Modernize and secure your applications

The Cloudflare Web Application Firewall with Azure Active Directory B2C

From Cloudflare and Microsoft

What's impacting your business today?

148%

Year-on-year increase in Distributed Denial of Service (DDoS) incidents.

Source: State of the Web Security, CDNetwork 2020

43%

Of data breaches in 2020 involved web applications.

Source: 2020 Data Breach Investigations Report, Verizon

119K

Threats detected per minute in 2020 with more than 16 million COVID-related threats detected.

Source: Trend Micro 2020 Annual Cybersecurity Report

Your APIs and applications are vulnerable

Modern application attacks

How are you keeping your applications and APIs secure?

It's imperative to stop both known OWASP attacks, including SQL, injection, cross-site scripting (XSS), comment spam, and new exploits targeting zero-day vulnerabilities in applications.

Complicated security postures

How much time are you spending on application security?

It takes organizations time and resources to set up security, train staff on rule writing and syntax, and pay for professional services.

Piecemeal application security and performance

How do you balance application security with high performance?

To improve application performance, companies have had to deploy and manage technology separate from their security – even though both apply to the same application.

Cloudflare + Azure Active Directory B2C

Safeguard customer data and Azure-hosted web properties + Azure AD business-to-consumer apps

Protect your customer's identities with Azure AD B2C

Apply security control and application or policy-based multi-factor authentication to help protect your customer's personal data using Azure AD B2C.

Azure AD B2C 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.

Optimize performance of your network and services

Protect your Azure deployments with enterprise-grade security without sacrificing web performance.

Leverage deeply integrated products for faster network routing, serverless computing, content acceleration, DDoS protection, and more with Cloudflare.

Protect customer-facing apps with Cloudflare's WAF

Extend Azure AD B2C capabilities by enabling Cloudflare Web Application Firewall (WAF) with a custom domain to extend greater protection over your consumer services.

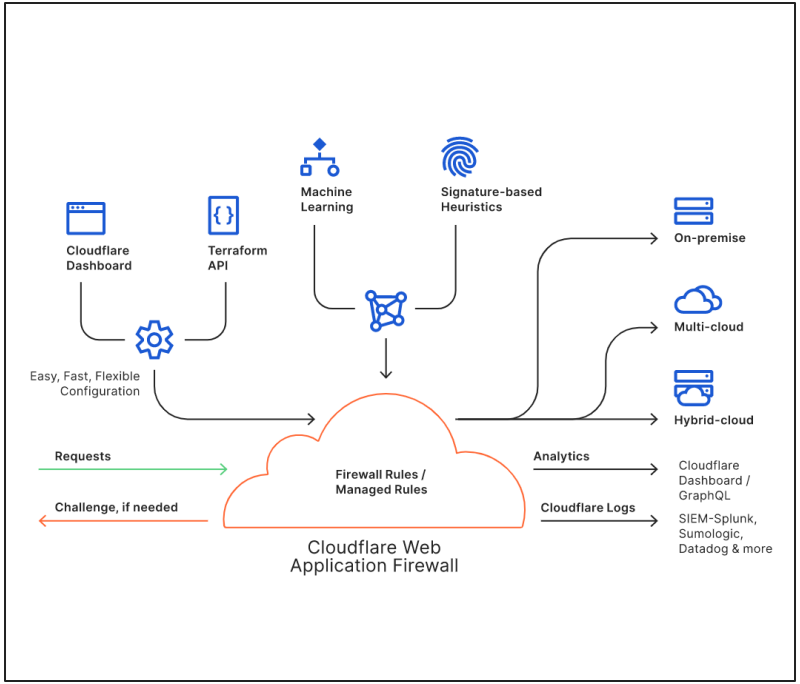
WAF identifies and blocks malicious application attacks – both known attack techniques and exploits targeting zero-day vulnerabilities.

Cloudflare WAF integration includes the following components

- **Azure AD B2C Tenant** – Microsoft's leading customer identity access management (CIAM) solution that provides business-to-consumer identity as a service. Your customers use their preferred social, enterprise, or local account identities to get single sign-on access to your applications and APIs.

- **Azure Front Door** – Responsible for enabling custom domains for Azure B2C tenant. All traffic from Cloudflare WAF will be routed to Azure Front Door before arriving at Azure AD B2C tenant.

- **Cloudflare** – The web application firewall manages all traffic that is sent to the authorization server.



Optimize customer access while delivering performance and security to applications and services

Streamline authentication with Azure AD B2C

Azure AD B2C is the central authentication authority for your web apps, mobile apps, and APIs, enabling you to build a single sign-on (SSO) experience that's custom-branded for streamlined customer login.

Modernize authentication and enhance application security

Cloudflare's cloud-based performance and security solution, WAF, assists enterprises by accelerating and securing their Azure-hosted web properties and Azure AD business-to-consumer apps.

Easily create and activate Firewall Rules within your WAF

Block any threat with Cloudflare's Firewall Rules by constructing custom expressions to match and filter HTTP requests and determine how the WAF should handle the matching traffic.

Streamline authentication with Azure AD B2C

Enable single sign-on access to your apps and web properties with a user-provided identity.

- Securely authenticate customers using their preferred identity provider.
- Use standards-based authentication protocols, including OpenID Connect, Oauth 2.0, and SAML.
- Enable single sign-on for most modern apps and commercial software.
- Capture detailed analytics about sign-in behavior and sign-up conversion.

Modernize authentication and enhance application security

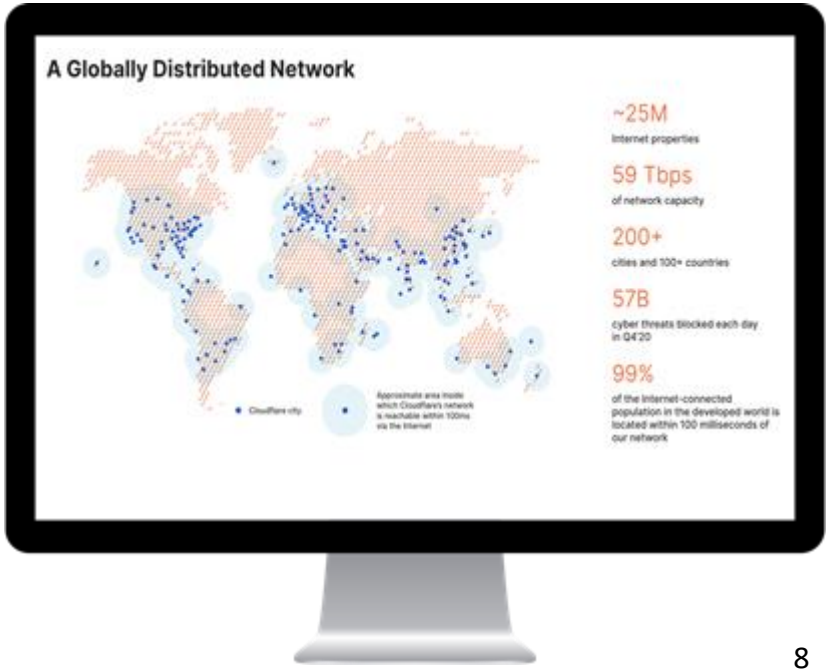
Modernize authentication with Azure AD B2C and secure applications with Cloudflare's WAF.

Ensure your Azure-hosted services and Azure AD B2C apps are constantly optimized and protected.

Benefit from an evolving, sharpened threat intelligence.

Tap into Cloudflare's global network with 2 trillion requests processed daily.

Gain granular custom rules, proven tested protections.



Easily create and activate Firewall Rules within your WAF

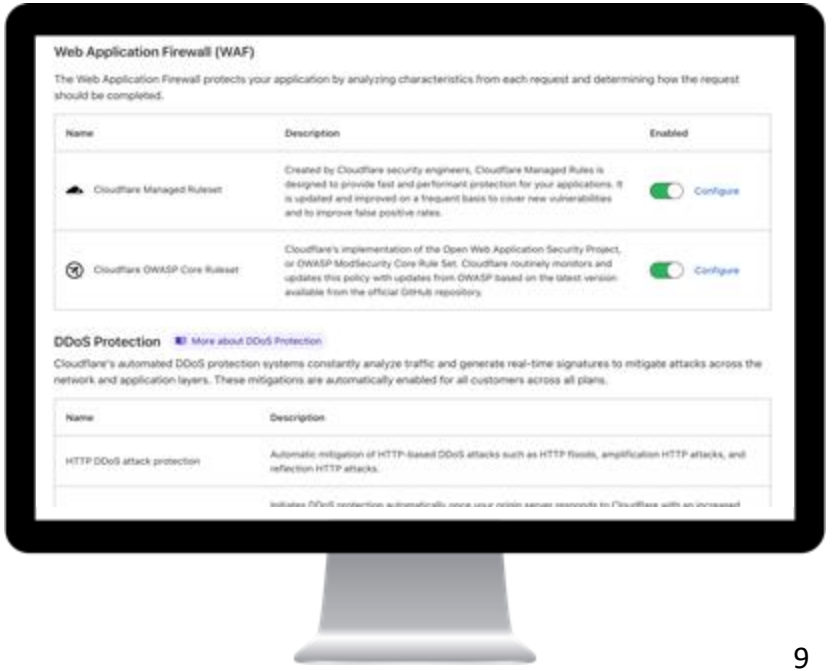
Simplify management with a powerful, single pane of glass.

Leverage Cloudflare Firewall Rules to target HTTP traffic and apply customer criteria.

No overly complex interfaces or rule syntax needed.

Examine all incoming site traffic before it reaches Azure Front Door.

Activate new rule sets in seconds for instant protection.



Why choose Cloudflare's WAF?

10x faster than competitors

Gain the fastest and most precise protection that's been tested against vast amounts of traffic. Cloudflare's global network ensures customers are protected up to 10x faster than competitors.

Source: Internal Cloudflare Data

57 billion cyberthreats detected

The Cloudflare global network blocks more than 57 billion cyberthreats per day. That is 650k blocked HTTP requests per second.

Source: Cloudflare

Customer's choice for WAF 2021

Cloudflare was recognized by Gartner's Peer Insights report as the "Customer's Choice" for WAF in 2021.

Source: Cloudflare

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 and Workers and Enterprise Domains.

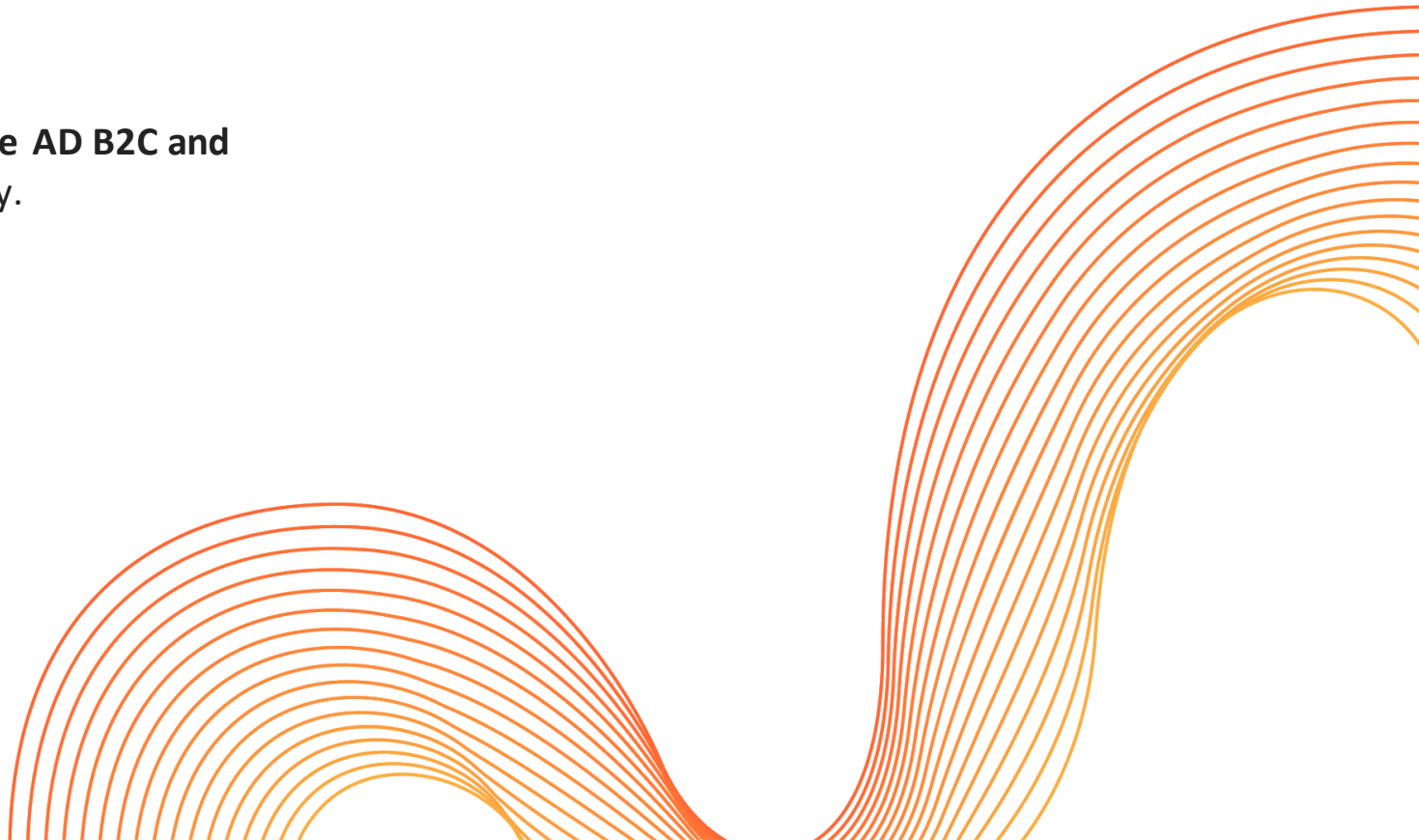
Results

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 powerful customized rules for specific application security needs.

Next steps

Learn more about **Azure AD B2C and Cloudflare's WAF** today.

Get started.



Thank you