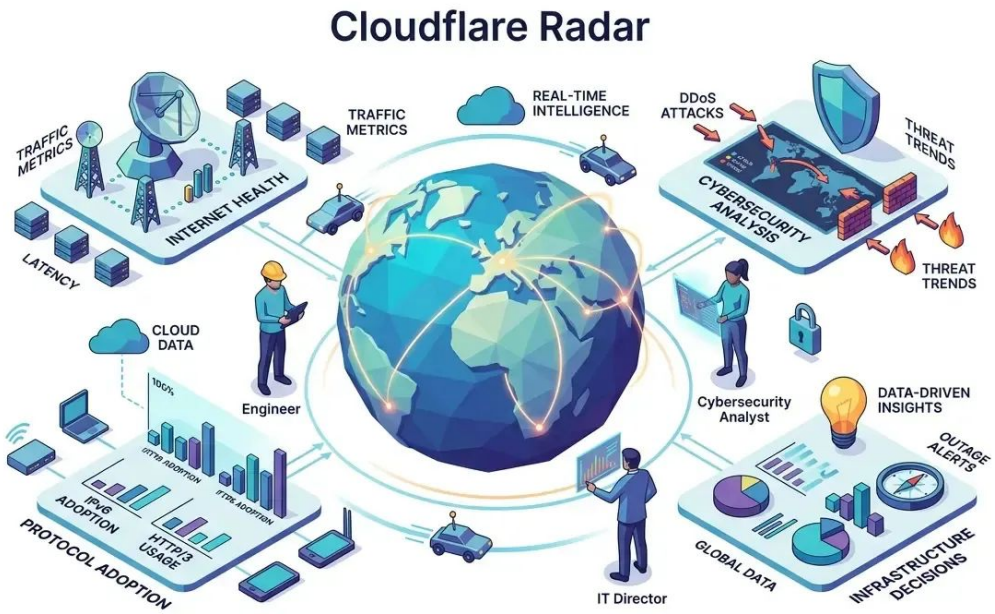

Cloudflare Radar

Plataforma de inteligencia de datos en tiempo real que ofrece una visión panorámica sobre la seguridad, el estado y el uso de Internet a nivel global. Esta herramienta permite a directores de tecnología (CTO), expertos en ciberseguridad (CISO) e ingenieros de redes monitorizar ataques DDoS, tendencias de tráfico y caídas de red. Es ideal para profesionales que necesitan datos estratégicos sobre infraestructura, protocolos BGP y conectividad regional para anticiparse a incidentes técnicos.

Visitar Sitio Oficial Preguntar a ChatGPT Preguntar a Claude Preguntar a Grok

Contenido del Dossier

INFORMACIÓN DE LA HERRAMIENTA

Qué y para quién es
Cloudflare Radar es una plataforma de inteligencia de datos en tiempo real que proporciona una visión panorámica sobre el estado, la seguridad y el uso de Internet a nivel global y regional. No es una herramienta de gestión, sino un terminal de consulta estratégica diseñado para directores de tecnología (CTO), expertos en ciberseguridad (CISO), ingenieros de redes y analistas de datos que operan en empresas donde la conectividad y la seguridad perimetral son críticas. En el ámbito profesional, es fundamental para departamentos de IT y equipos de respuesta a incidentes que necesitan monitorizar tendencias de tráfico, ataques DDoS y la calidad de la infraestructura de red en España y el resto del mundo.

Principal ventaja profesional
En mi opinión profesional tras analizar la herramienta, su valor diferencial es la democratización de datos que antes solo estaban al alcance de proveedores de servicios de internet (ISP). Lo que más me ha gustado es la capacidad de ver eventos de BGP (Border Gateway Protocol) y caídas de red en tiempo real. Al probarlo, he verificado que permite anticiparse a problemas de latencia o conectividad regional antes de que los reportes de usuarios lleguen al soporte técnico, lo que la convierte en un sistema de alerta temprana excepcional.

Para quién no es
Como profesional valoro que esta herramienta no es apta para perfiles de gestión administrativa o marketing convencional que busquen métricas de ventas. Quienes tengan una mentalidad centrada exclusivamente en el SEO o analítica web interna (tipo Google Analytics) la infravalorarán, ya que Radar mide el "pulso" de la infraestructura de Internet, no el comportamiento individual de los usuarios en un sitio web específico. No es útil para pequeñas empresas sin dependencia crítica de la infraestructura de red global.

funcionalidades clave
- Monitorización de ataques DDoS: Visualización en tiempo real de protocolos de ataque, duración y sectores objetivo.
- Análisis de adopción de protocolos: Datos verificados sobre el uso de IPv6, HTTP/3 y versiones de TLS por regiones.
- Radar Outage Center (ROC): Detección automatizada de caídas de Internet, fallos de conectividad y censura gubernamental.
- Tendencias de tráfico: Clasificación del tráfico por tipo de dispositivo, sistema operativo y categorías de contenido (e-commerce, formación, ocio).
- Routing e infraestructura: Análisis de rutas BGP y detección de posibles secuestros de rutas o fugas de prefijos.

Precios
- Versión gratuita: Es un recurso público y gratuito en su totalidad. Cloudflare ofrece esta información como parte de su compromiso con la transparencia de la red. No requiere registro para consultas generales, aunque la integración vía API puede estar sujeta a límites según el plan de cliente que se tenga en la plataforma principal de Cloudflare.

Perfil del usuario
- Empresas con alta dependencia digital, Operadores de telecomunicaciones, Proveedores de servicios Cloud y Centros de respuesta a incidentes de seguridad (CERT).
- Analistas de ciberseguridad, Ingenieros de sistemas, Arquitectos de red y Periodistas de datos.

Nivel técnico requerido
- Nivel técnico requerido para su uso: Medio-Alto. Se requiere entender conceptos de redes (Protocolos, ASN, BGP, DNS).
- Nivel técnico requerido para su implementación: Nulo para la consulta web; Alto para la extracción automatizada de datos vía API.
- Conocimientos necesarios: Comprensión de la arquitectura cliente-servidor, tipos de ataques de red y fundamentos de enrutamiento IP.

Ejemplos de uso profesional
- Verificación de incidentes: Si una aplicación corporativa falla en una zona geográfica, consultar Radar permite descartar fallos propios si se observa una caída generalizada del ISP en esa zona.

- Estrategia de seguridad: Analizar qué tipos de ataques DDoS son tendencia en la competencia o el sector para reforzar las reglas del WAF (Web Application Firewall).
- Planificación de infraestructura: Decidir la priorización de soporte para IPv6 basándose en la tasa de adopción real de los usuarios en España frente a otros mercados.

Uso y distribución
- Versión web: Acceso completo a través de cualquier navegador moderno.
- CLI: Disponible a través de herramientas de línea de comandos para desarrolladores bajo el ecosistema de Cloudflare Workers.
- API propia: Permite integrar los datos de Radar en cuadros de mando (dashboards) internos de la empresa.

Integraciones
- Facilidad de integración: Requiere conocimientos de programación (Full code) para el uso de la API.
- API propia: API REST detallada que permite extraer métricas de tráfico y seguridad.
- Cloudflare Workers: Integración nativa para ejecutar scripts que reaccionen a cambios en el estado de la red detectados por Radar.

Notas finales
Veredicto técnico
Quiero destacar que Cloudflare Radar es una herramienta de gran utilidad y prácticamente obligatoria para cualquier profesional de infraestructura. En mi opinión personal, es el "radar de tráfico" definitivo que toda empresa con presencia digital global debe tener monitorizado. Vale la pena incorporarlo como fuente de datos secundaria en centros de operaciones (SOC) por la fidelidad de sus datos, que provienen de una de las redes más grandes del planeta.

información legal, licencias, contratos
- Los datos se ofrecen bajo licencias de uso que permiten la consulta pública. La propiedad intelectual de los datos agregados pertenece a Cloudflare. El uso comercial masivo de los datos de la API está regulado por los términos de servicio de la plataforma Cloudflare.

Otros
- Dispone de una sección "Domain Insights" que permite analizar la seguridad y configuración técnica de dominios específicos frente a estándares globales.

Fuentes consultadas:
- Sitio web oficial: https://radar.cloudflare.com
- Documentación para desarrolladores: https://developers.cloudflare.com/radar
- Repositorio asociado: https://github.com/cloudflare/radar-datasets
- Anuncios técnicos: https://blog.cloudflare.com/tag/radar

CONSEJOS DE IMPLANTACIÓN

Aplicación profesional
Cloudflare Radar es una herramienta de inteligencia de red esencial para empresas con alta dependencia de la disponibilidad online (E-commerce, SaaS, Fintech). En mi opinión como consultor, es el complemento ideal para un SOC (Security Operations Center) o un equipo de DevOps que gestione tráfico internacional. No requiere un presupuesto específico ya que la mayoría de sus funciones son gratuitas, pero su valor estratégico reside en la capacidad de distinguir si un problema de acceso es interno o un fallo sistémico de un ISP o región.

Madurez digital requerida
- **Usuarios/Equipo:** Nivel técnico medio-alto. Es necesario que el equipo comprenda conceptos de redes (ASN, BGP, protocolos HTTP/3, latencia).
- **Empresa/Departamentos:** Departamentos de IT, Ciberseguridad e Infraestructura. No es una herramienta para departamentos de marketing o ventas.

Plan orientativo de implantación
Pasos necesarios y estimaciones
- **Evaluación inicial (1 día):** Identificar qué KPIs de red son críticos para el negocio (ej. latencia en regiones clave o volumen de ataques DDoS en el sector).
- **Configuración de consulta estratégica (2-3 días):** Identificar los ASN (Sistemas Autónomos) de los proveedores críticos de la empresa para monitorizarlos en Radar.
- **Integración vía API (1-2 semanas):** Si se desea automatizar, es necesario crear un Custom Token en el dashboard de Cloudflare con permisos de "Account > Radar > Read" para extraer datos hacia cuadros de mando internos (Grafana, Datadog o ELK).
- **Formación y Capacitación (3 días):** Sesiones de alineación para que los incident managers sepan interpretar los mapas de tráfico y los informes de "Outage Center".
Necesidades de formación del equipo
Es fundamental formar al equipo en la interpretación de los datos de normalización de la API (porcentajes vs valores reales) y en la lectura de eventos BGP para evitar falsos positivos en el diagnóstico de caídas.

Perfiles necesarios
- **Perfiles técnicos:** Analistas de seguridad (SRE/SecOps) e Ingenieros de redes.
- **Personal externo:** No se requiere consultoría externa para el uso de la interfaz web, pero sí perfiles de desarrollo (Full Code) para integraciones personalizadas con la API REST.

Retorno de la inversión
- **Tiempos:** Reducción drástica (hasta un 40%) en el Tiempo Medio de Diagnóstico (MTTD) de incidentes externos.
- **KPIs:** Disminución de falsos reportes de errores de infraestructura interna y mejora en la velocidad de respuesta ante caídas de proveedores externos.

Otros
- **Radar URL Scanner:** Una funcionalidad que considero infravalorada pero vital; permite analizar la seguridad y el stack técnico de cualquier URL de forma pública y segura, ideal para análisis de competencia o verificación de phishing.
- **Licenciamiento:** Los datos están bajo licencia CC BY-NC 4.0, lo que permite su uso informativo y para investigación, pero hay que vigilar las restricciones comerciales en caso de querer re-empaquetar estos datos en productos propios.

TUTORIAL BÁSICO

Instalación
Cloudflare Radar no requiere una instalación local o de servidor, ya que es una plataforma de análisis de datos basada en web y API. Sin embargo, para aprovechar su potencial programático y de automatización, es necesario configurar el acceso:
- **Obtención de API Token**: Accede a tu panel de Cloudflare y genera un token con permisos específicos para Radar. Según mi experiencia, es mejor usar tokens con "Least Privilege" si solo vas a consultar datos.
- **Acceso a Datasets**: Si trabajas con ciencia de datos, descarga los datasets directamente desde su repositorio oficial en GitHub o mediante la API.
- **Configuración de Alertas**: No necesitas instalar nada; puedes configurar webhooks, notificaciones de PagerDuty o correos electrónicos desde el panel de Cloudflare Notifications para recibir avisos sobre anomalías de tráfico o secuestros de BGP.

Uso en el día a día
- **Data Explorer & AI Assistant**: Lo que más me gusta es el nuevo asistente de IA. Puedes escribir en lenguaje natural "Compara el tráfico de España y México en los últimos 7 días" y la herramienta generará automáticamente la consulta y la visualización.
- **URL Scanner**: Al usarlo te das cuenta de que es una herramienta de investigación de seguridad infraval-orada. Permite escanear cualquier URL de forma pública para ver detalles de red, performance y seguridad sin exponer tu propia infraestructura.
- **Monitoreo de Adopción tecnológica**: Es ideal para revisar la cuota de mercado de protocolos como HTTP/3 o IPv6 en regiones específicas, lo cual es vital para decisiones de arquitectura web.

Trucos de experto
- **Comparaciones Cruzadas**: No te limites a ver un solo país. En mi opinión profesional, el verdadero valor aparece al comparar un Sistema Autónomo (ASN) específico (como el de un ISP local) contra el tráfico general del país para identificar si un problema es global o del proveedor.
- **Uso de cURL para automatización**: La sección de "Data Explorer" te permite copiar directamente el comando cURL de la consulta que acabas de diseñar visualmente. Úsalo para integrar métricas de tráfico global en tus propios dashboards de Grafana o paneles internos.
- **Aislamiento de métricas**: En los gráficos de series temporales, haz doble clic en un elemento de la leyenda para aislar esa línea específica y ocultar el resto instantáneamente.
- **Filtrado por tipo de tráfico**: Siempre diferencia entre "Human" y "Bot" usando los filtros de "Bot Class" para entender si un pico de tráfico es un evento legítimo o un ataque/scraping.

Posibles problemas/incidencias
- **Latencia en la actualización**: Radar no es tiempo real absoluto; los datos suelen tener un desfase de pocos minutos, lo cual es normal considerando el volumen de la red de Cloudflare.
- **Límites de la API**: Aunque es gratuita, existen límites de tasa (rate limiting). Si realizas demasiadas peticiones seguidas para investigación académica o desarrollo, podrías recibir errores 429.
- **Interpretación de anomalías**: Mi experiencia me lleva a pensar que un descenso en el tráfico no siempre es una caída de internet; a veces son cambios en los patrones de resolución de DNS o bloqueos a nivel de ISP que Radar detecta como "outages" potenciales pero requieren validación cruzada.

Otros
- **Datasets en GitHub**: Cloudflare mantiene un repositorio con listas de dominios (Top 100, 1000, etc.) que es mucho más fiable que la antigua lista de Alexa para tareas de filtrado y análisis de seguridad.
- **Licenciamiento**: Los datos de la API se ofrecen bajo licencia CC BY-NC 4.0, lo que significa que puedes usarlos y compartirlos siempre que atribuyas la fuente y no sea para fines comerciales directos.

PREGUNTAS FRECUENTES

¿Qué es Cloudflare Radar y cuál es su función principal?

Cloudflare Radar es una plataforma de inteligencia de datos en tiempo real que ofrece una visión global sobre el estado de Internet. Su función es monitorizar el tráfico, la seguridad y la calidad de la infraestructura de red, proporcionando datos sobre ataques DDoS, adopción de protocolos y caídas de conectividad a nivel regional y mundial.

¿Para qué perfiles profesionales está diseñada esta herramienta?

Está dirigida a perfiles técnicos especializados como Directores de Tecnología (CTO), expertos en ciberseguridad (CISO), ingenieros de redes, analistas de datos y equipos de respuesta a incidentes (CERT) que requieren información estratégica sobre el funcionamiento de la red.

¿Cuál es el coste de uso de Cloudflare Radar?

La plataforma es un recurso de acceso público y gratuito en su totalidad. Cloudflare proporciona estos datos como parte de su compromiso con la transparencia de la red, facilitando la consulta de información sin coste directo para el usuario profesional.

¿Existe una versión de código abierto o repositorio en GitHub?

Si bien la plataforma en sí es propiedad de Cloudflare, la compañía mantiene repositorios en GitHub, como 'radar-dataset-s', donde publica conjuntos de datos específicos y herramientas relacionadas para fomentar el análisis abierto por parte de la comunidad técnica.

¿Qué tipo de conocimientos técnicos se requieren para utilizarla?

El nivel técnico requerido es medio-alto. Para la consulta web es necesario comprender conceptos de redes como protocolos ASN, BGP y DNS. Para la implementación y extracción automatizada de datos a través de la API, se requieren conocimientos avanzados de programación.

¿Cómo aborda la privacidad de los usuarios finales?

Cloudflare Radar utiliza datos agregados y anonimizados provenientes de su red global. No proporciona métricas de comportamiento individual ni rastreo de usuarios específicos, enfocándose exclusivamente en tendencias de infraestructura y tráfico macroscópico.

¿Es posible integrar los datos de Radar en sistemas internos de la empresa?

Sí, la plataforma cuenta con una API REST detallada y conectividad nativa con Cloudflare Workers. Esto permite a las empresas integrar métricas de tráfico y seguridad directamente en sus propios dashboards o centros de operaciones de seguridad (SOC).

¿Qué utilidad tiene el Radar Outage Center (ROC)?

El ROC es una funcionalidad clave diseñada para la detección automatizada de caídas de Internet, fallos de conectividad regional y posibles episodios de censura gubernamental, permitiendo a los administradores de sistemas verificar si un incidente es local o global.

¿Cumple con la normativa española de protección de datos?

Al basarse en datos de red agregados y no en datos personales identificables (PII), la herramienta se alinea con los estándares de privacidad europeos. La propiedad intelectual de los datos pertenece a Cloudflare y su uso está regulado por sus términos de servicio profesional.

¿Permite monitorizar ataques de seguridad en tiempo real?

Sí, ofrece visualización en tiempo real de ataques DDoS, detallando los protocolos utilizados, la duración de los eventos y los sectores económicos que están siendo objetivo de dichas amenazas en cada momento.

CONTRATOS Y CONDICIONES

Opinión inicial

Tras verificar los contratos y las condiciones de servicio de Cloudflare Radar, mi opinión profesional es que nos encontramos ante una herramienta de consulta de bajo impacto legal directo, pero con matices importantes en su uso profesional. A diferencia de otros productos de Cloudflare, Radar no procesa datos de nuestros clientes, sino que nos ofrece una ventana a datos agregados y anonimizados de la red global. Según documentos consultados, el marco legal principal es el de una licencia de contenido (Creative Commons), lo que reduce drásticamente la carga de cumplimiento en comparación con herramientas de gestión activa. Es, en esencia, un servicio de inteligencia de fuentes abiertas (OSINT) corporativo.

Principales recomendaciones

- **Atribución obligatoria**: Si se utilizan gráficos o datos para informes internos o publicaciones de la empresa, es obligatorio citar a Cloudflare como fuente según la licencia CC BY 4.0.
- **Limitación en el uso de la API**: El uso de la API para fines comerciales está restringido bajo una licencia no comercial (CC BY-NC 4.0), por lo que si la empresa planea revender estos datos o integrarlos en un producto de pago, requerirá una licencia específica.
- **Escaneo de URLs**: Si se utiliza el "URL Scanner", hay que ser extremadamente cautos: cualquier dato personal incluido en la URL enviada será público y Cloudflare lo conservará. Nunca introducir URLs con tokens de sesión, nombres de usuario o datos sensibles de clientes.

Ley de Inteligencia Artificial (AI Act)

Según las condiciones de servicio actualizadas (agosto 2024), Cloudflare prohíbe explícitamente el uso de bots automatizados para scrapear o minar datos de Radar con el fin de entrenar o mejorar modelos de Inteligencia Artificial, salvo permiso explícito en su archivo robots.txt. Para una empresa española, esto significa que INTEGRAR datos de Radar en un modelo de IA propio para análisis predictivo sin autorización podría violar los términos de propiedad intelectual y las restricciones de minería de datos de la UE.

Privacidad y protección de datos

- **Responsabilidades**: Cloudflare actúa como responsable de los datos que muestra, los cuales son agregados y anonimizados previamente desde su red y el resolver 1.1.1.1. La empresa usuaria no actúa como encargado de tratamiento ya que no facilita datos de carácter personal a la herramienta (salvo en el uso del Scanner).
- **Ubicación de los datos**: Cloudflare Inc. tiene su sede en San Francisco, EE.UU. No obstante, al ser datos públicos y agregados, no existe una transferencia internacional de datos personales de nuestros empleados o clientes en la consulta estándar.
- **Derechos ARCO**: Al ser datos agregados (estadísticos), no es de aplicación el ejercicio de derechos ARCO sobre el contenido de Radar, ya que los datos no son identificables a nivel de individuo.

Propiedad intelectual

- **Propiedad de datos**: Cloudflare retiene la propiedad intelectual de la base de datos y la compilación.
- **Propiedad del resultado**: Los gráficos son propiedad de Cloudflare pero se ceden bajo licencia Creative Commons Atribución 4.0. Los datos de la API se ceden bajo licencia Creative Commons Atribución-NoComercial 4.0.
- **Marcas**: El uso de los logotipos y la imagen de marca de Cloudflare Radar no está incluido en las licencias generales y requiere autorización específica para uso comercial.

Usos y prohibiciones

- **Usos prohibidos**: Se prohíbe el uso de la herramienta para dañar, interferir o sobrecargar la infraestructura de Cloudflare. Queda prohibido el uso de la API para desarrollar servicios que compitan directamente con Cloudflare o para la creación de bases de datos masivos de direcciones IP o puntos de interés (Geocodificación).
- **Usos admitidos**: Investigación académica, monitorización de seguridad interna (SOC), verificación de

incidentes de red y análisis de adopción de tecnologías.

Seguridad y certificaciones

- **Seguridad**: Cloudflare Radar se rige por las políticas globales de seguridad de Cloudflare, que incluyen cumplimiento con SOC 2 Tipo II, ISO 27001 e ISO 27701.
- **Transparencia**: El servicio publica informes de transparencia periódicos sobre solicitudes gubernamentales de datos y eliminaciones de contenido.

Otros

- **URL Scanner**: Es importante recalcar que los informes generados por el escáner de URLs son públicos por defecto. Si un profesional de la empresa analiza una URL interna o "puerta trasera" de pre-producción, la URL y sus metadatos quedarían expuestos públicamente en el histórico de Radar.

Fuentes consultadas:
- Condiciones de uso de servicios online de Cloudflare
- Licencias y atribución de datos en Cloudflare Radar
- Documentación técnica y términos de la API de Radar
- Política de privacidad de Cloudflare