Due Diligence Pack

Managed-device deployment

July 2026

Proxara, Inc.

28 Geary St. Suite 650 PMB 5328

San Francisco, CA 94108

proxara.ai

What Proxara Is

Proxara is a semantic anonymization proxy for regulated firms. It sits between your employees and the external AI tools they use, redacting sensitive data before prompts leave your environment.

Proxara operates as a native background service on macOS and Windows. It intercepts AI-bound HTTPS traffic at the operating system network layer, covering every application on the device: browsers, desktop AI apps (Claude Desktop, ChatGPT Desktop), coding tools, command-line interfaces, and API calls.

Employees type prompts as they normally would. Proxara detects client names, account numbers, SSNs, portfolio values, and other sensitive entities in real time. Those values are swapped out for context-aware placeholders that keep the prompt useful while stripping anything that would violate FINRA or SEC Reg S-P. The AI responds based on the cleaned prompt. Proxara restores the original values in the response so the employee sees natural text.

Proxara provisions and manages all backend infrastructure. Nothing to set up on your end beyond installing the service on employee devices.

When something needs attention, Proxara sends it directly to you through email, Slack, or Microsoft Teams. No dashboard to check. No login to remember. Everything comes to you.

A governance console exists for initial setup and configuration (vocabulary policies, sensitivity thresholds, archive connection). But day-to-day, you do not need to open it. Weekly summary emails and real-time alerts keep you informed without adding another tool to your stack.

Coverage

- **AI tools:** ChatGPT, Claude, Gemini, Perplexity, DeepSeek, Grok, Copilot
- **Desktop apps:** Claude Desktop, ChatGPT Desktop, and other Electron-based AI applications
- **API calls:** Direct API usage through curl, Python scripts, coding assistants, and custom integrations

- **File uploads:** Spreadsheets, PDFs, CSVs, and documents uploaded to AI tools are analyzed before transmission
- **Platforms:** macOS and Windows
- **Browsers:** All browsers (Chrome, Edge, Firefox, Safari, Brave, Arc) covered at the OS network layer with nothing for the employee to install

How It Works

The service runs as a privileged background process (LaunchDaemon on macOS, Windows Service on Windows). It installs a locally-generated root certificate authority whose X.509 Name Constraints exclude sign-in, banking, healthcare, government, and security-tooling domains in the certificate itself. It decrypts a connection only on positive evidence the destination is an AI service, and leaves all other traffic untouched.

1. Employee opens an AI tool (browser, desktop app, or CLI) and types a prompt
2. The operating system routes the HTTPS connection through the local proxy (via Network Extension on macOS, system proxy on Windows)
3. The service inspects the request and extracts the prompt text and any attached files
4. Proxara's classifier identifies sensitive entities based on your industry profile (wealth management, legal, healthcare, etc.)
5. Sensitive identifiers are replaced with context-aware placeholders that keep the prompt intact and useful
6. The cleaned prompt is forwarded to the AI provider over the original HTTPS connection
7. The AI responds. The service restores original values in real time, including in streaming responses.
8. If the interaction is flagged, an alert is delivered to your workflow (email, Slack, or Teams)

KEY PROPERTY

Full device coverage at the OS network layer

Proxara intercepts at the OS network layer, so desktop applications, CLI tools, and API calls are covered automatically alongside the browser. There is nothing for the employee to install, enable, or configure. The service starts at boot and runs silently.

The Root Certificate

The device service installs a root CA in the operating system's trust store. This is the mechanism that allows it to inspect encrypted HTTPS traffic to AI domains.

What it can do

Sign TLS certificates for AI provider domains (claude.ai, chatgpt.com, gemini.google.com, etc.) so the service can decrypt, inspect, redact, and re-encrypt traffic to those domains.

What it cannot do

The root CA contains an X.509 Name Constraints extension whose excluded subtrees bar sign-in and identity, banking and payments, healthcare, government, and security-tooling domains. On platforms that enforce name constraints, a certificate this CA issues for an excluded domain does not validate, and the exclusions are readable directly out of the certificate. Beyond that, the agent decrypts a connection only on positive evidence the destination is an AI service and tunnels everything else through without inspection, so sign-in, banking, healthcare, and government traffic is never intercepted.

Covered domains

Out of the box, the certificate covers the major AI providers:

- claude.ai
- anthropic.com
- chatgpt.com
- openai.com
- gemini.google.com
- perplexity.ai
- copilot.microsoft.com
- deepseek.com

- grok.com
- x.ai

This list is not fixed. Internal AI tools, third-party AI wrappers, and new providers can be added through the governance console. The domain registry refreshes automatically every 30 minutes across all devices.

The certificate is unique to each device. It is generated locally during installation and the private key never leaves the device. Uninstallation removes the certificate from the trust store and deletes all key material.

Data Handling

Proxara is a real-time processing layer, not a data store. Prompts are classified and redacted as they pass through. Nothing is retained beyond what is needed to deliver an alert to you.

What happens when something is flagged

You receive the full context in an alert (email, Slack, or Teams): the interaction, any files involved, and the classification. From there, one click sends it to your compliance archive (Smarsh, Global Relay, or equivalent) for immutable retention. Once archived or dismissed, Proxara purges it.

What happens when nothing is flagged

The interaction passes through and is not stored. Proxara does not log benign usage.

Redaction mappings

The link between a placeholder like [Client_A] and the original value is stored in a local database on the employee's device. This database uses session-scoped keys with a 24-hour time-to-live. Expired mappings are automatically purged. The database is not accessible to other applications and is deleted on uninstall.

On-device data

DATA	LOCATION	LIFETIME
Redaction mappings	Local embedded database (sessions.redb)	24-hour TTL, auto-purged hourly
Service configuration	config.json in data directory	Persistent until uninstall
Root CA key material	PEM files in data directory (root-only permissions)	Persistent until uninstall
Cached file uploads	In-memory only	5-minute TTL, max 10 files, max 5 MB each
Service logs	Log files in data directory	Overwritten on restart

Classification engine

The classification engine (hosted via AWS Bedrock) processes prompts in real time and discards them immediately. Inputs and outputs are not stored. For firms that require fully on-premises processing with zero external calls, Proxara also supports a locally hosted model running within the dedicated environment.

Each deployment is single-tenant and fully isolated. No shared infrastructure. No data commingling. Your compliance archive (Smarsh, Global Relay, or equivalent) is the system of record. Proxara is not.

Security

Encryption

- **In transit:** TLS 1.2+ on all connections between the device service and Proxara's API. AI domain traffic is intercepted via locally-generated per-domain certificates signed by the Name Constrained root CA.
- **At rest:** AES-256 encryption across the backend database, archives, and storage (AWS KMS, customer-managed keys).

- **On device:** The local session database and CA private key are stored in a directory accessible only to root/SYSTEM.

Network isolation

- The backend runs in a dedicated VPC with private subnets
- No direct inbound internet access to backend services
- Traffic restricted to required ports only
- The device service binds exclusively to 127.0.0.1 (localhost). No ports are exposed to the network.

Certificate pinning

- Some applications enforce certificate pinning, which rejects any certificate not matching a pre-configured fingerprint. The service detects this automatically (a fast TLS failure within 3 seconds of the CONNECT tunnel) and adds the host to a bypass list. Future connections to that host pass through without interception.

QUIC blocking

- Modern browsers may use QUIC (HTTP/3 over UDP/443) for AI domains, which would bypass the TCP proxy. The service installs platform-specific firewall rules (pf on macOS, WFP on Windows) that block UDP/443 to resolved AI domain IPs, forcing browsers to fall back to standard HTTPS over TCP.
- These rules apply only to AI domain IPs and are removed on uninstall.

Access controls

- Role-based access for the governance console
- All actions logged with identity and timestamp

Audit logging

- Append-only, immutable log for all compliance actions
- Entries are never updated or deleted

- Tamper-evident by design

Subprocessors

AWS is the only subprocessor. No third-party analytics, data enrichment, or external processing.

Full security documentation: proxara.ai/legal/security-overview

Compliance Support for Wealth Management

FINRA Rule 3110 (Supervision)

Real-time monitoring of all employee AI interactions across every application on the device. Flagged events delivered to you through your existing workflow. Immutable audit log of all supervision actions.

SEC Regulation S-P

Client PII is redacted before it reaches any external AI tool, regardless of whether the employee uses a browser, a desktop app, or an API client. The redaction preserves the usefulness of the prompt while protecting client data.

Recordkeeping (SEC Rule 17a-4)

One-click archive from any flagged alert to your compliance archive provider (Smarsh, Global Relay, or equivalent). Proxara holds flagged events for up to 7 days so you can review and act. Long-term retention is handled by your archive provider.

Vocabulary enforcement

Configurable term policies. Block or warn on firm-specific language (performance guarantees, misleading claims, restricted terminology). Each term supports rewrite suggestions and a visible reason for the employee.

Employee monitoring disclosure

A customizable disclosure notice is shown to employees on their first visit to any AI tool. The notice is injected directly into the AI tool's page by the device proxy. The notice can

be pre-accepted for MDM deployments by setting `consent_given: true` in the configuration profile.

Deployment

The device service is distributed as a signed installer package (.pkg for macOS, .msi for Windows). Deployment requires administrative access and is intended to be coordinated with IT.

For firms with MDM (JAMF, InTune, Kandji, Mosyle), the installer is uploaded as a managed application and pushed to target devices. For smaller firms, the installer can be run manually with administrative privileges.

A detailed deployment guide with technical specifications, verification steps, and configuration reference is included separately in this pack.

Backend Infrastructure

Proxara provisions a dedicated, single-tenant cloud environment for your firm on AWS. This is a fully isolated deployment. There is no shared infrastructure, no multi-tenant database, and no data commingling with any other customer. Proxara has no ability to read your data outside of the operational access needed to keep the environment running.

COMPONENT	WHAT IT DOES
Classification API (EC2)	Receives prompts from the device service, classifies sensitive entities, returns redaction instructions. Processes in real time and discards inputs immediately.
AWS Bedrock (Claude)	AI inference for classification. Runs within a dedicated AWS account in the region you choose. No model training on your data. Optionally replaced with a self-hosted model on GPU instances for zero external API calls.
PostgreSQL (RDS)	Stores audit records, vocabulary policies, and configuration. AES-256 encrypted with customer-managed KMS keys.
S3 Archive Storage	Stores flagged interaction records for up to 7 days until archived or dismissed. AES-256 encrypted. S3 Object Lock (WORM) available.
Governance Console	Web interface for managing policies, sensitivity thresholds, alert routing, and archive connections.

Proxara manages provisioning, updates, monitoring, and maintenance. Your firm does not need to set up or maintain anything on the server side.

If your firm prefers to host the environment yourself, Proxara provides deployment templates and documentation for customer-managed AWS deployments. In that model, Proxara has no access to your data and acts as a software licensor only. This is also available as an MSP-managed deployment through your existing IT provider.

Auto-Update

The service checks for updates every 4 hours. When a new version is available, it downloads the signed installer, verifies the code signature (pkgutil on macOS, Authenticode on Windows), and installs silently. The service restarts automatically. No IT intervention is needed for routine updates.

The domain registry (list of AI provider domains to intercept) refreshes every 30 minutes from the Proxara API. New AI tools can be covered without updating the service binary.

Corporate Information

Entity	Proxara, Inc.
Type	Delaware C-Corporation
Incorporated	April 1, 2026
Filing number	10569090
Registered agent	Northwest Registered Agent Service, Inc.
Founder	Jex Pearce

Address

28 Geary St. Suite 650 PMB 5328
San Francisco, CA 94108

Formation documents

The following are included as separate attachments in this pack:

- Certificate of Incorporation (State of Delaware)
- Corporate Bylaws
- Incorporator Initial Resolutions

Additional Documentation

Full legal and compliance documentation is available at proxara.ai/legal:

- Master Subscription Agreement
- Data Processing Addendum
- Product Privacy Policy
- Service Level Agreement
- Data Protection Impact Assessment
- Acceptable Use Policy
- Security Overview
- Employee Monitoring Disclosure
- Subprocessor List
- HIPAA Business Associate Agreement

Technical Support

Jex Pearce

jex@proxara.ai

proxara.ai