Security

How Bleedpoint Protects Your Data

Document Version: 0.9 **Last Updated:** April 26, 2026

TL;DR

When you connect your Stripe account to Bleedpoint, you're trusting us with sensitive financial data. We take that seriously. Here's what that means in practice:

- **Read-only access.** We can never modify, create, or delete anything in your Stripe account.
- **No card data, ever.** Credit card numbers, bank accounts, and payment credentials never reach our servers.
- **Encryption everywhere.** TLS 1.3 in transit, AES-256 at rest, dedicated keys for your OAuth tokens.
- **Magic link auth.** No passwords stored. No password leaks possible.
- **Audit trail.** Every action against your data is logged and reviewable.
- **24-hour breach notification.** If something goes wrong, you'll know within a day.

The full details are below. If you have specific security questions, email security@bleedpoint.com.

How Bleedpoint Connects to Stripe

Read-Only OAuth via Stripe Connect

Bleedpoint uses Stripe Connect — Stripe's official OAuth integration platform — to access your account data.

When you click "Connect Stripe" in Bleedpoint:

1. You're redirected to Stripe's own login page (you sign in directly with Stripe, not us)
2. Stripe shows you exactly what permissions Bleedpoint is requesting (read-only access)
3. You explicitly approve the connection
4. Stripe sends us a token that lets us read — and only read — from your account

What "Read-Only" Means

We can:

- View your subscriptions, customers, payments, invoices, plans, and discounts
- Analyze patterns to identify revenue leakage
- Generate reports based on what we see

We cannot:

- Charge anyone
- Issue refunds
- Cancel subscriptions
- Modify customer records
- Update pricing or coupons
- Create new resources of any kind

This isn't a promise — it's enforced by Stripe's permission system. The OAuth token we receive simply doesn't include write permissions. Even if our servers were compromised, an attacker couldn't use our token to modify your Stripe account.

What We Don't Receive

Even with read-only access, certain data never reaches us:

- **Credit card numbers.** Stripe doesn't expose full card numbers via the API. They never reach our servers, our logs, or our reports.
- **Bank account details.** Same — never exposed to us.
- **Customer authentication data.** Passwords, 2FA secrets, login tokens for your customers' accounts in your own products — none of this is in Stripe, so none of it reaches us.

You Can Disconnect Anytime

You can revoke Bleedpoint's access at any time:

- From your Bleedpoint dashboard, or
- Directly from your Stripe Dashboard → Settings → Connected Accounts

Once you disconnect:

- We delete the OAuth token from our systems within 24 hours
- We can no longer access your Stripe account
- Past audit reports remain available in your Bleedpoint dashboard (they're already-generated PDFs, not live data)

How Your Data Is Protected

Encryption

Everything is encrypted, both in motion and at rest.

In transit (between you and us, and between us and our infrastructure):

- TLS 1.3 for all HTTPS traffic

- Modern cipher suites only (no SSL, no older TLS versions)
- HSTS enabled to force HTTPS on every connection

At rest (in our databases and storage):

- AES-256 encryption for all stored data
- AWS Key Management Service (KMS) manages encryption keys
- Audit reports stored in encrypted S3 buckets

OAuth tokens specifically:

- Encrypted with a dedicated KMS key, separate from the keys used for general data
- This means even an internal compromise of one part of our system can't decrypt connected platform credentials

Authentication

We don't use passwords. Period.

Magic link authentication:

- You enter your email; we send you a one-time login link
- Links expire after 15 minutes if unused
- Links can only be used once
- No password storage means no password leaks possible

Session security:

- After magic link verification, you receive a signed session token (JWT)
- Tokens stored as httpOnly, secure, SameSite=Lax cookies (resistant to common attack patterns)
- Tokens expire after 30 days of inactivity
- All token signing keys stored in AWS Secrets Manager

Access Controls

Customer access:

- Each Bleedpoint account can only see its own data
- Authorization checks happen on every API call, not just at login
- Cross-account access is prevented at the database query level (not just the UI)

Internal access:

- Administrative access to infrastructure requires multi-factor authentication
- Least-privilege IAM roles — every component only has the permissions it strictly needs
- All administrative access is logged via AWS CloudTrail with timestamps and identifiers
- Personnel review and audit access controls regularly

Network Security

- Application logic isolated from public internet where possible
- Public endpoints are rate-limited to prevent abuse and credential-stuffing attacks
- Web Application Firewall (WAF) protects against common web attacks (SQL injection, XSS, etc.)
- DDoS protection through AWS Shield

Audit Logging

We log access to data using AWS CloudTrail:

- Every administrative action is recorded with user identifier, timestamp, and operation
- Logs are encrypted, tamper-evident (log file validation enabled), and retained for at least 1 year
- Critical events trigger automated alerts

If you ever need to know who accessed your data and when, the logs are there.

How Reports Are Stored and Delivered

When we generate your audit report:

1. The PDF is encrypted at rest in an S3 bucket (AES-256 + KMS)
2. We send you an email notification with a presigned download link
3. The presigned link expires after 7 days
4. After expiration, you can still download the report from your dashboard for as long as your account is active
5. Reports are deleted within 90 days of account termination

Why presigned URLs? Even if a notification email gets forwarded or leaked, the download link expires. After 7 days, the original recipient (you) is the only one who can access the report — and only by logging into your dashboard.

How We Detect and Respond to Incidents

Detection

- Continuous monitoring of infrastructure for anomalies
- AWS CloudWatch alerting on unusual error rates, suspicious traffic patterns, and access anomalies
- AWS Cost Anomaly Detection alerts us to unusual resource usage that might indicate compromise

Response

- Documented incident response plan, reviewed periodically
- Contained scope: immediate isolation of affected systems
- Forensic preservation: relevant logs and state snapshots preserved for investigation

- Customer notification: within 24 hours of identifying an incident affecting your data

Notification Commitments

If we discover a security incident affecting your data:

- We email you within 24 hours (faster than the 72-hour GDPR requirement)
- We tell you what we know, what we're doing, and what (if anything) you should do
- We provide updates as we learn more
- We document the resolution and make it available to you on request

We do this even when we're not legally required to. It's the standard we want to be held to.

Responsible Disclosure

We welcome security researchers who help us identify vulnerabilities.

How to Report

Email **security@bleedpoint.com** with:

- A description of the vulnerability
- Steps to reproduce
- Potential impact
- Your contact information (for follow-up)

Our Commitments to Researchers

- We will acknowledge your report within 2 business days
- We will provide updates as we investigate and remediate
- We will not pursue legal action against good-faith researchers who follow responsible disclosure practices and avoid:
  - Accessing customer data beyond what's necessary to demonstrate the issue
  - Disrupting service availability
  - Public disclosure before we've had a chance to fix the issue

What's In Scope

- bleedpoint.com and all subdomains
- Bleedpoint application logic and APIs
- Authentication and authorization flows

What's Out of Scope

- Issues in third-party platforms we use (report those directly to AWS, Stripe, etc.)
- Social engineering of our team or customers

- Physical attacks
- DoS/DDoS testing without prior coordination
- Findings from automated scanners that we already know about

We don't currently offer monetary bounties, but we'll publicly credit researchers who responsibly report valid issues (with permission).

Subprocessors

We rely on a small number of trusted infrastructure providers. Each is audited, encrypted, and contractually obligated to protect your data. The current list:

- **Amazon Web Services (AWS):** infrastructure, database, file storage, automated email
- **Stripe:** payment processing for Bleedpoint subscriptions; OAuth platform for connected accounts
- **Microsoft 365:** team mailboxes
- **Namecheap:** marketing site hosting and DNS
- **CookieYes:** cookie consent management
- **Google Analytics 4:** anonymized usage analytics
- **Microsoft Clarity:** anonymized session replay

Full subprocessor details, including data handled and transfer mechanisms for international customers, are in our Data Processing Agreement and Privacy Policy.

Questions

We'd rather you ask than guess.

- Security questions: security@bleedpoint.com
- General questions: hello@bleedpoint.com
- Privacy questions: legal@bleedpoint.com

For postal mail:

CloudSec Global LLC Attn: Bleedpoint Security 6881 W Charleston Blvd, Ste A, Unit #5209 Las Vegas, NV 89117 United States

---

Bleedpoint is a product of **CloudSec Global LLC**, a Nevada limited liability company.

This Security page is informational. The legally binding terms governing your relationship with Bleedpoint are in our Terms of Service, Privacy Policy, and Data Processing Agreement.