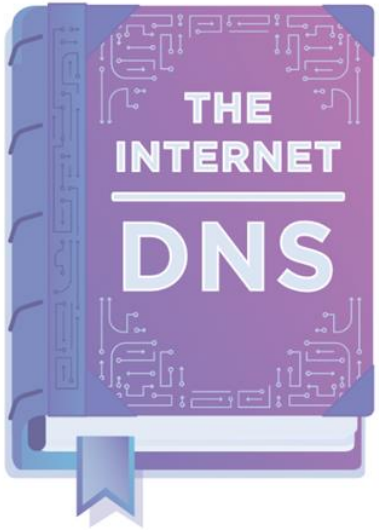
Tendencias de ataques DDoS del primer trimestre de 2022

Información del informe Tendencias de ataques DDoS del primer trimestre de 2022

Armando Navarro
Director Comercial
CentroAmerica

Cloudflare



DNS: Directorio de Internet

Casi todo en Internet comienza con una solicitud de DNS. DNS es el directorio de Internet. Al hacer clic en un enlace, abrir una aplicación o enviar un mensaje de correo electrónico, lo primero que hace el dispositivo es preguntar al directorio: **¿Dónde puedo encontrar esto?**

Lamentablemente, de forma predeterminada, DNS suele ser lento y poco seguro. El ISP, y cualquier persona experta en Internet, puede ver todos los sitios que visita, así como las aplicaciones que utiliza, incluso si el contenido se ha cifrado. Aunque no lo crea, los proveedores de DNS venden datos relativos a su actividad en Internet, o los utilizan para mostrarle anuncios.

Creemos que esto es intolerable. En el caso de que también opine del mismo modo, dispone ahora de una alternativa: `1.1.1.1`

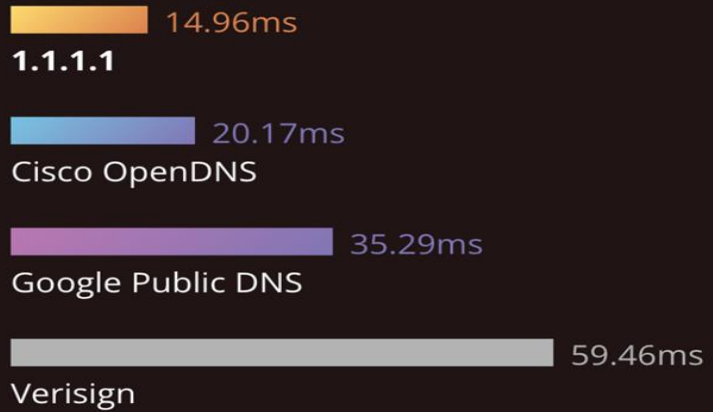
DNSperf.com (fuente)

El más rápido del mercado.

Hemos desarrollado 1.1.1.1 para que sea el directorio de DNS más rápido de Internet. No es necesario que confíe en nuestra palabra. El monitor de DNS independiente DNSPerf califica 1.1.1.1 como el servicio de DNS más rápido del mundo.

Dado que casi toda su actividad en Internet empieza por una solicitud de DNS, optar por el directorio de DNS más rápido para todos tus dispositivos, le permitirá acelerar prácticamente toda su actividad en línea.

* March, 2020



radar.cloudflare.com

CLOUDFLARE

Cloudflare Radar

DDoS Attack Trends for Q1 2022

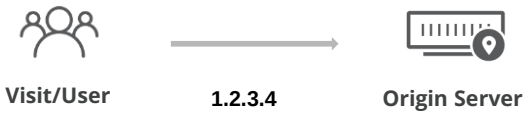
Visit DDoS report for

2022 Q1

Created by Cloudflare DDoS Team
Published on April 12, 2022
Tags DDOS SECURITY 2022 Q1
Links Cloudflare Blog: DDoS Attack Trends for Q1 2022

Table of Contents

Con un proxy inverso, la configuración es un cambio de DNS



Sin Cloudflare, un servidor de origen está expuesto a visitantes y atacantes.

Con Cloudflare, todas las solicitudes se envían al centro de datos más cercano a través de Anycast y proxy al origen.

CLOUDFLARE

Resumen de 2021

Ataques de rescate

Los ataques a infraestructuras críticas predominaron en el primer semestre de 2021 y continuaron a lo largo del año.

Los ataques DDoS de rescate fueron llevados a cabo en solitario por bandas, como Fancy Bear, Fancy Lazarus, o en conjunto con ataques de ransomware por bandas como REvil y **Conti**.

Nuevos botnets

Botnet Meris

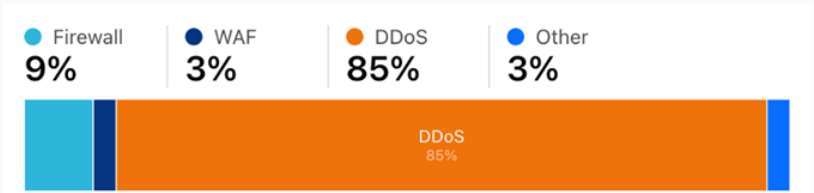
- responsable de algunos de los ataques DDoS más grandes jamás vistos;
- solía lanzar un promedio de 104 ataques DDoS diarios a clientes de Cloudflare.

Ataques a VoIP

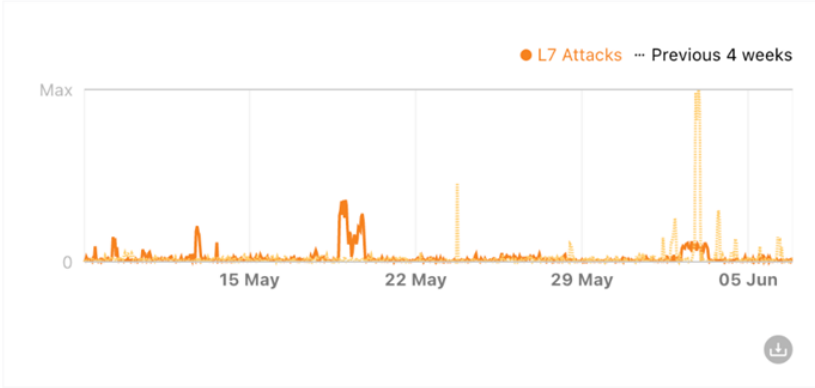
Gran cantidad de ataques a servicios VoIP (puertos SIP) en octubre/noviembre de 2021

Importantes interrupciones de servicio en los principales proveedores de VoIP

Distribution of Layer 7 attacks by mitigation techniques deployed to block them.



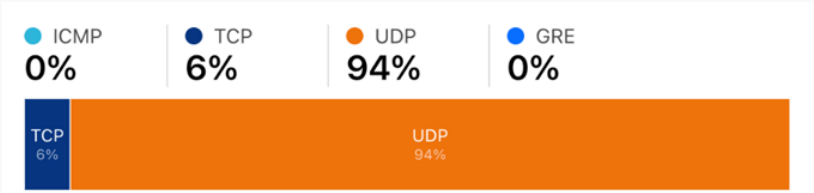
Layer 7 attack volume over the selected time period. Explore the right security solution for your Internet properties.



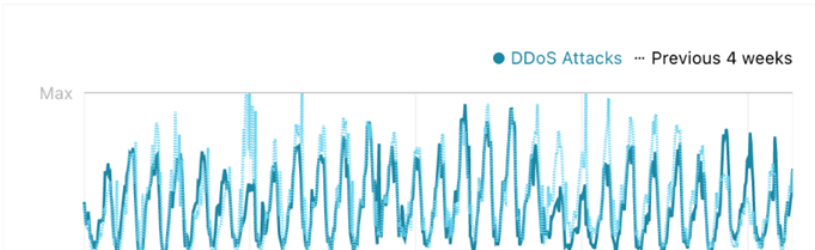
Network-level DDoS Attacks originating in Costa Rica

Learn More

Distribution of Layer 3/4 DDoS attacks by different attack types.



Layer 3/4 DDoS attack volume over the selected time period. Learn how to secure your websites, applications, and networks against DDoS attacks.



TP240PhoneHome (CVE-2022-26143)

La vulnerabilidad de Mitel

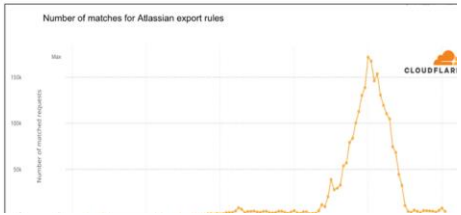
Zero Day threats

CLOUDFLARE

Cloudflare observations of Confluence zero day (CVE-2022-26134)

06/05/2022

On 2022-06-02 at 20:00 UTC Atlassian released a Security Advisory relating to a remote code execution (RCE) vulnerability affecting Confluence Server and Confluence Data Center products. This post covers our current analysis of this vulnerability...



Protection against CVE-2021-45046, the additional Log4j RCE vulnerability

12/15/2021

How Cloudflare helped mitigate the Atlassian Confluence OGNL vulnerability before the PoC was released

WAF Rules | Security | Vulnerabilities | Cloudflare Access

On August 25, 2021, Atlassian released a security advisory affecting their Confluence application. The Cloudflare WAF soon after started mitigating an increase in malicious traffic to vulnerable endpoints ensuring customers remained protected....

Protecting against recently disclosed Microsoft Exchange Server vulnerabilities: CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065

Vulnerabilities | WAF | WAF Rules

Cloudflare has deployed managed rules protecting customers against a series of remotely exploitable vulnerabilities that were recently found in Microsoft Exchange Server....

 Patrick R. Donahue  Gabriel Gabor

November 13, 2020 7:06PM

Stopping Drupal's SA-CORE-2019-003 Vulnerability

Drupal | WAF | WAF Rules | Security | Vulnerabilities

Drupal discovered a severe vulnerability and said they would release a patch. When the patch was released we analysed and created rules to mitigate these. By analysing the patch we created WAF rules to protect Cloudflare customers running Drupal....

 Richard Sommerville

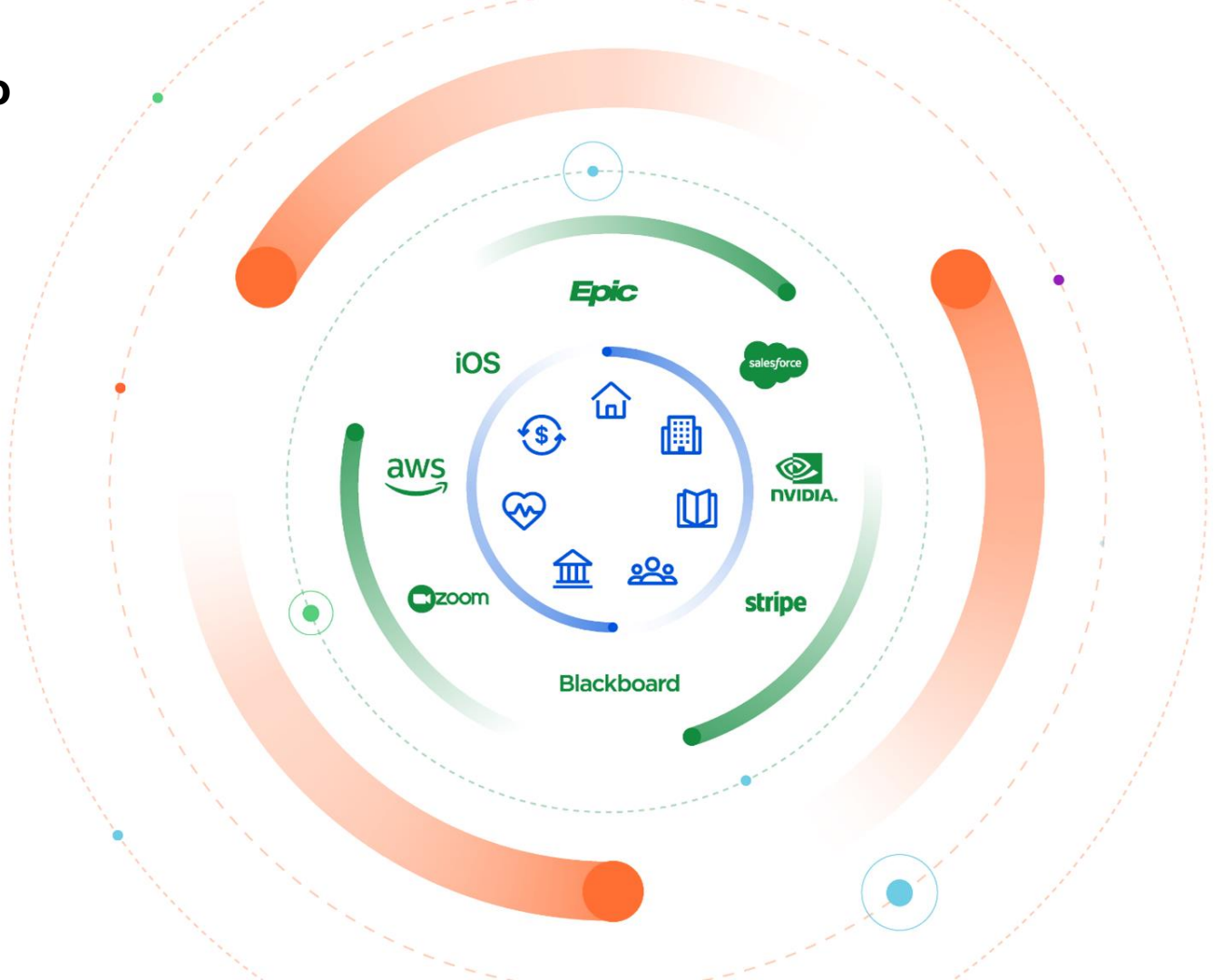
September 05, 2018 3:58PM

¿Qué está ocurriendo en el mundo actual?

Todo tiende a la digitalización

Con el uso de plataformas especializadas en la nube

Y todo funciona con Internet, pero...



CLOUDFLARE

Internet no es lo bastante:

Seguro 

Fiable 

Privado 

Automatizado 

CLOUDFLARE

La red troncal global de fibra óptica de Cloudflare

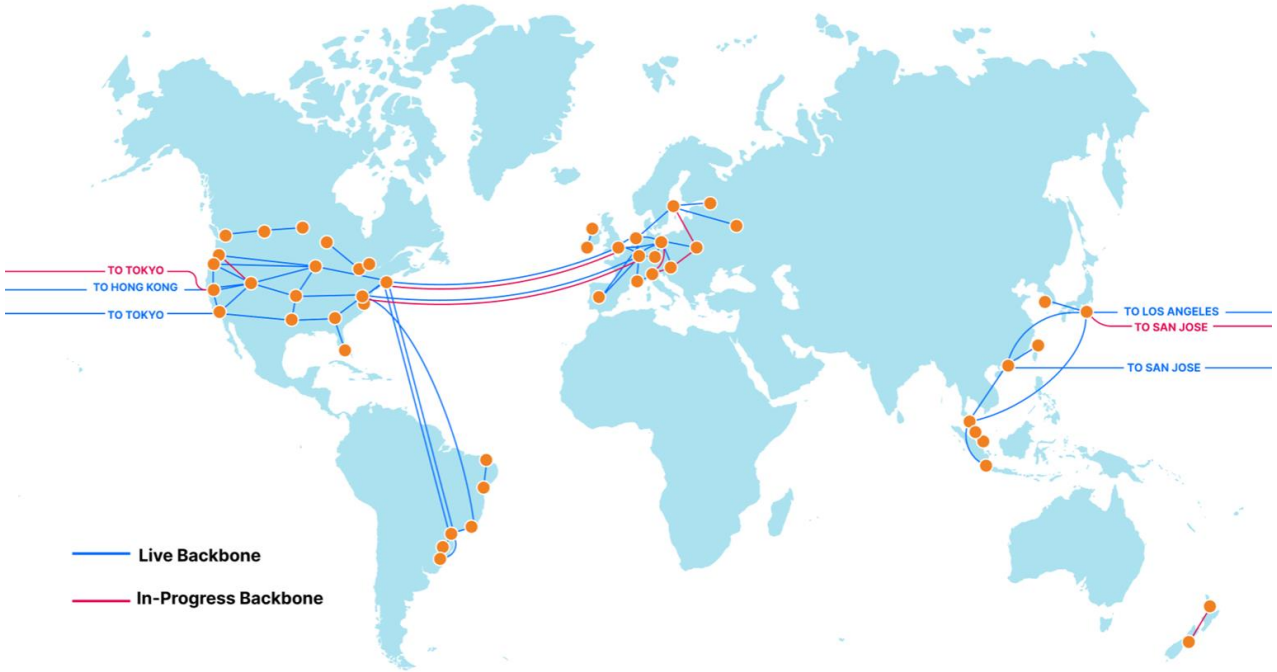
Red troncal de fibra óptica global de rápido crecimiento

Más de 230 enlaces de fibra óptica
45% metro, 55% larga distancia

Mejor confiabilidad y rendimiento

Mayor seguridad y privacidad

Ingeniería de tráfico inteligente con Argo Smart Routing



https://blog.cloudflare.com/250-cities-is-just-the-start/

As of Sept 2021

Datos de inteligencia sobre amenazas gracias a la red global de Cloudflare

Más de 275

ciudades en más de 100 países, incluida China continental

10 500

redes directamente conectadas a Cloudflare, incluidos ISP, proveedores en la nube y grandes empresas

142 Tbps

de capacidad del perímetro de la red en constante crecimiento

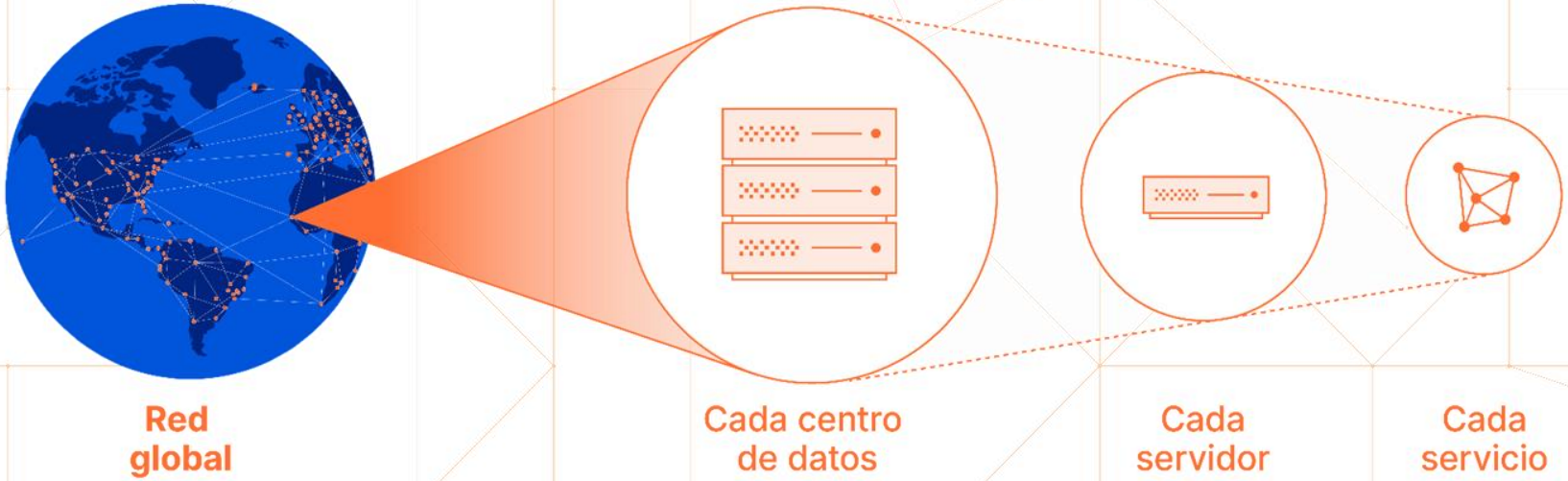
117 mil millones

de amenazas cibernéticas bloqueadas por día, incluyendo unos de los más grandes de la historia

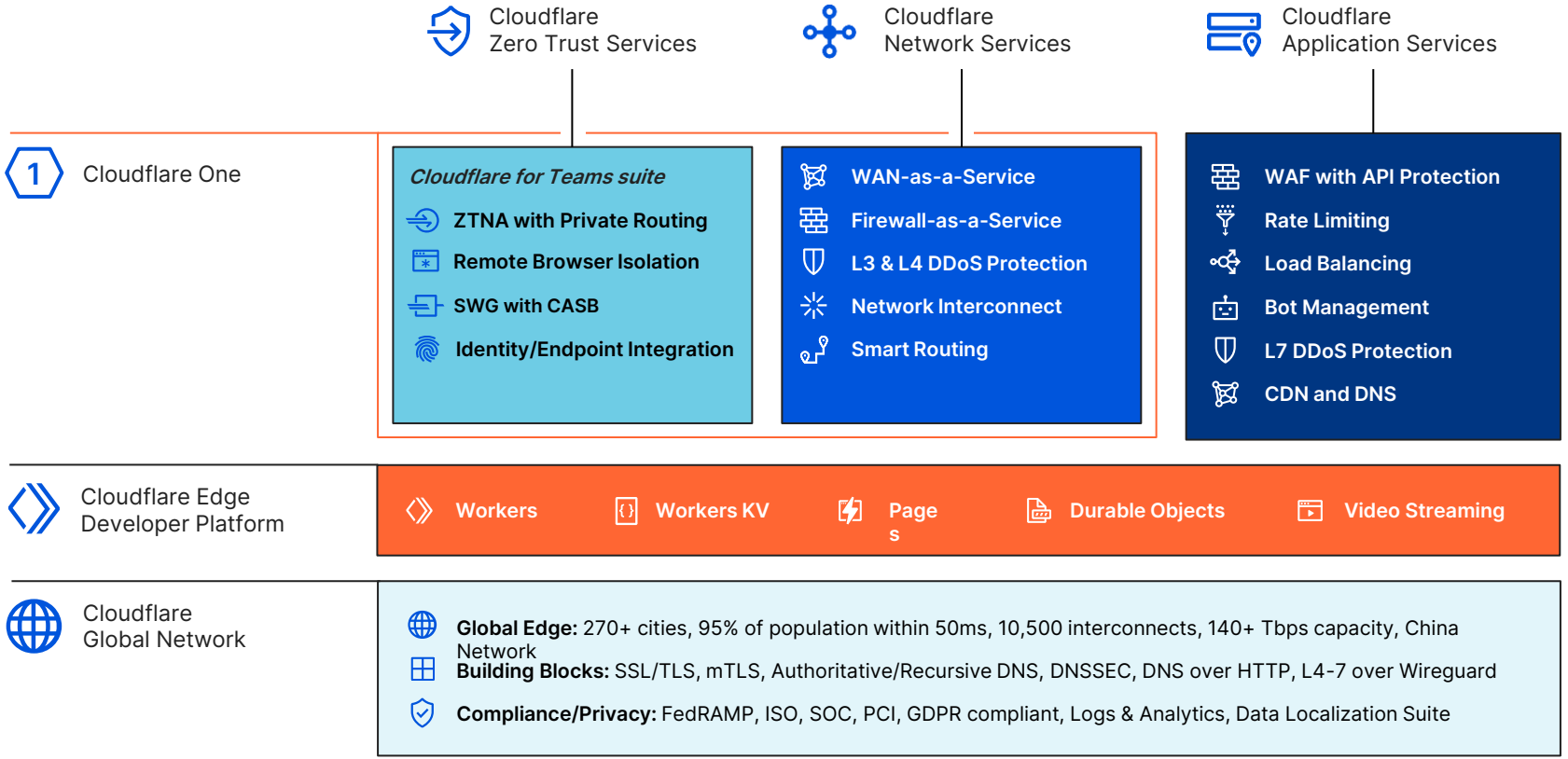
● = ciudad de Cloudflare (datos del mapa a fecha 15 de diciembre de 2021)

CLOUDFLARE

El poder de cada servicio en todas partes



Cloudflare at a Glance



ZTNA = Zero Trust Network Access | SWG = Secure Web Gateway | CASB = Cloud Access Security Broker

Cloudflare Zero trust: Access y Gateway Integrado

Access

Seguridad Zero Trust para
todas las aplicaciones

- Aplique políticas de acceso unificado a las aplicaciones internas que tradicionalmente requieren conexiones a una VPN, así como aplicaciones SaaS
- Aplique señales adicionales, como la postura del dispositivo, a sus políticas de acceso, mejorando la seguridad sin costosas actualizaciones de IDP
- Registre y revise cada evento y solicitud con una granularidad sin precedentes
- Agregue identidad de múltiples fuentes para simplificar el control de acceso para fusiones y adquisiciones, contratistas, socios y más
- Mejore la velocidad de entrega de aplicaciones con la escala de red y el enrutamiento inteligente de Cloudflare

Gateway

Usuarios, dispositivos y redes seguras
en la Internet abierta

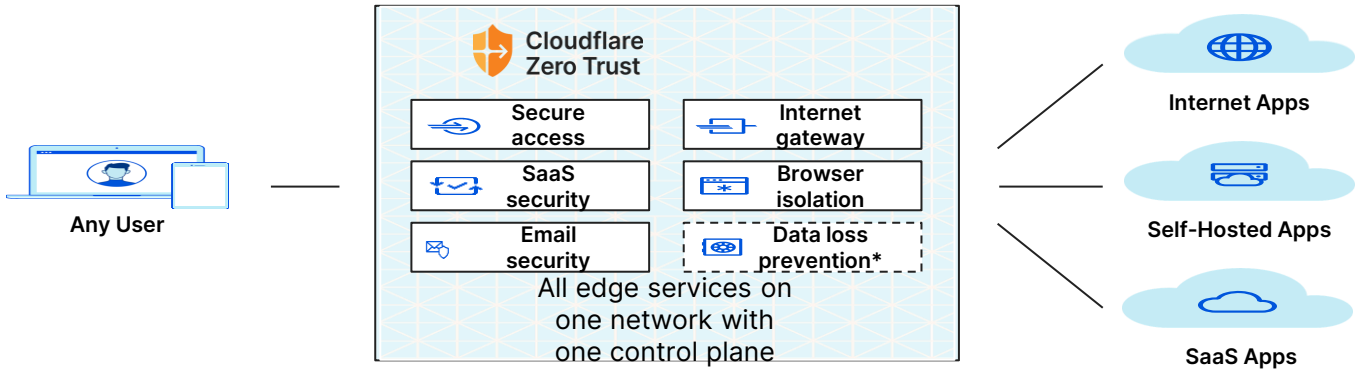
- Pase del sandboxing de amenazas en las instalaciones a la captura de amenazas en el perímetro de nuestra red
- Hacer cumplir el filtrado de URL sin tarifas de software adicionales
- Proteja el tráfico de las sucursales sin hardware o backhauling centralizado
- Inspeccione el tráfico de aplicaciones SaaS para prevención de pérdida de datos y auditoría de cumplimiento
- Aislar páginas web en Edge de Cloudflare con Browser isolation
- Elimine costosas tarifas de MPLS

PLATFORM OVERVIEW: CLOUDFLARE ZERO TRUST

Cloudflare Zero Trust incluye capacidades que abarcan múltiples áreas:

- Zero Trust Network Access (ZTNA)
- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB)
- Integrated Cloud Email Security (ICES)
- Data Loss Prevention (DLP)
- Remote Browser Isolation (RBI)

También es un componente fundamental de la oferta perimetral del servicio de acceso seguro (SASE) de Cloudflare, Cloudflare One™.

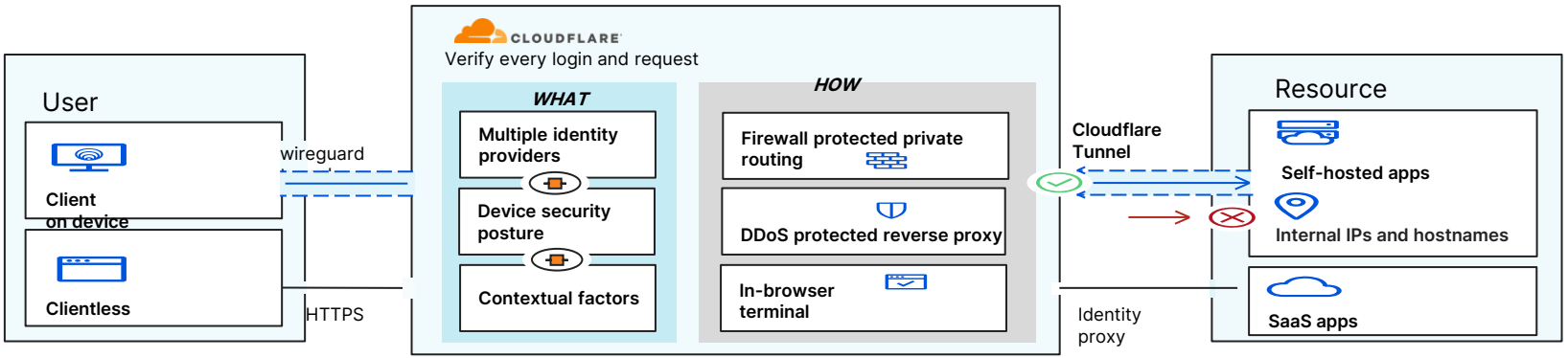


PRODUCT OVERVIEW: CLOUDFLARE ACCESS

Con la tecnología de la amplia y eficaz red Anycast de Cloudflare, hace que las conexiones de los usuarios sean más rápidas que una VPN.

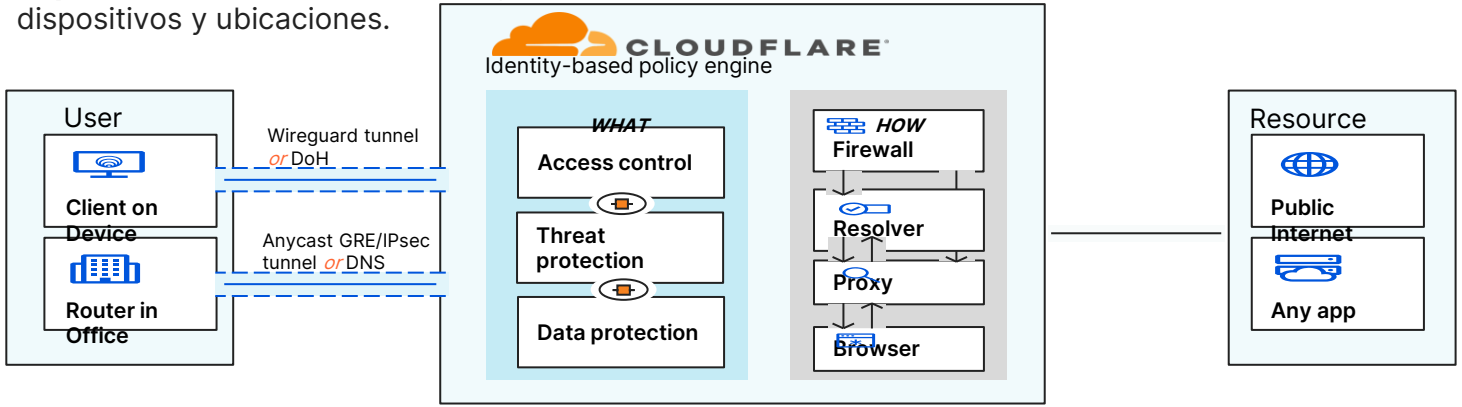
Cloudflare Access puede proteger:

- Aplicaciones web privadas o self hosted
- aplicaciones SaaS
- Aplicaciones no web (incluidas las conexiones SSH, VNC y RDP, SMB, Kubectl, CLI)
- IP internas y nombres de host



DESCRIPCIÓN DEL PRODUCTO: GATEWAY DE CLOUDFLARE

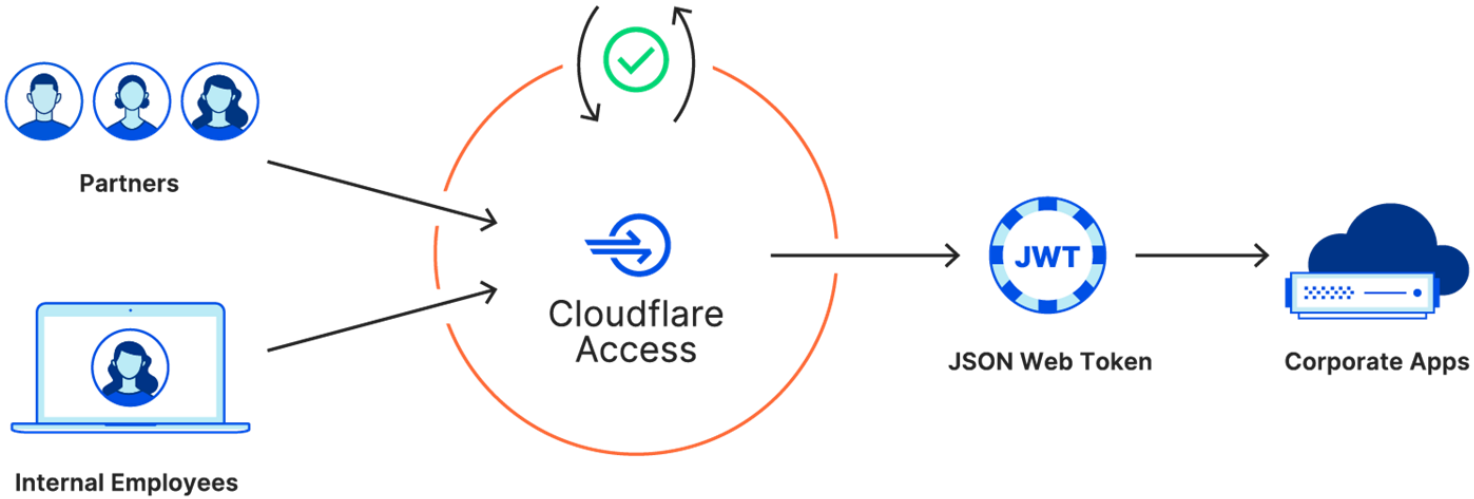
- **Bloquee amenazas conocidas y desconocidas en Internet:** bloquee el acceso a sitios potencialmente riesgosos a nivel de dominio o URL con nuestro corpus masivo de inteligencia de amenazas, que incluye más de 100 categorías de seguridad, contenido y basadas en aplicaciones para facilitar la creación de políticas.
- **Controle el flujo de datos dentro y fuera de su organización:** implemente la prevención de pérdida de datos (DLP) con controles de tipo de archivo que pueden evitar que los usuarios carguen archivos en los sitios. Impida las descargas maliciosas impidiendo que los usuarios descarguen tipos específicos de archivos.
- **Fortalecer el control de aplicaciones SaaS:** descubra el uso no aprobado de aplicaciones SaaS y use el motor de políticas de Gateway para bloquear el acceso a aplicaciones no aprobadas. Integre las identidades y los roles de los usuarios para limitar el acceso a subdominios y funciones específicos de las aplicaciones SaaS empresariales.
- **Supervise el tráfico en su red:** Proporcione visibilidad de su tráfico web y de Internet, en todos los usuarios, dispositivos y ubicaciones.



Access: Endpoint Protection

CLOUDFLARE

Identity Providers	Endpoint Protection Providers
SAML	vmware Carbon Black
	CROWDSTRIKE TANIUM



CLOUDFLARE

Cloudflare Gateway

Identity-Based Policy Engine

Office user

Known location IP

DNS query

Coming soon:
L4-7 traffic

Remote user

Device Agent

Encrypted
L4-7 traffic

Recursive DNS Resolver

Security, Content, and Application Groups
Domain and IP Filters

Traffic Inspection Proxy

HTTPS Decryption, File and Data Scanning, AV
URL, HTTP, and MIME/File Type Filters

Zero Trust Browser

Untrusted Web Code Executed Away From Device

app.com

CLOUDFLARE

This month, CISA will be focused on ensuring the public is practicing good “cyber hygiene,” easy and common-sense steps to protect yourself online. We urge everyone to implement these four easy things you can do on your devices:

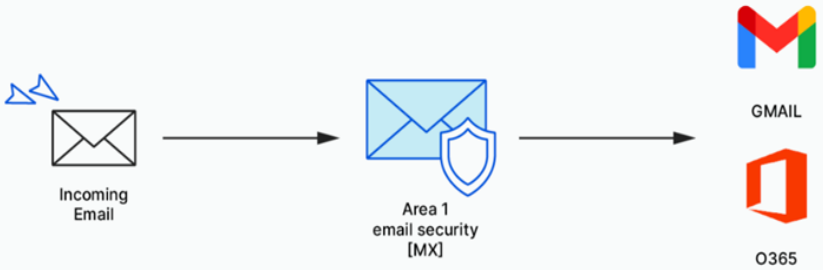
- Implement multi-factor authentication on your accounts and make it 99% less likely you’ll get hacked.
- Update your software. In fact, turn on automatic updates.
- Think before you click. Over 90% of successful cyber attacks start with a phishing email.
- Use strong passwords, and ideally a password manager to generate and store unique passwords.

More information on the 4 Things You Can Do to Keep Yourself Cyber Safe is available on CISA.gov.

Se integra a traves de DNS records MX

Se adapta perfectamente a cualquier estructura de seguridad del correo electrónico

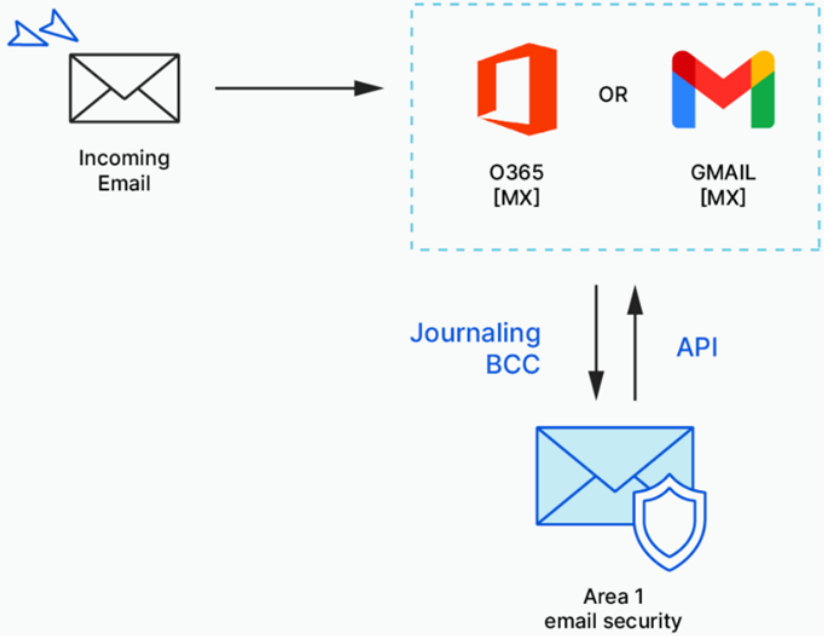
- Implementa en minutos sin necesidad de hardware, agentes o dispositivos.
- Elige la opción de implementación que mejor se adapte a tu organización: en línea, API o multimodo.
- Amplía la protección del correo electrónico a tus proveedores y socios preferidos.
- Agiliza las investigaciones del centro de operaciones de seguridad con retracciones de mensajes posteriores a la entrega e integraciones con plataformas SIEM/SOAR.



Implementación via API

Se adapta perfectamente a cualquier estructura de seguridad del correo electrónico

- Implementa en minutos sin necesidad de hardware, agentes o dispositivos.
- Elige la opción de implementación que mejor se adapte a tu organización: en línea, API o multimodo.
- Amplía la protección del correo electrónico a tus proveedores y socios preferidos.
- Agiliza las investigaciones del centro de operaciones de seguridad con retracciones de mensajes posteriores a la entrega e integraciones con plataformas SIEM/SOAR.



CLOUDFLARE

La red para la transformación digital

ENERO DE 2022

CLOUDFLARE

Gracias!

armando@cloudflare.com
+1 512 287 1519