McAfee Email Gateway

기업 이메일 방어.

모든 비즈니스 환경에서 이메일은 없어서는 안 될, 업무에 가장 필수적인 서비스 중 하나입니다. 조직, 지리 및 정치적 경계를 넘나들며 광범위한 정보 페이로드를 즉각적으로 배포하는 기능으로 인해 이메일은 필수 도구이면서도 특별한 보안 문제를 일으키고 있습니다. McAfee® Email Gateway는 배포하기 쉬운 단일 어플라이언스에서 이메일 보안을 개선하고 인바운드 위협 방지, 아웃바운드 데이터 유실 방지, 암호화, 고급 컴플라이언스 및 중앙 집중식 관리로 방어 기능을 강화합니다.

주요 이점

철저한 인바운드 및 아웃바운드 보호

- 모든 이메일에 포함된 위협으로부터 포괄적인 인바운드 보안
- 내장된 이메일 암호화
- 중요한 정보 손실을 막기 위한 내장된 컴플라이언스 템플릿 및 데이터 유실 방지

지능형 보안, 관리 및 확장성

- 가상 어플라이언스, 하드웨어 어플라이언스, 블레이드 서버로 사용 가능하거나 McAfee SaaS Email Protection과 함께 통합 하이브리드 솔루션으로 사용 가능.
- 중앙 집중식 관리, 메시지 검색, 보고 및 격리.
- 가장 까다로운 사내 요구 사항도 충족할 수 있는 클러스터링 및 통합된 로드 균형 조정 확장

McAfee® ePolicy Orchestrator®(McAfee ePO™) 소프트웨어, McAfee GTI(Global Threat Intelligence), McAfee Advanced Threat Defense 및 하이브리드 이메일 보안 방식을 통해 Security Connected를 활용합니다.

이메일 보안 문제

오늘날 기업이 직면한 심각한 이메일 보안 문제를 살펴보겠습니다.

- 인바운드 이메일 공격은 점차 금전적인 이득을 얻을 수 있는 정보를 찾는 조직적인 범죄 행위가 되어가고 있습니다. 이러한 공격은 정교한 사회 공학 기술을 사용하고 신속하게 변화하여 기존의 시그니처 기반 방어 시스템을 신속하게 회피합니다.
- 이메일은 악의는 없지만 부주의한 직원이나 악의적인 내부 소행자에 의한 기밀 데이터 및 중요한 데이터의 도난이나 유실과 관련된 기본 매개체가 됩니다.
- 이러한 운영상의 중요도와 광범위한 취약성으로 인해 이메일은 정치 및 산업 경계를 초월해 규제 기관의 감시를 받고 있습니다. 이메일을 규제하는 법률 분야로는 지불 카드(PCI DSS), 금융 서비스(GLBA), 보건(HIPAA) 및 모든 미국 공기업(SOX)이 있습니다.
- 국가마다 수치에 차이가 있지만, 전체 이메일의 약 75%는 스팸입니다. 스피어 피싱은 갈수록 대상이 분명해지고 있으며, 재정적인 집중성 및 효과가 점점 향상되고 있습니다.
- McAfee Labs는 2013년 4분기에 매일 약 2,250개의 피싱 URL을 확인했으며 이 숫자는 일년 내내 계속 변함이 없었습니다.

왜 단편적이고 부적절한 방어에 안주하십니까?

오늘날의 기업 이메일 방어 기능은 발전했지만, 기존 이메일 보안은 대부분 전적으로 인바운드에만 집중하고 아웃바운드 데이터 유실에 대해서는 방어 기능을 제공하지 않습니다. 즉 안티맬웨어, 안티스팸, 안티피싱, 안티바이러스, 암호화, 데이터 유실 방지 등 다양한 솔루션으로 구성되어 있는 방어 기능을 여러 공급업체에서 구입하고, 개별적으로 배포하며, 반복해서 조정해야 합니다. 이 중 다수가 현재의 모범 사례 성능 표준을 충족하지 못하고 있습니다.

intel Security

2013년 수상 내역

- 보안 이메일 게이트웨이 부문 선두업체, Gartner Magic Quadrant
- 이메일 콘텐츠 보안 부문 선두업체, Forrester Wave
- *SC Magazine* 최고의 이메일 콘텐츠 보안 별 5개 Best Buy
- 업계 혁신: *SC Magazine* 데이터 보호 부문.

업계 최고의 안티스팸 솔루션에서는 99% 이상의 스팸 탐지 정확도를 달성하는 반면 대다수의 이메일 방어 시스템은 95% 이하의 정확도를 달성할 뿐입니다. 4% 차이가 별 것 아닌 것처럼 보일 수 있습니다. 그러나 실제 스팸 침입 및 잠재적인 시스템 감염에서의 차이는 400%가 됩니다. 수십억 개의 이메일에서 스팸이 발견된 경우 스팸이 4%의 증가는 메일 인프라 부담과 대역폭 과부하에 시달리는 비즈니스에 현저한 영향을 미칠 수 있습니다. 소수의 원치 않는 이메일이 방어 시스템을 침입한 경우 사용자는 스팸을 가려내고 삭제하느라 업무에 지장을 받을 수 있습니다. 악성 프로그램에 감염될 가능성이 높아져 비용이 늘어나고, 생산성이 떨어지며, 잠재적인 데이터 유실의 가능성이 커집니다.

따라서 대부분의 IT 조직에서 단편적인 방어 시스템을 유지하고, 기밀 정보가 조직에서 빠져나가지 못하게 하고, 컴플라이언스 규제 정책을 입증하며, 부적절한 이메일 보안의 영향을 수습하는 데 너무 많은 시간과 비용을 투자할 수밖에 없습니다. 인바운드와 아웃바운드 방어 시스템을 통합하고, 관리를 간소화하며, 컴플라이언스를 능률화한 포괄적인 이메일 보안 솔루션의 뛰어난 비즈니스 사례가 있습니다. 바로 McAfee Email Gateway입니다.

포괄적인 이메일 보호

시장 최고의 보안 솔루션

McAfee Email Gateway는 아웃바운드 데이터 유실 방지, 첨단 컴플라이언스 및 이메일 암호화, 성능, 보고 및 간소화된 관리 기능을 모두 강화된 단일 플랫폼에서 단일 비용으로 첨단 인바운드 위협 방지 기능과 통합합니다.

- 로컬 네트워크 정보를 McAfee GTI의 평판 지능과 결합하여 인바운드 위협, 스팸 및 악성 프로그램에 대해 사용할 수 있는 가장 완벽한 보안을 제공합니다.
- McAfee Gateway Anti-Malware Engine의 동작 에뮬레이션 기능을 사용한 클릭 시 링크 검색으로 악성 URL을 촉매로 사용하는 공격을 방지합니다.
- McAfee Advanced Threat Defense와 통합되어 정적 코드 및 동적(모래상자) 분석의 혁신적인 결합을 통해 가장 정교하고 우회적인 악성 프로그램을 탐지할 수 있습니다.
- McAfee Email Gateway의 정교한 콘텐츠 검색 기술, 다수의 암호화 기술 및 세분화된 정책 기반 메시지 처리 기능은 아웃바운드 데이터 유실을 방지하고 컴플라이언스를 능률화합니다.
- McAfee ePO 소프트웨어와 완전히 통합되므로, 관리 및 컴플라이언스 워크로드를 간소화하여 비용을 크게 줄이는 엔터프라이즈급 로깅 및 보고 기능을 통해 클러스터 내에서 또는 클러스터 간에 솔루션을 완전히 관리할 수 있습니다.

포괄적인 인바운드 위협 방지

McAfee Email Gateway는 99% 이상의 정확도로 들어오는 스팸을 차단하는 한편 바이러스, 악성 프로그램, 피싱, 디렉터리 수집, 서비스 거부 공격(DDoS) 및 바운스백 공격에 대한 통합된 보안을 제공합니다. 또한 제로 시간 위협과 표적 공격 및 복합 공격을 방지하고, 동적 스팸 분류 및 위협 대응의 강력한 결합을 통해 스팸 급증의 영향력을 크게 줄입니다. McAfee Email Gateway는 McAfee GTI의 발신자, 메시징 및 URL 평판을 사용하는 업데이트를 제공합니다.

고객이 악성 프로그램에 대한 계층적 보호를 제공하고 컴플라이언스 요구 사항을 충족할 수 있도록 보조 안티바이러스 엔진도 포함됩니다.

클릭 시 링크 검색으로 진화하는 공격을 방지하다.

McAfee Email Gateway의 특징인 McAfee ClickProtect는 이메일 메시지에 포함된 URL로 인한 위협을 제거합니다. 설령 무해하게 보일지라도 메시지가 검색되는 시간(검색 시간)과 사용자가 URL을 클릭하는 시간(클릭 시간) 사이에 발생하는 URL의 의도 변화를 확인합니다. 이러한 재검사에는 McAfee Web Protection에서와 동일한 업계 선도적인 Gateway Anti-Malware 기술을 활용하는 URL 평판 검사와 사전 예방적인 에뮬레이션이 모두 포함됩니다. 관리자는 검색 시간과 클릭 시간 정책을 모두 구성하고 URL 에뮬레이션을 통해 클릭으로부터 사용자를 보호합니다. Safe Preview는 사용자 인텔리전스를 추가 보안 계층으로 활용하여 곧 출시 예정인 페이지에 대한 미리보기를 제공합니다. 전적으로

이메일 메시지로부터 시작되는 웹 액세스를 완전히 방지하기 위해 URL을 함께 탐지하여 삭제하거나 설명 문구로 교체할 수 있습니다.

McAfee Advanced Threat Defense로 정교한 우회성 악성 프로그램을 탐지하다.
McAfee Advanced Threat Defense는 혁신적인 계층화된 접근 방법을 사용하여 오늘날의 은폐형 제로 데이 악성 프로그램을 탐지합니다. 이 기능은 상세한 정적 코드와 동적 분석(sandboxing)을 결합하여 악성 프로그램의 실제 동작을 분석합니다. Mcafee Email Gateway와 McAfee Advanced Threat Defense가 완벽하게 통합됨으로써 의심스러운 이메일 첨부 파일에 대해 이러한 분석을 수행하고 받은 편지함에 수신되기 전에 악성임이 확인된 파일을 차단할 수 있습니다.

서명 및 실시간 에뮬레이션과 같은 분석 강도가 낮은 방법이 더 나은 성능을 제공하지만, 전체 정적 코드 분석을 sandboxing에 추가하여 자세한 악성 프로그램 분류 정보를 얻을 수 있으며 고도로 위장한 침입 위협에 대해 광범위한 보호를 제공하고 코드 재사용을 이용하는 관련 악성 프로그램을 식별할 수 있습니다. 종종 동적 환경에서 실행되지 않는 지연되었거나 우발적으로 나타나는 실행 경로를 언패킹 및 전체 정적 코드 분석을 통해 탐지할 수 있습니다.

정적 코드와 동적 분석은 결합하여 완전한 평가와 동작 요약, 악성 프로그램 심각도, 악성 프로그램 연관, 실행 경로, 동적 분석 중에 실행된 코드 비율 등과 같은 자세한 정보를 제공합니다.

그레이메일 필터링으로 원하지 않는 메일이 감소하다.
원하지 않는 메일에는 사용자가 전에는 원했지만 지금은 원하지 않는 합법적인 대량 메일도 포함될 수 있습니다(예: 산업 뉴스레터 및 알림). 그레이메일은 일반적으로 스팸으로 간주되지 않지만 수신자 입장에서는 매우 성가실 수 있습니다. 차단과 격리를 비롯한 필터링을 적용하면 사서함을 깨끗하게 유지할 수 있습니다.

내용을 안전하게 보관하기 위한 포괄적인 아웃바운드 보호
이메일 암호화가 포함되다.
정책이 적용된 통합 이메일 암호화가 표준 기능으로서 포함되어 B2B(TLS, S/MIME 및 OpenPGP) 및 B2C 기술(푸시 또는 풀)이 함께 사용되며, 암호화 기능이 없는 수신자도 보안 이메일을 받고 답장할 수 있습니다. 푸시/풀 기술에는 브랜딩 가능한 웹 메일 클라이언트가 포함되어 있으며 모바일 장치에서 암호화된 메시지를 검색하고 볼 수 있도록 지원합니다. 데스크톱 대신 게이트웨이에서 암호화를 적용하면 사용자가 암호화 요구 사항을 확인할 필요가 없고, 중요한 데이터를 암호화하는 것을 잊어버리는 일반적인 사용자 문제를 피할 수 있습니다.

컴플라이언스 및 데이터 유실 방지
McAfee Data Loss Prevention에 포함된 것과 같은 강력한 기본 제공 컴플라이언스 템플릿 모음도 표준 기능으로서 통합 및 포함되어 있습니다. 구조화되거나 구조화되지 않은 데이터를 둘 다 종합적으로 탐지하기 위해 지문 인식, 어휘 분석 및 클러스터링 기술은 키워드 및 패턴 일치를 보완합니다. 게이트웨이는 규제 대상 콘텐츠(HIPAA, SOX, GLBA), 개인 식별이 가능한 정보(신용카드, 주민등록번호, 지역별 식별자 등), 기타 고객 및 직원 데이터를 정확히 식별합니다. 소스 코드, 특허, 금융 정보 및 비즈니스 계획과 같이 구조화되지 않은 데이터 및 지적 재산 역시 탐지하여 그에 관한 조치를 취할 수 있습니다. 이러한 정보를 탐지한 후에는 강제 암호화(푸시, 풀, TLS), 경보, 경로 재지정, 격리, 차단 및 기타 사용자 지정 작업을 비롯한 광범위한 정책 기반 조치를 지원합니다.

포괄적인 강력한 관리 기능

McAfee Email Gateway를 통해 관리자는 최적의 이메일 보호 기능을 제공할 수 있으며 엔터프라이즈급 보고, 내보낼 수 있는 포괄적 로그, 실시간 구성 가능한 대시보드, 경보 및 드릴다운 보고를 사용하여 이를 문서화하는 기능도 제공합니다. McAfee Email Gateway에서는 성능, 확장성, 안정성이 유연한 공급 모델과 통합되어 관리 간접 비용이 최소화되고 최대 ROI가 보장됩니다. 이 솔루션은 McAfee Email Gateway 관리 콘솔 또는 McAfee ePO 소프트웨어에서 완전히 관리할 수 있으며 다음과 같은 기능도 제공합니다.

정교한 사용 및 정책 제어를 토한 손 쉬운 관리.

- 마법사 기반 설치 및 구성 기능을 갖춘 매끄러운 직관적인 인터페이스.
- 디렉터리/LDAP(Lightweight Directory Access Protocol) 통합.
- 세부적인 정책 시행, 메시지 검색, 자세한 대화 로그를 갖춘 이메일 보안용 중앙 집중식 관리.
- 대화형 대시보드와 드릴다운 보고 기능을 포함한 실시간 보고.

지능형 아키텍처를 통한 우수한 성능.

- 비동기 메모리 기반 검색.
- 고가용성을 위한 통합 클러스터링 및 로드 균형 조정.
- 온박스 또는 확장성이 뛰어난 McAfee Quarantine Manager는 여러 McAfee Email Gateway 어플라이언스에 대한 통합 격리 서비스와 사용자 지정 격리 대기열을 제공하며, 150만 개의 메시지 처리 용량으로 저장소 및 프로세스 워크로드 부담을 줄이고 최대 200,000 명의 사용자를 지원합니다.

인증 및 지원

- NDPP 컴플라이언스를 포함한 EAL2+의 Common Criteria 인증.
- FIPS 140-2 L1 소프트웨어 검증 및 인증.
- CAC 카드(x.509) 지원.
- IPv6 지원.

미래에도 경쟁력을 갖춘 솔루션: 모든 기업에게 적합한 완벽한 이메일 보안

배포 유연성

McAfee Email Gateway는 하드웨어 어플라이언스(4가지 다양한 어플라이언스 크기) 또는 가상 시스템으로서 배포하거나, 블레이드 서버 아키텍처에 배포할 수 있습니다. 이러한 유연성은 가장 까다로운 비즈니스 메시징 환경에 경제적인 보안 및 확장성을 제공합니다. 또한 McAfee Email Gateway는 단일 가입 비용의 통합 하이브리드 조합, 클라우드 기반의 SaaS(Security-as-a-Service) 또는 사내 이메일 게이트웨이(하드웨어 또는 가상)로서 이메일 보안을 배포할 수 있는 유연성을 제공하는 McAfee Email Protection의 일부입니다.

클라우드의 이점을 활용하고 싶지만 현장 제어 유지 관리를 선호하는 조직은 통합 하이브리드 솔루션을 사용하여 McAfee Email Gateway를 클라우드 기반 및 사내 정책 관리, 통합 보고, 메시지 검색 및 격리를 위한 제어 센터로서 활용할 수 있습니다. 일반적인 하이브리드 시나리오의 조직은 네트워크에서 악의적이거나 성가신 콘텐츠를 차단하여 대역폭을 줄이고, 현장 어플라이언스에서 중요한 정보 취급 및 암호화를 처리하고자 하는 조직입니다.

Security Connected

고객은 Security Connected 프레임워크를 통해 보안 상황을 개선하고, 보안을 최적화하여 비용 효율성을 높이고, 보안을 비즈니스 이니셔티브에 맞게 전략적으로 조정할 수 있습니다. McAfee ePO 소프트웨어와의 통합을 통해 보안 솔루션 내에서 또는 솔루션 간에 관리 및 보고 기능을 통합할 수 있습니다. McAfee 솔루션의 전체 포트폴리오를 사용하는 McAfee GTI(Global Threat Intelligence)는 McAfee 솔루션에서 차단하는 가능한 모든 위협 벡터로부터 종합적인 인텔리전스를 수집합니다. 상관관계 데이터 및 인텔리전스가 McAfee의 제품 및 솔루션과 공유됩니다. 따라서 Intel Security의 일부로 McAfee에서 제공하는 이메일 보안에는 항상 최신의 제로 시간 정보가 포함되어 있습니다. McAfee Advanced Threat Defense는 최신의 은폐형 제로 데이 악성 프로그램을 탐지하고 McAfee Email Gateway를 포함한 여러 제품과 완벽하게 통합됩니다. McAfee Advanced Threat Defense는 여러 솔루션 간의 공유 리소스 역할을 수행하며 네트워크에 전체에서 비용 효율적으로 확장되고 운영 비용을 최소화합니다.

그러므로 관리 감독 및 비용을 최소화하면서 가장 규모가 크고 까다로운 워크로드에 적합한 엔터프라이즈급 기능을 얻을 수 있습니다. McAfee Email Gateway는 기능, 성능, 안정성 및 가치를 고유하게 결합할 수 있으므로 Fortune 500대 IT 조직의 절반 이상에서 이메일 보안 솔루션으로 채택하고 있습니다. McAfee Email Gateway 솔루션에 대한 자세한 내용은 **www.mcafee.com/kr/products/email-and-web-security/email-security.aspx**를 참조하십시오.

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