McAfee Web Gateway Cloud Service

공통적인 보호를 지원하는 클라우드 제공 웹 보안

주요 이점

- 웹 보안을 배포하기 위한 가장 경제적인 방식 - 사내 하드웨어 또는 소프트웨어가 필요하지 않습니다.
- 기본 보호를 넘어서는 기능 - 동작 에뮬레이션으로 트래픽이 처리될 때 밀리초 단위로 제로 데이 악성 프로그램을 차단할 수 있습니다.
- 네트워크에 연결되어 있지 않은 사용자에까지 보호 범위를 확대합니다. 클라우드 제공은 기존의 네트워크 경계를 없앱니다.
- McAfee® ePolicy Orchestrator®(McAfee ePO™) Cloud 플랫폼을 모든 Intel Security 클라우드 서비스를 위한 통합된 관리 콘솔로 사용하여 탁월한 관리 효율성을 제공합니다.
- 검증된 아키텍처: McAfee® Web Gateway Cloud Service는 전 세계 기업에 사용되는 신뢰할 수 있는 사내 어플라이언스인 McAfee Web Gateway의 멀티테넌트 버전으로 구축되었습니다.

웹의 정교한 위협으로부터 방어하기 위해서는 고급 기술이 요구되지만, 반드시 복잡하고 비용이 많이 드는 것은 아닙니다. 클라우드에서 웹 보안을 제공할 경우 보안 팀은 사내 어플라이언스로 지능적인 위협 방지의 이점을 동일하게 누릴 수 있지만 그러한 기능을 유지 관리하는 데 사용되는 하드웨어 또는 리소스 관련 비용이 소요되지 않습니다. 네트워크 경계 바깥에서 발생하는 웹 액세스가 증가함에 따라 클라우드는 로밍하는 장치 및 사용자를 위한 일관된 접촉 지점이 되고 있습니다. 단일 위치로 이동하는 트래픽에 대한 보안을 구축하는 대신 엔드포인트에서 보안을 구축하는 것이 더 효과적입니다. 엔드포인트를 비롯한 전체 위치를 클라우드에 연결하면 네트워크 경계를 넘어 확장된 새로운 경계를 벗어나지 않는 공통적인 보호가 제공됩니다.

비용 효과적이고 공통적인 보호

사내 웹 보안 어플라이언스를 관리하려면 비용이 많이 소요되며, 이미 할 일이 많이 있는 보안 팀에 부담을 가중시킬 수 있습니다. 웹 보안을 클라우드 서비스로 배포하면 총 소유비용을 낮출 수 있습니다. 더 이상 하드웨어 어플라이언스를 구매, 소유 및 유지 관리할 필요가 없습니다. 이전에 어플라이언스를 유지 관리하고, 소프트웨어 업그레이드 및 패치와 같은 작업을 수행하는 데 사용되었던 리소스를 모두 IT 또는 IT 보안 조직 내에서 보다 전략적인 이니셔티브에 재할당할 수 있습니다.

어플라이언스와 클라우드 서비스를 모두 하이브리드 배포에서 사용할 수 있습니다. 대부분의 조직은 이 모델을 선택하여 네트워크에 있는 어플라이언스의 소유권 및 제어권을 유지하고 클라우드 제공 보호를 소규모 원격 사무소 및 로밍 사용자에까지 확대합니다.

원격 사무소에서 MPLS(Multiprotocol Label Switching) 회로를 통해 웹 트래픽을 백홀링하여 네트워크의 웹 게이트웨이 어플라이언스로 필터링하는 IT 팀은 클라우드 제공 웹 보안을 통해 즉각적으로 이점을 누릴 수 있습니다. 트래픽 백홀링은 비용이 많이 소요되며 네트워크에 복잡성을 가중시킵니다. 대신, 원격 사무소는 보호를 위해 클라우드로 직접 라우팅하여 MPLS 회로를 없애고 네트워크 아키텍처를 간소화할 수 있습니다.

마지막으로 웹에 대한 직원 액세스는 더 이상 네트워크 경계로 제한되지 않으며 네트워크에 연결되어 있지 않은 사용자 및 장치를 보호되지 않는 상태로 유지하고 IT에 보이지 않게 할 수 있습니다. 웹 보안을 클라우드로 전환하면 이러한 경계가 반전됩니다. 집, 공항, 커피숍 또는 기타 네트워크에 연결되어 있지 않은 위치에서 작업하는 경우 네트워크에 연결되어 있지 않은 사용자 및 장치의 웹 트래픽이 자동으로 엔드포인트에서 클라우드로 라우팅되어 보안 연결을 유지할 수 있습니다. 더 이상 네트워크에서 물리적 경계 내의 트래픽에 집중하지 않아도 됩니다. 대신 엔드포인트가 이동하는 모든 위치로 범위가 확장됩니다.

intel Security

글로벌 고성능 아키텍처

McAfee Web Gateway Cloud Service는 엔터프라이즈용으로 설계되었으므로 많은 조직들은 현재 사내에서 경험하는 것보다 높은 수준의 성능을 얻을 수 있습니다. 예를 들어 사내에서 용량을 증설해야 하는 경우 IT 부서는 새 어플라이언스를 구입하여 배포해야 하는데 이를 위해서는 며칠 내지 몇 주가 걸릴 수 있습니다. McAfee 클라우드에서는 서비스에 내장된 탄력적인 클라우드 설계 덕분에 불과 15분 정도면 용량을 증설할 수 있습니다.

사내 어플라이언스에 장애가 발생하여 복구해야 하는 경우 인터넷을 중단해야 하며, 웹에 대한 페일오픈이 허용되는 경우 보안 상황에 피해를 줄 수 있습니다. 데이터 센터 위치 중 한 곳에서 장애가 발생하는 경우 클라우드 서비스는 모든 웹 트래픽을 자동으로 가장 가깝고 빠른 데이터 센터 위치로 재라우팅하여 즉각적인 연속성이 보장됩니다.

또한 McAfee 클라우드 서비스 아키텍처는 세계 최대의 IXP(Internet Exchange Point)에서 인터넷 백본과 "피어"를 이루도록 구축되었습니다. 따라서 연결 대기 시간을 증가시키는 중간 ISP(인터넷 서비스 공급자)의 라우팅 홉이 없어집니다. Microsoft Office 365 및 Google 과 같은 인기 있는 콘텐츠 공급자에 대한 홉이 감소함에 따라 사용자는 개방된 인터넷에 직접 연결하는 경우보다 더 빠르게 클라우드 서비스를 통해 연결할 수 있습니다.

McAfee Web Gateway Cloud Service는 글로벌 서비스입니다. 웹 트래픽이 처리되는 데이터 센터의 현재 위치 및 상태를 보려면 **https://trust.mcafee.com**을 참조하십시오. 웹 콘텐츠를 지역별 언어로 제공할 수 있으므로 사용자는 연결되는 위치에 관계없이 로컬 Google 검색 결과 등을 볼 수 있습니다.

정교한 위협에 대한 방어

보안 팀은 종종 기존의 방어를 우회하는 정교한 악성 프로그램 및 표적 공격에 대처하지 못하는 경우가 있습니다. 이로 인해 리소스 유출이 발생하며 엔드포인트 교정을 통해 끊임없는 "사후 대처" 방식으로 문제를 해결하는 데 급급하게 됩니다. 기존의 URL 필터링 및 웹 위협 차단을 위한 시그니처 기반 접근법과 달리, McAfee Web Gateway Cloud Service는 파일, JavaScript 및 HTML의 인라인 에뮬레이션을 통해 제로 데이 및 파일리스(fileless) 악성 프로그램으로부터 엔드포인트를 보호합니다. 이를 통해 제로 데이 악성 프로그램이 사용자에게 도달하기 전에 미리 차단하고 URL 필터링 및 시그니처 기반 솔루션에 비해 차단율을 약 20% 향상시킬 수 있습니다. 보안 운영 팀은 전체 악성 프로그램 인시던트의 수를 줄이는 방식으로 비용을 절약하고 리소스 유연성을 높일 수 있는 이점을 얻을 수 있습니다.

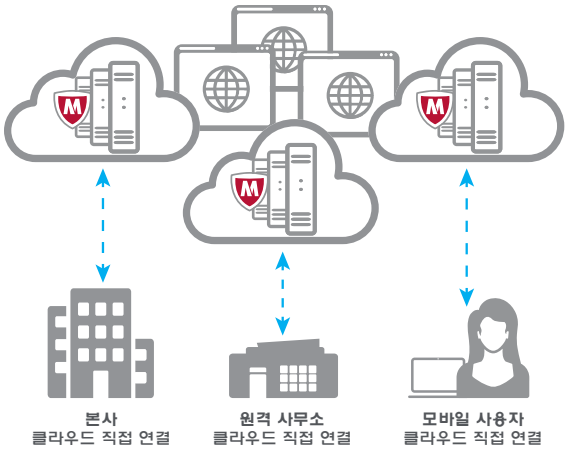

그림 1. McAfee Web Gateway Cloud Service 배포.

웹 위협은 웹 보안 방어를 피해 숨기 위해 암호화된 트래픽을 통해 전달되는 경우가 종종 있습니다. 클라우드 저장소 또는 소셜 미디어 같은 거의 모든 클라우드 응용프로그램에서 기본적으로 암호화된 트래픽을 사용합니다. McAfee Web Gateway Cloud Service는 HTTPS 암호화된 트래픽을 완벽히 암호 해독하고 검사하여 악성 프로그램을 차단하고 암호화된 채널에 대한 클라우드 응용프로그램의 가시성을 보장할 수 있습니다.

대부분의 IT 팀에서 클라우드 응용프로그램의 확산을 제어하는 것은 까다로운 과제입니다. 사용자가 선택한 서비스로 인해 발생하는 위험 및 "그림자 IT" 의 경우 특히 더 그렇습니다. HTTPS 를 비롯한 모든 웹 트래픽에 대한 완벽한 가시성을 제공하는 미리 구성된 보고서에서는 위험 평가를 위해 액세스되는 웹 사이트, 사용 중인 클라우드 응용프로그램 및 해당 데이터 포인트를 보여줄 수 있습니다. 실제로 사용 중인 IT와 허용되지 않은 IT를 비교하면 그림자 IT는 쉽게 드러날 수 있습니다. 클라우드 응용프로그램, 특히 클라우드 저장소도 악성 프로그램의 전달 메커니즘으로 사용이 확대되고 있습니다. 악성 프로그램을 전달하는 응용프로그램을 식별하면 정책 결정 사항을 알리는 데 도움이 될 수 있습니다. 클라우드 서비스가 액세스되는 전체 범위에서 업로드, 메시징 방지 또는 전면적인 응용프로그램 차단 등 1,600개 이상의 클라우드 응용프로그램 제어 기능을 구현하여 위험을 최소화할 수 있습니다.

McAfee Web Gateway Cloud Service는 어디에 있습니까?

라이브 업데이트와 데이터 센터 위치, 가용성 상태 등에 대한 정보를 확인하려면 **https://trust.mcafee.com**을 참조하십시오.

효율적인 보안 관리

여러 콘솔 및 정책을 통해 보안을 관리하는 것은 부담이 많이 되는 작업으로, 특히 사내 및 클라우드 기반 웹 보안을 개별적으로 관리하는 경우 더욱 그러합니다. 하이브리드 환경에는 사내 배포와 클라우드 배포 모두를 위한 하나의 관리 콘솔, 단일 정책 집합 및 하나의 보고 인터페이스가 있습니다.

사내 하드웨어 또는 소프트웨어 없이 단독으로 배포하는 McAfee Web Gateway Cloud Service는 엔드포인트 보안과 함께 Intel Security의 모든 클라우드 기반 보안 서비스를 위한 통합된 관리 콘솔인 McAfee ePO Cloud에 의해 관리되므로 보안 관리 측면에서 탁월한 효율성을 제공합니다.

엔드포인트 장치를 위한 웹 보안, 특히 라우팅 및 인증을 배포하는 것은 까다로운 과제입니다. 선택적 엔드포인트 클라이언트인 McAfee Client Proxy는 클라우드 서비스에 대한 라우팅 및 인증을 자동화하여 일관된 정책 실시로 클라우드에 대한 광범위한 연결을 보장합니다. McAfee Client Proxy는 사내 어플라이언스가 있는 하이브리드 배포에서 원활히 작동하여 네트워크에 연결되어 있는 경우 지능적으로 어플라이언스로 라우팅하고, 네트워크에 연결되어 있지 않은 경우 클라우드 서비스로 라우팅합니다. 조직별 요구 사항에 따라 추가적인 라우팅 및 인증 옵션을 사용할 수 있습니다.

자세한 내용

자세한 내용은 **www.mcafee.com/kr/products/web-protection.aspx**을 참조하십시오.

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