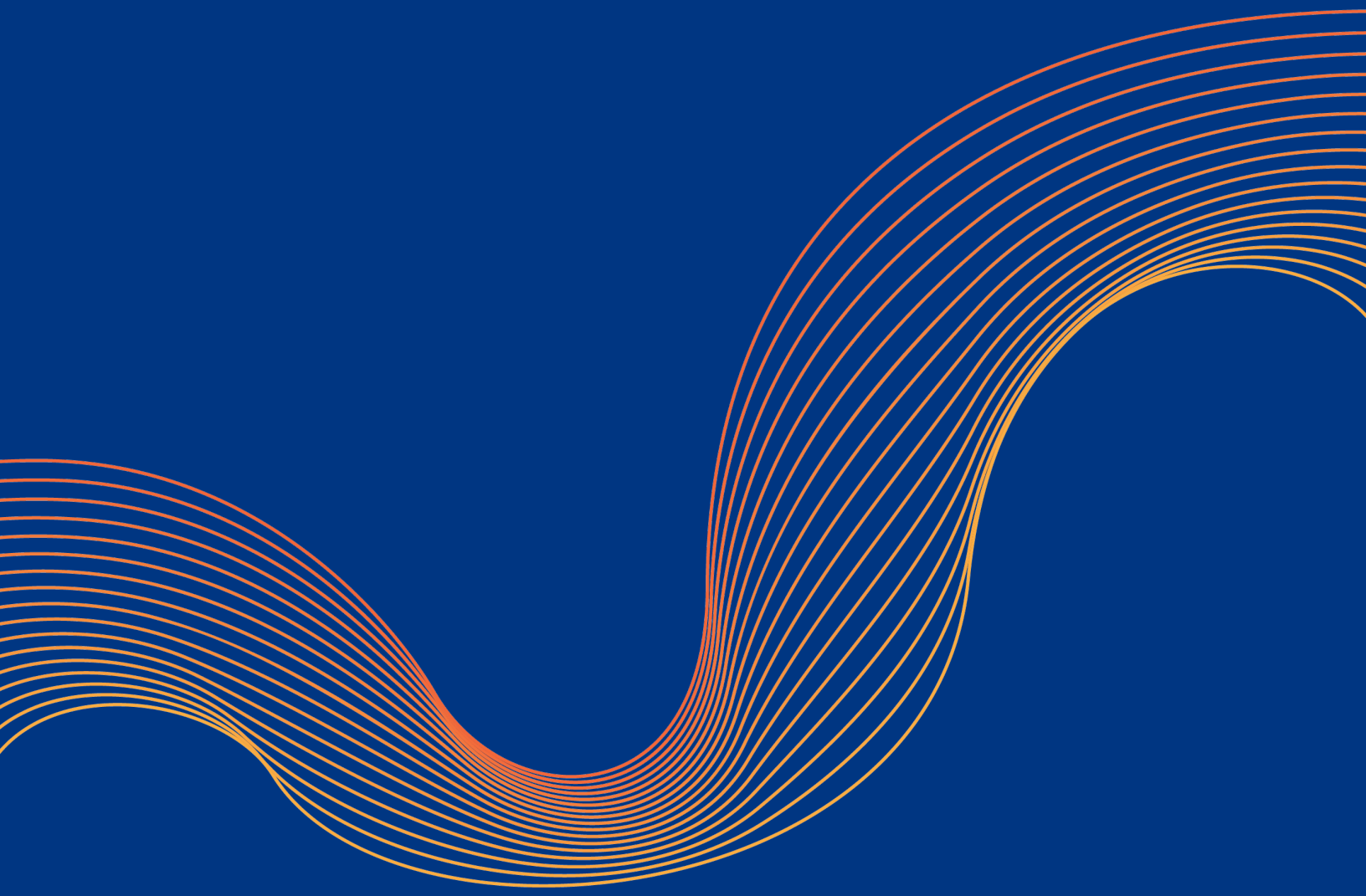
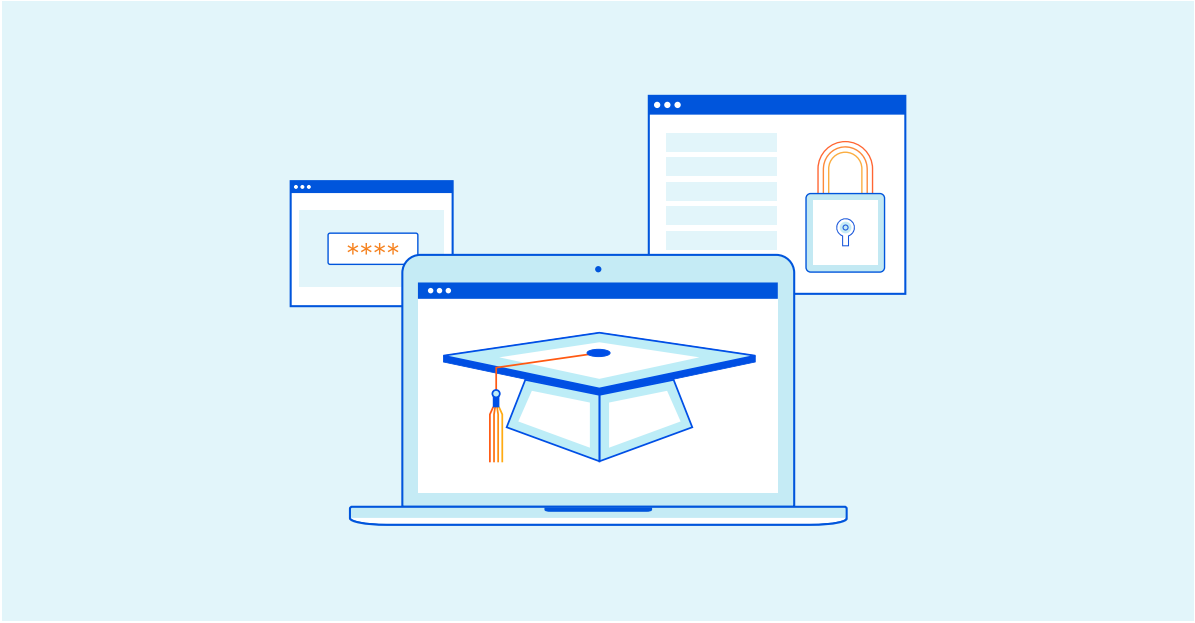
백서

CLOUDFLARE

안전하고 확장 가능한 원격 학습 인프라 설계



+82 70 4515 6893 | enterprise@cloudflare.com | www.cloudflare.com/ko-kr/



소개

최근 몇 년 동안 원격 학습은 더욱 대중적인 교육 모델이 되었습니다.
COVID-19 팬데믹이 시작되면서 학생과 교직원을 바이러스로부터 안전하게 보호하기 위해 많은 교육 기관들이 원격 학습으로 전환해야 했고, 혼합형 및 완전 원격 학습 모델로의 전환은 더욱 가속화되었습니다.

원격 학습에는 전통적인 대면 학습과는 다른 접근 방식이 필요합니다. 교육자들은 강의, 비디오, 대화형 콘텐츠 등 다양한 스타일과 유형의 학습 콘텐츠를 이용할 수 있어야 합니다. 또한, 학급의 모든 학생이 공유된 콘텐츠를 동시에 빠르게 이용할 수 있어야 합니다.

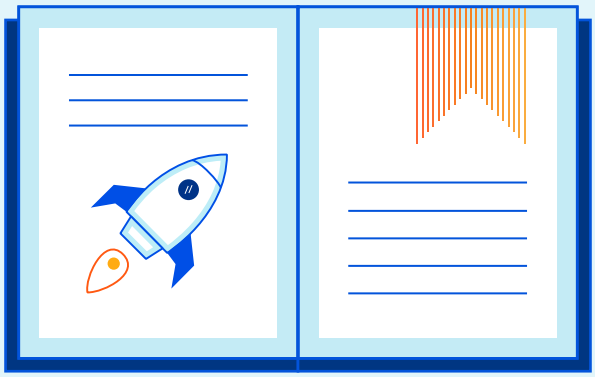
기술적 측면에서, 교육 기관은 이처럼 광범위한 콘텐츠 유형을 지원할 수 있어야 하며, 학생들이 필요할 때 시스템이 작동하도록 보장해야 합니다.
따라서 다음과 같은 다양한 과제를 해결해야 합니다.

- 대규모 콘텐츠 전달
- 분산 서비스 거부 공격 완화
- 계정 탈취 방지
- 악의적 콘텐츠 및 맬웨어 차단

대규모 콘텐츠 전달

원격 학습에서는 학교의 IT 인프라가 조직 운영의 필수적인 요소가 됩니다. 교육자들 입장에서는 많은 학생들에게 동시에 콘텐츠를 제공할 수 있어야 하고, 그러한 콘텐츠를 전달하는 데 필요한 시간이 최소화되어야 합니다.

교육자들은 학생들에게 다양한 컨텐츠를 전달할 수 있어야 합니다. 여기에는 정적 웹 페이지부터 온라인 학습 도구와 스트리밍 비디오 등의 동적 콘텐츠까지 모든 것이 포함됩니다. 교육 기관의 IT 인프라는 이러한 콘텐츠를 멀리 있는 학생에게 효율적이고 신속하게 전달할 수 있어야 합니다.



정적 콘텐츠

교육자들이 학생들에게 제공해야 하는 콘텐츠 중에는 정적인 것이 있습니다. 여기에는, 포함된 정보가 변경되지 않고 자주 업데이트할 필요가 없는 웹 페이지가 포함됩니다.

이러한 유형의 콘텐츠에서는 확장성 및 대기 시간이 IT 부문의 주요 과제입니다. 많은 학생들이 동시에 동일한 컨텐츠에 액세스하려고 시도하려고 할 때 웹 서버가 유지될 수 있습니까? 또한, 원격 학습에서 웹 서버의 위치가 중요할 수도 있습니다. 학생과 서버의 거리가 멀어지면 콘텐츠 전송의 대기 시간도 길어집니다.

정적 컨텐츠의 경우, 콘텐츠의 로컬 캐시를 작성할 수 있으면 이러한 문제를 완화할 수 있습니다. 학생이 특정 페이지를 자주 방문할 경우, 해당 페이지의 사본을 로컬로 저장하면 필요할 때 빠르게 액세스할 수 있습니다.

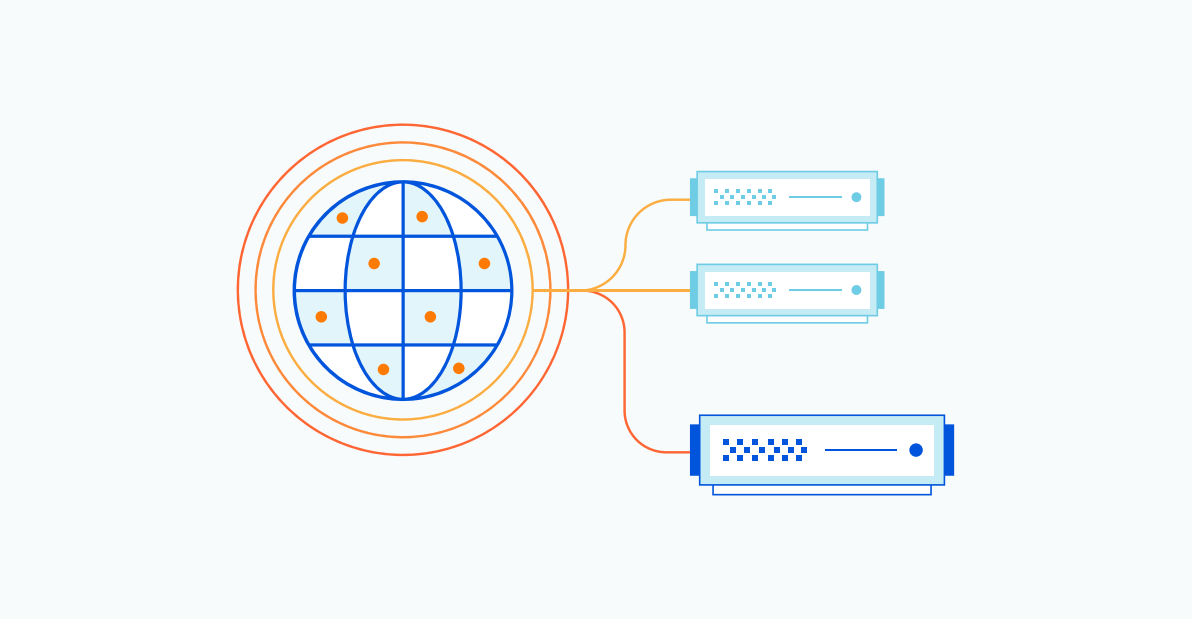
CDN(콘텐츠 전송 네트워크)을 이용하여 대규모로 캐시를 구현할 수도 있습니다.
CDN은 정적 콘텐츠의 로컬 사본을 저장하고 정기적으로 업데이트 하는 노드들의 네트워크로 구성됩니다. 전 세계를 대상으로 하는 CDN은 효과적인 원격 학습에 필요한 확장성과 짧은 대기 시간을 제공합니다.

동적 및 대화형 콘텐츠

정적 컨텐츠와 마찬가지로 대화형 온라인 학습 및 기타 콘텐츠에도 확장성에 대한 문제가 잠재하고 있습니다. 그러나 이러한 유형의 콘텐츠에 대해서, CDN 노드로 구성된 네트워크를 사용할 수 없습니다. 콘텐츠의 업데이트가 빈번하거나 거의 항상 필요한 경우, CDN 노드가 업데이트된 버전을 얻기 위해 메인 웹 서버를 계속 쿼리할 것이기 때문입니다. 그 결과, 사용자의 대기 시간이 길어지고 메인 웹 서버가 압도될 수도 있습니다.

동적 콘텐츠의 확장성 문제는 CDN이 아니고 로드 밸런싱을 통해 해결할 수 있습니다. 하나의 서버로 학생들의 요청을 처리하는 것이 아니고 다수의 서버에 트래픽을 분산시켜 처리하는 것입니다. 이렇게 하면 어떠한 서버도 압도되지 않으며 대기 시간은 최소화됩니다.

이 방식이 효과를 보려면, 로드 밸런스된 서버는 완전히 독립적으로 작동하거나 로드 밸런스된 다른 장치에만 의존할 수 있어야 합니다. 모든 서버가 동일한 데이터베이스 서버를 사용하도록 설정되어 있다면, 데이터베이스 서버가 병목 지점이 될 것이며 로드 밸런스된 서버를 추가한다고 해도 그 효과는 전혀 없거나 미미할 것입니다. 원격 학습 솔루션은 필요할 때 확장 가능하고 로드 밸런싱의 이점을 완전히 누릴 수 있도록 신중하게 설계해야 합니다.

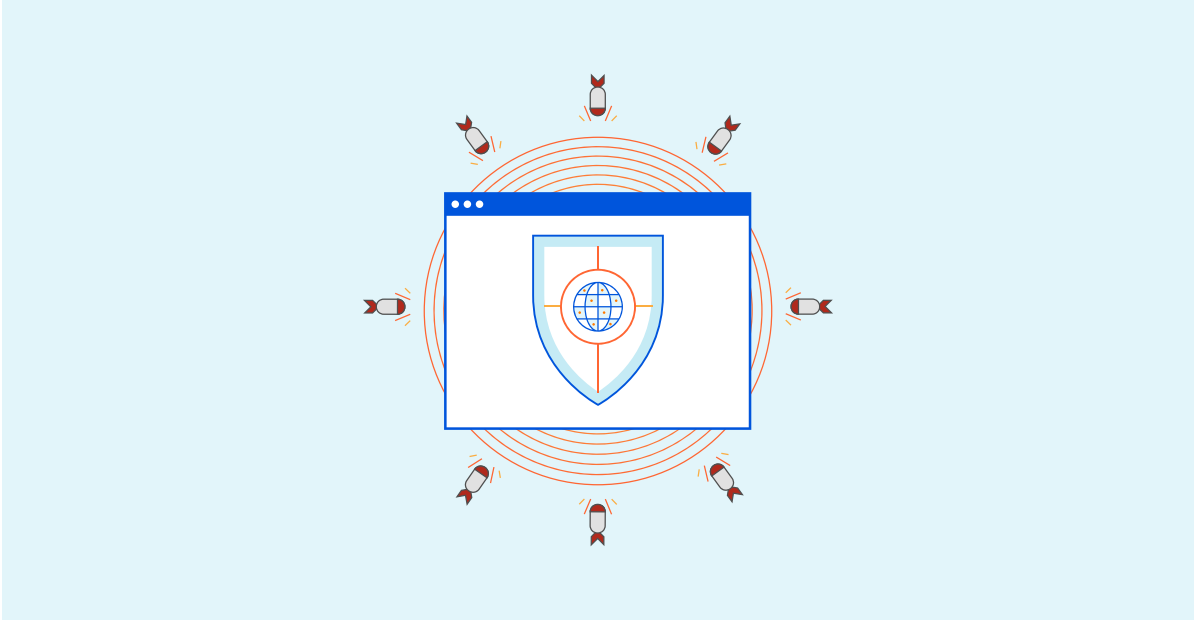


분산 서비스 거부 공격

사용자가 웹 자산에 액세스하면 해당 장치는 DDoS(분산 서비스 거부) 공격이 크게 증가하는 해당 자산 도메인을 찾는 DNS 확인자에 쿼리를 보냅니다. 사물 인터넷(IoT)과 클라우드 컴퓨팅이 확산되면서 공격자들이 인터넷에 연결된 컴퓨팅 파워를 확보하는 것이 저렴해지고 용이해지고 있습니다. 이러한 손상된 장치를 사용하여 악성 트래픽을 발송하여 합법적인 요청에 응답할 수 없게 만드는 것입니다.

원격 교육의 경우, DDoS 공격은 서비스 제공 기능에 상당한 위험을 가져옵니다. 2020년 상반기에 많은 조직이 원격 학습으로 전환하면서 온라인 교육 자원에 대한 DDoS 공격이 350% 증가했습니다[1].

랜섬 요소를 포함하여 발전한 DDoS 공격도 있습니다.
공격자가 DDoS 공격으로 조직을 위협하면서 공격을 하지 않을 테니 대가를 달라고 요구하는 것입니다. 이러한 위협 중 상당수는 근거 없는 것입니다. 하지만 DDoS 방어 기능을 갖추지 못한 교육 기관 입장에서는 이를 무시하기에는 인프라에 대한 위험이 너무 크다고 생각할 수 있습니다.

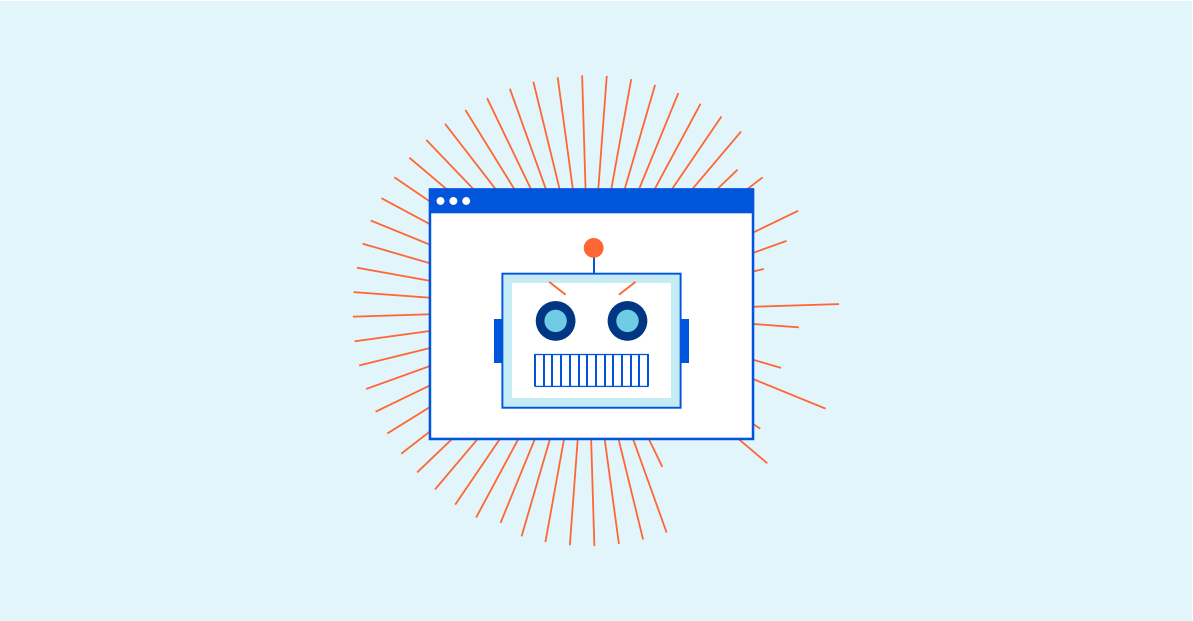


다행히도 상대적으로 예산이 경직된 교육 기관들도 다양한 효과적인 DDoS 완화 전술을 이용할 수 있습니다. 고려해야 할 점들:

- 큰 완화 용량: 조직에서 필요할 것으로 예상하는 보호에 대한 비용만 지불한다면 구미가 당기기는 하지만, 이렇게 한다면 예기치 않은 대형 공격이 발생하는 경우에 서비스를 업그레이드하는 데 걸리는 시간으로 인해 가동 중단 시간이 길어질 수 있습니다.
- 분산 완화: DDoS 트래픽 스크러빙은 분산되어야 합니다. 조직의 모든 트래픽이 하나의 중앙 집중식 위치를 통해 필터링된다면 이는 확장성이 없으며 네트워크 대기 시간이 증가할 수 있습니다.
- 주문형 보호와 상시 보호 비교: 주문형 DDoS 완화에서는 트래픽이 공공 인터넷에서 조직의 서버/네트워크 인프라로 정상적으로 흐르지만, 잠재적인 공격이 감지되면 트래픽을 철저하게 검사하고 필터링하기 시작합니다. 한편, 상시 보호에서는 항상 모든 트래픽을 필터링합니다. 상시 완화는 주문형 서비스보다 비싸지만, 서비스를 수동으로 켜야 하는 일이 없기 때문에 보호 기능이 중단되는 일이 없고 응답 시간이 빠릅니다.

DDoS 완화 전략에 대한 자세한 내용은 Cloudflare Resource Hub에 있는 "DDoS 공격 완화의 5가지 모범 사례" 문서를 참조하시기 바랍니다.

[1] https://www.infosecurity-magazine.com/news/ddos-attacks-on-virtual-education/



계정 탈취

사이버 공격 중에는 시스템 상의 합법적인 사용자 계정을 탈취하여 시작하는 것이 많습니다. 계정 탈취 공격에는 네트워크, 응용 프로그램 등의 시스템에서 합법적인 사용자 자격 증명 정보를 손상하는 일이 포함됩니다. 공격자는 피싱 공격, 자격 증명 스터핑 등 다양한 방식으로 계정 자격 증명 정보에 액세스할 수 있습니다.

이러한 자격 증명 정보를 사용하여 합법적인 사용자로 가장하여 맬웨어를 심거나 데이터를 훔치거나 하는 등 대상 시스템에서 추구하고자 하는 목표를 달성하게 됩니다. 아동의 온라인 개인정보 보호법(COPPA), 가족 교육권 및 개인정보 보호법(FERPA) 등의 규제에 의해 보호되는 데이터에도 접근할 수 있습니다. 또한, 이를 통해 중요한 학생 기록을 삭제하거나 이를 보유하며 랜섬웨어를 이용해 대가를 요구할 수 있습니다.

교육 기관은 알려진 악성 콘텐츠를 감지하는 것은 물론, 기계 학습을 이용해 의심스러운 언어 및 기타 알 수 없는 위협을 감지함으로써 공격을 감지할 수 있는 피싱 완화 솔루션을 배포해야 합니다. 이러한 접근 방법에는 이메일 스캐닝이 있으며 알려진 악성 사이트를 차단하고 사용자가 특정 유형의 파일을 다운로드하지 못하도록 보안 웹 게이트웨이를 사용하는 방법도 있습니다.

자격 증명 스터핑

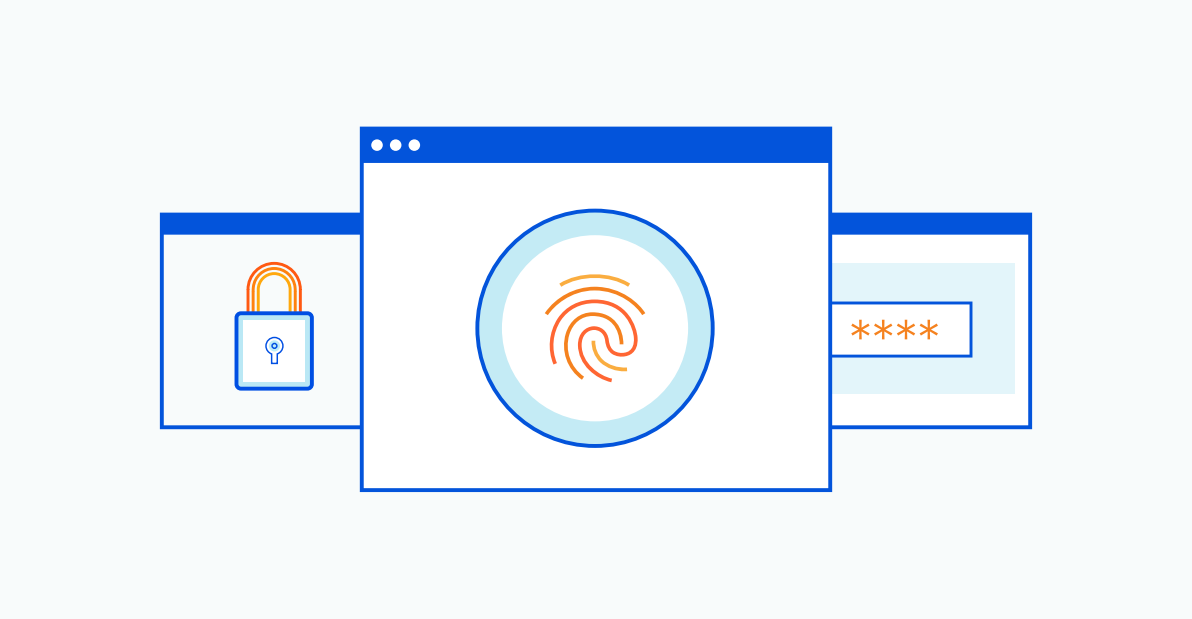
한편, 공격자는 가상 사설 네트워크(VPN), 원격 데스크탑 프로토콜(RDP), 웹 액세스 포털 등 일반에 공개하는 로그인 시스템을 활용하여 사용자 자격 증명 정보를 손상시킬 수도 있습니다. 일반적인 사용자는 13개의 온라인 계정에 대해 동일한 로그인 자격 증명을 사용하며[2] 복잡하지 않으면서 쉽게 추측할 수 있는 암호를 사용하는 것이 일반적입니다. 자격 증명 스터핑 공격은 자동화된 봇을 사용하여 이러한 인증 포털에서 사용자의 비밀번호를 맞추려 시도합니다. 성공하면 합법적인 로그인 자격 증명 정보를 알게 되므로 합법적인 사용자 계정에 액세스할 수 있게 됩니다. 자격 증명 스터핑 공격은 자동화를 활용하므로 이러한 유형의 공격으로부터 보호하려면 로봇 감지 솔루션이 필요합니다. 그러나 좋은 봇과 나쁜 봇을 구별하는 것도 중요합니다.

[2] *https://www.lastpass.com/state-of-the-password/global-password-security-report-2019*

다양한 상이한 방법으로 봇을 감지하고 차단할 수 있습니다. 악의적인 봇 완화 전략의 기본 요소는 다음과 같습니다.

- **속도 제한:** 특정 IP 주소가 사이트 또는 네트워크에 요청을 제출할 수 있는 횟수를 제한합니다. 이는 비교적 단순한 무차별 대입 봇 공격에 가장 효과적입니다.
- **캡차 2단계 인증:** 이 두 가지 방법 모두 봇이 페이지에 로그인하지 못하도록 할 수 있지만, 사용자 경험에 부정적인 영향을 줄 수도 있습니다.
- **봇 차단 목록 및 허용 목록 유지:** 알려진 악성 로봇을 추적하고 검색 엔진 크롤러 등의 양호한 봇은 여전히 과업을 수행할 수 있도록 하기 위한 것입니다.

그러나, 이러한 전술이 전문화된 특수 봇에는 효과가 없는 경우가 있습니다. 봇 완화에 대한 자세한 내용은 Cloudflare Resource Hub에 있는 " 악성 봇 플레이북을 참고하십시오.

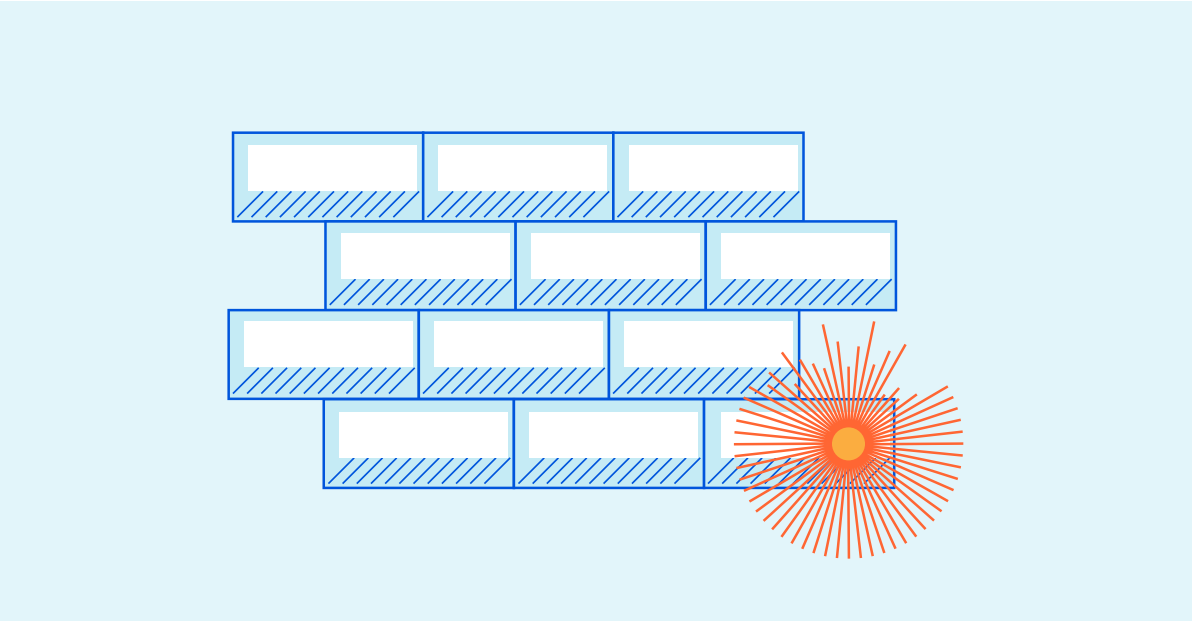


악성 콘텐츠 및 맬웨어

교육자들이 원격 학습을 수용함에 따라 공공 인터넷에 노출되는 시스템이 증가할 것입니다. 학생들은 웹 응용 프로그램을 통해 온라인 학습을 활용할 수 있습니다. 원격 학습자와 교육자는 VPN, RDP및 유사한 솔루션을 이용하여 원격 네트워크 및 컴퓨터에 액세스할 수도 있습니다. 이러한 시스템도 사이버 위협으로부터 보호해야 합니다.

웹 응용 프로그램 보안

교육용 웹 응용 프로그램은 중요한 데이터에 광범위하게 액세스하기도 합니다. COPPA, FERPA 및 유사한 법률의 적용을 받는 학생 데이터가 이들 플랫폼에 저장될 수 있으므로 교육 기관은 이러한 정보를 적절히 보호해야만 합니다.



이러한 응용 프로그램은 소프트웨어이므로 취약성이 악용될 소지가 있습니다. 이러한 응용 프로그램을 사이버 공격으로부터 보호하려면 네트워크 트래픽을 검사하여 해당 소프트웨어의 버그를 악용하려는 시도를 감지하고 차단해야 합니다.

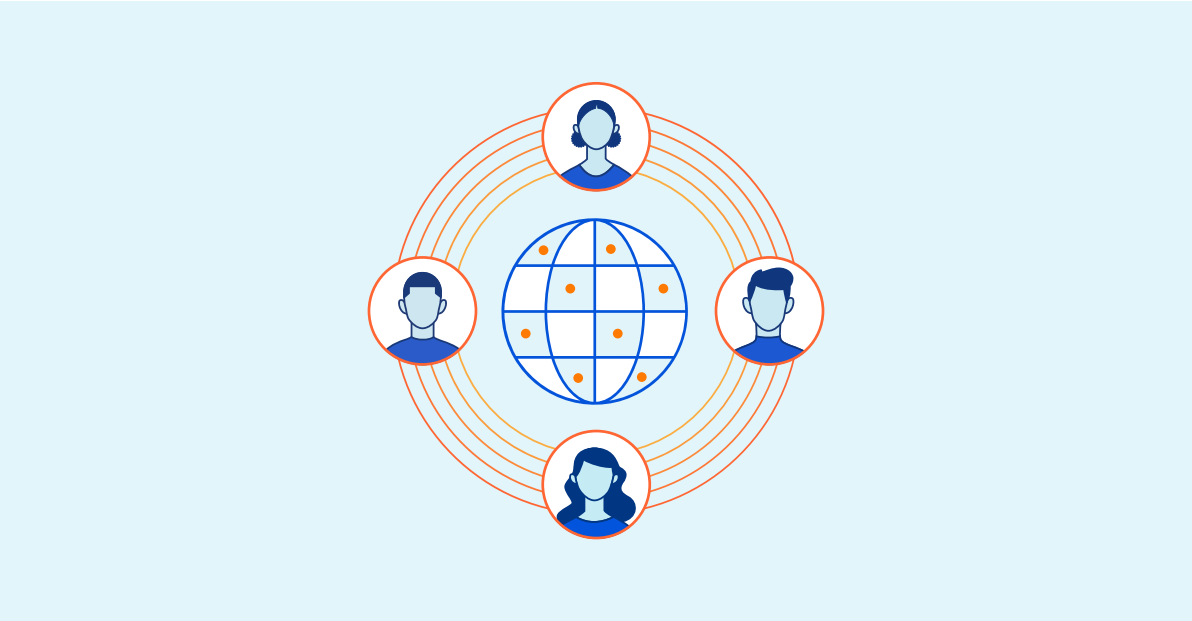
웹 애플리케이션 방화벽(WAF)은 다양한 웹 응용 프로그램의 다양한 취약성을 보호합니다. 서명 기반 감지와 기계 학습을 조합하여 사용함으로써 알려진 공격과 신규 공격을 모두 식별할 수 있습니다. 따라서 웹 기반 인프라에 대한 제로 데이 공격에 대해서도 보호할 수 있게 됩니다.

안티 랜섬웨어 보호

랜섬웨어는 가장 빠르게 증가하고 있는 맬웨어 유형 중 하나입니다. 랜섬웨어가 컴퓨터에 액세스하게 되면 컴퓨터에 저장된 파일을 암호화한 후 이를 복구하기 위한 대가를 요구합니다. 학교가 즉시 대가를 지불할 수 있는 경우라고 해도 영향 받은 시스템을 복구하려면 상당한 시간과 비용이 필요할 수 있습니다.

랜섬웨어는 VPN및 RDP와 같은 원격 액세스 기술을 통해 침투하는 경우가 증가하고 있습니다. 합법적인 로그인 자격 증명을 확보한 공격자는 이를 이용하여 컴퓨터에 로그인하고 맬웨어를 설치할 수 있습니다. 맬웨어가 일단 조직의 네트워크에 들어오게 되면, 확산되어 네트워크 상의 다른 컴퓨터들을 감염시키는 것이 일반적입니다.

교육 기관에는 업무용 네트워크 트래픽을 모두 검사할 수 있는 방화벽 솔루션이 필요합니다. 이렇게 함으로써 유입되는 악의적 콘텐츠(예: 랜섬웨어)가 조직의 컴퓨터를 감염시키기 전에 차단하고 (보호된 학생의 개인 데이터를 포함한) 데이터 빼내기 시도를 차단할 수 있습니다.



Cloudflare를 사용한 원격 학습 보안

COVID-19 팬데믹은 언젠가 지나가겠지만, 원격 학습으로 쉽게 전환할 수 있는 능력은 교육 기관에 소중한 역량입니다. 온라인 학습 자원은 강의실 내 대면 교육에서도 이용할 수 있는 소중한 자산이며, 일단 원격 학습에 필요한 인프라를 갖추게 되면 악천후 등 예상치 않은 사건으로 인해 학교를 이용할 수 없을 경우에도 회복력이 뛰어납니다.

Cloudflare는 사용자 친화적인 통합 플랫폼과 모든 교육 기관에 공통된 IT및 보안 문제에 대한 솔루션을 함께 제공합니다. 교육 기관은 Cloudflare와 같은 단일의 통합 솔루션을 활용함으로써 불필요한 복잡성을 피하면서 예기치 않은 시나리오에 적응하는 탄력성을 높일 수 있습니다. Cloudflare는 다음을 제공합니다.

- 글로벌 콘텐츠 전송 네트워크: 전세계 200개 도시에 있는 데이터 센터를 활용
- 47Tbps의 DDoS 방어 용량과 네트워크 에지에서의 상시 가동 완화 기능.
- Cloudflare의 네트워크에서 약 2500만개의 인터넷 자산으로부터 위협 인텔리전스를 지속적으로 수집하는 웹 애플리케이션 방화벽.
- 고급 봇 완화: 기계 학습 및 지문을 사용하여 네트워크에서 트래픽 패턴을 분석하고 첨단 봇도 감지.
- 보안 웹 게이트웨이: 네트워크 에지에서 작동하여 지리적으로 격리된 데이터 센터로 트래픽을 이동시킴으로써 발생하는 대기 시간 감축.

자세한 내용은 www.cloudflare.com를 참조하시기 바랍니다.