McAfee Data Loss Prevention Monitor

중요한 데이터를 보호합니다.

오늘날 모든 사람들은 고객 및 직원의 개인 정보 데이터(예: 주민등록번호, 신용카드 번호 또는 기타 개인 정보)의 보호를 염두에 두고 있습니다. 직원의 실수, 랩톱 분실 및 잘못 놔둔 USB 장치로 인한 우발적인 데이터 공개는 거의 모든 조직의 보안 과제입니다. 문제를 더욱 악화시키는 것은 Google Gmail, Yahoo! Mail, 메신저, Facebook 등의 웹 응용프로그램을 통해 데이터를 전송 및 공유할 경우 데이터가 유출되어 결국 잘못 악용될 수 있다는 점입니다. McAfee® Data Loss Prevention (DLP) Monitor는 모든 인터넷 통신을 분석하고 정보가 잘못된 곳으로 전송되지 않았는지 확인할 수 있는 고성능 데이터 손실 방지 솔루션입니다. 이 솔루션은 보안 팀의 작업 부담을 최소화하고, 컴플라이언스 요구 사항을 충족하며, 지적 재산 및 기타 중요한 자산을 보호할 수 있도록 지원합니다.

주요 이점

중요한 정보 파악 및 보호

- 직관적 검색 엔진을 통해 중요한 정보를 신속하게 파악
- 포렌식 분석을 수행하여 현재 및 과거 위험 이벤트의 상관 관계를 밝히고, 위험 추세 감지 및 위협 식별
- 향후 동작 방지를 위한 즉각적인 규칙 생성

모든 네트워크 트래픽 캡처 및 색인화

- 중요한 정보를 필터링 및 제어하여 숨겨져 있거나 알려지지 않은 위험 파악
- 모든 유형의 콘텐츠를 색인화한 다음 쿼리 및 마이닝하여 중요한 데이터와 해당 데이터의 전송 위치 파악
- 내부 파일 공유 액세스 모니터링

정교한 규칙 작성 및 조정

- 모든 포트 및 응용프로그램에서 300개 이상의 고유한 콘텐츠 유형 식별
- 포트와는 독립적으로 네트워크 트래픽 분류
- 동시에 수십만 개의 연결을 지원하도록 확장

이동 중 데이터 모니터링, 추적 및 보고

어떤 업계에 있든지 모든 응용프로그램, 프로토콜, 포트에 있는 모든 형태의 중요한 정보를 정확하게 파악하기 위한 가시성이 필요합니다.

McAfee DLP Monitor를 사용하면 전체 네트워크에서 실시간으로 데이터를 수집, 추적 및 보고할 수 있으므로 사용자와 조직 간에 주고받는 정보와 그 방식을 파악할 수 있습니다. 모든 포트 또는 프로토콜을 통과하는 300개 이상의 콘텐츠 유형을 고유하게 탐지하는 고성능 맞춤형 어플라이언스인 McAfee DLP Monitor를 통해 데이터에 대한 위협을 감지하고 데이터 유실로부터 조직을 보호하기 위한 조치를 취할 수 있습니다. 또한 McAfee DLP Monitor는 손쉽게 최종 사용자에게 알림을 보내 사용자에게 데이터 유실 위반에 대해 알려 다른 동작을 취하게 할 수 있습니다.

실시간 정보 검색 및 분석

SPAN 또는 탭 포트를 사용하여 네트워크로 통합된 McAfee DLP Monitor는 네트워크 트래픽을 실시간으로 검색 및 분석합니다. 컴플라이언스부터 지적 재산의 적절한 사용에 이르는, 150개 이상의 사전 수립된 규칙을 사용하여 McAfee DLP Monitor는 세부적인 표절을 비롯해 전체 및 부분 문서를 전체 규칙 모음과 일치시킵니다. 따라서 규모에 관계 없이 네트워크 트래픽에서 이상한 점을 감지할 수 있습니다.

intel Security

사양

시스템 처리량

- 샘플링 없이 최대 200Mbps로 콘텐츠 분류

네트워크 통합

- SPAN 포트 또는 물리적 인라인 네트워크 탭(옵션)을 사용하여 네트워크에 수동으로 통합

내용 유형

다음을 비롯하여 300개 이상의 콘텐츠 유형에 대한 파일 분류 지원

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

프로토콜 지원

- 전송 프로토콜로 TCP를 사용하는 모든 프로토콜이나 포트를 통한 모든 전송을 지원합니다.
- HTTP, HTTPS, SMTP, IMAP, POP3, FTP, Telnet, Rlogin, SSH, 웹 메일, Yahoo! Chat, AOL Chat, MSN Chat, ICY, RTSP, SOCKS, PCAnywhere, RDP, VNC, SMB, Citrix, Skype, IRC, LDAP, DASL, NTLM, Kazaa, BitTorrent, eDonkey, Gnutella, DirectConnect, MP2P, WinMX, Sherlock, eMule 등에 대한 프로토콜 처리기가 포함됩니다.

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.

이전에 고려하지 못했던 위험 탐지

실시간 규칙과 일치하는 정보뿐만 아니라 모든 네트워크 트래픽의 자세한 분류, 색인 및 저장소를 통해 McAfee DLP Monitor에서 기록 정보를 신속하게 활용하여 중요한 정보, 해당 정보의 사용 방식, 사용자 및 전송 위치를 파악할 수 있습니다. 또한 정보를 세분화하여 조사하고 정보 기록을 조사하여 이전에 고려한 적이 없었던 위험 이벤트 및 데이터 노출을 탐지할 수 있습니다. McAfee DLP Discover와 함께 배포하면 네트워크 내에서 데이터의 저장 위치 및 데이터 소유자를 파악할 수도 있습니다.

사건 보고서를 보고 필요한 조치 알리기

McAfee DLP Monitor는 자체 분류 엔진을 사용하여 트래픽을 검색, 분석 및 분류한 다음 고유한 데이터베이스에 관련 정보를 모두 저장합니다. 직관적인 검색 인터페이스를 사용하여 정보, 전송한 사람, 전송 위치 및 사용 방법으로 구성된 종합적인 보고서를 볼 수 있습니다. 따라서 유출되는 정보, 유출 위치 및 방법을 파악할 수 있습니다. 이러한 정보를 바탕으로 규정 컴플라이언스를 보장하고 중요한 데이터를 보호하기 위한 다양한 작업을 적용하여 위협을 처리하기 위한 조치를 취할 수 있습니다.

사양: McAfee DLP 5500 Appliance

구성 요소	설명
프로세서	Intel E5-2620 6 코어 2개, 15M 캐시, 2.0GHz, 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)

모든 유형의 데이터 분류

McAfee DLP Monitor를 통해 조직에서는 고정된 형식의 일반적인 데이터부터 복잡하고 매우 가변적인 지적 재산에 이르기까지 모든 종류의 중요한 데이터를 검색할 수 있습니다. 이러한 개체 분류 메커니즘을 결합하여 McAfee DLP Monitor는 중요한 정보를 필터링하고 숨겨져 있거나 알려지지 않은 위험을 파악하는 매우 정확하고 세밀한 분류 엔진을 구축합니다.

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.

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