데이터시트

McAfee DLP Prevent

중요한 정보 보호를 위한 정책 시행

전자적으로 정보를 공유하는 사람들이 늘어날수록 누군가가 실수 또는 의도적으로 권한이 없는 개인에게 중요한 데이터를 전송하거나 회사의 기밀 데이터를 위험에 노출시킬 가능성이 커지고 있습니다. 이메일, 웹, IM(메신저) 또는 FTP와 같은 여러 가지 다양한 전자적 채널을 거쳐 정보가 회사에서 빠져나갈 수 있습니다. 일부 메시지 또는 트랜잭션은 허용 가능하지만 데이터 개인 정보 보호를 위해 암호화되어야 합니다. 다른 유형의 통신은 모든 경우에 허용되지 않으며 차단되어야 합니다. 적시에 적절한 정책을 시행하는 것은 데이터 보안, 규정 컴플라이언스 및 지적 재산 보호에 중요합니다.

전송 중인 데이터에 대한 보안 정책 시행

모든 기업의 각 부서에서 개인은 여러 응용프로그램과 다양한 프로토콜을 사용하여 데이터를 공유하고 있습니다. 중요한 정보가 네트워크 외부로 빠져나가지 않도록 사전에 예방하고 올바른 비즈니스 프로세스를 시행하여 실수 또는 의도적인 데이터 손실을 방지합니다.

McAfee® DLP Prevent는 SMTP(Simple Mail Transfer Protocol) 또는 ICAP-컴플라이언트 웹 프록시를 사용하여 MTA(Message Transfer Agent) 게이트웨이와 통합함으로써 전자 메일, 웹 메일, 메신저, Wikis, 블로그, 포털, HTTP/HTTPS 및 FTP 전송을 통해 네트워크에서 빠져나가는 정보에 대한 정책을 시행할 수 있도록 지원합니다. 정책 위반 발견 시 McAfee DLP Prevent를 통해 암호화 적용, 차단, 리디렉션, 검역 등을 비롯한 다양한 조치를 취할 수 있습니다. 따라서 중요한 정보 보호를 제어하는 규정 컴플라이언스를 보장하고 보안 위협을 약화시킬 수 있습니다.

McAfee ePolicy Orchestrator 소프트웨어와 완전히 통합

McAfee DLP Prevent는 공통 정책, 사건 및 사례 관리와 함께 McAfee® ePolicy Orchestrator®(McAfee ePO™) 소프트웨어 및 McAfee® Data Loss Prevention Endpoint(McAfee DLP Endpoint)와 완전히 통합됩니다. 관리자는 McAfee ePO 소프트웨어에서 하나의 이메일과 웹 보호 정책을 생성하여 이를 엔드포인트 및 네트워크에 배포할 수 있습니다. 또한 McAfee DLP Endpoint 및

주요 이점

기존 인프라 활용

- 차단, 바운스, 암호화, 검역 및 리디렉션에 X-헤더가 지정된 SMTP를 사용하여 MTA(Message Transfer Agent) 게이트웨이와의 통합을 통해 회사 전자 메일 보호
- ICAP(Internet Content Adaptation Protocol)-컴플라이언트 웹 프록시와의 통합을 통한 트래픽 시행으로 HTTP, HTTPS, IM, FTP 및 웹 메일을 통한 콘텐츠 위반 차단

사전 예방 차원에서 모든 유형의 정보에 대한 정책 시행

- 300개 이상의 고유한 콘텐츠 유형 보호
- 중요하다고 알려진 정보 이외에도 미처 파악하지 못한 정보에 대한 정책 시행
- 동시에 수십만 개의 연결을 지원하도록 확장

McAfee에 문의

McAfee DLP Prevent는 단일한 이메일과 웹 정책을 허용하는 공통 분류 엔진을 공유합니다. 공통 사전과 정규 표현식(regex) 구문은 공통적인 웹 및 이메일 보호 규칙을 생성하기 위한 연속성을 제공합니다. McAfee DLP 솔루션은 중앙 집중식 관리를 통해 단일창 가시성을 제공하며 비즈니스 효율성 향상을 돕고 관리 간접 비용을 줄여줍니다.

모바일 이메일 모니터링

모바일 전자 메일용 McAfee® DLP Prevent는 DLP 기능으로 ActiveSync 프록시를 통해 모바일 장치로 다운로드되는 이메일을 차단하여 모바일 이메일에 콘텐츠 인식형 보호 기능을 제공합니다. 또한 사내 Microsoft Exchange 및 Microsoft Office 365 Hosted Exchange 모두에서 ActiveSync를 차단할 수 있습니다. McAfee ePO 소프트웨어에서 완전하게 제어되며 McAfee DLP Prevent 라이센스의 일부로 포함됩니다. 모바일 장치에 에이전트를 설치할 필요가 없습니다. 모바일 전자 메일용 McAfee DLP Prevent를 통해 엔터프라이즈는 규정 준수 및 증거 수집을 위해 이메일을 모니터링할 수 있으며 관리형 및 비관리형 모바일 장치를 모두 보호할 수 있습니다.

웹 프록시 및 MTA와 통합해 보호 향상

McAfee DLP Prevent는 필요한 조치를 취하기 위해 웹 프록시(ICAP 사용) 및 MTA(X-헤더 사용)와 통합됩니다. 응용프로그램의 동작을 수정하는데 아무런 조치를 취하지 않는 TCP 세션을 단순히 삭제하는 대신, 응용프로그램 계층에서 권한이 없는 트랜잭션을 종료함으로써 McAfee DLP Prevent는 시작 응용프로그램에 정책 위반으로 인해 전송이 거부되었음을 알립니다. 따라서 McAfee DLP Prevent에서 보호해야 할 정보를 파악하고 응용프로그램이 동일한 동작을 시도하지 못하도록 방지하므로 조직의 데이터 보안을 향상시킬 수 있습니다.

알려지거나 알려지지 않은 중요한 정보 보호

300개 이상의 다양한 콘텐츠 유형을 분류할 수 있는 기능을 통해 McAfee DLP Prevent는 주민등록번호, 신용카드 번호 및 재무 데이터와 같이 알려진 정보를 기밀로 유지하도록 도와줍니다. 또한 이는 고도로 복잡한 지적 재산 등 보호가 필요한 정보나 문서가 어떤 것인지 파악하는 데 도움이 됩니다. McAfee DLP Prevent에는 컴플라이언스부터 지적 재산의 적절한 사용에 이르기까지 광범위한 정책이 기본적으로 포함되어 있습니다. 따라서 전체 규칙 집합에 문서의 전체 또는 일부를 일치시켜 알려지거나 알려지지 않은 중요한 정보를 모두 보호할 수 있습니다.

보기 및 사건 보고서 사용자 지정

McAfee ePO 소프트웨어를 이용해 컨텍스트에 맞는 두 가지 피벗점을 기준으로 보안 사건 및 후속 조치에 대한 요약 보기를 사용자 지정할 수 있습니다. 목록 및 세부 정보 보기와 경향이 반영된 요약 보기를 손쉽게 사용할 수 있습니다. 또한 McAfee DLP Prevent에는 사전에 작성된 수 많은 보고서가 포함되어 있으며 이러한 보고서를 보거나, 이후에 사용할 수 있도록 저장하거나 정기적으로 제공되도록 예약할 수도 있습니다.

데이터 유출 분류, 분석 및 처리

- 알려진 위험 및 알려지지 않은 위험으로부터 보호하기 위해 중요한 정보 필터링 및 제어
- 모든 유형의 콘텐츠에 대해 세분화된 보안 정책 색인화 및 시행
- 사용자가 무단으로 정보 또는 리포지토리에 액세스할 수 없도록 내부 파일 공유 액세스에 관한 정책 적용

사양

시스템 처리량

최대 150Mbps의 전체 콘텐츠 분석, 색인화 및 저장 처리량

네트워크 통합

MTA 및 ICAP-컴플라이언트 웹 프록시를 사용하여 데이터 경로 내에서 활성 상태인 오프패스(off-path) 어플라이언스로 네트워크에 통합

내용 유형

다음과 같은 300개 이상의 콘텐츠 유형에 대한 파일 분류 지원

- Microsoft Office 문서
- 멀티미디어 파일
- P2P
- 소스 코드
- 디자인 파일
- 보관
- 암호화된 파일

복잡한 데이터 분류

McAfee DLP Prevent를 통해 조직에서는 고정된 형식의 일반적인 데이터부터 복잡하고 매우 가변적인 지적 재산에 이르기까지 모든 종류의 중요한 데이터를 보호할 수 있습니다. 이러한 개체 분류 메커니즘을 결합하여 McAfee DLP Prevent는 중요한 정보를 차단하고 숨겨져 있거나 알려지지 않은 위험을 파악하는 매우 정확하고 세밀한 분류 엔진을 활용합니다. 개체 분류 메커니즘은 다음과 같습니다.

- **다단계 분류:** 컨텍스트에 맞는 정보와 계층적 형식의 콘텐츠를 모두 포함합니다.
- **문서 등록:** 변화하는 정보의 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.

포렌식 및 규칙 조정 기능

고유한 캡처 기능으로 자체 기록 데이터를 활용하여 추측, 수개월의 시행착오 또는 비즈니스 중단 없이 훨씬 빠르고 효율적으로 배포할 수 있습니다. 따라서 계속 변하는 비즈니스 요구에 따라 정확하게 DLP 규칙(분류 조정 포함)을 세밀하게 조정할 수 있습니다. 캡처 기술은 사후 디지털 녹화기 역할을 하고 사후 DLP 사고를 재생하여 포렌식 조사에도 도움이 되며 철저한 조사가 가능합니다. 캡처 기술은 가상 환경 또는 SAS 케이블을 통해 NDLP 6600 어플라이언스에 연결된 2U 16TB 스토리지 어레이로 이용 가능합니다.

폼 팩터 및 어플라이언스 옵션

McAfee DLP Prevent는 하드웨어 어플라이언스 또는 가상 어플라이언스로 제공됩니다. 자세한 내용은 **McAfee DLP 6600 하드웨어 어플라이언스 데이터시트**에서 참조하십시오.

프로토콜 지원

ICAP-컴플라이언트 프록시에 대해 ICAP 프로토콜을 통해 HTTP, HTTPS, FTP 및 메신저 프로토콜을 지원합니다. 프록시에서 지원하는 프로토콜에 대해서는 해당 프록시 공급업체에 문의하십시오. MTA와의 통합을 통해 SMTP를 지원합니다.

기본 제공 정책

- 컴플라이언스 규제정책, 지적 재산 및 허용 가능한 사용을 비롯하여 일반적인 요구 사항에 대한 광범위한 정책 및 규칙을 기본적으로 제공합니다.
- McAfee 캡처 데이터베이스를 활용하여 규칙을 사용자 정의함으로써 비즈니스 관련 요구 사항을 충족합니다.

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