>SOLUTION BRIEF_

Cribl Guard

THE CHALLENGE

Sensitive data 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.

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.

Cribl Stream™ GUARD

Cribl Guard combines advanced artificial intelligence with a human-in-the-loop governance layer to detect and control sensitive data—such as payment card details, passport identifiers, and Social Security numbers—as it traverses Cribl Stream. With over 200 configurable policy rules, security teams can review, approve, or override actions in real time to enforce organizational and regulatory requirements. Detected data is automatically masked or blocked prior to storage, supporting compliance with frameworks such as PCI DSS, HIPAA, and GDPR while minimizing the risk of unauthorized exposure.

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, leaving organizations vulnerable to breaches and compliance breakdowns.

THE BENEFITS

Intelligent, Context-Aware Detection

- AI-driven analysis identifies sensitive data with high precision across different geographies and formats, reducing false positives.

Dynamic and Adaptive Rule Management

- Continuously evolves detection rules based on live data and changing compliance requirements, ensuring up-to-date security.

Proactive Remediation with Human Oversight

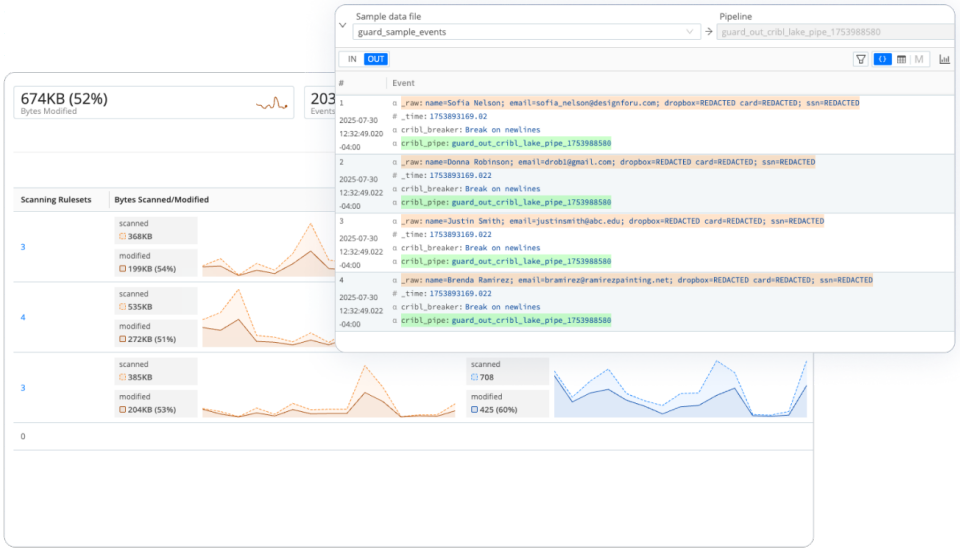
- Combines AI decision-making with human review to ensure accurate data masking, blocking, or rerouting before exposure.

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 into data flows, with auditable records that simplify adherence to regulations like GDPR, HIPAA, and CCPA.



The solution

Cribl Guard strengthens data security by combining advanced AI with a human-in-the-loop enforcement layer to minimize the risk of sensitive data exposure. 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 in real time, ensuring that sensitive content is masked, encrypted, blocked, or rerouted before reaching storage or downstream systems. With more than prebuilt, customizable rules—and support for user-defined policies—Guard enables organizations to reduce breach likelihood, enforce compliance, and contain risks at scale.

Key capabilities include:

1. **Intelligent contextual detection** — AI-powered analysis accurately identifies sensitive data across geographies and formats, reducing false positives.
2. **Dynamic rule recommendations** — Tailors detection rules based on live data and evolving compliance requirements.
3. **Proactive action and remediation** — Human-reviewed AI decisions ensure precision before masking or blocking data in flight.
4. **Adaptive monitoring and optimization** — Provides deep visibility into data flows while continuously improving rule accuracy.

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

Key facets of Cribl Guard

Real-time detection and remediation

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

High accuracy with fewer false positives

AI-driven, context-aware analysis reduces noise and flags only truly sensitive data, improving precision and response confidence.

Rapid, flexible deployment

Integrates natively with Cribl Stream pipelines and includes more than 200 prebuilt detection patterns to accelerate adoption.

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.

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-in-the-loop oversight, giving security 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 (GDPR, CCPA, HIPAA, PCI DSS), enhances operational efficiency, and lowers overhead by automating sensitive data management at scale.

Cribl Guard transforms sensitive data risk into operational resilience—empowering organizations to prevent leaks, contain threats, and maintain compliance without adding manual complexity.

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Customers use Cribl's suite of products to collect, process, route, and analyze all IT and security data, delivering the flexibility, choice, and control required to adapt to their ever-changing needs.

We offer free training, certifications, and a free tier across our products. Our community Slack features Cribl engineers, partners, and customers who can answer your questions as you get started and continue to build and evolve. We also offer a variety of hands-on Sandboxes for those interested in how companies globally leverage our products for their data challenges.