Akamai

구매자 가이드:

클라우드 기반의 보안 웹 게이트웨이를 선택하는 방법

원격 근무 직원을 보호하고 기업 보안 간소화하기

목차

최신 기업 보안: 데이터센터 백홀에 대한 재고

클라우드 컴퓨팅, SaaS(Software as a Service), 모빌리티, 최신 네트워크 아키텍처는 비즈니스 방식을 혁신했습니다. 하지만 이러한 신기술의 가치를 제한하지 않으면서 인력을 보호하고자 하는 IT 팀은 막대한 타격을 입었습니다. 이제 새로운 과제가 주어졌습니다. 2020년 많은 기업들은 원격 근무 직원의 급격한 증가에 대응하기 위해 디지털 전환 단계에 상관 없이 빠르게 움직여야 했습니다.

보안 웹 게이트웨이는 기업의 인력을 보호하는 중요한 구성 요소입니다. 하지만 많은 기업들은 여전히 자사 데이터 센터에 배치된 물리적 어플라이언스를 사용하고 있습니다. 이런 하드웨어는 지속적인 유지 관리, 업그레이드가 필요하고 복잡한 트래픽 백홀을 사용해 웹 트래픽을 검사 및 제어하기 때문에 결국 성능 저하로 이어집니다.

분산된 기업 환경이라는 새로운 현실에 대응하려면 효율적인 최신 접근 방식이 필요합니다. 이에 대한 해결 방안은 하드웨어 어플라이언스 사용을 멈추고 보안 웹 게이트웨이 기능을 클라우드로 이동시키는 것입니다.

이 구매자 가이드는 클라우드 기반의 보안 웹 게이트웨이의 장점과 최신 웹 게이트웨이 기술에서 확인해야 할 기능에 대해 설명합니다.

원격 근무의 증가로 발생한 새로운 IT 및 보안 요구사항

지난 10년 동안 기업의 원격 근무 인력은 꾸준히 증가해 왔습니다. 이런 추세는 코로나19의 여파로 더욱 가속화되었고 코로나 이후에도 지속될 것으로 예상됩니다. Gartner는 설문 조사에 참여한 CFO 중 74%가 팬데믹 이후에 이전 현장 근무 인력의 5% 이상을 영구적으로 원격 근무로 전환할 것이라고 답변했습니다.[1]

동시에 피싱, 랜섬웨어, 멀웨어 등 정교한 표적형 공격이 급증했습니다. 최근 설문 조사에 따르면 응답자의 53%가 코로나19 펜데믹이 시작된 이후 피싱 활동이 증가하고 있다고 답했습니다.[2] 최근 미국 재무부는 사람들의 지속적인 비즈니스 활동의 기반이 되는 온라인 시스템을 사이버공격자들이 표적으로 삼기 때문에 코로나19 팬데믹 중에 랜섬웨어 결제에 대한 수요가 증가했다고 경고했습니다.[3]

기업들은 전통적으로 데이터 센터에 보안 웹 게이트웨이와 같은 보안 어플라이언스를 설치해 본사와 지사에 근무하는 사용자 및 원격 근무 직원들의 인터넷 접속을 보호했습니다. 그런 다음 모든 웹 트래픽을 중앙으로 백홀시켜 검사하고 제어했습니다.

이러한 보안 웹 게이트웨이를 사용해 사용자가 시작한 웹 트래픽에서 원치 않는 멀웨어를 필터링하고, 사용자가 악성 웹 사이트에 접속하지 못하도록 차단하고, 기업의 규제 정책을 실행했습니다.

이런 게이트웨이 솔루션은 원래 대부분의 직원들이 책상에서 기업이 관리하는 디바이스를 사용하는 환경에 맞게 설계되고 배치되었습니다. 그러나 원격 근무 및 지사 근무를 하는 사용자가 증가하고 SaaS 애플리케이션에 접속하기 위해 퍼블릭 인터넷으로 이동하는 트래픽이 증가함에 따라 기업은 만족스러운 성능을 유지하기 위해 중앙 데이터 센터에 여러 개의 중복 보안 웹 게이트웨이를 설치하기 시작했습니다. 이러한 하드웨어를 구입 및 관리하는 일은 점점 더 복잡해지고, 비용과 시간이 많이 소요됩니다.

> **"데이터 센터에 지출되는 IT 예산의 비율은 지난 몇 년간 감소했으며 현재는 전체 예산의 17%에 불과합니다."**
>
> — Gartner, 2019 IT 핵심 지표 데이터

또는 기업은 모든 원격 사용자의 트래픽을 백홀하면서 보안 웹 게이트웨이 어플라이언스를 지사에 추가했습니다. 이러한 중복성으로 인해 어플라이언스가 증가하고 이와 관련된 비용 뿐만 아니라 노동 집약적인 배치 및 관리도 증가했습니다.

또한 여러 장소에서 일관된 보안 정책을 유지하는 것이 점점 어려워지고 있습니다. 어플라이언스의 확대를 줄이기 위해 가상화된 어플라이언스를 구축한다 해도 하드웨어를 추가적으로 배포하고 관리해야 합니다.

세 번째 접근 방식은 하이브리드 배치입니다. 기업의 본사에서는 온프레미스 보안 웹 게이트웨이를 계속 사용하고 지사의 웹 트래픽은 클라우드 기반 보안 웹 게이트웨이로 전송하면서 원격 근무 직원의 트래픽을 다시 백홀하는 것입니다. 이 접근 방식은 온프레미스 장비에 대한 기존 하드웨어 투자를 보존합니다. 그러나 서로 다른 시스템을 관리해야 하기 때문에 복잡성이 가중됩니다. 장비를 추가적으로 구매해 관리하는 방식이 순수 클라우드 접근 방식보다 훨씬 더 많은 비용이 소요될 뿐만 아니라 로컬 및 클라우드 기반 시스템 전반에 걸쳐 일관된 정책을 유지하는 것도 어려웠습니다.

> **Gartner는 2025년까지 80%의 기업이 기존 데이터 센터를 폐쇄할 것으로 전망합니다.[4]**

설상가상으로 기업이 채택하는 솔루션의 복잡성은 증가하지만 사이버 보안 인력은 부족해지기 시작했습니다. (ISC)[2]의 연구에 의하면 현재 미국에서 필요한 보안 인력의 수요를 채우기 위해서는 공급이 62% 증가해야 하는 것으로 나타났습니다.[5]

클라우드 기반의 보안 웹 게이트웨이가 필요한 이유

기업은 자사의 클라우드 전략에 맞춰 웹 보안에 대한 최신 접근 방식을 채택하고 원격 근무를 지원해야 합니다. 클라우드 기반 보안 웹 게이트웨이는 높은 수준의 보안을 제공합니다. 동시에 인터넷에 직접 연결되기 때문에 여러 개의 어플라이언스와 백홀이 필요하지 않습니다.

클라우드 기반의 보안 웹 게이트웨이를 사용하는 기업은 다음과 같은 장점을 얻을 수 있습니다.

보안의 복잡성 감소: 클라우드 기반의 보안 웹 게이트웨이를 사용하면 하드웨어 또는 가상 어플라이언스를 배치할 필요가 없고 3년마다 하드웨어를 설정·관리·교체·업그레이드하지 않아도 됩니다.

성능 병목 현상의 최소화: 인터넷 기반 보안 웹 게이트웨이를 사용하면 웹 트래픽 부하 증가 및 암호화된 트래픽 증가에 대응하기 위해 어플라이언스를 추가할 필요가 없습니다. 고객은 성능에 미치는 영향을 최소화하면서 필요에 따라 서비스를 간단하게 추가할 수 있습니다.

트래픽의 백홀 및 헤어핀 비용 절감: 클라우드 기반 보안 웹 게이트웨이는 트래픽을 백홀하지 않고 웹 트래픽에 보안을 적용하여 인터넷에 직접 연결할 수 있으므로 멀티프로토콜 라벨 스위칭 네트워킹 비용이 절감됩니다.

보안팀의 효율성 개선: 클라우드 보안 웹 게이트웨이를 사용하면 하드웨어나 소프트웨어를 지속해서 유지 관리할 필요가 없기 때문에 부족한 보안 인력들이 다른 보안 조치에 선제적으로 더 많은 시간을 할애할 수 있습니다.

보안 정책의 일관성: 디바이스에 상관 없이 모든 사용자를 대상으로 중앙에서 관리하고 전 세계적으로 배포되는 정책을 적용할 수 있습니다. 기업의 정책이 지역마다 다르더라도 동일한 UI를 사용해 모든 지역을 관리할 수 있습니다.

보안 웹 게이트웨이의 핵심 요구사항

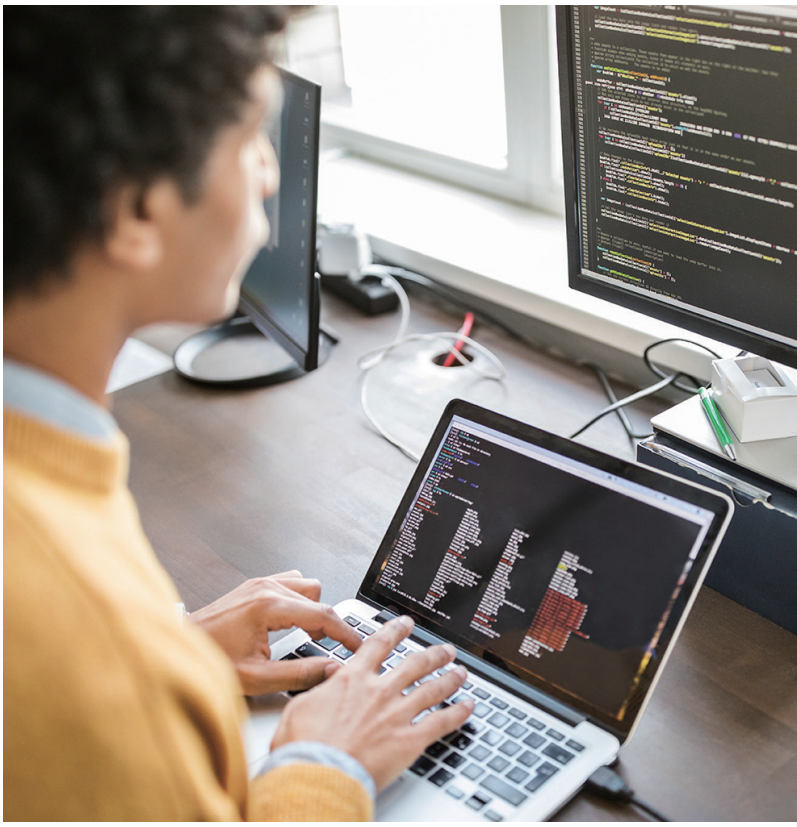
클라우드 기반 보안 웹 게이트웨이를 선택할 때는 보안이 핵심 요구 사항임을 반드시 인식해야 합니다. 기존 보안 웹 게이트웨이에는 지금은 사라진 문제를 해결하는 기능이 포함된 경우가 많습니다. 예를 들어 대역폭이 비쌀 때 사용하도록 고안된 대역폭 제어가 포함되어 있습니다. 또는 직원들이 근무 시간에 YouTube나 Facebook을 사용하지 못하도록 차단하는 기능도 있습니다. 이런 기능은 더이상 필요하지 않습니다. 지금은 대역폭이 충분하고 많은 사람들이 모바일 디바이스를 사용하기 때문에 기업들은 이제 이런 서비스를 회사 디바이스에서 차단하려고 하지 않습니다.

오늘날 기업이 필요로 하는 것은 최신 보안 문제를 처리하도록 특별히 설계된 클라우드 기반 보안 웹 게이트웨이입니다. 특히 여러 보안 조치를 통해 가장 높은 수준의 보안을 제공하는 심층적인 방어 전략을 갖춘 솔루션이 필요합니다. 이러한 접근 방식은 사이버 보안의 모든 관점에 적용되어야 하며 이중화된 보안 조치를 제공해야 합니다. 이렇게 하면 하나의 방어선이 감염되었을 때 공격이 틈새로 스며드는 것을 막기 위해 추가적인 방어 레이어가 배치됩니다. 이러한 계층화된 접근 방식을 사용하면 사용자의 디바이스가 감염되기 전에 멀웨어, 랜섬웨어, 피싱과 같은 위협을 더 빠르게 차단할 수 있습니다.

심층 방어 전략을 배치하는 보안 웹 게이트웨이는 다음과 같은 보안 기능을 제공해야 합니다.

모든 DNS 요청 및 URL 요청에 대한 평가

클라우드 기반 보안 웹 게이트웨이 솔루션은 모든 URL 및 DNS 요청을 실시간 위협 인텔리전스와



비교하여 평가하고, 킬 체인에서 악성 요청을 조기에 차단해야 합니다. 보안 웹 게이트웨이가 아웃바운드 연결을 설정하기 전에 위협을 차단할 수 있다면 웹 리소스는 반환된 콘텐츠를 열거나 검사할 필요가 없습니다. 이러한 효율성으로 인해 계산 집약적인 프로세스를 막을 수 있고 페이로드 단계에서 보안 웹 게이트웨이가 반드시 분석해야 하는 트래픽 양이 줄어듭니다. 결과적으로 전반적인 보안 웹 게이트웨이 성능이 향상됩니다.

위협 인텔리전스는 멀웨어, 랜섬웨어, 피싱, 처리량이 낮은 DNS 기반의 데이터 유출을 차단해야 합니다. 또한 현재와 관련성이 있고 오탐률이 낮은 보안을 제공한다는 목적에 부합해야 합니다.

다양한 페이로드 분석 기술

모든 위협이 각각 다르기 때문에 하나의 탐지 기술이나 접근 방식으로 모든 종류의 멀웨어를 방어할 수 없습니다. 따라서 보안 웹 게이트웨이 솔루션에는 여러 멀웨어 분석 엔진이 포함되어야 합니다. 이러한 엔진은 시그니처와 시그니처리스, 머신러닝과 샌드박스 등의 다양한 식별 기술을 사용하여 인라인 또는 오프라인에서 HTTP 및 HTTPS 페이로드를 스캔해야 합니다. 이런 분석을 통해 실행 파일 및 문서 파일 등의 악성 파일에 대한 포괄적인 제로데이 방어 기능을 제공합니다.

제로데이 피싱 탐지

코로나19가 시작된 후 원격 근무 직원들에 대한 피싱 공격이 증가하고 있습니다. 공격자들은 이메일, 소셜 미디어, 인스턴트 메시징 애플리케이션 뿐만 아니라 온라인 파일 공유 및 협업 채널을 통해 피싱 공격을 일으키고 기업 네트워크에 진입할 수 있는 기업 인증정보를 빼냅니다. 그런 다음 측면으로 이동해 데이터 및 지적 재산을 찾아 유출시키거나 랜섬웨어 캠페인을 공표합니다.

피싱 페이지에 대한 접속을 식별 및 차단하기 위해 대부분의 보안 벤더들은 다음과 같은 활동을 진행합니다.

1. 도메인에 대한 비정상적인 트래픽을 관찰합니다.

2. 해당 도메인을 분석합니다.

3. 피싱 도메인인지 확인합니다.

4. 차단 목록에 추가합니다.

5. 고객에게 업데이트된 차단 목록을 푸시합니다.

이 프로세스는 몇 시간이 소요될 수 있습니다. 게다가 오늘날의 사이버 범죄자들은 피싱 키트를 사용하여 단기 공격을 쉽게 생성·실행하기 때문에 이를 탐지하는 일은 이전보다 어려워졌습니다. 피싱 도메인 또는 피싱 URL이 발견되면 공격이 끝납니다. 실제로 피싱 공격이 정교하고 명확할수록 지속 시간이 더 짧습니다.

그러나 이러한 캠페인이 신속히 끝난다 해도 최신 제로데이 피싱 탐지 엔진은 이러한 캠페인을 식별하고 차단할 수 있습니다. 이러한 키트 기반 공격의 반복적인 구성 요소는 피싱 코드 페이지에서 확인할 수 있습니다. 이 정보를 사용하여 정확한 식별이 가능한 페이지에 대한 '핑거프린트'를 탐지할 수 있습니다.

보안 웹 게이트웨이 솔루션에는 요청된 웹 페이지를 분석하고 이를 이전에 본 피싱 페이지의 '핑거프린트'와 비교할 수 있는 제로데이 피싱 탐지 엔진이 포함되어야 합니다.

암호화된 트래픽 검사

인터넷은 본질적으로 데이터를 전송하기에 안전하지 않습니다. 따라서 공격자가 도청하거나 위조하거나 트래픽 변조하는 것을 방지하기 위해 항상 웹 트래픽 암호화합니다. TLS(Transport Layer Security)는 보안 웹 브라우징을 제공하기 위한 사실상의 암호화 표준입니다. TLS는 클라이언트 브라우저와 웹 서버와 같은 두 개의 엔드포인트 사이에 보안 터널을 만듭니다.

> **인터넷 상에서 암호화된 웹 트래픽의 비율은 2014년 약 50%에서 현재 80~90%로 꾸준히 증가해 왔습니다. 전 세계 상위 사이트 100곳 중 대부분(96%)의 기본 설정이 HTTPS로 되어 있습니다.**
>
> — 2020년 Google 투명성 보고서

하지만 모든 HTTPS 트래픽이 정상은 아닙니다. 또한 공격자와 멀웨어 작성자는 암호화를 사용하여 자신의 활동을 숨기고, 사용자가 랜섬웨어를 통해 파일에 접속하는 것을 방지하며, 악의적인 네트워크 통신을 보호합니다. 최근 연구에 의하면 인터넷에 접속한 멀웨어의 1/4가량이 통신할 때 TLS를 사용하는 것으로 나타났습니다.[6]

HTTPS 웹 트래픽을 선제적으로 검사·제어하려면 반드시 프록시 서버(신뢰할 수 있는 중개자)를 사용하여 보안 터널의 내부를 살펴보고 암호화된 트래픽을 검사해야 합니다. 프록시 서버는 HTTPS 트래픽을 일반 텍스트로 해독·분석하고 트래픽을 재암호화한 다음 MITM(Machine in the Middle)이라는 기술로 다른 보안 연결을 생성해야 합니다. MITM은 요청된 URL이 정상인지 악성인지 여부를 검사하고, TLS 암호화 트래픽에 대한 가시성을 제공하며, 기업이 위협을 받지 않도록 보호하면서 오리진 웹 사이트에 대한 트래픽의 기밀성 및 무결성을 유지합니다.

MITM 검사를 진행하려면 상당한 처리 역량이 필요합니다. 따라서 지연 시간 때문에 웹 검색 속도가 느려질 수 있습니다. 보안 웹 게이트웨이는 애플리케이션 성능을 개선하는 서비스를 제공해야 합니다. 또한 전 세계적으로 분산된 서버와 인텔리전트 소프트웨어가 사용자 및 데이터센터와 가까운 곳에 위치해야 하고 애플리케이션 성능 및 가용성을 개선시키는 웹 최적화를 지원해야 합니다.

또한 MITM은 클라우드 보안 웹 게이트웨이 벤더가 제대로 작동하지 않으며 우회되어야 하는 도메인 및 URL 목록을 한 곳에서 관리하는지 확인해야 합니다. 또한, 클라우드 보안 웹 게이트웨이는 금융 서비스 및 의료와 같은 민감한 특정 유형의 웹 콘텐츠에 대한 MITM 검사를 우회할 수 있어야 합니다.

통합 데이터 유출 차단

PII(Personally Identifiable Information)와 기타 기밀 비즈니스 데이터의 손실을 사전에 차단하는 일은 금전적 손실이나 평판 저해의 가능성을 고려할 때 매우 중요합니다. 클라우드 보안 웹 게이트웨이는 설정이 간편하고 빠르게 배포할 수 있는 통합 데이터 손실 차단 기능을 갖추어야 합니다. 자주 업데이트되는 데이터베이스에는 PII, PCI DSS, HIPAA와 같은 데이터 개인정보 보호 규정이 포함되어야 하며, 기업은 맞춤형 데이터베이스를 쉽게 만들 수 있어야 합니다.

섀도우 IT 식별 및 관리

사용자는 매니지드 디바이스에 수십만 개의 애플리케이션을 간편하게 다운로드, 설치, 사용하는데 기업 보안팀은 이를 인지하지 못할 수 있습니다. 그러나 허가되지 않은 애플리케이션을 사용하면 기업의 공격면이 크게 확대되고 리스크 프로필이 높아질 수 있습니다.

> **기업은 평균적으로 1,295여 개의 앱과 클라우드 서비스를 사용합니다. 이들 중 95% 이상이 관리되지 않으며 IT 관리 권한도 없습니다.**
>
> — Cybersecurity Insiders
> 2019년 클라우드 보안 보고서

클라우드 보안 웹 게이트웨이는 사용 중인 애플리케이션을 식별하고, 특정 애플리케이션을 설치한 사용자의 수를 파악하며, 심각한 보안 리스크를 초래할 수 있는 애플리케이션을 표시할 수 있어야 합니다. 확인 후에는 전체 애플리케이션 또는 특정 애플리케이션의 작업을 차단할 수 있어야 합니다. 예를 들어, 업로드는 허용하지만 다운로드는 허용하지 않을 수 있습니다.

위치에 상관없이 모든 디바이스 보호

지난 10년간 근무 방식은 상당히 유연해졌습니다. 사용자들은 장소에 상관 없이 모든 디바이스에서 업무를 할 수 있습니다. 또한 글로벌 팬데믹으로 인해 재택근무를 하게 되면서 기업용 사용자 컴퓨팅의 59%가 모바일 디바이스로 이동하면서 PC와 노트북을 확장하거나 대체하고 있습니다. 이러한 변화는 직원들이 사무실로 복귀한 후에도 계속될 것으로 예상됩니다.[7]

모바일 디바이스로 이동하고 와이파이 네트워크 사용이 증가하면서 모든 기업의 보안 체계에 틈새가 생길 수 있습니다. 기업은 디바이스 성능에 영향을 주지 않으면서도 동일하고 보편적인 수준의 보안을 적용할 수 있어야 합니다.

클라우드 보안 웹 게이트웨이는 사용자가 사용하는 네트워크 전반에 걸쳐 모든 디바이스(iOS, Android OS, Chrome OS)에 대한 제로데이 공격, 피싱, 멀웨어와 랜섬웨어 같은 위협을 선제적으로 탐지, 차단, 완화해야 합니다. 또한, 최적의 디바이스 성능을 유지하면서 전 세계적으로 모든 곳에서 제어와 효율적인 관리 기능을 제공해야 합니다.

모든 기업 애플리케이션에 대한 보안 접속

클라우드 보안 웹 게이트웨이는 사용자와 디바이스가 퍼블릭 인터넷에 접속할 때 사용자를 멀웨어로부터 보호합니다. 그러나 이는 기업의 보안 기능 중 하나에 불과합니다.

비즈니스 전반에 대한 종합적인 보안 접근 방식을 구축하려면 기업 데이터센터 또는 IaaS 환경에 배치된 기업이 소유하고 관리하는 애플리케이션을 공격자로부터 보호해야 합니다. 기존 네트워크 보안 툴은 네트워크 경계를 보호하지만 경계를 침범한 공격자는 사용자 인증정보를 유출하거나 사용자 디바이스에 멀웨어를 설치함으로써 네트워크 내에서 자유롭게 이동할 수 있습니다.

기업 피싱 공격의 증가

2020년 3월~10월에 관측된 공격

64%

기업에 대한
공격 증가

17%

소비자에 대한
공격 증가

출처: Akamai Enterprise Threat Protector 보안 웹 게이트웨이

따라서 기업은 기업용 애플리케이션을 보호하는 ZTNA(제로 트러스트 네트워크 접속) 기술이 포함된 클라우드 보안 웹 게이트웨이가 필요합니다. ZTNA는 제로 트러스트 보안을 도입할 때 핵심적인 구성요소로서 사용자 ID를 기반으로 전체 네트워크 또는 세그먼트가 아닌 특정 애플리케이션에 대한 접속 권한만 사용자에게 제공합니다. 이 솔루션은 ID 및 접속 관리, MFA(멀티팩터 인증), Single Sign-On 기술과의 통합을 통해 사용자 ID를 보호합니다. ZTNA 툴을 사용하는 기업은 디바이스를 안전하게 관리하거나 복잡한 광역 네트워크 또는 가상 프라이빗 네트워크 연결을 유지하는 복잡한 업무에서 벗어나게 됩니다. 적절한 인증을 받은 사용자가 필요한 애플리케이션과 데이터에만 접속하기 때문에 애플리케이션 공격면이 없어지고 측면 이동 리스크가 최소화됩니다. 기업은 클라우드 보안 웹 게이트웨이를 평가할 때 벤더의 ZTNA 서비스 기능을 고려해야 합니다. 해당 서비스를 통해 기존의 비 웹 애플리케이션뿐 아니라 최신 웹 애플리케이션에 접속할 수 있습니까? 해당 서비스를 기업의 기존 ID 제공업체 서비스와 통합할 수 있습니까? MFA를 지원합니까?

보안 웹 게이트웨이는 ZTNA 서비스와 통합되어 작동해야 합니다. 만약 감염된 것으로 확인된 디바이스는 기업용 애플리케이션에 접속하지 못하게 해야 합니다. 보안 웹 게이트웨이의 로그는 다른 위협 신호를 강화하기 때문에 디바이스의 보안 상태를 보다 정확하게 파악할 수 있습니다. 예를 들어, 디바이스가 서버에게 명령을 내리고 제어하기 위해 호출하는 경우에 솔루션은 이것을 디바이스가 수정될 때까지 애플리케이션 접속을 제한하기 위한 신호로 사용해야 합니다.

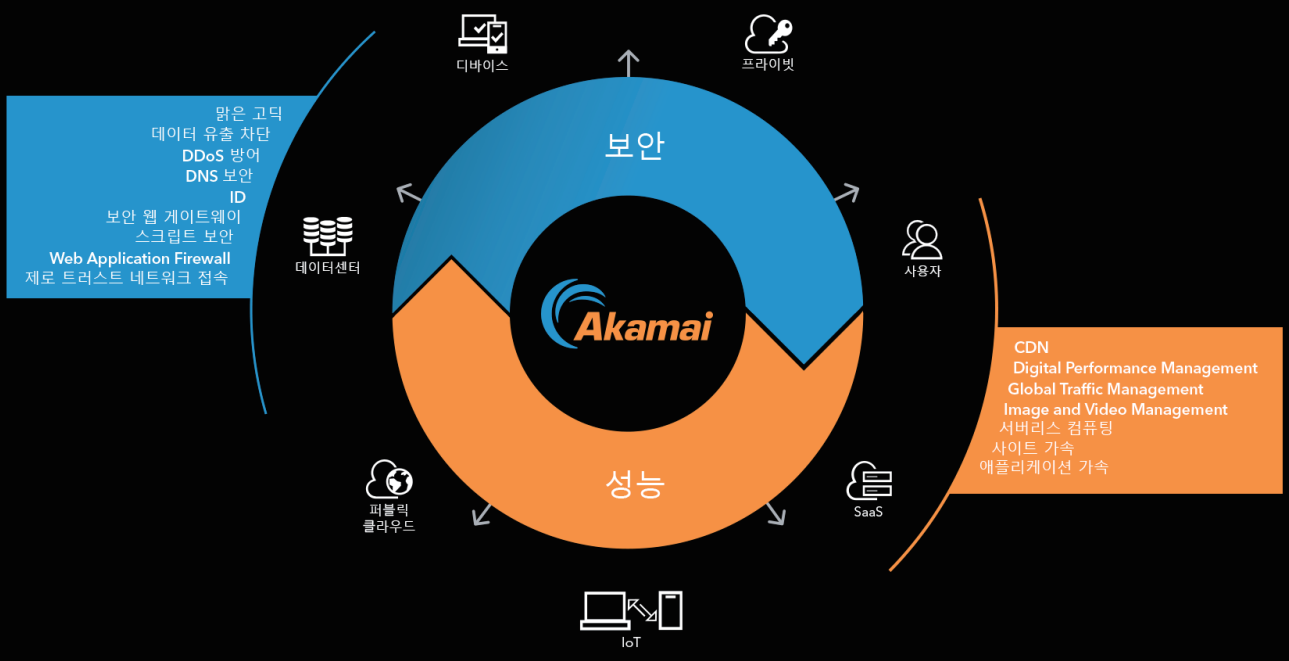
보안 웹 게이트웨이 및 ZTNA 기능을 추가하는 기업은 SASE(Secure Access Service Edge) 프레임워크를 도입하는 단계로 진입하게 됩니다. SASE는 기업 보안 활동을 데이터센터 중심, 하드웨어 어플라이언스 중심의 보안 아키텍처에서 벗어나게 합니다. 이런 보안 아키텍처에서 오늘날의 고도로 분산된 근무 및 비즈니스 환경에서는 더이상 작동하지 않습니다. 대신 SASE는 사용자 또는 디바이스의 ID를 기반으로 정책 기반 접속을 제공합니다. 또한 SASE는 웹 애플리케이션 방화벽과 API 보안, 봇 관리, 웹 대면 애플리케이션에 대한 분산형 서비스 거부 방어를 비롯한 광범위한 보안 제어 기능을 추가적으로 제공합니다.

제로 트러스트 네트워크 접속(ZTNA)은 내부 애플리케이션을 직접 인터넷에 노출하지 않기 때문에 공격 리스크를 감소시키며 디지털 비즈니스가 성공할 수 있도록 애플리케이션 접속의 유연성, 민첩성, 확장성을 개선합니다.

— Gartner, Market Guide for Zero Trust Network Access, Steve Riley, Neil MacDonald, Lawrence Orans, 2020년 6월 8일

또한 사용자와 한 번의 인터넷 홉만큼 떨어진 SASE 플랫폼에서 보안 제어 기능을 제공하기 때문에 사용자와 디바이스, 클라우드 서비스에 대한 접속 지연 시간이 모든 곳에서 짧습니다.

Akamai 클라우드 전송 SASE



최적의 성능

보안이 무엇보다 중요하지만 열악한 성능으로 사용자 경험에 영향을 주어서는 안 됩니다. 클라우드 기반 보안 웹 게이트웨이는 보안에 대한 심층적 방어 접근 방식을 제공해야 할 뿐만 아니라 지연 시간 없이 서비스를 제공해야 합니다.

지연 시간을 방지하려면 클라우드 보안 웹 게이트웨이를 사용자가 접속하는 곳과 가까운 PoP에 전 세계적으로 배포해야 합니다. 결국 백홀을 다른 백홀로 대체하는 것은 의미가 없습니다.

또한 클라우드 플랫폼은 트래픽이 폭주할 때도 사용자 경험에 영향을 주지 않도록 신속하게 확장되어야 합니다. 용량은 HTTPS 트래픽을 검사할 때 특히 중요합니다. HTTP 트래픽이 기하급수적으로 증가하고 있으며 결국은 모든 웹 트래픽의 100%를 차지할 것이기 때문입니다. 이제 대부분의 멀웨어가 HTTPS를 통해 전송되기 때문에 암호화된 트래픽을 검사할 때 사용자에게 미치는 영향을 최소화하는 것은 아주 중요합니다. 또한 이 플랫폼은 100% 가용성 SLA를 제공해야 합니다.

> **현재 클라우드 서비스로 전환한 전체 기업 중 81%에서 Office 365 사용자는 절반 이상을 차지합니다.[8]**

Office 365 통합: 많은 기업들이 Microsoft Office 365를 필수 생산성 제품군으로 사용하고 있기 때문에 Microsoft Office 365에 대한 높은 수준의 보안과 성능을 보장하는 것은 특히 중요합니다. 클라우드 보안 웹 게이트웨이를 배치할 때 한 가지 어려운 점은 다른 인기 있는 SaaS 애플리케이션과 마찬가지로 사용자가 TLS MITM 검사를 담당하는 포워드 프록시를 통해 해당 애플리케이션에 접속할 때 O365 성능이 떨어진다는 것입니다.

O365 성능에 영향을 주지 않으려면 반드시 다음과 같은 성능을 갖춘 글로벌 엣지 플랫폼을 통해 클라우드 보안 웹 게이트웨이를 제공해야 합니다.

- 요청을 기업의 DNS 리졸버와 가장 가까운 데이터 센터에 전달하는 백홀된 DNS 솔루션 대신 요청의 소스 IP를 사용해 지리상 가장 가까운 Microsoft O365 데이터 센터에 요청을 전달합니다. 예를 들어, 사용자가 싱가포르에서 O365에 접속하여 뉴욕의 O365 서버로 라우팅될 경우 매우 불쾌한 사용자 경험을 하게 됩니다.

- 보안 웹 게이트웨이 서버는 Microsoft O365 데이터 센터와 가까운 곳에 위치해야 하고 해당 서버와 데이터 센터가 상호 연결되어 있는 것이 이상적입니다.

- Microsoft에서 게시하고 업데이트하는 O365 도메인 및 IP 주소 목록을 사용하는 O365 트래픽 최적화 설정을 한 번 클릭으로 제공합니다. 이러한 도메인에 대한 요청은 Microsoft 권장 사항에 따라 O365 서버에 직접 전송되어야 합니다. 따라서 Microsoft가 새 도메인이나 IP 주소를 추가할 때 방화벽 및 기타 보안 제품을 수동으로 업데이트할 필요가 없어 시간과 노력을 절약할 수 있습니다.

보안을 엣지로 이동

원격 근무 인력이 빠른 속도로 증가함에 따라 사이버 공격에 보다 취약해지고 공격의 빈도와 파괴력도 커지고 있습니다. 최고의 클라우드 기반 보안 웹 게이트웨이 솔루션은 검증된 심층적 방어 기능을 통해 이러한 최신 보안 요구사항에 부합하는데 집중할 것입니다. 또한 사용자의 위치에 관계없이 모든 사용자에 대한 접속을 확보함으로써 제로 트러스트 및 SASE와 같은 최신 기업 보안 모델을 지원합니다.

종합적인 클라우드 보안 웹 게이트웨이는 모든 DNS 및 URL 요청을 평가하고, 여러 페이로드 분석 기술을 제공하고, 제로데이 피싱을 해결하며, 암호화된 트래픽을 검사하고, 데이터 손실 차단 기능을 통합하며, 섀도우 IT를 식별·관리할 뿐 아니라 장소와 디바이스에 상관 없이 보안 기능을 제공해야 합니다. 동시에 높은 수준의 성능을 제공하고 기업용 애플리케이션 보안 기술과 통합되어야 합니다. 이러한 솔루션을 사용하면 보안 복잡성을 줄이고, 많은 비용이 드는 백홀을 제거하고, 보안 팀의 효율성을 개선하며, 일관된 보안 정책을 지원할 수 있습니다.

Akamai의 클라우드 기반 보안 웹 게이트웨이인 Secure Internet Access에 대해 자세히 알아보고 akamai.com에서 무료체험을 시작하세요.

1. https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2
2. https://www.helpnetsecurity.com/2020/09/02/phishing-attacks-pandemic/
3. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
4. https://blogs.gartner.com/david_cappuccio/2018/07/26/the-data-center-is-dead/
5. https://www.brinknews.com/a-global-shortage-of-cybersecurity-professionals-leaves-businesses-at-risk/
6. https://news.sophos.com/en-us/2020/02/18/nearly-a-quarter-of-malware-now-communicates-using-tls/
7. https://www.mobolize.com/2020/10/29/mobolize-announces-technology-partnership-with-akamai-to-enable-security-on-mobile-devices/
8. https://blog.goptg.com/microsoft-office-365-statistics#:~:text=According%20to%20Bitglass%2C%20usage%20of,the%20shift%20to%20cloud%20services

Akamai는 온라인 라이프를 지원하고 보호합니다. 전 세계 대표적인 기업들은 매일 수십억 명의 사람들의 생활, 업무, 여가를 지원할 디지털 경험을 구축하고, 전송하고, 보호하기 위해 Akamai를 선택합니다. 클라우드에서 엣지까지 전 세계에서 가장 분산된 컴퓨팅 플랫폼을 구축한 Akamai는 고객의 애플리케이션 개발과 실행이 용이하도록 도우며, 사용자와 가까운 곳에서 경험을 제공하고 위협을 먼 곳에서 차단합니다. Akamai의 보안, 컴퓨팅, 전송 솔루션에 대한 자세한 정보는 akamai.com 및 akamai.com/blog를 방문하거나 Twitter 및 LinkedIn에서 Akamai Technologies를 팔로우하세요. 2022년 6월 발행.