McAfee Data Loss Prevention Discover

위치에 관계없이 중요한 데이터를 찾고 분류하고 보호합니다.

주요 이점

데이터 유출 위험 식별

- 사내에 또는 클라우드에 저장된 정보를 검색합니다.
- 중요한 데이터가 저장된 위치 및 콘텐츠 소유자 파악
- 직관적인 인터페이스를 통해 데이터 검색 및 검색된 모든 데이터 보기

정책 및 사용자 정의 보고서 작성

- 쿼리 수행 후 보호 규칙으로 결과 전송
- 사전에 수립된 컴플라이언스, 기업 관리 및 지적 재산 정책 사용
- 인접한 정보 보안 시스템에 중요한 정보 등록

데이터 유출의 분류, 분석 및 교정

- 멀티 벡터 분류를 통해 중요한 정보 필터링 및 제어
- 중요한 데이터를 파악할 수 있도록 모든 콘텐츠를 색인화한 후 쿼리하고 마이닝
- 문서와 그 안에 포함된 정보를 보호하기 위해 정보가 표절되거나 위치가 바뀐 경우에도 시그니처 등록 및 생성
- 콘텐츠가 보호 정책을 위반한 경우 경고 알림 전송

노트북, 공유 파일 서버, 클라우드 저장소에 있는 중요 정보로 인해 조직이 위험에 처할 수도 있습니다. 테라바이트 및 페타바이트에 이르는 대용량 정보에 대한 보안이 필요합니다. 중요한 정보에 늘 적절하게 레이블이 지정되어 있는 것이 아니기 때문에 적절한 보안을 제공하는 것은 특히 어렵습니다. 또한 대부분의 조직에서는 액세스 제어를 사용하더라도 중요한 데이터가 위험에 노출되어 있는지 파악하거나 이러한 데이터가 확산되는 곳을 알 수 있는 방법이 없습니다. 일반적으로 중요한 데이터는 신용카드 또는 주민등록번호와 같이 구조화된 데이터보다 정의하기가 더 까다로운 지적 재산(IP)과 같이 구조화되지 않은 데이터로 구성되어 있기 때문에 문제가 더 복잡해 집니다. McAfee® Data Loss Prevention(DLP) Discover는 중요한 데이터를 찾아서 분류하고 그 데이터가 어떻게 사용되는지 파악하며 도난이나 유출로부터 보호합니다.

McAfee DLP Discover의 새로운 기능

McAfee DLP Discover는 이제 클라우드 저장소에 있는 데이터를 스캔하고 보호할 수 있습니다. McAfee ePolicy Orchestrator® (McAfee ePO™) 중앙 집중식 관리 소프트웨어에서 쉽게 정책을 정의하고 스캔을 자동화하고 미리 예약할 수 있습니다. 문제에 대한 특별 보고와 상세한 분석이 제공됩니다.

기능 하이라이트:

- 소프트웨어 전용 McAfee DLP Discover는 하드웨어나 VM 기반 어플라이언스가 필요 없기 때문에 비용이 더욱 절약됩니다.
- McAfee ePO 소프트웨어로 완벽한 배포와 관리가 가능합니다. DLP Endpoint와 동일한 관리 확장과 DLP 정책을 공유합니다.
- DLP Endpoint 분류 기능에 완벽히 대응합니다.
- Windows Server 2008 및 Windows Server 2012와 호환됩니다.
- 기존 서버의 유휴 용량을 활용하는 분산 배포를 지원하고 넓은 지역에 걸쳐 배포할 수 있습니다.
- DLP Discover 어플라이언스 버전 9.3.x 또는 DLP Discover 소프트웨어 전용 버전 9.4를 위한 호환 사용권.

intel Security

사양

내용 유형
다음을 비롯하여 300개 이상의 콘텐츠 유형에 대한 파일 분류 지원

- "Box" 클라우드 저장소
- Microsoft Office 문서
- 멀티미디어 파일
- 소스 코드
- 디자인 파일
- 보관
- 암호화된 파일
- 기본 제공 정책
- 지적 재산

지원되는 리포지토리
- Common Internet File System (CIFS)/Server Message Block (SMB)[1]
- Network file system (NFS)
- HTTP/HTTPS
- FTP/FTPS
- Microsoft SharePoint[1]
- EMC Documentum
- 데이터베이스: Microsoft SQL, Oracle, DB2, MySQL Enterprise

문서 등록

문서를 모든 리포지토리에서 등록할 수 있습니다. 등록된 문서의 시그니처를 중요한 자료의 확산 탐지를 위해 로컬로 사용하거나 다른 McAfee DLP 어플라이언스에서 사용하도록 설정할 수 있습니다.

보고

사고 및 검색 결과 보기를 위한 강력한 분석 엔진을 통해 컨텍스트에 맞는 두 개의 피벗 포인트를 기반으로 요약 보기를 사용자 지정할 수 있습니다. 목록 및 세부 정보 보기와 경향이 제공되는 요약 보기를 사용할 수 있습니다. 사전에 작성된 사용자 지정 가능한 보고서가 시스템에 20개 이상 제공됩니다.

중요한 데이터의 유실 방지

소스 코드, 영업 비밀, 전략적 비즈니스 계획, IP 및 기타 정보 자산은 브랜드, 대외적 평판 및 경쟁 우위에 중요합니다. 전송 중 데이터를 보호하는 것도 중요하지만 중요한 데이터에 대한 부적절한 액세스 또는 이동이 발생하기 전에 데이터를 보호하고 중요한 데이터가 있는 위치를 파악하는 것이 무엇보다 중요합니다.

McAfee DLP Discover를 통해 조직에서 데이터 유실을 방지할 수 있습니다. 보호하려는 콘텐츠를 정확히 파악해야 했던 기존 솔루션과 달리 McAfee DLP Discover는 명백한 정보에 대한 종합적인 보호를 제공하므로 명백하지 않는 정보를 찾을 수 있습니다.

보호해야 할 정보 확인

정보 및 확산 위험을 파악하기 위해 특정 리포지토리를 검색하고 확실한 보호가 필요한 데이터를 식별할 수 있도록 McAfee DLP Discover를 구성할 수 있습니다. 또한 McAfee DLP Discover가 크롤링하는 모든 데이터가 색인화되어 직관적인 인터페이스를 통해 이러한 데이터에 액세스할 수 있으므로 콘텐츠 소유자와 저장 위치를 파악하기 위해 중요한 데이터를 신속하게 검색할 수 있습니다.

보호 정책 정의

보호할 정보를 파악하면 McAfee DLP Discover를 통해 해당 정보를 정확하게 보호할 수 있습니다. McAfee DLP Discover는 직관적인 통합 정책 생성, 보고 및 관리 성능을 제공하므로 보관 중인 데이터에 대한 정보 보호 전략을 보다 강력히 제어할 수 있습니다. McAfee DLP Discover의 정책, 규칙 및 분류의 주요 이점은 다음과 같습니다.

- 간단한 초기 사용자 환경을 위한 다양한 기본 제공 정책
- 단순하게 구조화된 데이터(신용카드, 주민등록번호)부터 복잡한 정보(지적 재산)에 이르는 강력한 규칙 구성 엔진
- 보호 규칙으로 검색 결과 분석을 전송하여 규칙 작성 및 확인 간소화
- 일관된 보호를 위한 인접 정보 보안 벡터와의 통합
- 정상적인 정보에서 사고가 발생하지 않도록 공개 문서 및 일반 텍스트 제외

네트워크에서 위반 검색

정책 정의 후 정책 위반이 발생했는지 네트워크 리소스를 정기적으로 검색하도록 McAfee DLP Discover를 설정할 수 있습니다. 또한 유연한 일정 계획 옵션을 이용해 지속적으로, 매일, 매주 또는 매월 검색을 실시할 수 있습니다.

McAfee DLP Discover는 랩톱, 데스크톱, 서버, 문서 리포지토리, 포털 및 파일 전송 위치를 비롯한 액세스 가능한 모든 리소스에서 정책 위반이 발생했는지 자동으로 검색합니다. IP 주소, 서브넷, 범위 또는 네트워크 경로를 기반으로 검색 그룹을 정의할 수 있습니다. 또한 시스템 폴더가 아니라 모든 사용자의 내 문서 폴더만 검색하거나 특정 사용자가 소유한 파일이나 특정 형식 또는 크기의 파일을 검색하는 것처럼 특정 매개 변수를 기반으로 검색 작업을 집중할 수 있습니다.

위반 사항 검토 및 교정

DLP Discover는 통합 사건 워크플로와 사례 관리를 통해 중요한 자료의 확산을 제거 또는 최소화합니다. McAfee DLP Discover는 보호 정책을 위반하는 콘텐츠를 찾은 경우 사건을 생성하고 통보를 전달합니다. McAfee DLP Discover에서 생성된 사고를 사례 관리 프레임워크에 추가하여 회사 내 다양한 조직의 전문가가 위반에 대한 조치를 취하기 위해 협력할 수 있습니다. 또한 위험 대시보드는 보안 담당자가 정책 위반 사항에 대한 프로파일을 확인하여 관심 있는 저장된 매개 변수의 데이터를 기반으로 보고서를 생성할 수 있는 손쉬운 방법을 제공합니다.

사양: 소프트웨어 전용

McAfee DLP Discover는 소프트웨어 버전으로 제공됩니다. 아래는 시스템 최소 요구 사항입니다.

하드웨어 요구 사항

- CPU: Intel Core 2 64비트
- RAM: 최소 4GB
- 디스크 공간: 최소 100GB

지원되는 플랫폼

- Windows Server 2008 R2 Standard, 64비트
- Windows Server 2012 Standard, 64비트
- Windows Server 2012 R2 Standard, 64비트

지원되는 가상화 시스템

- vSphere ESXi 5.0 업데이트 2
- vCenter Server 5.0 업데이트 2

McAfee ePO 소프트웨어 및 에이전트

- McAfee ePO 4.6.8 이상, 5.1 이상
- McAfee Agent 4.8.2 이상, 5.0 이상

저장된 데이터 캡처 및 분석

McAfee DLP Discover는 네트워크 리소스를 검색하여 정책 위반사항을 찾을 뿐만 아니라 네트워크에서 찾은 저장된 모든 콘텐츠를 색인화하여 중요한 데이터를 파악할 수 있도록 해당 정보를 쿼리 및 마이닝할 수 있는 기능을 제공합니다. McAfee DLP Discover를 통해 중요한 데이터와 이러한 데이터의 사용 방법, 소유자, 저장 위치 및 확산된 위치를 신속하게 파악할 수 있습니다.

복잡한 데이터 분류

McAfee DLP Discover를 통해 조직에서는 고정된 형식의 일반적인 데이터부터 복잡하고 매우 가변적인 지적 재산에 이르기까지 모든 종류의 중요한 데이터를 보호할 수 있습니다. McAfee DLP Discover는 이러한 개체 분류 메커니즘의 입력된 정보를 결합하여 매우 정확한 멀티 벡터 분류를 구축할 수 있습니다. 이러한 분류는 중요한 정보를 필터링 및 제어하고 숨겨져 있거나 알려지지 않은 위험을 파악하는 검색을 수행하는데 사용됩니다. 개체 분류 메커니즘은 다음과 같습니다.

- 다단계 분류: 컨텍스트에 맞는 정보와 계층적 형식의 콘텐츠를 모두 포함합니다.
- 문서 등록: 변화하는 정보의 생체 인식 시그니처를 포함합니다.
- 문법 분석: 텍스트 문서부터 스프레드시트 및 소스 코드에 이르기까지 모든 유형의 문서에서 문법 또는 구문을 검색합니다.
- 통계 분석: 특정 문서 또는 파일에서 시그니처, 문법 또는 생체 인식 일치가 발생한 횟수를 추적합니다.
- 파일 분류: 파일 또는 압축에 적용된 확장명과 관계 없이 콘텐츠 유형을 식별합니다.

사양: McAfee DLP 5500 어플라이언스

McAfee DLP Discover는 물리적 또는 가상 어플라이언스로 제공됩니다. 아래는 어플라이언스 사양입니다.

구성 요소	설명
프로세서	Intel E5-2620 6 코어 2개, 15MB 캐시, 2.0 GHz, 7.20GT/s Intel QPI
메모리	32GB DDR3-1333MHz
전원 공급 장치	2 x 760W 핫스왑 전원 공급 장치 모듈
하드 드라이브	2TB SATA 7200RPM 드라이브 8개
NIC 카드	Intel Dual Copper 1Gbps 이더넷 I/O 모듈
IPMI	Intel Remote Management Module 4(AXXRMM4)
제품 크기	2 랙 유닛(2U)

사양: 가상 시스템

McAfee DLP Discover는 VMware 환경에서 실행될 수 있는 가상 어플라이언스로 제공됩니다. 다음은 가상 어플라이언스 실행을 위한 최소 하드웨어 요구 사항입니다.

구성 요소	요구 사항
프로세서	Intel x86 vCPU 4개
메모리	16GB RAM
하드 디스크 드라이브	드라이브 1: 최소 크기, VM 소프트웨어용 100GB 드라이브 2: 최소 크기, DLP 가상 이미지용 512GB
네트워크	가상 NIC 4개
BIOS	VT 스레드 사용

1. McAfee DLP Discover 9.4 소프트웨어 전용 버전은 현재 CIFS, Microsoft SharePoint 2010, 및 Microsoft SharePoint 2013을 지원합니다.

McAfee. Part of Intel Security.
서울특별시 강남구 역삼동 737
강남파이낸스센터 5층 135-984
+82.2.3458.9800
www.intelsecurity.com