Modernize and secure your applications

Keep your business moving forward by coupling Azure Active Directory B2C secure authentication with Cloudflare Web Application Firewall to keep your applications and APIs protected and productive.

Contents

Web applications and APIs are the lifeblood of modern enterprises—and attackers know this

Digital transformation is critical to your success, but it exposes you to new threats as attack surfaces increase.

Two years' worth of digital transformation took place in the first two months of the COVID-19 pandemic. And security and IT teams have been working overtime to meet business goals while simultaneously staying ahead of new threats and scams.

148%

Distributed Denial of Service (DDoS) incidents saw a 148% year-on-year increase.[1]

43%

43% of data breaches in 2020 involved web applications.[2]

119K

119K threats detected per minute in 2020 with more than 16 million COVID-related threats detected.[3]

API

API traffic now accounts for nearly half of internet traffic.[4]

45%

Automated traffic from bots makes up some 45% of internet traffic.[5]

Modernize authentication with Azure Active Directory B2C while ensuring your connected applications and websites remain secure with Cloudflare Web Application Firewall.

Modernize authentication
Build a single sign-on experience for all your web apps, mobile apps, and APIs for streamlined customer login.

Supercharge your application security and performance
Accelerate and secure Azure-hosted web properties and Azure AD business-to-consumer apps.

Dynamically manage web requests with custom rules
Easily create and activate Firewall Rules within the Cloudflare Web Application Firewall solution.

Modernize authentication

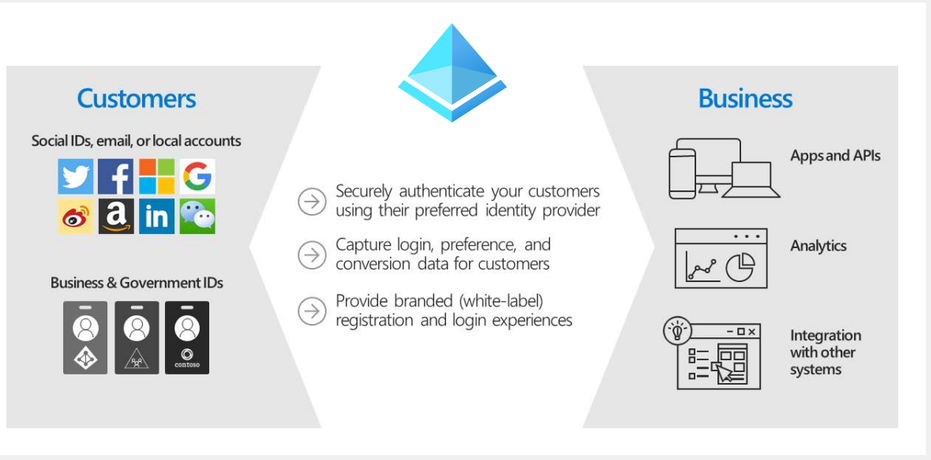
How do you enable access to your company's applications, websites, and APIs?

A crucial component of modern-day enterprises is customer identity access management (CIAM). How do you safely and seamlessly provision access to your customers without compromising their identity or exposing your company to a data breach?

With Azure Active Directory B2C, organizations are providing business-to-consumer identity as a service. Your customers can use their own preferred social, enterprise, or local account identities to get single sign-on access to your business' applications and APIs.

Microsoft's trustworthy CIAM solution for business-to-consumer services

Azure Active Directory B2C supports millions of users and billions of authentications per day. It takes care of the scaling and safety of the authentication platform, monitoring and automatically handling threats like denial-of-service, password spray, or brute force attacks.



CLOUDFLARE Microsoft

Supercharge your application security and performance

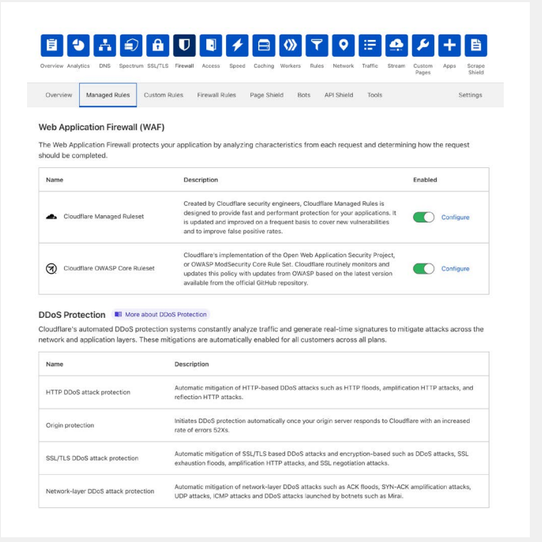
How are you protecting your applications, web properties, and APIs from threats?

As attackers become more sophisticated, enterprises must similarly adapt to combat both known OWASP attacks like SQL injection, cross-site scripting, and comment spam as well as new application zero-day vulnerabilities. To achieve this, Cloudflare extends the secure authentication capabilities of Azure AD B2C by enabling their Web Application Firewall (WAF) to extend greater protection over your consumer services.

Cloudflare's cloud-based performance and security platform assists enterprises by accelerating and securing their Azure-hosted web properties and Azure AD business-to-consumer applications. Cloudflare WAF thwarts application attacks and bots while detecting anomalies and malicious payloads.

Benefit from an evolving, sharpened threat intelligence

By integrating Cloudflare with your Azure AD B2C account, you'll be protected by threat intelligence constantly sharpened by insights gained from our global network that processes 2 trillion daily requests.



CLOUDFLARE Microsoft

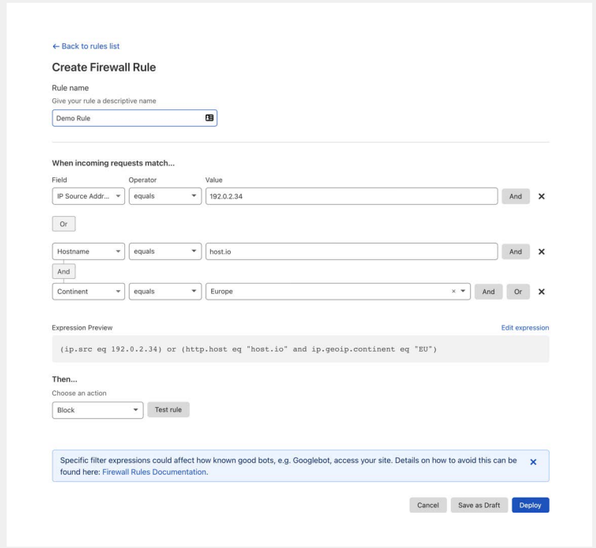
Dynamically manage web requests with custom rules

How much time are you spending on application security?

It takes organizations time and resources to take proper precautions around writing rules and examining all incoming site or application traffic to ensure security. But what if you could easily create and activate Firewall Rules within your WAF without requiring overly-complex interfaces or rule syntax? Organizations can block any threat with Cloudflare Firewall Rules that let you target HTTP traffic and apply customer criteria to block, challenge, log, or allow certain requests before they reach custom domains inside your Azure AD B2C tenant.

Easily create and activate your own Firewall Rules

Cloudflare Firewall Rules allow you to construct expressions to match and filter HTTP requests and determine how your WAF should handle the matching traffic. New rules are active in seconds for instant protection unlike other WAFs that need 45 minutes to take effect.



Case study: Panasonic

Challenge
Panasonic, a longstanding household brand in Japan, the US, and Europe, was facing high potential risks for application and DDoS attacks.

Solution
Panasonic's European cybersecurity team selected Cloudflare's WAF and Advanced DDoS Protection, along with Cloudflare's CDN, Workers, and Enterprise Domains.

Result
Cloudflare WAF strengthens Panasonic's cybersecurity posture, enhancing their visibility into web requests through a single pane of glass and improving security management with advanced analytics to distill actionable intelligence.

The company is now protected against vast amounts of malicious traffic with Cloudflare default rules, and their IT team can create custom rules for specific application security needs.

Conquer your biggest security fears with Cloudflare and Microsoft

Passwords are vulnerable to attacks and painful to remember. Using ThinC-AUTH Biometric Security Key, users can authenticate seamlessly with the touch of their finger and log in to any FIDO2-supported service including Azure Active Directory.

Learn More

[1]State of the Web Security, 2020
[2]2020 Data Breach Investigations Report, Verizon
[3]Trend Micro 2020 Annual Cybersecurity Report
[4]Cloudflare 2021 internal data
[5]Cloudflare Radar