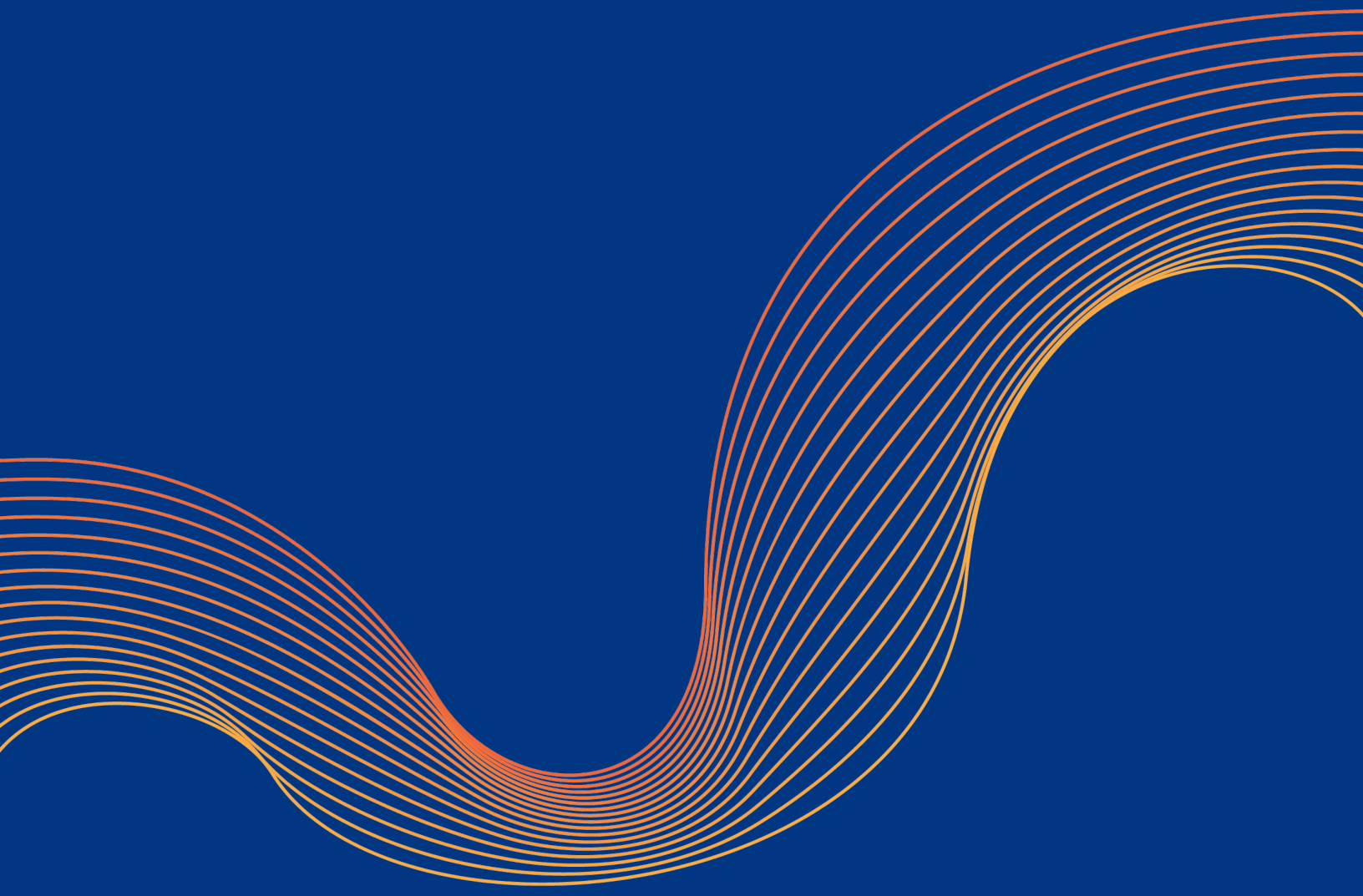
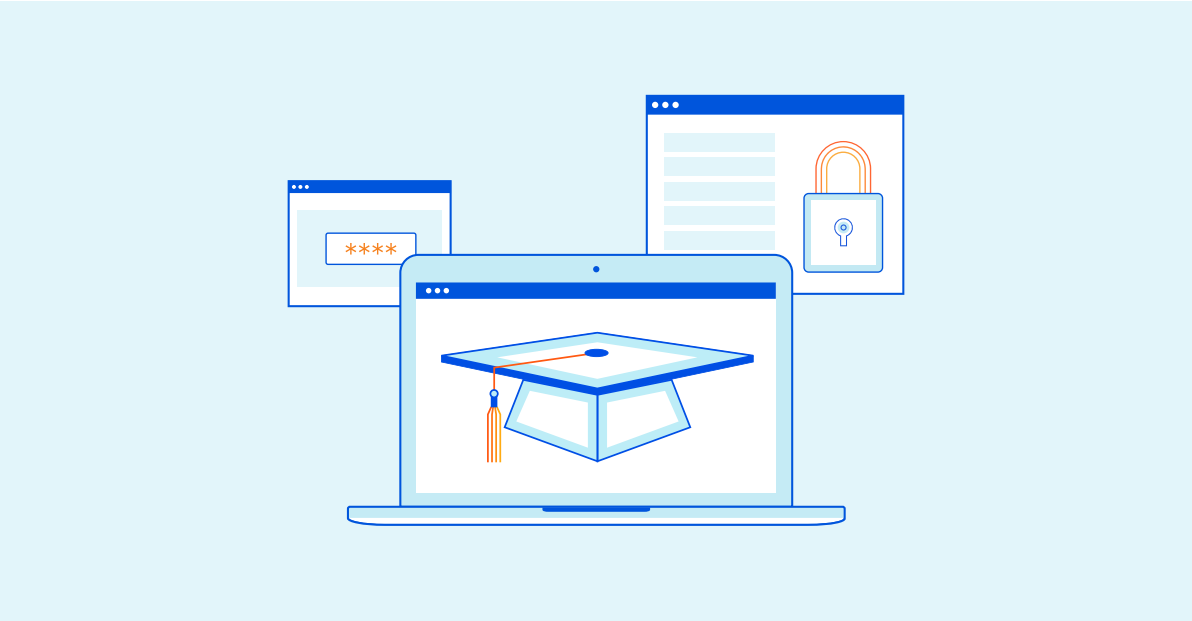
WHITEPAPER

CLOUDFLARE

Progettazione di un'infrastruttura di apprendimento remota, sicura e scalabile



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com/it-it/



Introduzione

Negli ultimi anni, l'apprendimento a distanza è diventato un modello didattico sempre più comune. La pandemia di COVID-19, che ha costretto molte istituzioni a passare all'apprendimento a distanza per proteggere studenti ed insegnanti dal virus, ha accelerato la transizione a modelli di apprendimento ibridi e completamente remoti.

L'apprendimento a distanza richiede un approccio molto diverso rispetto all'istruzione tradizionale in presenza. Gli insegnanti devono essere in grado di supportare una serie di stili di apprendimento e tipi di contenuti diversi, tra cui conferenze, video, contenuti interattivi e altro ancora. Con l'apprendimento a distanza, tutti gli studenti di una classe devono poter accedere rapidamente e simultaneamente ai contenuti condivisi.

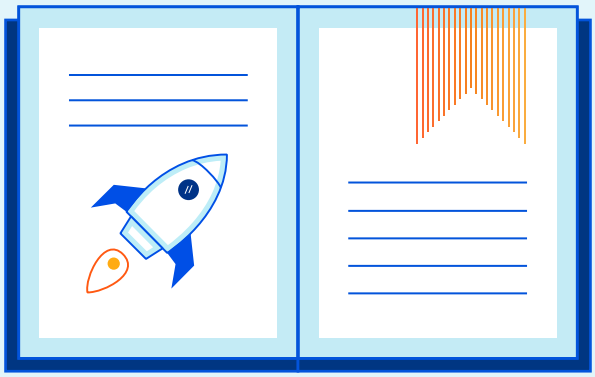
Dal punto di vista tecnico, un istituto scolastico deve essere in grado di supportare questa varietà di tipi di contenuti e garantire che i sistemi funzionino correttamente quando gli studenti ne hanno bisogno.
Ciò richiede di affrontare una serie di problemi, tra cui:

- Distribuzione di contenuti su larga scala
- Mitigazione degli attacchi DDoS
- Impedire l'acquisizione di account
- Blocco di contenuti dannosi e malware

Distribuzione di contenuti su larga scala

Con l'apprendimento a distanza, l'infrastruttura IT delle scuole è diventata una componente fondamentale della capacità operativa dell'organizzazione. Gli insegnanti devono poter fornire contenuti a più studenti contemporaneamente e garantire che questi contenuti siano distribuiti con una latenza minima.

Devono inoltre essere in grado di fornire ai propri studenti un'ampia gamma di contenuti. Ciò include tutto quello che va dalle pagine Web statiche ai contenuti dinamici, come strumenti di apprendimento online interattivo e video in streaming. L'infrastruttura IT di un istituto scolastico deve essere in grado di fornire in modo efficiente e scalabile questi contenuti ai suoi studenti remoti.



contenuti statici

Alcuni dei contenuti che gli insegnanti devono fornire ai loro studenti sono statici, ad esempio le pagine Web in cui le informazioni incluse non cambiano e non richiedono aggiornamenti frequenti.

Per questi tipi di contenuto, le principali difficoltà con cui ci si scontra sono la scalabilità e la latenza. Se molti studenti provano ad accedere allo stesso contenuto nello stesso momento, il server Web sarà in grado di tenere il passo? Anche la posizione del server Web ha un ruolo molto importante nell'apprendimento a distanza. Più lo studente è lontano dal server, maggiore sarà la latenza nella diffusione del contenuto.

Per i contenuti statici, la possibilità di creare cache di contenuto locali può contribuire a semplificare questi problemi. Se uno studente visita spesso una determinata pagina, è possibile che una sua copia venga memorizzata in locale, consentendo un più rapido accesso quando necessario.

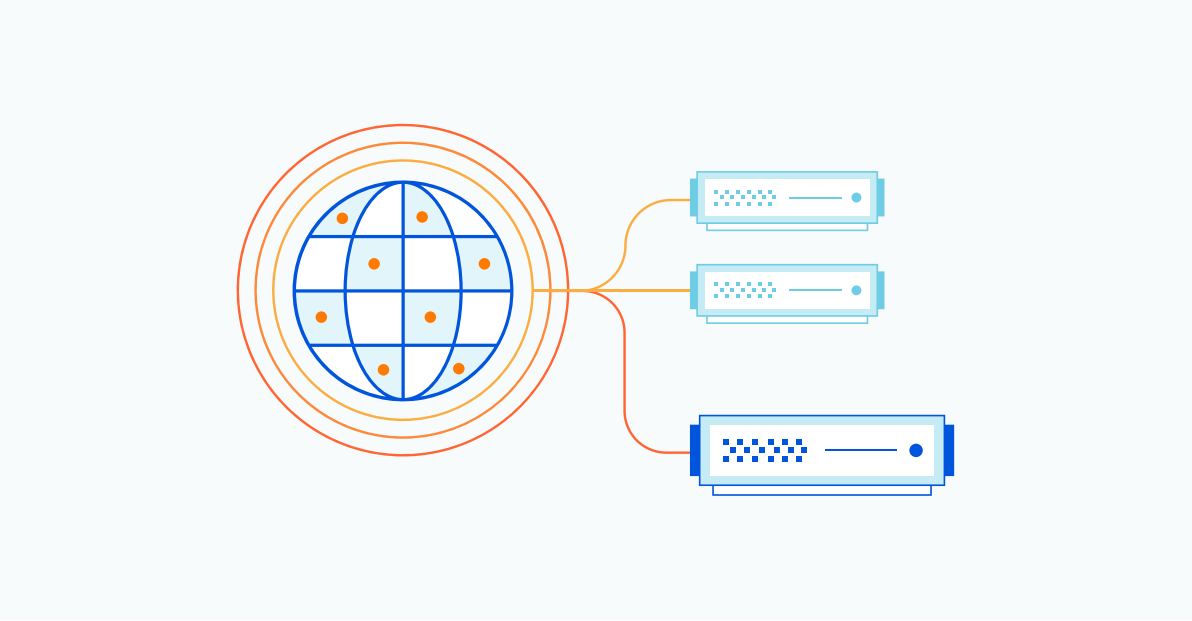
La memorizzazione nella cache può essere implementata anche su larga scala utilizzando una rete di distribuzione dei contenuti (CDN).Una CDN è costituita da una rete di nodi su cui sono memorizzate copie locali di contenuti statici e su cui vengono effettuati periodicamente controlli alla ricerca di aggiornamenti. Una CDN con copertura globale offre la scalabilità e la bassa latenza necessarie per un apprendimento a distanza davvero efficace.

Contenuto dinamico e interattivo

Come i contenuti statici, l'apprendimento interattivo online e altri contenuti presentano potenziali problemi di scalabilità. Tuttavia, l'uso di una rete di nodi CDN non funziona altrettanto bene per questo tipo di contenuto. Se il contenuto richiede aggiornamenti frequenti o quasi costanti, i nodi della CDN interrogheranno continuamente il server Web principale alla ricerca di una versione aggiornata, aumentando in questo modo la latenza per gli utenti e sovraccaricando il server.

I problemi legati alla scalabilità dei contenuti dinamici possono essere invece risolti tramite il bilanciamento del carico. Invece di utilizzare un singolo server per gestire tutte le richieste degli studenti, vengono utilizzati più server con traffico distribuito tra di loro. Ciò garantisce che nessun server venga travolto dal numero elevato di richieste e che la latenza sia ridotta al minimo.

Per essere efficace, un server con carico bilanciato deve poter funzionare in modo del tutto indipendente o affidarsi soltanto ad altri dispositivi con carico bilanciato. Se tutti i server sono impostati per utilizzare lo stesso server di database, è possibile che questo diventi il collo di bottiglia e che i server con carico bilanciato aggiuntivi offrano pochi vantaggi o addirittura nessuno. Le soluzioni di apprendimento a distanza devono essere progettate attentamente in modo da garantire che la scala richiesta sia disponibile quando necessaria e che il sistema sia progettato in modo da offrire tutti i vantaggi del bilanciamento del carico.

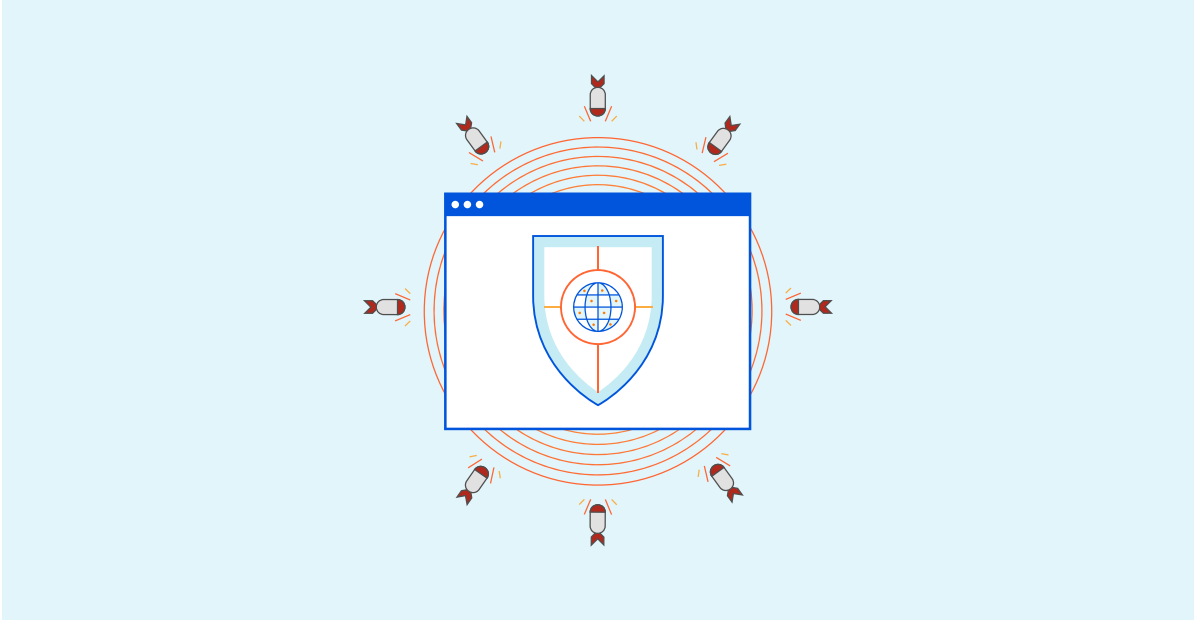


Attacchi Distributed Denial of Service (DDoS)

Gli attacchi Distributed Denial of Service (DDoS) stanno diventando sempre più comuni. Con l'espansione dell'Internet of Things (IoT) e del cloud computing, per gli aggressori è sempre più facile e conveniente accedere alla capacità di elaborazione connessa a Internet. Questi dispositivi compromessi possono quindi essere utilizzati per inviare traffico nocivo a un servizio, impedendo di rispondere a richieste legittime.

Nella formazione a distanza, gli attacchi DDoS rappresentano un rischio significativo per la capacità di fornire servizi. Nella prima metà del 2020, quando molte organizzazioni sono passate all'apprendimento a distanza, gli attacchi DDoS contro le risorse didattiche online sono aumentati del 350%[1].

Inoltre, alcuni attacchi DDoS si sono evoluti in modo da integrare un componente di riscatto. Un aggressore può minacciare un'organizzazione con un attacco DDoS e richiedere un riscatto per bloccare l'attacco. Molte di queste minacce sono infondate, ma un istituto scolastico senza protezione da attacchi DDoS potrebbe ritenere che il rischio per la propria infrastruttura sia troppo elevato da ignorare.

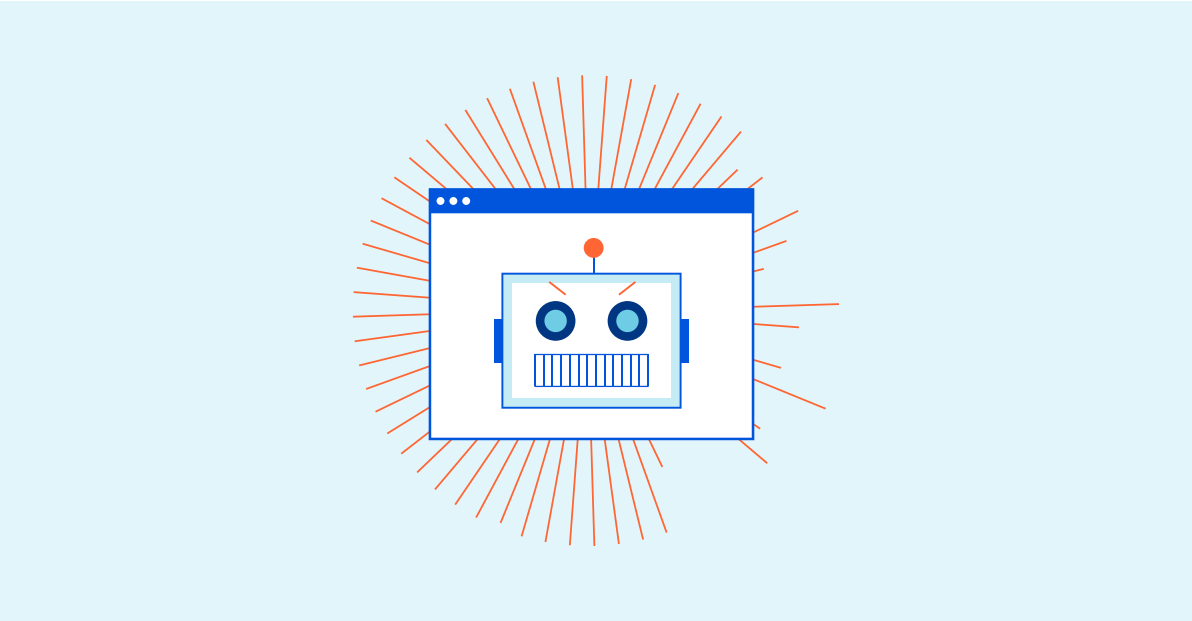


Fortunatamente, anche le organizzazioni formative con budget relativamente rigidi hanno ancora accesso a una varietà di tattiche di mitigazione DDoS efficaci. Le organizzazioni dovrebbero prendere in considerazione:

- Elevata capacità di mitigazione: può essere allettante pagare pagare solo per la protezione prevista dalla propria organizzazione ma se si verifica un attacco inaspettatamente grande, il tempo necessario per l'upgrade del servizio può comportare tempi di inattività aggiuntivi.
- Mitigazione distribuita: lo scrubbing del traffico DDoS deve essere distribuito, poiché l'instradamento di tutto il traffico di un'organizzazione attraverso un unico punto centrale per il filtraggio può non essere scalabile e aumentare la latenza di rete.
- Protezione "on-demand" e "sempre attiva": nella mitigazione DDoS on-demand, il traffico scorre normalmente da Internet pubblico ai server o all'infrastruttura di rete di un'organizzazione fino a quando non viene rilevato un potenziale attacco e a quel punto viene ispezionato e filtrato in modo più approfondito. Nel frattempo, la protezione "sempre attiva" filtra continuamente tutto il traffico. Anche se la protezione "sempre attiva" può essere più costosa dei servizi on-demand, la mitigazione "sempre attiva" offre una protezione senza interruzioni e porta a tempi di risposta più rapidi poiché il servizio non deve mai essere attivato manualmente.

Per maggiori informazioni sulle strategie di mitigazione DDoS, consulta il documento “Cinque best practice per la mitigazione degli attacchi DDoS” nel Centro risorse Cloudflare.

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



Acquisizione degli account

Molti attacchi informatici iniziano con l'acquisizione dell'account legittimo di un utente sul sistema. Gli attacchi con acquisizione di account sono caratterizzati dall'iniziale compromissione delle credenziali utente legittime su rete, applicazioni o altri sistemi. Un aggressore può accedere alle credenziali dell'account in diversi modi, ad esempio con attacchi di phishing o sottrazione e uso illecito delle credenziali.

Con queste credenziali, l'aggressore può mascherarsi da utente legittimo e impiantare malware, rubare dati o raggiungere altri obiettivi sul sistema di destinazione. Ciò può consentire l'accesso ai dati protetti da regolamenti quali il Children's Online Privacy Protection Act (COPPA) e il Family Educational Rights and Privacy Act (FERPA). In alternativa, tale accesso potrebbe consentire agli aggressori di eliminare i record critici degli studenti o di tenerli in mano per richiedere un riscatto tramite ransomware.

Le istituzioni scolastiche devono implementare una soluzione di mitigazione del phishing in grado di rilevare attacchi basati su contenuti nocivi noti e sull'utilizzo del machine learning per rilevare linguaggio sospetto e altre minacce sconosciute. La scansione della posta elettronica è uno di questi approcci; un altro è l'utilizzo di un gateway Web sicuro per bloccare i siti dannosi noti e impedire agli utenti di scaricare determinati tipi di file.

Sottrazione e uso illecito delle credenziali

In alternativa, un aggressore può sfruttare i sistemi di accesso rivolti al pubblico di un'organizzazione come le reti private virtuali (VPN), il protocollo desktop remoto (RDP) o i portali di accesso Web per compromettere le credenziali dell'utente. La persona media utilizza le stesse credenziali di accesso per 13 account online[2] e l'uso di password deboli e facilmente individuabili è molto comune. Gli attacchi con sottrazione e uso illecito delle credenziali utilizzano bot automatici per provare a indovinare la password di un utente su questi portali di autenticazione. In caso di successo, l'aggressore ottiene l'accesso all'account dell'utente perché ora ne conosce le credenziali di accesso.

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

Gli attacchi del genere sfruttano l'automazione e la protezione da questi tipi di attacco richiede soluzioni di rilevamento dei bot. Tuttavia, è anche fondamentale distinguere tra bot buoni e bot cattivi.

I bot possono essere rilevati e bloccati tramite una varietà di metodi diversi. Tra gli elementi di base di una strategia di mitigazione da bot dannosi vi sono:

- **Rate limiting:** consiste nel limitare il numero di volte che un indirizzo IP può inviare richieste a un sito o alla rete. Questo metodo è efficace per attacchi bot brute-force, di natura più semplice.
- **CAPTCHA e autenticazione a due fattori:** Entrambe queste strategie possono impedire a molti bot di accedere alle pagine di accesso. Tuttavia, possono avere anche un impatto negativo sull'esperienza dell'utente.
- **Gestione di blocklist e di allowlist di bot:** questo metodo consente di tenere traccia dei bot dannosi noti e garantisce che i crawler dei motori di ricerca e altri bot non dannosi siano comunque in grado di svolgere le loro attività.

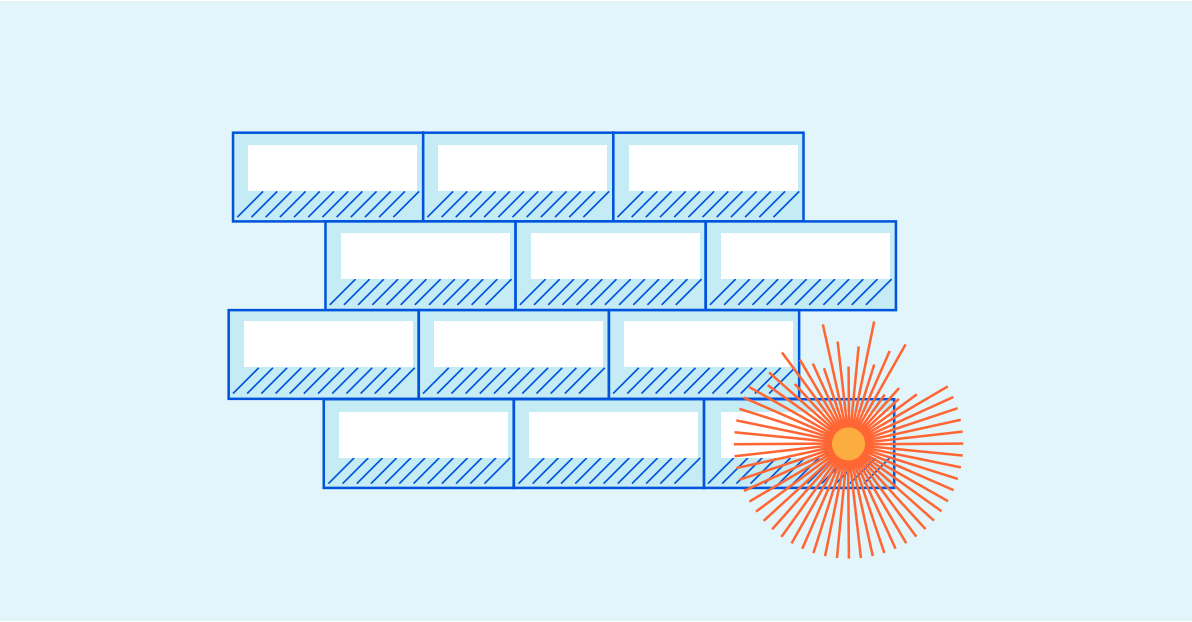
Tuttavia, queste tattiche potrebbero non essere altrettanto efficaci per i bot più avanzati e specializzati. Per maggiori informazioni sulla mitigazione dei bot, consulta il Centro risorse Cloudflare.

Contenuti dannosi e malware

Man mano che gli insegnanti implementano l'apprendimento a distanza, un numero di sistemi sempre maggiore sarà esposto a Internet. Gli studenti possono trarre vantaggio dall'apprendimento online tramite le applicazioni Web. Gli studenti e gli insegnanti remoti possono avere accesso remoto alla rete e al computer anche tramite VPN, RDP e soluzioni simili, pertanto anche questi sistemi devono essere protetti dalle minacce informatiche.

Sicurezza delle applicazioni Web

Le applicazioni Web didattiche possono avere accesso a una vasta gamma di dati sensibili. I dati degli studenti tutelati da COPPA, FERPA e normative simili possono essere archiviati su queste piattaforme, rendendo necessaria per gli istituti scolastici un'adeguata protezione.



Poiché queste applicazioni sono di stampo software, potenzialmente contengono vulnerabilità facilmente sfruttabili. La protezione di queste applicazioni dagli attacchi informatici richiede l'ispezione del traffico di rete per rilevare e bloccare i tentativi di trarre vantaggio dai bug di questi software.

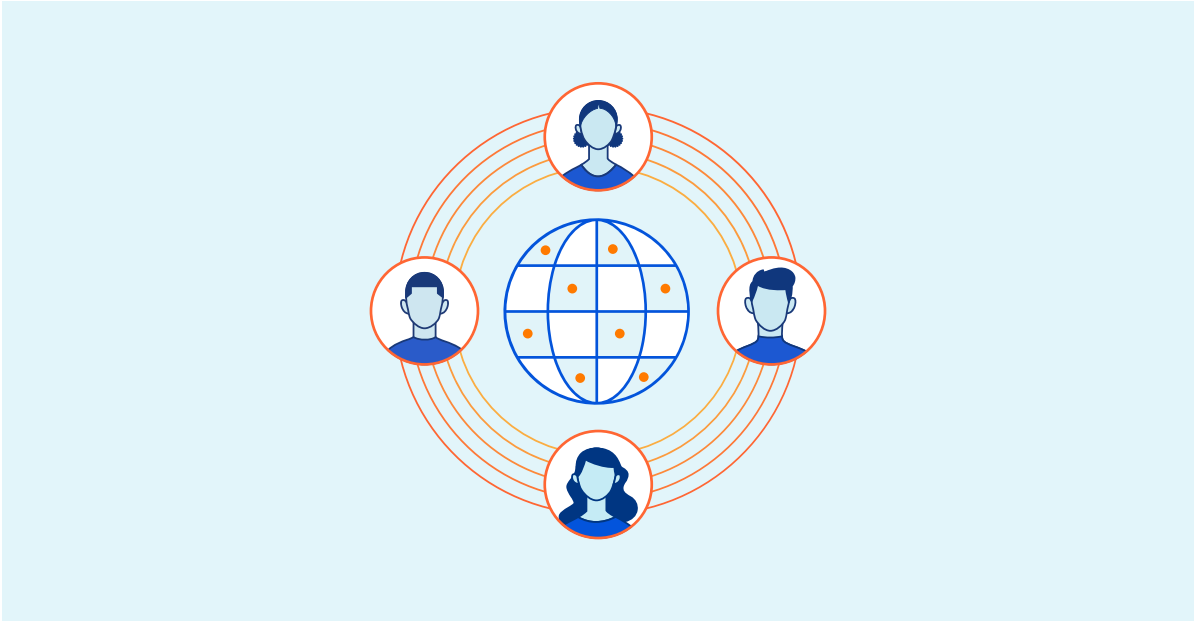
Un Web Application Firewall (WAF) fornisce protezione contro un'ampia varietà di vulnerabilità delle applicazioni Web. Questo firewall può utilizzare una combinazione di rilevamento basato su firma e machine learning per identificare attacchi noti e nuovi. Ciò consente di proteggere l'infrastruttura basata sul Web di un'organizzazione anche dagli attacchi zero-day.

Protezione anti-ransomware

Il ransomware è uno dei tipi di malware in più rapida crescita. Una volta che il ransomware ha accesso a un computer, crittografa i file memorizzati e richiede un pagamento per ripristinare l'accesso. Anche se l'istituto scolastico è in grado di pagare immediatamente il riscatto, il ripristino dei sistemi interessati potrebbe richiedere spese e tempi significativi.

Il ransomware viene distribuito sempre più tramite tecnologie di accesso remoto come VPN e RDP. Un aggressore con accesso alle credenziali di accesso legittime può utilizzarle per accedere a un computer e installarvi malware. Una volta all'interno della rete dell'organizzazione, il malware si diffonde velocemente per infettare altri computer sulla rete.

Gli istituti scolastici richiedono una soluzione firewall che consenta loro di ispezionare tutto il traffico di rete aziendale. Ciò consente loro di rilevare contenuti dannosi in entrata (come il ransomware) prima che infetti i computer di un'organizzazione e di bloccare i tentativi di estrazione dei dati (inclusi i dati personali protetti degli studenti).



Protezione dell'apprendimento a distanza co Cloudflare

Mentre la pandemia di COVID-19 passerà, la capacità di passare facilmente all'apprendimento a distanza sarà preziosa per un istituto scolastico. Le risorse di apprendimento online sono un valore prezioso anche per l'apprendimento in presenza e disporre dell'infrastruttura necessaria per l'apprendimento a distanza rende un'organizzazione resiliente contro le interruzioni causate da intemperie o altri eventi imprevisti.

Cloudflare offre una piattaforma consolidata e intuitiva con soluzioni per tutte le problematiche più comuni legate all'IT e alla sicurezza degli istituti scolastici. Sfruttando un'unica soluzione integrata come quella di Cloudflare, gli istituti scolastici possono evitare una complessità inutile e diventano più adattivi e resilienti agli scenari imprevisti. Cloudflare offre:

- **Una rete globale per la distribuzione di contenuti**, con datacenter in oltre 200 città in tutto il mondo
- **47 Tbps di capacità di mitigazione DDoS**, con mitigazione sempre attiva sul perimetro di rete.
- **Un WAF (Web Application Firewall)** che attinge continuamente all'intelligence sulle minacce dai circa 25 milioni di proprietà Internet sulla rete di Cloudflare.
- **Mitigazione avanzata dei bot**, che utilizza il machine learning e il fingerprinting per analizzare i modelli di traffico nella nostra rete e rilevare i bot più avanzati.
- **Un gateway Web sicuro** che funziona sul perimetro di rete e che riduce la latenza che deriva dal traffico di backhauling verso un datacenter geograficamente isolato.

Scopri di più sul sito www.cloudflare.com.