DATA SHEET

Cribl Search™

Cribl

The **AI Platform** for Telemetry

Una experiencia de búsqueda para toda su telemetría

Cribl Search es una plataforma unificada de búsqueda e investigación que ofrece una forma más rápida, sencilla y colaborativa de investigar logs.

Los equipos de seguridad y tecnología pueden ingerir datos en minutos, colaborar en Notebooks compartidas y utilizar flujos de trabajo asistidos por IA para pasar de las preguntas a las respuestas rápidamente.

Reemplace herramientas fragmentadas y stacks de logging antiguos y costosos con una experiencia de búsqueda única, diseñada para equipos de tecnología y seguridad que operan en la era de la IA.

Cribl search está impulsado por:

1. **Motor de búsqueda de alta velocidad en el Lakehouse, sobre datos recopilados directamente en Search**
   - **Incorporación de datos con mínima intervención:** Recopile datos en minutos, detecte formatos automáticamente con tipos de datos y almacénelos en datasets listos para investigación, sin necesidad de construir pipelines complejos ni necesitar diferentes equipos para un mismo trabajo.
   - **Motor de búsqueda de alto rendimiento:** Ejecute búsquedas rápidas y concurrentes sobre datos recientes y antiguos, recopilados directamente en Search; almacene datos en un almacenamiento gestionado e ilimitado, optimizado para búsquedas en fracciones de segundo.
   - **Investigaciones potenciadas por IA:** Use Copilot y Notebooks para guiar la exploración, correlacionar contexto y documentar investigaciones completas en un espacio de trabajo compartido y de colaboración.
   - **Arquitectura unificada desde recopilación hasta el análisis:** Combine su recolección, almacenamiento, búsqueda, dashboards y alertas en un solo producto para reducir la proliferación de herramientas, bajar costos y simplificar las operaciones.

2. **Motor federado para búsqueda en el lugar (search-in-place) de bajo costo sobre datos en reposo**
   - **Busque los datos donde residen:** Ejecute consultas directamente dentro de data lakes, almacenamiento de objetos, servicios en la nube y APIs en tiempo real, sin necesidad de restaurar ni mover sus datos.
   - **Retención a largo plazo con optimización de costos:** Mantenga datos históricos en almacenamiento de objetos de bajo costo mientras acelera las investigaciones sobre los datos más críticos de su data lake.
   - **Búsqueda unificada y agnóstica:** Utilice un único lenguaje de consulta para federar búsquedas en múltiples almacenes y tipos de datos, tanto estructurados como no estructurados, a través de una interfaz única.
   - **Amplio soporte de APIs y proveedores:** Consulte fuentes en tiempo real como AWS, Okta, Zoom, Microsoft Graph, GCP y Google Workspace mediante Dataset Providers y recolectores integrados.
   - **Funciona con su stack actual:** Agregue búsqueda federada sobre sus herramientas actuales de SIEM, observabilidad y almacenamiento, sin necesidad de migrar plataformas, reemplazar soluciones ni depender de ningún proveedor.

En conjunto, Cribl Search ofrece una experiencia de búsqueda unificada y de alto rendimiento sobre todos sus datos, activos o fríos, en su lugar o ingeridos, para que pueda investigar más rápido mientras reduce costos y complejidad y a su vez no dependa de ningún proveedor.

Valor inmediato

Recopile datos en solo minutos y ejecute búsquedas de inmediato.

Investigaciones 10× más rápidas

Flujos de trabajo optimizados, parsing automático y vistas unificadas que eliminan el trabajo manual.

Consolidación de herramientas

Una arquitectura única para recopilación, almacenamiento, búsqueda, dashboards y alertas.

Reduzca los costos de gestión de logs

Migre cargas de trabajo fuera de herramientas SIEM y APM para reducir costos.

Investigaciones impulsadas por IA

Exploración guiada que presenta contexto, próximos pasos y raíz del problema con mayor rapidez.

Características del Producto

SERVICIO

- **Búsqueda impulsada por IA con enfoque en la pregunta.** Investigue con lenguaje natural mientras la IA agéntica sugiere y refina consultas de principio a fin.
- **Recopile directamente en Search.** Envíe datos directamente al motor Lakehouse de Search sin necesidad de Stream.
- **Arquitectura unificada desde la recopilación hasta la investigación.** Use un solo producto para recopilación, almacenamiento, búsqueda y análisis con configuración y facturación unificadas.
- **Experimente una investigación potenciada por IA.** Interfaz de búsqueda intuitiva mejorada con IA para acelerar la exploración y reducir la dependencia de conocimientos especializados en consultas.
- **Motor de consultas de alto rendimiento.** Diseñado para manejar la concurrencia y los volúmenes de consultas a escala de IA, entregando resultados rápidos en datasets de gran tamaño.
- **Búsqueda federada en plataformas de análisis.** Consulte Snowflake, ClickHouse, Azure Data Explorer, Prometheus y otros servicios en su lugar sin necesidad de re-indexar. Permite a usuarios y administradores consultar múltiples almacenes y fuentes de datos y funciona en conjunto con las herramientas de búsqueda y análisis existentes.
- **Incorporación de datos con mínima intervención.** Recopile datos fácilmente en Search con detección automática de tipos de datos y almacenamiento local optimizado para investigaciones de alta velocidad.
- **Formatos y fuentes de datos flexibles.** Compatible con logs, métricas, eventos y telemetría estructurada o no estructurada en entornos híbridos y multi-nube.
- **Automatización de API y Search-as-Code.** Automatice la configuración, permisos y despliegue mediante credenciales de API y gestione Cribl Search como código, incluyendo soporte para Terraform.
- **Búsqueda en APIs en tiempo real.** Ejecute búsquedas directamente contra endpoints de API como AWS, Okta, Zoom, Microsoft Graph, GCP, Google Workspace o cualquier API REST personalizada.
- **Arquitectura elástica distribuida.** Despliegue automáticamente los recursos de búsqueda distribuida necesarios para satisfacer las demandas de volumen de datos y concurrencia.
- **Amplio soporte de diferences formatos de archivos.** Busque archivos de texto y formatos binarios específicos, incluyendo Parquet, JournalD, archivos de índice de Splunk y archivos comprimidos.

GESTIÓN

- **Almacenamiento de objetos gestionado e ilimitado con distribución automática.** Retenga datos el tiempo que necesite en almacenamiento respaldado por S3 que se distribuye automáticamente según los patrones de acceso.
- **Lakehouse multi-región y multi-nube.** Ejecute Lakehouse en múltiples regiones de AWS y Azure para mejorar el rendimiento y cumplir con los requisitos de residencia de datos.
- **Control centralizado de datasets.** Defina, administre y gobierne datasets desde un panel de control unificado.
- **Datasets acelerados con Lakehouse.** Ejecute búsquedas rápidas y eficientes sobre datos recientes mientras retiene el historial completo en almacenamiento de objetos de bajo costo.
- **Retención desde la recopilación y filtrado con reconocimiento de almacenaje.** Evite vacíos en búsquedas históricas con políticas de retención y filtrado inteligente de tiempo, incluso cuando las marcas de tiempo están incompletas.
- **Simplificación de pipelines.** Reduzca la complejidad de su recopilación y la proliferación de pipelines con flujos de trabajo optimizados.
- **Lógica de búsqueda reutilizable.** Guarde, estandarice y comparta búsquedas para mejorar la colaboración y la consistencia en las investigaciones.
- **Control de acceso basado en roles (RBAC).** Permisos granulares que aseguran que los equipos correctos accedan a los datos correctos.
- **Particionamiento flexible de datasets.** Busque subconjuntos optimizados de datos utilizando particiones basadas en tiempo o personalizadas (por ejemplo, tecnología, geografía, entorno) en S3 y otros sistemas de almacenamiento.
- **Configuración guiada y datasets listos para usar.** Asistente de configuración sencillo y datasets preconfigurados, incluyendo logs de sistema de Cribl, Amazon S3, logs de Cribl Edge y más, para generar valor de sus datos más rápidamente.

SEGURIDAD

- **Arquitectura segura por diseño.** Construida con cifrado en tránsito y en reposo para proteger los datos sensibles.
- **Controles de acceso a datos.** Gestión de acceso granular para datasets y resultados de búsqueda.
- **Registro de auditoría.** Seguimiento de actividad en sesiones de búsqueda y acciones administrativas.
- Prácticas de seguridad nativas de la nube. Compatible con las mejores y más modernas prácticas y normativas de seguridad en la nube.
- **Búsqueda con reconocimiento de cifrado sobre datos cifrados por Stream.** Busque y descifre campos cifrados por Stream en tiempo real para usuarios autorizados, sin exponer los datos en reposo.
- **RBAC granular para credenciales de API.** Asigne claves de API a datasets y acciones específicas utilizando el mismo modelo basado en roles utilizado por usuarios y equipos.

DESPLIEGUE Y ARQUITECTURA

- **Arquitectura unificada.** Integra recopilación, almacenamiento y búsqueda para reducir la proliferación de herramientas y simplificar las operaciones.
- **Soporte Cloud e Híbrido.** Disponible a través de servicios en la nube gestionados por Cribl o despliegues manejados por el cliente.
- **Escalabilidad elástica.** Escala para soportar volúmenes de consultas generados por IA y volúmenes crecientes de datos.
- **Abierto y flexible.** Diseñado para funcionar dentro de ecosistemas de datos existentes, sin forzar la dependencia al proveedor ni migraciones costosas.
- **Bring Your Own AI (BYOAI).** Conecte las funciones de IA de Cribl a sus propios modelos de IA (Anthropic u OpenAI) para cumplir con requisitos estrictos de privacidad y cumplimiento. eal a la telemetría de

INTERFAZ DE BÚSQUEDA

- **Experiencia de búsqueda tipo IDE.** Barra de búsqueda interactiva con sugerencias de escritura anticipada para operadores, funciones, campos y consultas recientes.
- **Validación de consultas en tiempo real.** Detecte errores antes de la ejecución para ahorrar tiempo y costos.
- **Vista previa local de consultas.** Optimice consultas antes de ejecutarlas ante datasets completos.
- **Dashboards interactivos.** Las categorizaciones con reconocimiento de tokens permiten transiciones fluidas desde gráficos hacia investigaciones profundas o herramientas externas.
- **Amplia biblioteca de operadores y funciones.** Más de 250 operadores y funciones para dar forma, filtrar, enriquecer y analizar datos.
- **Documentación e historial integrados.** Acceda a la documentación de operadores, consultas recientes y búsquedas guardadas directamente dentro de la interfaz.

TRABAJO CON RESULTADOS

- **Notebooks de investigación asistidos por IA con exportación a PDF.** Documente investigaciones en Notebooks compartidos y exporte como PDFs para tickets, auditorías y reportes.
- **Interfaz de resultados completa e interactiva.** Visualice resultados como eventos, campos, tablas, líneas de tiempo o gráficos.
- **Opciones de visualización avanzadas.** Cree dashboards con tipos de gráficos, diseños y categorizaciones personalizables.
- **Descubrimiento y enriquecimiento de campos.** Calcule automáticamente los valores principales, conteos únicos y estadísticas de presencia, y enriquezca los resultados con tablas de búsqueda.
- **Búsquedas programadas y alertas.** Automatice búsquedas recurrentes y dispare notificaciones por correo electrónico, SMS, PagerDuty, Webhook y más.
- **Reutilización de resultados de búsqueda.** Reutilice resultados anteriores cuando los datos subyacentes no han cambiado, reduciendo el cómputo redundante.
- **Search Packs.** Dashboards preconstruidos y paquetes de configuración alineados con fuentes de datos y casos de uso comunes, acelerando la incorporación y generando valor de sus datos de manera más rápida.
- **Notebooks de investigación con colaboración.** Combine búsquedas, gráficos y notas detalladas en flujos de trabajo de investigación que pueden compartirse, refinarse y reutilizarse.

REQUISITOS TÉCNICOS

Sistema

- Cribl Search está disponible como servicio en https://cribl.cloud/

Navegadores compatibles

- Firefox 65+, Chrome 70+, Safari 12+, Microsoft Edge

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 1000 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