McAfee Application Data Monitor

응용 프로그램 계층 검사를 통한 사기, 데이터 손실, 숨겨진 위협 탐지

위협 활동은 응용 프로그램 층으로 그 활동 영역을 넓히고 있고 컴플라이언스 요건은 민감한 데이터에 대한 모든 액세스를 완벽하게 모니터링하고 기록 및 감사할 것을 요구합니다. McAfee® Application Data Monitor 어플라이언스는 응용 프로그램 층까지 모니터링함으로써 보안과 컴플라이언스를 로그 관리의 한계 이상으로 이끕니다. 고객은 응용 프로그램 내용을 모두 조사하여 고객의 네트워크가 어떻게 사용되고 있는지에 대해 가장 심층적으로 파악할 수 있습니다.

주요 장점

- 수백 개의 응용 프로그램에 대해 전체 응용 프로그램 세션을 계층 7까지 디코딩
- 기밀 데이터와 보안 데이터에 대해 사전 구축된 탐지 규칙 포함
- 사용자가 정의할 수 있는 사전과 규칙을 지원하여 사용자 정의 달성
- 응용 프로그램 이벤트의 전체 감사 추적을 생성하여 컴플라이언스 달성
- 수동적으로 작동하여 응용 프로그램 중단 방지
- McAfee Enterprise Security Manager와 통합되어 응용 프로그램 내용과 이벤트 및 기타 데이터 입력의 상관관계 구축 허용
- 유연한 혼합형 제공 옵션에 물리적 어플라이언스와 가상 어플라이언스 포함

McAfee Application Data Monitor 어플라이언스는 계층 7까지 전체 응용 프로그램 세션을 디코딩하여 기본 프로토콜과 세션 무결성에서부터 응용 프로그램 자체의 내용(예: 이메일의 텍스트 또는 첨부 문서)까지 모든 것에 대한 완벽한 분석을 제공합니다. 이와 같은 세밀한 수준 덕분에 실제 응용 프로그램의 사용에 대한 정확한 분석이 가능하게 되고 고객이 응용 프로그램 사용 정책을 이행하고 악성, 비밀 트래픽을 탐지할 수 있습니다.

이러한 심층 검사는 네트워크에 있는 중요한 데이터에 대한 모든 사용 내역을 추적함으로써 컴플라이언스를 지원합니다. McAfee Application Data Monitor 어플라이언스가 위반을 감지하면 사고 응답 및 포렌직에 사용하기 위한, 또는 컴플라이언스 감사 요건을 위한 해당 응용 프로그램 세션의 모든 세부 사항을 보존합니다.

동시에, McAfee Application Data Monitor 어플라이언스는 다음과 같이 합법적인 응용 프로그램으로 위장할 수 있는 위협에 대한 가시성을 제공합니다.

- 고급 응용 프로그램 계층 위협
- 기밀 데이터의 무단 사용 또는 도용
- 보안 "사각지대"에 대한 공격 또는 보안 "사각지대"로부터의 공격
- 위험한 레거시 코드의 사용
- 사용자 비밀 정보의 도용 또는 오용
- 응용 프로그램을 통한 중요 데이터의 전송
- 파괴된 비즈니스 프로세스

데이터 손실 및 컴플라이언스 위반

McAfee Application Data Monitor 어플라이언스는 중요한 정보가 이메일 첨부문서, 인스턴트 메시지, 파일 전송, HTTP 포스트 또는 다른 응용 프로그램 내부로 전송되는 시기를 탐지하여 손실이 완화될 수 있도록 고객에게 즉시 통보할 수 있습니다. 신용카드 정보와 사회보장번호와 같은 민감한 데이터를 간단하게 탐지하거나 기업만의 민감한 정보 및 기밀 정보에 대한 사전을 정의함으로써 McAfee Application Data Monitor 어플라이언스의 탐지 기능을 사용자 정의할 수 있습니다. McAfee Application Data Monitor 어플라이언스는 이와 같은 민감한 데이터 유형을 탐지하여 담당 직원에게 경보를 발신하고 위반을 기록하여 감사 추적을 유지합니다.

문서 탐지

McAfee Application Data Monitor 어플라이언스는 500개 이상의 문서 유형이 이메일, 채팅, P2P, 파일 공유 및 기타 수단을 통해 네트워크에서 교환될 때 이들 문서를 탐지합니다. McAfee Application Data Monitor 어플라이언스는 확장자와 관계 없는 문서, 즉 이메일 게이트웨이와 IDS/IPS 장치를 우회하도록 시도하면서 다른 유형으로 위장하는 문서를 탐지합니다. 다른 문서에 숨겨져 있는 문서나 아카이브 문서, 압축 문서, 암호화된 문서도 파일명과 작업과 같은 실행 가능 메트릭스를 통해 탐지됩니다.

응용 프로그램 계층 위협

새롭게 발생하는 첨단 위협은 일반적인 비즈니스 응용 프로그램 내의 취약성을 공격해 기업 네트워크에 침투하여 민감한 데이터를 가져갑니다. 이들 응용 프로그램 계층 위협은 기존의 방화벽 및 침입 탐지 시스템(IDS), 침입 방지 시스템(IPS)을 사용해서는 탐지하기가 어렵지만, McAfee Application Data Monitor 어플라이언스는 응용 프로그램의 전체 내용(기본 프로토콜 포함)을 조사하여 숨겨진 페이로드, 멀웨어, 비밀 통신 채널까지도 탐지할 수 있습니다(예: PDF 문서 내부에 내장된 실행 파일).

프로토콜 이상

이상 탐지는 임박한 위협을 사전에 파악하여 위험을 줄이고 손실을 최소화할 수 있습니다. 기존의 보안 솔루션들은 네트워크 흐름의 분석에 한정되어 있는 반면, McAfee Application Data Monitor 어플라이언스는 이러한 접근 방식을 한 차원 높게 끌어올립니다. 우리는 과거의 네트워크 동작을 분석하여 응용 프로그램과 프로토콜의 이상을 탐지하고 더 강력하고 더욱 사전적인 위험 탐지 방법론을 제공합니다.

응용 프로그램의 중단이 수반되지 않음

McAfee Application Data Monitor 어플라이언스는 SPAN 포트에서 작동하기 때문에 응용 프로그램의 성능이나 신뢰성을 방해하거나 시간 지연을 유발하지 않습니다.

기업 인프라에 통합

대부분의 네트워크 모니터링 솔루션은 독립적으로 작동되지만 McAfee Application Data Monitor 어플라이언스는 다른 정보 보안 시스템들과 함께 작동합니다. McAfee Application Data Monitor 어플라이언스는 McAfee Enterprise Security Manager를 통해 기업 보안 인프라의 나머지 부분에 연결되어 보안 운영을 간소화하고 전체적인 효율성을 향상시키겨 비용을 절감시킵니다. 손실 및 사기 탐지를 강력한 분석, 네트워크 검사, 데이터베이스 이벤트 모니터링 등과 통합할 수 있습니다.

사용 예

McAfee Application Data Monitor 어플라이언스는 여러 가지 무단 활동, 정책 위반, 도용, 사기를 탐지할 수 있습니다. 그 예는 다음과 같습니다.

기밀 정보의 도용

한 직원이 jdoe@company.com으로 로그인하여 accomplice@gmail.com으로 이메일을 보냈습니다. 이 이메일에는 shoo.doc이라는 파일이 첨부되어 있었고 이 파일에는 "비밀 공식"라는 단어가 포함되어 있었습니다. 이 이메일은 오후 12시 20분에 호스트 데스크탑0232(192.168.0.36)에서 SMTP 서버(10.0.2.13)를 사용하여 got it이라는 제목으로 전송되었습니다.

무단응용 프로그램의 사용

한 직원이 P2P 파일 공유 응용 프로그램을 설치하여 음악을 전송함으로써 정책을 위반했습니다. 그는 근무 시간에 소중한 대역폭을 소비하면서 대용량 파일을 전송했습니다. 이 직원이 상습범이라는 사실이 추가 조사를 통해 밝혀졌습니다. 그는 Jabber와 IRC를 사용하고 있었고 자신의 데스크탑에서 무단 웹 서버를 운영하고 있습니다.

직장에서의 사이버슬래킹

몰래 데이트레이딩을 하는 직원이 있습니다. 주중에 그녀는 매일 아침과 오후에 평균 한 시간 동안 금융 거래 사이트에 접속합니다. 또한, 회사의 VoIP(SIP) 시스템을 사용하여 매일 평균 여섯 번 통화를 하고 Yahoo! 메신저에서 "traderjoe"라는 이름으로 "traderbob"과 "tradergill"과 수 시간 동안 대화를 나눕니다.

취약한 암호의 사용

회사는 모든 사용자 시스템과 응용 프로그램 계정에 대해 강력한 암호를 사용할 것을 요구합니다. Microsoft Active Directory 계정은 엄격하게 관리됩니다. 그러나 Active Directory를 사용하지 않는 외부 연결 FTP 서버, 메일 서버, 중요 웹 응용 프로그램에서 수십 개의 취약한 암호들이 사용되고 있습니다.

500개 이상의 지원 응용 프로그램 및 프로토콜

- *저레벨 네트워크 프로토콜*—TCP/IP, UDP, RTP, RPC, SOCKS, DNS 및 기타
- *이메일*—MAPI, NNTP, POP3, SMTP, Microsoft Exchange
- *웹메일*—AOL Webmail, Hotmail, Yahoo! Mail, Gmail, Facebook, MySpace 이메일
- *인스턴트 메시지*—AOL,ICQ, Jabber, MSN, SIP, Yahoo
- *파일 전송 프로토콜*—FTP, HTTP, SMB, SSL
- *압축 및 압축 해제 프로토콜*—BASE64, GZIP, MIME, TAR, ZIP 및 기타
- *아카이브 파일*—RAR 아카이브, ZIP, BZIP, GZIP, Bin-hex, UU 인코딩 아카이브
- *설치 패키지*—Linux 패키지, InstallShield 캐비닛, Microsoft 캐비닛
- *이미지 파일*—GIF, JPEG, PNG, TIFF, AutoCAD, Photoshop, Bitmap, Visio, Digital RAW, Windows 아이콘
- *오디오 파일*—WAV, MIDI, RealAudio, Dolby Digital AC-3, MP3, MP4, MOD, RealAudio, SHOUTCast 및 기타
- *비디오 파일*—AVI, Flash, QuickTime, Real Media, MPEG-4 , Vivo, Digital Video(DV), Motion JPEG 및 기타
- *기타 응용 프로그램 및 파일*—데이터베이스, 스프레드시트, 팩스, 웹 응용 프로그램, 폰트, 실행 파일, Microsoft Office 응용 프로그램, 게임, 소프트웨어 개발 툴
- *기타 프로토콜*—네트워크 프린터, 셸 액세스, VoIP, P2P

자세한 내용은 mcafee.com/ADM에서 확인할 수 있습니다.

McAfee
An Intel Company

서울특별시 강남구 역삼동 737
강남파이낸스센터 16층 135-984
전화: (02)3458-9800
www.mcafee.com/kr

41607ds_app-data-monitor_0412_fnl_ETMG