Cerbi

SOURCE-LEVEL DATA GOVERNANCE

Stop Sensitive Data Before It Reaches Your Logs

Your applications are leaking passwords, tokens, and PII through logs right now. Most engineering teams don't realize the scope of exposure until it's too late.

The Hidden Crisis

- **Uncontrolled Data Capture**

  Applications log everything developers send—passwords, API keys, user data—without filtering or governance.

- **Infrastructure Sprawl**

  Sensitive data spreads across Splunk, Datadog, CloudWatch, and backup systems beyond your control.

- **Permanent Exposure**

  Once ingested into distributed logging infrastructure, sensitive data cannot be fully removed.

- **Reactive Compliance**

  GDPR violations and breach notifications happen after exposure, creating expensive remediation cycles.

96%

APPS LEAK SENSITIVE DATA

$4.4M

AVERAGE BREACH COST

4%

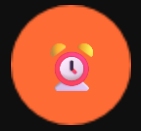
GDPR PENALTY (OF REVENUE)

95%

BREACHES INVOLVE HUMAN ERROR

Source: IBM Security, GDPR.eu, Android App Privacy Study 2026

Why Current Approaches Fail

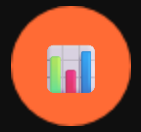


Masking Too Late

Data already exposed before filtering occurs at ingestion point

Reactive Detection

SIEM tools alert after breach occurs, not before exposure



No Prevention

Dashboards show problems but don't prevent bad logs

Developer Disconnect

No governance integration in the coding workflow process

The Shift

> *Logging needs to be governed at the source. Control what gets logged before it leaves the application.*

NIST SP 800-92 Rev. 1

Federal Log Management Standards

CerbiShield

In-process logging governance that prevents data exposure at the source

- **Runtime Enforcement**
  Runs directly inside your application process with zero-latency policy enforcement
  NO PERFORMANCE IMPACT

- **Intelligent Detection**
  Pattern-based detection blocks PII, credentials, and tokens before they leave your application
  95% EXPOSURE PREVENTION

- **Policy Automation**
  Automated schema validation and governance rules with real-time compliance monitoring
  AUDIT-READY REPORTS

- **Seamless Integration**
  Works with existing logging infrastructure—Splunk, Datadog, Azure Monitor
  NO PIPELINE CHANGES

DEPLOYMENT TIME

1 Day

vs 6-month infrastructure overhaul

ROI TIMELINE

1 Week

Immediate compliance visibility

One-line code integration with existing loggers

How It Works

1

App Logs as Usual

Your application continues logging normally with existing frameworks and libraries

→

2

Cerbi Enforces Rules

Runtime enforcement blocks or redacts sensitive data before it leaves your application

→

3

Clean Logs Delivered

Only compliant logs reach your observability tools

Splunk • Datadog • Azure Monitor

→

4

Track Violations

Policy violations are captured in your governance dashboard for monitoring and compliance

Why It's Different

Traditional logging vs Cerbi's source-level control

Traditional Logging

- Data leaks into observability pipelines before any control
- Reactive detection only after sensitive data is exposed
- Compliance becomes expensive and reactive process
- Developers don't consider governance when logging

VS

Cerbi Approach

- Prevents exposure at source before data leaves application
- Proactive compliance with real-time policy enforcement
- Enforces structure and policy automatically at runtime
- Governance built into development workflow seamlessly

Developer Experience

One-Line Integration

Add CerbiShield to your application with minimal code changes.

```
logger .UseCerbi( cfg =>  cfg .LoadProfile( "governance.json" ))
```

No Pipeline Changes

Works with your existing logging infrastructure without modifications.

Existing Logger Compatibility

Integrates seamlessly with Serilog, NLog, and other popular logging frameworks.

Lightweight Runtime Impact

Minimal performance overhead with efficient in-process governance enforcement.

Enterprise Ready

Built for security, compliance, and enterprise scale

DEPLOY IN 1 DAY

Your Azure Tenant

Runs entirely within your Azure environment. Complete data sovereignty with zero external dependencies.

- ✓ No data leaves your infrastructure
- ✓ SOC 2 & ISO 27001 compliant
- ✓ Regional compliance (GDPR, CCPA)

SSO READY

Identity Integration

Native Entra ID integration with role-based access control. Use your existing identity infrastructure.

- ✓ Zero additional user management
- ✓ Conditional access policies
- ✓ Audit trails in Azure AD logs

REAL-TIME

Complete Visibility

Full audit trails and governance dashboards. Real-time compliance monitoring with automated reporting.

- ✓ Automated compliance reports
- ✓ Policy violation alerts
- ✓ Executive dashboards

NO PROCUREMENT DELAYS

Azure Marketplace

Simple deployment through Azure Marketplace. Enterprise billing, support, and SLAs included.

- ✓ Use existing Azure credits
- ✓ Unified billing with Azure
- ✓ 24/7 enterprise support

Stop Data Leaks Today

Get CerbiShield running in your environment

Every day of delay increases your compliance risk

1

Start Free Trial

14-day full-feature trial with your actual logs and applications

SEE EXPOSURE IN 24 HOURS

→

2

Deploy Securely

One-click Azure Marketplace deployment in your tenant with Entra ID integration

PRODUCTION READY IN 1 DAY

→

3

See Results

Immediate governance visibility with compliance dashboards and audit reports

ROI VISIBLE WITHIN FIRST WEEK

Ready to secure your logs? Let's get you started.

sales@cerbi.io | **cerbi.io/demo** | **cerbi.io/trial**