McAfee Email Protection

언제 어디서나 사서함을 보호하는 첨단 성능

현대 기업은 첨단 이메일 보호 성능을 그 어느 때보다 필요로 합니다. SANS Institute에 따르면 네트워크 공격의 95%는 성공한 스피어 피싱의 직접적인 결과로 발생합니다.[1] 사용자들은 계속해서 소셜 엔지니어링 기술에 열중하고, 사이버 범죄자들은 보안을 중요시하는 조직이라도 경계를 풀고 걸려들 수 있도록 교묘한 술책으로 방법을 다양화하고 있습니다. 지능형 악성 프로그램 및 기업 지적 재산의 손실과 관련한 문제는 점점 심각해지고 있으며 조직에 심각한 부정적 영향을 미칠 수 있습니다. 또한 기업은 이메일을 호스팅된 사서함으로 마이그레이션하기 시작했습니다. 이로 인해 위험 수준이 높아질 수 있습니다. 마지막으로 레거시 이메일 보호 솔루션의 유연성 부족으로 인해 더 나은 대안을 찾게 됩니다. McAfee® Email Protection이 해답입니다. 이 강력한 솔루션은 통합 Data Loss Prevention(DLP) 기술과 이메일 Email Continuity를 통해 타겟화된 피싱 위협을 완벽하게 차단하는 엔터프라이즈급 보호 성능을 제공합니다. 클라우드 기반, 구내형 또는 통합 하이브리드 솔루션과 같은 유연한 배포 옵션을 사용하여 원하는 시간에 원하는 방식으로 이메일 보안을 구현할 수 있습니다.

주요 이점

타겟화된 피싱 공격으로부터 보호

- ClickProtect를 사용하여 악의적인 URL 위협을 실시간으로 탐지합니다.
- McAfee Advanced Threat Defense와 통합하여 은폐형 악성 프로그램을 방어합니다.
- 데이터 유실 방지 기술을 기본 제공합니다.

호스팅된 사서함 보안

- 이메일이 전송되는 위치에 상관없이 타겟화된 공격 차단
- 그레이메일 최종 사용자 콘솔
- 이메일 연속성
- 세분화된 데이터 유실 방지 및 암호화 기능

유연한 배포 옵션

- 원하는 시간에 원하는 방식으로 배포합니다.
- 단일 관리 및 보고 콘솔을 지원하는 하이브리드 배포 옵션입니다.

소셜 엔지니어링을 능가하는 위협: 새로운 스피어 피싱 전략

피싱 공격에 있어서 사용자는 가장 취약한 링크입니다. *Verizon Data Breach Investigation Report(Verizon 데이터 유출 조사 보고서), 2014*[2]에 따르면 약 5명 중 한 명의 사용자가 피싱 이메일에 제공된 링크를 클릭한다고 합니다. 사이버 범죄자들은 소셜 엔지니어링 기술을 통해 사용자의 취약성을 계속해서 활용하지만, 한 단계 더 나아가 다른 정교한 전술로 이메일 위협을 추적하기 어렵게 만듭니다. 몇 가지 예를 들어 보겠습니다.

- **일회성 URL:** 사이버 범죄자들은 사용자가 피싱 사기에 희생되어 감염되면 악성 URL을 남겨 놓습니다. 따라서 불가능한 것은 아니지만 감지 및 포렌식 수사가 어렵습니다.
- **지연된 감염:** 공격자가 이메일이 검색 후 승인되어 회사 받은 편지함에 제공될 *때까지* 기다렸다가 대상 웹 사이트에 페이로드를 남기는 경우도 있습니다. 직원들은 회사에 수신된 이메일을 신뢰하는 경향이 있으므로 악성 링크를 클릭할 수 있습니다.
- **샌드박스 인식 악성 프로그램:** 이러한 유형의 악성 코드는 잠재된 상태로 탐지를 회피하여 나중에 큰 피해를 발생합니다.

Advanced Layered Defense

클릭 시 보호

McAfee Email Protection은 정교한 스피어 피싱 공격과 이러한 공격에 연결된 은폐형 악성 프로그램을 차단할 수 있도록 다양한 보호 계층을 제공합니다. McAfee Web Gateway의 업계 1위 McAfee Gateway Anti-Malware Engine[3]을 활용하는 McAfee Email Protection은 ClickProtect라는 스캔 시 및 클릭 시 URL 보호

기능을 포함합니다. ClickProtect는 어디서나 모든 장치에서 스피어 피싱 시도를 차단합니다. ClickProtect는 이메일 메시지에 내장된 URL에서 위협을 탐지하여 제거합니다. 또한 메시지가 얼마나 무해한 것처럼 보이는지에 상관 없이 메시지가 검색된 시간과 사용자가 URL을 클릭하는 시간 사이에 발생한 URL 의도 변경을 확인합니다.

공격자가 조직 내의 재무 관리자를 대상으로 하는 악의적이지 않은 것처럼 보이는 URL로 이메일을 작성하는 지연된 악성 프로그램 시나리오에 대해 살펴보겠습니다. 이메일 보안 솔루션은 이메일을 수신한 후 조사를 통해 안전한 것으로 확인되면 받은 편지함으로 전달합니다. 하지만 이메일이 재무 관리자의 받은 편지함으로 전달된 이후에 공격자는 대상 웹 페이지에 악성 프로그램을 심어 놓습니다. 관리자가 링크를 클릭하면 네트워크가 감염됩니다.

ClickProtect를 사용하면 이메일의 URL을 클릭할 때 다음과 같은 질문이 표시됩니다. "URL이 안전합니까?" 모든 전달된 URL은 McAfee Gateway Anti-Malware Engine에서 다시 작성하여 검사합니다. 이때 서명을 신뢰하지 않고 동작 에뮬레이션을 사용하여 악의적인 웹 콘텐츠를 감지합니다.

사용자는 안전한 미리 보기를 통해 악의적인 웹 사이트를 안전하게 확인하고 모범 사례를 학습할 수 있으므로 보안을 강화하고 전체 위험을 낮출 수 있습니다. 따라서 메시지를 안전하게 전달할 수 있을 뿐만 아니라, 수신자가 ClickProtect를 사용하지 않는 경우에도 어디서나 이메일이 보호됩니다.

은폐형 악성 프로그램 탐지 및 차단
McAfee Advanced Threat Defense와 통합한 덕분에 McAfee Email Protection은 의심스러운 첨부 파일에서 은폐형 제로 데이 악성 프로그램을 탐지하여 받은 편지함에 도달하기 전에 차단할 수 있습니다. 이 혁신적인 계층화 접근 방식은 상세한 정적 코드(역설계)와 동적 분석(sandboxing)을 결합하여 악성 프로그램의 실제 동작을 분석합니다. 완전 정적 코드 분석을 사용하여 세부적인 악성 프로그램 분류 정보를 제공하고, 은밀하고 우회적인 위협에 대한 예방을 확대하며 코드 재사용을 활용하는 관련 악성 프로그램을 식별합니다. 지연되거나 조건부 실행 경로(종종 동적 샌드박스 환경에서 실행되지 않음)를 언패킹 및 완전 정적 코드 분석을 통해 감지할 수 있습니다.

기본 제공 데이터 유실 방지
타겟화된 스피어 피싱 공격은 궁극적으로 중요한 데이터를 목적으로 합니다. McAfee DLP 솔루션의 업계 최고 기술이 McAfee Email Protection에 통합되어 있습니다. 중요 데이터의 식별, 저장소 및 전송에 대한 컴플라이언스 정책을 개발할 수 있도록 돕기 위해 PCI DSS, 의료, 금융 정보, 지역 개인정보 규정 등에 대한 기본 제공 콘텐츠 사전이 포함되어 있습니다.

선택한 문서의 디지털 지문 인식을 생성하고 저장하면 McAfee Email Protection은 정책을 통해 제어하고 보호해야 할 콘텐츠 종류를 학습합니다. 정규 표현식 도구, 사용자 지정 가능한 사전, 임계값 카운터, 300개 이상의 문서 유형에서의 고급 콘텐츠 검색 및 화이트리스트를 통해 고객은 조직 내의 다른 사용자 그룹에 대한 첨부 파일 및 콘텐츠 정책을 생성하고 시행할 수 있습니다.

McAfee Email Protection에는 가상 어플라이언스로 배포하기 위한 온박스, 푸시, 풀 또는 TLS, S/MIME, PGP 이메일 암호화, 하드웨어 어플라이언스 또는 블레이드 서버가 추가 비용 없이 포함됩니다.

비즈니스 연속성을 위한 이메일 연속성
이메일 네트워크가 중단되어도 업무가 정지되지 않습니다. 네트워크가 자연재해, 정전 심지어 정기적인 유지 관리 때문에 액세스할 수 없는 상황에서도 McAfee Email Protection은 직원, 고객, 파트너 및 공급업체를 24시간 연중무휴로 연결할 수 있는 옵션을 제공합니다. 이메일 연속성 기능으로 정전 시 보내고 받은 메일을 모두 보존하며, 이메일 서버가 다시 온라인에서 작동할 때 해당 기간 동안 이루어진 모든 메시지 활동의 정확한 기록을 지능적으로 동기화합니다.

인텔리전스 및 위협 평판
McAfee Email Protection에는 1억 개 이상의 센서를 통해 파일, 웹, 메시지 및 네트워크 등의 모든 벡터에서 실시간 데이터를 수집하여 재배포하는 업계에서 가장 포괄적인 위협 인텔리전스 서비스인 McAfee Global Threat Intelligence(McAfee GTI)라는 강력한 도구가 추가되었습니다. McAfee GTI의 평판 분석은 의심스러운 출처에서 보냈거나, 의심스러운 웹 사이트를 연결하는 링크가 포함되어 있거나, 알려진 의심스러운 파일이 첨부된 이메일을 차단하여 위험을 최소화합니다.

McAfee Email Gateway

가상 어플라이언스 환경 및 시스템 요구 사항

- VMware vSphere 4.x 이상
- VMware vSphere Hypervisor(ESXi) 4.x 이상
- 프로세서: 가상 프로세서 2개
- 사용 가능한 가상 메모리: 2 GB
- 사용 가능한 하드 디스크 공간: 80 GB

하드웨어 어플라이언스

- 두 모델에서 사용 가능(별도 판매)
- 블레이드 서버 폼 팩터에서도 사용 가능

McAfee Email Protection, 3년 연속 별 5개 등급 수상(SC Magazine 선정).

악성 프로그램, 피싱 공격, 지능형 지속가능 위협 공격이 네트워크에 침투할 가능성을 대폭적으로 낮추어 조직을 더 안전하게 유지하고 비용이 많이 드는 교정 작업을 줄여 줍니다.

호스팅된 이메일의 보안 문제

Microsoft Office 365, Google Apps for Work 등과 같은 호스팅된 이메일 서비스를 통해 제공되는 엔터프라이즈 이메일 주소 수가 점점 증가하고 있습니다. 많은 호스팅된 이메일 솔루션이 서비스의 일환으로 보안을 제공할 수 있습니다. 하지만 그것으로 충분할까요? 그렇지 않을 것입니다. 피싱 시도, 스팸 및 그레이메일이 지속적으로 발생함에 따라 기본 제공 보안 기능만으로는 데이터 유출을 완전히 차단할 수 없습니다. 예를 들어, Office 365와 관련한 이메일 중단으로 인해 생산성이 감소할 수 있습니다. McAfee Email Protection은 테스트, 마이그레이션, 사후 마이그레이션 중에 타겟화된 피싱 공격과 진화한 악성 프로그램을 방어하는 엔터프라이즈급 보호 성능을 제공합니다. 사서함이 배포되는 시간과 장소에 상관없이 McAfee Email Protection은 전체 적용 범위와 이메일 연속성을 제공합니다.

현재와 미래를 위한 유연한 배포 옵션

McAfee Email Protection은 원하는 방식으로 이메일 보안을 배포할 수 있는 유연성을 제공합니다. 클라우드 기반 SaaS(Software-as-a-Service) 솔루션, 사내 솔루션(가상 어플라이언스, 하드웨어 어플라이언스, 블레이드 서버) 또는 둘을 조합한 하이브리드 솔루션 중에서 선택할 수 있습니다. McAfee Email Protection을 사용하면 현재 요구 사항에 가장 적합한 방식으로 이메일 보안을 배포하고 나중에 확장하거나 방침을 변경할 수 있습니다.

배포 옵션에 상관없이 McAfee Email Protection은 이메일 보안 프로그램의 효율성을 쉽게 측정할 수 있는 통합 보고를 위한 단일의 중앙 집중식 관리 콘솔을 제공합니다. 정책은 솔루션의 클라우드 기반 구성 요소와 사내 구성 요소 모두에 적용됩니다.

McAfee Email Protection에 관한 자세한 정보를 확인하거나 제품 평가를 시작하려면 McAfee 담당자에게 문의하거나 www.mcafee.com/kr/products/email-and-web-security/email-security.aspx를 방문하십시오.

1. http://blogs.mcafee.com/business/security-connected/is-there-something-phishy-in-your-inbox
2. https://dti.delaware.gov/pdfs/rp_Verizon-DBIR-2014_en_xg.pdf
3. AV-TEST: *McAfee Web Gateway Security Appliance Test(McAfee Web Gateway 보안 어플라이언스 테스트)*

McAfee. Part of Intel Security.
서울특별시 강남구 역삼동 737
강남파이낸스센터 5층 135-984
+82.2.3458.9800
www.intelsecurity.com

61523ds_email-protection-o365_0115