Resolute Security

Everything your security team needs for a pre-sale review, in one document. Generated June 1, 2026.

Contents

Quick links

Live trust page: https://tools.resolute-security.com/trust/resolute

Status: https://tools.resolute-security.com/status

Data Processing Addendum: https://tools.resolute-security.com/dpa

Service Level Agreement: https://tools.resolute-security.com/legal/sla

Security policy (vuln reporting, etc.): github.com/irresolute-sec/smb-tools/blob/main/SECURITY.md

How we keep your data safe

Authentication

- SSO via Google or Microsoft, plus magic-link / passwordless email. TOTP and WebAuthn passkeys both supported for MFA.
- All production access requires MFA. Sessions are hashed (SHA-256) — raw tokens never sit at rest.

Multi-tenancy

- Every customer record is scoped by organization_id at the schema level. Multi-tenancy is enforced in code on every query — no shared tables without org keys.

Encryption

- TLS 1.2+ in transit on every endpoint.
- AES-256 at rest via the managed-Postgres provider (Neon) and Redis (Upstash).

Abuse + rate limiting

- Per-organization daily quotas on outbound email (phishing campaigns, training, vendor invites, trust-page grants). Hard backstops against compromised-account abuse.
- Domain-ownership verification (TXT record or auto-add via Cloudflare/GoDaddy) required before phishing or monitoring.

Backups + DR

- Daily Postgres snapshots + point-in-time recovery via Neon. Documented restore runbook in the operations handbook.

Incident response

- Public security policy at SECURITY.md with vulnerability reporting instructions. 72-hour breach-notification commitment per the Data Processing Addendum.

Compliance frameworks (in-product)

We help customers run readiness assessments against:

CMMC L1 / L2 / L3 | SOC 2 (Trust Services Criteria) | NIST CSF 2.0 | DMARC / SPF / DKIM

2 · SUB-PROCESSORS

Third-parties that process your data

Each sub-processor is bound by their own privacy and security commitments plus a contractual DPA with us. Always-current list: https://tools.resolute-security.com/sub-processors

VENDOR	ROLE	REGION	CERTIFICATIONS
Neon	Managed Postgres — primary data store for all customer records.	US (AWS us-east-1)	SOC 2 Type II, ISO 27001
Fly.io	Application + worker hosting (compute, networking).	US + EU (per app region)	SOC 2 Type II
Upstash	Managed Redis — background-job queue + ephemeral rate-limit state.	US (AWS us-east-1)	SOC 2 Type II
Resend	Transactional email delivery (magic links, alerts, digests, training).	US	SOC 2 Type II
Stripe	Payment processing, subscription management, invoicing.	US + EU	PCI DSS Level 1, SOC 1 / SOC 2, ISO 27001
Sentry	Error and exception monitoring (stack traces + metadata only).	US	SOC 2 Type II, ISO 27001, HIPAA-eligible
Google	OAuth sign-in (only invoked when a user chooses Google sign-in).	US + global	SOC 2 Type II, ISO 27001, ISO 27017, ISO 27018
Microsoft	OAuth sign-in + M365 integration for connected tenants.	US + global	SOC 2 Type II, ISO 27001, FedRAMP High
Cloudflare	CDN, DNS, DDoS mitigation, WAF in front of the application.	Global edge	SOC 2 Type II, ISO 27001, PCI DSS Level 1

What we collect, why, and how long

What we collect

- Account: email, name, organization, hashed password if enabled, MFA secret if enrolled, OAuth identifiers from Google/Microsoft when used.
- Subscription metadata from Stripe (no card data — Stripe tokenizes and stores; we hold only the customer + subscription IDs).
- Scan + monitoring data: domain names, DNS query results, scoring metadata. No SMTP message bodies; no mailbox contents.
- Compliance content: assessment answers, notes, and evidence files uploaded by the customer.
- Operational: IP addresses, user-agent strings, audit-log events (sign-in, configuration changes). Used for security forensics and rate limiting.

How long we keep it

- Account + compliance content: until the customer deletes the account; backups age out per schedule (typically 35 days).
- Audit logs: 12 months.
- Magic-link tokens, expired sessions, rate-limit counters: pruned daily.

What we don't do

- We don't sell or share customer data. We don't train AI models on customer data.
- We don't use third-party advertising, marketing pixels, or cross-site trackers. Only strictly-necessary first-party cookies (session, current-org, OAuth state).

Data subject rights

GDPR / UK GDPR / CCPA rights are honored regardless of jurisdiction. Self-serve at https://tools.resolute-security.com/your-rights. We respond within 30 days (45 under CCPA with notice).

Where everything lives

Contractual

Data Processing Addendum: https://tools.resolute-security.com/dpa

Terms of Service: https://tools.resolute-security.com/terms

Service Level Agreement: https://tools.resolute-security.com/legal/sla

Privacy Policy: https://tools.resolute-security.com/privacy

Operational

Sub-processor list: https://tools.resolute-security.com/sub-processors

Status + incident history: https://tools.resolute-security.com/status

Security policy (SECURITY.md): github.com/irresolute-sec/smb-tools/blob/main/SECURITY.md

Gated artifacts

SOC 2 Type II report, pen test summary, and other gated artifacts are available on request through the public trust page at https://tools.resolute-security.com/trust/resolute. NDA acknowledgement may be required for some items.

Contact

Security questions: security@resolute-security.com

Privacy / data-subject requests: privacy@resolute-security.com

General: hello@resolute-security.com