



The **AI Platform**
for Telemetry

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

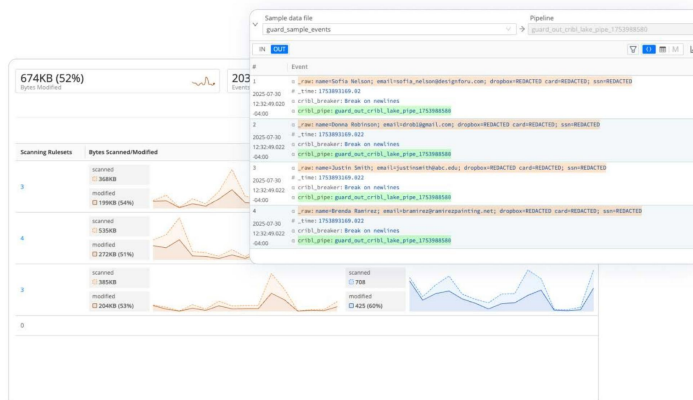
Cribl Guard combines advanced artificial intelligence with a human-assisted governance layer for detection and mitigation of sensitive data, such as payment card details, passport identifiers, and Social Security numbers, as it traverses Cribl Stream and across your telemetry estate.

Built on Cribl's data engine, Guard ships with over 200 configurable policy rules, teams can review, approve, or override actions in real-time. Detected data is automatically masked or blocked prior to storage, supporting compliance with PCI DSS, HIPAA, GDPR, and CCPA not only for data inspected inline, but also for sensitive information surfaced by AI-powered background detection.

The challenge

Sensitive data moving through enterprise telemetry pipelines introduces significant security risk. The inadvertent exposure of personally identifiable information (PII) or any sensitive data can compromise customer trust, invite regulatory sanctions, and create security risks. Equally at risk are system configurations, application secrets, and other business-critical data that adversaries can exploit.

Traditional safeguards often rely on manually tagging sensitive fields, a process that is slow, inconsistent, and error-prone. Regex-based pattern matching adds only limited protection, frequently under-detecting true risks while over-flagging benign content. Without context-aware detection, distinguishing between low-risk identifiers (e.g., hardware serial numbers) and regulated identifiers (e.g., Social Security numbers) becomes unreliable. As data pipelines scale in volume, velocity, and variety, these manual and static approaches fail to provide adequate coverage especially as new sources are added or changed outside of scheduled reviews.



The challenge

Sensitive data leakage poses significant security risks, including exposure of PII, regulatory penalties, and system vulnerabilities. Traditional manual safeguards and regex-based methods are slow, inconsistent, and ineffective at detecting true threats, leaving organizations exposed as data scales and as new data sources quietly introduce fresh risk.

The solution

Cribl Guard enhances data security by using AI with human oversight to prevent sensitive data exposure in real time. Integrated into Cribl Stream, it inspects events for high-risk data, allowing operators to refine actions and ensure compliance while scaling security measures.

Background detection complements out-the-box rulesets by continuously scanning your environment, proactively surfacing new sensitive data before they become incidents.

The solution

Cribl Guard strengthens data security by combining advanced AI with a human-assisted enforcement layer. Embedded directly within Cribl Stream, it continuously inspects every event for PII, financial records, government identifiers, and other high-risk data types. Operators can validate, override, or refine actions, ensuring that sensitive content is masked, encrypted, blocked, or rerouted before reaching storage or downstream systems. With prebuilt, customizable rules and support for user-defined policies Guard enables organizations to reduce breach likelihood, enforce compliance, and contain risks at scale.

Cribl Guard also includes AI-powered background detection that continuously scans telemetry for data leakage and policy drift, with flexible model choices to balance fidelity and throughput.

Purpose-built transformer models run on Cribl Workers in your own environment to proactively discover sensitive data while keeping it in your control.

Key capabilities

INTELLIGENT CUSTOMIZED DETECTION

AI-powered analysis accurately identifies sensitive data across geographies and formats, reducing false positives and false negatives.

DYNAMIC RULE RECOMMENDATIONS

Tailors detection rules based on live data and evolving compliance requirements, including mitigating background detection findings with enforced Guard rules.

PROACTIVE ACTION AND REMEDIATION

Detects issues before they become incidents and human-reviewed mitigation ensure precision before masking, encrypting, blocking, or rerouting data in flight.

ADAPTIVE MONITORING AND OPTIMIZATION

Provides deep visibility into data flows while continuously improving rule accuracy, coverage, and performance.

By enforcing controls at the point of ingestion, Cribl Guard prevents data leaks before they occur, simplifies compliance with GDPR, CCPA, HIPAA, and PCI DSS, and reduces the operational burden on security teams.



The benefits

- **Intelligent, Context-Aware Detection**

AI-driven analysis identifies sensitive data with high precision, reducing false positives.

- **Dynamic and Adaptive Rule Management**

Continuously evolves detection based on live data and compliance requirements. AI-guidance helps you turn background detection findings into enforced Guard rules in one click.

- **Proactive Remediation with Human Oversight**

Combines AI decision-making with human review to ensure accurate data masking, blocking, or rerouting before exposure.

- **Seamless Deployment and Operational Efficiency**

Natively integrates with Cribl Stream, automating sensitive data handling and incident response while optimizing storage costs.

- **Compliance and Audit Readiness**

Ensures full visibility with auditable records that simplify adherence to GDPR, HIPAA, CCPA, and PCI DSS.

What makes Cribl Guard different?

REAL-TIME DETECTION AND EASY REMEDIATION

Continuously inspects live data streams, preventing sensitive information from reaching unauthorized or insecure destinations.

PROACTIVE, AI-POWERED RISK DISCOVERY

Intelligent background detection helps organizations move beyond static policy enforcement for sensitive data to proactive discovery by uncovering previously unknown sensitive data before it reaches downstream systems, reducing regulatory exposure and operational risk.

RAPID, FLEXIBLE DEPLOYMENT

Integrates natively with **Cribl Stream** Pipelines and includes more than 220 prebuilt detection patterns to simplify use.

OPERATIONAL EFFICIENCY

Automates sensitive data handling, reduces manual intervention, accelerates incident response, and optimizes storage costs.

COMPLIANCE AND AUDIT READINESS

Maintains an auditable record of detections and enforcement actions, streamlining adherence to governance, compliance and other regulatory frameworks.

SUPPORTS MULTIPLE DEPLOYMENT MODELS

Cloud, hybrid or on-premises deployments are all supported, providing powerful data scanning to meet varied organizational requirements.

Summary

Sensitive data exposure remains one of the most critical risks facing modern enterprises. Cribl Guard delivers proactive protection by combining AI-driven detection with human-assisted oversight, giving teams real-time visibility, automated remediation, and precise control over sensitive data as it moves through enterprise pipelines.

With context-aware detection, Guard reduces false positives, improves accuracy, and enables immediate enforcement actions such as masking, encryption, blocking, or rerouting. It streamlines compliance with global regulations, enhances operational efficiency, and lowers overhead by automating sensitive data management at scale.

Background detection extends these capabilities with AI by continuously scanning for emerging sensitive data exposures and policy drift, allowing teams to address issues before they lead to incidents or audit findings.

As part of The AI Platform for Telemetry, Guard helps prepare telemetry for both humans and AI agents by ensuring data meets governance standards and privacy requirements. **Cribl Guard** transforms sensitive data risk into operational resilience: preventing leaks, improving efficiency, and maintaining compliance without adding manual complexity.



Cribl Guard combines AI and human oversight to protect sensitive data in real time, reducing false positives, automating compliance, and reducing risk with proactive AI-powered discovery and mitigation.

FAQ: Cribl Guard and sensitive data detection

What is Cribl Guard?

Cribl Guard is an AI-powered sensitive data detection and masking solution built into Cribl Stream. It inspects logs and telemetry for PII, financial data, government identifiers, and other high-risk values, and applies masking, blocking, or rerouting actions before data reaches storage or downstream tools.

How does Cribl Guard detect sensitive data in telemetry?

Cribl Guard combines out-the-box rulesets with the option to use AI to detect sensitive data. Out-of-the-box rules can be used for credit cards, Social Security numbers, passport data, and 220+ data types, as well as customized logic. Background detection complements these rules by using AI to continuously scan telemetry for new patterns using purpose-built transformer models running on your Workers.

What is background detection in Cribl Guard?

Background detection is an AI-powered capability in Cribl Guard that continuously analyzes data flowing through Pipelines to uncover sensitive information that may have gone unnoticed. Rather than relying exclusively on static rules, background detection applies purpose-built AI models to identify unknown new patterns of PII, secrets, and regulated data as they emerge. As upstream systems evolve, schemas change, and new applications are onboarded, background detection monitors for drift and emerging risk. When new sensitive data is identified, it is surfaced in a centralized interface. Teams can investigate the finding, dismiss it if appropriate, or quickly create or update Guard rules to prevent future data that matches that pattern from reaching downstream systems such as SIEMs, data lakes, and observability platforms.

How does Cribl Guard help with compliance?

By identifying and controlling sensitive data in telemetry real-time in Worker Groups before it is stored, Cribl Guard supports compliance with PCI DSS, HIPAA, GDPR, and CCPA. It maintains an auditable record of detections and actions, helping teams demonstrate effective controls and continuous improvement to auditors and regulators.



The **AI Platform** for Telemetry

Learn more at cribl.io

Try [Cribl Sandboxes](#)

Join our [Slack community](#)

Follow us on [LinkedIn](#) and [X](#)

© COPYRIGHT 2026 CRIBL, INC. ALL RIGHTS RESERVED
SB-0000-EN-1-0626