McAfee Database Activity Monitoring

준수 요구 사항을 충족하는 비용 효율적 데이터베이스 보호

조직에서는 대부분의 중요한 데이터를 데이터베이스에 저장하지만 데이터베이스와 함께 제공되는 경계 보호 및 기본 보안은 오늘날의 정교한 해커 또는 위험한 내부자의 잠재적인 위협으로부터 보호해 주지 못합니다.연구1에 따르면 침해된 레코드의 96% 이상이 데이터베이스와 관련되어 있으며, 이 중 66%는 침해 사실이 몇 개월 이상이나 발견되지 않기도 한다고 합니다. McAfee® Database Activity Monitoring은 네트워크의 데이터베이스를 자동으로 찾아 사전 구성된 일련의 방어 시스템을 통해 데이터베이스를 보호하고, 환경에 대한 사용자 지정 보안 정책 구축할 수 있도록 도와 감사자에게 쉽게 컴플라이언스를 입증하고 중요한 데이터 자산의 더 잘 보호합니다.

주요 이점

- 가시성 및 모든 공격 소스로부터의 보호 극대화
- 외부 위협, 권한이 있는 내부자 및 데이터베이스 내의 정교한 위협 모니터링
- 손상을 입히기 전에 공격을 저지하여 위험 및 책임 최소화
- 신속한 배포와 더 효율적인 아키텍처로 시간 및 비용 절약
- 선택한 IT 인프라에 쉽게 배포할 수 있도록 유연성 제공
- McAfee® ePolicy Orchestrator®(McAfee ePO™) 관리 플랫폼 및 McAfee Vulnerability Manager for Databases와 같은 핵심 McAfee 제품과 통합

조직은 McAfee Database Activity Monitoring을 통해 데이터베이스 내의 권한이 있는 로컬 액세스와 정교한 공격을 비롯한 모든 데이터베이스 활동에 대해 가시성을 확보할 수 있습니다. McAfee Database Activity Monitoring은 외부 위협과 악의적인 내부자로부터 소중하고 중요한 대부분의 데이터를 보호하는 데 유용합니다. McAfee Database Activity Monitoring은 신뢰할 수 있는 감사 추적을 제공할 뿐만 아니라 보안 정책을 위반하는 세션을 종료하여 침입을 방지합니다.

McAfee Database Activity Monitoring을 사용하는 조직에 다음과 같은 이점이 있습니다.

- 업계 규정이나 내부 IT 관리 표준을 충족하기 위한 사용자 지정 보안 정책을 신속하게 구축할 수 있습니다.
- 감사를 위해 전체 트랜잭션 세부 정보 등의 중요한 데이터에 대한 액세스를 기록할 수 있습니다.
- 정책을 위반하는 세션을 종료하고 의심스러운 사용자를 격리하여 데이터 손상을 방지할 수 있습니다.
- 여러 규정에서 요구하는 대로 업무 분장을 유지 관리할 수 있습니다.

McAfee Database Activity Monitoring은 각 데이터베이스 서버의 활동을 로컬로 모니터링하고 실시간으로(가상화된 환경이나 클라우드 컴퓨팅 환경에서 실행될 때에도) 악성 동작에 대해 경고하거나 해당 동작을 종료하여 데이터를 모든 위협으로부터 비용 효율적으로 보호합니다.

모든 데이터베이스 위협 벡터로부터 보호

데이터베이스에 저장된 중요한 데이터를 대상으로 한 공격은 네트워크 전체 및 서버 자체에 로그인한 로컬 사용자로부터 발생할 수 있으며, 저장된 절차나 트리거를 통해 데이터베이스 자체 내부에서도 발생할 수 있습니다. McAfee Database Activity Monitoring에서는 메모리 기반 센서를 사용하여 하나의 비침입 솔루션을 통해 세 가지 유형의 위협을 모두 탐지합니다.그러면 이 정보를 사용하여 감사 용도로 컴플라이언스를 입증하고 조직에서 가장 중요한 데이터의 전반적인 보안을 향상할 수 있습니다.

발생하는 위협을 식별하여 위험 및 책임 축소

피해 이후에 발생한 사항만 알려주는 기본 감사나 로그 분석과는 달리, 실시간 모니터링 및 침입 방지 기능은 손상이 발생하기 전에 위반을 중단합니다.경고는 교정을 위해 정책 위반에 대한 전체 세부 정보와 함께 모니터링 대시보드로 바로 보내집니다.의심스러운 세션을 자동으로 종료하고 악성 사용자를 검역하도록 고위험 위반을 구성하여 보안 팀에 침입을 조사할 시간을 제공할 수 있습니다.

가상 패치를 통해 알려진 취약성 공격 및 여러 제로데이(Zero-Day) 위협으로부터 보호

대부분 응용프로그램 테스트 및 업데이트 적용을 위한 다운타임이 필요하므로 때로는 공급업체 패치를 즉시 설치하지 못할 수 있습니다. 또한 일부 응용프로그램은 패치가 더 이상 제공되지 않는 이전 릴리스의 데이터베이스를 사용하고 있습니다. McAfee Database Activity Monitoring은 일반적인 위협 벡터는 물론 알려진 취약성을 악용하려는 공격을 탐지하며, 실시간으로 경고를 발행하거나 세션을 종료하도록 구성될 수 있습니다.새로 탐색되는 취약성을 위한 가상 패치 업데이트가 정기적으로 제공되며, 이는 데이터베이스 중단 시간 없이 구현되므로 패치가 데이터베이스 공급업체에서 릴리스되어 적용되기 전까지 중요한 데이터를 보호할 수 있습니다.

최소한의 리소스를 사용한 빠르고 비침입적인 배포

소프트웨어 전용 솔루션인 McAfee Database Activity Monitoring은 특수 하드웨어나 추가 서버 없이 한 시간 이내에 구현되어 데이터베이스 보호를 시작할 수 있습니다.또한 McAfee Database Activity Monitoring은 배포를 가속화하여 데이터베이스에 대한 네트워크를 자동으로 검색하고 다양한 규제 환경에 대한 마법사 방식의 템플릿을 사용하여 사용자가 신속하게 사용자 지정 보안 정책을 만들어 감사 요구 사항을 충족할 수 있도록 안내합니다. McAfee Database Activity Monitoring은 각 데이터베이스 서버에서 실행되는 자체 센서에 보안 정책을 구현할 책임을 배포함으로써 대기업 지원을 위해 비용 효율적으로 확장됩니다.

가상화 및 클라우드를 비롯한 오늘날의 최신 IT 인프라 지원

데이터베이스 모니터링을 위한 다른 시스템은 데이터 센터 가상화 및 클라우드 컴퓨팅에 사용되는 고도의 동적 분산 아키텍처에서는 사용할 수 없거나 비효율적인 네트워크 트래픽 분석에 의존하여 정책 위반을 식별합니다.하지만 McAfee 센서는 각각의 새 데이터베이스를 자동으로 제공하고 호스팅하는 데이터를 기반으로 한 보안 정책을 요청하며 관리 서버에 경고 전송을 시작하도록 구성될 수 있습니다. 네트워크 연결이 중단되더라도 센서가 보안 정책을 로컬로 구현하므로 데이터는 여전히 보호되며, 관리 서버가 다시 연결되면 전달되도록 경고는 대기 상태에 있게 됩니다.

McAfee ePolicy Orchestrator 플랫폼과의 통합

McAfee Database Activity Monitoring는 McAfee ePolicy Orchestrator 소프트웨어와 완벽하게 통합되어 있어 통합된 대시보드의 모든 데이터베이스에 대한 중앙 집중식 보고 및 요약 정보를 제공합니다. McAfee ePO 소프트웨어는 데이터베이스 보호 이외의 추가적인 McAfee 보안 솔루션과 연결되어 간편한 관리 및 완벽한 가시성을 지원하는 단일 뷰를 제공합니다.

McAfee 데이터베이스 보안 솔루션

McAfee는 전반적인 데이터베이스 환경 및 보안 상황에 대해 완벽한 가시성을 갖출 수 있도록 지원하는 여러 가지 데이터베이스 보안 솔루션을 제공합니다.자세한 내용은 www.mcafee.com/kr/products/database-security/index.aspx를 방문하거나 해당 지역의 McAfee 담당자 또는 가까운 리셀러에게 문의하십시오.

McAfee 엔드포인트 보안 정보

McAfee 엔드포인트 보안은 모든 장치, 해당 장치를 통해 전달되는 데이터 및 해당 장치에서 실행되는 응용프로그램 전체를 보호합니다. McAfee의 포괄적인 맞춤형 솔루션을 통해 복잡성을 줄여 생산성에 영향을 미치지 않는 다단계 엔드포인트 방어 시스템을 구축할 수 있습니다.자세한 내용은 www.mcafee.com/kr/products/endpoint-protection/index.aspx를 참조하십시오.

McAfee
An Intel Company

한국맥아피(주)
서울특별시 강남구 역삼동 737
강남파이낸스센터 5층 135-984
+82.2.3458.9800
www.mcafee.com/kr

[1] *Verizon Business 연구*, 2013.