CLOUDFLARE®

# Securing Applications in the Cloud

## Fast, easy-to-deploy, and scalable layered defense against DDoS data compromise, and malicious bots

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

# Securing Applications in the Cloud

**Fast & easy-to-deploy layered defense to protect against DDoS, data compromise & malicious bots**

Companies are facing increased pressures to strengthen their security posture. Three forces contributing to the pressure are:

- Attackers are stronger, more sophisticated, and highly motivated
- Attack surface area grows because of applications exposing more public APIs, higher SaaS adoption, and the integration with more third-party applications
- Heightened public and government scrutiny of data, privacy, and security

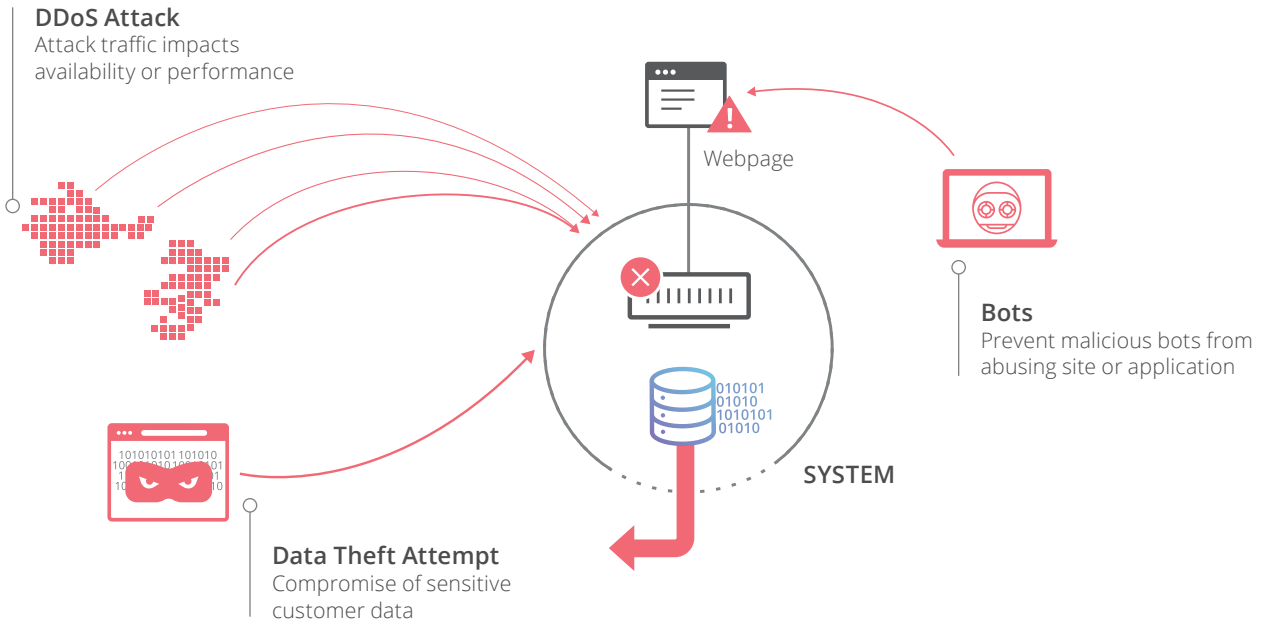
Attackers are increasing their frequency and volume of Distributed Denial-of-Service (DDoS) attacks. By leveraging botnets and the millions of Internet-of-Things (IoT) devices online, they are able to wage highly distributed volumetric attacks with greater ease and impact.

In addition to sending higher volumes, attackers are shifting their focus from the network layer to the application layer. Application-layer or "Layer 7" attacks are harder to detect, often require fewer resources to bring down a website or application, and disrupt operations.

Attackers are able to monetize their attempts to bring down sites or steal sensitive data, for example, by holding sites for ransom. As a result, because of the successful ransom payouts by their enterprise targets, the attackers are more motivated, organized and pervasive.

With increased exposure, companies need to strengthen their defense against three primary problems and risks:

- A DDoS attack against applications, websites and APIs degrading availability or performance, which results in decreased revenue, higher operational costs and brand degradation
- Compromise of sensitive customer and business data such as personally identifiable information (PII) or intellectual property, that results in losing customers and their trust
- Malicious bots abuse customer applications through content scraping, account takeovers, and fraudulent check outs



While the dollar costs for a DDoS, a data breach or malicious bots may vary by company size or industry, the severity of business impact is growing across all businesses.

According to an IDC report in 2015, the average cost of infrastructure downtime is $100k per hour.[1]

A data compromise could be leaked user information or the exfiltration of sensitive customer data, such as credit cards and passwords from an application's data store. The average global cost of data breach per lost or stolen record was $141 in 2017, and the average total cost of a data breach was $3.62 million.[2] With heightened scrutiny by governments and the media, companies are facing bigger repercussions from even the smallest data compromise, not only through financial penalties, but from the loss of public trust.

Malicious bots can not only takeover a user's account, but could also conduct fraudulent checkouts and content scraping. Checkout fraud from a bot that repeatedly and automatically purchases inventory in limited-supply can hurt a store's brand, discourage future customers resulting in lower future sales, and even damage relationships with suppliers. Content scraping, particularly for advertising-driven businesses, can directly reduce revenue by lowering SEO rankings, reducing cost-per-thousand impressions (CPMs), or losing advertisers.

## The Advantage

To combat both the rising exposure and the heightened business impacts, companies need to not just address the specific tactical problems, but find an advantage over bad actors in an ever-evolving threat landscape.

Three critical differences are **scale, performance, and ease-of-use**.

### Scale Matters

Cloudflare has the advantage of network size and traffic variability for data analysis. By protecting over 6M customer websites, Cloudflare has insight into emerging, global threats. As a result, Cloudflare's DDoS protections and Web Application Firewall proactively defend customers from attacks that cause downtime and loss of revenue.

Designed for scale, Cloudflare's network delivers both speed and resilience. In order to provide all of its services across over 300B requests per day, the services running on each server in every data center, like DNS, Encryption, and WAF, can process huge traffic loads with low latency and high reliability.

As the size of DDoS attacks grow, the size and resilience of the network benefits customers. Cloudflare's scale from its 116+ datacenters, combined with the Anycast network, enables Cloudflare to resist even the largest distributed attacks.

### Increase performance while securing applications

Customers traditionally have had to trade-off between security and performance. TLS and WAF solutions would often degrade the performance of a site. For example, TLS, a protocol for encrypting connections, can introduce up to four round trips just to initiate a single secure session. Those additional round-trips can increase latency. Similarly, because a WAF inspects each request in-line, it introduces additional delays.

[1] IDC, DevOps and the Cost of Downtime: Fortune 1000 Best Practice Metrics Quantified, Stephen Elliot, March 2015

[2] Ponemon Institute, 2017 Cost of Data Breach Study, June 2017

Cloudflare removes the need to sacrifice performance for security. Instead of decreasing performance, Cloudflare's security features can increase application performance because of low-latency security services integrated with traffic acceleration. Support for TLS 1.3 and global session resumption can reduce the number of round trips, and HTTP/2 which allows multiplexed downloads, speeds up page load times. Because Cloudflare's security services integrate with traffic acceleration services, such as caching and smart routing, applications can experience faster performance than running insecurely without Cloudflare.

Caching brings static content closer to the website's visitors. This not only reduces the load on the origin servers, but speeds up the application's response. Smart routing determines the fastest path from Cloudflare to the origin, accelerating both dynamic and static content.

**Scale**

Built for resilience
from the ground up


**Ease-of-Use**

Intuitive UI and API for agile
configuration and administration

**Speed**

High performance security
integrated with traffic acceleration

### Ease-of-Use Improves Security Posture

Ease-of-use of a security solution for the users and administrators is not just about a pretty interface; it also contributes to improving a company's security posture. Research from Gartner suggests that, through 2020, 99% of firewall breaches will be caused by simple firewall misconfigurations, not flaws.[3]

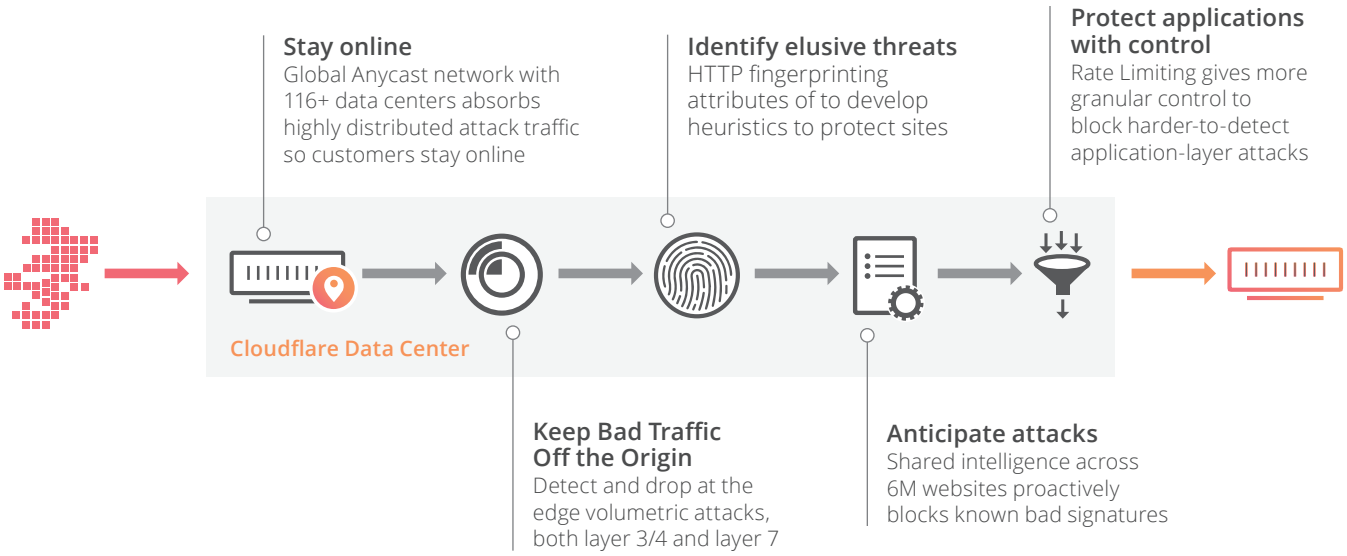
Good User Experience (UX) reduces security risks from misconfiguration and improves agility in an ever-shifting threat landscape. Setting up Cloudflare can take under 5-minutes. This ease-of-use enables companies to scale security policy management to more employees who may not be security experts, reduce time to change and deploy new policies, and improve timely adjustments to security posture of complex applications.

Cloudflare applies these advantages to protect customers from three primary challenges: DDoS attacks that can degrade their applications' performance and availability, customer data compromise from multi-vector attacks, and malicious bots abusing their website.

## Protect Your Applications from DDoS

A DDoS attack sends high volumes of traffic in an attempt to bring down a site or service. By overloading the origin servers, this malicious traffic makes the target application slow or unavailable for end users. Cloudflare provides a multi-layer defense.

[3] Gartner, Inc., One Brand of Firewall Is a Best Practice for Most Enterprises, Adam Hils and Rajpreet Kaur, June 5, 2017




## Global Anycast network

The Anycast network of 116+ data centers increases the surface area across which Cloudflare can disperse DDoS attacks. With Anycast, multiple machines share the same IP address. When a request is sent to an Anycast IP address, routers will direct it to the closest machine on the network. This mitigates highly distributed attacks by botnets since a portion of the DDoS traffic is absorbed by each of our data centers, instead of being concentrated in a single point.

## Intelligent and automated mitigations at the edge

Because Cloudflare has visibility across its 6M sites, the DDoS protection service can develop heuristics based on attacks on one site to protect many others.

Automated mitigations by fingerprinting network flows and HTTP attack traffic proactively identifies and stops attack traffic before hurting customer sites.

By dropping these high-volume attacks at the network's edge, the customer's origin servers remain protected and online.

## Integrated Stack of DNS, Network and Layer 7 Protections

Because each edge server has an integrated stack of security services, such as DNS, firewall, rate limiting and WAF, Cloudflare can provide not only distributed protection, but a layered defense against different types of DDoS attacks, particularly DNS, network, and application layer DDoS.

Cloudflare's distributed DNS service can withstand attacks directed against domain-name servers. Network attacks, such as Layer 3 and 4, are not only automatically blocked, but can be configured by customers to block bad sources by IP, country of origin, or ASN through an IP Firewall. Security settings can leverage Cloudflare's visibility into any IP address' reputation across its 6M websites to proactively block identified bad traffic.

> We love the peace of mind that we get knowing that we can set up Cloudflare, forget about it, and trust that we won't be affected by any kind of malicious DDoS attack.

BUYCRAFT | LEE MCNEIL, CTO

### Configurable rate-based mitigations

Although Cloudflare's DDoS solutions automatically protect customers from volumetric network and application attacks, some customers need configurable controls to protect themselves from lower-volume, yet still malicious, traffic.

The ability to customize the request rate thresholds, the target URI, and request attributes such as method and response code gives customers the flexibility to tune their defense based on their application and traffic profile.

## Reduce risks of data compromise through layered defense

Attackers often use several attack vectors when attempting to compromise customer data. To protect themselves, companies need a layered defense.

| ATTACKS | CLOUDFLARE SOLUTIONS |
|---|---|
| 1. Inject malicious payloads through forms and APIs | **Block top OWASP and emerging application-level attacks through the WAF** |
| 2. Snoop unencrypted sensitive data entered by customers | **Encryption through SSL/TLS blocks snooping** |
| 3. Brute-force their way into login pages | **Log-in protection through rate limiting** |
| 4. Attackers try to forge DNS answers to intercept customer credentials | **Resilient DNS and DNSSEC prevents forged answers** |

### Reduce spoofing through secure DNS

Cache poisoning or "spoofing" tricks unsuspecting site visitors to enter sensitive data, such as credit card numbers, into an attacked site. This type of attack occurs when an attacker poisons the cache of a DNS name server with incorrect records. Until the cache entry expires, that name server will return the fake DNS records. Instead of being directed to the correct site, visitors are routed to an attacker's site, allowing the bad actor to steal sensitive data.

DNSSEC verifies DNS records using cryptographic signatures. By checking the signature associated with a record, DNS resolvers can verify that the requested information comes from its authoritative name server and not a man-in-the-middle attacker.

### Reduce spoofing through encryption

Attackers can intercept or "snoop" on customer sessions to steal sensitive customer data, including credentials such as passwords or credit-cards numbers. In the case of a "man-in-the-middle" attack, the browser thinks it is talking to the server on an encrypted channel, and the server thinks it is talking to the browser, but they are both talking to the attacker who is sitting in the middle. All traffic passes through this man-in-the-middle, who is able to read and modify any of the data.

Fast encryption/termination, easy certificate management, and support of the latest security standards enable customers to secure transmission of user data.

### Block malicious playloads through auto-updated, scalable WAF

Attackers exploit application vulnerabilities by submitting malicious payloads that can extract sensitive data from the database, the user's browser, or from by injecting malware that can compromise targeted systems.

A Web Application Firewall (WAF) examines web traffic looking for suspicious traffic; it can then automatically filter out illegitimate requests based on rule sets that you ask it to apply. It looks at both GET and POST-based HTTP requests and applies a rule set, such as the ModSecurity core rule set covering the OWASP Top 10 vulnerabilities to determine what traffic to block, challenge or let pass. It can block comment spam, cross-site scripting attacks and SQL injections.

The Cloudflare WAF updates rules based on threats identified from 6M customers, and can protect customers without hurting application performance because of its low-latency inspection and integration with traffic acceleration.

### Reduced account take-overs through login protection

Attackers can wage "dictionary attacks" by automating logins with dumped credentials to "brute force" their way through a login-protected page. Cloudflare enables users to customize rate-limiting rules to identify and block at the edge these hard-to-detect attacks.

### Protect through monitoring and scoring

By monitoring a website for vulnerabilities, scoring a company's security maturity, and integrating into your development process, Cloudflare's third-party apps provide an additional layer of proactive protection.

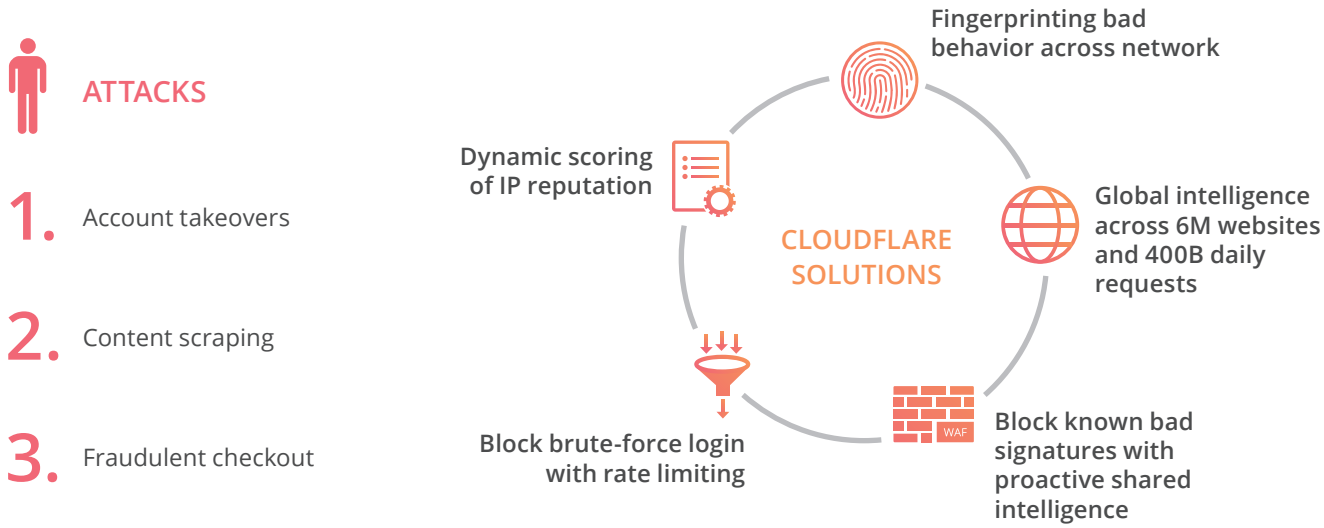
> The security features of Cloudflare freed up our developers from worrying about keeping the site online and allowed them to focus on other site improvements.

Gazeta Esportiva | DAVID VERZOLLA
Head of Technology

## Prevent abusive bots

Three forms of abusive bots are growing in frequency, sophistication, and customer impact. As a result, a bot prevention solution needs different elements to address the different potential attack profiles.

The most common attacks are account take-overs, content scraping and fraudulent checkout. All three can use different bot "styles", each of which can be detected and mitigated with different approaches.




### Rate-based detection and mitigation

Because some bots are automated and need to hit the site at a high-rate in order to achieve their objective, rate-based automation can detect and mitigate these attacks. For example, brute-force logins have a higher rate of failed logins from a single IP address than a normal user. Rate-based thresholds can detect these types of account takeover attempts. Similarly, content scrapers hitting pages that can no longer be found (404 errors) will generate these at a higher rate than a normal user.

### Blocking based on known bad signatures

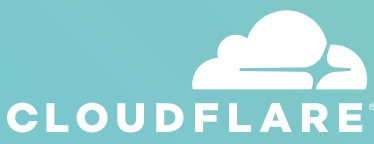
With 6M websites protected on Cloudflare, known bad signatures for abusive bots can be detected on one site and then blocked on all the others.

## Conclusion

To remain secure and 'always-on' in an always-evolving threat landscape, companies need performance, intelligent security at scale, and layered defenses to protect against denial-of-service, data theft and malicious bots.

Because humans will always be part of the equation, ease-of-use to deploy, configure, and fine-tune security policies impacts the overall security posture by reducing 'fat-fingering' and allowing more employees to react to changes without risks or unnecessary friction.

Cloudflare's cloud security defends against the growing sophistication of DDoS attacks, attempts at data compromise by bad actors and malicious bots.



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