McAfee Web Gateway

보안. 연결된 인텔리전스. 성능.

오늘날 기업들은 웹을 통해 과거 어느 때보다도 많은 일을 해낼 수 있습니다. 오늘날 웹은 동적인 사용자 환경을 실시간으로 제공합니다. 그러나 정교한 공격이 나날이 증가함에 따라, 웹은 위험한 곳이 되어가고 있기도 합니다. McAfee® Web Gateway는 새로운 악성 프로그램의 위협으로부터 조직을 보호하기 위한 핵심 방어 기능을 수행합니다. 이 어플라이언스를 통해 조직은 보안 인터넷 액세스를 강화하고, 강력한 로컬 의도 분석 기능을 McAfee Labs의 클라우드 기반 보호 기능과 결합된 고급 보안 접근 방식을 통해 위험을 크게 낮출 수 있습니다.

McAfee Web Gateway

- 다중 하드웨어 모델 및 VMware 및 Microsoft Hyper-V 지원 가상 시스템으로 제공됩니다.
- McAfee Endpoint Security, McAfee Advanced Threat Defense, McAfee Threat Intelligence Exchange, McAfee Cloud Data Protection 및 McAfee Cloud Visibility—Community Edition을 포함한 보완 McAfee 솔루션과 통합되었습니다.
- Common Criteria EAL2+ 및 FIPS 140-2 Level 2 인증.
- Gemalto SafeNet 하드웨어 보안 모듈(HSM), Thales nShield HSM 및 Thales PCIe 카드를 포함한 여러 암호화 키 저장소 옵션을 지원합니다.
- 보안 웹 게이트웨이(AV-TEST) 부분에서 업계 1위로 선정된 안티맬웨어입니다.

인터넷 사용이 늘어나고 더 정교해지면서 고급 웹 보안에 대한 요구도 증가하고 있습니다. 겉으로는 "안전하게" 보이는 사이트라도 악성 프로그램 배포의 표적이 될 수 있습니다. 오늘날에는 단순히 알려진 바이러스를 차단하거나 알려진 악성 웹 사이트에 대한 액세스를 차단하는 것만으로는 충분하지 않습니다. 시그니처 기반 안티바이러스 및 범주만 사용하는 URL 필터링과 같은 사후 대처 기술이 필요하지만 클라우드 응용프로그램에 대한 액세스를 보호하거나 오늘날의 취약성 공격에 대응하기에는 충분하지 않습니다.

이러한 솔루션은 알려진 콘텐츠 및 악성 개체 또는 실행 파일에 초점을 두기 때문에 신뢰할 수 있는 것처럼 보이는 HTTP 또는 HTTPS 트래픽 내에 악성 코드를 숨기는 오늘날의 공격을 막을 수 없으며, 알려지지 않은 위협이나 새롭게 등장하는 위협도 막을 수 없습니다. 오늘날에는 알려진 위협뿐 아니라 알려지지 않은 위협도 사전에 차단하면서 클라우드 응용프로그램을 안전하게 세분화하여 액세스할 수 있는 기능이 매우 중요합니다.

포괄적인 인바운드 및 아웃바운드 보호

McAfee Web Gateway는 웹 트래픽의 모든 측면을 위한 포괄적인 보안 기능을 단일 고성능 어플라이언스 소프트웨어 아키텍처로 제공합니다. McAfee Web Gateway는 사용자가 시작한 웹 요청에 대해 먼저 조직의 인터넷 사용 정책을 적용합니다. 허용된 트래픽에 대해서는 요청된 웹 페이지를 통해 네트워크에 진입하는 모든 콘텐츠 및 활성 코드의 특성과 의도를 로컬 및 글로벌 기술을 활용하여 분석하고, 악성 프로그램 및 기타 숨겨진 위협으로부터 즉시 보호합니다. 기본적인 패킷 검사 기술과 달리, McAfee Web Gateway는 SSL(Secure Sockets Layer) 트래픽을 검사하면서 암호화를 거쳐 악성 코드나 컨트롤 응용프로그램을 찾아내는 심층적인 보호 기술을 발휘합니다.

또한 인바운드 보호는 외부 소스로부터의 데이터 또는 문서 업로드를 허용하는 웹사이트를 호스팅하는 조직이 직면할 수 있는 위험을 완화합니다. 역 프록시 모드에서 McAfee Web Gateway는 모든 콘텐츠를 업로드하기 전에 스캔하여 서버와 콘텐츠를 모두 보호합니다.

아웃바운드 트래픽 보호를 위해 McAfee Web Gateway는 업계 선두의 McAfee 데이터 유실 방지 기술을 사용해서 HTTP, HTTPS, FTP 등 모든 주요 웹 프로토콜에서 사용자 생성 콘텐츠를 검사합니다. 또한 소셜 네트워킹 사이트, 블로그, 위키 또는 웹 기반 메일, 일정 및 캘린더와 같은 온라인 생산성 도구를 통해 조직으로부터 누출되는 기밀 정보, 민감한 정보 또는 규제 정보의 손실을 방지합니다. 또한 McAfee Web Gateway는 봇에 감염된 시스템을 통해 홈에 연결하거나 중요한 데이터를 전송하는 등 조직에서 데이터를 무단으로 유출하려는 시도를 차단합니다.

McAfee
Together is power.

업계 최고의 보안을 제공하는 McAfee Web Gateway

업계 1위1로 선정된 악성 프로그램 방지 웹 보안 솔루션인 McAfee Web Gateway는 McAfee Gateway Anti-Malware Engine과 함께 시그니처 없는 의도 분석에 특허 출원된 접근 방식을 사용합니다. 사전 예방적 의도 분석 기술은 웹 트래픽에서 이전에 알려지지 않은 또는 제로 데이 악성 콘텐츠를 실시간으로 필터링합니다. McAfee Web Gateway는 웹 페이지의 활성 콘텐츠를 스캔하고, 해당 동작을 에뮬레이션 및 식별하고, 의도를 예측함으로써, 제로 데이 악성 프로그램이 엔드포인트에 도달하는 것을 방지하여, 시스템 정리 및 치료와 관련된 비용을 크게 줄여줍니다.

이러한 분석 기술을 알려진 악성 프로그램 및 악성 사이트를 신속하게 차단할 수 있도록 McAfee 안티바이러스 및 McAfee Labs의 글로벌 평판 기술과 결합하였습니다. McAfee Web Gateway의 여러 기술을 통해 서로 다른 상호보완적 기술을 사용하여 단일 플랫폼의 보안을 최적화하는 동시에 더 뛰어난 보안을 제공할 수 있는데, 이는 많은 조직이 계층형 방어 보안 접근 방식을 위해 구축하고자 하는 기능입니다.

- **실시간 McAfee Global Threat Intelligence(McAfee GTI) 파일 평판이 적용된 McAfee 안티바이러스**: 클라우드 기반 McAfee GTI 파일 평판 조회 기능을 통해 바이러스 발견과 시스템 업데이트/보호 간의 격차를 좁혔습니다.
- **McAfee GTI 웹 평판 및 웹 분류**: McAfee Web Gateway는 평판과 범주 기반 필터링의 강력한 결합을 통해 웹 필터링 기능 및 보안을 제공합니다. McAfee GTI는 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 매우 세분화된 규칙을 적용할 수 있습니다.
- **위치정보**: McAfee Web Gateway에는 위치정보 기능이 포함되어, 웹 트래픽 및 사용자의 원래 지역을 기준으로 지리적 가시성 및 정책 관리를 가능하게 해줍니다.

웹 분류 및 웹 평판을 위해 이제 조직에서는 사내 또는 클라우드 조회 중 하나를 선택하거나 이 두 가지 방법을 결합하여 사용할 수 있습니다. 클라우드 조회는 발견/변경과 시스템 업데이트 간의 보안상 허점을 없앴으며, 수억 개의 고유 악성 프로그램 샘플 데이터를 통해 적용 범위를 넓혔습니다.

지능형 위협 분석 통합

McAfee Web Gateway는 McAfee Advanced Threat Defense와 통합되어 맞춤형 샌드박싱 및 심층적인 정적 코드 분석이 결합된 McAfee의 진화한 악성 프로그램 탐지 기술을 제공합니다. McAfee Advanced Threat Defense와 함께 McAfee Web Gateway의 Gateway Anti-Malware Engine에서 제공되는 인라인 검색 기능은 인터넷 기반 위협에 대해 사용할 수 있는 가장 강력한 보호 솔루션을 제공합니다. 조직에서 비용을 낮추고 지능형 위협 분석 옵션을 간소화하고자 한다면 클라우드 기반 샌드박스인 McAfee Cloud Threat Detection을 여러 추가적인 위협 분석 계층과 통합할 수 있습니다.

위협 인텔리전스 공유

현재 많은 보안 도구는 엔드포인트, 네트워크, SIEM(보안 정보 및 이벤트 관리) 솔루션, 게이트웨이 등에서 핵심 인텔리전스를 사용할 수 있음에도 불구하고 서로 간에 위협 인텔리전스를 공유할 수 없는 사일로 형태로 존재합니다. 이러한 인텔리전스를 공유하여 사용한다면 위협에 대한 보호 수준을 향상시키고, 기존 위반 사항들을 보다 효과적으로 탐지하고, 손상된 시스템을 효율적으로 수정하여 사고 대응 효율을 높일 수 있습니다. McAfee 솔루션(McAfee Web Gateway 포함) McAfee Threat Intelligence Exchange를 통해 은 서로 간에 인텔리전스를 공유함으로써 이러한 격차를 극복합니다. McAfee Web Gateway는 Gateway Anti-Malware Engine에서 발견된 제로 데이 악성 프로그램에 대한 새로운 파일 평판을 작성 및 공유하여 이 프로세스의 가치를 극대화하고 새로운 DAT가 릴리스되기 전에 엔드포인트 장치를 보호할 수 있도록 지원합니다. 또한 McAfee Threat Intelligence Exchange에서 제공되는 확장된 위협 인텔리전스를 통해 McAfee Web Gateway로 더 많은 위협을 차단할 수 있습니다.

암호화된 트래픽 내 통찰력 및 보호
더 정교해진 사이버 범죄자들은 기업의 보안 장벽을 뚫는 백도어로서 SSL 트래픽(HTTPS 및 HTTP/2)으로 눈을 돌렸습니다. 반어적이지만, 보안을 제공하도록 디자인된 프로토콜도 위험 요소가 없는지 확인해야 합니다. McAfee Web Gateway는 악성 프로그램 탐지, SSL 검사 및 인증서 유효성 검사를 모두 통합하여 암호화된 트래픽 검사에 대한 포괄적인 접근 방식을 제공합니다.

McAfee Web Gateway는 이러한 모든 기능을 단일 하드웨어 또는 가상 어플라이언스 아키텍처에서 수행하므로 SSL 검색 하드웨어에 추가로 투자할 필요가 없습니다. McAfee Web Gateway는 모든 SSL 트래픽을 직접 검사하여 암호화된 트랜잭션의 완벽한 보안, 무결성과 개인 정보 보호를 보장합니다.

SSL 트래픽을 더 심층적으로 검사하기 위한 이니셔티브를 실행하려는 조직은 McAfee Web Gateway 내 SSL(Secure Sockets Layer) 탭을 통해 정책에 따라 암호화되지 않은 트래픽 또는 개별 스트림의 전체 스트림을 오프로드할 수 있습니다. 이 소프트웨어 지원 기능을 사용하면 암호 해독된 SSL 트래픽의 전체 또는 부분 미러를 IPS(침입 방지 시스템) 또는 네트워크 기반 DLP(데이터 유실 방지) 솔루션 같은 추가 보안 솔루션으로 전송할 수 있습니다.

데이터 유실 방지
McAfee Web Gateway는 SSL을 비롯한 모든 주요 웹 프로토콜에서 아웃바운드 콘텐츠를 검사함으로써 기밀 정보 유출과 같은 아웃바운드 위협으로부터 조직을 보호합니다. 따라서 지적 재산 손실을 방지하고, 규정 컴플라이언스를 보장 및 문서화하며, 보안 위반 시 포렌직 데이터를 제공하는 데 강력한 도구 역할을 합니다. McAfee Data Loss Prevention(McAfee DLP) 솔루션 집합의 강력한 기능을 이용하는 McAfee Web Gateway는 기본 제공되고 사전 정의된 DLP 사전을 포함하며, 키워드 일치 및/또는 정규 표현식을 통해 사용자 지정 사전을 만들 수 있도록 지원합니다.

클라우드 기반 스토리지를 사용하는 조직들을 위해 내장된 파일 암호화는 파일 공유 및 협업 사이트에 업로드되는 데이터를 무단 액세스로부터 보호합니다. 사용자는 McAfee Web Gateway를 통과하지 않고 데이터를 검색하거나 볼 수 없습니다.

네트워크 외부 사용자를 위한 보호
근무 인력이 더욱 분산되고 그 이동성이 높아지면서, 사무실에서 이동 중인 환경으로 원활하게 전환할 수 있게 하기 위해 웹 필터링 및 보호에 대한 필요성이 점점 중요해지고 있습니다. 조작 방지 클라이언트 에이전트인 McAfee Client Proxy는 로밍 사용자가 원활하게 인증을 수행할 수 있도록 지원하고, 완충 영역(DMZ) 또는 McAfee Web Gateway Cloud Service에 있는 사내 McAfee Web Gateway로 리디렉션할 수 있습니다. 그러면 로밍 중이거나 원격 위치에 있는 사용자가 커피숍, 호텔 또는 기타 Wi-Fi 핫스폿 같은 공용 포털을 통해 인터넷에 액세스하더라도 인터넷 액세스 정책 실시 및 전체 보안 검색을 적용할 수 있습니다.

그뿐만 아니라 McAfee Web Gateway를 통해 기업은 McAfee Web Gateway에 웹 트래픽을 지정하여 모바일 장치에 대해서도 보안 정책을 확장하여 시행할 수 있습니다. McAfee Web Gateway는 모바일 장치 관리 공급자인 AirWatch, MobileIron와의 파트너십을 통해 고급 악성 프로그램 방지 및 기업 웹 필터링 정책으로 Apple iOS 및 Google Android 모바일 장치가 보호되도록 지원합니다.

McAfee Web Gateway로 유연성 확보

McAfee Web Gateway는 정책 유연성 및 제어를 위해 강력한 규칙 기반 엔진을 사용합니다. 정책을 간단하게 만들 수 있도록 McAfee Web Gateway는 일반적인 정책 작업과 관련하여 사전 수립된 광범위한 규칙 라이브러리를 제공합니다. 따라서 조직에서는 다양한 규칙을 선택하고, 해당 규칙을 쉽게 수정하며, 온라인 커뮤니티를 통해 고유한 규칙을 공유할 수 있습니다. 고급 관리를 위한 컨텍스트 기반 규칙 기준 및 공유 목록의 고유한 조합은 문제 해결 및 웹 보안 최적화를 위한 무제한 가능성의 길을 열어줍니다. 규칙 디버깅은 대화형 규칙 추적을 통해 간소화됩니다.

McAfee Web Gateway는 클라우드 응용 프로그램에 대한 제어 기능을 확장하여 웹 응용 프로그램의 사용 방법에 대한 세부적이고 프록시에 기반한 제어를 가능하게 해줍니다. 조직은 수천 가지의 제어 기능을 클라우드 응용프로그램에 적용함으로써 필요에 따라 특정 기능을 사용 또는 사용하지 않도록 설정하고, 웹 응용프로그램 사용자 및 사용 방식을 제어할 수 있습니다. Dropbox에 대한 액세스는 허용하지만 업로드할 수 없도록 설정하길 원하십니까? 문제 없습니다.

유연성 및 제어 기능은 사용자 인증 및 액세스까지 확장됩니다. McAfee Web Gateway는 NT LAN Manager(NTLM), Remote Authentication Dial In User Service(RADIUS), Active Directory(AD)/ Lightweight Directory Access Protocol(LDAP), eDirectory, 쿠키 인증, Kerberos, 로컬 사용자 데이터베이스 등 다양한 인증 방법을 지원합니다. McAfee Web Gateway 인증 엔진을 통해 관리자는 여러 인증 방법의 사용을 비롯한 유연한 규칙을 구현할 수 있습니다. 예를 들어 McAfee Web Gateway는 사용자를 투명하게 인증하고 그 결과를 바탕으로 사용자에게 자격 증명을 입력하도록 메시지를 표시하거나, 다른 인증 방법을 사용하거나, 제한된 정책을 적용하거나, 단순히 액세스를 거부할 수 있습니다.

선택 추가 기능인 McAfee Web Gateway Identity에는 널리 사용되는 수백 개의 클라우드 기반 응용프로그램을 위한 싱글 사인온(SSO) 커넥터가 포함되어 있습니다. McAfee Web Gateway Identity에서는 클릭 한 번으로 인증된 클라우드 응용프로그램에 액세스할 수 있는 SSO 시작 패드를 사용하여 보안을 개선하고 암호와 관련된 헬프 데스크 전화 문의를 줄여주는 기능을 제공합니다. HTTP Power-On Self-Test(POST)와 Security Assertion Markup Language(SAML) 커넥터를 모두 지원하므로 광범위한 응용프로그램에 사용할 수 있습니다. 시스템 관리자는 프로비저닝 커넥터를 사용하여 엄선된 SaaS(서비스형 소프트웨어) 응용프로그램에 대한 사용자 계정을 생성하고 종료할 수 있습니다.

또한 McAfee Web Gateway는 기본 스트리밍 프록시 지원을 통한 스트리밍 콘텐츠까지 액세스 제어 기능을 확장하여 대역폭을 줄이고 지연 시간을 줄일 수 있습니다. 조직이 사용 가능한 대역폭의 사용을 최적화할 수 있도록 추가적인 대역폭 제어를 설정하여 정의된 트래픽 클래스에 대한 최소값, 최대값, 우선 순위 지정을 적용할 수 있습니다.

McAfee Web Gateway가 있는 애자일 인프라 및 성능

McAfee Web Gateway는 고가용성, 가상화 옵션 및 McAfee Web Gateway Cloud Service를 통한 하이브리드 배포 기능을 갖춘 고성능 엔터프라이즈급 프록시이며, 확장 가능한 어플라이언스 모델군으로 제공됩니다. McAfee Web Gateway는 단일 환경에서 수십만 명의 사용자를 지원할 수 있는 확장성과 함께 고객에게 필요한 배포 유연성과 성능을 제공합니다.

배포 옵션을 혼합하여 사용할 수도 있습니다. 예를 들어 모든 웹 트래픽을 네트워크 사용자를 위한 사내 어플라이언스로 라우팅하고, 모든 네트워크 외부 사용자를 클라우드 서비스로 라우팅하여 MPLS(Multiprotocol Label Switching) 회로 또는 VPN(Virtual Private Network)을 통한 트래픽 역전송 비용을 크게 절감할 수 있습니다 하이브리드 구내형 배포 및 클라우드 배포에 대한 자동화된 정책 동기화 및 보고 등을 통해 관리를 간소화하고 일관된 정책 시행을 보장하며 보고, 추적 및 조사를 단순화할 수 있습니다.

McAfee Web Gateway는 명시적 프록시부터 투명 브리지 및 라우터 모드에 이르기까지 다양한 구현 옵션을 제공하여 네트워크 아키텍처에 대한 지원을 보장합니다.

다양한 통합 표준을 지원하는 McAfee Web Gateway는 고객의 고유한 환경에서 제 역할을 하도록 설계되었습니다. McAfee Web Gateway는 WCCP(Web Cache Communication Protocol), WebSocket 프로토콜에서 ICAP/ICAPS(Internet Content Adaptation Protocol) 및 SOCKS(Socket Secure) 프로토콜에 이르기까지, 다른 네트워크 장치 및 보안 어플라이언스와 효율적으로 통신합니다.

또한 McAfee Web Gateway는 IPv6에 대한 지원을 제공하여 대규모 조직 및 정부 기관에서 규정을 준수할 수 있도록 돕습니다. McAfee Web Gateway는 내부 IPv4와 외부 IPv6 네트워크 간의 차이를 메워 트래픽에 사용 가능한 모든 보안 및 인프라 기능을 적용합니다.

미래를 위한 통합 플랫폼

McAfee Web Gateway는 여러 독립형 제품이 있어야 제공할 수 있는 다양한 보호 기능을 통합하여 제공합니다. URL 필터링, 안티바이러스, 제로 데이 안티맬웨어, SSL(Secure Sockets Layer) 검색, 데이터 유실 방지 및 중앙 관리 등 모든 것이 하나의 어플라이언스 소프트웨어 아키텍처에 통합되어 있습니다. 배포 관리가 모든 폼 팩터에 통합되어 있기 때문에 하나의 정책을 사내 어플라이언스, 어플라이언스 클러스터, 가상 어플라이언스 및 클라우드 서비스까지 단일 관리 콘솔로 확장할 수 있습니다.

보안 위험 관리 및 보고 기능

가장 널리 사용되고 인정받은 보안 관리 기술인 McAfee ePolicy Orchestrator®(McAfee ePO™) 소프트웨어가 McAfee Web Gateway에서 모든 보안 보고를 위한 단일 소스로 지원됩니다.

McAfee ePO 소프트웨어는 McAfee Content Security Reporter 확장 기능을 통해 상세한 웹 보안 보고 기능을 제공합니다. McAfee Content Security Reporter는 조직에서의 웹 사용 현황 이해, 규정 준수, 동향 파악, 문제 격리, 웹 보안 정책 실시를 위한 필터링 설정 맞춤 구성에 필요한 정보와 포렌직 도구를 제공합니다. McAfee Content Security Reporter는 기존의 McAfee ePO 서버에서 리소스 집약적인 데이터 처리 및 저장소를 오프로드하는 외부의 독립형 보고 서버를 제공함으로써 확장을 통해 가장 큰 글로벌 조직의 보고 요구 사항도 충족할 수 있습니다.

또한 McAfee Web Gateway는 McAfee 데이터 유실 방지의 무료 서비스인 McAfee Cloud Visibility—Community Edition, 암호화 및 McAfee 웹 보안 고객과 통합되어 클라우드 응용프로그램 사용 현황 및 위험에 대한 가시성을 제공합니다. 직원이 클라우드 응용프로그램을 사용하더라도 IT 팀에서는 그중 일부만 파악하므로 가시성 부재로 인한 위험이 높아집니다. 모든 클라우드 응용프로그램 액세스, 위험 수준 및 데이터 분류를 보여주는 간단한 대시보드는 이러한 부담을 덜어줍니다. 따라서 보안 전문가는 클라우드 액세스 제어와 함께 클라우드로 이동하는 데이터를 실질적으로 보호하는 데 시간과 노력을 집중하여 조직의 위험을 최소화할 수 있습니다.

또한, McAfee Cloud Visibility—Community Edition은 클라우드의 데이터를 보호하기 위한 다음 단계인 McAfee Cloud Data Protection과 함께 무료 서비스로 포함됩니다.

사용권

McAfee는 궁극적인 배포 유연성을 갖추고 투자에 대한 미래 경쟁력을 확보할 수 있도록 McAfee Web Gateway 및 McAfee Web Gateway Cloud Service의 모든 기능을 단일 솔루션으로 제공합니다. **McAfee Web Protection**. 유연성과 고가용성을 향상하기 위해 사내 또는 클라우드에서 배포할지 아니면 두 가지 방법을 같이 사용할지 선택할 수 있습니다. 이러한 옵션을 갖춘 수상 경력이 있는 McAfee 악성 프로그램 방지 및 포괄적인 웹 필터링을 구매할 수 있습니다.

McAfee Web Gateway 하드웨어는 별도로 판매됩니다.

McAfee™
Together is power.

1. AV-TEST에서 시행한 테스트에서 McAfee Web Gateway가 제로 데이 악성 프로그램을 94.5%, 악성 Windows 32 이식 가능(PE) 파일을 99.8%, 비 PE 파일을 98.63% 탐지하는 것으로 밝혀졌습니다. "**McAfee Web Gateway Security Appliance Test**"(McAfee Web Gateway 보안 어플라이언스 테스트), AV-TEST GmbH.

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

2017년 6월