

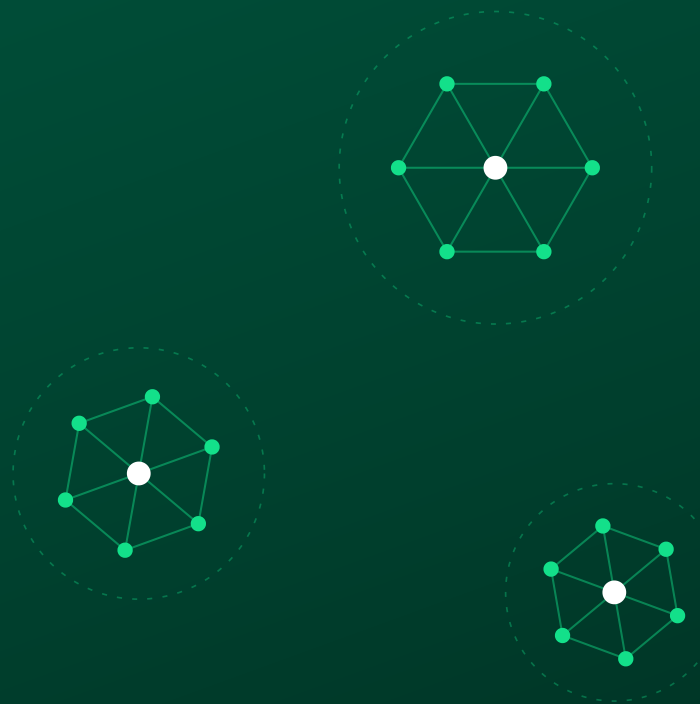


SECURITY WHITEPAPER

TRUST & SECURITY

Security architecture

How StratIQ AI protects your deal, property, and client data, and how our controls line up with SOC 2 and other industry standards.



AT A GLANCE

Isolation by design, not by policy

Every StratiqAI customer runs in a dedicated environment with its own virtual machine, encrypted volume, private network, and encryption key. This paper explains how that design protects your data and how it maps to SOC 2 and other industry frameworks.

1 : 1

Dedicated microVM, encrypted volume, and private network per customer

AES-256

GCM envelope encryption with a key unique to your environment

60 sec

Lifetime of the signed, single-use handoff into your workspace

60 days

Volume snapshot retention, plus off-platform archives

Contents

01 Executive summary

02 Shared responsibility and infrastructure foundation

03 Customer isolation

04 Architecture and data authority

05 Identity and access

06 Encryption and key management

07 Connecting outside systems

08 AI agent safety

09 Application security

10 Change management and supply chain

11 Resilience, backup, and monitoring

12 Data lifecycle

13 SOC 2 and industry standards alignment

14 Security roadmap

15 Contact and responsible disclosure

This paper describes controls in place as of October 2026. Controls that are planned but not yet in place are listed only in section 14.

Executive summary

Commercial real estate teams trust StratiqAI agents with offering memoranda, rent rolls, leases, underwriting models, and client relationships. We built the platform so that this material is isolated by design, not just by policy.

Our core commitments:

A dedicated environment for every customer.

Each organization's web application, data, and StratiqAI agents run inside a dedicated, hardware-isolated virtual machine with its own encrypted volume and its own private network. Your working data never shares a runtime, a database, or a network with another customer's.

Encryption everywhere.

Traffic is encrypted in transit with TLS. Data is encrypted at rest. Credentials you connect are encrypted again at the application layer with a key that belongs only to your environment.

Least privilege by default.

Your environment holds no credential that can read another customer's data. Agents start read-only. People get only the role they need, and sensitive actions require a fresh sign-in.

Humans approve consequential actions.

Agents ask before running risky commands, and a fixed set of dangerous operations is refused outright.

Privileged actions are recorded.

Operator actions and sensitive administrative changes, such as credential and connection changes, are written to an append-only audit log.

Aligned with SOC 2.

Our controls are designed to align with the AICPA SOC 2 Trust Services Criteria, and our infrastructure providers hold their own independent SOC 2 Type II and PCI DSS attestations.

SECTION 02

Shared responsibility and infrastructure foundation

StratiqAI runs on established cloud infrastructure providers. Each supplies a layer, and each is independently audited.

Layer	What it provides	Provider attestation
Compute and networking	Hardware-virtualized microVMs, encrypted block volumes, private IPv6 networking, global TLS edge	SOC 2 Type II; hardware in ISO 27001 certified data centers
Control-plane database	Managed PostgreSQL with automated backups and row-level security	SOC 2 Type II
Object storage	Encrypted storage for file attachments and backup archives	SOC 2 Type II
Payments	Hosted checkout, subscription billing, and card storage	PCI DSS Level 1 Service Provider; SOC 2 Type II

Responsibility is shared as follows:

- **Our infrastructure providers** secure physical data centers, hardware, the hypervisor, and the underlying network.
- **StratiqAI** secures everything we build and operate on top: customer isolation, identity and access, encryption and key management, the agents and their permissions, application security, change management, monitoring, and backups.
- **Your organization** decides who on your team has access and in what role, which outside systems you connect, which agents may write to those systems, and how your people review agent output.

SECTION 03

Customer isolation

A dedicated virtual machine per customer

Every customer environment is its own lightweight virtual machine (a microVM). Each microVM has its own kernel and runs behind hardware virtualization, which is a stronger boundary than the shared-kernel containers many multi-tenant services use. Your web application and your StratiqAI agents run on that machine together, and no other customer's workload runs inside it.

A dedicated encrypted volume

Your conversations, files, agent memory, and connected credentials live on a block volume attached only to your virtual machine. The volume is encrypted at rest by the infrastructure provider.

A private network per customer

Each customer environment is attached to its own private IPv6 network (6PN) for its entire life. Private networks for different customers have no route and no private DNS between them, so one customer's environment cannot even discover another's. **The network is the security boundary.** Your web address separates browser sessions, but isolation does not depend on it.

A minimal public surface

Inside your environment, the StratiqAI agent runtime and its management dashboard listen only on the local machine. They are not published to the internet or to any private network. Your web application is the only service your environment exposes:

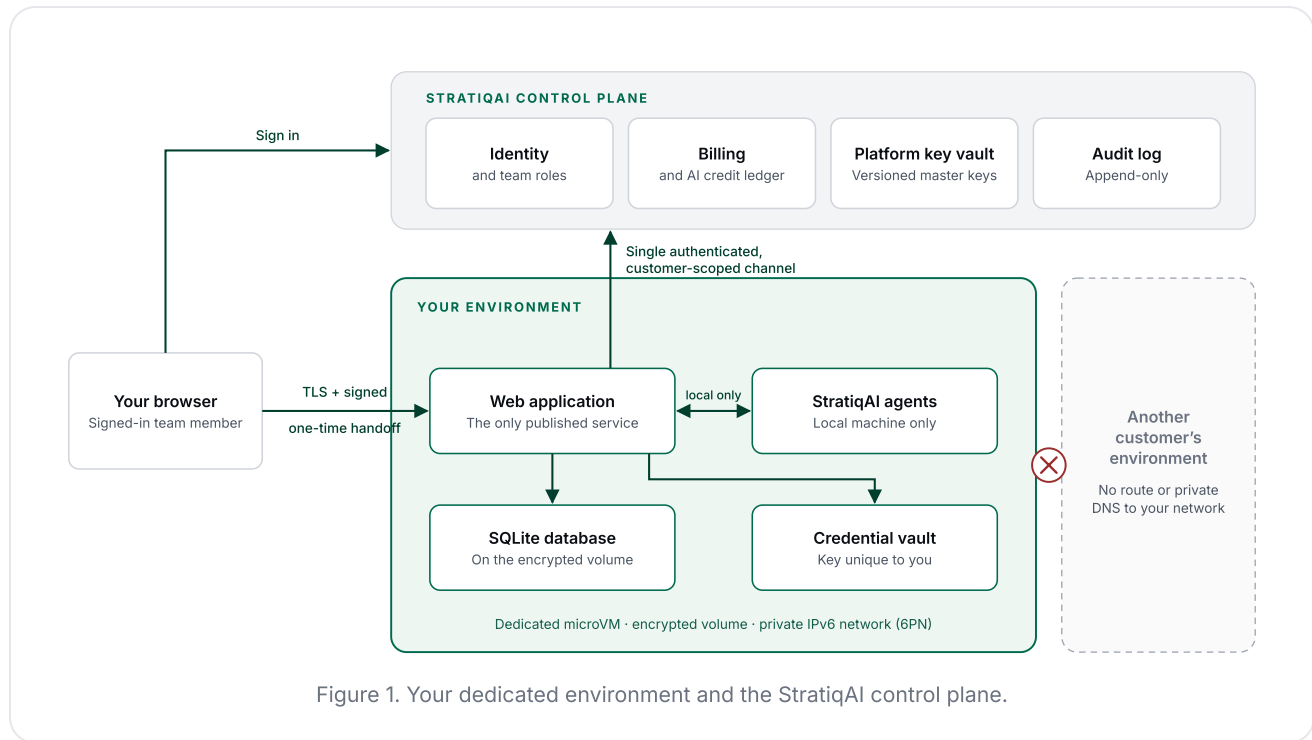
- It accepts HTTPS (TLS) and redirects plain HTTP to HTTPS.
- Agents reach their tool endpoints over the local machine, and the team collaboration endpoint refuses requests from anywhere else.
- Internal maintenance endpoints are never exposed on the public edge.
- A private health-check path exposes only health and readiness status.

Suspend when idle

Environments that are not in use suspend to zero compute and resume when you return. Nothing runs in a suspended environment until a request wakes it.

Architecture and data authority

StratiqAI separates a central **control plane**, which handles accounts, billing, and fleet operations, from your **dedicated customer environment**, which handles your work.



What lives where

Kept in your dedicated environment	Kept in the control plane
Conversations and messages	User accounts and sign-in
Team chat, tasks, and activity	Organizations, memberships, and invitations
Attachment records	Subscriptions, billing, and the AI credit ledger
Your sessions	Fleet provisioning, monitoring, and image rollouts
Your connected-system credentials (encrypted)	Workspace settings and agent roster
Agent memory and working files	Audit log of administrative actions

Your working data is stored in a SQLite database on your environment's encrypted volume, so the busiest paths, like chat and agent tool calls, stay on local disk and never cross a shared database.

One narrow, accountable link to the control plane

Your environment talks to the control plane over a single outbound HTTPS channel. It authenticates with a credential unique to your environment, which can be rotated, and the control plane accepts that credential for your organization only. Only an explicit allowlist of operations is accepted. Anything else is rejected.

The control plane sends your environment a minimal snapshot: your agent roster, settings, status, and whether AI credits are available. It does not send other customers' data.

No cross-customer credentials

No customer environment holds the central database credentials, the infrastructure management token, the payment processor secret, or the platform key vault's master keys. Even if your environment were fully compromised, it would hold nothing that can read another customer's data.

SECTION 05

Identity and access

Signing in

People sign in to StratiqAI with an email and password or with a supported single sign-on provider such as Google. Sign-in, organization membership, and workspace selection are handled centrally by the control plane.

Sessions

- Session cookies are `HttpOnly` (not readable by page scripts), `Secure` (sent only over HTTPS), and `SameSite=Lax` (withheld from cross-site requests other than following a link).
- A session lasts at most 8 hours. Account sessions also end after 1 hour of inactivity.

Signed handoff into your environment

When you open your workspace, the control plane issues a **handoff token** signed with Ed25519 (RFC 8032). The token:

- names the person, their role, and the one customer environment it is for;
- expires within 60 seconds;
- can be used only once. Your environment records each token's identifier and refuses a replay;
- is rejected by any environment it was not issued for.

Your environment checks the signature, then creates its own session cookie. The token-exchange endpoint is rate-limited per network address.

Live permission checks

Alongside the handoff, your environment receives a signed **actor token** that identifies the person on each request it makes to the control plane. The control plane checks the signature and then reloads the person's current membership before it authorizes anything. **When you remove a team member, their access to administrative operations ends on their next request**, not when a session eventually expires.

Step-up for sensitive actions

Destroying a workspace, rotating credentials, and replacing or disconnecting a connected system's key all require a sign-in from the last 10 minutes. Otherwise StratiqAI asks the person to confirm who they are again first.

Team roles

Each organization has three roles: **owner**, **admin**, and **member**. Billing, settings, team membership, agent hiring, and connected-system changes are limited to the roles that need them.

StratiqAI operator access

StratiqAI support access is limited to a named allowlist of staff accounts that sign in through single sign-on. Every operator change must give a written reason and is recorded in the audit log. Destructive operations also require the operator to type the workspace's name to confirm. Infrastructure credentials are scoped to a single environment, and production tooling refuses to run with credentials from any other environment.

SECTION 06

Encryption and key management

In transit

- All browser traffic uses TLS. HTTP Strict Transport Security (HSTS) tells browsers to use HTTPS only for one year, including subdomains.
- Traffic between your environment and the control plane, and between StratiqAI and outside services, uses HTTPS.
- Traffic between your web application and your StratiqAI agents never leaves the local machine.

At rest

- Customer volumes are encrypted at rest.
- Object storage for attachments and backup archives is encrypted at rest.
- The control-plane database is encrypted at rest by the managed database provider.

Application-layer envelope encryption

Credentials for the systems you connect, such as OAuth tokens and API keys, get a second layer of encryption on top of storage encryption:

- Each secret is encrypted with its own random 256-bit data key using **AES-256-GCM** (NIST SP 800-38D), which provides both confidentiality and tamper detection.
- That data key is in turn encrypted (wrapped) with a **key-encryption key**.
- Each encrypted secret is cryptographically bound to its owner (your organization and the kind of secret). A secret copied into another context will not decrypt.

A key that belongs only to your environment

Every customer environment has its **own independently generated key-encryption key**. It is installed only in that environment and is never stored in the control-plane database. Compromise of one environment can expose only that environment's own connections. The control plane's vault keys are never present in customer environments.

Rotation

Key-encryption keys are versioned. When a new version is installed, your environment re-encrypts every stored secret under it at startup. The previous version is retired only after an operator confirms that nothing still uses it.

Escrow and recovery

So that a lost environment key does not mean lost connections, each environment key is sealed to an **offline recovery key** using X25519 key agreement (RFC 7748), HKDF-SHA256, and AES-256-GCM. Only the sealed copy is kept centrally. The recovery private key is held offline, outside production systems, source control, and the database. Each environment pins the fingerprint of the expected recovery key and refuses to seal to any other, so the recovery key cannot be quietly swapped.

SECTION 07

Connecting outside systems

StratiqAI agents work with the tools your team already uses, such as Microsoft 365, Google Workspace, CRMs, and data providers. Each connection is designed so that your credentials stay in your environment.

OAuth connections

Providers require a fixed sign-in return address, so the OAuth sign-in starts and finishes at the control plane. Then:

1. Your environment collects the encrypted connection bundle over its authenticated channel.

2. It stores the bundle in its own encrypted vault and confirms it has done so.
3. The control plane then deletes its temporary copy.

When a token expires, your environment refreshes it on demand and stores the new token locally.

API key connections

When an admin pastes an API key, it goes straight to your environment. StratiqAI checks the key with the vendor and stores it only in your environment's encrypted vault. The key is **never returned to the browser, written to logs, or sent to the control plane**. The control plane only learns that the connection exists and whether it is healthy.

Read-only by default

- Connections start **read-only**. Writing to an outside system has to be turned on for that connection.
- Even then, each **agent** must be granted write access individually. Otherwise, write tools are not offered to that agent at all.
- Our Microsoft 365 connector requests read-only permissions to mail, calendar, and files.

Protection against request forgery

Outbound connector requests are restricted to protect your network and ours from server-side request forgery (SSRF):

- HTTPS only.
- Only the hosts listed for that connector can be called.
- Redirects are refused.
- Destinations that resolve to private, loopback, link-local, or internal network addresses are refused.
- Response sizes are capped.

SECTION 08

AI agent safety

StratiqAI agents are capable assistants, so we give them the same kind of guardrails you would give a new hire.

- **Approval before action.** By default, agents must get a person's approval before they run a command flagged as risky. Workspace admins can choose a less strict mode, but the deny rules below always apply.
- **Hard deny rules.** A fixed set of operations is refused regardless of approval mode, including accessing credential files, editing the agent's own configuration, touching the workspace database directly, piping downloaded content into a shell, and wiping the data volume.

- **Guarded memory and skills.** When enabled, changes an agent makes to its long-term memory or skills require approval.
- **Separate agents, separate keys.** Each agent you hire has its own profile, memory, and access keys inside your environment. Roles you have not hired are not installed.
- **Spending controls.** Each customer has its own key for the AI model gateway, capped by a spending limit tied to your prepaid AI balance. When the balance runs out, new AI work pauses instead of running up charges. Your environment can read its credit status but cannot change balances. The ledger is kept centrally.
- **Bring your own model keys.** Organizations with their own model provider agreements can supply their own keys.
- **No cross-customer context.** Agents see only your environment's data, because no other customer's data exists on your virtual machine.

SECTION 09

Application security

The web application applies defenses aligned with the OWASP Top 10 and the OWASP Application Security Verification Standard (ASVS):

- **Content Security Policy.** By default, only first-party scripts, styles, fonts, and connections are allowed. Plugins are blocked, and form submissions and the base URL are restricted to our own origin.
- **Clickjacking protection.** Pages cannot be framed by other sites (`frame-ancestors 'none'` and `X-Frame-Options: DENY`).
- **Browser isolation headers.** `X-Content-Type-Options: nosniff` , `Cross-Origin-Opener-Policy` and `Cross-Origin-Resource-Policy` set to same-origin, a strict `Referrer-Policy` , and a `Permissions-Policy` that turns off the camera, microphone, and geolocation.
- **Cross-site request forgery protection.** State-changing requests must come from a trusted origin.
- **Rate limiting** on sign-in handoff, chat, attachments, connections, and agent tool endpoints.
- **Secret redaction in logs.** Structured logs automatically redact cookies, API keys, credential values, encryption keys, and payment secrets.
- **Short-lived file links.** Attachments upload directly to encrypted object storage through signed links that expire after 15 minutes by default. Downloads go through the application, which checks access first.
- **Signed webhooks.** Payment webhooks are accepted only with a valid cryptographic signature.
- **No card data.** Payments use the payment processor's hosted checkout and billing portal. Card numbers never touch StratiqAI systems.
- **Database protections.** Row-level security is enabled on control-plane tables. Private application data is closed to the database's public and anonymous roles, and browsers never query the database directly.
- **Least-privilege services.** The web application runs as an unprivileged operating-system user.

SECTION 10

Change management and supply chain

Separate environments

Development, staging, demo, and production run in separate cloud accounts, each with its own database, encryption keys, access tokens, and payment configuration. Non-production environments use the payment processor's test mode. Credentials and encryption keys are never shared between environments.

Tracked and reviewed changes

Every code, configuration, and documentation change is tied to a tracked work item and lands through a pull request on its own branch. A person approves the merge. Changes are tested in development and staging before they reach production, and database schema changes follow the same order.

Immutable, pinned images

- Runtime images are referenced by cryptographic digest, never by a movable tag. The platform refuses image references that are not digest-pinned.
- An image is built once and promoted between environments unchanged, with the same digest.
- Base images, dependencies, and build automation are pinned to exact versions, and automated pull requests keep them current.
- The parts of the image that define agent roles are read-only at runtime.

Careful rollouts

New images go to one canary customer environment first, then expand. If an environment fails its readiness checks after an update, the platform tries to roll it back automatically. A rollback never deletes volumes or environments.

SECTION 11

Resilience, backup, and monitoring

Two independent backup mechanisms

- **Volume snapshots.** Snapshots of each customer volume are kept for 60 days. One is also taken right before every configuration change, agent hire or removal, and software rollout, so a recovery point always predates the change.
- **Off-platform archives.** A full archive of each environment is taken weekly, with a quicker archive on the other days. Archives go to separate encrypted object storage, so they survive even if the compute platform itself is unavailable.

- **Control-plane database.** The managed database provider backs it up automatically, and we take a manual backup before each schema migration.

Tested restores

A restore builds a **new** volume from a snapshot and keeps the old one, so a restore is itself reversible. It also rotates each agent's access keys and rebuilds configuration from the control plane. We rehearse the full sequence in staging: destroy an environment, restore it, and verify that agents, their instructions, and their memory all come back.

Continuous monitoring

- Health and readiness checks run against every customer environment.
- An automated reconciler compares the intended state of the whole fleet with what is actually running every 15 minutes. It reports drift and never deletes anything on its own.
- Critical findings, failed jobs, failed rollouts, and failed restores alert the operations team.

SECTION 12

Data lifecycle

- **You own your data.** Your organization keeps ownership of everything you provide. We process it only to operate your agents.
- **Retention.** Chat messages and agent tool activity are kept for 90 days on base plans and 365 days on higher plans, then deleted automatically.
- **Disconnecting a system** deletes its stored credentials from your environment.
- **Removing an agent** deletes that agent's profile and keys from your environment.
- **Cancellation.** After a subscription is cancelled, there is a 7-day grace period, and then the environment, including its virtual machine and volume, is deprovisioned.
- **Data residency.** Customer environments and the control-plane database run in United States regions by default.

SECTION 13

SOC 2 and industry standards alignment

StratiqAI's controls are designed to align with the AICPA SOC 2 Trust Services Criteria. StratiqAI has not yet completed an independent SOC 2 audit. That audit is on our roadmap (see section 14). The providers listed in section 2 hold their own current SOC 2 Type II reports.

Trust Services Criteria mapping

Criteria	Focus	How StratiqAI addresses it
CC6.1	Logical access security	Dedicated environment per customer; private per-customer network; owner, admin, and member roles; envelope encryption with per-customer keys
CC6.2 and CC6.3	Granting and removing access	Central identity and membership; live membership check on every administrative request, so removals take effect on the next one; per-agent write grants
CC6.6	Protection from outside threats	Single published service per environment; agent runtime on local machine only; TLS and HSTS; SSRF protection; rate limiting; strict browser security headers
CC6.7	Protecting data in transit	TLS on every external connection; local-only traffic between application and agents
CC6.8	Preventing unauthorized software	Digest-pinned immutable images; read-only role definitions; pinned dependencies with automated updates
CC7.1 and CC7.2	Monitoring and detection	Health and readiness checks; 15-minute fleet reconciliation; alerting; append-only audit log of operator and sensitive administrative actions
CC7.3 to CC7.5	Incident response and recovery	Operator triage procedures; automatic rollback; manual, reversible restores rehearsed in staging
CC8.1	Change management	Tracked work items; branch and pull request flow with human merge approval; staged promotion through development, staging, and production; canary rollouts
CC9.2	Vendor and business partner risk	Infrastructure providers selected for independent SOC 2 Type II and PCI DSS Level 1 attestations
A1.2 and A1.3	Availability, backup, and recovery	60-day volume snapshots; snapshot before every change; weekly full and daily quick off-platform archives; restore drills

Criteria	Focus	How StratiqAI addresses it
C1.1 and C1.2	Confidentiality and disposal	Per-customer encryption keys; secrets never logged or returned; retention limits; credential deletion on disconnect; deprovisioning after cancellation
P series	Privacy	Data used only to operate your agents; retention schedule; published privacy policy

Other frameworks

- **NIST Cybersecurity Framework 2.0.** Our controls cover all six functions: Govern (tracked change management and operator accountability), Identify (a single source of truth for every environment), Protect (isolation, encryption, least privilege), Detect (reconciliation and alerts), Respond (triage and rollback), and Recover (snapshots, archives, and restore drills).
- **NIST SP 800-207 zero-trust principles.** No request is trusted because of where it comes from. Every cross-boundary call carries a signed, audience-bound credential, and permissions are re-checked against live membership.
- **OWASP Top 10 and ASVS.** See section 9.
- **CIS-style secure configuration.** A minimal exposed surface, services that listen only on the local machine, unprivileged application processes, and configuration rendered from a central source rather than edited by hand.
- **Cryptographic standards.** AES-256-GCM (NIST SP 800-38D), Ed25519 signatures (RFC 8032), X25519 key agreement (RFC 7748), and HKDF (RFC 5869).

SECTION 14

Security roadmap

We publish what we have not finished as well as what we have. The following work is planned:

PLANNED

Multi-factor authentication.

A second sign-in factor for customer accounts and StratiqAI operator accounts.

PLANNED

Least-privilege agent runtime.

Running the agent runtime as an unprivileged user inside each virtual machine, matching the web application.

PLANNED

Zero data retention with AI model providers.

Prompts and outputs will not be retained by upstream model providers.

PLANNED

Signed and scanned images.

Every runtime image will be signed, ship with a software bill of materials (SBOM), and be scanned automatically for vulnerabilities.

PLANNED

Independent SOC 2 Type II audit.

An outside auditor's examination of StratiqAI's own controls over time.

PLANNED

Custom domains per customer.

Each provisioned individually rather than through shared wildcard routing.

PLANNED

Recovery objectives and incident response.

Published recovery point and recovery time objectives (RPO and RTO), and a formal incident response policy that includes customer notification commitments.

SECTION 15

Contact and responsible disclosure

To request our security questionnaire responses, discuss your organization's requirements, or report a suspected vulnerability, use the [contact page](#). We review every security report and appreciate responsible disclosure: please give us a reasonable chance to fix an issue before you share it publicly.