McAfee Enterprise Log Manager

자동 로그 수집, 스토리지 및 관리를 통해 컴플라이언스 비용 절감

로그를 바르게 수집하고 저장하면 거부할 수 없는 활동에 대한 분명한 감사 추적을 통해 컴플라이언스 비용을 줄일 수 있습니다. McAfee® Enterprise Log Manager는 모든 로그 파일을 효율적으로 수집, 압축 및 저장합니다. McAfee Enterprise Security Manager와의 통합으로 고급 검색, 분석, 상관관계, 경고, 리포팅을 제공합니다. 모든 이벤트 및 경고는 원래의 소스 로그 기록에 대한 간편한 원클릭 액세스를 제공하므로 포렌식 작업에도 도움이 됩니다.

주요 이점

- 컴플라이언스 요구 사항 충족을 위한 일반 로그 수집 및 보존
- 각 로그 소스에 적합한 유연한 스토리지 및 보존
- 관리 연속성 및 포렌식 지원
- 로그 분석 및 검색
- 로그를 로컬로 저장하거나 관리형 SAN(Storage Area Network)을 통해 저장
- McAfee Enterprise Security Manager와 완전히 통합
- 유연한 혼합 배달 옵션에는 물리적 어플라이언스 및 가상 어플라이언스가 포함됩니다.

McAfee Enterprise Log Manager는 모든 로그 파일을 수집하고 서명하며 저장합니다. McAfee는 Microsoft Windows 이벤트 로그, 데이터베이스 로그, 응용프로그램 로그, 시스템 로그를 포함한 모든 로그 유형 분석 및 로그 관리를 자동화합니다. 로그는 서명되고 검증되므로 규정 컴플라이언스의 필수 요소인 인증과 무결성을 보장합니다. 기본 제공 컴플라이언스 규칙 세트와 보고서를 통해 조직이 규정을 준수하고 있으며 정책이 시행 중임을 간단하게 증명할 수 있습니다.

이처럼 긴밀히 통합된 로그 수집, 관리 및 분석 환경은 보안 프로파일을 강화하고 PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA 및 SOX와 같은 표준 준수 기능을 크게 개선합니다.

지능형 로그 관리

McAfee Enterprise Log Manager는 지능적으로 로그를 수집하고 컴플라이언스에 적합한 로그를 저장하며 보안에 적합한 로그를 분석합니다. 특정 컴플라이언스 요구 지원이 필요한 경우 언제나 로그를 원래의 형식으로 보존할 수 있습니다. McAfee는 원래의 로그 파일을 변경하지 않기 때문에 관리 연속성 및 거부할 수 없는 작업을 지원합니다.

정보 보존 필요성은 로그 소스와 반드시 준수해야 하는 다양한 컴플라이언스 요구 사항에 따라 달라집니다. McAfee Enterprise Log Manager는 쉽게 사용자 지정할 수 있는 스토리지 풀을 사용하여 로그가 적절한 기간 동안 올바르게 저장됨을 보장합니다. 어플라이언스의 하드 드라이브 디스크 스토리지와 고속 SAN을 위한 파이버 채널 카드 옵션 등 수요에 적합한 최적의 스토리지 옵션을 선택하십시오.

로그 파일 자체로는 필요한 모든 것을 알 수는 없습니다. 로그 파일은 중요한 증거를 포함하며 관리 연속성을 확립하는 핵심적인 연결 고리이지만 중요한 보안 문제를 제기하기도 합니다. 예를 들어 액세스 로그에서 사용자 이름을 볼 수 있지만 사용자의 역할이나 권한에 대한 정보는 알 수 없습니다. 또한 어떤 시스템을 액세스했는지 알 수 있어도 해당 시스템이 어떤 정보를 사용했는지 또는 누가 이를 액세스해야 하는지는 알 수 없을 수 있습니다.

intel Security

McAfee Enterprise Security Manager와 통합

McAfee Enterprise Log Manager는 McAfee Enterprise Security Manager에 통합되는 구성요소입니다. McAfee Enterprise Log Manager는 로그를 저장하는 반면 McAfee Enterprise Security Manager는 로그 정보를 심층적으로 분석하고 정규화하여 실시간 보안 조사와 사고 응답에 즉시 이용할 수 있습니다.

보안 이벤트가 만들어질 때 분석된 이벤트 파일은 소스 로그 파일 및 특정 로그 기록에 직접 연결되어 이벤트 관리 및 포렌식 과정 중에 원클릭 액세스를 가능하게 합니다. 추가 단계, 추가 실행 응용프로그램이 필요 없으며 수동으로 로그를 검색하느라 시간을 낭비할 필요가 없습니다.

분석을 위한 풍부한 컨텍스트

McAfee Enterprise Security Manager와 McAfee Enterprise Log Manager는 함께 모든 로그에 대한 컨텍스트를 제공하여 모든 분석된 로그 기록의 가치를 높입니다. 정보에는 다음이 포함됩니다.

- 소스 또는 대상 IP 주소
- ID 컨텍스트
- 사용 중인 호스트 이름 또는 서비스
- 취약성 평가 검색기의 취약성 정보
- 네트워크 토폴로지 정보
- 정책 및 개인 정보 보호 정보

유연한 스토리지 풀

McAfee Enterprise Log Manager 스토리지 풀은 장기적인 로그 보존에 대한 유연성을 제공합니다. 스토리지 풀은 다양한 로그 관리 수요를 충족할 수 있도록 여러 물리적 스토리지 장치(로컬 스토리지, NFS, SAN, CIF 및 기타) 그룹에 걸쳐 배포할 수 있는 사용 가능한 스토리지의 가상 그룹입니다.

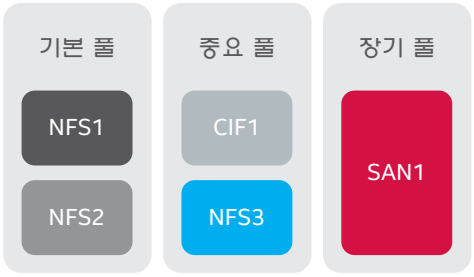

그림 1. 사용자 지정 로그 보존을 지원하는 유연한 스토리지 풀.

스토리지 풀은 여러 장치로 구성될 수 있으며 데이터를 소스 장치에 따라 특정한 풀에 할당할 수 있으므로 로그를 보안, 컴플라이언스, 기밀성 또는 다른 기준에 따라 별도의 위치에 저장할 수 있습니다. 예를 들어 컴플라이언스에 중요한 로그는 여러 중복 네트워크 스토리지 장치로 구성된 풀에 저장 가능합니다. 덜 중요한 로그는 보다 적은 중복 시스템에 저장하고 포렌식에 가장 유용한 로그는 빠른 분석을 위해 로컬로 저장할 수 있습니다.

빠른 배포

단일 조합 어플라이언스를 사용하여 McAfee Enterprise Log Manager와 McAfee Enterprise Security Manager를 함께 구현하거나 가장 큰 엔터프라이즈 네트워크도 지원할 수 있도록 배포할 수 있습니다. 유연한 혼합 배달 옵션에는 물적 및 가상 어플라이언스가 포함됩니다.

인프라와 통합

대부분의 로그 관리 솔루션은 단독으로 작동하는 반면, McAfee Enterprise Log Manager는 다른 정보 보안 시스템과 조화롭게 작동합니다. McAfee Enterprise Log Manager는 McAfee Enterprise Security Manager를 통해 나머지 보안 인프라와 연결되어 보안 작업을 간소화하고 전반적인 효율성을 높이며 비용을 낮춥니다. 강력한 분석, 네트워크 검사, 데이터베이스 이벤트 모니터링 등과 지능적인 로그 관리를 통합할 수 있습니다.

자세한 내용을 보려면 **mcafee.com/siem**을 방문하십시오.

intel Security

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