ONE PAGER

Cribl Guard

AI-powered sensitive data detection for proactive identification, mitigation and compliance

Cribl
The AI Platform for Telemetry

The challenge

With growing legal, security, and AI governance pressures, organizations need tighter control over where sensitive data is stored and how it moves. A single leak can damage customer trust and trigger costly regulatory action, yet many teams still lack visibility into sensitive data slipping into fast-changing logs and telemetry.

PII such as Social Security numbers, credit card numbers, and passport identifiers is heavily regulated, but internal system and application data must also be protected from unauthorized access, ransomware, or accidental exposure. Traditional regex-only or manual approaches are too slow and brittle to keep up.

The Cribl solution

Cribl Guard is an intelligent, modern solution for proactively detecting and protecting sensitive data in real time. It helps you reduce risk, meet compliance requirements, and enforce consistent data protection policies by automatically identifying sensitive information as it moves through Cribl Stream. Your teams can review and take action masking, blocking, or allowing the data before it reaches downstream systems, reducing false positives and avoiding manual, error-prone processes.

Beyond rule-based scanning, Cribl Guard's background detection is an optional AI-powered capability that continuously analyzes data flowing through Pipelines to uncover previously unknown sensitive data. Purpose-built custom models run directly on your Cribl Workers so sensitive data is proactively discovered and mitigated.

Cribl Stream™ GUARD

Typical use cases

- Inline protection: Identify, mask, encrypt, or delete sensitive data before it reaches downstream systems such as SIEMs, data lakes, and observability platforms.
- Safeguarded routing: Detect and redirect events containing PII to specialized destinations for further review, secure storage, or restricted access.
- Continuous validation: Monitor data flows to validate that no PII or sensitive data is being passed into high-risk systems, and generate auditable evidence of enforcement.
- Early-warning for drift: Use background detection to leverage AI to continuously monitor Pipelines for new PII, secrets, and regulated data patterns and then quickly turn findings into Guard rules.

Key features of Cribl Guard

1. **Real-time detection and action**
   Cribl Guard scans live data streams for sensitive information and takes immediate action based on customizable rules. This proactive approach reduces risk, ensures compliance, stops data leaks before they occur, and supports audit readiness for GDPR, HIPAA, CCPA, and PCI DSS.
2. **Flexible rulesets**
   Use built-in rules or create your own with custom logic such as regular expressions and anchor terms. Whether detecting common data types or industry-specific formats, Cribl Guard adapts quickly to new detection needs and reduces false positives.
3. **Seamless pipeline integration**
   Easily start using Cribl Guard with your existing Pipelines. Define which fields to scan and how to respond by masking, redacting, tagging, or rerouting sensitive content so you can protect what matters without slowing down critical workloads.
4. **Comprehensive monitoring**
   Gain full visibility into Guard's performance, including event volume, bytes scanned, and data flagged. These metrics help fine-tune rule accuracy, reduce noise, and demonstrate compliance readiness.
5. **Background detection for hidden risk**
   Background detection continuously analyzes data in your Pipelines and applies purpose-built AI to uncover sensitive information that existing rules may have missed, reducing regulatory and operational risk
6. **AI-driven insights**
   AI enhancements help your teams build smarter, more context-aware rules that evolve with your data. Cribl Guard uses AI to recommend and refine rulesets, accelerate rule authoring, and reduce manual effort so teams stay focused on high-value investigations.
7. **Deploy anywhere**
   Cribl Guard supports cloud, hybrid, or on-premises deployments without sending Stream data outside your environment. As part of Cribl's AI governance and with the option to Bring Your Own Model (BYOM), Guard's AI features keep sensitive telemetry under your control.

Summary

Protecting sensitive data is too important and too complex to rely on manual processes and static rules. Cribl Guard transforms this process by automatically detecting and protecting sensitive information in real time. With built-in rules, AI-assisted rule authoring, and always-on background detection powered by custom models, Guard helps you uncover hidden risk, take action before leaks reach critical systems, and continuously adapt to new data patterns. It improves compliance, reduces risk, and enhances your team's productivity while giving your organization the visibility and control it needs to meet evolving regulatory requirements with confidence.

Please **contact sales** for pricing.