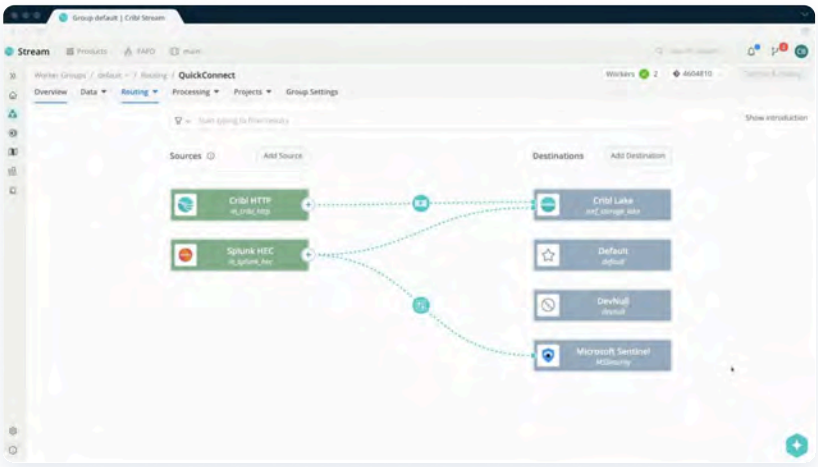
DATA SHEET

Cribl Stream™

Cribl

The **AI Platform** for Telemetry

Cribl Stream es una plataforma de manejo, procesamiento y envío de datos de tecnología y seguridad cibernética. Con Stream, puedes enviar, reducir, reformatear, enriquecer o dar forma a los datos desde cualquier origen hacia cualquier destino.



Elección y flexibilidad.

- Transmita eventos, métricas y rastros desde cualquier origen hacia cualquier destino, en cualquier formato.
- Agregue nuevas herramientas de análisis y otros destinos sin necesidad de añadir agentes o recolectores.

Controle sus datos.

- Envíe los datos a los equipos y las herramientas correctas.
- Implemente seguridad de alto nivel.
- Controle las políticas, los estándares y los formatos de datos utilizados en todo su arsenal de herramientas.

Observe más y gaste menos.

- Optimice la incorporación y recolección de datos y consiga datos que ni sabía que existía.
- Optimice su infraestructura, la ingesta de datos, el rendimiento de las herramientas y las horas de trabajo de su personal.

Cribl Stream ofrece a los administradores, un sólido control de acceso basado en roles, para que puedan asignar secciones específicas de flujos de datos a los usuarios o grupos responsables de llevar dichos datos a herramientas de análisis, seguridad u otros destinos.

Recolecte los datos correctos

Envíe datos de cualquier origen hacia cualquier herramienta (destino) en el formato correcto.

Reduzca sus datos

Elimine datos poco interesantes o innecesarios para controlar costos.

Dele forma a sus datos

Capture los datos de cualquier fuente y transfórmelos según sus necesidades.

Envíe sus datos

Coloque los datos donde generen mayor valor.

Repetición

Mantenga una copia de alta fidelidad de sus datos en almacenamiento de bajo costo y solicitelos según sea necesario.

Características del Producto

ARQUITECTURA

- Arquitectura distribuida sin estado compartido, súper escalable.
- Escala desde un portátil hasta cientos de nodos y miles de núcleos.
- Plataforma altamente paralelizable y de alto rendimiento, construida para la extensibilidad.
- Latencia inferior al milisegundo.
- Capacidad probada de hasta 20PB/día.
- **Opciones de despliegue:**
  - **OnPrem:** Binarios para Linux o Windows, contenedores Docker y charts de Helm para despliegue sencillo en cualquier entorno y runtime de K8s.
  - **Cloud:** Experiencia SaaS a través de Cribl.Cloud; completamente gestionada por Cribl, sin sobrecarga de infraestructura, con escalabilidad según sea necesario.
  - **Híbrido:** Plano Líder / Control en la nube y nodos Edge realizando el procesamiento local.
- Más de 80 integraciones de origen/destino disponibles de forma nativa, ahora con Packs para incorporar y compartir más rápido.
- Soporte nativo de protocolos para las principales fuentes y destinos de logs, métricas y rastros.
- Soporte TLS nativo para todas las integraciones que lo soportan.
- Soporte nativo para IAM compatible con SAML 2.0 y Assume Roles.
- Captura de datos en vivo para integración, resolución de problemas e inspección.
- Registro enriquecido, métricas y estado en tiempo real para cada integración.
- Pruebas de conectividad integradas y resultados para cada integración.
- Soporte para recolección de datos desde endpoints REST arbitrarios.
- Soporte para recolección de datos basada en scripts arbitrarios.
- Soporte para envío y recolección desde todos los principales servicios de almacenamiento Cloud PaaS.

GESTIÓN

- Control total de todos sus datos de tecnología y seguridad cibernética desde un centro de control único.
- Arquitectura de alta disponibilidad que ofrece conmutación del Líder (centro de control) con tolerancia a fallos en tiempo casi real on-premises y 99.9% de disponibilidad en Cribl.Cloud.
- El soporte de AuthZ mejora la seguridad al dar control sobre quién tiene permisos y privilegios para acceder a los productos, capacidades y recursos de Cribl.
- Stream Projects permite a los usuarios de Cribl acceder de forma segura a los datos a través de un modelo de autoservicio, liberando tiempo del administrador de Cribl para trabajar en tareas críticas para el negocio.
- Soporte de autenticación de nivel empresarial (LDAP, SSO, etc.).
- RBAC basado en políticas para permisos granulares.
- Interfaz de usuario intuitiva para la gestión de sistemas distribuidos.
- Gestión centralizada única a través de cloud o software autogestionado para cientos de grupos/nodos.
- Control de versiones de configuración con capacidad de revertir cambios.
- Soporte centralizado para la gestión de certificados y claves.
- Validación de cambios de configuración en tiempo real integrada.
- Generadores de datos integrados para pruebas de pipelines y destinos.
- Validación de cambios de configuración en tiempo real integrada.
- Generadores de datos integrados para pruebas de pipelines y destinos.
- Actualizaciones completamente automatizadas y distribuidas de todos los Workers de Stream.
- Acceso a servicios externos de gestión de claves para administrar secretos/tokens en todos los nodos.
- Sincronización integrada con repositorios de código externos para integraciones CI/CD y recuperación de desastres.
- Actualizaciones completamente automatizadas y distribuidas de todos los Workers de Stream.
- Acceso a servicios externos de gestión de claves para administrar secretos/tokens en todos los nodos.
- Sincronización integrada con repositorios de código externos para integraciones CI/CD y recuperación de desastres.

MONITOREO

- Sistema de notificaciones que alerta a los operadores cuando los flujos de datos se han detenido.
- Sistema de notificaciones que alerta a los operadores cuando hay demasiada variación en el volumen de datos desde orígenes/recolectores para identificar problemas.
- Los formatos de notificación incluyen SMS, PagerDuty, Webhook, AWS SNS y más.
- Monitoreo integrado que cubre todos los aspectos de un despliegue distribuido.
- Búsqueda centralizada e integrada de logs en cientos de grupos, nodos y flotas.
- Dashboards ricos y visualmente densos, diseñados para administradores y operadores.
- Monitoreo contextual para todos los orígenes y destinos.
- Sistema de notificaciones que alerta a los operadores cuando los flujos de datos se han detenido.
- Visualizaciones de flujo de datos que ofrecen una vista panorámica de todos los orígenes, rutas, pipelines y destinos.

TRABAJO CON DATOS

- Interfaz de usuario interactiva, amigable y eficiente para trabajar con datos en streaming.
- Creación visual, validación y resolución de problemas de pipelines de datos.
- Vista previa de datos con retroalimentación instantánea para la inspección visual de eventos mientras se transforman.
- Captura en vivo en múltiples puntos mientras los eventos viajan desde el origen hasta el destino.
- Documentación integrada y tooltips contextuales de ayuda en cada pantalla.
- Más de 30 Funciones nativas que soportan transformaciones de datos arbitrarias, aseguramiento y enriquecimiento.
- Más de 40 métodos de función C. integrados para un procesamiento más detallado.
- ... además de todo el poder de JavaScript para transformaciones de datos casi arbitrarias.
- Experiencia tipo IDE con autocompletado y asistencia de escritura anticipada.
- Conversión/segmentación automática de flujos de bytes a eventos utilizando reglas inteligentes con anulaciones opcionales del usuario.
- Reconocimiento automático de formato de marca de tiempo con capacidad de anularlas por parte del usuario.
- Reconocimiento y/o corrección de zona horaria.
- Editor de expresiones JavaScript integrado con vista previa de resultados en vivo.
- Editor de Regex integrado con vista previa de coincidencias y grupos de captura en vivo.
- Biblioteca de Regex integrada para las expresiones regulares más comunes, extensible.
- Soporte de análisis nativo para muchas fuentes de datos bien conocidas.
- Analizadores de datos definidos por el usuario para K=V, CSV, ELFF, CLF, JSON y valores basados en delimitadores.
- Utilice Regex para extraer campos, también con soporte nativo de patrones Grok.
- Soporte de validación de esquema de eventos utilizando el estándar JSON Schema.
- Soporte para Variables Globales – expresiones JS reutilizables y componibles que pueden ser referenciadas por cualquier función.
- Análisis granular de pipelines para mejor monitoreo y resolución de problemas más rápida en modo de vista previa utilizando Pipeline Profiling.
- Enriquecimiento de datos en tiempo real a través de tablas de búsqueda. Soporte de coincidencia Exacta, Regex y CIDR de forma nativa, con soporte basado en disco para mayor eficiencia.
- Soporte para enriquecimiento GeoIP utilizando bases de datos binarias de Maxmind.
- Soporte de Packs para construir, desplegar y compartir muestras de datos, Funciones, Orígenes, Destinos, Event Breakers, Rutas y Pipelines internamente o con miembros de la comunidad.
- Acceso a una comunidad creciente de Stream Packs con pipelines preconstruidos, funciones personalizadas y otras características nativas para acelerar y mejorar el valor de Stream.
- La búsqueda global facilita encontrar cualquier cosa en Stream de manera rápida y sencilla.
- Recolecte muestras de datos en vivo para ayudar en el desarrollo de pipelines o para compartir con compañeros de equipo que trabajan en proyectos similares.

REQUISITOS TÉCNICOS

Sistema

- Solución SaaS accesible a través de Cribl.Cloud.
- Solución autogestionada.
  - +4 núcleos físicos.
  - +8GB RAM.
  - 5GB de espacio libre en disco (más si PQ está habilitado).
- También disponible como solución SaaS a través de Cribl.Cloud.

Guía de dimensionamiento

- 1 core físico por cada 400GB/día de rendimiento de ENTRADA + SALIDA.
  - Ej.: 4 TB ENTRADA -> 4TB completos al Destino A, más 2 TB al Destino B = 10TB total = 25 cores físicos.

ACERCA DE CRIBL

Cribl, el Motor de Datos para Tecnología y Seguridad, permite a las organizaciones transformar su estrategia de datos. Nuestros clientes utilizan las soluciones agnósticas de Cribl para analizar, recolectar, procesar y enviar todos los datos de tecnología y seguridad desde cualquier origen y/o hacia cualquier destino, ofreciendo elección, control y flexibilidad necesaria para adaptarse a sus necesidades cambiantes. La suite de productos de Cribl, utilizada por empresas del Fortune 100 a nivel global, está diseñada específicamente para Tecnología y Seguridad, incluyendo **Cribl Stream**, el pipeline de observabilidad líder en la industria, **Cribl Edge**, un agente inteligente y agnóstico, **Cribl Search**, la primera solución de búsqueda en seco de la industria, y **Cribl Lake**, un data lake llave en mano. Fundada en 2018, Cribl es una empresa con fuerza laboral remota y una oficina en San Francisco, CA.

Cribl

The AI Platform for Telemetry

Más información: cribl.io | **Únase:** Comunidad de Slack
Pruebe ahora: Cribl Sandboxes | **Síganos:** LinkedIn y X