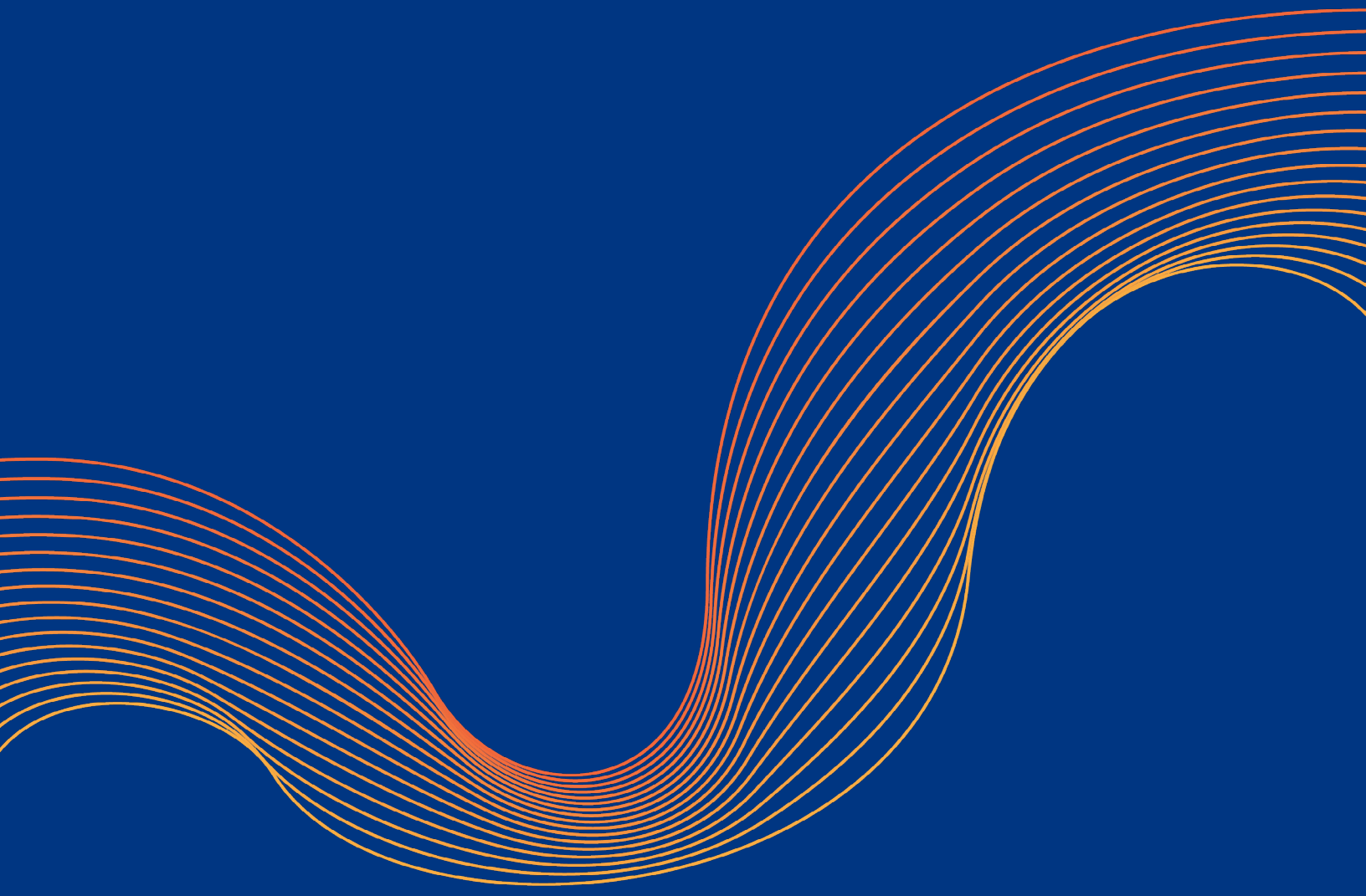
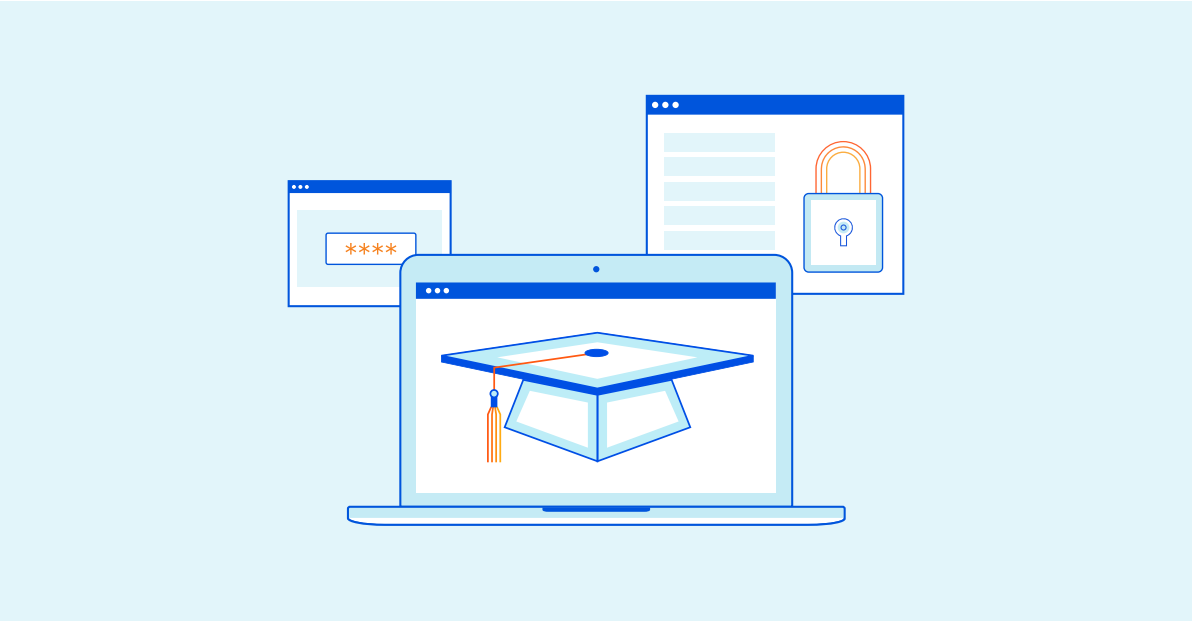
WHITEPAPER

CLOUDFLARE

Designing a secure, scalable remote learning infrastructure



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



Introduction

In recent years, remote learning has become an increasingly popular educational model. The COVID-19 pandemic — which forced many institutions to transition to remote learning to keep students and educators safe from the virus — accelerated the transition to hybrid and fully-remote learning models.

Remote learning requires a much different approach than traditional, in-person education. Educators require the ability to support a range of learning styles and types of content, including lecture, videos, interactive content, and more. With remote learning, all students in the classroom need to be able to quickly and simultaneously access the shared content.

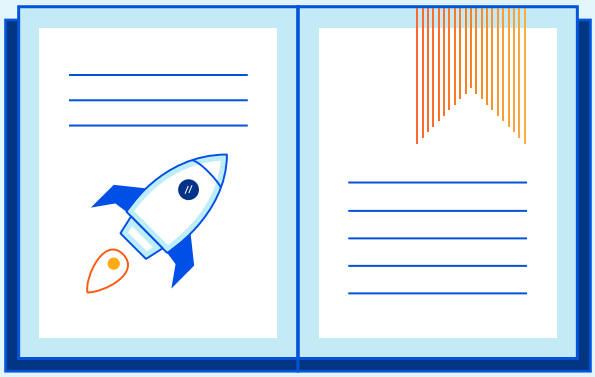
On the technical side, an educational institution needs to be able to support this wide range of content types and ensure that systems are functional when students need them. This requires addressing a range of challenges, including:

- Delivering content at scale
- Mitigating Distributed Denial of Service attacks
- Preventing account takeovers
- Stopping malicious content and malware

Delivering Content at Scale

With remote learning, schools' IT infrastructure is a vital component of the organization's ability to operate. Educators require the ability to serve content to many students simultaneously, and to ensure that it is delivered to students with minimal latency.

Educators need to be able to deliver a wide range of content to their students. This includes everything from static webpages to dynamic content like interactive online learning tools and streamed video. An educational institution's IT infrastructure needs to be able to efficiently and scalably deliver this content to its remote students.



Static Content

Some of the content that educators need to provide to their students is static. This includes webpages where the information included on the page does not change and does not require frequent updates.

For these types of content, the main IT challenges are scalability and latency. If many students are attempting to access the same content at the same time, will the webserver be able to keep up? Additionally, the location of the webserver can matter significantly for remote learning. The further that the student is from the server, the greater the latency in delivery of the content.

For static content, the ability to create local caches of content can help to alleviate these challenges. If a student visits a particular page frequently, it is possible that a copy of it will be stored locally, enabling them to access it quickly when needed.

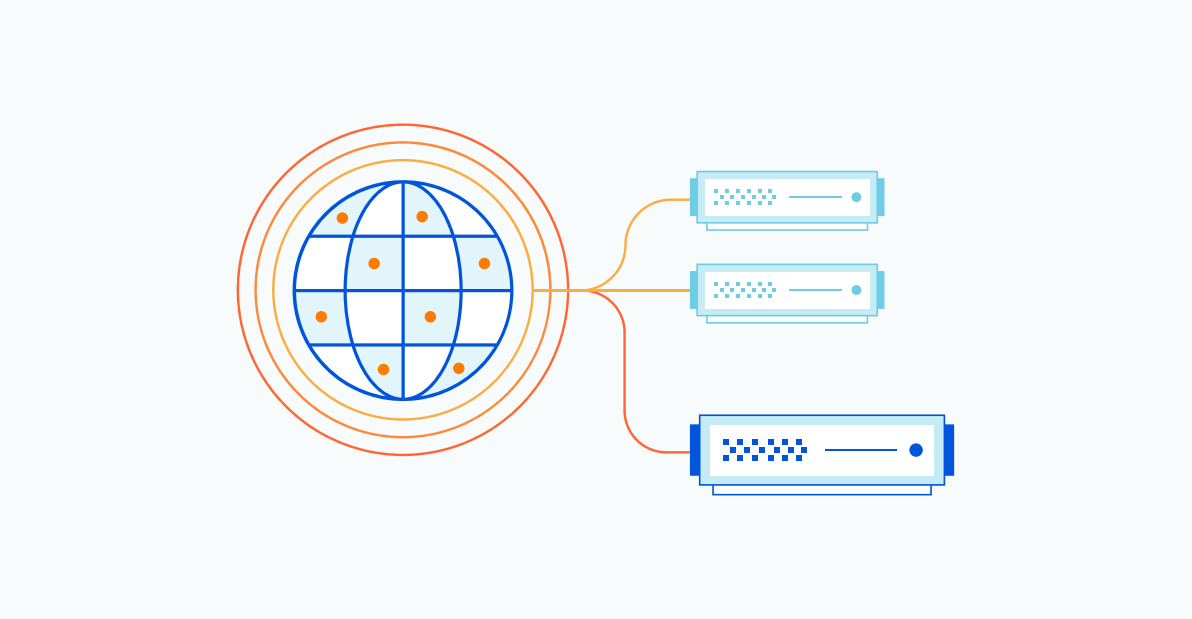
Caching can also be implemented as scale using a content distribution network (CDN). A CDN consists of a network of nodes that store local copies of static content and check in periodically for updates. A CDN with global reach offers the scalability and low latency required for effective remote learning.

Dynamic and Interactive Content

Like static content, interactive online learning and other content has potential issues with scalability. However, the use of a network of CDN nodes does not work as well for this type of content. If content requires frequent or near-constant updates, then the CDN nodes will be continually querying the main webserver for an updated version. This increases the latency for users and can overwhelm the main webserver.

Instead, dynamic content scalability issues can be solved via load balancing. Instead of using a single server to handle student requests, multiple servers are used with traffic distributed between them. This ensures that no single server becomes overwhelmed and that latency is minimized.

To be effective, a load-balanced server needs to be able to act completely independently or only rely upon other load-balanced devices. If all servers are set up to use the same database server, it is possible that the database server becomes the bottleneck and the additional load-balanced servers provide little or no benefit. Remote learning solutions must be carefully designed to ensure that the required scale is available if needed and that the system is architected in a way that provides the complete benefits of load balancing.

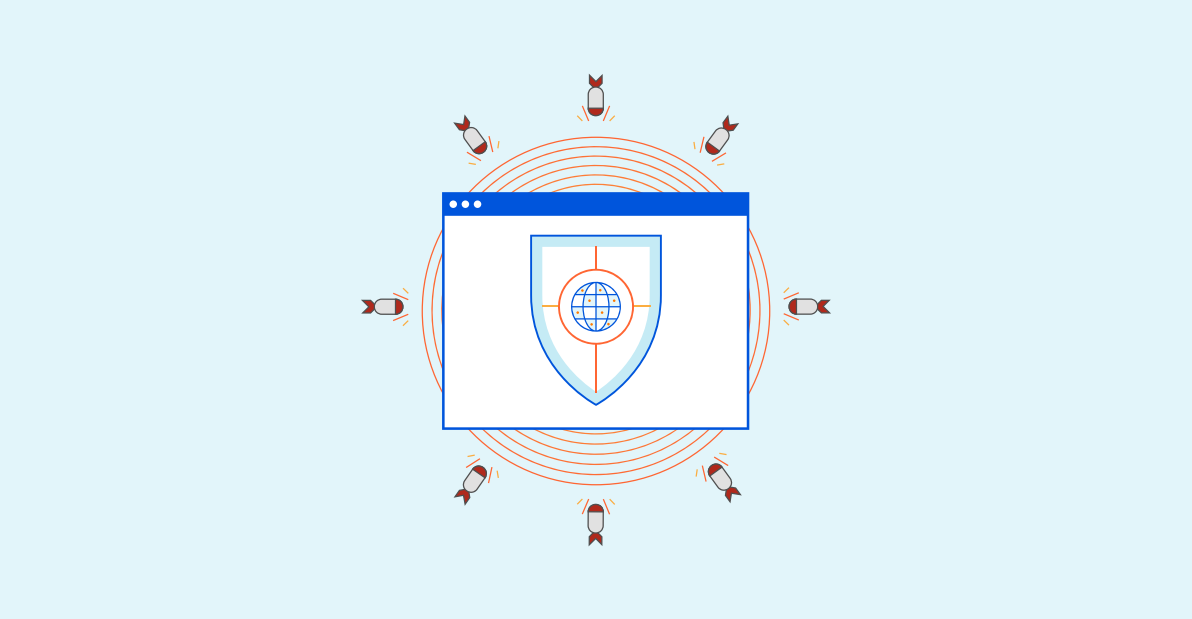


Distributed Denial of Service Attacks

When users access a web asset, their devices query a DNS resolver that maps the asset's domain Distributed Denial of Service (DDoS) attacks are growing increasingly common. As the Internet of Things (IoT) and cloud computing expand, it becomes cheaper and easier for attackers to gain access to Internet-connected computing power. These compromised devices can then be used to send malicious traffic to a service, making it unable to respond to legitimate requests.

In remote education, DDoS attacks pose a significant risk to the ability to provide services. In the first half of 2020, when many organizations transitioned to remote learning, DDoS attacks against online educational resources increased by 350%[1].

Additionally, some DDoS attacks have evolved to incorporate a ransom component. An attacker may threaten an organization with a DDoS attack and demand a ransom to stop the attack. Many of these threats are unfounded, but an educational institution without DDoS protection may feel the risk to their infrastructure is too great to ignore.

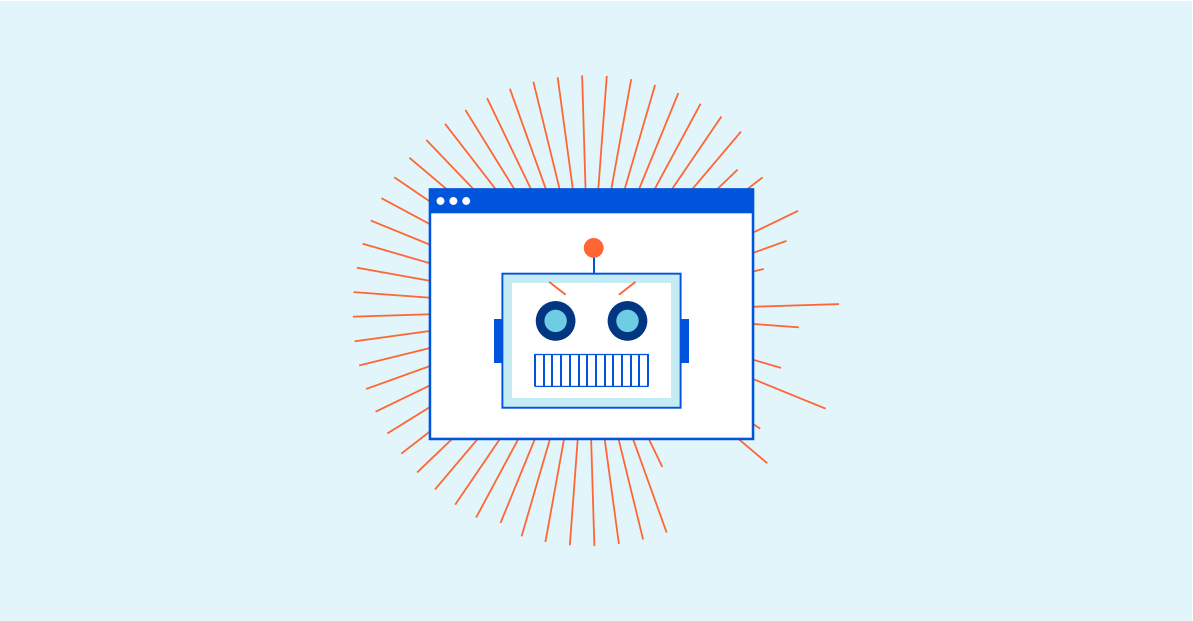


Fortunately, even education organizations with comparatively inflexible budgets still have access to a variety of effective DDoS mitigation tactics. Organizations should consider:

- High mitigation capacity: It can be tempting to only pay for as much protection as your organization expects to need, but if an unexpectedly large attack occurs, the time it takes to upgrade your service can result in extra downtime.
- Distributed mitigation: DDoS traffic scrubbing should be distributed, as routing all of an organization's traffic through a single, central point for filtering can be unscalable and increases network latency.
- On-demand vs always-on protection: In on-demand DDoS mitigation, traffic flows normally from the public Internet to an organization's servers or network infrastructure until a potential attack is detected, at which point it is inspected and filtered more thoroughly. Meanwhile, always-on protection continually filters all traffic. While always-on protection can be more expensive than on-demand services, always-on mitigation provides uninterrupted protection, and leads to faster response times since the service never needs to be turned on manually.

To learn more about DDoS mitigation strategies, read the paper "Five Best Practices for Mitigating DDoS Attacks" in the Cloudflare Resource Hub.

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



Account Takeover

Many cyberattacks begin with the takeover of a legitimate user's account on the system. Account takeover attacks involve compromising legitimate user credentials on a network, application, or other systems. An attacker can gain access to account credentials in a variety of different ways, including phishing attacks and credential stuffing.

With these credentials, the attacker can masquerade as a legitimate user and plant malware, steal data, or achieve other objectives on the target system. This could provide an attacker with access to data protected by regulations such as Children's Online Privacy Protection Act (COPPA) and Family Educational Rights and Privacy Act (FERPA). Alternatively, this access could allow attackers to delete critical student records or hold them for ransom using ransomware.

Educational institutions should deploy a phishing mitigation solution capable of detecting attacks based upon both known malicious content and the use of machine learning to detect suspicious language and other unknown threats. Email scanning is one such approach; another is using a secure web gateway to block known malicious sites and prevent users from downloading certain types of files

Credential Stuffing

Alternatively, an attacker can take advantage of an organization's public-facing login systems like virtual private networks (VPNs), the remote desktop protocol (RDP), or web access portals to compromise user credentials. The average person uses the same login credentials for 13 online accounts[2], and the use of weak and easily-guessable passwords is common. Credential stuffing attacks use automated bots to attempt to guess a user's password on these authentication portals. If successful, the attacker gains access to the legitimate user's account because they now know their legitimate login credentials.

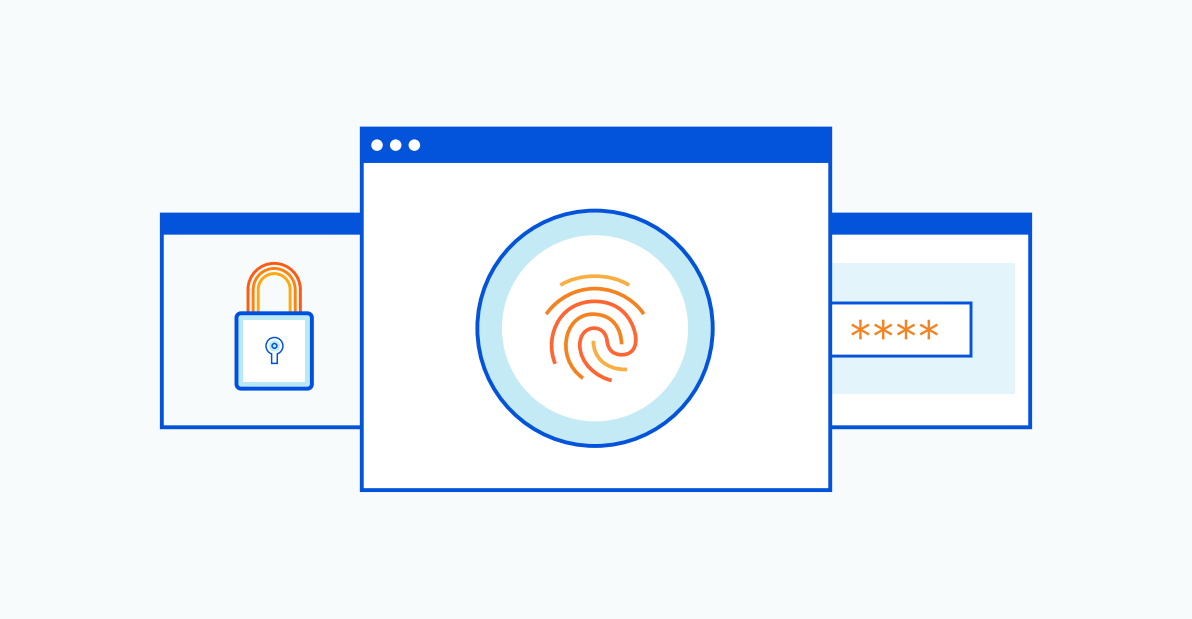
[2] *https://www.lastpass.com/state-of-the-password/global-password-security-report-2019*

Credential stuffing attacks take advantage of automation. Protecting against these types of attack requires bot detection solutions. However, it is also vital to differentiate between good bots and bad bots.

Bots can be detected and blocked via a variety of different methods. Basic elements of a malicious bot mitigation strategy include:

- **Rate limiting:** Limiting the number of times an IP address can submit requests to your site or network. This is most effective for simpler, brute-force bot attacks.
- **CAPTCHAs and two-factor authentication:** Both of these tactics can keep many bots from being able to access login pages at all. However, they can also negatively impact the user experience.
- **Maintaining a bot blocklist and allowlist:** to keep track of known malicious bots, and to ensure that search engine crawlers and other good bots are still able to carry out their tasks.

However, these tactics may not be as effective for more advanced, specialized bots. To learn more about bot mitigation, check out the “Malicious Bot Playbook” in the Cloudflare Resource Hub.

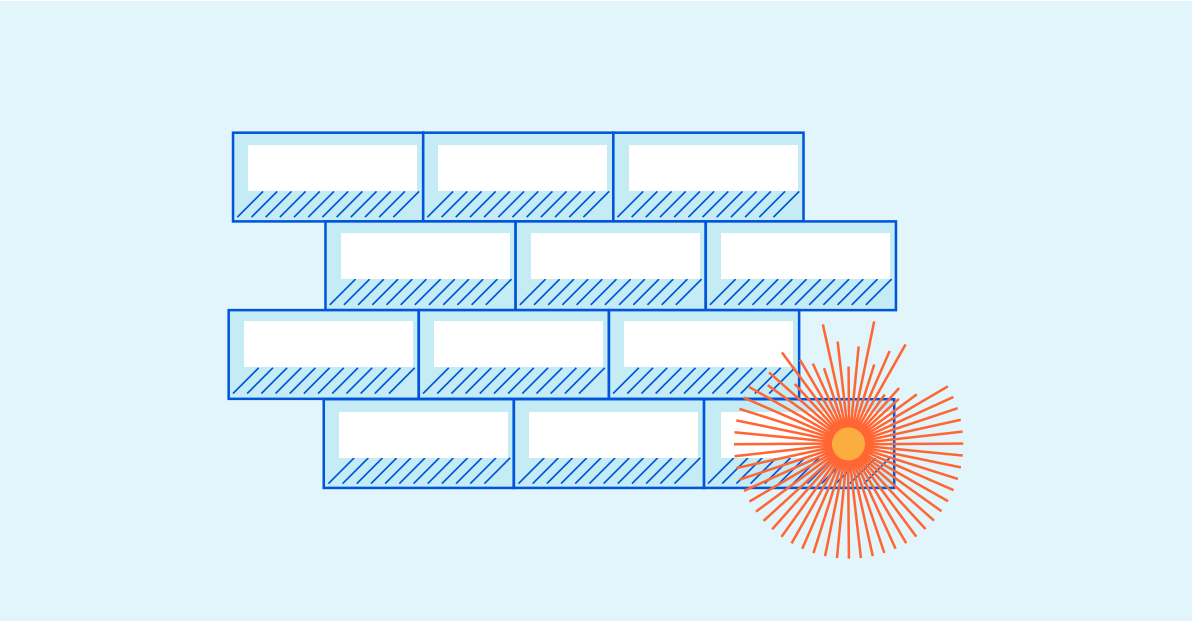


Malicious Content and Malware

As educators embrace remote learning, a growing number of systems will be exposed to the public Internet. Students may take advantage of online learning via web applications. Remote learners and educators may also have remote network and computer access using VPNs, RDP, and similar solutions. These systems must also be protected against cyber threats.

Web Application Security

Educational web applications may have access to a wide range of sensitive data. Student data covered under COPPA, FERPA, and similar legislation may be stored on these platforms, making it vital for educational institutions to properly secure them.



Since these applications are software, they potentially contain exploitable vulnerabilities. Protecting these applications against cyberattack requires inspecting network traffic to detect and block attempts to take advantage of these software bugs.

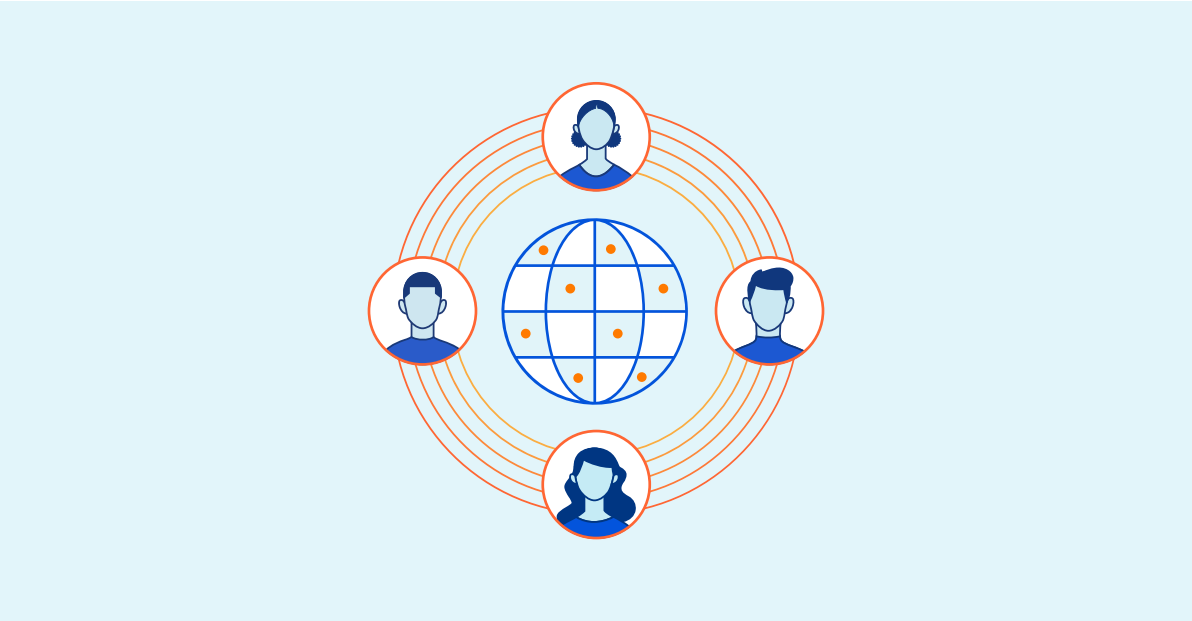
A web application firewall (WAF) provides protection against a wide variety of web application vulnerabilities. It can use a combination of signature-based detection and machine learning to identify both known and novel attacks. This allows it to protect against even zero-day attacks on an organization's web-based infrastructure.

Anti-Ransomware Protection

Ransomware is one of the fastest-growing types of malware. Once ransomware has access to a computer, it encrypts the files stored there and demands payment to restore access. Even if the school is able to immediately pay the ransom, significant time and expense can be required to restore impacted systems.

Ransomware is increasingly being delivered via remote access technologies like VPNs and RDP. An attacker with access to legitimate login credentials can use them to sign into a computer and install malware on it. Once inside the organization's network, malware commonly spreads to infect other computers on the network.

Educational institutions require a firewall solution that enables them to inspect all business network traffic. This enables them to both detect incoming malicious content (like ransomware) before it infects an organization's computers and to block attempted data exfiltration (including students' protected personal data).



Securing Remote Learning with Cloudflare

While the COVID-19 pandemic will pass, the ability to transition easily to remote learning is valuable to an educational institution. Online learning resources are a valuable asset for in-classroom learning as well, and having the necessary infrastructure for remote learning in place makes an organization resilient against disruption caused by inclement weather and other unanticipated events.

Cloudflare offers a consolidated and user-friendly platform with solutions for all of educational institutions' most common IT and security challenges. By leveraging a single, integrated solution like Cloudflare's, educational institutions avoid unnecessary complexity and become more adaptive and resilient to unexpected scenarios. Cloudflare offers:

- **A global content delivery network**, with data centers in over 200 global cities
- **47 Tbps of DDoS mitigation capacity**, with always-on mitigation taking place at the network edge.
- **A web application firewall** which continually draws on threat intelligence from the approximately 25 million Internet properties on Cloudflare's network.
- **Advanced bot mitigation**, which uses machine learning and fingerprinting to analyze traffic patterns across our network and detect the most advanced bots.
- **A secure web gateway** which operates at the network edge, reducing the latency that comes from backhauling traffic to a geographically isolated data center.

Learn more at www.cloudflare.com.