McAfee Complete Data Protection—Advanced

언제 어디에서든 종합적인 데이터 보호

중요한 데이터는 지속적인 손실, 도난 및 노출 위험에 처해 있습니다. 많은 경우 데이터는 랩톱 또는 USB 장치에서 직접 유실되곤 합니다. 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—Advanced는 이러한 모든 고민을 비롯한 많은 문제를 해결합니다.

주요 기능

- McAfee Data Loss Prevention Endpoint
- McAfee Device Control
- Drive Encryption
- File and Removable Media Protection
- Management of Native Encryption

주요 이점

- **사무실에서든, 사무실 밖에서든 이메일, IM, 인쇄 및 USB 드라이브 같은 일반적인 채널을 통해 직원이 어떻게 데이터를 사용 및 전송하는지 모니터링하고 규제함으로써 데이터를 제어할 수 있습니다.**
- **중요한 개인 정보를 가로채가는 정교한 악성 프로그램에 의한 데이터 손실을 막을 수 있습니다.**
- **데스크톱, 랩톱, 태블릿 및 클라우드에 데이터를 저장할 경우 이를 안전하게 보호합니다.**
- **McAfee ePO에서 바로 엔드포인트의 Apple FileVault 및 Microsoft BitLocker 기본 암호화를 관리합니다.**

데이터 손실 방지로 더욱 강력한 제어 지원

엔드포인트의 데이터 손실을 방지하게 되면 데이터에 대한 가시성 및 제어가 향상되며, 데이터가 위장한 경우에도 마찬가지입니다. McAfee Complete Data Protection—Advanced **는 이메일, IM, 인쇄 및 USB 드라이브 같은 일반적인 채널을 통해 직원이 어떻게 중요한 데이터를 사용 및 전송하는지 규제하고 제한하는 전사적인 보안 정책을 구현 및 시행할 수 있도록 지원합니다. 또한 사무실에서든, 집에서든, 이동 중에든 언제나 데이터를 제어할 수 있도록 합니다.**

엔터프라이즈급 드라이브 암호화

FIPS 140-2 **및** Common Criteria EAL2+ **인증을 받고** Intel AES-NI(Intel® Advanced Encryption Standard - New Instructions) **세트로 가속화된 엔터프라이즈급 보안 솔루션으로 중요한 데이터를 보호하십시오.** McAfee Complete Data Protection—Advanced**는 부팅 전 이중 인증을 통해 강력한 액세스 제어와 결합된 드라이브 암호화를 사용하여 데스크톱,** VDI **워크스테이션, 랩톱,** USB **드라이브,** CD/DVD **등을 비롯한 엔드포인트의 기밀 데이터에 무단으로 액세스하지 못하도록 방지합니다.**

McAfee™
Together is power.

주요 이점(계속)

- 엔드포인트가 전원이 꺼지고 비활성화되거나 암호화된 경우에 상관없이, 하드웨어 수준에서 엔드포인트와 커뮤니케이션을 수행하고 제어하여 보안 사고, 아웃브레이크 또는 잊어버린 암호 문제로 인해 현장 방문을 해야 하거나 헬프데스크에 끊임없이 문의 전화가 오는 경우를 방지합니다.
- 고급 보고 및 감사 기능을 활용하여 컴플라이언스를 입증합니다. 이러한 기능은 이벤트를 모니터링하며, 내부 및 규정 개인 정보 요구 사항의 컴플라이언스 여부를 감사 담당자 및 기타 관계자에게 표시하는 자세한 보고서를 생성합니다.

이동식 미디어, 파일 및 폴더, 클라우드 스토리지 암호화

데이터를 편집, 복사 또는 저장한 위치에 관계없이 특정 파일 및 폴더를 항상 암호화합니다. McAfee Complete Data Protection—Advanced는 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.

Management of Native Encryption

Management of Native Encryption을 사용하여 사용자가 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. 따라서 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.

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.

McAfee Complete Data Protection—Advanced 기능

장치 제어

- 직원이 데이터를 이동식 미디어로 전송하는 방식을 모니터링 및 규제하며, 직원이 기업 네트워크에 연결되어 있지 않을 때에도 이를 수행합니다.

데이터 유실 방지

- 사용자가 물리적 또는 가상 엔드포인트에서, 응용프로그램을 통해 또는 저장 장치에서 중요한 데이터를 전송, 액세스 및 인쇄하는 방식을 제어합니다.
- 트로이 목마, 웜 및 직원의 자격 증명을 가로채는 파일 공유 응용프로그램으로 인한 기밀 데이터 유실을 방지합니다.
- 데이터를 수정, 복사, 붙여넣기, 압축 또는 암호화한 경우에도 모든 데이터, 형식 및 파생 요소를 보호합니다.

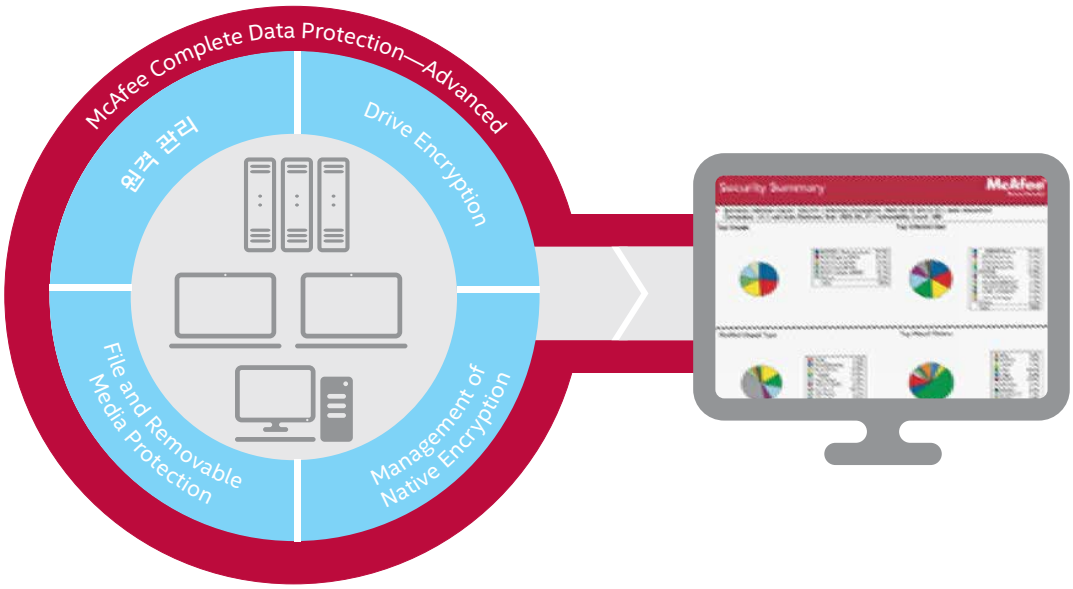

그림 1. McAfee Complete Data Protection.

McAfee Complete Data Protection—Advanced 사양

Microsoft Windows운영 체제

- Microsoft Windows 7, 8 및 10(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 El Capitan, Yosemite, Mountain Lion 및 Mavericks

하드웨어 요구 사항

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

중앙 집중식 관리

엔터프라이즈급 드라이브 암호화

- 사용자 작업 또는 교육이 필요하지 않으며 시스템 리소스에 영향을 주지 않으면서 전체 장치를 자동으로 암호화합니다.
- 강력한 다단계 인증을 사용하여 인증된 사용자를 식별 및 확인합니다.
- Intel® Software Guard Extensions (Intel® SGX)를 지원합니다.
- 타사 자격 증명 공급자와 호환됩니다.
- Windows 10 1주년 업데이트의 인플레이스 업그레이드를 지원합니다.

이동식 미디어 암호화

- 기업에서 제공한 또는 그 외의 거의 모든 모바일 저장 장치에 대해 자동으로 즉각적인 암호화를 지원합니다.
- 어떠한 추가 소프트웨어도 필요없이 모든 장소에서 암호화된 데이터에 액세스할 수 있습니다.

파일, 폴더 및 클라우드 스토리지 암호화

- 하드 디스크, 파일 서버, 이동식 미디어 및 클라우드 스토리지(예, Box, Dropbox, Google Drive 및 Microsoft OneDrive)를 포함해 저장 장소에 관계 없이 파일 및 폴더를 안전하게 보호합니다.

Mac 및 Windows의 기본 암호화 관리

- McAfee ePO 소프트웨어에서 직접 Mac OS X Mountain Lion, Mavericks, Yosemite 및 El Capitan를 실행할 수 있는 모든 Mac 하드웨어의 FileVault를 관리합니다.
- 별도의 MBAM(Microsoft BitLocker Management and Administration) 서버 없이도 Windows 7, 8 및 10 시스템의 BitLocker를 McAfee ePO 소프트웨어에서 바로 관리할 수 있습니다.

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.
- 집중적인 감사 기능을 통해 장치를 암호화했음을 입증합니다.
- 데이터 트랜잭션을 로깅하여 보낸 사람, 받는 사람, 타임스탬프, 데이터 증거, 그리고 마지막으로 로그인을 성공한 날짜 및 시간과 같은 정보를 기록합니다.

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

McAfee
Together is power.

1. *The Billion Dollar Lost Laptop Problem Study*(랩톱 분실로 야기되는 막대한 비용 문제 연구), Ponemon Institute, 2010년 9월

McAfee (Singapore) Pte Ltd
10 Kallang Avenue #08-10
Aperia Tower 2
Singapore 339510
www.mcafee.com/kr