McAfee Application Data Monitor

응용프로그램 계층 검사로 숨은 위협 탐지.

McAfee® Application Data Monitor 어플라이언스는 응용프로그램 계층까지 모니터링함으로써 로그 관리의 한계를 넘어선 보안 및 컴플라이언스를 제공합니다. 응용프로그램 콘텐츠를 완벽하게 검사하여 네트워크 사용에 대한 최고 수준의 가시성을 실현할 수 있습니다.

McAfee Application Data Monitor 어플라이언스는 계층 7까지 전체 응용프로그램 세션을 디코딩하여 기본 프로토콜 및 세션 무결성에서 응용프로그램 콘텐츠 자체(전자 메일 텍스트 또는 첨부 파일 등)에 이르는 모든 것에 대한 분석을 제공합니다. 이러한 수준의 상세함은 실제 응용프로그램 사용의 정확한 분석을 가능하게 하며 응용프로그램 사용 정책을 적용하고 악성, 비밀 트래픽을 감지할 수 있게 합니다.

네트워크의 모든 중요 데이터 사용을 추적함으로써 컴플라이언스를 지원하는 심층적인 검사 기능입니다. McAfee Application Data Monitor 어플라이언스가 위반 사항을 감지하면 사고 대응과 포렌식에서의 활용 또는 컴플라이언스 감사 요구 사항을 위해 해당 응용프로그램 세션의 모든 세부 정보를 보존합니다.

동시에 McAfee Application Data Monitor 어플라이언스는 정상적인 응용프로그램으로 위장할 수 있는 위협에 대한 가시성을 제공합니다.

- 고급 응용프로그램 계층 위협
- 기밀 데이터의 무단 사용 또는 도난
- 보안 "맹점"에 대한 공격
- 위험한 레거시 코드의 사용
- 사용자 자격 증명 도난 또는 오용
- 모든 응용프로그램을 통한 중요 데이터 전송
- 중단된 비즈니스 프로세스

데이터 손실 및 컴플라이언스 위반

McAfee Application Data Monitor 어플라이언스는 전자 메일 첨부 파일, 메신저, 파일 전송, HTTP 게시물 또는 기타 응용프로그램 내부에서 중요 정보가 전송되면 이를 즉시 사용자에게 알려 손실을 완화합니다.

주요 이점

- 전체 응용프로그램 세션을 수백 개의 응용프로그램에 대한 계층 7까지 완벽하게 디코드
- 규제된 데이터 및 중요 데이터에 대해 사전 수립된 탐지 규칙 포함
- 사용자 정의 가능 사전 및 사용자 정의 규칙 지원
- 컴플라이언스에 대한 완벽한 응용프로그램 이벤트 감사 추적 생성
- 응용프로그램 간섭 방지를 위해 수동으로 작동
- McAfee Enterprise Security Manager와 통합되어 응용프로그램 콘텐츠와 이벤트 및 기타 데이터 피드의 상관관계 분석 가능
- 유연한 혼합 배달 옵션에는 물적 및 가상 어플라이언스가 포함됩니다.

즉시 신용 카드 정보와 주민 등록 번호와 같은 중요 정보를 감지할 수 있고 중요한 기밀 정보의 자체 사전을 정의함으로써 McAfee Application Data Monitor 어플라이언스의 탐지 기능을 사용자 정의할 수도 있습니다. McAfee Application Data Monitor 어플라이언스는 이러한 중요한 데이터 유형을 감지하고 적절한 관계자에게 알리며 위반 내용을 기록하여 감사 추적을 유지합니다.

문서 검색

McAfee Application Data Monitor 어플라이언스는 전자 메일, 채팅, P2P, 파일 공유 등의 방법으로 교환되는 500종 이상의 문서를 검색할 수 있습니다. McAfee Application Data Monitor 어플라이언스는 확장자에 관계없이 메일 게이트웨이와 침입 탐지 시스템 (IDS)/침입 방지 시스템 (IPS) 장치를 통과하기 위해 다른 유형으로 위장한 문서를 검색할 수 있습니다. 다른 문서에 포함된 문서, 보관, 압축 및 인코딩된 문서까지도 파일 이름이나 수행 작업과 같은 실행 가능한 메트릭을 통해 검색 가능합니다.

응용프로그램 계층 위협

새롭고 교묘한 위협은 일반적인 비즈니스 응용프로그램의 취약성을 이용하여 네트워크에 침입하여 중요한 데이터를 빼냅니다. 이러한 응용프로그램 계층 위협은 기존의 방화벽, IDS 및 IPS로는 탐지가 어렵지만 McAfee Application Data Monitor 어플라이언스는 기본 프로토콜을 포함하여 전체 응용프로그램 콘텐츠를 검색할 수 있으므로 숨겨진 페이로드, 악성 프로그램, 비밀 통신 채널(예: PDF 문서에 포함된 실행 가능한 파일)까지 감지할 수 있습니다.

프로토콜 이상

이상 탐지는 긴급한 위협을 미리 파악하여 위험을 줄이고 손실을 최소화할 수 있습니다. 기존의 일부 보안 솔루션은 네트워크 흐름 분석으로 제한되어 있지만 McAfee Application Data Monitor 어플라이언스는 이러한 접근 방식을 한 단계 발전시킵니다. 과거의 네트워크 동작을 살펴 응용프로그램 및 프로토콜 내 이상을 감지함으로써 보다 강력하고 사전 대응적인 위험 탐지 방법을 제공합니다.

응용프로그램 간섭 없음

McAfee Application Data Monitor 어플라이언스는 SPAN 포트에서 작동하므로 응용프로그램 성능 또는 신뢰성을 간섭하거나 지연되지 않습니다.

인프라와 통합

대부분의 네트워크 모니터링 솔루션은 단독으로 작동하지만 McAfee Application Data Monitor 어플라이언스는 다른 정보 보안 시스템과 조화롭게 작동합니다. 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 손실 및 사기 탐지를 통합할 수 있습니다.

사용 사례 예시

McAfee Application Data Monitor 어플라이언스는 다양한 무단 활동, 정책 위반, 도난 및 사기를 탐지할 수 있습니다. 예를 들면 다음과 같습니다.

500개 이상의 지원 응용프로그램과 프로토콜

- **낮은 수준의 네트워크 프로토콜:** TCP/IP, UDP, RTP, RPC, SOCKS, DNS 및 기타
- **이메일:** MAPI, NNTP, POP3, SMTP, Microsoft Exchange
- **웹메일:** AOL 웹 메일, Hotmail, Yahoo! Mail, Gmail, Facebook 및 MySpace 전자 메일
- **인스턴스 메시징:** AOL, ICQ, Jabber, MSN, SIP 및 Yahoo
- **파일 전송 프로토콜:** FTP, HTTP, SMB 및 SSL
- **압축 및 추출 프로토콜:** BASE64, GZIP, MIME, TAR, ZIP 및 기타
- **아카이브 파일:** RAR 보관, ZIP, BZIP, GZIP, BinHex 및 UU 인코딩 보관
- **설치 패키지:** Linux 패키지, InstallShield 캐비닛, Microsoft 캐비닛
- **이미지 파일:** GIF, JPEG, PNG, TIFF, AutoCAD, Photoshop, Bitmap, Visio, Digital RAW 및 Windows 아이콘
- **오디오 파일:** WAV, MIDI, RealAudio, Dolby Digital AC-3, MP3, MP4, MOD, Supprime, SHOUTCast 등
- **비디오 파일:** AVI, Flash, QuickTime, Real Media, MPEG-4 , Vivo, Digital Video (DV), Motion JPEG 등
- **기타 응용프로그램 및 파일:** 데이터베이스, 스프레드시트, 팩스, 웹 응용프로그램, 폰트, 실행 가능한 파일, Microsoft Office 응용프로그램, 게임 및 소프트웨어 개발 도구
- **기타 프로토콜:** 네트워크 프린터, 셸 액세스, VoIP 및 P2P더

기밀 정보 도난

업무용 이메일인 gildongHong@company.com으로 로그인한 직원이 정보 도난을 공모한 gongmoja@gmail.com으로 전자 메일을 보냈습니다. 이 전자 메일에는 “비밀 공식”이라는 단어를 포함한 shoo.doc라는 파일이 들어 있었습니다. 이 전자 메일은 호스트 데스크톱 0232 (192.168. 0.36)에서 SMTP 서버(10.0. 2.13)를 통해 “받음”이라는 제목으로 오후 12시 20분에 전송되었습니다.

무단 응용프로그램 사용

한 직원이 P2P 파일 공유 응용프로그램을 사용하여 음원을 전송하여 정책을 위반했습니다. 그는 업무 시간 중 대용량 파일을 전송하여 귀중한 대역폭을 소비했습니다. 조사를 통해 해당 직원이 반복적으로 정책을 위반했음이 드러났습니다. 그는 Jabber와 IRC를 사용하고 본인의 데스크톱에서 무단 웹 서버를 운영하고 있습니다.

작업장의 사이버슬래킹

몰래 단타 거래를 하는 직원도 있습니다. 그 직원은 업무일 중 매일 아침과 저녁에 평균 1시간씩 금융 거래 사이트에 접속합니다. 또한 회사의 VoIP (SIP) 시스템을 사용하여 매일 평균 6개의 통화를 하고 수 시간 동안 "주식거래_길동"으로 Yahoo! 메신저에 접속하여 "주식거래_현수"와 "주식거래_희진"과 대화합니다.

약한 암호 사용자

회사의 보안 정책은 모든 사용자 시스템 및 응용프로그램 계정에 대한 강력한 암호 사용을 요구합니다. Microsoft Active Directory 계정은 엄격하게 관리됩니다. 하지만 Active Directory를 사용하지 않는 외부를 향한 FTP 서버, 메일 서버, 중요 웹 응용프로그램에서 수십 개의 약한 암호가 사용되고 있습니다.

자세히 알아보기

자세한 내용은 **www.mcafee.com/kr/products/siem/index.aspx**를 참조하십시오.

McAfee Together is power.

McAfee (Singapore) Pte Ltd
10 Kallang Avenue #08-10
Aperia Tower 2
Singapore 339510
www.mcafee.com/kr

61322ds_app-data-monitor_0914
2014년 9월