 유지** – 256비트 암호화와 함께 사이트 간 VPN을 제공하여 여러 가상 데이터 센터 사이에서 전송되는 모든 데이터의 보안을 완벽하게 유지합니다.
- **웹 서비스의 성능과 가용성 보장** – 가상 머신 클러스터 전체에 발생하는 인바운드 웹 트래픽을 효과적으로 관리하고 에지 보안과 함께 또는 자체적으로 구축 가능한 웹 트래픽 로드 밸런싱 기능을 제공합니다.
- **규정 준수 관리 지원** – 상세 이벤트 로깅, 플로우 통계 등 업계 및 정부 규정과 기업 정책에 대한 준수 사실을 입증하기 위해 필요한 제어 기능을 구축합니다.

애플리케이션 및 데이터

vShield Bundle에는 다음 용도로 사용 가능한 애플리케이션 인식 방화벽이 포함되어 있습니다.

- **가상화된 호스트에 대한 데이터 규정 준수 감사 충족** – REST API를 통해 직접 또는 프로그래밍 방식으로 검색을 수행하여 선택한 정책에 대한 준수 여부를 검증합니다.
- **애플리케이션 인식 보호 기능 제공** – 가상 NIC(네트워크 인터페이스 카드)를 통과하는 모든 트래픽에 대한 세분화된 정책을 정의하고 적용하여 내부 가상 데이터 센터 트래픽을 훨씬 심층적으로 파악할 수 있으며 물리적 방화벽으로 우회할 필요가 없어집니다.
- **변경 인식 보호 기능 유지** – 가상 머신을 호스트 간에 마이그레이션할 때에도 이에 대한 지속적인 방화벽 보호 기능을 구축하여 네트워크 토폴로지의 변경이 애플리케이션 보안에 영향을 미치지 않도록 합니다.
- **효율적인 동적 정책 관리** – 정책 정의를 간소화하고 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** – 신뢰할 수 있는 애플리케이션으로 포트를 동적으로 할당하여 봇넷 및 기타 공격으로부터 안전하게 보호합니다.
- **공유 리소스에 대한 보안 허용** – 보안 관리자가 vSphere 호스트상의 공유 서비스(예: 스토리지, 백업)에 대한 액세스를 IP 주소에 따라 제한할 수 있도록 지원합니다.
- **IT 규정 준수 촉진** – 내부 정책과 외부 규정 요구 사항의 준수를 입증하기 위해 필요한 로깅 및 감사 컨트롤을 사용하여 가상 머신 네트워크 보안을 더욱 심층적으로 파악하고 제어합니다.

엔드포인트

vShield Bundle에는 다음을 지원하는 엔드포인트 기능이 포함되어 있습니다.

- **바이러스 백신 및 맬웨어 보호 구축 간소화** – 엔터프라이즈 바이러스 백신 엔진과 서명 파일을 vSphere 호스트상의 모든 개별 가상 머신에 구축할 필요 없이 하나의 보안 가상 어플라이언스에 간단하게 구축합니다.
- **가상 머신 성능 개선** – 바이러스 백신 및 맬웨어 방지 에이전트 검색 등의 활동을 각 가상 머신에서 각 vSphere 호스트의 단일 보안 가상 어플라이언스로 오프로드하여 통합률을 더욱 확실하게 높여줍니다.
- **바이러스 백신 "과부화" 방지 및 병목 현상 해소** – 바이러스 백신과 맬웨어 방지 검색 및 업데이트를 단일 가상 어플라이언스에 구축하여 바이러스 백신이 "과부화"되거나 병목 현상이 발생하는 일이 없도록 합니다.
- **각종 공격으로부터 바이러스 백신 보호 소프트웨어 보호** – 강력한 보안 가상 어플라이언스 내의 바이러스 백신 및 맬웨어 방지 클라이언트 소프트웨어를 구축하고 실행하여 바이러스 백신과 맬웨어 방지 솔루션을 노리는 각종 공격으로부터 보호합니다.

주요 특징

vShield Bundle에는 다음과 같은 핵심 기능과 구성 요소가 제공됩니다.

네트워크 에지

방화벽

- NAT(네트워크 주소 변환)가 필요 없는 경계(계층 3) 방화벽
- 다음을 기준으로 인바운드/아웃바운드 연결 제어 규칙을 사용하는 상태 추적 방화벽
  - IP 주소 – 소스/대상 IP 주소
  - 포트 – 소스/대상 포트
  - 프로토콜 – 유형(TCP 또는 UDP)

NAT(네트워크 주소 변환)

- 가상화된 환경 내외부로 IP 주소 변환
- 신뢰할 수 없는 위치에 대해 가상 데이터 센터 IP 주소를 마스커레이딩

DHCP(Dynamic Host Configuration Protocol)

- vSphere 환경 내의 가상 머신으로 자동 IP 주소 프로비저닝
- 관리자 정의 매개 변수(예: 주소 풀, 리스 기간, 전용 IP 주소)

사이트 간 VPN

- 가상 데이터 센터(또는 에지 보안 가상 머신) 간 안전한 커뮤니케이션
- IKE(Internet Key Exchange) 프로토콜에 기반하여, 공유 키와 인증서 인증을 지원하는 IPsec(Internet Protocol Security) VPN

웹 로드 밸런싱

- 웹 트래픽(HTTP)을 비롯한 모든 트래픽에 대한 인바운드 로드 밸런싱
- 라운드 로빈 알고리즘
- 세션 라우팅(sticky session)

에지 플로우 통계

- 가상 데이터 센터 리소스 활용도를 측정하고 테넌트로 다시 귀속시킵니다.
- 통계가 REST API를 통해 액세스되고 서비스 공급업체 차지백 애플리케이션에서 활용됩니다.

정책 관리

- vShield Manager를 통해 완전한 기능으로 관리 수행(상당수의 기능이 vCenter Server 인터페이스를 통해서도 액세스 가능)
- REST API를 사용하는 맞춤형 관리용 인터페이스
- 엔터프라이즈 IT 보안 관리 툴 지원

로깅 및 감사

- 업계 표준 syslog 형식 기반
- REST API 및 vShield Manager 사용자 인터페이스를 통해 액세스 가능
- 주요 에지 보안 이벤트(오류, 경고 등)에 대한 관리자 정의 로깅 설정/해제
  - 방화벽: 규칙 수준에서 실행
  - NAT: 규칙 수준에서 실행
  - VPN: 사이트 간 연결 이름
  - 웹 로드 밸런싱 장치: 풀 수준에서, URL 또는 폴더를 포함한 웹 요청에 따라 실행
  - DHCP: 서비스 수준, 바인딩(릴리스와 갱신)에 따라 실행

애플리케이션 및 데이터

민감한 정보 검색

- 정책 기반 콘솔로 관리자가 규정 준수 검색에 사용할 규정을 선택할 수 있습니다.
- PII(Personally Identifiable Information), PCI-DSS(PCI-Data Security Standard) 카드 소지자 정보, PHI(Protected Health Information) 및 기타 전 세계(북미, EMEA, 아시아 태평양) 규정 등 80개 이상의 규정 템플릿을 제공합니다.
- 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 등 다양한 유형의 공격으로부터 보호합니다. 또한 SNMP(Simple Network Management Protocol) 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(Lightweight Directory Access Protocol), SMTP 등의 광범위한 프로토콜을 지원하며 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.
- 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.
- 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.

엔드포인트

바이러스 백신 및 맬웨어 방지 오프로드

- vShield Bundle ESX 모듈을 통해 바이러스 검색 활동을 저장된 바이러스 백신 파일 서명과 검색 엔진을 제공하는 보안 가상 어플라이언스로 오프로드합니다.
- 파일, 메모리, 프로세스 검색 및 기타 작업이 씬 클라이언트 에이전트와 파트너 ESX 모듈을 통해 가상 머신에서 보안 가상 어플라이언스로 오프로드됩니다.
- EPsec(Endpoint Security)는 하이퍼바이저 계층에서 자체 검사 기능을 사용하여 가상 머신과 보안 가상 어플라이언스 간의 커뮤니케이션을 관리합니다.
- 바이러스 백신 엔진과 서명 파일은 보안 가상 어플라이언스 내부에서만 업데이트되지만, 정책(관리자 정의된 규정)은 vSphere상의 모든 가상 머신에 적용될 수 있습니다.

보안 가상 어플라이언스에 의해 문제 해결 시작

- 파트너의 바이러스 백신 엔진 정책을 보유하여 악성 파일의 삭제, 차단 또는 기타 처리를 결정합니다.
- 가상 머신 내의 파일 문제 해결 활동에 씬 클라이언트를 사용합니다.

파트너 통합

- vShield Bundle EPsec API를 사용하여 하이퍼바이저 계층을 통해 파일 활동을 자체 검사함으로써 VMware 파트너가 제공하는 보안 가상 어플라이언스 솔루션과의 통합을 지원합니다.

vShield Manager, 정책 관리 및 자동화

- 엔드포인트 구축에 대한 완전한 기능을 갖춘 구성 제공
- REST API를 사용하여 엔드포인트 기능을 솔루션 내로 자동으로 맞춤형 통합
  - 모니터링 보고서 제공
  - vShield Manager를 vCenter 플러그인으로 활용 가능

로깅 및 감사

- 업계 표준 syslog 형식을 기반으로 이벤트 로깅

지원되는 릴리스

vSphere, ESX 및 VMware View 환경에 지원되는 릴리스에 대한 자세한 내용은 http://www.vmware.com/products를 참조하십시오.

관련 제품

이 밖에도 vShield 보안 제품군에는 경계 보안을 제공하는 vShield Edge, 네트워크 기반 공격으로부터 애플리케이션을 보호하고 민감한 데이터를 검색하는 vShield App with Data Security, 엔드포인트 보안과 가상 데이터 센터의 성능을 강화하는 vShield Endpoint 및 vShield Manager가 있습니다. vShield Bundle은 vShield Edge, vShield App with Data Security, vShield Endpoint 및 vShield Manager로 구성됩니다.

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.

vShield Bundle의 구성

- **vShield Edge** — 가상 데이터 센터 경계를 보호하는 네트워크 게이트웨이 솔루션입니다.
- **vShield App with Data Security** — vShield App에 민감한 데이터를 동적으로 검색하는 기능을 추가하여 규정 준수 감사를 지원합니다.
- **vShield Endpoint** — 바이러스 백신 및 맬웨어 방지 에이전트 처리를 전용 보안 가상 어플라이언스로 오프로드하여 가상 머신에 대한 보안을 강화하고 엔드포인트 보호 성능을 개선합니다.
- **vShield Manager** — 타사 보안 서비스에 대한 관리, 구축, 보고, 로깅 및 통합을 중앙에서 제어합니다.

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
Copyright © 2011 VMware, Inc. All rights reserved. 본 제품은 미국 및 국제 저작권 및 지적 재산권 법률의 보호를 받습니다. VMware 제품은 여러 건의 특허 보호 대상이며 일부는 특허 출원 중입니다. 자세한 내용은 웹사이트(http://www.vmware.com/go/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-DS-vSHLD-BUNDLE-A4-102_KR