McAfee Vulnerability Manager

실시간 고성능 연속 자산 모니터링

주요 차별 요소

- 탁월한 확장성, 정확성 및 유연성
- 네트워크에 나타나는 새로운 장치를 실시간으로 평가, 전체 소프트웨어 및 하드웨어 자산 인벤토리, 사용자 자산 매핑, 자동 네트워크 토폴로지
- 활성 및 비활성 네트워크 검색과 모니터링을 결합하여 가상화된 모바일의 숨겨진 장치 표시
- 심층적인 장치 감사로 검색하고 신뢰할 수 있는 자산 데이터베이스 제공
- 동적 시스템 태그 지정으로 취약성 평가의 완전한 자동화
- McAfee Global Threat Intelligence™를 통해 최신 취약성 및 위협 정보 업데이트
- Cyber-Ark 통합으로 자격 증명 기반 보안 향상
- IPv4 및 IPv6 네트워크를 모두 검색
- 완벽하게 유연한 보고 - 자산을 한 번 검색하고 언제든지 보고 가능
- McAfee 내부 및 타사 응용프로그램을 포함하는 자동 위험 관리 워크플로

포괄적인 취약성 관리를 실시간으로 간편하게 수행하는, 업계에서 가장 유연하고 확장 가능한 인증된 솔루션으로 비즈니스를 보호하십시오. McAfee Asset Manager 기능을 포함한 McAfee® Vulnerability Manager는 최고의 확장성과 성능을 제공하며 네트워크의 모든 것을 능동/수동적으로 조사합니다. 장치 또는 자산이 IP 주소를 가지고 있거나 네트워크를 사용하고 있으면 McAfee Vulnerability Manager가 이를 자동으로 검색 및 평가하여 네트워크에 있는 모든 자산의 컴플라이언스 상태를 나타냅니다.

McAfee Vulnerablity Manager 솔루션은 비즈니스를 정의하는 현실을 기반으로 모든 유형의 네트워크 및 자산 구성을 조사하여 시장 표준을 설정합니다. 중단 없이 수동적으로 검색할 수도 있고 필요한 시간과 장소에서만 능동적으로 검색할 수도 있으므로 모든 자산에 대해 검색, 평가, 교정 및 보고가 가능합니다. 예약된 검색 사이에서 누락될 수 있는 스마트폰, 태블릿, 랩톱은 물론 네트워크의 숨겨진 장치도 찾을 수 있습니다. 사용자를 놀라게 하거나 컴플라이언스 문제를 일으킬 수 있는 사항이 발견될 수도 있습니다. 수백 개의 노드가 있는 배포에서부터 4백만 개의 IP를 지속적으로 검색하는 배포에 이르기까지 수천 개의 조직이 취약성을 신속하게 찾고 우선 순위를 지정하는 데 McAfee Vulnerability Manager를 사용합니다.

간편한 구현

McAfee 솔루션을 사용하면 신뢰할 수 있는 검색 기능을 간편하게 구현할 수 있습니다. McAfee Vulnerability Manager는 실제 또는 가상 하드웨어에 손쉽게 설치할 수 있으며, McAfee 의 강화된 어플라이언스를 사용할 수도 있습니다. 불과 몇 분 만에 최초 검색을 시작할 수 있습니다.

자산 인벤토리를 로드 및 유지 관리하는 일도 간단합니다. McAfee Asset Manager 모듈을 사용하면 새로운 장치로 온라인 연결 시 자산 데이터베이스가 즉시 업데이트되므로 장치 현황을 실시간으로 알 수 있습니다. 또한 McAfee Vulnerability Manager는 LDAP, Microsoft Active Directory 및 McAfee® ePolicy Orchestrator®(McAfee ePO™) 관리 플랫폼 등의 엔터프라이즈 자산 관리 도구와 직접 통합되므로 자산 데이터의 단일 중앙 리포지토리를 유지 관리할 수 있습니다.

모든 자산에 대한 가시성 확보

McAfee Asset Manager 옵션은 상시 가동하는 수동 검색 및 모니터링을 통해 가시성을 높입니다. SPAN 포트에 빠르게 배포할 수 있는 이 시스템은 트래픽을 모니터링하여 위험한 장치와 잊고 있었던 VMware 호스트 및 모바일 장치를 포함한 네트워크의 모든 것을 매핑합니다. 감시하는 동안 위험 측정 및 완화를 돕는 장치, 패턴 및 통신 등의 세부 정보를 열거합니다. 장치 세부 정보는 즉각적인 평가를 위해 McAfee Vulnerability Manager로 자동 전송됩니다. 또한 McAfee Asset Manager는 발견되는 각 장치에 대해 완전한 소프트웨어 및 하드웨어 인벤토리를 수행할 수 있습니다.

요구 사항에 맞도록 검색을 사용자 지정

McAfee Vulnerability Manager는 산업 규정 컴플라이언스를 벤치마크하고 문서화하는 데 도움이 되는 몇 가지 옵션을 제공합니다. 정책을 빠르게 정의하려면 골드 스탠다드(Gold Standard) 시스템을 검색하여 기준을 정하고, 제공된 컴플라이언스 템플릿을 사용하거나, SCAP(Security Content Automation Protocol)를 활용하는 정책을 로드하십시오.

McAfee Vulnerability Manager는 모든 네트워크 자산을 검색할 수 있고 심지어 에어 갭(air-gapped) 환경 및 중요한 인프라 환경에 있는 까다로운 자산도 검색할 수 있습니다. 예를 들어 외부 연결이 없는 네트워크의 경우 랩톱 기반 또는 가상 스캐너를 배포하여 이러한 자산을 검색할 수 있습니다. 그런 다음 제한된 환경에 검색 결과를 보존하거나 필요한 경우 중앙 집중식 시스템으로 보낼 수도 있습니다.

대부분의 운영 체제에서는 중요한 구성 정보를 공개하기 전에 자산 자격 증명을 요구하지만 일부 보안 팀에게 이러한 자격 증명에 대한 액세스 확보는 매우 까다롭습니다. Cyber-Ark Privileged

스캔 적용 범위

- Microsoft Windows, UNIX, Cisco, Android, Linux, Apple Macintosh, Apple iOS 및 VMware 플랫폼을 포함한 450 가지 이상의 운영 체제 검색
- 웹 응용프로그램에 대한 심층적인 검색(OWASP 상위 10개 및 CWE 상위 25개)
- Adobe, AOL, Apple, Microsoft(Office, IIS, Exchange), Blue Coat, CA, Cisco, Citrix, Facebook, Google, HP, IBM(Lotus Notes 및 WebSphere), Novell, Oracle, Real Networks, RIM(BlackBerry Enterprise Server), SAP, Oracle Java, Symantec 및 VMware 소프트웨어의 취약성 및 악성 프로그램 검색
- DB2, MySQL, Oracle, Microsoft SQL Server 및 Sybase 등의 주요 데이터베이스 검색

표준 및 인증

- ASCI 33, BASEL II, BILL 198(CSOX), BSI IT(GR), COBIT, FDCC, FISMA, GLBA, HIPAA, ISO 27002, JSOX, MITS, PCI, SOX, NIST SP 800-68, SANS Top 20, SCAP, OVAL 등을 위한 템플릿 포함
- CIS 인증 감사, COBIT, CPE, CVE, CVSS, DISA STIG, FDCC/SCAP, ISO17799/ISO 27002/FINRA, ITIL, NIST-SP800, NSA, OVAL 및 SANS Top 20을 비롯한 표준 지원
- 인증된 일반 기준
- 검증된 FIPS-140-2 암호화

기술 사양

현재 하드웨어 및 소프트웨어 사양과 요구 사항을 확인하려면 www.mcafee.com/kr을 방문하십시오.

Identity Management 제품와의 통합으로 높은 수준의 보안을 갖춘 자격 증명 기반 검색을 쉽고 안전하게 우수한 성능으로 수행할 수 있습니다.

몇 분 만에 위험을 판단

McAfee Asset Manager가 네트워크에서 새로운 시스템을 파악하면 시스템에 대한 상세한 정보를 McAfee Vulnerability Manager로 전달하여 목표 검색을 트리거합니다. 곧 시스템 상태와 네트워크 환경에 대한 위험을 알 수 있게 됩니다.

효율성을 위한 자산 태그 지정

또한 태그 지정 정책을 사용하여 검색 그룹의 새로운 장치를 각 장치의 프로필과 위험에 따라 자동으로 배치할 수 있습니다. 정의한 정책에 따라 올바른 검색은 즉시 검색이 될 수도 있고 다음 주기 검색의 일부가 될 수도 있습니다.

취약성과 악성 프로그램 모두 탐지

타사 제품은 개방된 포트와 구성을 피상적으로만 다루지만 McAfee Vulnerability Manager는 훨씬 더 깊이 들어갑니다. McAfee Vulnerability Manager는 시스템 및 응용프로그램 수준의 평가를 수행하며 여기에는 데이터베이스 배너, 정책 설정, 레지스트리 키, 파일 및 드라이브 권한, 실행 서비스 등이 포함됩니다. 취약성을 가장 광범위하게 탐지하기 위해 450개가 넘는 운영 체제를 테스트합니다. 검사를 통해 트로이 목마, 바이러스, 기타 악성 프로그램 등의 악성 콘텐츠도 탐지됩니다.

독점 및 레거시 프로그램을 테스트하기 위해 사용자 지정 스크립트 및 검사를 작성하여 제로 데이 위협에 대비한 미리 정의된 검사 및 업데이트를 보강할 수 있습니다. McAfee Vulnerability Manager는 XCCDF, OVAL 및 기타 SCAP 표준을 따르는 타사 콘텐츠도 평가합니다.

웹 응용프로그램에 특히 주의

McAfee Vulnerability Manager는 관리자가 전통적인 네트워크 기반 자산을 관리하듯이 웹 응용프로그램도 관리할 수 있게 합니다. 웹 응용프로그램 자산은 그룹으로 묶여 각자의 중요도, 자산 소유자 및 특성을 가질 수 있습니다. McAfee Vulnerability Manager는 완전 자동화 기능을 통해 다양한 웹 취약성 범위에서 풍부한 웹 응용프로그램 검색을 수행합니다.

최신 정보 유지

수백 명의 McAfee Labs™ 연구원은 전 세계 수백만 개의 센서를 통해 위협 환경의 최신 변경 사항을 파악합니다. McAfee Global Threat Intelligence는 실시간 위험 평가 및 위협 권고 사항을 McAfee Vulnerability Manager로 직접 제공함으로써 새로운 위협으로부터 사용자를 미리 보호합니다.

필요에 따라 관리, 확장 및 통합

McAfee는 각자 선호하는 방식대로 검색, 보고 및 관리를 구성할 수 있는 유연성을 제공합니다. 단일 콘솔에서 스캐너의 로컬 자산만 모니터링하거나 수백 개에 달하는 원격 검색 엔진의 진행 상태를 볼 수도 있습니다. 모든 규모의 조직 요구에 맞게 다중 계층 아키텍처를 조정할 수 있습니다.

McAfee Vulnerability Manager는 API(application programming interface)를 통해 대부분의 응용프로그램과 통합할 수 있습니다.

위험을 기준으로 대응

취약성에 대한 하나의 실행 가능한 보기를 통해 패칭 및 감사 비용을 낮춥니다. 예를 들면 Patch Tuesdays를 통해 새로운 Microsoft Windows 또는 Adobe 취약성에 의해 어떤 시스템이 영향을 받을지 신속하게 파악할 수 있습니다. 전체 네트워크를 다시 검색하지 않고도 McAfee Vulnerability Manager는 기존 구성 데이터와 위험 점수를 기반으로 몇 분 만에 새 위협의 위험 잠재성 우선 순위를 지정하고 등급을 매길 수 있습니다.

이러한 정보를 통해 중요도를 기반으로 자산을 선택하고 마우스 오른쪽 단추를 클릭하여 대상을 즉시 검색할 수 있습니다.

확실한 컴플라이언스

예상 및 실제 검색 결과, 검색되지 않은 시스템, 실패한 검색 같은 확실한 결과를 통해 특정 시스템이 "취약하지 않다거나" 일반 감사가 더 필요하다는 점을 알 수 있습니다. McAfee Vulnerability Manager는 능동 및 수동 모니터링, 침투 테스트, 인증 검색, 비자격 증명 검색의 조합을 통해 최고 수준의 정확성으로 취약성과 정책 위반 사항을 찾아낼 수 있습니다. 그 어느 때보다 간편하게 포괄적인 취약성 관리를 수행할 수 있습니다.

McAfee
An Intel Company

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

53000ds_mvm-mam_1012_fnl_ETMG