



O Cribl Stream é um mecanismo de pipeline de dados para roteamento e processamento de dados de TI e segurança. Com o Stream, você pode rotear, reduzir, reformatar, enriquecer ou formatar dados de qualquer origem para qualquer destino.

O Cribl Stream oferece aos administradores controles de acesso robustos baseados em funções, permitindo que eles atribuam seções específicas de fluxos de dados aos usuários ou grupos responsáveis por enviar dados para ferramentas de análise, ferramentas de segurança ou outros destinos.

Escolha e flexibilidade.

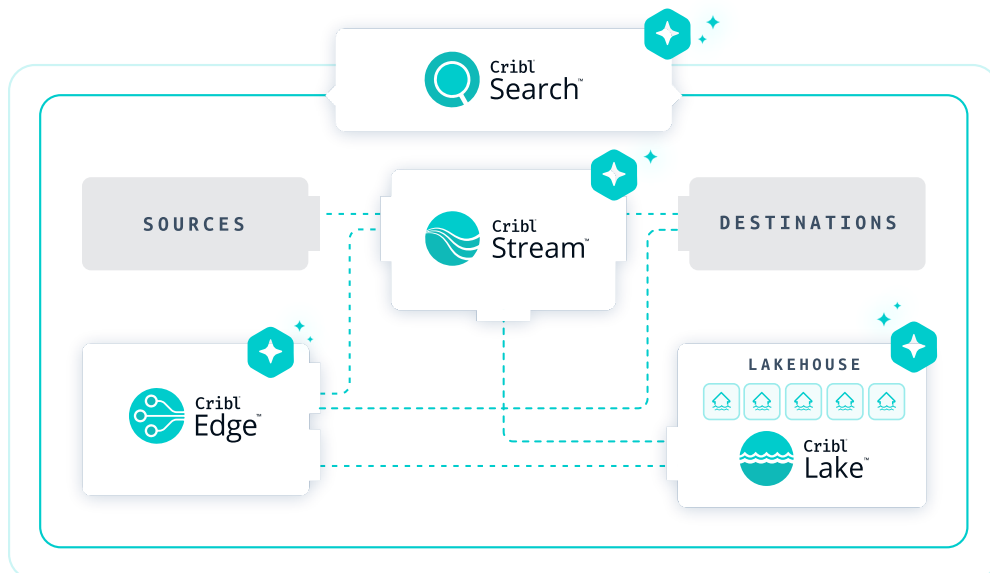
- Transmita eventos, métricas e rastreamentos de qualquer origem para qualquer destino, em Qualquer formato.
- Adicione novas ferramentas de análise e outros destinos sem adicionar agentes ou coletores.

Controle seus dados.

- Direcione os dados para as equipes e ferramentas certas.
- Implemente segurança de nível empresarial.
- Garantir o cumprimento das políticas, padrões e formatos de dados em todos os conjuntos de ferramentas.

Observe mais e gaste menos.

- Simplifique a integração e a coleta de dados para expor dados que você nem imaginava ter. Sabia que existia.
- Otimizar a infraestrutura, a ingestão de dados, o desempenho das ferramentas e as horas de trabalho da equipe.



COLETE O DADOS CORRETOS

Obtenha dados de qualquer fonte para qualquer ferramenta no formato correto.

REDUZA SEUS DADOS

Elimine dados irrelevantes ou desnecessários para controlar custos.

MODELE SEUS DADOS

Analise os dados conforme forem surgindo e molde-os de acordo com suas necessidades.

ENCAMINHE SEUS DADOS

Coloque os dados onde eles estão. Maior valor.

REPLAY

Armazene dados de alta fidelidade em armazenamento de baixo custo para reproduzi-los sob demanda, conforme necessário.

Características do produto

ARQUITETURA

- Arquitetura distribuída, super escalável e sem compartilhamento de recursos.
- Escalável desde laptops até centenas de nós e dezenas de milhares de nós. De núcleos.
- Plataforma altamente paralelizável e de alto desempenho, criada para extensibilidade.
- Latência inferior a um milissegundo.
- Testado para mais de 20PB/dia.
- As opções de implantação incluem:
 - Software incluindo binários Linux e contêineres Docker e gráficos Helm para fácil implantação em qualquer ambiente K8s.
 - A nuvem proporciona uma experiência SaaS através do Cribl. Na nuvem, totalmente gerenciada pela Cribl, sem sobrecarga de infraestrutura e escalável conforme a necessidade.
 - Implantação híbrida com plano de líder/controlador na nuvem e nós de trabalho responsáveis pelo processamento de dados.
- Mais de 80 integrações de origem/destino disponíveis imediatamente.
- Suporte nativo a protocolos para as principais fontes e destinos de logs, métricas e rastreamentos.
- Suporte TLS integrado para todas as integrações que o suportam.
- Suporte nativo para IAM compatível com SAML 2.0 e assumir papéis.
- Captura de dados em tempo real para integração, resolução de problemas e inspeção.
- Registro detalhado, métricas e status em tempo real para cada integração.
- Testes de conectividade integrados e resultados para cada integração.
- Suporte para coleta de dados de endpoints REST arbitrários.
- Suporte para coleta de dados baseada em scripts arbitrários.
- Suporte para envio e recebimento de todas as principais operadoras Serviços de armazenamento em nuvem PaaS.

GERENCIAMENTO

- Controle total de todos os seus dados de TI e segurança a partir de um plano de controle central.
- Arquitetura de alta disponibilidade que oferece transição perfeita Failover do líder (plano de controle) com tolerância a falhas quase em tempo real em infraestrutura local e disponibilidade de 99,9% na Cribl.Cloud.
- O suporte a AuthZ aprimora a segurança, permitindo o controle sobre quem tem permissões e privilégios para acessar os produtos, funcionalidades e recursos da Cribl.
- O Stream Projects permite que os usuários do Cribl acessem dados com segurança por meio de um modelo de autoatendimento, liberando o tempo da equipe administrativa do Cribl para se dedicar a tarefas essenciais para os negócios.
- Suporte para autenticação de nível empresarial (LDAP, SSO, etc.).
- RBAC baseado em políticas para permissões refinadas.
- Interface de usuário intuitiva e completa para sistemas distribuídos gerenciamento de sistemas.
- Gestão única e centralizada via nuvem ou Software auto-hospedado para centenas de grupos/nós.
- Controle de versão de configuração confiável com capacidade para reverter as alterações.

- Suporte centralizado para gerenciamento de certificados e chaves.
- Validação de alterações de configuração integrada e em tempo real.
- Geradores de dados integrados para testes de pipeline e destino.
- Atualizações totalmente automatizadas e distribuídas de todos os sistemas. Trabalhadores de fluxo.
- Utilize serviços externos de gerenciamento de chaves para gerenciar segredos/tokens em todos os nós.
- Sincronização integrada com código externo Repositórios para integrações de CI/CD e recuperação de desastres.

MONITORAMENTO

- O sistema de notificação alerta os operadores quando o fluxo de dados é interrompido.
- O sistema de notificação alerta os operadores quando há muita variação no volume de dados das fontes/ coletores para identificar problemas a montante.
- Os formatos de notificação incluem SMS, PagerDuty, Webhook, AWS SNS e muito mais.
- Monitoramento integrado que abrange todos os aspectos de um Implantação distribuída.
- Busca centralizada de logs integrada em centenas de grupos/nós.
- Painéis de controle ricos e visualmente densos, criados para administradores/operadores.
- Monitoramento contextual para todas as origens e destinos.
- Capacidade de encaminhar logs e métricas internas com total fidelidade para soluções externas.
- As visualizações de fluxo de dados fornecem uma visão geral de todas as origens, rotas, dutos e destinos.

TRABALHANDO COM DADOS

- Interface de usuário interativa, intuitiva e eficiente para trabalhar com dados de streaming.
- Criação visual, validação e resolução de problemas em fluxos de dados.
- Pré-visualização de dados com feedback instantâneo para visualização Inspeção dos eventos à medida que se transformam.
- Captura ao vivo em múltiplos pontos à medida que os eventos se deslocam da origem ao destino.
- A documentação integrada e as dicas contextuais ajudam no processo. Em todas as telas.
- Mais de 30 funções prontas para uso que o ferecem suporte a transformações de dados arbitrárias, segurança e enriquecimento.
- Mais de 40 métodos de função C integrados para maior precisão capacidades de processamento.
- ... além de todo o poder do JavaScript para transformações de dados praticamente arbitrárias.
- Experiência semelhante a um IDE (ambiente de desenvolvimento integrado) com preenchimento automático e auxílio de digitação preditiva.
- Conversão/separação automática de fluxo de bytes em eventos usando regras inteligentes com opções de substituição pelo usuário.
- Reconhecimento automático do formato de carimbo de data/hora com Opções de personalização do usuário.
- Reconhecimento e/ou correção de fuso horário.
- Editor de expressões JavaScript integrado com pré-visualização de resultados em tempo real.
- Editor de expressões regulares integrado com correspondência em tempo real e pré-visualização de captura de grupo.

- Biblioteca de expressões regulares integrada para as expressões regulares mais comuns, extensível.
- Suporte imediato para análise sintática de muitas linguagens conhecidas. Fontes de dados.
- Analisadores de dados definidos pelo usuário para valores baseados em K=V, CSV, ELFF, CLF, JSON e delimitadores.
- Extração de campos baseada em expressões regulares e suporte nativo a padrões Grok.
- Suporte para validação de esquema de eventos usando o padrão JSON Schema.
- Suporte para variáveis globais – reutilizáveis e Expressões JS compostáveis que podem ser referenciadas por qualquer função.
- Análise detalhada de dutos para melhor monitoramento e solução de problemas mais rápida no modo de visualização usando o Perfil de Dutos.
- Enriquecimento de dados em tempo real por meio de tabelas de consulta. Suporte nativo para expressões exatas, regulares e CIDR.
- Suporte para enriquecimento de geolocalização usando bancos de dados binários Maxmind.
- Oferece suporte para construção, empacotamento e compartilhamento rotas, fluxos de trabalho, amostras de dados, funções internas ou com membros da comunidade.
- Acesso a uma comunidade crescente de Stream Packs com pipelines pré-construídos, funções personalizadas e outros recursos prontos para uso, que aceleram e melhoram o valor do Stream.
- A busca global facilita encontrar qualquer coisa no Stream e rápido.
- Coletar amostras de dados em tempo real para auxiliar no desenvolvimento de fluxos de trabalho ou para compartilhar com colegas que trabalham em projetos semelhantes.

REQUISITOS TÉCNICOS

Sistema

- Solução SaaS acessível via Cribl.Cloud.
- Solução autogerenciável.
 - +4 núcleos físicos.
 - +8 GB de RAM.
 - 5 GB de espaço livre em disco (mais se o PQ estiver ativado).
 - Também disponível como solução SaaS através do Cribl.Cloud.

Guia de tamanhos

- 1 núcleo físico para cada 400 GB/dia de Taxa de transferência de entrada e saída.
Exemplo: 4 TB de entrada -> 4 TB completos para o Destino A, mais 2 TB para o Destino B = 10 TB no total = 25 núcleos físicos.

SOBRE CRIBL

A Cribl, o mecanismo de dados para TI e segurança, capacita as organizações a transformarem sua estratégia de dados. Os clientes usam as soluções independentes de fornecedores da Cribl para analisar, coletar, processar e rotear todos os dados de TI e segurança de qualquer origem ou destino, oferecendo a escolha, o controle e a flexibilidade necessários para se adaptarem às suas necessidades em constante mudança. O conjunto de produtos da Cribl, usado por empresas da Fortune 1000 em todo o mundo, foi desenvolvido especificamente para TI e segurança, incluindo o **Cribl Stream**, O principal pipeline de observabilidade do setor, **Cribl Edge**, um agente inteligente independente de fornecedores e a **Busca Cribl**, a primeira solução de busca local do setor. Fundada em 2018, a Cribl é uma empresa com foco em trabalho remoto, mas com um escritório em São Francisco, Califórnia.

Saiba mais: www.cribl.io | Experimente agora: [Caixas de areia Cribl](#) | Junte-se a nós: [Comunidade Slack](#) | Siga-nos: [LinkedIn](#) and [X](#)

©2025 Cribl, Inc. Todos os direitos reservados. 'Cribl' e a marca Cribl Flow são marcas registradas da Cribl, Inc. nos Estados Unidos e/ou em outros países. Todas as marcas comerciais de terceiros são propriedade de seus respectivos proprietários.

DS-0001-PT-3-1125