



McAfee SaaS Email Protection and Continuity

생산적인 비즈니스를 위한 이메일 보호, 가용성 및 컴플라이언스

이메일과 이메일 액세스를 간단하게 보호하는 방법

McAfee SaaS Email Protection and Continuity은 다음과 같은 주요 이메일 보호 기능을 포함합니다.

- 위협이 고객 네트워크에 도달하기 전에 위협을 차단하는 경계 IP 필터링
- 고급 스팸, 그레이메일 방지 및 불법 행위 금지
- 알려진 모든 바이러스를 100퍼센트 차단하는 계층화된 바이러스 및 웹 검색
- 이메일 공격 보호
- 아웃바운드 메시지 및 첨부 파일에 대한 필터링 및 정책 적용
- 완벽한 메시징 연속성
- 그룹 정책 관리
- 메시지 감사 메시지 추적 및 처리 도구
- 선택적 McAfee SaaS Email Encryption



McAfee® SaaS(Security-as-a-Service) Email Protection and Continuity를 사용하여 쉽게 이메일 보안 문제를 해결하십시오. 이 클라우드 기반 서비스는 스팸, 피싱 스팸, 악성 프로그램, 그레이메일 및 부적절한 이메일 내용이 네트워크에 접근하기 전에 차단하는 것 외에도, 발신 메일 정책을 적용하여 데이터 유출을 방지합니다. 또한 조직에서 이메일에 연중 무휴로 액세스할 수 있도록 상시 이메일 연속성을 활용합니다. 추가 하드웨어 구입 및 추가 소프트웨어 설치 없이 최신 위협에 대항하여 자동 업데이트되므로 응용프로그램의 실행이 아닌 비즈니스 보호에 집중할 수 있습니다.

이메일은 오늘날 일반적인 회사의 이메일 서버를 통해 매일 수 많은 메시지가 이동하는 생산성 엔진입니다. 그래서 보안과 연결성을 보장하기 위해 이메일을 관리하는 일은 거대한 작업이 되어 IT 리소스가 회사의 목표를 이루는 전략적인 업무에 집중하지 못하도록 만들고 있습니다.

저렴하고 관리가 용이한 이메일 보호

배포가 간편한 McAfee SaaS Email Protection and Continuity는 어떤 상황에서도 이메일에 대한 지속적인 액세스를 유지하면서 인바운드 및 아웃바운드 이메일 위협이 네트워크 및 사용자에게 영향을 주지 못하게 합니다. 이 보안 Software-as-a-Service는 항상 작동하며 항상 최신으로 유지되고, 유지 관리를 위한 시간 및 리소스 투자가 추가적으로 필요하지 않습니다. 이 프록시 기반 서비스는 스팸과 이메일 기반 위협을 네트워크에 침투하기 전에 차단하므로 이메일 서버에 대한 부하가 크게 줄어들어 귀중한 대역폭과 서버 저장 공간을 절약할 수 있습니다. 또한, 세계적 수준의 24시간 연중무휴 McAfee 고객 지원은 전화 통화만큼이나 쉽게 이용하실 수 있습니다.

단순화된 웹 기반 관리 및 보고

하나의 직관적인 웹 기반 관리 콘솔을 사용하는 이 서비스에는 모범 사례가 내장되어 있으며 이메일 정책 업데이트를 모든 도메인과 위치에서 간단히 관리할 수 있어서 IT 리소스를 자유롭게 하고 총 소유 비용을 줄여줍니다. 관리자는 콘텐츠 필터링 및 첨부 파일 콘텐츠 규칙 등의 정책을 구성 및 적용할 수 있습니다. 정책은 최고의 유연성을 위해 사용자 그룹이나 개인에게 포괄적으로 적용되며 광범위한 보고, 로그 및 검역이 최고의 가시성을 제공합니다.

신뢰할 수 있고 역동적인 인프라

McAfee의 SaaS 데이터 센터 전략에는 네 개 대륙에 걸쳐 있는 여러 개의 데이터 센터에 대한 유지 관리를 포함합니다. 각 데이터 센터는 ISO 27001 인증을 획득했으며 방화벽, 라우터 및 로드밸런서 스위치를 비롯한 모든 네트워크 계층에서 액티브-액티브 중복 하드웨어로 완전한 중복성을 제공합니다. McAfee는 각 데이터 센터 내에서, 자동화된 네트워크 및 응용프로그램 모니터링 기능을 제공하여 원격 작업 담당자가 의심스럽거나 문제가 되는 경보 및 경고를 볼 수 있도록 하고 24시간 연중무휴로 보안 전문가가 항상 시스템을 감시할 수 있습니다.

저렴하고, 관리가 용이한 이메일 보안 및 연속성

- 구입, 유지, 관리 또는 업데이트할 하드웨어 또는 소프트웨어가 없습니다.
- 선불 자본 지출이 필요 없습니다.
- 설정 또는 업그레이드 수수료가 없습니다.
- 원활한 연속성을 위해 자동으로 연속성을 활성화 및 동기화합니다.
- 단순한 웹 기반 관리입니다.
- 추가 비용 부담이 없는 24 시간 연중무휴 고객 지원을 제공합니다.
- ISO 27001을 획득했습니다.

비즈니스 평판, 사업 및 생산성 보호를 위한 자동 이메일 연속성

- 중단 탐지 시 자동 서비스 수행
- 안전한 웹 인터페이스를 통해 중단 시 받은 이메일 사용
- 읽기, 작성, 회신, 전달 및 삭제 기능을 포함한 모든 이메일 기능 사용 가능
- 자동 중단 후 이메일 활동 동기화
- 중단 알림 및 시스템 업데이트
- 인바운드 및 아웃바운드 메시지 필터링

Microsoft Office 365 및 Google Apps for Business 와 호환 가능

자세한 내용

McAfee SaaS Email Protection and Continuity 를 포함한 모든 McAfee SaaS 솔루션의 시간 절약, 생산성 및 보안 이점에 대한 자세한 내용은 www.mcafee.com/kr/products/security-as-a-service/index.aspx 를 참조하십시오.

엄중한 이메일 보안

우수한 스팸 방지 기능

특허 받은 기술을 사용하는 McAfee의 Stacked Classification Framework 스팸 탐지 시스템은 다층적 분석을 적용하여 언어에 상관없이 이메일이 스팸일 가능성을 판단합니다. 각 필터링 기술에는 이미지 기반 스팸을 포함한 특정 위협을 식별하도록 설계된 특별한 강점들이 있기 때문에 이 필터링 기술들의 조합은 업계에서 가장 정확하고 포괄적인 필터링 프로세스 중 하나를 만들어냅니다.

McAfee Global Threat Intelligence(McAfee GTI) 메시지 평판 기능은 각 메시지를 조사함으로써, 메시지가 화이트리스트 회사 내의 감염된 시스템과 같은 평판이 좋은 소스로부터 오는 경우에도 스팸과 같이 알려졌거나 새로 출현하고 있는 메시지 기반 위협을 탐지할 수 있습니다. 성능을 최대로 발휘할 수 있도록 효율적이고 정확하게 이메일을 차단 또는 격리하기 위해 점수는 McAfee 클라우드에 귀리하는 센서의 종합적인 지능과 McAfee Labs 연구원 및 자동화된 도구가 수행하는 분석뿐만 아니라 파일, 웹 및 네트워크 위협 데이터의 매개체 통합 지능의 상관 관계도 기반으로 합니다.

받은 편지함을 안전하게 보호하는 그레이메일 필터링

원하지 않는 메일에는 사용자가 전에는 원했지만 지금은 원하지 않는 합법적인 대량 메일도 포함될 수 있습니다(예: 산업 뉴스레터 및 알림). 관리자는 그레이 메일 필터를 사용하여 개인 또는 그룹용 그레이 메일 정책을 설정할 수 있으며 사용자는 이 기능을 통해 사서함에 원치 않는 메일이 들어오지 않도록 유지할 수 있습니다.

바이러스 및 웜을 효과적으로 차단하는 다계층화된 검색 사용

McAfee SaaS Email Protection and Continuity에는 McAfee 소유의 WormTraq 탐지 기술이 포함되어 있습니다. 이 서비스는 McAfee GTI에서 제공하며 업계를 선도하는 시그니처 기반 안티바이러스 엔진을 사용하여 메시지 본문과 모든 첨부 파일에서도 악성 프로그램을 검색합니다. 인바운드 공격을 차단하는 것만큼이나 중요하게 아웃바운드 이메일도 필터링하여 클라이언트를 악성 프로그램으로부터 보호합니다.

대규모 이메일 공격으로부터 조직을 보호해 주는 완전한 확장성

McAfee의 완전한 솔루션은 디렉터리 수집 공격, 이메일 폭탄 및 채널 범람을 포함한 서비스 거부(DoS) 및 기타 SMTP 기반 공격을 순간적으로 차단하여 네트워크와 중요한 메시징 게이트웨이를 이메일 공격으로부터 보호합니다.

안전한 조직 간 통신을 위한 내장 TLS(Transport Layer Security) 암호화

인바운드 및 아웃바운드 이메일에 대한 더 높은 수준의 보안을 필요로 하는 조직의 경우 McAfee의 TLS 프로토콜에서 암호화된 인바운드 및 아웃바운드 메시지를 받아 필터링하고, TLS 인증 기관 확인을 포함하여 안전한 터널을 통해 이메일을 전달합니다.

어떤 상황에서도 이메일 연속성 유지

이메일 네트워크 환경이 중단되어도 업무가 정지되지 않습니다. 자연 재해, 정전, 심지어 정기적인 유지 관리로 인해 네트워크에 액세스할 수 없는 경우에도 McAfee SaaS Email Protection and Continuity에서는 직원, 고객, 파트너 및 공급업체를 24시간 연중무휴 연결합니다. 안전하고 사용하기 간편한 웹 인터페이스는 지속적인 보호를 받으며 메시지를 보내고 받고, 저장된 메시지를 검색 및 회수하며, 검역 및 메시지 보관 상태를 관리할 수 있도록 해줍니다.

사전 구축된 규칙, 고급 콘텐츠 검색 및 문서 지문 인식

McAfee의 업계 최고 기술을 활용하여 고급 데이터 유실 방지(DLP) 및 컴플라이언스 기능을 쉽게 이용할 수 있습니다. McAfee SaaS Email Protection and Continuity 외에도 McAfee SaaS Email Encryption을 사용하면 PCI DSS, 보건, 재무 데이터, 지역 개인 정보 보호 규정 등에 대한 사전 구축된 콘텐츠 규칙을 이용할 수 있으므로 컴플라이언스 정책을 빠르게 생성할 수 있습니다. 300가지 이상의 문서 종류를 검색하고 보호하여 기업이 아웃바운드 데이터를 유실하지 않도록 할 수도 있습니다.

고급 문서 지문 인식 기술을 사용하면 이메일 보안 기능이 어떤 종류의 콘텐츠가 정책 제어 대상이 되는지 알 수 있도록 선택한 문서의 디지털 지문 인식을 생성하고 저장할 수 있습니다. 이메일

및 첨부 파일에서 콘텐츠의 전체 또는 일부 일치 항목에 대해 정책을 세부적으로 시행할 수 있습니다. 키워드 및 구문을 식별하는데 정규식 기술을 사용할 수도 있습니다.

사용하기 쉬운 푸시/풀 암호화

McAfee SaaS Email Encryption을 사용하면 수신자에게 암호화 솔루션이 없어도 중요 정보의 암호화에 대한 소유권을 가져올 수 있습니다. 비즈니스 사용자를 위해 설계된 사용하기 쉬운 푸시/풀 암호화 기술은 모바일 장치에서도 무단으로 엿보지 못하게 데이터를 보호해줍니다.

McAfee의 Security Connected를 통한 보호, 관리 및 컴플라이언스 최적화

이 모든 것을 통합하면 관리가 단순해지고, 보안 솔루션이 철저히 작동하여 학습 곡선을 최소화하며, 단일 창을 통해 실시간으로 확인할 수 있습니다. 전체 McAfee SaaS 솔루션 제품군은 원스톱 콘솔을 통해 관리될 수 있습니다.

변화를 위한 시간

어떻게 유지 관리를 최소화하고 IT 담당자의 과중한 업무를 줄여서 더 전략적인 프로젝트에 집중할 수 있는지 확인해 보십시오. 자세한 정보를 확인하시고 www.mcafeesaas.com에서 무료 평가판에 등록하세요.



McAfee. Part of Intel Security.

서울특별시 강남구 역삼동 737
강남파이낸스센터 5층 135-984
+82.2.3458.9800
www.intelsecurity.com

Intel 및 Intel 로고는 미국 및/또는 기타 국가에서 Intel Corporation의 등록 상표입니다. McAfee 및 McAfee 로고는 미국 및 기타 국가에서 McAfee, Inc. 또는 자회사의 등록 상표 또는 상표입니다. 기타 이름 및 브랜드는 각 소유자의 재산으로 주장될 수 있습니다. 이 문서의 제품 계획, 사양 및 설명은 정보용으로만 제공되고, 사전 통보 없이 변경될 수 있으며, 어떤 종류의 명시적 또는 암시적 보증 없이 제공됩니다. Copyright © 2014 McAfee, Inc. 60166ds_saas-protect-continuity_0313B_fnl_ETMG