McAfee Data Loss Prevention Endpoint

데이터 유실을 미연에 방지하십시오.

미처 깨닫지 못한 새에 데이터가 유실되고 있습니까? 고객 정보, 지적 재산, 재무 데이터 및 개인 파일이 지금 회사 외부로 유출되고 있을 수 있습니다. 이러한 가해자는 해커만이 아니라 내부 직원일 수도 있습니다. 이메일, 웹 게시, USB 드라이브, 클라우드 업로드와 같은 일반적인 수단을 통해 실수 및 악의적인 데이터 유실이 일어나 큰 비용 피해가 발생할 수 있습니다. 매일 회사가 악의적이거나 실수에 의한 정보 유출로 인한 막대한 데이터 유실의 희생양이 되고 있습니다. 데이터 유실을 간단하면서도 효과적으로 방지할 수 있다면 어떻습니까? 또한 업계 및 정부 컴플라이언스를 충족하는 동시에 지적 재산도 보호할 수 있다면 어떨까요? 이제 포괄적인 McAfee® Data Loss Prevention Endpoint(McAfee DLP Endpoint)를 통해 이러한 결과를 실현할 수 있습니다.

장치-클라우드 간 DLP

McAfee DLP Endpoint가 MVISION Cloud DLP와 통합됩니다. 클릭 한 번으로 1분 안에 온-프레미스 DLP 정책을 클라우드로 쉽게 확장할 수 있습니다.[1] 온프레미스 DLP 분류 태그는 클라우드 DLP 정책과 공유되어 데이터 손실을 지속적으로 탐지합니다.

지능형 보호 기능

McAfee DLP Endpoint는 이동식 저장 장치, 클라우드, 이메일, 메신저, 웹, 인쇄, 클립보드, 화면 캡처, 파일 공유 응용프로그램을 비롯한 모든 가능성 있는 유출 채널을 포괄적으로 차단합니다.

주요 이점

- **장치-클라우드 간 DLP:** 온프레미스 DLP 정책을 클라우드로 간편하게 확장하여 데이터 손실을 지속적으로 탐지합니다.
- **지능형 보호 기능:** 지문, 분류 및 파일 태그 지정을 활용하여 구조화되지 않은 중요 데이터(예: 지적 재산 및 영업 비밀)를 보호합니다.
- **중앙 집중식 관리:** McAfee® MVISION ePolicy Orchestrator®(MVISION ePO™) 소프트웨어와의 기본 통합은 정책 및 사고 관리 간소화에 도움이 됩니다.[2]
- **컴플라이언스 시행:** 사용자의 일상 작업(예: 이메일, 클라우드 게시, 이동식 미디어 장치에 다운로드 등)을 처리하여 컴플라이언스를 보장합니다.
- **사용자 교육:** 교육 팝업을 통한 실시간 피드백을 사용하여 회사 보안 인식과 문화를 구축할 수 있습니다.

McAfee에 문의

McAfee DLP Endpoint 핵심 기능에는 다음이 포함됩니다.

- 전송 중인 데이터에 대한 Microsoft Azure Information Protection (AIP) 레이블을 설정하고 AIP 레이블이 설정된 파일을 식별하는 기능.[3]
- 타사 사용자 행동 분석(UEBA)과의 통합으로 내부 위협을 해결합니다. 보안 분석을 수행하여 비정상적인 고위험 사용자 및 단체 행동을 감지합니다.
- 수동 분류는 사용자가 문서를 수동으로 분류할 수 있게 하여 직원들의 데이터 보호 인식을 강화하고 관리자의 부담을 덜어줍니다.
- 사용자 주도 검색 및 교정을 통해 사용자가 엔드포인트 검색을 실행하고 자가 교정 작업을 수행할 수 있습니다.
- 사전, 정규식 및 유효성 검사 알고리즘, 등록 문서, 타사 사용자 분류 솔루션 지원을 비롯하여 유연한 분류가 가능합니다.
- 출처에 따라 문서를 식별하기 위한 특별한 태깅 기술은 웹 응용프로그램, 네트워크 응용프로그램 및 네트워크 공유의 중요 정보가 복제 또는 이름 변경되거나 사내에서 유출되지 않도록 보호하는 데 도움이 됩니다.
- 개선된 가상화 지원으로 원격 데스크톱 및 VDI(가상 데스크톱 인프라) 솔루션을 보호합니다.

중앙 집중식 관리

- 클라우드 네이티브 관리 콘솔인 MVISION ePO로 관리하여 정책 및 사고 관리를 간소화합니다.[4]
- McAfee® MVISION Cloud(CASB) 및 McAfee® Network DLP와 동일한 정책 및 분류 엔진, 사고 워크플로우를 공유합니다.
- 다양한 정책과 재사용 가능한 규칙 세트를 통해 조직 전반에서 여러 DLP 정책을 정의하고, 사무실, 부서, 규정 등에 따라 정책을 작성할 수 있도록 돕습니다.
- 사고 관리에 대한 정밀 제어 성능이 향상되어 원하는 사고 속성(예: 장치 일련 번호, 증거 파일 이름, 그룹 등)별로 쿼리, 필터링, 조회할 수 있습니다.
- 중앙 집중식 이벤트 모니터링 및 감사 기능.
- 정책 관리 및 사고 검토를 위한 개선된 역할 기반 액세스 제어(업무 분장이라고도 함).
- Help Desk 인터페이스에 손쉽게 액세스.

지원되는 플랫폼

- Windows 10(32비트 및 64비트)
- Windows 8 또는 8.1(32비트 및 64비트)
- Windows 7(32비트 및 64비트)
- Windows Server 2019
- Windows 2016(64비트)
- Windows 2012(64비트) 및 Windows 2012 R2(64비트)
- Windows 2008(32비트 및 64비트) 및 Windows 2008 R2(32비트 및 64비트)
- macOS Catalina 10.15 이상
- macOS Mojave 10.14 이상
- macOS High Sierra 10.13 이상
- macOS Sierra 10.12 이상
- OS X El Capitan 10.11 이상
- OS X Yosemite 10.10 이상
- OS X Mavericks 10.9.0 이상

지원 브라우저

- Internet Explorer 버전 11 이상
- Mozilla Firefox 48 이상
- Google Chrome 65 이상

컴플라이언스 시행 및 사용자 교육

기업 경계가 사라짐에 따라 회사에서 컴플라이언스를 시행하는 것이 점점 더 어려워지고 있습니다. McAfee DLP Endpoint를 사용하면 최종 사용자의 일상 동작을 모니터링할 수 있을 뿐만 아니라, 사용자 교육을 통해 컴플라이언스를 보장할 수 있습니다. 단추 하나만 클릭하면 간단하게 사용할 수 있는 McAfee DLP Endpoint는 자세한 보고서를 제공하여 감사자, 상급 관리자 및 기타 관계자에게 내부 및 규정 컴플라이언스 수단이 올바르게 적용되고 있음을 입증합니다. 또한 규정 및 사용 사례에 템플릿화된 정책을 제공하여 컴플라이언스를 쉽게 유지할 수 있도록 해줍니다. 사용자는 회사 정책에 따라 시행 그룹으로부터 실시간 피드백을 받게 되며, 이러한 소규모 교육 기회를 통해 강력한 회사 보안 문화를 구축할 수 있습니다.

지원되는 McAfee ePO 소프트웨어

- McAfee ePO 5.9.1 및 5.10 (DLP 11.1 이상)

McAfee MVISION ePO(SaaS) 지원

- DLP 11.5 이상은 소프트웨어 또는 DLP 확장을 설치할 필요가 없습니다. MVISION ePO에 액세스하려면 인증을 위한 사용자 이름과 암호가 필요합니다.

지원되는 플랫폼, 브라우저 및 소프트웨어의 전체 목록은 McAfee 기술 자료를 참조하십시오.

자세히 알아보기

자세한 내용은 www.mcafee.com/kr/products/dlp-endpoint.aspx를 참조하십시오.

1. 일관된 McAfee 내부 랩 테스트를 기준으로 합니다.
2. McAfee DLP Endpoint 버전 11.5 이상
3. 동일 자료
4. 동일 자료

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