

McAfee Web Protection

클라우드, 사내 또는 하이브리드 조합에 구매받지 않고 조직에 필요한 웹 보안 구축

웹 필터링 및 안티멀웨어 검색부터 심층적인 콘텐츠 검사와 클라우드 응용프로그램 사용 방식에 대한 세부적인 제어에 이르기까지, McAfee® Web Protection은 엔터프라이즈 보안을 위해 필요한 보안, 제어 및 배포 유연성을 제공합니다. 사내 솔루션의 제어 기능을 원하든, 클라우드 서비스의 탁월한 확장성과 저렴한 비용을 추구하든, 아니면 이 두 가지가 혼합된 조합을 찾고 있든 상관없이, McAfee Web Protection은 기존 요구나 변화하는 요구에 가장 적합한 방식으로 웹 보안을 배포할 수 있게 해줍니다.

웹이 계속 성장하고 발전함에 따라 웹 기반 악성 프로그램 공격도 심화되고 증가하면서 엔드포인트 및 중요 데이터를 위협하고 있습니다. 위험 수준이 꾸준히 증가함에 따라 이에 걸맞은 최고의 웹 보안이 필요하게 되었습니다. McAfee는 오늘날과 같이 클라우드로 연결된 환경의 보안 요구사항을 이해하고 있으며 위협 방어 지향 엔터프라이즈에 포괄적인 웹 보안을 제공합니다.

사내, 클라우드 또는 하이브리드

McAfee는 궁극적인 배포 유연성을 갖추고 투자에 대한 미래 경쟁력을 확보할 수 있도록 **McAfee Web Gateway** 및 **McAfee Web Gateway Cloud Service**의 모든 기능을 단일 솔루션으로 제공합니다. **McAfee Web Protection**. 엔터프라이즈급 유연성과 가용성을 위해 확장할 수 있는 전용 하드웨어 또는 가상 어플라이언스 제품군이 있는 사내에

배포할지, 클라우드 서비스로 배포할지 아니면 두 가지 방법을 같이 사용할지 선택할 수 있습니다. 예를 들어 조직은 하드웨어 또는 가상 어플라이언스를 사용하여 기업 본사의 직원을 보호하고, 클라우드 서비스를 사용하여 원격 직원 또는 이동 중인 직원을 보호할 수 있습니다. 또한 지사에서는 사이트의 트래픽을 모두 클라우드 서비스로 라우팅하여 일반적으로 모든 공개 웹 트래픽을 처리를 위해 중앙 위치로 역전송하는 MPLS (MultiProtocol Label Switching) 네트워크의 비용을 절감할 수 있습니다. 모든 옵션을 갖춘 수상 경력이 있는 수상 경력이 있는 McAfee 악성 프로그램 방지 및 포괄적인 웹 필터링을 구매할 수 있습니다. 사내에서 클라우드로 동기화된 정책 관리를 통해 모든 플랫폼에서 일관된 규칙 기반 정책을 시행할 수 있도록 해줍니다.

주요 이점

최고의 유연성

- McAfee Web Gateway 어플라이언스 소프트웨어 및 McAfee Web Gateway Cloud Service의 모든 기능을 단일 구독으로 이용할 수 있습니다.
- 현재의 요구를 해결하면서 이후 상황에 따라 자유롭게 조정 가능
- 배포 방식과 관계없이 예측 가능한 사용자 기반 가입 가격

고급 보안

- McAfee Web Protection에서는 동작 분석에 대한 특허 출원된 접근법을 포함하는 McAfee Gateway Anti-Malware Engine을 사용해 제로 데이 악성 프로그램을 실시간으로 차단합니다.
- McAfee Endpoint Security, McAfee Advanced Threat Defense, McAfee Cloud Threat Detection 및 McAfee Threat Intelligence Exchange

McAfee에 문의



클라우드 인프라

AWS (Amazon Web Services) 등의 IaaS (Infrastructure as a Service) 기술은 동적인 기업 확장성과 더불어 거의 제한 없는 리소스를 제공합니다. 보안 전문가는 웹 보안이 해당 환경에서 실행될 수 있으며 클라우드 워크로드를 보호할 수 있는지 확인해야 합니다. McAfee Web Gateway 고객에게는 AWS 내에서 포워드 프록시, 리버스 프록시 또는 엔드포인트, 데이터 및 응용프로그램을 보호하기 위한 ICAP (Internet Content Adaptation Protocol) 서버로 배포할 수 있는 유연성이 부여됩니다. 이를 통해 조직에서는 고도의 위험성이 있는 트래픽을 지능형 안티맬웨어 엔진으로 라우팅할 수 있습니다. 이는 또한 McAfee Web Gateway 데이터 유실 방지 기능을 이용하거나 기존 데이터 보호 솔루션을 활용하여 잠재적으로 중요한 정보에 대한 데이터 흐름을 확인하는 기능도 제공합니다.

고급 보안

McAfee Web Protection에는 제로 데이 위협 및 알려진 위협을 차단하는 고급 보호를 제공하는 다양한 위협 탐지 기술이 포함되어 있습니다. 이 기능을 사용하면 McAfee Web Protection이 여러 가지 보완적인 기술을 사용하여 단일 플랫폼의 보안을 최적화할 수 있으며, 이러한 능력은 많은 조직이 계층형 방어 보안 접근 방식을 위해 구축하고자 하는 기능입니다. 심층 콘텐츠 검사는 Zip 파일 PDF 및 그래픽도 검색하여 숨겨진 악성 프로그램을 찾아냅니다. 독립적인 조사 기관들은 악성 프로그램을 최대 99%까지 정확하게 탐지하고 차단하는 McAfee 웹 보안 솔루션을 높이 평가했습니다.

McAfee의 고급 계층 보안에는 다음이 포함됩니다.

- **실시간 조회를 사용하여 포괄적인 시그니처 기반 안티바이러스 보호:** McAfee는 첨단 바이러스 탐지 기술과 실시간 조회 기능을 갖춘 McAfee Global Threat Intelligence (McAfee GTI) 파일 평판을 통해 바이러스 발견과 시스템 보호 간의 차이를 좁혔습니다.
- **웹 평판 및 웹 분류를 포함한 McAfee GTI:** McAfee Web Protection은 평판과 범주 기반 필터링의 강력한 결합을 통해 뛰어난 웹 필터링 기능 및 보안을 제공합니다. McAfee GTI는 McAfee Web Protection의 웹 필터링 기술을 더욱 강화하고 McAfee Labs의 방대한 글로벌 데이터 수집 기능을 통해 수집된 수백 개의 다양한 특성을 기반으로 웹 사이트, 이메일 및 IP 주소와 같은 모든 인터넷 엔티티의 프로파일을 만듭니다. 그런 다음 잠재된 보안 위험을 기준으로 평판 점수를 할당하므로 관리자가 허용 또는 거부할 항목에 대해 세분화된 규칙을 적용하고 계속해서 이러한 항목을 모니터링할 수 있습니다. 동적 콘텐츠 분류에서는 이전에 알려지지 않은 웹 사이트의 콘텐츠를 분석하고 콘텐츠가 바람직하지 않은 범주(도박, 음란물, 게임 등)에 속하는지를 판단합니다.
- **제로 데이 방지를 위해 콘텐츠를 실시간으로 공개하는 동작 분석:** McAfee Web Protection에서는 제로 데이 악성 프로그램 방지를 위한 특허 출원된 접근법을 통해 웹 트래픽이 통과할 때 기계 학습 인텔리전스를 실시간 동작 에뮬레이션에 통합합니다. McAfee Web Protection은 웹 페이지의 활성 콘텐츠를 검색하고, 동작을 에뮬레이션하고, 의도를 예측하여 제로 데이 공격 및 표적 공격이 엔드포인트 시스템에 도달하기 전에 사전 대응적으로 방지합니다.

철저한 인바운드 및 아웃바운드 보호

- 셀 수 없을 만큼 다양하게 사용자 지정할 수 있는 규칙 기반 정책 엔진을 통해 조직의 인터넷 사용 정책을 실시합니다.
- 계층 보안을 통해 악성 프로그램과 기타 숨겨진 위협에 대한 즉각적이고 효과적인 보호 제공
- 랩톱, Apple iOS 및 Google Android 장치를 비롯하여 원격 사용자를 위한 모바일 필터링을 제공합니다.
- 수천 가지의 클라우드 응용프로그램 제어 기능을 포함하고 있습니다.

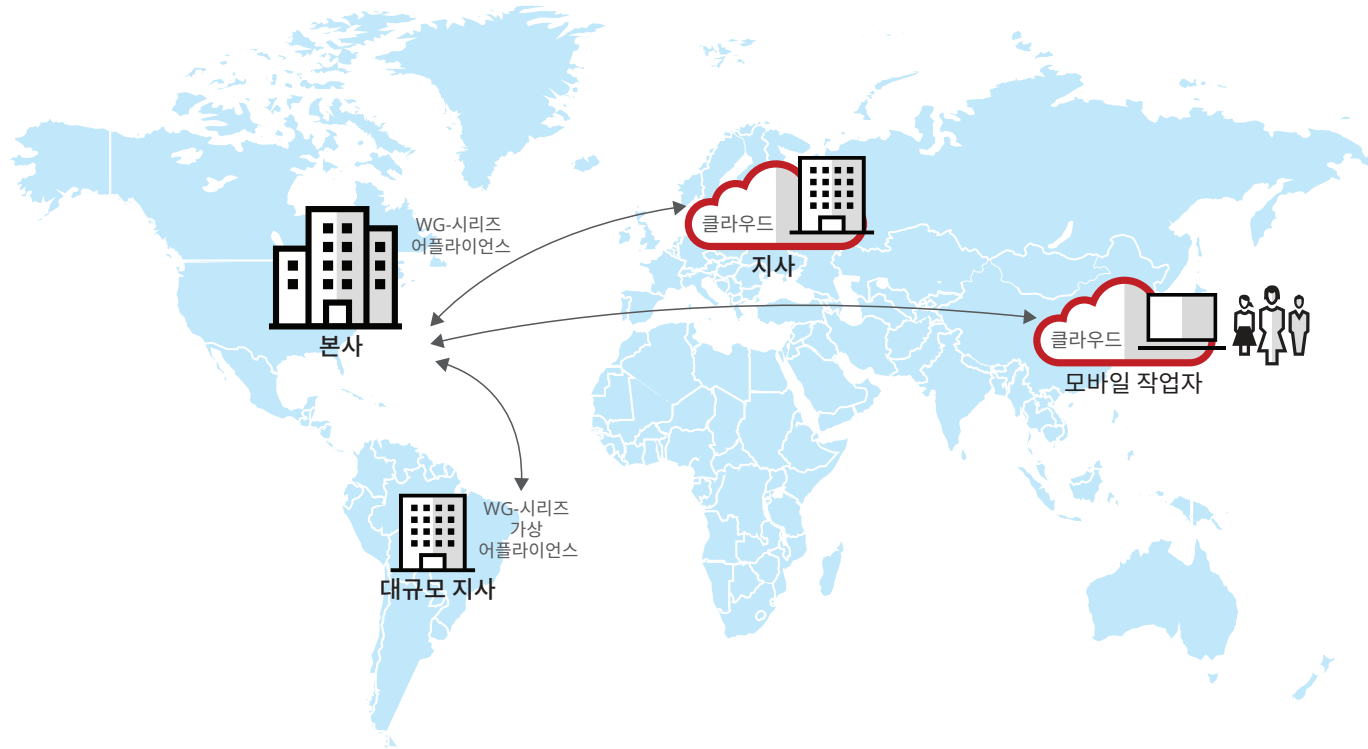


그림 1. McAfee Web Protection은 궁극의 배포 유연성을 제공합니다. 배포 유연성과 고가용성을 향상하기 위해 어플라이언스가 있는 사내 또는 클라우드의 가상 환경에서 배포할지 아니면 두 가지 방법을 같이 사용할지 선택할 수 있습니다.

클라우드 응용프로그램 제어

클라우드 응용프로그램으로 전환할 때 따르는 결과 중 하나는 그림자 IT가 발생할 가능성이 높아진다는 점입니다. 승인되지 않은 클라우드 응용프로그램을 보안 전문가가 추적하지 못할 경우 데이터 유출 및 잠재적인 재정적 손실이 발생할 위험이 있습니다. McAfee Web Protection은 모든 웹 트래픽에 대한 완벽한 가시성을 제공하며 수천 가지의 클라우드 응용프로그램 제어 기능을 포함하고 있습니다. 그러한 기능은

비즈니스 기준(예: 응용프로그램 위험 또는 사용자 프로파일)에 따라 액세스를 관리하거나 제한하는 데 사용할 수 있습니다.

어디에서나 보호 가능

근무 인력이 더욱 분산되고 그 이동성이 높아지면서, 사무실에서 이동 중인 환경으로 원활하게 전환할 수 있는 웹 필터링 및 보호 기능에 대한 필요성이 점점 중요해지고 있습니다. McAfee Web Protection 고객은 McAfee Web

점점 더 커지는 위협의 세계

오늘날의 웹 위협은 스팸 및 피싱 이메일 링크, 멀버타이징, 소셜 미디어는 물론 직원들이 매일 사용하는 걸보기엔 무해한 파일까지 다양한 형태와 규모, 수단을 취합니다. McAfee Web Protection은 모든 각도에서 보안을 제공합니다.

- 악성 프로그램 샘플의 70%~90%는 조직에 고유합니다.
- McAfee Labs는 분당 300개 이상, 혹은 초당 5개꼴로 새로운 악성 프로그램을 식별하고 있습니다.¹

1. McAfee Labs

데이터시트

Protection 및 McAfee Endpoint Security에 포함된 McAfee Client Proxy를 활용하여 네트워크 외부 사용자를 위한 웹 액세스를 보호하는 동시에 제어할 수 있습니다. 액세스를 보호하는 동시에 제어할 수 있습니다. 이러한 통합 게이트웨이 인식 솔루션은 완벽한 정책 실시를 위해 사내 또는 클라우드와 같은 사용자 위치에 따라 웹 트래픽을 지능적으로 McAfee Web Protection 솔루션으로 라우팅합니다. 모바일 장치 관리 파트너인 AirWatch 및 MobileIron과의 통합을 통해 기업은 시스템상의 다른 모든 장치와 동일한 웹 보안 정책을 통해 Apple iOS 및 Google Android 장치를 보호할 수 있습니다.

통합 보고

광범위하게 활용되고 높은 평가를 받고있는 엔터프라이즈 보안 관리 McAfee® ePolicy Orchestrator® (McAfee ePO™) 소프트웨어는 McAfee Web Protection용 보고 솔루션입니다. 통합된 정보를 위한 단일 소스인 McAfee ePO 플랫폼을 통해 문제를 신속하게 파악하여 완화시키고 컴플라이언스 관리를 개선할 수 있습니다. McAfee ePO 소프트웨어는 McAfee Content Security Reporter 확장 기능을 통해 상세한 웹 보고 기능을 제공합니다.

McAfee Content Security Reporter는 조직이 통합 보고 인프라를 위해 사내 및 클라우드 McAfee Web Protection 제공 플랫폼을 포괄하여 데이터를 집계할 수 있게 해줍니다. McAfee Content Security Reporter는 해당 조직에서의 웹 사용 현황을 이해하고 규정을 준수하며 동향을 파악하고 문제를 격리하며 부적절한 웹 활동을 문서화하고 웹 사용 정책에 따라 필터링 설정을 맞춤 구성하는 데 필요한 정보와 도구를 전달합니다. 웹 트래픽에 대한 대시보드 보기 및 드릴다운을 강력한 오프라인 처리 기능과 결합한 이 제품은 필요한 모든 기능을 두루 갖춘, 사용하기 편리한 단일 솔루션입니다.

McAfee Content Security Reporter는 기존의 McAfee ePO 소프트웨어 서버에서 리소스 집약적인 데이터 처리 및 저장소를 오프로드하는 외부의 독립형 보고 서버를 제공함으로써 확장을 통해 가장 큰 글로벌 기업의 보고 요구 사항도 충족할 수 있습니다.

자세한 내용은 www.mcafee.com/kr/products/web-protection.aspx를 참조하십시오.



McAfee (Singapore) Pte Ltd
10 Kallang Avenue #08-10
Aperia Tower 2
Singapore 339510
www.mcafee.com/kr

McAfee 및 McAfee 로고, ePolicy Orchestrator 및 McAfee ePO는 미국 및 기타 국가에서 McAfee, LLC 또는 자회사의 상표 또는 등록 상표입니다. 기타 이름 및 브랜드는 각 소유자의 재산으로 주장될 수 있습니다. Copyright © 2018 McAfee, LLC. 4176_1118
2018년 11월