



McAfee Complete Data Protection—Essential

필수 엔드포인트 암호화 솔루션

중요한 데이터는 지속적인 손실, 도난 및 노출 위험에 처해 있습니다. 데이터가 랩톱 또는 USB 장치에서 직접 유실되는 경우가 종종 있습니다. 이러한 데이터 손실로 어려움을 겪는 기업의 경우 법적 불이익, 대외적인 공개, 브랜드 손상, 고객 불신, 재정적 불이익을 비롯하여 심각한 결과에 처할 위험이 있습니다. Ponemon Institute의 보고서에 따르면, 모든 기업의 랩톱 중 7%가 아직 수명이 끝나지 않은 기간 동안 분실되거나 도난당한다고 합니다.¹ 대용량 저장 기능이 있는 모바일 장치가 급속하게 확산되고 이를 통한 인터넷 액세스가 빈번해지면서 데이터 손실 또는 도난이 발생할 수 있는 채널이 더욱 많아지고 있는 만큼, 민감한 재산적 정보 및 개인 식별 정보 보호를 최우선으로 생각해야 합니다. McAfee® Complete Data Protection—Essential 제품군은 이러한 모든 고민을 비롯한 많은 문제를 해결합니다.

주요 기능

- Management of Native Encryption
- File and Removable Media Protection

주요 이점

- 중요한 개인 정보를 가로채가는 정교한 악성 프로그램에 의한 데이터 손실을 막을 수 있습니다.
- 데이터를 데스크톱, 랩톱, 태블릿 및 기타 모바일 장치에 저장할 경우 이를 안전하게 보호합니다.
- McAfee ePO 소프트웨어에서 바로 엔드포인트의 Apple FileVault 및 Microsoft BitLocker 기본 암호화를 관리합니다.
- 고급 보고 및 감사 기능을 활용하여 컴플라이언스를 입증합니다.
- 이벤트를 모니터링하며, 내부 및 규정 개인 정보 요구 사항의 컴플라이언스 여부를 감사 담당자 및 기타 관계자에게 표시하는 자세한 보고서를 생성합니다.

Management of Native Encryption

Management of Native Encryption을 사용하여 고객은 Mac OS X 플랫폼의 Apple FileVault 및 Windows 플랫폼의 Microsoft BitLocker가 제공하는 기본 암호화 기능을 McAfee ePO™(McAfee® ePolicy Orchestrator®) 소프트웨어에서 직접 관리할 수 있습니다. Management of Native Encryption은 Apple 및 Microsoft의 OS X 및 Windows 패치, 업그레이드, 펌웨어 업데이트에 대해 제로 데이 호환성을 제공하고 Apple의 새 하드웨어에 대해서도 제로 데이 지원을 제공합니다. 사용자가 이미 FileVault 및 BitLocker를 사용하도록 설정한 경우 Management of Native Encryption을 사용하여 관리자는 복구 키를 수동으로 가져올 수 있습니다.

영구적이고 투명한 이동식 미디어 및 파일/폴더 암호화

데이터를 편집, 복사 또는 저장한 위치에 관계없이 특정 파일 및 폴더를 항상 암호화합니다. McAfee

Complete Data Protection 제품군은 조직 내에서 파일 및 폴더를 이동하기 전에, 사용자가 경우에 따라 선택한 이러한 파일 및 폴더를 자동으로 투명하게 암호화하는 내용 암호화 기능을 제공합니다. 사용자의 수동 작업 없이도 특정 파일 및 폴더의 사용자 및 사용자 그룹을 기준으로 중앙 집중식 정책을 생성하고 시행할 수 있습니다.

중앙 집중식 보안 관리 및 고급 보고

중앙 집중식 McAfee ePO 소프트웨어 콘솔을 이용해 데이터의 암호화, 모니터링 및 유출 방식을 제어하는 전사적 필수 보안 정책을 구현하고 시행합니다. 중요한 데이터를 암호화, 필터링 및 모니터링하고 이에 대한 무단 액세스를 차단하는 보안 정책을 중앙 집중식으로 정의, 구현하고 관리, 업데이트합니다.

사양

Microsoft Windows 운영 체제

- Microsoft Windows 10(2015년 하반기)
- Microsoft Windows 7, 8, 8.1(32/64비트 버전)
- Microsoft Windows Vista(32/64비트 버전)
- Microsoft Windows XP (32비트 버전만)
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003(32비트 버전만)

하드웨어 요구 사항

- CPU: Pentium III 1GHz 이상의 랩톱 및 데스크톱 컴퓨터
- RAM: 최소 512MB(1GB 권장)
- 하드 디스크: 최소 200MB의 사용 가능한 디스크 공간

Apple Mac 운영 체제

- Mac OS X Yosemite, Mountain Lion 및 Mavericks

하드웨어 요구 사항

- CPU: Intel 기반 Mac 랩톱 (64비트 EFI 포함)
- RAM: 최소 1GB
- 하드 디스크: 최소 200MB의 사용 가능한 디스크 공간

중앙 집중식 관리

- 기술 사양에 대해서는 McAfee ePO 플랫폼 데이터시트를 참조하십시오.

McAfee Complete Data Protection 제품군 기능

Mac 및 Windows의 기본 암호화 관리

- McAfee ePO 소프트웨어에서 직접 Mac OS X Mountain Lion, Mavericks 및 Yosemite를 실행할 수 있는 모든 Mac 하드웨어의 FileVault를 관리합니다.
- 별도의 MBAM(Microsoft BitLocker Management and Administration) 서버 없이도 Windows 7, 8 및 10² 시스템의 BitLocker를 McAfee ePO 소프트웨어에서 바로 관리할 수 있습니다.
- McAfee ePO 소프트웨어의 다양한 보고서 및 대시보드를 통해 컴플라이언스를 보고합니다.

영구적인 파일 및 폴더 암호화

- 이메일 수신자가 암호화 소프트웨어를 갖고 있지 않아도 파일 및 폴더를 하드 디스크, 파일 서버, 이동식 미디어에 저장할 때마다 안전하게 보호하며, 이메일 첨부 파일의 경우에도 마찬가지입니다.

중앙 집중식 관리 콘솔

- McAfee ePO 소프트웨어 인프라 관리를 사용하여 풀 디스크, 파일 및 폴더, 이동식 미디어 암호화를 관리하고, 정책 및 패치 관리를 제어하고, 분실한 암호를 복구하고, 규정 컴플라이언스 여부를 나타낼 수 있습니다.
- 보안 정책을 Microsoft Active Directory, Novell NDS, PKI 및 기타 서비스와 동기화합니다.

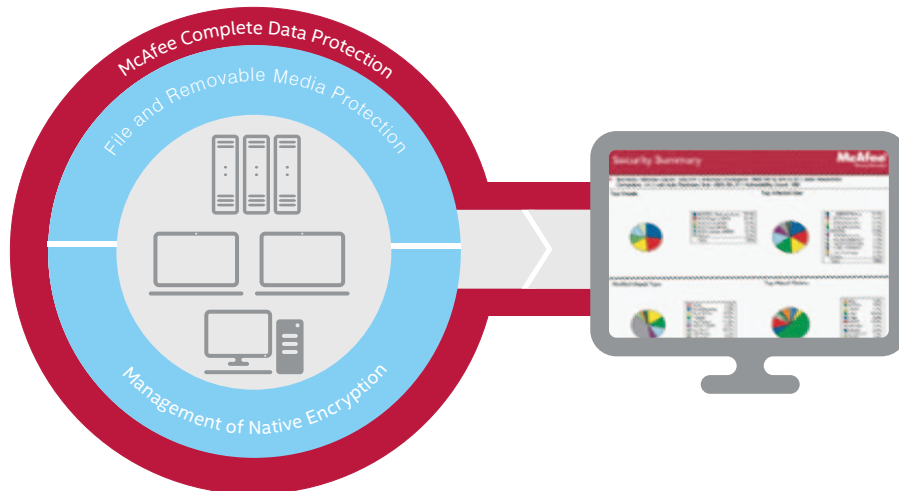


그림 1. McAfee Complete Data Protection—Essential 제품군

이동식 미디어 암호화

- 기업에서 제공한 또는 그 외의 거의 모든 모바일 저장 장치에 대해 자동으로 즉각적인 암호화를 지원합니다.
- VDI 워크스테이션에서 이동식 미디어에 쓰기를 암호화하거나 차단합니다.
- 장치 호스트에서 추가 소프트웨어 설치 작업이나 로컬 관리 권한 없이도 어디에서든지 암호화된 데이터에 액세스할 수 있습니다.

- 집중적인 감사 기능을 통해 장치를 암호화했음을 입증합니다.

- 데이터 트랜잭션을 기록하여 보낸 사람, 수신자, 타임스탬프, 데이터 증거, 최종 로그인 날짜 및 시간, 최종 업데이트 수신 날짜 및 시간, 암호화 성공 여부와 같은 정보를 기록합니다.

McAfee 데이터 보호에 대한 자세한 내용은 www.mcafee.com/kr/products/data-protection/index.aspx를 방문하십시오.



1. The Billion Dollar Lost Laptop Problem Study(랩톱 분실로 야기되는 막대한 비용 문제 연구), Ponemon Institute, 2010년 9월
2. Windows 10은 2015년 하반기 지원 예정