CLOUDFLARE®

SaaS 공급자 서바이벌 가이드

온라인 애플리케이션에 필수적인 성능, 보안 및 암호화

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

핵심 요약

SaaS 시장은 2016년에서 2020년까지 196% 성장할 것으로 예상됩니다.[1] SaaS 시장이 계속해서 확대되고 SaaS가 비즈니스 인프라의 필수 구성 요소가 되면서 보안 및 성능은 SaaS 공급자와 고객 모두에게 최우선 고려 사항이 되었습니다. 이처럼 성장세가 이어지면서 SaaS 공급자는 고객에게 가장 안전하고 성능이 뛰어난 애플리케이션을 제공하기 위해 더욱 치열한 경쟁을 벌일 것입니다. 성능이 뒤떨어지고 공격에 취약한 애플리케이션은 수익, 최종 사용자 참여, 브랜드 평판 및 고객 이탈에 대한 부정적인 영향을 필연적으로 겪을 것입니다. SaaS 공급자의 주요 하위 집합의 경우, 브랜드 베니티 고객 도메인 암호화 요구 사항이 발생하면 SSL 수명 주기를 수동으로 관리해야 하므로 배포 시간이 길어지고 오버헤드 비용이 발생합니다. 또는 복잡하게 자동화된 사내 솔루션을 구축할 경우 엔지니어링 리소스가 핵심 역량에 집중할 수 없게 됩니다.

SaaS 공급자를 위한 Cloudflare의 성능 및 보안 솔루션을 사용하면 SaaS 공급자, 최종 고객 및 최종 방문자 경험을 보호하고 가속화할 수 있습니다. Argo Smart Routing, 부하 분산 및 성능 최적화와 결합된 Cloudflare의 10Tbps 글로벌 CDN(콘텐츠 전송 네트워크)은 방문자 대기 시간을 최대 2배까지 줄여 줍니다. Rate Limiting 및 WAF(웹 애플리케이션 방화벽)와 결합된 Cloudflare의 고급 DDoS 방어는 네트워크, 전송 및 애플리케이션 계층을 표적으로 삼는 복잡한 대규모 공격을 완화해 줍니다. 또한 SaaS 공급자는 쉽게 구현하고 완벽하게 관리되는 SSL 솔루션을 통해 사용자 지정 베니티 도메인의 고객 데이터를 안전하게 전송하도록 지원할 수 있습니다.

대기 시간 및 부적절한 보안이 비즈니스에 미치는 영향

SaaS 애플리케이션 대기 시간과 형태와 무관하게 잘못된 보안으로 인해 고객 경험, 전환율 및 검색 엔진 순위가 저하될 수 있으며, 이로 인해 수익 손실 및 고객 이탈이 증가할 수 있습니다.

성능 및 가용성이 SaaS 애플리케이션 사용에 미치는 영향

고객은 웹 사이트, 애플리케이션 및 API를 사용할 때 빠르고 가용성이 높은 환경을 원합니다. 온라인 자산이 대기 중이거나 사용 불가일 경우 SaaS 애플리케이션 사용 및 전환율에 대한 부정적인 영향이 눈에 띄게 커집니다.

예를 들어, Google은 사이트 대기 시간이 100~400ms이면 소비자 행동에 유의미한 영향을 미치고[1], Walmart는 사이트 로드 시간이 불과 몇 초만 증가해도 전환율이 급격하게 감소하고[2], Amazon에서는 사이트 대기 시간이 100ms 감소할 때마다 매출이 1% 증가한다고 보고했습니다.[3]

일반적인 SaaS 애플리케이션 성능 문제는 SaaS 공급자의 공유 호스팅 인프라 또는 애플리케이션 설정에 따라 작동하는 내부 요소와 관련이 있습니다. 방문자와 SaaS 애플리케이션 원본 서버 위치 간의 지리적 거리는 이러한 내부 요소 중 하나로, 대략 100마일씩 멀어질 때마다 대기 시간이 0.82 밀리초씩 증가한다고 합니다.[4] 이러한 상황에서 최적화되지 않은 대규모 정적 콘텐츠를 이용할 경우 방문자의 대기 시간은 더욱 길어집니다.

그러나 성능은 서버, 네트워크, 애플리케이션에만 좌우되지 않습니다. 공유 인프라에 과부하를 일으켜 애플리케이션을 대기 상태로 만들거나 전혀 사용할 수 없게 하는 트래픽 급증 또는 계절성 트래픽도 성능에 영향을 미칩니다.

느리게 로드되거나 사용할 수 없는 SaaS 애플리케이션은 수익, 전환율, 이탈률, 검색 엔진(SEO) 순위, 브랜드 평판, 고객 만족도 및 SLA(서비스 수준 계약)에 큰 영향을 미칠 수 있습니다.

[1] http://www.sfgate.com/business/article/Google-s-speed-need-instantaneous-Internet-3251049.php
[2] https://www.slideshare.net/devonauerswald/walmart-pagespeedslide
[3] https://blog.gigaspaces.com/amazon-found-every-100ms-of-latency-cost-them-1-in-sales/
[4] http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/

SaaS 애플리케이션 공격 대상이 될 경우의 영향

시장에 진출한 신규 SaaS 공급자 또는 로컬 애플리케이션을 클라우드로 마이그레이션하는 소프트웨어 회사를 막론하고, 온라인 연결이 기본인 애플리케이션에는 보안을 반드시 고려해야 합니다.

SaaS 애플리케이션 및 서비스가 공공 인터넷에 노출되면서 이들에 대한 공격 영역은 점점 확대되고 있고, 많은 경우 공유 인프라 간의 워크로드가 여기에 해당합니다. 그 예로, SaaS 제공업체의 공격 벡터에는 로그인 포털, 공유 DNS 및 호스팅, 복잡한 애플리케이션 취약성 등이 포함됩니다. 여기서 주목할 점은 많은 SaaS 제공업체가 공유 인프라 내에서 여러 클라이언트 애플리케이션을 호스팅한다는 것으로 데이터 유출, 안정성 문제 또는 해당 공유 인프라에 대한 공격이 발생할 경우 다른 고객에게 부정적인 영향을 줄 수 있습니다.

위에서 언급한 벡터를 표적으로 삼는 특정 공격으로는 복잡한 볼류메트릭 DDoS 공격, 무차별 로그인 시도, 애플리케이션 취약성 공격, 암호화되지 않은 고객 데이터 가로채기 등이 있으며 모두 각종 장치의 웹 사이트, 애플리케이션 및 API를 노립니다. 공격이 성공할 경우 비즈니스에는 서비스 중단, 브랜드 평판 저하, 고객 이탈에서부터 상당한 매출 손실 및 피해 대응 비용에 이르기까지 다양한 영향이 미칩니다.

2013년에 Adobe에 침투한 해커는 Adobe 고객 290만 명분의 신용카드 정보 및 기타 개인 데이터에 액세스했습니다.[5] Adobe의 최고 보안 책임자인 Brad Arkin은 "사이버 공격은 오늘날 비즈니스를 수행하며 마주할 수 있는 불행한 현실 중 하나입니다."라며 온라인 비즈니스의 위험을 인정했습니다.

2016년 10월 16일에는 악명 높은 Mirai 봇넷의 공격으로 Airbnb, Amazon.com, Netflix, The New York Times, Paypal, Pinterest, Reddit, Tumblr, Twitter, Verizon, Visa, The Wall Street Journal, Yelp, Zillow를 비롯한 많은 기업에서 장시간 다운을 겪었습니다. 애플리케이션은 직접적인 공격 대상이 아니었지만 DNS 서비스 공급자인 Dyn에서 이러한 웹 사이트 및 애플리케이션을 공유하고 있었습니다. Dyn은 11시간 만에 가까스로 문제를 해결했고, 영향을 받은 모든 웹 사이트의 서비스는 그제서야 정상화되었습니다.[6]

암호화와 사용자 지정 베니티 도메인 중 선택

온라인 조직에서 SSL/TLS 암호화를 채택하는 것이 보안 모범 사례가 되었고 대규모 기술 기업의 안전한 인터넷 구축을 요구하는 목소리가 높아지면서, SSL/TLS 암호화는 하나의 요구 사항으로 자리 잡고 있습니다. 예를 들어, 2016년 말부터는 Google Chrome 웹 브라우저에서 HTTPS를 사용하지 않는 웹 사이트에 접속하면 사용자가 잘 볼 수 있는 곳에 '안전하지 않음'이라는 문구가 표시됩니다.[7] 또한, Apple은 이제 App Store에 제출하려는 iOS 애플리케이션에 HTTPS 연결을 의무화하고 있습니다.[8]

SSL 도입 초기에 온라인 조직은 HTTPS로 트래픽을 암호화할지 또는 성능 기대치를 충족하는 방문자 경험을 제공할지 선택해야 했습니다. 몇 년 전까지만 해도 SSL 프로토콜을 사용하면 대기 시간이 늘어나고 웹 사이트 및 애플리케이션 성능이 저하될 수 있었습니다. 또한 조직이 보안 강화를 위해 성능을 포기하기로 결정하더라도 당시 SSL 구현에는 운영상의 어려움이 있어 광범위한 채택에 한계가 있었습니다. HTTP/2(HTTP 1.1의 후속 버전) 개발과 같은 첨단 SSL 개선 덕분에, 이제는 HTTPS 트래픽 보호에 SSL을 사용해도 암호화되지 않은 HTTP보다 월등한 성능을 발휘합니다.

과거에 조직에서 암호화 또는 성능 중 하나를 선택해야 했던 경우처럼, 오늘날 SaaS 제공업체의 주요 하위 집합은 고객의 트래픽을 암호화할지 아니면 고객의 자체 브랜드 베니티 도메인을 허용할지 선택해야 합니다. 무엇을 선택하든 핵심은 적절한 브랜드 표현, 보안, 검색 엔진 순위 및 사용 가능한 최적의 성능의 이점을 모두 누리는 것입니다.

[5] http://www.nytimes.com/2013/10/04/technology/adobe-announces-security-breach.html
[6] http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
[7] https://techcrunch.com/2016/06/14/apple-will-require-https-connections-for-ios-apps-by-the-end-of-2016/
[8] https://techcrunch.com/2016/06/14/apple-will-require-https-connections-for-ios-apps-by-the-end-of-2016/

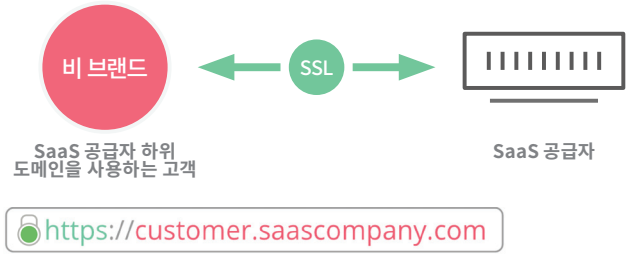
SaaS 공급자의 이 하위 집합은 일반적으로 고객에게 방문 페이지, 웹 사이트, 지원 포털 등의 공개 온라인 자산을 생성하는 기능을 제공합니다. SaaS 공급자는 일반적으로 새로 생성된 고객 자산을 기본 도메인의 하위 도메인에서 호스팅합니다. 예를 들어, SaaS 공급자의 고객이 만든 자산의 URL은 **customercompany.com** 또는 **support.customercompany.com**과 같은 브랜드 베니티 URL이 아닌 **customercompany.saasprovider.com**으로 읽힐 수 있습니다. 이는 고객에게 어려운 문제인데, 브랜드 베니티 도메인이 없으면 브랜드 인지도, SEO 순위 및 방문자 신뢰도가 손실되기 때문입니다.

SaaS 공급자와 고객은 customercompany.com 또는 support.customercompany.com URL을 customercompany.saasprovider.com으로 CNAME화하여 도메인 브랜드 문제를 극복했습니다. 이렇게 하면 고객이 자체 브랜드 베니티 도메인을 사용할 수 있습니다. 그러나 SaaS 공급자는 SSL을 쉽게 사용할 수 없으며 전체 SSL 수명 주기 프로세스를 관리하기가 더 어려워집니다. SSL 수명 주기 프로세스를 수동으로 관리하거나 최종 고객을 위한 사내 솔루션을 구축하려고 하면 상당한 시간 소비, 수작업 및 비용이 발생합니다.

앞서 언급한 문제를 해결할 때 SaaS 공급자가 따를 수 있는 세 가지 시나리오가 있습니다.

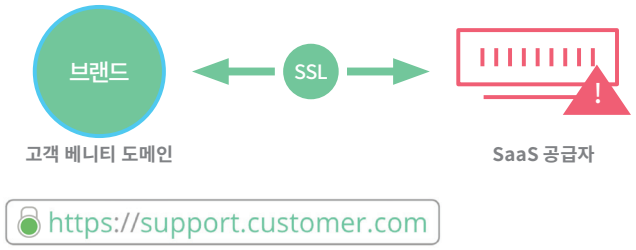
암호화되지 않은 브랜드 베니티 도메인

SSL을 사용하지 않는 사용자 정의 베니티 도메인은 SSL의 성능 이점을 누릴 수 없고 데이터 전송을 보호하지 못하므로 스누핑에 취약하며, 방문자에게 도달하기 전에 콘텐츠가 수정되거나 삽입될 수 있습니다.



암호화된 비 브랜드 도메인

SaaS 공급자를 통해 SSL을 사용할 수 있는 도메인에는 사용자 지정 베니티 도메인이 없으므로 브랜드 평판 저하 및 SEO 순위 하락이 발생합니다.

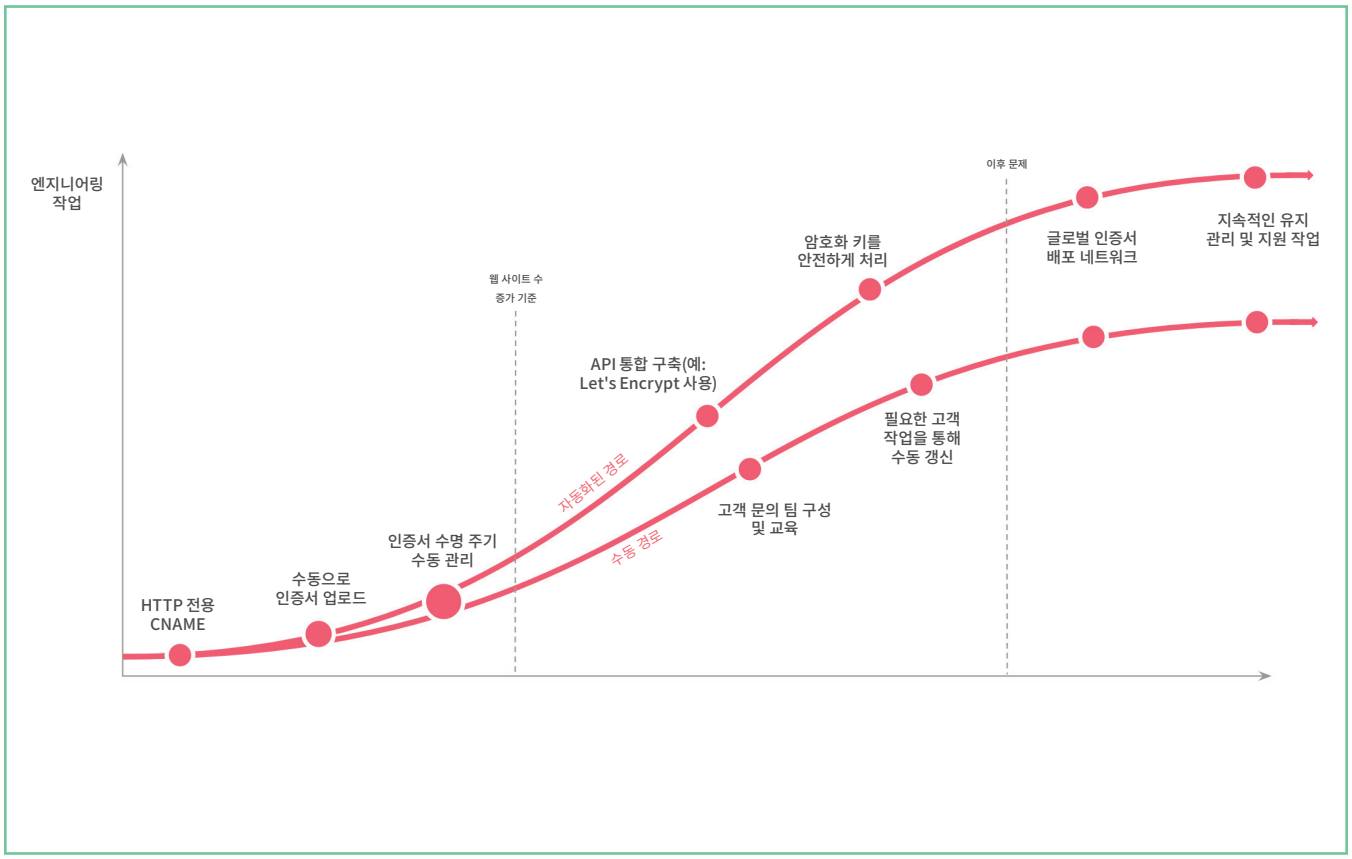


까다로운 사내 방식

암호화된 브랜드 베니티 도메인이 필요한 SaaS 공급자는 SSL 수명 주기를 수동으로 관리할 수 있는데, 이로 인해 배포 시간과 오버헤드 비용이 증가하거나 복잡하게 자동화된 사내 솔루션을 구축하게 됩니다.

SaaS 공급자가 고객 도메인용 SSL을 관리하기 위한 자체 솔루션을 개발할 때 직면하는 기술적인 문제점에 주목하는 것이 중요합니다. 아래 그림은 자동화된 사내 SSL 솔루션을 구축하려는 SaaS 공급자가 제시하는 일반적인 로드맵을 보여줍니다.

사내 솔루션을 구축하는 데 두 가지 경로를 이용할 수 있지만 둘 다 이상적이지는 않습니다. 첫 번째(위쪽) 경로는 SSL 프로세스 자동화라는 장점이 있지만 충분한 엔지니어링 작업이 필요하며 복잡한 문제가 있습니다. 두 번째 경로는 SaaS 공급자와 최종 고객 모두에게 충분한 수작업이 요구됩니다.



SaaS 애플리케이션 보안, 성능 및 가용성을 위한 Cloudflare

Cloudflare는 대기 시간을 줄이고 콘텐츠 전송 성능을 최적화하여 SaaS 공급자 웹 사이트, 애플리케이션 및 API의 최종 사용자 환경을 개선하는 동시에 최종 고객 인터넷 자산에서도 이러한 이점을 누리도록 합니다.

전 세계에 분산된 데이터 센터

Cloudflare 솔루션의 핵심은 전 세계 57개국에 117 + 5 데이터 센터로 구성된 글로벌 Anycast CDN(콘텐츠 전송 네트워크)으로, 모든 지역의 방문자에게 SaaS 애플리케이션 콘텐츠를 제공합니다. 또한 Cloudflare는 세계에서 가장 권위 있는 DNS 네트워크 중 하나를 운영하는 관리형 DNS 도메인의 38% 이상을 지원합니다. 평균 쿼리 속도가 수 밀리초에 불과한 Cloudflare는 관리형 DNS 공급자 중 가장 빠른 전역 성능을 제공합니다.

대규모 애플리케이션 가용성

Cloudflare의 고가용성 DNS 인프라와 글로벌 Anycast™ 네트워크를 확장한 Cloudflare 부하 분산은 트래픽 부하를 여러 서버에 분산하고 트래픽을 가장 가까운 지역으로 라우팅하여 대기 시간을 줄입니다. 부하 분산에는 빠른 페일오버와 상태 검사가 포함되어 있으므로 방문자를 장애로부터 빠르게 격리합니다. 또한 여러 클라우드 공급자 또는 온프레미스 인프라 전체에서 부하 분산을 사용하면 단일 공급자 또는 서버로 인한 중단의 영향을 완화하고 클라우드 공급업체에 종속되는 것을 피할 수 있습니다.

더욱 빨라진 방문자 경험

Cloudflare의 CDN은 HTML, CSS 및 JavaScript의 자동 최소화, 파일 및 리소스의 크기를 20% 이상 줄이는 Gzip 압축을 포함한 고급 최적화 기능을 사용해 구축되었습니다. 또한 독점적인 이미지 및 모바일 최적화로 SaaS 애플리케이션의 성능을 더욱 높입니다.

Cloudflare는 전 세계 인터넷 트래픽의 10% 이상을 제공하면서 네트워크 경로의 실제 상태와 신뢰성을 실시간으로 분석합니다. Cloudflare의 Argo Smart Routing 알고리즘은 수집된 정보를 사용하여 사용 가능한 가장 빠른 경로를 통해 트래픽을 라우팅하는 동시에, 안전하게 개방된 연결을 유지하여 연결 설정으로 인한 대기 시간을 없앱니다. Argo Smart Routing은 인터넷 대기 시간을 평균 35%, 연결 오류를 27% 줄입니다.

"Cloudflare로 Crisp의 서비스 품질을 극대화하고 서비스 응답 시간은 최소화했습니다. 덕분에 고가의 네트워크 인프라가 대중들에게 상용화되었습니다. 이제 Cloudflare 없는 비즈니스는 상상도 할 수 없습니다."

crisp™ | Valérian Saliou
Crisp의 CTO

SaaS 애플리케이션 및 고객 데이터 보호

Cloudflare의 클라우드 기반 보안 솔루션은 SaaS 공급자의 웹 사이트, 애플리케이션 및 API를 보호하여 최종 고객의 인터넷 자산까지 안전하게 유지합니다.

10Tbps의 처리량을 자랑하는 117개 이상의 Cloudflare 데이터 센터 Anycast 네트워크는 지금까지 기록된 가장 큰 DDoS 공격보다 10배나 더 크기 때문에 OSI 모델의 계층 3, 4 및 7을 표적으로 삼는 공격을 막아줍니다. Rate Limiting 및 WAF (웹 애플리케이션 방화벽)와 결합된 Cloudflare의 보안 솔루션은 애플리케이션 계층을 대상으로 하는 복잡한 공격도 완화해 줍니다. 또한 SaaS용 Cloudflare SSL을 사용하면 SaaS 공급자 및 최종 고객은 통신을 암호화하여 데이터 가로채기 및 악의적인 콘텐츠 삽입을 방지하고 사용자 지정 베니티 도메인을 계속 사용할 수 있습니다.

민감한 고객 데이터 보호

SaaS 애플리케이션이 상업적으로 중요한 비공개 데이터를 더 많이 보유하게 되면서 무차별 로그인 시도, 데이터 유출 및 메시지 가로채기(man-in-the-middle) 공격으로부터 보호하는 것이 중요해졌습니다.

먼저 Cloudflare의 WAF(웹 애플리케이션 방화벽)를 통해 이러한 유형의 공격을 차단하여 애플리케이션 계층을 노리는 복잡한 공격을 완화합니다. Cloudflare의 WAF는 기본적으로 OWASP 상위 10개 취약성뿐만 아니라 다음과 같은 공통 통합 및 언어(예: PHP, Magento, WordPress, Drupal, Atlassian 등)를 표적으로 삼는 애플리케이션 관련 취약성도 보호합니다. Cloudflare의 WAF를 통해 SaaS 공급자는 새로 발견된 공격 벡터 및 취약성을 방어하기 위한 사용자 정의 규칙 세트를 즉시 생성하고 이를 Cloudflare 네트워크에서 30초 이내에 전파할 수 있습니다.

Cloudflare의 DDoS 방어와 함께 작동하는 Rate Limiting은 요청 비율이 의심스러운 방문자를 차단하는 세분화된 제어 기능을 제공합니다. Rate Limiting은 애플리케이션 또는 웹 사이트의 허가되지 않은 영역에 액세스하려는 무차별 로그인 시도를 완화하기 위해 마련된 기능으로, 지정된 시간 동안 특정 IP 주소에서 특정 끝점으로 전달되는 요청 수를 제한합니다.

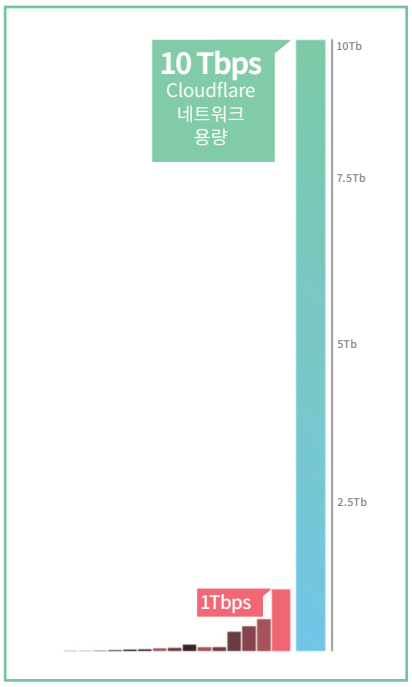
"Cloudflare의 솔루션은 완벽하게 작동합니다. Cloudflare 팀 덕분에 우리 회사의 모든 요구 사항과 사용자 지정 사항을 순식간에 전파할 수 있었습니다."

zendesk | **Amanda Kleha GM**
Zendesk 온라인 사업부

SaaS용 Cloudflare SSL은 맞춤 CNAME 베니티 도메인에 대한 SSL/TLS 인증서 관리를 가장 효율적으로 자동화하는 방법을 제공합니다. 메시지 가로채기 공격을 통한 데이터 가로채기 또는 암호화되지 않은 연결로 인한 트래픽 스누핑을 방지합니다.

악의적인 트래픽을 차단하여 가용성 보장

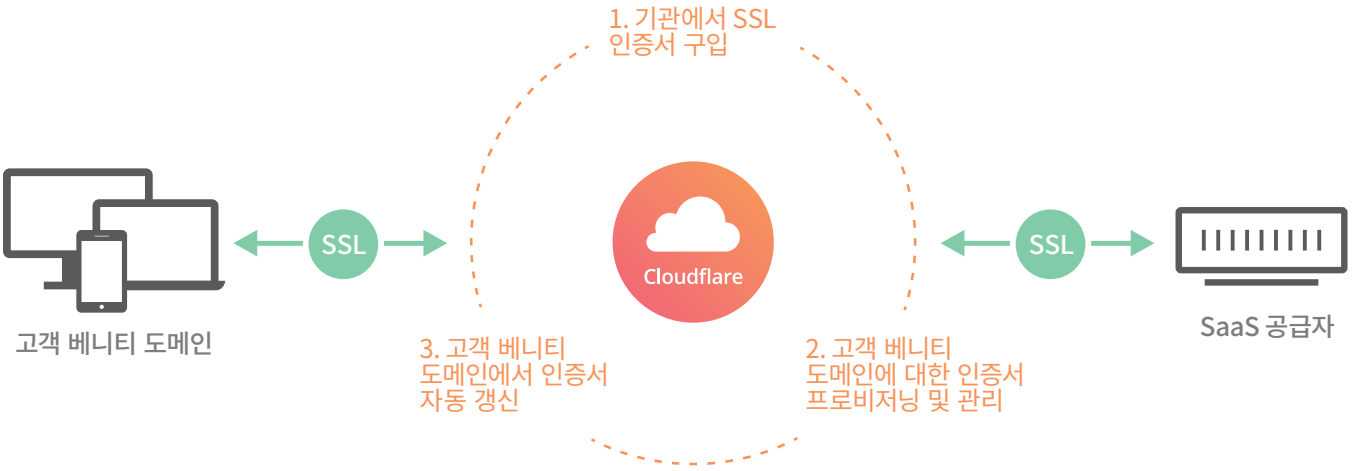
민감한 고객 데이터의 도난이나 분실은 재앙이나 다름없지만, 서비스 가용성을 저해하려는 공격의 희생자가 되는 것 역시 파괴적인 결과를 초래할 수 있습니다. Cloudflare의 백본은 57개국 117개 이상의 데이터 센터로 구성된 글로벌 CDN(콘텐츠 전송 네트워크)입니다. Cloudflare의 총 네트워크 처리량은 10Tbps를 넘으며, 이는 지금까지 기록된 공격 중 가장 규모가 컸던 DDoS 공격의 약 10배에 달합니다. 계층 3, 4, 7을 노리는 볼류메트릭 DDoS 공격은 Cloudflare의 네트워크 전체에서 흡수되어 균등하게 분산되므로, 다운타임이 발생하지 않고 SaaS 고객에게 최고의 가용성을 보장합니다. Cloudflare의 Rate Limiting 솔루션은 DDoS 방어와 함께 작동하여 의심스러운 요청이 있는 방문자를 차단하는 세밀한 제어가 가능합니다. 특정 IP가 정의된 임계값을 초과하면 할당된 시간 동안 특정 끝점에 대한 추가 요청을 차단할 수 있습니다.



SaaS 공급자를 위한 자동화된 SSL 솔루션

SaaS용 SSL은 SaaS 공급자에게 Cloudflare의 네트워크 보안 및 성능 이점을 최종 고객에게도 제공할 수 있는 역량을 제공하여 최종 고객이 사용자 지정 베니티 도메인을 사용할 수 있도록 합니다. Cloudflare의 SaaS 솔루션용 SSL을 통해

고객은 계속해서 베니티 도메인을 SaaS 공급자 하위 도메인으로 CNAME화해 브랜드 URL의 이점을 제공하고, Cloudflare는 SaaS 공급자 및 고객을 위해 전체 SSL 수명 주기를 지원 및 관리할 수 있습니다. 고객 도메인에서 SSL을 사용하면 방문자에 대한 신뢰가 강화되고, SEO 검색 순위가 향상되고, 최신 HTTP/2 프로토콜을 활용할 수 있게 되므로 속도가 훨씬 빨라집니다.



브랜드 방문자 경험

사용자 지정된 자체 브랜드 베니티 도메인을 가져올 수 있는 SaaS 공급자의 고객은 완벽하게 관리되는 SSL 인증서의 이점을 누리는 동시에 계속해서 사용자 지정 베니티 도메인을 사용할 수 있습니다. 사용자 지정 CNAME 베니티 도메인은 SaaS 고객에게 브랜드 가시성과 SEO 순위를 높이는 동시에 웹 사이트 또는 애플리케이션 방문자에게 더 큰 신뢰감을 제공합니다.

안전하고 성능이 뛰어난 고객 자산

SaaS용 SSL을 사용하면 CNAME 사용자 지정 베니티 도메인에 전용 SSL/TLS 인증서를 추가할 수 있습니다. HTTPS를 통해 데이터를 전송하면 민감한 고객 데이터의 안전한 전송을 보장하고 메시지 가로채기 및 네트워크 스누핑으로부터 보호합니다. SSL을 사용하면 속도가 더 빠른 HTTP/2 프로토콜을 사용할 수 있게 됩니다.

자동화된 수명 주기 관리 및 신속한 SSL 배포

Cloudflare는 SaaS 공급자의 CNAME 고객 베니티 도메인의 개인 키 발급/보호에서 도메인 유효성 검사, 발급, 갱신 및 재발급과 같은 전체 SSL 수명 주기를 관리합니다. SaaS 공급자와 최종 고객 모두 SSL 수명 주기 처리 부담을 덜 수 있습니다. SSL 발급 과정에서 Cloudflare는 새로운 인증서 요청을 전송하고 몇 분 이내에 HTTPS를 가용 가능한 상태로 만듭니다.

"Cloudflare를 사용한다는 건 엔지니어에게 최고의 행복입니다."

UDACITY

Paul Bauer
Udacity 플랫폼 엔지니어

요점

Cloudflare에 가입하여 SaaS 애플리케이션의 성능과 보안을 향상시키고 최종 고객 CNAME 베니티 URL에 SSL을 손쉽게 배포하십시오. 간편하게 설정할 수 있으며 실행되기까지 5분도 걸리지 않습니다. Free에서부터 Enterprise에 이르는 요금제를 살펴보고(www.cloudflare.com/plans/) SaaS 공급자용 Cloudflare에 대해 자세히 알아보십시오 (www.cloudflare.com/saas/).

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com