



McAfee SaaS Web Protection

안전하게 보호되는 네트워크를 위한 클라우드 기반 웹 보안

주요 이점

- 연속적인 업데이트로 빠르게 변화하는 제로 데이 악성 프로그램 공격으로부터 네트워크 외부의 사용자를 포함한 모든 사용자 보호.
- 인터넷 사용 정책 시행 및 사용자나 그룹별 세부 보고서를 통해 웹 사용에 대한 가시성 제공
- 100개 이상의 콘텐츠 범주를 통해 유연한 콘텐츠 제어가 가능하여 법적 책임으로부터 비즈니스 보호
- 생산성을 저해할 수 있는 소셜 미디어 사이트를 포함하여 수백 개의 온라인 미디어 유형과 응용프로그램에 대한 통제 지원
- 예측 가능하고 완벽하게 확장형 가입 서비스를 통해 사내 자본 장비 비용과 인력 요구의 증가를 대신함
- 검증된 보호 기능 : McAfee SaaS Web Protection은 현 전 세계적으로 수천에 달하는 고객과 수십만 사용자의 웹 사용을 보호하고 있음

웹은 불행히도 귀사의 비즈니스뿐만 아니라 사이버 범죄 비즈니스에도 무한한 비즈니스 기회의 문을 열어주었습니다. 웹에 연결하면 감염, 악성 프로그램 침입, 기업을 위험에 노출시키는 요인이 진입할 수 있는 잠재적인 경로가 생성됩니다. McAfee® SaaS Web Protection은 McAfee Global Threat Intelligence에서 가져온 최신의 광범위한 위협 데이터를 사용하여 웹 기반의 동적 악성 프로그램 공격에 맞서 간편하고 기능이 풍부하며 필수적인 방어 기능을 제공합니다. McAfee 웹 및 클라우드 보안 전문가가 업계 모범 사례를 활용하여 24시간 연중무휴로 관리하는 McAfee SaaS Web Protection을 통해 위협 및 원하지 않는 인터넷 액세스를 효과적이며 경제적으로 제어할 수 있게 됩니다.

웹의 동적 콘텐츠 및 상호 작용으로 인해 기존의 보안 조치를 피해 정교한 웹 기반 위협을 시스템에 전달하는 사례가 늘어나고 있습니다. 기업은 직원, 고객, 네트워크 및 지적 재산을 보호하기 위해 사전 예방 차원의 웹 보안을 필요로 합니다. 즉, '알려진 불량' URL뿐만 아니라 알려지지 않았거나 숨겨진 공격, 혼합된 위협 및 스파이웨어까지 차단하는 솔루션이 요구됩니다. McAfee SaaS Web Protection은 웹 콘텐츠의 동작과 그것이 사용되는 컨텍스트를 파악함으로써 McAfee Gateway Anti-Malware Engine을 사용하여 악의적인 의도를 예측하고 다른 보안 솔루션으로는 방지할 수 없는 위협을 차단합니다.

규제 없이 웹을 사용하면 사용자 생산성이 낮아지고 법적인 문제로 연결될 수도 있습니다. 안전하고 적절한 인터넷 액세스 관리로 인해 리소스가 소모될 수 있지만 반드시 그런 것은

아닙니다. 클라우드 기반 콘솔을 통한 정책 규칙 설정 방법은 간단하면서도 온라인 콘텐츠, 미디어 유형, 응용프로그램, 심지어 특정 웹 서비스에 대한 액세스 허용 시간까지도 세밀하게 제어할 수 있습니다.

하드웨어나 소프트웨어를 설치할 필요가 없는 McAfee SaaS Web Protection은 포괄적인 웹 보안을 위한 안정적이고 경제적인 솔루션입니다. 검증된 SaaS(서비스형 소프트웨어) 플랫폼을 바탕으로 구축된 이 글로벌 서비스는 거의 지연이 없으며 업계 최고의 가동 시간과 전사적인 확장성을 지원하여 까다롭고 분산된 환경에 필요한 성능을 보장합니다. 사내 웹 필터링을 이미 갖춘 기업의 경우 McAfee 서비스는 위협이 적고 경제적인 솔루션으로서 지능형 안티멀웨어를 사용하여 보호 프로파일을 향상시키거나 지사 및 모바일 사용자를 보호합니다.

주요 동기 요인

- 기존 웹 보안 기술의 유지 관리 간접 비용 절감을 위한 노력
- 악성 프로그램 관련 문제 증가
- 원거리에 있거나 이동하는 사용자에게 전사 차원의 보안을 제공하기 위한 요구 사항

McAfee Global Threat Intelligence에서 전 세계의 위협 데이터를 수집

웹 위협 및 악성 콘텐츠가 전 세계로 확장되면서, McAfee 방화벽도 다음과 같이 확대됩니다. McAfee Global Threat Intelligence 네트워크를 통해 120개 이상 국가에서 1억 개 이상 센서로부터 실시간으로 데이터를 수집하고, 분석하며 배포합니다.

- 북미에서는 스팸 URL이 모든 웹 위협의 41%를 차지하며 악성 사이트와 의심스러운 악성 사이트가 그 뒤를 잇고 있습니다.
- 유럽/중동/아프리카에서는 스팸과 피싱 URL이 각각 전체의 31%를, 다른 사이트를 대체하는 악성 사이트가 29%를 차지하고 있습니다.
- 중남미에서는 악의적인 URL의 36%가 스팸 호스팅과 연관되어 있으며, 30%는 피싱 사이트, 25%는 다른 종류의 악성 웹 사이트를 호스팅하고 있습니다.
- 아시아/태평양 지역에서는 전체의 31%가 의심스러운 사이트로 구성되어 있으며, 해당 서버는 사이트를 면밀하게 모니터링하는 방식으로 등록되어 있습니다. 그 다음으로 큰 그룹은 스팸 URL로 29%를 차지하고 그 다음은 24%를 차지한 악성 사이트입니다.

(출처: McAfee Labs)

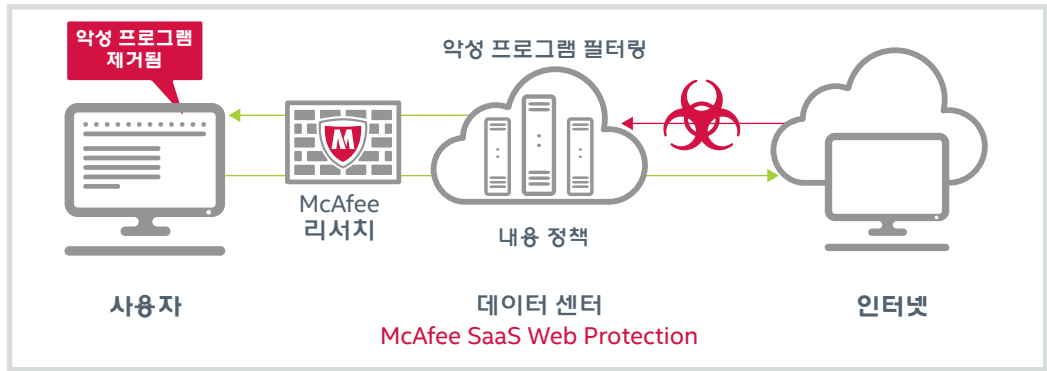


그림 1. McAfee SaaS Web Protection 웹 요청 흐름

완벽한 웹 보호

McAfee SaaS Web Protection은 인바운드 및 아웃바운드 웹 트래픽을 모두 보호합니다. 정책이 적용되는 모든 사용자에게 액세스 규칙을 자동으로 적용하여 조직의 인터넷 사용 정책을 시행합니다. 기업의 정책을 위반하는 트래픽은 네트워크에 진입하기 전에 차단됩니다. 허용된 트래픽의 경우 McAfee SaaS Web Protection은 안티바이러스 및 글로벌 위협 평판 필터 위에 추가된 지능형 안티맬웨어 엔진을 통해 정교한 기술을 사용하여 요청된 웹 페이지에서 모든 콘텐츠와 활성 코드의 특성과 의도를 분석합니다. 이는 악성 프로그램을 차단하고 위협 요소를 제거하며 안전한 콘텐츠를 제공함으로써 사용자가 업무를 계속할 수 있도록 악성 프로그램, 바이러스 및 기타 취약성 공격에 대한 즉각적인 보호를 제공합니다.

내용 분석을 통해 악성 프로그램 변경 감지

웹 사이트의 악성 프로그램은 의심하지 않는 방문자 장치에 아무도 모르게 다운로드되어 지적 재산이나 고객 정보의 유출을 일으킬 수 있습니다. McAfee는 수상 경력이 있는 McAfee Gateway Anti-Malware Engine을 활용하여 웹 페이지의 활성 콘텐츠를 검색하고 그 의도나 예상 동작을 파악함으로써 제로 데이 악성 프로그램, 복합 보안 위협, 피싱 사이트 및 개인 정보를 빼돌리려는 타겟화된 공격으로부터 사전에 보호합니다.

유연하고 포괄적인 제어

비즈니스 환경에서의 웹 사용은 양날의 검과 같습니다. 생산성의 중심이면서 편리하지만 부적절한 활동이 발생하기 쉽고 때론 큰 비용을 발생시키기도 하는 플랫폼입니다. 사용자를 악성 프로그램으로부터 보호하는 것은 꼭 필요하지만 그게 전부는 아닙니다. 데이터 손실을 막고 직원의 생산성을 유지하면 비용을 절약하고 잠재적인 심각한 법적 책임을 방지할 수 있습니다.

약 100개의 사이트 범주를 포함한 포괄적인 웹 필터링 옵션, 수백 개의 미디어 유형, 1000개 이상의 온라인 응용프로그램 및 암호화된 SSL 트래픽을 통해 불쾌하거나 바람직하지 않은 활동 또는 비생산적인 활동이 없는 웹 액세스를 보장할 수 있습니다. 사용자는 시간을 낭비하는 방해 요소 없이 여전히 자유로운 웹을 경험할 수 있습니다. 동시에 다음을 할 수 있게 됩니다.

- 특정 웹 응용프로그램을 드릴다운하고 직원이 특정 시간에 소셜 미디어 사이트를 액세스할 수 있도록 허용합니다.
- 온라인 파일 공유 사이트로의 업로드 기능을 중지하거나 파일을 업로드하기 전에 파일 암호화를 시행하는 한편 외부 협력자가 전송한 파일 다운로드를 허용함으로써 데이터를 사내에 유지합니다.
- 원거리에서 근무하거나 이동하는 직원은 각자 판단하여 웹에 액세스하도록 허용하는 한편 전사적 차원의 보안을 계속 시행합니다.

이와 같은 세부 제어는 인터넷 액세스에 대한 무분별한 차단보다 효율적이므로 생산적이고 안전한 온라인 환경을 조성할 수 있습니다.

간소화되고 투명한 인증, 추가로 네트워크 보안 사용 또는 사용 중지

McAfee SaaS Web Protection을 사용하면 직원의 웹 트래픽을 라우팅하기가 쉬워집니다. 브라우저 프록시 설정 또는 프록시 자동 구성(PAC) 파일 같은 표준 라우팅 기술을 사용하거나 McAfee Client Proxy로 훨씬 더 쉽게 만들 수 있습니다. 이 무료 선택 사항인 클라이언트 소프트웨어 기술을 사용하면 브라우저 플러그인 또는 쿠키를 관리하거나 중앙 허브로 트래픽을 역전송하거나 PAC 파일을 쓰지 않고도 원활한 인증 및 리디렉션을 구현할 수 있습니다. 쉽게 조작할 수 없는 McAfee Client Proxy를 사용하면 커피숍, 호텔 또는 기타 WiFi 핫스팟 같은 공개 포털을 통해 인터넷에 액세스하더라도 웹 보호 정책 및 웹 보안을 네트워크 밖에 있는 로밍 사용자에게 적용할 수 있습니다.

편리한 관리 및 보고

사용자 지정 가능한 대시보드를 통해 각 관리자는 경향을 모니터링하고 해당 조직의 웹 및 이메일 리소스 사용 방법을 보다 잘 파악할 수 있습니다. 브라우저에서 문제를 격리하고, 부적절한 활동을 문서화하고, 규제 보고를 준수하고, 웹 사용 정책을 시행할 필터링 설정을 상세 조정할 수 있습니다. 맞춤형 통보는 사용자에게 정책 위반 및 차단된 웹 콘텐츠에 대해 알립니다. 관리 경보는 중요한 보안 이벤트에 대한 정보를 즉시 제공합니다.

자세한 내용

McAfee 클라우드 기반 보안 서비스를 사용하면 쉽고 경제적으로 비즈니스를 보안할 수 있습니다. McAfee SaaS Web Protection을 McAfee SaaS Endpoint Protection, McAfee SaaS Email Protection 및 McAfee SaaS Email Archiving 서비스와 함께 사용하여 모든 디지털 위협과 컴플라이언스 취약성을 해결할 수 있습니다.

McAfee는 SaaS 제품 외에도 가장 유연한 솔루션을 찾는 고객을 위해 어플라이언스, 가상 및 SaaS 폼 팩터를 갖추어 모든 기능이 하나로 통합된 제품을 제공합니다.

자세한 내용은 www.mcafee.com/kr/products/security-as-a-service/index.aspx 또는 www.mcafee.com/kr/products/web-protection.aspx를 참조하십시오.

