CLOUDFLARE

백서

더 적은 투자로 더 큰 효과

7개 회사의 비용 효율적 애플리케이션 보안 및 성능 전략.

핵심 요약

악성 봇, DDoS 공격, 코드 주입, 기타 취약점으로부터 웹 애플리케이션과 API를 보호하는 일은 조직에 아주 중요한 과제입니다. 하지만 탄탄한 보안 전략을 구축하는 일은 특히 예산이 한정되어 있고 팀 확대가 제한되어 있는 경우 까다로운 일입니다.

본 백서에서는 애플리케이션 보안 전략을 통해 효율을 끌어올리고 비용을 절감하는 데 성공한 회사들의 실제 사례를 공유합니다. 이 성공 사례를 살펴봄으로써 기업은 애플리케이션 보안 정책을 이용해 어떻게 비용을 절감할 수 있는지 가치 있는 인사이트를 얻게 될 것입니다.

보안 및 IT 팀이 더 적은 투자로 더 많은 효과를 창출해야 하는 시기

조직에서 예산 한계에 맞닥뜨렸을 때 아무런 타격도 받지 않는 팀은 없습니다. 경제적 불확실성, 급감하는 매출, 조직 개편 때문이든 그 밖의 다양한 이유에서든 보안 및 IT 팀에서는 예산 확대를 기대할 수 없는 경우에도 운영 효율을 개선해야 하는 압박에 종종 직면하며, 상황이 더 안 좋을 때는 아울러 비용까지도 절감해야 합니다.

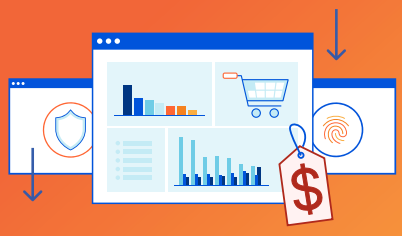
하지만 애플리케이션 보안과 성능은 결과를 타협해도 되는 분야가 아닙니다. 보안 측면에서, 애플리케이션을 보호하는 일은 해가 갈수록 더 복잡해지고 있습니다. 그 어느 때보다 공격은 그 규모가 더 커지고 더 복잡해지고 있으며, 조직이 성장하면 그만큼 공격 표면도 넓어집니다. CVE Program에서는 새로운 취약점 수가 2021년부터 2022년까지 25% 증가하여, 2022년 확인된 수만 총 25,059개에 달할 것으로 추정했습니다.

그리고 성능 측면에서 소비자는 모든 디지털 경험이 빠르고 안정적이면서 맞춤화되어 있을 것으로 기대합니다. 미미한 속도 저하도 사용자 참여와 전환율에 큰 영향을 미칠 수 있으므로 고객 기대를 충족하지 못하는 기업은 큰 타격을 받습니다.

예산 제약과 고객 기대 증가라는 이중고 속에서 보안 및 IT 팀은 더 적은 투자로 더 많은 효과를 창출할 수 있는 방법을 찾아내야 합니다. 본 백서에서는 성과에 아무런 타격도 없이 비용 효율적인 보안 및 성능 정책을 구축하는 데 성공한 기업들의 사례를 소개합니다.

애플리케이션 보안 정책과 관련한 비용을 절감하는 방법

최신 위협으로부터 웹 애플리케이션과 API를 보호하는 가장 좋은 방법은 계층화된 보안 서비스를 제공하는 동시에 조직에서 불필요한 비용을 줄일 수 있도록 지원하는 것입니다. 이를 위해 조직은 벤더 통합, 인증서 관리 간소화, 트래픽 비용을 증가시키는 공격을 방어하는 전담 솔루션 도입, 송신 수수료 절감 등 다양한 핵심 전략을 활용할 수 있습니다.



보안 벤더 통합을 통한 비용 절감

인증서 관리 자동화를 통한 인력 및 인프라 비용 절감

트래픽 비용을 증가시키는 공격 차단

대역폭, 클라우드, 송신 수수료 등 예기치 않은 수수료와 비용 제거

보안 벤더 통합을 통한 비용 절감

최근 Gartner 설문에 따르면 75%의 기업에서 보안 정책 측면에서 벤더 통합을 고려합니다. 벤더 수를 줄임으로써 조직은 공급망 프로세스를 최적화하고 효율을 높여 비용 절감이라는 목표를 달성할 수 있습니다.

온라인 럭셔리 시계 마켓플레이스인 Chrono24는 Cloudflare를 이용한 통합을 통해 여러 벤더에 대한 의존성을 줄였습니다.

그 전까지 Chrono24는 EdgeCast의 CDN 솔루션과 그 밖의 여러 벤더의 DDoS 완화 및 WAF 솔루션을 이용했습니다. 이처럼 여러 솔루션을 사용하다 보니 성능이 떨어졌고, 이는 상당한 대기 시간, 열악한 보안 성능, 벤더 비용 낭비로 이어졌습니다.

CDN, WAF, DDoS 완화가 포함된 Cloudflare의 솔루션으로 통합한 후에 Chrono24에서는 웹 사이트 보안 및 성능 비용을 67% 절감할 수 있었습니다.

"성능 및 보안 솔루션을 단일 공급자로 통합하면서 이제 기본 비용이 크게 낮아졌습니다"라고 기술 디렉터 Sven Ferber는 이야기합니다. "전보다 비용이 삼분의 일 정도로 줄어들었죠."

벤더 통합은 구매 비용과 관리 비용을 절감하고 싶은 기업에 아주 효과적인 전략일 수 있습니다. 아래는 벤더 통합을 고려할 때 생각해 볼 수 있는 세 가지 질문입니다.

1. 현재의 벤더가 위협 방어 성능을 제공하고 앱 성능을 개선해 주는가?
2. 단일 콘솔에서 애플리케이션과 API를 관리할 수 있는가?
3. 조직 내 여러 팀에서 동일한 벤더를 활용함으로써 예산을 효율적으로 쓰고 있는가?

위의 통합 팁을 따르면 비용을 절감하고, 공급망 관리를 간소화하며, 핵심 벤더와의 관계를 강화할 수 있습니다.

chrono24
The World's Watch Market

요점

75%의 기업에서 벤더 통합을 고려 중입니다

Chrono24에서는 Cloudflare와의 통합 이후 웹 사이트 보안 비용과 IT 비용을 **67%** 절감했습니다

벤더 수를 줄이고 서비스를 통합함으로써 기업에서는 **비용을 절감하고** 공급망 관리를 간소화할 수 있습니다

인증서 관리 자동화를 통한 인력 및 인프라 비용 절감

보안 구성을 여러 도메인 및 지역에 걸쳐 배포하는 일은 IT 팀에게는 비용이 많이 들고 지나치게 긴 시간이 소모되는 프로세스일 수 있습니다. 또한 예기치 않은 비용 때문에 특히 예산이 제한되어 있는 조직에게는 또 다른 문제가 야기될 수 있습니다.

때로는 이 숨겨진 비용이 인증서 관리의 모습을 띨 수도 있습니다. SSL/TLS 인증서는 네트워크의 디지털 정체성을 구성합니다. 평균적으로 기업의 웹 프레즌스에는 수천 개까지는 아니더라도 수백 개의 인증서가 필요합니다. 하지만 이 인증서를 관리하려면 큰 비용이 들 수 있습니다. 예기치 않은 인증서 오류로 인한 수익 손실은 물론이고 인력과 인프라 비용도 증가하기 때문입니다.

전자 상거래 플랫폼인 SHOPYY에서는 Cloudflare를 이용해 SSL 인증서 관리를 자동화합니다. 여기에는 개인 키 생성, 보호, 도메인 검증, 발급, 갱신, 재발급까지 모든 과정이 포함됩니다.

SHOPYY는 원래 인증서의 신뢰도가 낮고 유효 기간이 짧은 무료 인증서 관리 도구를 사용했습니다. 결국 SHOPYY는 인증서 관리 및 갱신 프로세스를 담당할 직원을 추가로 고용해야 했습니다.

Cloudflare SSL for SaaS를 도입하면서 SHOPYY는 Cloudflare에 인증서 관리 프로세스를 맡겼고, 덕분에 내부 직원 한 명이 전체 프로세스를 관리할 수 있게 되었습니다.

"Cloudflare 제품을 사용하게 되면서 운영 및 유지 관리 측면에서만 60%까지 비용을 절감할 수 있었습니다"라고 창립자 겸 CTO인 Yuanming Chen은 말합니다.

비효율적인 인증서 관리 방식은 인증서 만료로 인한 수익 저하로 이어질 수도 있습니다. 온라인 대출업체 LendingTree에서는 Cloudflare의 TLS 인증서를 이용해 비용을 절감하고 운영 중단 사태를 방지합니다.

"회사의 자산은 수천 개에 달합니다. 이 정도 규모에서 인증서 갱신 시기를 놓치는 건 시간 문제였죠"라고 애플리케이션 보안 책임자 John Turner는 이야기합니다. "Cloudflare의 TLS 인증서는 자동으로 갱신되므로 **연간 50,000달러 정도가 절감됩니다. 관리비가 줄고, 인증서가 만료되면서 운영이 중단되어 발생하는 수익 손실이 사라진 덕분이죠.**"

효율적인 인증서 관리 시스템을 구축하면 리소스를 효율적으로 재배치할 수도 있습니다. 독일에서 창업한 mogenius는 클라우드 기반 애플리케이션을 배포하는 자동화 플랫폼으로, Cloudflare를 이용해 인증서 관리 시스템을 자동화하여 핵심 비즈니스 성장에 더 많은 시간을 투입할 수 있게 되었습니다.

"Cloudflare 덕분에 내부에서 모든 걸 관리하는 시간은 20% 정도에 불과합니다."라고 공동창립자 겸 CPO인 Jan Lepsky는 말합니다. "**Cloudflare 덕분에 고객을 위해 클라우드 개발 및 배포 파이프라인을 최적화하는 데 집중할 수 있습니다.**"

인증서 관리 부담을 줄이는 일은 숨겨진 비용을 없애고 원활한 비즈니스 활동을 원하는 기업에게는 핵심 과제입니다. 비효율적이고 수동적이며 파편화된 인증 방식은 인력 및 인프라 비용을 증가시키고, 만료된 인증서로 인한 수익 손실과 리소스 낭비로 이어집니다.

SSL for SaaS 또는 TLS 인증 등의 기능을 이용해 인증서 관리를 구축한 기업은 상당한 비용을 절감하고 매출을 개선할 수 있습니다.

SHOPYY

lendingtree

mogenius®

요점

Cloudflare SSL for SaaS를 이용해 SHOPYY에서는 운영 및 유지 관리 비용을 60% 절감합니다

LendingTree에서는 Cloudflare TLS를 통해 관리 비용 및 수익 손실과 관련하여 연간 50,000 달러를 절감합니다

mogenius는 Cloudflare를 통해 인증서 관리를 자동화하여 20%의 시간을 핵심 비즈니스에 더 투입할 수 있게 되었습니다

트래픽 비용을 증가시키는 공격 차단

API 사용이 증가하면서 공격 표면 역시 커지고 있습니다. 악성 봇, DDoS 공격 등의 위협은 애플리케이션 및 API를 손상시킬 수 있으며, 최고 책임자와 기술 리더는 이러한 공격이 비즈니스에 상당한 영향을 미치는 것을 인식하고 있습니다.

API 보안 침해는 기업에 연간 최대 750억 달러의 비용을 발생시킨 것으로 추정됩니다.

이러한 공격은 자격 증명 스터핑 공격과 DDoS 공격을 유발하고, 합법적인 사용자에 대한 서비스를 방해할 뿐 아니라, 조직에서 공격 트래픽으로 인해 급증한 트래픽을 처리하는 비용을 소모하게 할 수 있습니다.

LendingTree에서는 DDoS 공격 중 발생한 트래픽 급증 비용을 청구한 이전의 보안 벤더에게 상당한 비용을 지불하고 있었습니다. 이 모델은 엄청난 초과 비용을 발생시켰을 뿐 아니라 합법적인 트래픽까지 차단되는 결과를 초래했습니다.

"새로운 TV 광고나 새 소셜 미디어 캠페인을 펼치면, 벤더의 요구에 따라 지정해 놓은 임의적인 제한을 넘어 요청이 급증했습니다. 그러면 벤더가 이러한 급증 현상을 DDoS 공격으로 해석해 정상적인 트래픽을 차단하게 되는 겁니다" 라고 애플리케이션 보안 리더 John Turner는 회상합니다. **"우리는 잠재 고객을 잃었을 뿐만 아니라, 고객이 사이트를 방문하도록 하려고 우리가 지출했던 비용도 잃었는데, 벤더는 'DDoS 방어' 서비스 비용을 청구하는 거죠."**

이러한 비효율을 해결하기 위해 LendingTree에서는 Cloudflare Bot Management 및 Rate Limiting 기능을 도입했습니다. **48시간이 지나기도 전에 특정 API 엔드포인트에 대한 공격이 70% 감소했고, 5개월이 채 되기도 전에 LendingTree에서는 API 엔드포인트 남용을 차단해 250,000달러를 절감했습니다**.

온라인 게임 지주 회사인 Flutter Entertainment에서는 70~90% 정도의 트래픽이 악의적임을 파악하고, 악성 봇을 필터링하고 차단하기 위한 솔루션을 원했습니다. Cloudflare Bot Management를 도입한 후, **Flutter는 악성 트래픽을 90% 줄이고, 매년 2백만 파운드 이상을 절감하고 있습니다**.

봇 관리 및 DDoS 방어 솔루션을 통해 조직에서는 공격 및 API 남용을 방지하고 공격 관련 비용을 절감할 수 있습니다. 보안 벤더를 알아볼 때는 다음이 가능한 벤더를 찾아야 합니다.

- 머신 러닝을 이용해 관찰된 트래픽 데이터를 기반으로 레이트 리미트를 설정
- 최신 공격은 IP 리미트를 쉽게 우회할 수 있으므로 지역 및 IP 위치 기반 레이트 리미트를 넘어서기
- 개발자가 모든 웹 애플리케이션 및 공개 API 트래픽을 WAF 및 API 게이트웨이를 통해 라우팅할 수 있도록 지원
- DDoS, WAF, API 게이트웨이 도구를 통합하여 보다 계층화된 위협 방어 구축
- 기업에서 트래픽을 처리할 때 보호 기능이 제 역할을 하도록 하여 대기 시간 단축
- 무제한 DDoS 완화 서비스를 제공하여 초과 수수료 지불을 없앰

올바른 벤더/보안 전략을 구축하면 연간 수백만 달러는 아니더라도 수천 달러를 절감할 수 있음.

Flutter™

요점

API 보안 실패는 **연간 최대 750억 달러의** 비용 유발

올바른 애플리케이션 보안 도구를 도입하면 **연간 수백만 달러는 아니더라도 수천 달러를 절감할 수 있음**

LendingTree에서는 DDoS 방어를 도입한 후 48시간도 채 되지 않아 특정 API 공격이 70% 감소하고, 5개월도 되기도 전에 공격 차단을 통해 250,000달러를 절감했음

Cloudflare Bot Management를 통해 Flutter는 악의적 트래픽을 90% 줄이고, 연간 2백만 파운드 이상을 절감

대역폭, 클라우드, 송신 수수료 등 예기치 않은 수수료와 비용 제거

많은 보안 서비스에서 클라우드에 의존하고 있고, 많은 클라우드 공급자가 기업에 스토리지 및 컴퓨팅 비용을 청구합니다. 기업에 데이터 전송 수수료를 청구하는 경우도 자주 있으며, 이는 스토리지의 데이터를 전송할 때 발생하는 비용입니다.

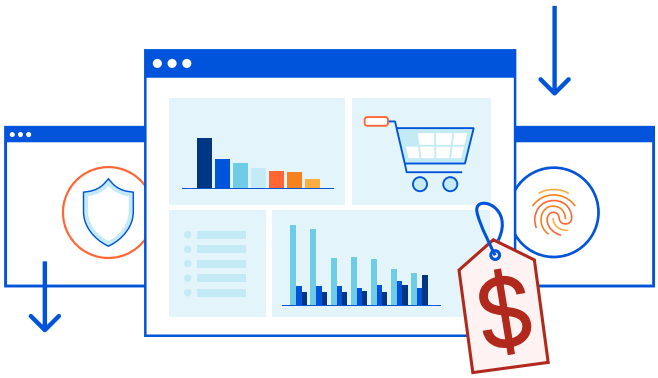
전송 수수료는 고객 등급, 구독 유형, 전송 데이터량 등 여러 요인에 따라 계산됩니다. 따라서 이러한 수수료의 발생 추세를 예측하기가 어렵고, 수수료가 급증하면 조직에 큰 부담이 됩니다. 실제로 IDC에서는 클라우드 스토리지 비용 중 6% 이상을 수수료 비용이 차지할 것으로 추정합니다.

이를 고려해 유럽의 디지털 디렉터리 및 로컬 검색 서비스 업체 PagesJaunes에서는 Cloudflare CDN을 도입하여 대역폭 수수료를 줄이고 캐시 및 DNS 관리를 개선하기로 했습니다.

"Cloudflare CDN이 트래픽을 흡수해 준 덕분에 회사 인프라의 부하가 줄고 탄력성이 증가하는 효과가 즉시 나타났습니다"라고 아키텍처, 성능, 보안 책임자 Loïc Troquet는 이야기합니다. "**70%의 대역폭은 더 이상 Solocal의 인프라를 통해 서비스할 필요가 없습니다.**"

이 대역폭 절감은 비용 절감으로 이어집니다. Cloudflare의 CDN, DNS, WAF, DDoS 완화 서비스를 도입한 후, 온라인 학습 및 연구 도구 **Quizlet에서는 매일 총 대역폭 중 10TB 이상을 절감하고 Google Cloud Services 네트워크를 이용한 전송 비용을 50% 이상 낮췄습니다**.

애플리케이션 보안 전략과 방식을 구축하면 예기치 않은 전송 수수료를 방지할 수 있습니다.



PagesJaunes

Quizlet

요점

올바른 CDN 벤더를 선정하는 등 애플리케이션 보안 전략을 구축하면 예기치 않은 전송 수수료를 없앨 수 있습니다

Cloudflare CDN을 통해 PagesJaunes에서는 대역폭을 70% 줄였습니다

Quizlet은 Cloudflare를 **이용해 매일 10TB 이상의 총 대역폭을 줄이고 있으며**, Google Cloud Services 네트워크 전송 수수료를 50% 이상 절감하여 매달 수천 달러를 아끼고 있습니다

Cloudflare를 통한 애플리케이션 보안 간소화 및 비용 절감

Cloudflare를 통해 조직에서는 애플리케이션 보안 전략을 구축하여 효율을 개선하고 비용을 줄일 수 있습니다. Cloudflare의 통합 애플리케이션 보안 포트폴리오는 동급 최강의 무제한 DDoS 방어, 최신 공격을 막아내는 웹 애플리케이션 방화벽, 선제적인 API 보안, 위협 인텔리전스를 기반으로 한 봇 관리, 첨단 클라이언트 측 공격 감지를 모두 제공합니다.

관심이 있으신가요?

귀사 은행의 온라인 보안을 강화하려면

CLOUDFLARE

+82 70 4515 6893 | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES/4588.2023JUN05