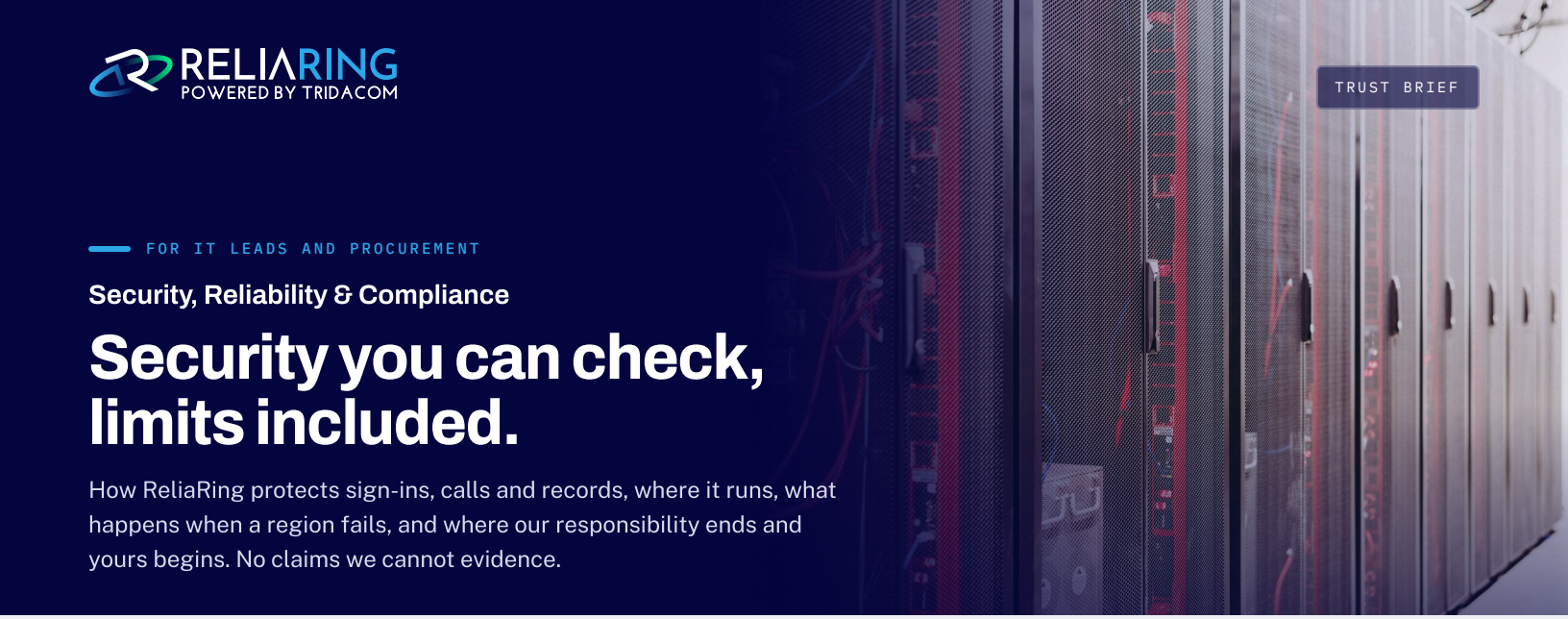
RELIARING
POWERED BY TRIDACOM



TRUST BRIEF

FOR IT LEADS AND PROCUREMENT

Security, Reliability & Compliance

Security you can check, limits included.

How ReliaRing protects sign-ins, calls and records, where it runs, what happens when a region fails, and where our responsibility ends and yours begins. No claims we cannot evidence.

SIX AREAS

What is in place today

Canadian hosting

Primary infrastructure runs on Microsoft Azure in Canadian data centres. We say plainly what can leave the country.

- Primary hosting on Microsoft Azure, Canada Central and Canada East.
- Call recordings sit in private Canadian cloud storage, reached through short-lived signed links.
- The database has no public network access; only the platform's private network reaches it.
- Speech (voicemail transcription, generated voices), AI, email, payments and push can process data outside Canada.
- Privacy policy written to PIPEDA and Alberta's PIPA; questions go to privacy@reliaring.com.

Encryption in transit

Connections are encrypted hop by hop. Calls carried over the public phone network are not end-to-end encrypted.

- Portal and API served over HTTPS, TLS 1.2 minimum, behind a web application firewall.
- SIP signalling over TLS 1.2 or later on port 5061.
- SRTP voice media for desk phones that negotiate it.
- Browser and mobile apps use secure WebSocket signalling with DTLS-SRTP media.
- Sign-in passwords stored as bcrypt hashes; SIP and trunk credentials encrypted with AES-256-GCM.

Identity and access

Each person has their own sign-in and a role. Access can follow your company directory.

- Single sign-on with Microsoft Entra ID, Google Workspace, Okta, or any SAML 2.0 / OIDC provider.
- SCIM 2.0 creates, updates and removes users and groups from your directory.
- Authenticator-app two-step sign-in with backup codes; administrators can require it for everyone.
- Four roles per organisation: Admin, Supervisor, User and Limited. Changes apply immediately.
- Sign any device out from the portal; it is refused on its very next request.

Resilience and failover

Each region runs a full calling stack, so one can fail without the other stopping.

- Each region has its own SIP edge, call server, media relay and WebRTC gateway.
- Phones and trunks get an endpoint in each region; failover behaviour depends on the device.
- Outbound calls retry on up to two alternate carrier routes if a carrier fails.
- The database keeps a hot standby in a second zone and a replica in Canada East.
- Public status page shows each region and incident history, with email alerts on changes.

Emergency calling (E911)

Register a validated street address for eligible calling numbers and check it by dialling 933.

- Addresses validated for Canada and the US, with building, floor and room detail.
- Dial 933 to hear your number and registered address read back. Free and unlimited.
- Up to 10 registered addresses per user; one endpoint included per user and per trunk.
- Alerts your own people by email, SMS, voice call or webhook when 911 is dialled.
- Outbound calling stays closed until someone accepts the VoIP 911 limitations in writing.

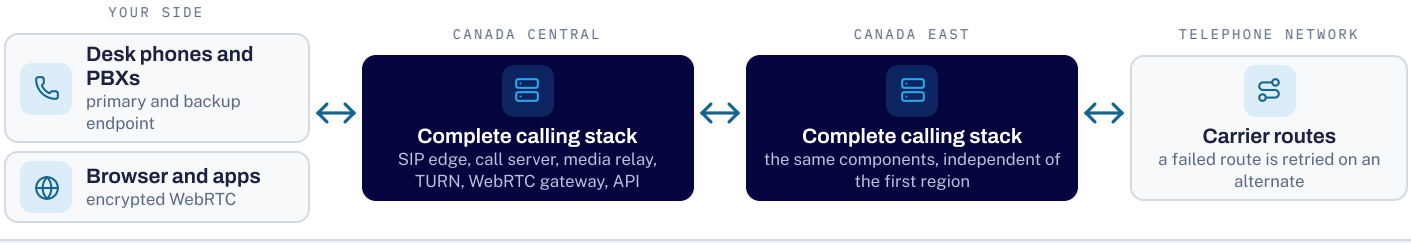
Fraud and caller ID

Controls aimed at the two things that go wrong on phone systems: toll fraud and spoofed caller ID.

- International calling is off by default, with separate switches per account, user and trunk.
- SIP trunks authenticate by registration or listed IP addresses, each with a concurrent-call ceiling.
- Pay-as-you-go trunks are prepaid, with the balance checked before each call.
- Failed sign-ins are rate-limited per account and per IP address.
- Outbound calls carry STIR/SHAKEN attestation; incoming calls get an attestation check, and likely spam is flagged or blocked.

ARCHITECTURE

How the Canadian calling network is built



SHARED RESPONSIBILITY

Where our part ends and yours begins

RELIARING

- Run the platform across multiple Canadian data centres, with database backups kept for 35 days.
- Encrypt application connections, and hash or encrypt every stored credential.
- Keep each account's data isolated from every other account.
- Keep a 365-day audit trail, staff access included, that your administrators can read and export.
- Carry 911 calls with the address you registered, and publish service status.

YOU

- Keep every E911 address current, and dial 933 after any move.
- Turn on two-step sign-in or single sign-on, and remove leavers promptly.
- Give each person the narrowest role that lets them do their job.
- Choose the recording notice and confirm the consent rules where you call.
- Keep power and internet backup on site; VoIP 911 needs both.

SPECIFICATIONS

For the questionnaire

Hosting	Microsoft Azure, Canada Central and Canada East (primary)
Calls	SIP over TLS 1.2+ (port 5061); SRTP for desk phones; DTLS-SRTP for browser and mobile apps
Web and API	HTTPS, TLS 1.2 minimum; web application firewall in blocking mode
Data at rest	Cloud-platform storage encryption; stored credentials encrypted with AES-256-GCM
Database	Zone-redundant standby, Canada East replica, 35-day point-in-time restore
Single sign-on	SAML 2.0 / OIDC (Entra ID, Google Workspace, Okta); SCIM 2.0 provisioning
Sign-in security	TOTP two-step with backup codes, enforceable account-wide; passwords 8+ characters, bcrypt-hashed

HONEST LIMITS

What we do not claim

- No independent security certification (SOC 2, ISO 27001) or completed penetration test is claimed. Send your security questionnaire; we answer it as things stand.
- ReliaRing is built for the Canadian market: HIPAA compliance and Business Associate Agreements are not offered. A SOC 2 audit is planned; no report exists yet.
- Primary hosting is Canadian, but this is not an all-data-in-Canada commitment: speech (voicemail transcription and generated voices), AI, email, payments and push delivery may process data elsewhere. Fax text recognition stays in Canada.
- No uptime percentage or service-credit SLA is published, and signup is open to Canadian businesses only today.

Audit trail	Sign-ins, failed sign-ins, member, role, settings, API-key and support-access events; CSV export; kept 365 days (fax access log 7 years)
Recording consent	One-party, all-party or geographic notice in English, French or Spanish, or your own recording
API keys	Read-only or read-write, per resource group; optional IP allowlist and expiry

Got a security questionnaire to fill in? Send it over, and we will answer it as things stand today.

Learn more
reliaring.com/features/security

Talk to a person
1-888-491-RING

Email
help@reliaring.com

SCAN FOR THE SECURITY PAGE

ReliaRing is a brand of Tridacom IT Solutions Inc. Prices are in Canadian dollars unless marked USD, exclude applicable taxes, are current as of November 2026 and may change. Service is available to businesses in Canada. Read the HTML edition