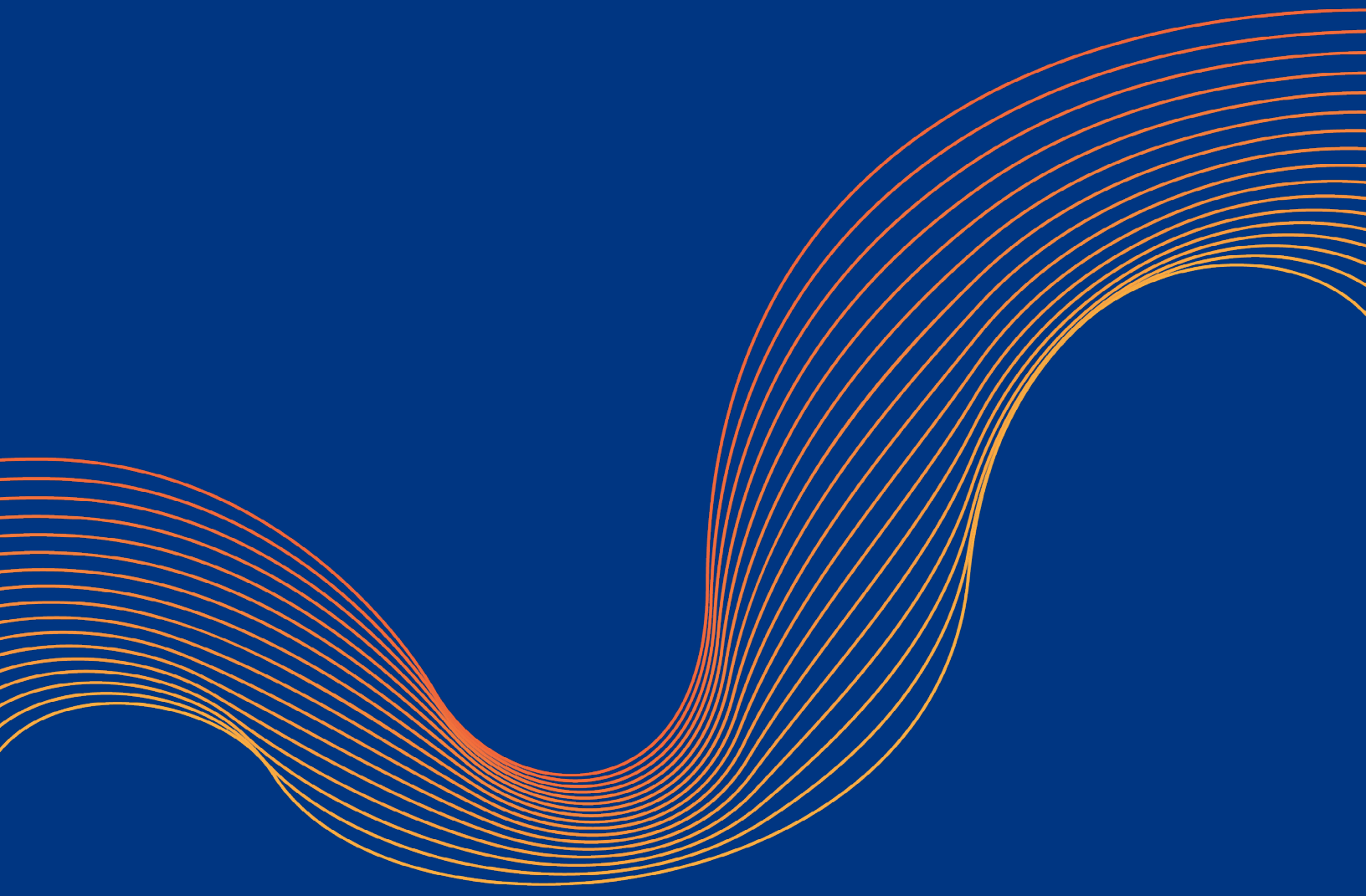
CLOUDFLARE®

Effective application security requires holistic, quick, and continuous protection



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

INDEX

INTRODUCTION

Application security threats are ever present. In 2020, the National Vulnerability Database (NVD) reported over 18,000 vulnerabilities — setting a new record. Alarmingly, over 10,000 of these vulnerabilities were labelled as critical or high severity.

At the same time, attackers continue to exploit well-known vulnerabilities. Joint research from the US' Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), the UK's National Cyber Security Center (NCSC), and The Australian Cyber Security Centre (ACSC) found that many of the top 30 vulnerabilities exploited by attackers during 2020 (and into 2021) were well-known, with all of them having an available patch.

The security risk from these well-known vulnerabilties is perpetuated as companies may struggle to patch their software. What's worse, even when companies attempt to patch a vulnerability before it is exploited, patching can take an average of 16 days — leaving applications open to attack.

Unfortunately, native vulnerabilities are not the only security concern for application owners. APIs introduce their own risks and data from the Cloudflare network shows over 50% of requests are API-related. On top of that, bots account for 40% of Internet traffic, making bot attack protection critical. Finally, third-party code, which many sites rely on to function, opens up applications to supply chain attacks.

With products and solutions available to protect an application from every possible attack, application security can quickly become fragmented and complex. Implementing a comprehensive application security strategy can help. An effective application security strategy should protect against a number of risks holistically, quickly, and continuously.

The landscape of application security concerns

The most pressing security concerns for application owners include:

Application vulnerabilities

Vulnerabilities within applications are incredibly common. A recent software security report from Veracode found that 83% of applications had at least one security flaw, with many applications having more than one. Additionally, over 20% of applications in the study had at least one severe flaw.

API attacks

Applications increasingly rely on application programming interfaces (APIs) to function. Recently, Gartner predicted "by 2022, API abuses will move from an infrequent to the most-frequent attack vector, resulting in data breaches for enterprise web applications.[1]"

[1] Gartner predicted "by 2022, API abuses will move from an infrequent to the most-frequent attack vector, resulting in data breaches for enterprise web applications. Source: Gartner "API Security: What You Need to Do to Protect Your APIs" ", Mark O'Neill, Dioniso Zumerle, Jeremy D'Hoinne, March 1, 2021, (Gartner subscription required)

Bot attacks

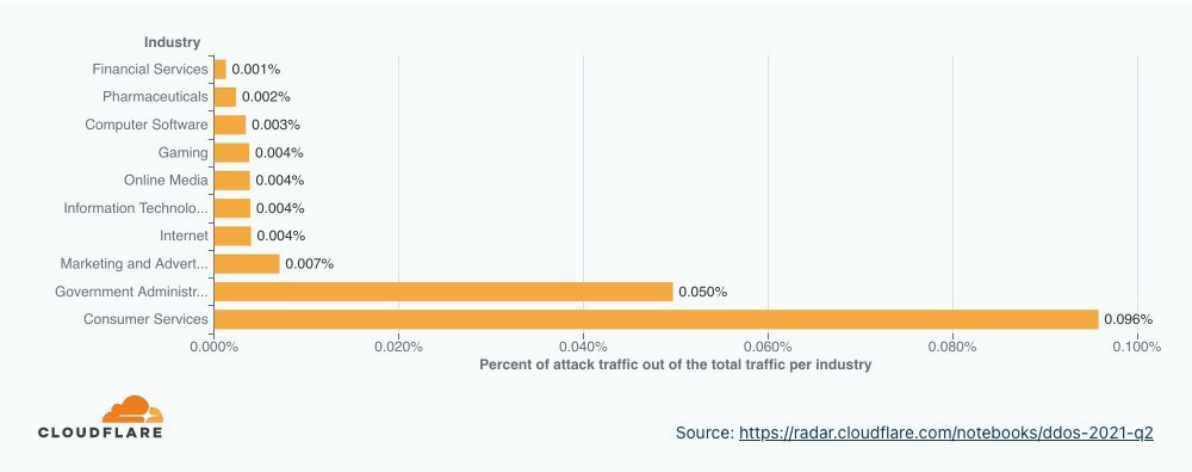
Bot attacks are very common. Attackers often use networks of infected devices — called botnets — to carry out a variety of malicious actions. One example is credential stuffing, in which bots attempt to "stuff" hundreds or thousands of stolen credentials into login pages in the hopes of gaining access to accounts. Bots are also used to carry out content scraping attacks, in which they download and duplicate a site's content to steal some search engine optimization (SEO) benefits.

Supply chain attacks

In supply chain attacks, attackers find an entry point through an external source, like software from trusted vendors, third-party web site dependencies, or suppliers. In 2015, a group called Magecart conducted a series of these attacks — stealing payment information from ecommerce websites by infecting third-party dependencies in the site with malicious code. The end users' browsers load the page containing the infected dependencies, allowing the attackers to steal information from their web page and sell it. The implication here is that working with third-parties, be it vendors or even web site dependencies, greatly increases an attack surface.

DDoS attacks

In DDoS attacks, attackers use an influx of junk traffic in an attempt to knock an application offline. Unfortunately, DDoS attacks are constantly shifting in size, vectors used, and more. Plus, they are not slowing down. Data from the Cloudflare network found that one out of every 200 HTTP requests destined to US-based organizations during Q2 2021 was part of a DDoS attack.



On-path attacks

Applications can also fall prey to on-path attacks, in which an attacker intercepts communication between two parties (like a browser and a server) for malicious purposes. The attacker can impersonate one of the parties and change their communication or collect sensitive information. On-path attacks can take many forms, targeting things like domain name system (DNS) servers and email servers, for example. In DNS on-path attacks, an attacker intercepts the DNS lookup process and sends users to a different — usually nefarious — website. Similarly, in email-hijacking, an attacker intercepts the connection between an email server and the web, giving them the power to read and interfere with email communications.

Best practices for defending against web application threats

Defending against these attack types should be a part of every organization's application security strategy. But how organizations defend against these attacks also matters. A sophisticated application security strategy should be:

- **Cloud edge network-based:** On-premise protection against web application threats used to be the norm, but this approach is difficult to scale. If an application is protected with a hardware-based WAF, for example, the only way to scale protection is to purchase additional hardware. Provisioning an application with more hardware-based protection can take a long time, leaving the application vulnerable. Cloud-based solutions do not have this issue. With more capacity always available, scaling protection is limitless.

  Beyond capacity limitations, on-premise protection is expensive to purchase and maintain. Hardware can age relatively quickly, so repair or replacement costs can add up. On top of that, hiring trained staff to manage the hardware also contributes to a high total cost of ownership. By contrast, using a cloud-based solution significantly reduces the ownership costs.

  Another benefit of cloud-delivered solutions is that they can be updated automatically — easily and often. This is particularly helpful for solutions like web application firewalls (WAFs), whose rules, mitigation mechanisms, and underlying software can be quickly updated when they are cloud-delivered. By contrast, on-premise providers can update solutions remotely, but the process is more complex and generally happens less frequently.

  Cloud edge networks take these benefits a step further. A cloud edge network is a group of servers spread out geographically running the same services. Protecting from the edge allows organizations to take advantage of the scalability benefits of the cloud while introducing additional performance advantages compared to centralized models.

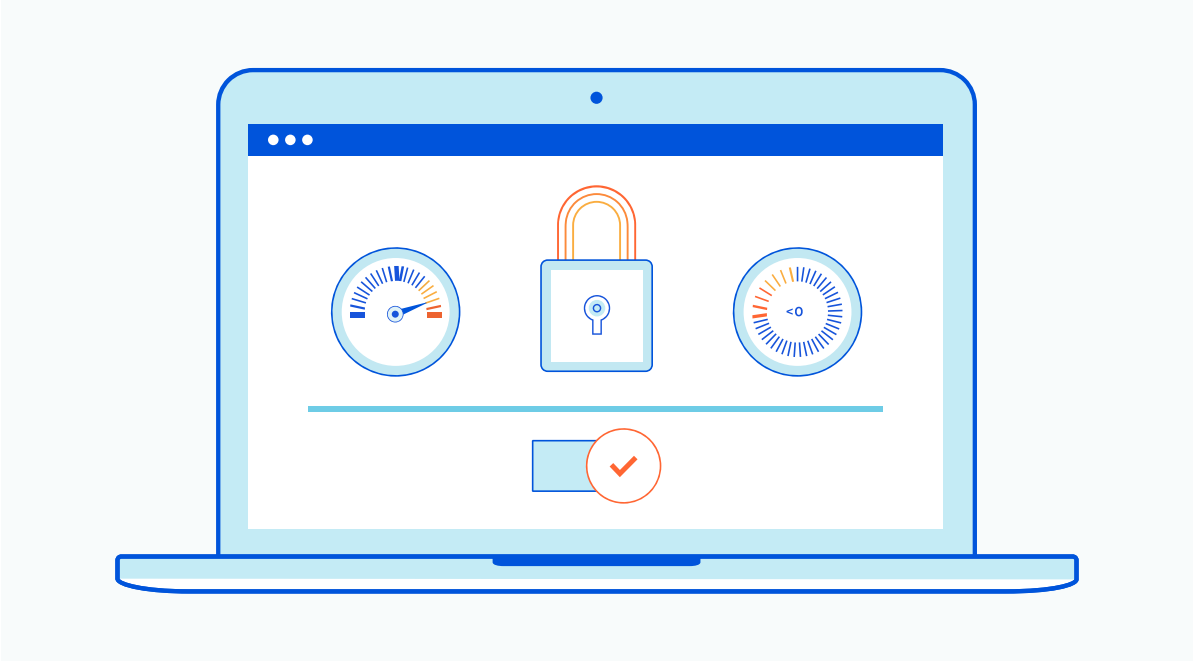
  In a cloud edge network, protection takes place as close to the end user as possible. By contrast, in a centralized model, protection takes place at a consolidated data center, much farther from end users who are spread out globally. To deliver security, all user traffic must be backhauled to the centralized data center, where the security appliances are deployed, regardless of where the end user is located. If data centers are located in the state of California, traffic will have to travel there first before being backhauled to an end user in New York, for example.

- **Unified:** Trying to apply consistent protection across multiple tools creates room for error. Thus, it is better to use a single, unified system to defend against attacks as opposed to stringing together multiple tools.

  When teams use disconnected tools, they often have different people managing different security products. This can mean important information does not get shared more broadly, creating security silos and information gaps. Plus, all tools need their own configuration and management, which creates a burden on teams and introduces unnecessary complexity.

  In addition, harboring too many tools can make it difficult to parse through all of the alerts. Each tool has its own set of rules and logic for sending out alerts and having several tools makes it difficult to determine which alerts are actually important.

  On the other hand, using a unified system allows teams to interact with fewer tools and centralized alerts, so understanding what needs attention is much easier. Integrated tools often reference consistent policies as well, which makes it easier to apply policies globally. Application owners can set data loss prevention (DLP) rules, for example, only once and have their WAF, API, and other applicable tools enforce them automatically.

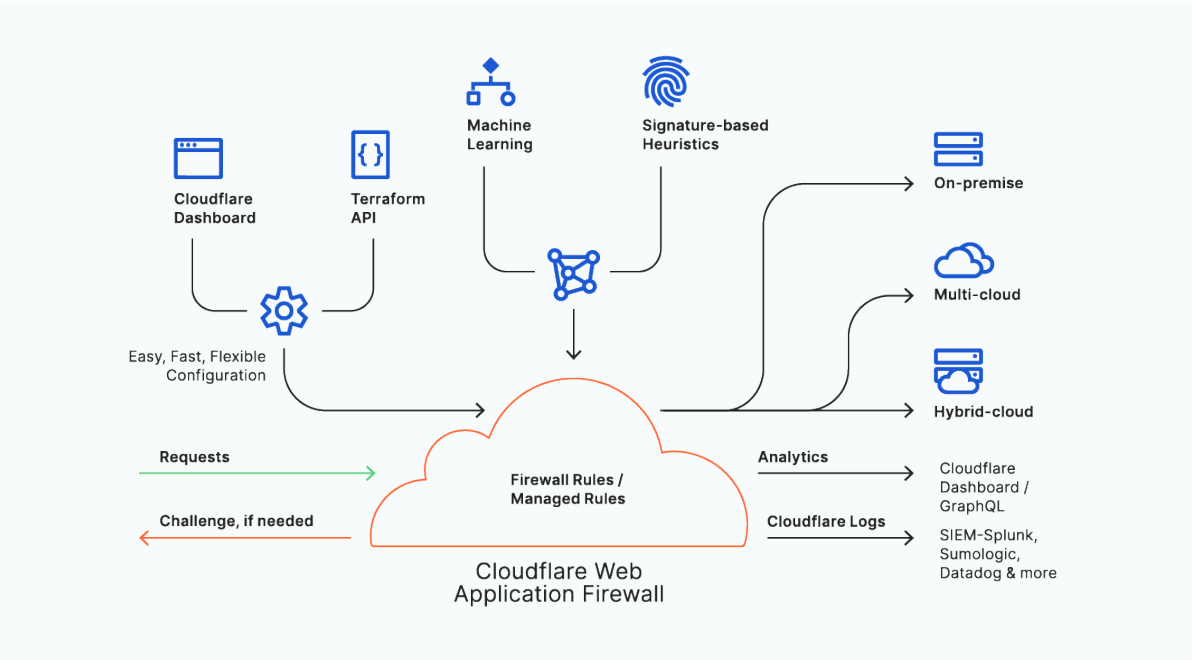


Attack-specific strategies

With so many different types of security risks facing applications, several types of protection are necessary. These are some of the attack-specific strategies application owners can use:

Application vulnerabilities

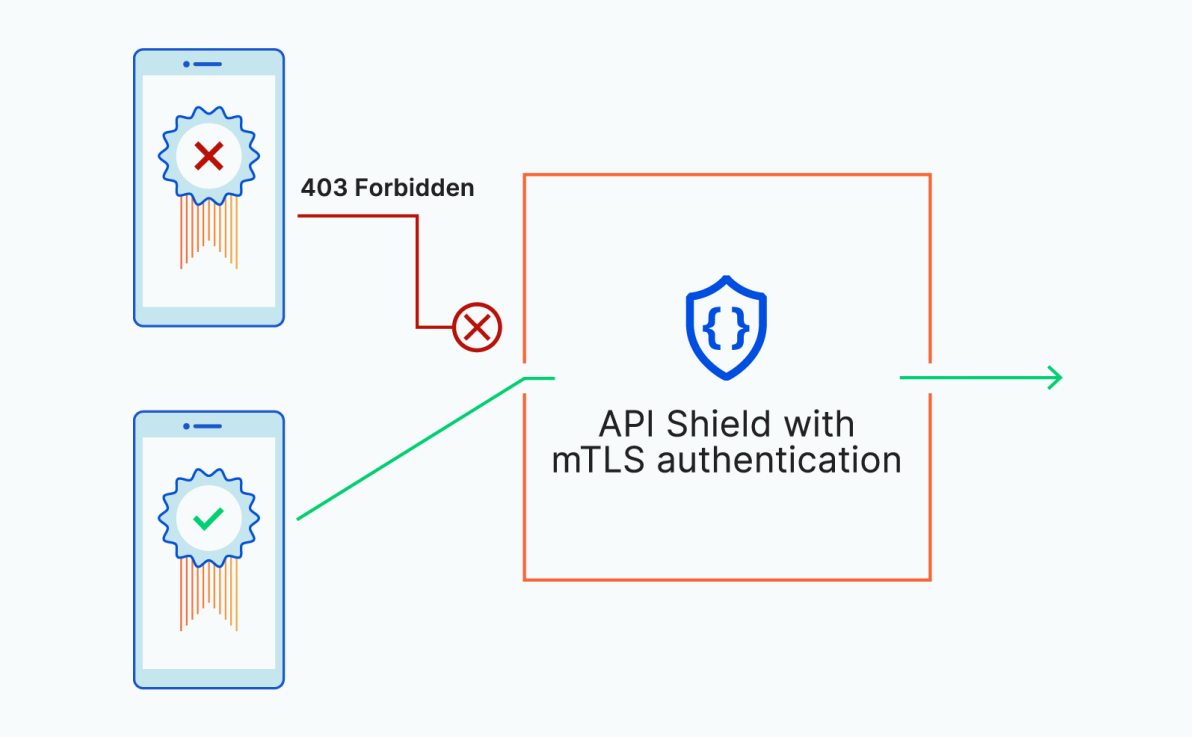
WAFs: A WAF is one of the best ways to prevent attackers from exploiting application vulnerabilities. WAFs use a set of security rules about known attack techniques to filter out malicious traffic and prevent attacks. WAFs with pre-set rules and customization options that deploy rule changes quickly are most effective. That is because these features mitigate two of the biggest issues with many WAFs: false positives and slow deployment of rule changes. False positives happen when WAF rules unintentionally block legitimate web traffic. Some WAFs require complex rule-setting procedures, making it difficult to maintain accurate, up-to-date lists and unblock legitimate traffic. Thus, WAFs that offer OWASP rulesets on top of managed and custom rulesets — reduce the frequency of false positives. However, if it takes too long to deploy these new rules, applications will be left vulnerable to attacks.



Data loss prevention: DLP is a strategy for preventing data exfiltration (or unauthorized movement of data outside of an organization). DLP tools and solutions monitor application and API activity to identify potential leaks and stop them before they happen. DLP tools inspect outgoing traffic and compare it against known types of data to determine if it is a data leak that should be blocked. For example, a DLP tool can identify a string of characters as a username. Based on the rules that the organization has put into place, the DLP tool can flag, stop, or allow the activity to continue. Some DLP tools integrate with role-based access controls (RBAC) — which dictate what access level user types have — to further secure how data moves within an organization or application.

API security risks

Schema validation and positive security models: API schema are contracts that describe the expected behavior for those interacting with an API. Schemas set the ground rules for what users are allowed to do when working with APIs. OpenAPI (or Swagger) is the most common schema format. Schemas are good templates to enforce positive API security. A positive security model validates requests against the schema, only allowing requests that conform to the schema, thereby preventing abuse and potential attacks. A positive security model is stricter than a negative security model, which allows all requests by default except for those it has been instructed to block.



Authentication and authorization: Authentication (or ensuring API requests are legitimate) and authorization (confirming what level of access an endpoint or client has) are also important aspects of API security. There are many ways to authenticate and authorize API requests. Mutual Transport Layer Security (mTLS), for example, is a process in which both a client and server have authentication certificates they use to verify each other's identity.

API discovery: "Shadow" APIs are APIs that a security team may be unaware of. Because a security team is not monitoring them, shadow APIs can introduce the possibility of data leaks or may not meet compliance standards. API discovery tools monitor endpoints to discover shadow APIs for better API management.

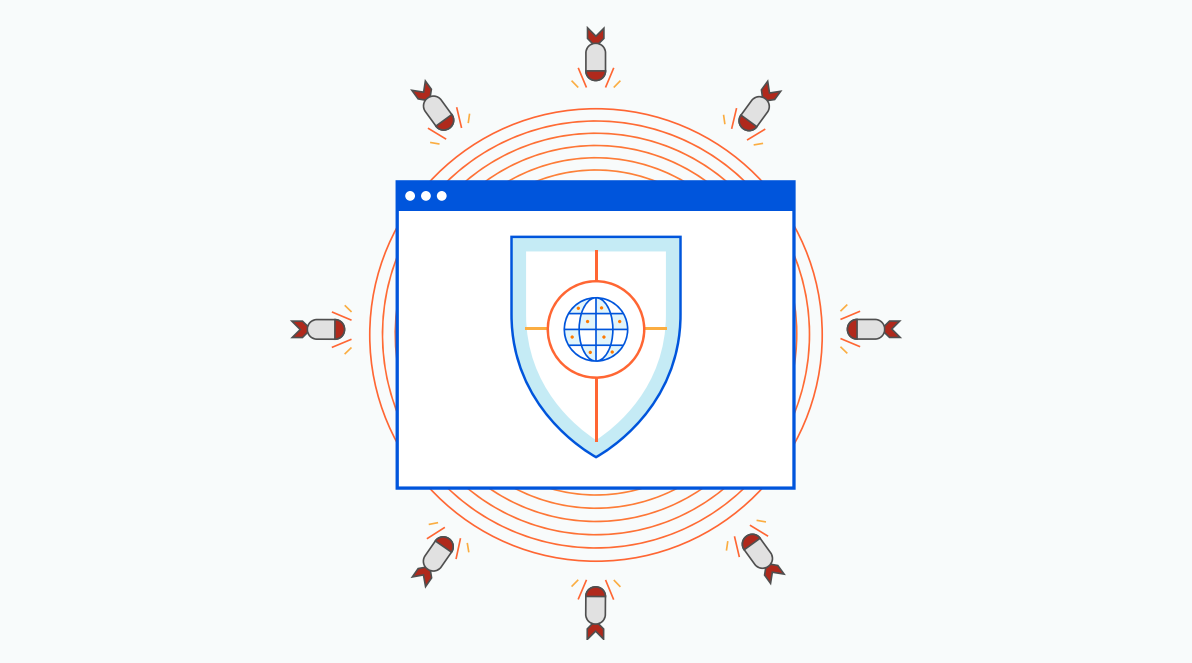
DLP: Data exfiltration can also happen with APIs, not just traditional applications. DLP tools can be used to monitor outgoing API traffic to detect and block any potential sensitive data in API responses.

Malicious bots

Managing bot traffic requires detecting and blocking bad bots without blocking good bots. Good bots, like SEO site crawlers, are necessary to understand key business metrics. Bad bots, on the other hand, can wreak havoc on an application — carrying out credential stuffing, content spam, and other types of attacks. A bot management solution will analyze traffic to detect bot activity and determine whether it is benign or malicious then block or permit the traffic accordingly. Managing bots effectively requires sophisticated detection methods, the ability to understand bot traffic trends over time with analytics, and the flexibility to use that data to customize bot-blocking rules.

DDoS attacks

Defending against DDoS attacks effectively means optimizing for time-to-mitigation and not sacrificing performance for security. One way to reduce time-to-mitigation is to use always-on DDoS protection, as opposed to the alternative, on-demand protection. Unlike on-demand protection, always-on mitigation does not wait until traffic reaches a particular threshold for protection to kick in, so all traffic is filtered and mitigation happens more quickly. DDoS mitigation from the edge enables application owners to enjoy performance and security. Unlike centralized protection, which takes place at a predefined location regardless of where the attack originates, DDoS mitigation happens as close to the attack source as possible, improving performance.



Third-party vulnerabilities

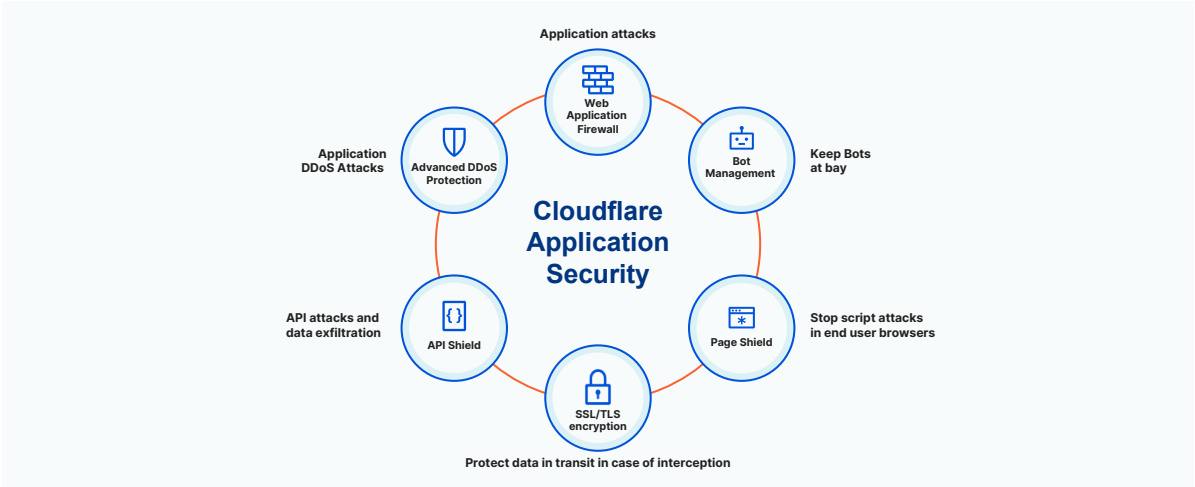
Client-side security solutions: Because many sites rely on third parties but do not often monitor these dependencies, they can be left vulnerable to supply chain attacks. In client-side security, activity is secured on the user's end, typically in their browser. Client-side security protects against supply chain attacks by monitoring changes to third-party dependencies and investigating the nature of code changes. For example, Content Security Policy (CSP) technology uses a list of approved resources and blocks any resource that is not on the list from executing. However, a shortcoming of CSP technology is that it is not dynamic. If a resource on the allowlist is compromised and becomes malicious, the CSP will not know to block it. Fortunately, some client-side security offerings build on the benefits of CSP. Some tools are able to track new JavaScript dependencies and alert site owners to investigate them. Similarly, some offerings can detect known-malicious URLs serving JavaScript on a site or alert site owners to investigate the nature of detected script changes.

On-path attacks

Encryption is key to defending against on-path attacks. Adopting Secure Sockets Layer (SSL)/ Transport Layer Security (TLS) encryption is one of the best methods to protect HTTP traffic. TLS encrypts data, authenticates the parties who are exchanging it, and validates it has not been tampered with. This process protects exchanges between web services and end users, preventing on-path attacks. However, some attackers can work around SSL/TLS, which is where the HTTP Strict Transport Security (HSTS) comes into play. HSTS blocks any unsecured connections from attackers, further preventing end users from on-path attacks.

Securing your application against external threats with Cloudflare

Protecting against external application threats is possible with Cloudflare. The Cloudflare edge network spans over 200 cities in more than 100 countries — protecting millions of Internet properties from DDoS attacks, application vulnerabilities, malicious bots, API abuse, and more. Every Cloudflare security service runs on every server in our network and draws from the same well of global threat intelligence.



Cloudflare application security offerings include:

- **Application vulnerabilities**
  - **WAF:** The Cloudflare WAF offers a layered ruleset — a managed ruleset that is regularly updated in response to the latest attacks, a core ruleset based on the OWASP Top 10, and custom rules customers can configure and deploy in seconds. Cloudflare WAF operates on the same Rust-based rules engine as Cloudflare Bot Management and API Shield, ensuring consistent protection.
- **API risks**
  - **API Shield:** Cloudflare API Shield defends APIs using client-certificate and schema-based validation. API Shield uses mTLS to verify devices/clients trying to access an API, scans outgoing traffic for DLP, and more.
    - **DLP:** Cloudflare also offers DLP functionality for APIs to block responses containing sensitive data like API keys or credit card information. Cloudflare DLP functionality extends beyond APIs, also securing applications and devices, for example.
- **Third-party vulnerabilities - browser supply chain attacks**
  - **Page Shield:** Script Monitor, a part of Cloudflare Page Shield, records a site's JavaScript dependencies over time and alerts organizations to investigate changes or new dependencies as they appear.
- **Bot attacks**
  - **Bot Management:** Cloudflare Bot Management uses machine learning, behavioral analysis, and global data to block bad bots. Use Bot Analytics to understand traffic patterns and fine-tune access with custom rules and allowlists.
- **DDoS attacks**
  - **DDoS:** With a 90 Tbps network that blocks an average of 87 billion threats per day, Cloudflare DDoS mitigation protects against the largest of attacks from the edge.
- **Encryption**
  - **Cloudflare Free SSL/TLS:** With Cloudflare Free SSL/TLS, you can encrypt web traffic to protect your application. Cloudflare SSL also supports the HSTS protocol for added protection.

To learn more, visit https://www.cloudflare.com/security/.