# VMware vShield Endpoint

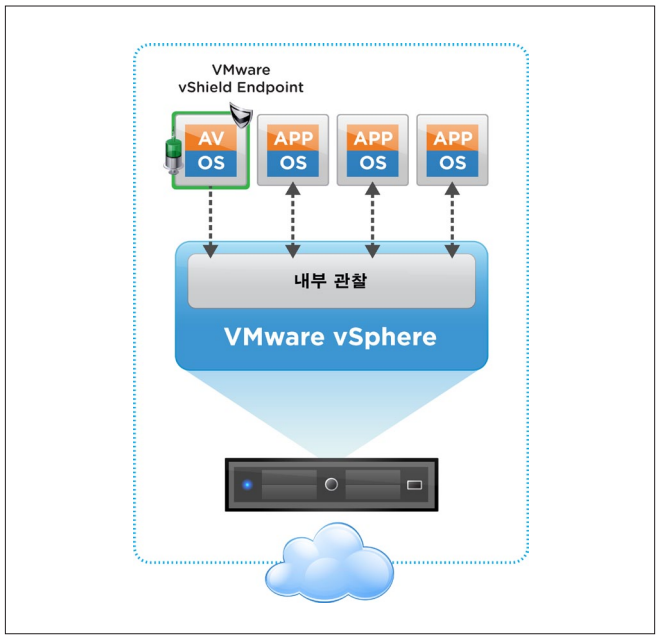
## 가상 데이터 센터를 위한 향상된 엔드포인트 보안 및 성능

### 요약 정보

VMware vShield™ Endpoint는 엔드포인트 보호 성능을 대폭 개선하고 동시에 가상 머신의 보안을 강화합니다. vShield Endpoint는 바이러스 백신 및 맬웨어 방지 에이전트 처리를 VMware 파트너가 제공하는 전용 보안 가상 어플라이언스로 오프로드합니다. 이 솔루션을 사용하는 고객은 물리적 환경 보안에 사용하는 관리 인터페이스와 동일한 인터페이스를 사용하여 가상화된 환경에 대한 바이러스 백신 및 맬웨어 방지 정책을 관리할 수 있어 기존 투자도 활용할 수 있습니다.

### 주요 장점

- 게스트 가상 머신에 바이러스 백신 에이전트가 필요 없어 통합 비율과 성능 향상
- VMware 환경 내에서 바이러스 백신과 맬웨어 방지를 더욱 손쉽게 구축 및 모니터링
- 바이러스 백신 소프트웨어 에이전트 통합을 통해 공격 범위를 축소하여 보안 강화
- 바이러스 백신 및 맬웨어 방지 활동을 로깅하여 규정 준수 및 감사 요구 사항 충족




vShield Endpoint는 가상화된 환경 내에서 바이러스 백신 및 맬웨어 방지를 위한 통합 비율과 성능을 향상시켜 줍니다.

# vShield Endpoint 개요

vShield Endpoint는 바이러스와 맬웨어로부터 게스트 가상 머신을 보호하는 기존의 방식을 혁신적으로 바꾼 솔루션으로, VMware vSphere® 및 VMware View™ 환경용 바이러스 백신 및 기타 엔드포인트 보안을 최적화합니다.

vShield Endpoint는 각 가상 머신의 바이러스 검색 활동을 저장된 바이러스 백신 서명과 검색 엔진을 제공하는 보안 가상 어플라이언스로 오프로드하여 성능을 향상시킵니다. 바이러스 백신 및 맬웨어 방지 기능을 지원하기 위해 이 아키텍처는 게스트 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. 게스트 가상 머신과는 달리, 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(또는 오프라인 상태였던 기존의 가상 머신) 또한 최신 바이러스 백신 서명으로 온라인 상태가 되는 즉시 보호됩니다.

vShield Endpoint는 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 Endpoint는 또한 VMware 파트너에게 파일 검색은 기본이고 메모리와 프로세스까지도 검색할 수 있는 인터페이스를 제공합니다. 따라서 조직은 한 보안 가상 어플라이언스에서는 VMware vShield App with Data Security에서 제공하는 민감한 데이터 검색 기능을 사용하면서 동시에 또 다른 보안 가상 어플라이언스에서는 바이러스 백신 솔루션을 사용하는 등 여러 보안 솔루션을 동시에 사용할 수 있습니다.

바이러스 백신 및 맬웨어 방지 서비스에 대한 상세 활동 로깅을 통해 규정 준수를 입증하고 감사 요구 사항을 만족할 수 있다는 점은 조직이 누릴 수 있는 또 하나의 혜택입니다.

관리자는 VMware vCenter™ Server에 매끄럽게 통합되어 가상 데이터 센터의 보안 관리 통합을 촉진하는 vShield Manager 콘솔을 통해 중앙에서 vShield Endpoint를 관리할 수 있습니다.

# vShield Endpoint의 작동 방식

vShield Endpoint는 vSphere에 직접 연결 가능하며 다음 세 가지 구성 요소로 구성됩니다.

- VMware 파트너에서 제공하는 강력한 보안 가상 어플라이언스
- 보안 이벤트 오프로드를 지원하는 가상 머신용 씬 에이전트(VMware Tools에 포함)
- VMware Endpoint ESX® 하이퍼바이저 모듈로 하이퍼바이저 계층의 맨 처음 두 구성 요소 간의 커뮤니케이션 실행

한 예로 바이러스 백신 솔루션의 경우, vShield Endpoint는 가상 머신 파일 이벤트를 모니터링하고 바이러스 백신 엔진에게 모니터링 상황을 알려 이를 검색하고 배치합니다. 이 솔루션은 액세스 시 그리고 필요 시(예정된) 보안 가상 어플라이언스 내에 존재하는 바이러스 백신 엔진이 파일 검색을 시작할 수 있도록 지원합니다.

파일에 대한 문제 해결이 필요할 경우에 관리자는 기존의 바이러스 백신 및 맬웨어 방지 관리 툴을 사용하여 수행할 조치를 지정할 수 있으며, vShield Endpoint는 영향을 받는 가상 머신 내에서 문제 해결 조치를 관리합니다.

# vShield Endpoint의 기능

VMware 파트너가 제공하는 관리 콘솔은 보안 가상 어플라이언스에서 호스트되는 파트너의 소프트웨어를 구성 및 제어하는 데 사용됩니다. 따라서 VMware 파트너는 사용자에게 전용 물리적 보안 어플라이언스에서 호스트되는 소프트웨어를 관리할 때와 동일한 관리 환경(정책 관리 포함)을 지원하는 인터페이스를 제공할 수 있습니다.

가상 인프라 관리자는 가상 머신에 관리해야 할 백신 에이전트가 없어 업무량이 대폭 감소하게 되며 대신, 파트너의 관리 콘솔을 사용하여 보안 가상 어플라이언스를 관리할 수 있습니다. 이 방식을 사용하면 각 가상 머신에 대해 업데이트를 자주 수행할 필요가 없습니다. 이 밖에도 VMware Tools에서는 씬 에이전트를 제공하고 ESX 모듈은 하이퍼바이저 자체 검사 기능을 실행하여 구축 작업을 돕습니다.

가상 인프라 관리자는 구축 상태를 쉽게 모니터링할 수 있어 바이러스 백신 솔루션이 정상 작동하고 있는지 등을 파악할 수 있습니다.

# 주요 특징

## 바이러스 백신 및 맬웨어 방지 오프로드

- vShield Endpoint는 vShield Endpoint ESX 모듈을 사용하여 바이러스 검색 활동을 바이러스 백신 검색이 실행되는 보안 가상 어플라이언스로 오프로드하여 성능을 향상시킵니다.
- 파일, 메모리, 프로세스 검색이 씬 클라이언트 에이전트와 파트너 ESX 모듈을 통해 가상 머신에서 보안 가상 어플라이언스로 오프로드됩니다.
- vShield Endpoint EPSEC는 하이퍼바이저 계층에서 자체 검사 기능을 사용하여 가상 머신과 보안 가상 어플라이언스 간의 커뮤니케이션을 관리합니다.
- 바이러스 백신 엔진과 서명 파일은 보안 가상 어플라이언스 내부에서만 업데이트되지만, 정책은 vSphere상의 모든 가상 머신에 적용될 수 있습니다.

## 패치 적용

- vShield Endpoint는 바이러스 백신 정책을 적용하여 악성 파일의 삭제, 차단 또는 기타 처리를 결정합니다.
- 씬 클라이언트가 가상 머신 내의 파일 문제 해결 활동을 관리합니다.

## 파트너 통합

- EPSEC API를 사용하면 하이퍼바이저 내의 파일 활동을 자체 검사하여 VMware 바이러스 백신 파트너를 vShield Endpoint와 통합할 수 있습니다. 기본적인 바이러스 백신 기능은 이 API를 통해 지원됩니다.

## vShield Manager, 정책 관리 및 자동화

- vShield Manager는 vShield Endpoint에 대한 완전한 구축 및 구성 기능을 제공합니다.
- REST(Representational State Transfer) API를 사용하여 vShield Endpoint 기능을 솔루션 내로 자동으로 맞춤형 통합할 수 있습니다.
- 모니터링 보고서를 제공합니다.
- vShield Manager를 vCenter 플러그인으로 활용할 수 있습니다.

## 로깅 및 감사

- 업계 표준 syslog 형식을 기반으로 이벤트를 로깅합니다.

## 지원되는 릴리스

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

## 관련 제품

이 밖에도 vShield 제품군에는 경계 보안을 제공하는 VMware vShield Edge, 네트워크 기반 공격으로부터 애플리케이션을 보호하고 민감한 데이터를 검색하는 vShield App with Data Security, 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