데이터시트

Symantec Endpoint Protection 14

클라우드 세대를 위한 업계 최고의 통합 엔드포인트 보안 솔루션

개요

단일 에이전트 아키텍처에서 업계 최고의 효율성을 발휘하면서 모든 공격 경로로부터 엔드포인트 보호

- 첨단 머신 러닝, 행위 분석, 익스플로잇 차단과 같은 시그니처리스(signatureless) 기술과 침입 차단, 평판 분석 등 검증된 보호 기능을 융합한 다계층 보호 솔루션으로 랜섬웨어 및 기타 신종 보안 위협 차단
- 보다 현명한 정책 결정을 지원하기 위해 튜닝 가능한 보호 기능으로 의심스러운 파일을 보다 면밀하게 모니터링
- 디셉션 기술로 숨어 있는 공격자와 그 의도를 밝혀 차원 높은 보안 실현
- 널리 사용되는 애플리케이션을 취약점 익스플로잇으로부터 보호하고 의심스러운 애플리케이션을 격리하여 악성 활동 차단

대규모의 통합 사이버 방어 체계 구축

- 웹 및 이메일 게이트웨이와 같은 네트워크 보안 인프라스트럭처와의 통합으로 어디서나 보안 위협 탐지, SEP와 연계하여 대응
- EDR과의 통합을 지원하므로 SEP 에이전트를 그대로 활용하면서 침해 사고 조사 및 대응
- 기존 IT 인프라스트럭처와의 통합으로 개방형 API를 통한 자동화 및 조정 지원

유연한 고성능 솔루션으로 비즈니스 지원

- 네트워크 대역폭 제약이 있는 엔드포인트의 경우 보안 효율성 저하 없이 컨텐트 업데이트 빈도 최적화
- SEP12 대비 70% 감축된 최소한의 네트워크 대역폭만 사용하는 경량화 에이전트 및 바이러스 정의 세트로 성능 향상
- 첨단 설계 기술 및 실시간 클라우드 조회 특허 기술을 사용하여 SEP12 대비 15% 향상된 검사 속도로 신속하게 탐지

소개

끊임없이 진화하는 IT 환경의 특성으로 인해 공격자들은 보다 정교한 공격 수법으로 네트워크 침투를 시도하고 있으며, 엔드포인트는 이러한 공격에 대한 마지막 방어선입니다. WannaCry 및 Petya 사태에서 확인된 것처럼 랜섬웨어 공격이 더욱 기세를 떨치는 가운데 사이버 피해 및 가동 중단에 대한 우려의 목소리가 커지고 있습니다. 뿐만 아니라 파일리스(file-less) 공격 및 은밀한 공격이 범용 IT 툴을 활용하는 "자급자족" 방식과 결합하여 더욱 확산되면서 엔드포인트 자산의 기밀성, 무결성, 가용성을 위협하고 있습니다.

그렇다면 보안 팀이 이러한 사이버 공격에 대응하려면 어떻게 해야 할까요? 여러 포인트 제품 및 기술을 관리하는 것은 만만치 않으며, 운영 체제 및 플랫폼이 각기 다른 여러 지역을 포괄하여 보안을 관리하는 경우 어려움이 가중됩니다. 보안 팀은 리소스 및 예산이 한정된 만큼 관리하기 쉬우며 상호 통합으로 전반적인 보안 수준을 높일 수 있는 기술을 찾고 있습니다. 이들은 "포인트 제품이 하나 더 늘어나는 것"은 원치 않습니다. 그림 1을 참조하십시오.

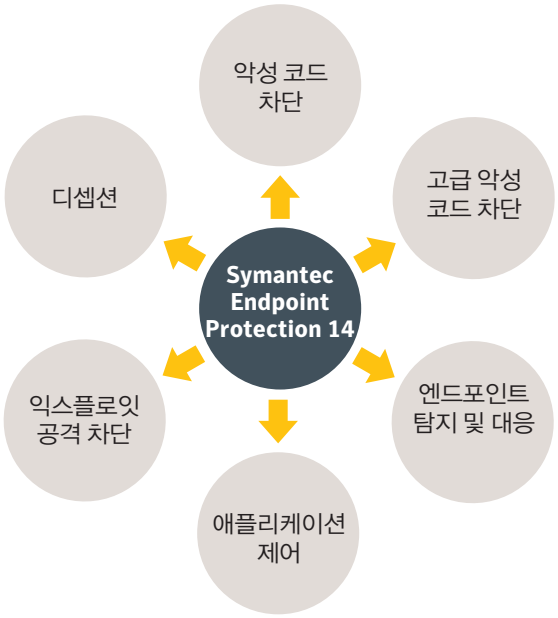

그림 1

그림 2. SEP 보안 프레임워크

Symantec Endpoint Protection(SEP)은 더 우수한 다계층 보호 기능을 제공하여 보안 위협이 엔드포인트를 공격하는 방식에 관계없이 보안 위협을 차단합니다. SEP는 기존 보안 인프라스트럭처와 통합하여 조직적으로 대응하면서 신속하게 보안 위협을 처리합니다. 단일 통합 경량화 SEP 에이전트가 엔드유저 생산성의 저하 없이 우수한 성능을 제공하므로 고객은 비즈니스에 집중할 수 있습니다. 보안 팀은 SEP를 통해 그림 2의 보안 프레임워크에 정리된 것과 같은 다양한 보안 활용 사례를 실행에 옮길 수 있습니다.

단일 에이전트 아키텍처에서 업계 최고의 효율성을 발휘하면서 모든 공격 경로로부터 엔드포인트 보호

방지

SEP는 그림 3이 보여주는 것처럼 공격자가 공격 체인의 어느 단계에 있든지 상관없이 엔드포인트를 보호합니다. 외부 평가에서도 입증된 것처럼 SEP의 보안 효율성은 업계 최고 수준입니다. 이 차원 높은 보호는 핵심 기술과 새로운 첨단 기술의 조합을 통해서만 가능합니다.

그림 3.

시그니처리스 기술

- **첨단 머신 언어(Advanced Machine Language, AML)** – 새로운 보안 위협 및 진화하는 보안 위협이 실행되기 전에 탐지합니다.
- **메모리 익스플로잇 차단** – 널리 사용되는 소프트웨어의 취약점을 공격하는 제로데이 익스플로잇을 차단합니다.
- **행위 모니터링** – 의심스러운 행위를 나타내는 파일을 모니터링하고 차단합니다.

고급 기능

- **Global Intelligence Network(GIN)** – 157개국에서 1억 7,500만 개의 엔드포인트 및 5,700만 개의 공격 센서로부터 정보를 수집하는 세계 최대 규모의 보안 위협 인텔리전스 네트워크입니다. 이렇게 수집한 데이터는 1,000명이 넘는 숙련된 보안 위협 분석 팀에서 분석하여 보안 위협에 대처하는 데 필요한 가시성을 확보하고 최첨단 보안 혁신을 실현하는 데 사용됩니다.
- **평판 분석** – 클라우드에서 GIN을 기반으로 하는 인공 지능 기술을 사용하여 파일 및 웹 사이트의 보안 수준을 확인합니다.
- **에뮬레이터** – 맞춤형 패커를 통해 숨어든 다형성 악성 코드를 탐지하기 위해 경량의 샌드박스를 활용합니다.
- **Intelligent Threat Cloud**에서 첨단 기법을 도입하여 빠른 검사를 수행하므로 엔드포인트에 모든 시그니처 정의를 다운로드하지 않고도 우수한 성능을 발휘할 수 있습니다. 즉 최신 보안 위협 정보만 다운로드하므로 시그니처 정의 파일의 크기가 최대 70% 줄어 대역폭 사용량도 감소합니다.
- **Secure Web Gateway 통합** – 프로그래밍 가능한 새로운 REST API를 통해 Secure Web Gateway를 비롯한 기존 인프라스트럭처와의 통합을 구현하여 엔드포인트상에서 조직적인 대응을 수행하면서 신속하게 감염 확산을 막을 수 있습니다.

핵심 기능

- **안티바이러스** – 시스템에 침투한 악성 코드를 검사하고 제거합니다.
- **방화벽 및 침입 차단** – 악성 코드가 시스템으로 확산되어 트래픽을 제어하기 전에 차단합니다.
- **애플리케이션 및 매체 제어** – 파일, 레지스트리, 디바이스 액세스 및 행위를 제어할 뿐 아니라 화이트리스팅/블랙리스팅도 수행합니다.
- **Power Eraser** – 원격 실행 가능한 이 강력한 툴은 지능형 지속 위협을 처리하고 끈질긴 악성 코드를 제거합니다.
- **호스트 무결성** – 요구 사항에 부합하지 않는 관리 대상 시스템을 격리하는 기능을 통해 정책을 적용하고 무단 변경을 탐지하며 손상 정도를 평가하면서 엔드포인트 보호 및 컴플라이언스를 보장합니다.
- **시스템 잠금** – 안전한 것으로 알려진 애플리케이션의 실행만 허용하고 위험한 것으로 알려진 애플리케이션의 실행은 차단할 수 있습니다.

또한 그림 4에서 보여주는 것처럼 IT 보안 팀이 개별 고객 환경에 대해 탐지 및 차단 레벨을 튜닝하여 보호 기능을 최적화하고 의심스러운 파일을 확실하게 모니터링할 수 있도록 지원하는 솔루션은 SEP가 유일합니다. 집중 보호(Intensive Protection)라고 불리는 이 튜닝 가능 보안은 새로운 클라우드 콘솔을 통해 제공되며, 이 콘솔은 온프레미스 SEP Manager와 자동으로 통합되며 의심스러운 파일을 블랙리스팅하거나 오탐지를 화이트리스팅하는 편리한 워크플로우를 제공합니다.

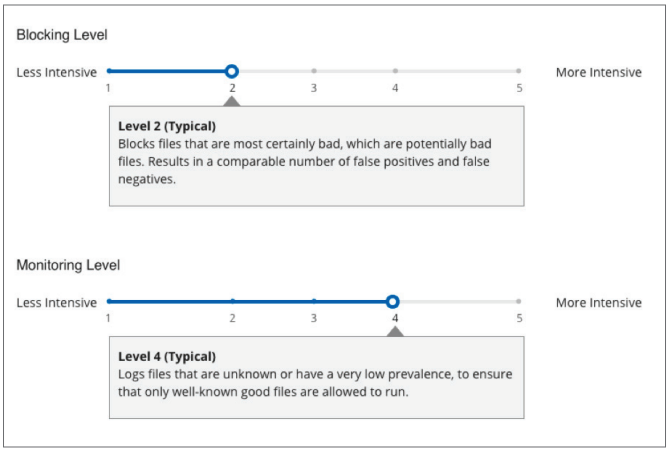

그림 4. 집중 보호를 통해 튜닝 가능한 모니터링 및 차단 기능이 제공됩니다.

IT 보안 팀은 시만텍의 단일 에이전트 아키텍처를 통해 간단하게 구축하고 혁신적인 보안 기술을 추가할 수 있습니다. 즉 신규 에이전트가 필요하지 않습니다.

탐지 및 대응(EDR)

Symantec Advanced Threat Protection: Endpoint는 SEP에 통합된 EDR 기능을 활용하여 침해 사고를 조사하고 대응합니다. 1시간 내로 구축 가능한 이 솔루션은 정밀한 머신 러닝, 행위 분석, 보안 위협 인텔리전스를 활용하여 지능형 공격을 밝혀내고 오탐지를 최소화하며 보안 팀의 생산성을 극대화할 수 있도록 지원합니다. Symantec EDR 기능으로 공격 대상 엔드포인트를 신속하게 검색, 식별, 억제할 뿐 아니라 온프레미스 또는 클라우드 기반 샌드박싱을 활용하여 보안 위협을 조사할 수 있습니다. 또한 시스템 활동을 중단 없이 기록하므로 철저한 엔드포인트 모니터링 및 실시간 쿼리가 가능합니다.

Symantec EDR:

- **탐지 및 규명** – 보안 위반 발견까지의 시간을 단축하고 신속하게 범위 파악
- **조사 및 억제** - 침해 사고 대응 팀의 생산성 향상 및 확실한 보안 위협 억제
- **해결** - 신속하게 엔드포인트의 문제를 해결하여 보안 위협 재발 방지
- **보안 투자의 효과 증대** - 사전 구현된 통합 및 공개 API

디셉션

SEP 디셉션[1]은 일종의 미끼인 디셉터를 심어 두고 조기 감시를 통해 숨어 있는 공격자를 찾아내 공격자의 의도와 전술을 밝혀냅니다. 이 정보는 보안을 강화하는 데 활용할 수 있습니다. SEP 디셉션 기능은 정확하고 심도 있게 탐지하면서 신속하게 가치를 창출합니다. Symantec Endpoint Protection과 Symantec Managed Security Services를 모두 선택한 고객은 글로벌 전문가 팀이 연중무휴 24시간 제공하는 SEP 디셉션 실시간 모니터링 및 대응 서비스를 이용할 수 있습니다. 디셉션 기능을 제공하는 엔드포인트 보호 플랫폼 벤더는 시만텍뿐입니다.

SEP 디셉션:

- 미끼 전략으로 공격자를 알아내고 지연시키는 사전 예방적 보안 실현
- 공격자의 의도를 파악하여 보안 수준 강화
- 대규모의 디셉션 전략으로 구축 및 관리 간소화

적응(ADAPTATION)

SEP 강화(Hardening)는 의심스러운 애플리케이션을 격리하고 신뢰할 수 있는 애플리케이션을 보호하면서 통합적으로 애플리케이션을 보호하는 클라우드 기반 첨단 애플리케이션 방어 솔루션입니다. 애플리케이션 격리를 지원하는 다른 벤더의 포인트 제품과 달리 SEP 강화(Hardening)는 SEP와 연계하여 전례 없는 효율성을 발휘하면서 악성 코드 및 의심스러운 애플리케이션을 차단합니다. 또한 SEP 강화(Hardening)는 표준 업무 워크플로우를 완벽하게 지원하면서 직원들의 업무 생산성을 향상시킵니다.

SEP 강화(Hardening):

- 공격 범위를 최소화하여 통합 애플리케이션 보안 실현
- 모든 엔드포인트 애플리케이션을 검색하고 분류하면서 새로운 차원의 가시성 제공
- SEP의 단일 에이전트 아키텍처를 활용하면서 가장 신속하게 가치 창출

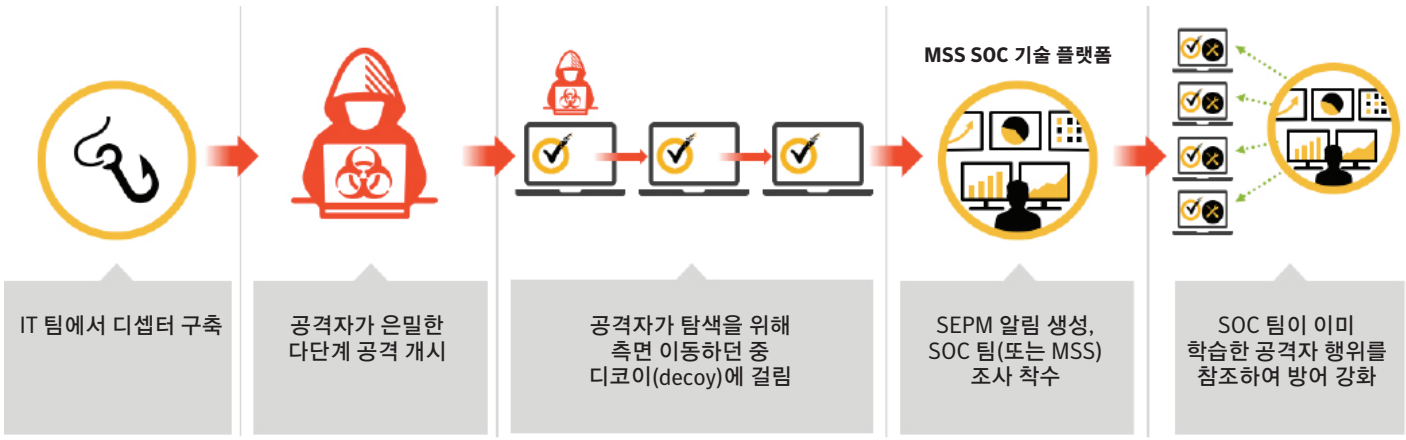

그림 5. SEP의 디셉션 작동 방식

[1] SEP 디셉션 기능을 구성하고 구축하려면 컨설팅 서비스가 필요합니다.

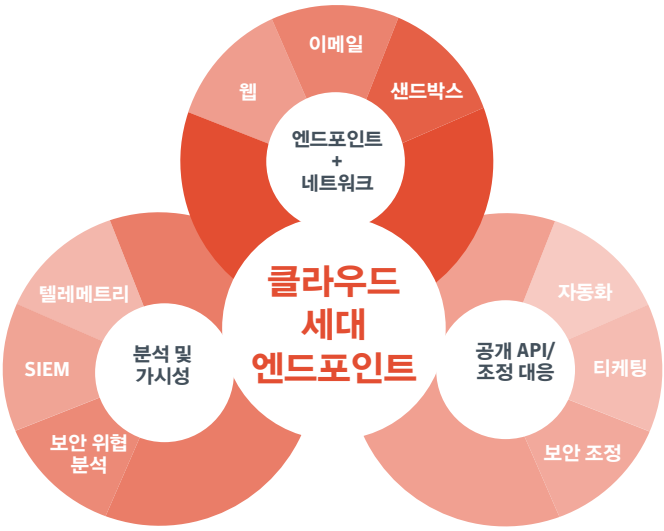

그림 6.

대규모의 통합 사이버 방어 체계 구축

대부분의 대기업이 운영하는 글로벌 IT 환경이 갈수록 복잡해지고 있습니다. 이러한 환경에 구현된 솔루션의 상당수는 특정 기능만 수행할 뿐입니다. 따라서 다른 IT 보안 솔루션과 통합하여 인텔리전스를 공유하고 함께 네트워크를 보호함으로써 더 큰 가치를 실현하고 종합적으로 보호할 수 있는 엔드포인트 보호 솔루션이 필요합니다.

SEP 14는 그러한 통합 구현의 근간이 되는 제품으로 IT 보안 팀이 네트워크의 어디서든 보안 위협을 탐지하고 조직적으로 대응하여 보안 위협을 해결할 수 있도록 지원합니다. SEP 14는 Integrated Cyber Defense Platform의 핵심 구성 요소로서 시만텍 솔루션과 통합하고 공개된 API를 통해 타사 제품과도 통합하면서 더 강력한 보안을 실현할 수 있습니다. Symantec Integrated Cyber Defense Platform은 클라우드 보안과 온프레미스 보안을 연계하고 업계 최고의 보안 위협 인텔리전스를 활용하면서 사용자, 정보, 메시징, 웹을 보호합니다. 네트워크 게이트웨이(웹 및 이메일 보안 게이트웨이)에서 보안 위협을 탐지하고 엔드포인트에서 조직적인 대응(블랙리스팅 및 위협 제거)을 수행하는 통합 솔루션은 오로지 시만텍에서만 제공합니다.

유연한 고성능 솔루션으로 비즈니스 지원

대용량 컨텐트 업데이트 또는 빈번한 컨텐트 업데이트로 인해 대역폭이 소모되고 엔드포인트의 속도가 느려져 생산성이 저하될 수 있습니다. 컨텐트 업데이트를 최적화하고 더 효과적으로 보안 위협을 탐지할 수 있다면 유용할 것입니다. IT 팀은 이러한 기능으로 빈번한 보안 업데이트 일정 관리의 부담을 덜 수 있습니다. 엔드유저는 생산성 저하를 감수하면서 번거롭게 보안 업데이트를 수행할 필요가 없습니다.

SEP 14는 성능을 높이고 대역폭 요구 사항을 완화하여 더 효과적으로 보호합니다. 시만텍은 외부 성능 테스트에서 항상 최고점을 받고 있으며, 그중 Passmark Software가 Windows 7 및 Windows 10 환경에서 엔터프라이즈 엔드포인트 보안 제품의 성능을 평가한 벤치마크 테스트도 포함되어 있습니다. 또 다른 외부 검증에 대해서는 시만텍 성과 센터 (symantec.com/products/performance-center)를 참조하십시오.

SEP로 아래와 같은 성능 향상 효과를 기대할 수 있습니다.

- 컨텐트 업데이트 크기 70% 감축[2]
- 탐지 검사 시간 15% 단축[2]

SEP는 신생 벤더와 달리 단일 경량화 에이전트에 여러 기능을 번들로 구성하여 엔드포인트의 복잡성을 줄입니다. 시만텍과 같은 수준의 엔드포인트 보안 기능을 제공하기 위해서는 여러 개의 최신 벤더, 복수의 솔루션, 복수의 에이전트가 필요할 것입니다.

[2] SEP 12에서 SEP 14로 업그레이드하여 얻을 수 있는 효과

시스템 요구 사항

클라이언트 워크스테이션 및 서버 시스템 요구 사항*

Windows® 운영 체제

- Windows Vista(32비트, 64비트)
- Windows 7(32비트, 64비트, RTM, SP1)
- Windows Embedded 7 Standard, POSReady, Enterprise(32비트, 64비트)
- Windows 8(32비트, 64비트)
- Windows Embedded 8 Standard(32비트, 64비트)
- Windows 8.1(32비트, 64비트), Windows To Go 포함
- Windows 8.1 2014년 4월 업데이트(32비트, 64비트)
- Windows 8.1 2014년 8월 업데이트(32비트, 64비트)
- Windows Embedded 8.1 Pro, Industry Pro, Industry Enterprise(32비트, 64비트)
- Windows 10(32비트, 64비트)
- Windows 10 2015년 11월 업데이트(32비트, 64비트)
- Windows 10 Anniversary Update 2016(32비트, 64비트)
- Windows Server 2008(32비트, 64비트, R2, SP1, SP2)
- Windows Small Business Server 2008(64비트)
- Windows Essential Business Server 2008(64비트)
- Windows Small Business Server 2011(64비트)
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2012 R2 2014년 4월 업데이트
- Windows Server 2012 R2 2014년 8월 업데이트
- Windows Server 2016

Windows 하드웨어 요구 사항

- 1.9GHz CPU 이상
- 1GB RAM(2GB 권장)
- 530MB의 하드 디스크 여유 공간

Macintosh® 운영 체제

- Mac OS X 10.10, 10.11, macOS 10.12, 10.13

Mac 하드웨어 요구 사항

- 64비트 Intel Core 2 Duo 이상
- 2GB RAM
- 500MB의 하드 디스크 여유 공간

가상 환경

- Microsoft Azure
- Amazon WorkSpaces
- VMware WS 5.0, GSX 3.2, ESX 2.5 이상
- VMware ESXi 4.1 - 5.5
- VMware ESX 6.0
- Microsoft Virtual Server 2005
- Microsoft Enterprise Desktop Virtualization(MED-V)
- Microsoft Windows Server 2008, 2012, 2012 R2 Hyper-V
- Citrix XenServer 5.6 이상
- Oracle Cloud
- Virtual Box by Oracle

Linux 운영 체제(32비트, 64비트 버전)

- Amazon Linux
- CentOS 6U3, 6U4, 6U5, 6U6, 7, 7U1, 7U2, 7U3(32비트, 64비트)
- Debian 6.0.5 Squeeze, Debian 8 Jessie(32비트, 64비트)
- Fedora 16, 17(32비트, 64비트)
- Oracle Linux(OEL) 6U2, 6U4, 6U5, 7, 7.1, 7.2, 7.3
- Red Hat Enterprise Linux Server(RHEL) 6U2 - 6U8, 7 - 7.3
- SUSE Linux Enterprise Server(SLES) 11 SP1 - 11, SP3(32비트, 64비트), 12
- SUSE Linux Enterprise Desktop(SLED) 11 SP1 - 11 SP3(32비트, 64비트)
- Ubuntu 12.04, 14.04, 16.04(32비트, 64비트)

Linux 하드웨어 요구 사항

- Intel Pentium 4(2GHz CPU 이상)
- 1GB RAM
- 7GB의 하드 디스크 여유 공간

관리자 시스템 요구 사항

Windows® 운영 체제

- Windows Server 2008(64비트, R2 포함)
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2012 R2
- Windows Server 2016

웹 브라우저

- Microsoft Internet Explorer 11
- Mozilla Firefox 5.x - 55.x
- Google Chrome 61.x
- Microsoft Edge

하드웨어

- Intel Pentium Dual-Core 또는 동급 이상
- 2GB RAM(8GB 권장)
- 8GB 이상의 하드 디스크 여유 공간

데이터베이스

임베디드 데이터베이스 포함 또는 다음 중에서 선택:

- SQL Server 2008, SP4
- SQL Server 2008 R2, SP3
- SQL Server 2012, RTM – SP3
- SQL Server 2014, RTM – SP2
- SQL Server 2016, RTM, SP1

아래 운영 체제에서 SEP 강화(Hardening) 기능을 사용할 수 있습니다.

- Windows 7(64비트, RTM 및 SP1)
- Windows Embedded 7 Standard, POSReady, Enterprise(64비트)
- Windows 8(64비트)
- Windows Embedded 8 Standard(64비트)
- Windows 8.1(64비트), Windows To Go 포함
- Windows 8.1 2014년 4월 업데이트(64비트)
- Windows 8.1 2014년 8월 업데이트(64비트)
- Windows Embedded 8.1 Pro, Industry Pro, Industry Enterprise(64비트)
- Windows 10(64비트), Windows 10 2015년 11월 업데이트(64비트)
- Windows 10 Anniversary Update 2016 (64비트)
- Windows 10 Creators Update 2017(64비트)

*전체 시스템 요구 사항 목록은 지원 페이지에서 확인하십시오.

시만텍 소개

글로벌 사이버 보안 분야를 선도하는 시만텍은 기업, 정부 기관 및 개인의 중요한 데이터가 어디에 있든 안전하게 보호될 수 있도록 지원한다. 시만텍은 엔드포인트, 클라우드, 인프라 전반을 정교한 공격으로부터 방어할 수 있는 전략적인 통합 솔루션을 전 세계 기업과 기관에 제공하고 있다. 또한, 전 세계 5천만 이상의 개인사용자와 가정에서 시만텍 노턴 제품과 라이프록(LifeLock) 제품을 이용해 가정과 다양한 기기에서 디지털 라이프를 보호하고 있다. 시만텍은 세계 최대 규모의 민간 사이버 인텔리전스 네트워크를 통해 고도화된 지능형 위협을 탐지하고 고객들을 보호한다. 보다 자세한 정보는 시만텍 웹사이트(www.symantec.com/ko/kr)와 페이스북, 트위터, 링크드인을 통해 확인할 수 있다.

시만텍코리아 | 서울시 강남구 테헤란로 152강남파이낸스센터 28층 |
TEL: 02-3468-2000 | FAX: 02-3468-2001 | www.symantec.com/ko/kr

Copyright © 2017 Symantec Corporation. All rights reserved. Symantec, Symantec 로고, Checkmark 로고는 미국 및 기타 국가에서 Symantec Corporation 또는 그 자회사의 상표 또는 등록 상표입니다. 다른 이름은 해당 회사의 상표일 수 있습니다.

SYMC_DS_SEP14_CloudGeneration_KR_v1a