전문 데이터베이스 보안 솔루션을 배포해야 하는 가장 큰 5가지 이유

철통 같은 마지막 방어선 구축

데이터베이스 내에 저장된 소중한 기밀 정보를 보호하는 일은 규정 컴플라이언스는 말할 것도 없고 전세계 어디서나 조직의 무결성과 명성을 유지하는 데 중요합니다. 그럼에도 불구하고 근본적으로 제한된 보안 솔루션에 의존하는 기업이 아직도 많습니다. 오늘날 데이터베이스 플랫폼의 복잡성과 정교해진 사이버 범죄를 감안하면 종합적인 전문 데이터베이스 보안 솔루션의 배포가 절실합니다. 여기 그 이유 5가지를 소개합니다.

McAfee Vulnerability Manager 이점

- 데이터베이스 보안 상태에 대한 완전한 가시성 제공
- 중앙 집중식 콘솔에서 기업 전체에 걸친 여러 데이터베이스 검색
- 준수 시간 가속화 및 감사 주기 최소화로 상당한 비용 절약
- 최소한의 데이터베이스 시스템 지식으로 배포 시간 단축
- 다양한 사용자 역할에 대해 사용자 지정된 보고서를 이해하기 쉬운 형식으로 신속히 생성

McAfee Database Activity Monitoring 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 달성

1. 자산이 있다는 것을 알아야 자산을 보호할 수 있다

평범한 기업의 IT 환경이라고 해도 매우 민감한 정보를 담고 있는 데이터베이스 인스턴스의 수가 수백 또는 수천 개에 달한다는 것은 결코 놀랄 일이 아닙니다. 하지만 IT 부서는 이런 데이터베이스의 정확한 개수, 위치, 데이터 민감도 및 보안 상태를 파악하는라 진땀을 흘리고 있습니다. 설상가상으로 사이버 범죄자도 이 점을 알고 항상 손길이 미치지 못하는 사각지대를 찾느라 이곳저곳을 누비고 다닙니다. 이들은 항상 충분한 시간과 기술적 자원을 갖고 안전하다고 생각했거나 존재조차 몰랐던 데이터베이스를 공격합니다. 결국 사용자의 가시성 부족은 사이버 범죄자에게 기회를 의미합니다.

데이터베이스 환경에 대한 완전한 가시성은 항상 환경 내에 존재하는 기존의 모든 데이터베이스를 빠짐없이 탐색할 수 있는 능력과 지불 카드 번호, 인적 자원 데이터, 매출액 등 민감한 데이터가 어디에 저장되어 있는지 파악할 수 있는 검색 능력에서 비롯됩니다. 이 외에 심층적인 데이터베이스 취약성 테스트의 자동화 역시 정확한 위험 수준을 파악하는 데 중요한 역할을 합니다. 이처럼 상세하고 실행 가능한 정보를 제공하여 보안 허점의 우선순위를 결정하고 그 허점을 개선할 뿐만 아니라 외부 보안 컨설턴트에게 들어가는 막대한 기업 비용을 절감할 수 있는 방법은 오직 전문 데이터베이스 보안 솔루션밖에 없습니다.

McAfee® Vulnerability Manager for Databases는 네트워크의 모든 데이터베이스를 자동으로 탐색하여 최신 패치의 적용 여부를 결정하고 취약성을 검색합니다. 실제로 McAfee Vulnerability Manager는 최고의 데이터베이스 시스템에 대해 4,200가지가 넘는 취약성 검사를 실시하여 그 위협 수준을 우선순위별로 분류하고 픽스 스크립트(fix script)와 권장사항도 함께 제공합니다. 또한 요구되는 데이터베이스 시스템에 대한 지식도 최소일 뿐만 아니라 다양한 사용자 직무를 고려하여 알아보기 쉬운 형식으로 사용자 지정 보고서도 작성할 수 있습니다. 이 모든 것이 중앙 집중식 보안 콘솔을 통해 실현됩니다.

2. 경계 보안은 내부 위협에 허술하다

대부분 기업은 방화벽과 기타 네트워크 보안 기술을 배포하는 데 엄청난 시간, 노력 및 자금을 쏟아부었습니다. 하지만 알고 계시듯이 데이터베이스 유출이 항상 경계 밖에서만 이루어지는 것은 아닙니다. 사실, 유출 건수의 절반 정도가 내부 사용자를 통해서 발생한다는 CERT(Computer Emergency Response Team)의 연례 연구 자료도 있습니다. 따라서 비즈니스에 중요한 데이터 보안은 내부의 적도 무시하지 못합니다. 액세스 권한 사용자 대부분은 기본적인 DBMS(Database Management System)의 보안 기능을 피해 액세스 로그를 조작함으로써 자신을 추적하지 못하게 할 수 있는 수단을 갖고 있습니다.

올바른 데이터베이스 보안 솔루션이 되려면 경계 안이든 밖이든 모든 가능한 위협을 탐지하여 사전에 방지할 수 있어야 합니다. 또한 특정 컴플라이언스 요건에 따라 데이터베이스 액세스 정책을 쉽게 설정하고 강화함으로써 진정한 의미의 역할 분담을 할 수 있는 프레임워크가 필요합니다.

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 자산을 더 잘 보호합니다. McAfee Database Activity Monitoring을 통해 데이터베이스 내의 권한이 있는 로컬 액세스와 정교한 공격을 비롯한 모든 데이터베이스 활동에 대해 가시성을 확보할 수 있습니다. 또한 위치에 상관 없이 각 데이터베이스의 서버 활동을 로컬에서 모니터링하고, 보안 정책을 위반했다는 의심이 들거나 위반한 경우 경보를 보내거나 또는 자동으로 세션을 종료함으로써 모든 데이터 위협을 사전에 차단합니다. McAfee Database Activity Monitoring은 가상화 또는 클라우드 컴퓨팅 환경에서도 데이터베이스의 보안과 정책을 강화합니다.

McAfee Virtual Patching 이점

- 공급업체에서 릴리스한 패치 업데이트를 설치하기 전에 위협으로부터 보호
- IT 및 보안 팀의 DBMS에 관한 지식 필요성 해소
- 침입이 불가능한 소프트웨어 설계로 프로덕션 데이터베이스의 온라인 유지
- 지속적인 업데이트의 자동 배포로 원활한 데이터베이스 보호
- PCI DSS, HIPAA 등과 같은 표준에 대한 컴플라이언스 용이성

3. 패치 속도보다 공격 속도가 빠르다

화요일 패치(Patch Tuesday)는 해커의 활동이 없는 날이 되어야 합니다. 그 이유는 데이터베이스 공급업체가 공격하기 좋은 절호의 대상을 공개하는 날이나 다름 없기 때문입니다. 뿐만 아니라 화요일 패치는 해커가 기회를 호시탐탐 노리는 날이기도 합니다. 이들도 데이터베이스 관리 팀이 데이터베이스 가동을 멈추고 패치를 단행한 다음 테스트를 거치는 일이 얼마나 힘든지 알고 있기 때문입니다. 실제로 해커는 패칭 프로세스로 인해 데이터베이스의 운영이 중단되었을 때를 노리는데, 이때 기업이 그 지연 시간을 최대한 늘려서 해커가 침입하는 데 충분한 시간을 벌 수 있기 때문입니다.

기존의 패칭 프로세스는 사이버 범죄자에게 기회만 제공할 뿐 실제 해결책이 없기 때문에 전문 데이터베이스 보안 솔루션이 절실합니다. 이 솔루션은 데이터베이스의 보안 상태를 실시간으로 업데이트해주므로 IT 담당자의 수고를 덜어줄 뿐만 아니라 비즈니스 운영이 중단될 염려도 없습니다.

McAfee Virtual Patching for Databases는 데이터베이스 다운타임이나 응용프로그램 테스트 없이도 실시간으로 공격 시도 및 침입을 탐지하고 막음으로써 패치가 적용되지 않은 취약성으로 인한 위험으로부터 데이터베이스를 보호합니다. 또한 공급업체의 패치 업데이트 제공부터 실제 설치까지 취약성이 최대인 시간에도 위협에 대한 보호를 받고 있다는 것을 알고 있기 때문에 안심할 수 있습니다.

McAfee ePolicy Orchestrator 소프트웨어 이점

- 중앙 집중식 관리 콘솔을 통한 데이터베이스 보안 및 컴플라이언스의 종합적 가시성 제공
- 단일 창구의 이점으로 데이터베이스를 통합 보안 관리 프로그램, 온-프레미스, 원격 위치 및 심지어 클라우드까지 쉽게 배포
- 확장형 오픈 아키텍처를 통한 McAfee 및 타사의 보안 솔루션 관리와 LDAP(Lightweight Directory Access Protocol), IT 운영 및 구성 관리 도구의 연동

McAfee Database Activity Monitoring은 침입을 방지하고 다운타임을 완전히 제거할 수 있는 또 하나의 솔루션으로 화요일 패치 및 그 이상에 대해 보안 계층을 추가했습니다. 이 솔루션의 메모리 기반 센서는 네트워크, 서버 자체에 로그인한 로컬 사용자, 저장된 프로시저 또는 트리거를 통한 데이터베이스 내부를 통한 데이터베이스 공격을 사전에 차단합니다.

4. 연속성을 위해 컴플라이언스를 포기하지 말라

보건, 금융 및 소매업과 같은 산업에 적용되는 규정 컴플라이언스 요건은 끊임없이 진화하여 점차 엄격해지고 있습니다. 공급업체가 제공하는 최신 DBMS 패치에 따라 데이터베이스를 업데이트해야 하는 컴플라이언스 절차가 비즈니스에 중요한 데이터베이스에 상당항 영향을 끼치는 것도 별로 놀랄 일은 아닙니다. 그렇기 때문에 각종 데이터베이스의 가동을 멈추고 패치한 다음 테스트까지 하는 부담을 생각하면 비즈니스 연속성을 지속한 채 컴플라이언스를 희생하는 기업이 대다수인 것도 이해가 됩니다. 또한 단 한 번의 패치 업데이트도 없이 계속 사용 중인 기존 데이터베이스들도 있을 것입니다.

McAfee Virtual Patching for Databases는 규정 컴플라이언스를 희생하지 않고도 비즈니스 연속성을 유지합니다. 데이터베이스 보안 및 컴플라이언스가 그대로 유지되기 때문에 자체 일정에 따라 예전처럼 패치를 진행할 수 있습니다. 컴플라이언스 감사관들은 McAfee Virtual Patching for Databases의 엄청난 시간 절감 효과와 유익한 제어 기능에 놀라게 될 것입니다. 이 밖에 DBMS 공급업체도 더 이상 지원하지 않는 기존 데이터베이스까지 최신 보호 기능을 확장할 수 있습니다.

5. 클라우드에 존재하는 데이터는 가시성이 극히 제한된다

클라우드는 엄청난 IT 비용 절감 효과와 운영 이점이 있지만, 아시다시피 문제점도 있습니다. 바로 IT 담당자가 민감한 데이터를 직접 제어하지 못하기 때문에 누가 액세스하는지 거의 감시할 수 없습니다. 하지만 올바른 데이터베이스 보안 솔루션만 갖추고 있다면 물리 및 가상 환경 모두에서 데이터를 안전하게 지켜낼 수 있습니다. 올바른 솔루션은 데이터베이스가 가상화되어 클라우드에서 사용될 때도 허용되지 않은 데이터베이스 활동을 방지하고 이런 활동이 있을 경우 자체 관리 콘솔에 보고할 수 있어야 합니다.

McAfee Database Activity Monitoring은 메모리 기반의 센서가 독자적으로 구현되어 있어서 새로운 가상 시스템과 함께 자동으로 프로비저닝되도록 구성할 수 있습니다. 또한 호스팅하는 데이터를 기준으로 보안 정책을 요청한 다음 관리 서버에 경보를 보낼 수 있습니다. 뿐만 아니라 센서가 서버에서 분리되더라도 자동으로 기능하기 때문에 데이터베이스가 온라인이거나 오프라인일 때도 또는 언제 어디에 상주하더라도 민감한 데이터를 보호하고 지킬 수 있습니다. 네트워크 연결이 중단되더라도 센서가 보안 정책을 로컬로 구현하므로 데이터는 여전히 보호되며, 관리 서버가 다시 연결되면 전달되도록 경고는 대기 상태에 있게 됩니다.

또한 McAfee® ePolicy Orchestrator®(McAfee ePO™) 소프트웨어를 통해 클라우드 기반 데이터베이스의 액세스 활동을 모니터링할 수 있습니다. 이 소프트웨어는 기업 보안 관리 콘솔을 통해 데이터베이스 보안, 기업 보안 및 컴플라이언스에 대한 종합적인 가시성을 제공합니다.

즉, 클라우드 여부에 관계없이 누구나 최고 수준의 가시성을 보유하게 되는 것입니다. 분명한 것은 McAfee는 운영 영역이 얼마나 넓든지 또는 데이터가 얼마나 민감하든지 관계없이 IT 환경을 위한 올바른 데이터베이스 보안 솔루션을 지원합니다.

McAfee 데이터베이스 보안 이점

- 배포 및 사용이 용이
- 데이터베이스 보안 상태에 대한 완전한 가시성 제공
- 보안 및 데이터베이스 관리 직원의 보안 정책 관리 업무 간소화
- 규정 컴플라이언스의 효율적 관리
- 손상을 입히기 전에 공격을 저지하여 위험 및 책임 최소화
- 중앙 집중식 콘솔을 이용한 데이터베이스 보안 관리

데이터베이스의 안전 및 가용성을 위한 정보

데이터베이스는 중요한 비즈니스 자산을 안전하게 저장할 수 있어야 한다는 사실을 McAfee는 잘 알고 있습니다. 또한 1년 365일 비즈니스 성과를 유지할 수 있는 가용성 역시 매우 중요합니다. 데이터베이스에게 단 하루의 휴일도 없듯이, McAfee 역시 고객 비즈니스를 위해 쉬지 않고 노력하고 있습니다. "안전은 멈추지 않는다(Safe never sleeps)"라는 말도 바로 여기서 비롯됩니다. 안심하십시오. McAfee의 데이터베이스 보안 전문 팀이 민감한 개인 정보의 안전과 가용성에 초점을 맞추고 물샐틈없는 보안을 강화하고 있을 뿐만 아니라 사내 정책과 산업 규정에 대한 기업의 컴플라이언스를 지원하고 있습니다.

McAfee 데이터베이스 보안을 통해 비즈니스에 중요한 데이터베이스를 어떻게 보호할 수 있는지 자세히 알고 싶으신 분은 http://www.mcafee.com/kr/products/database-security/index.aspx를 방문하거나 지역의 McAfee 담당자 또는 판매업체에 문의하십시오.

트위터 팔로우 계정: @McAfee_DBSecure.

McAfee 엔드포인트 보안 정보

Intel Corporation(NASDAQ:INTC)이 전체 지분을 소유한 자회사인 McAfee는 세계 최대의 전문 보안 회사입니다. McAfee의 차세대 엔드포인트 보안 솔루션은 모든 장치, 해당 장치를 통해 전달되는 데이터 및 해당 장치에서 실행되는 응용프로그램 전체를 보호합니다. 이 포괄적인 맞춤형 솔루션을 통해 복잡성을 줄여 생산성에 영향을 미치지 않는 다단계 엔드포인트 방어 시스템을 구축할 수 있습니다. 이 방어 시스템은 전통적인 악성 프로그램 스마트 검색, 동적 화이트리스팅, 동작 제로 데이 침입 방지, 통합 관리 및 통합 위협 인텔리전스가 완벽하게 혼합된 솔루션입니다. 자세한 내용은 www.mcafee.com/kr/products/endpoint-protection/index.aspx에서 확인할 수 있습니다.

한국맥아피(주)
서울특별시 강남구 역삼동 737
강남파이낸스센터 16층 135-984
+82.2.3458.9800
www.mcafee.com/kr

41903brf_top5-db-sec_0212_fnl_ASD