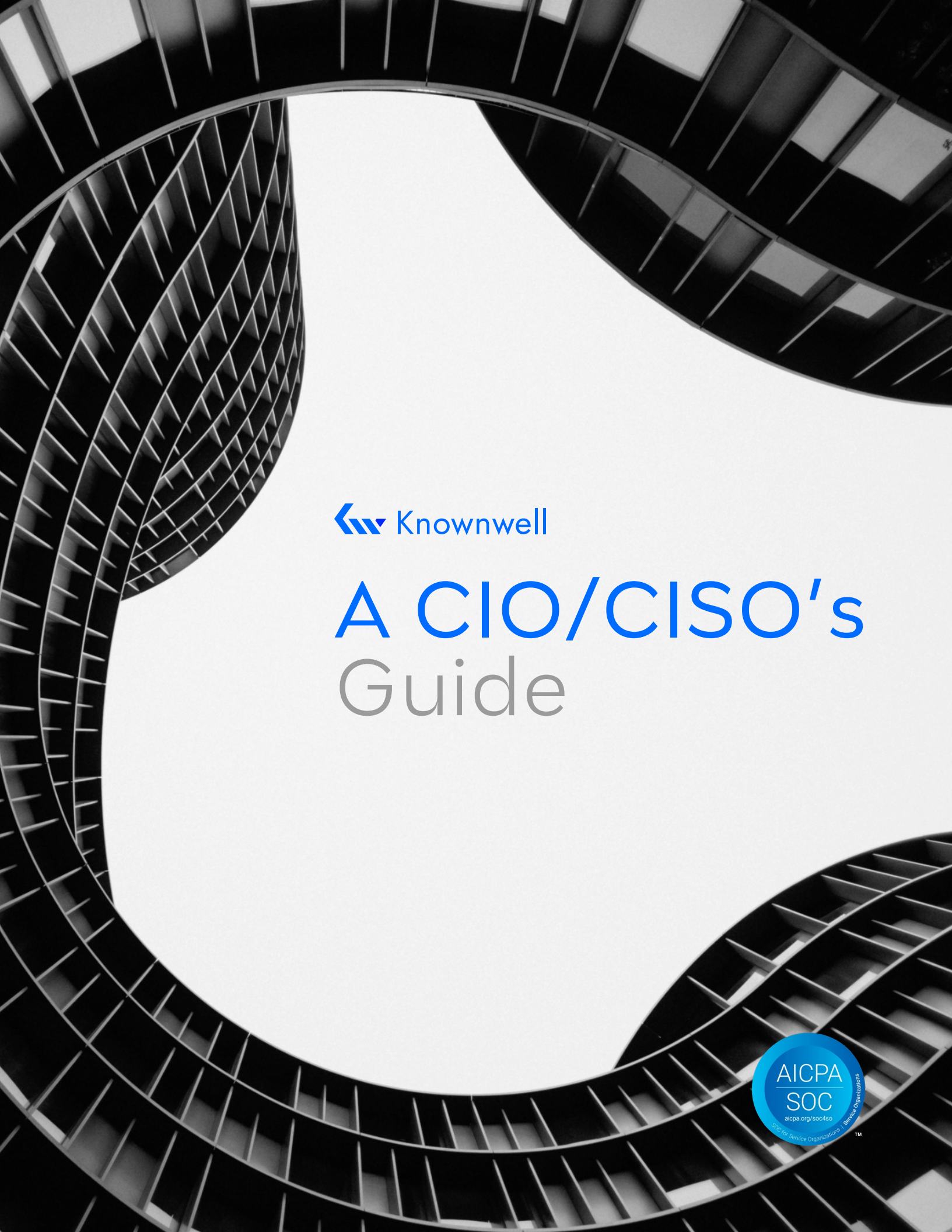


Knownwell

A CIO/CISO's Guide

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations
™

Introduction

Your organization has decided to implement Knownwell. Knownwell is a commercial intelligence platform that synthesizes your company's natural information into performance metrics and insights. It helps your client services, delivery, and sales teams support, retain, and grow your clients' economic relationships.

Knownwell has been designed from the ground up to comply with the latest security and privacy standards, minimize IT support requirements, and simplify monitoring and management.

This guide is intended to answer any configuration or security questions and assist you through the implementation. An appropriately credentialed IT Administrator can implement Knownwell in less than 30 minutes.

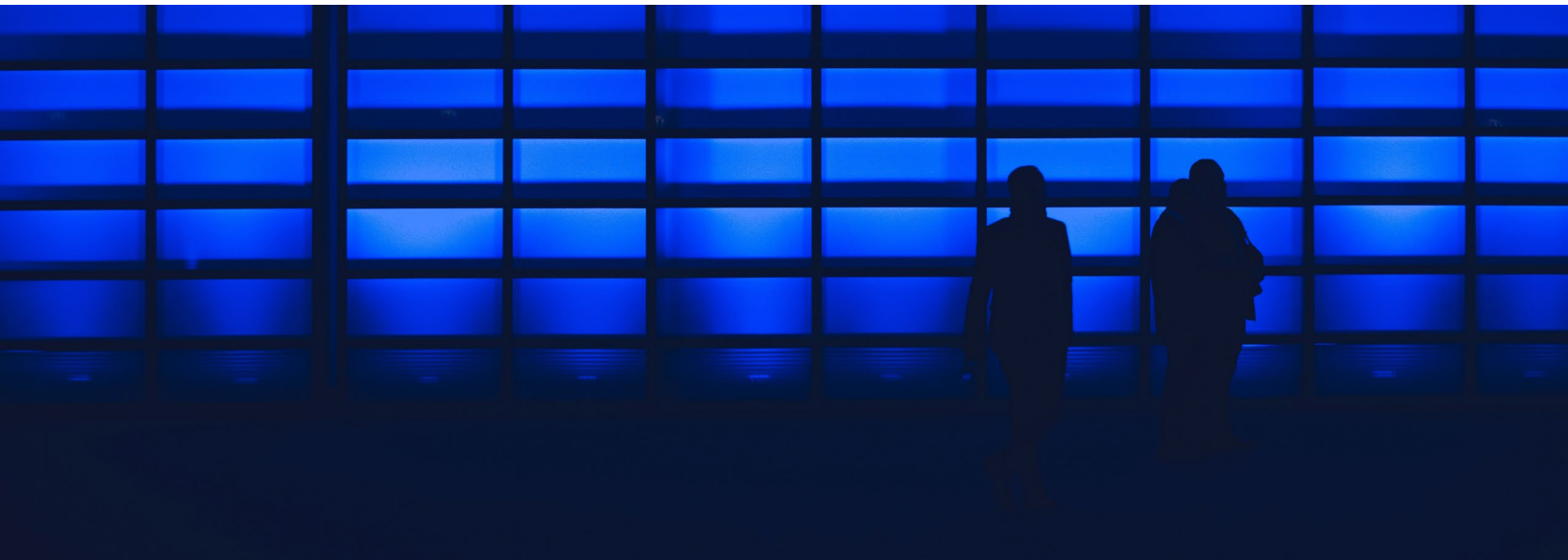
Before You Start

Welcome to Knownwell! We're excited to partner with you to help unlock your organization's commercial engine. This section outlines critical security and access considerations to ensure a smooth and secure implementation.

Security Fundamentals

At Knownwell, we take data security and privacy seriously. Our platform is built on a foundation of industry-leading standards, including:

- SOC 2 Type 2: We've undergone extensive audits to ensure your data's confidentiality, integrity, and availability.
- HIPAA: To ensure that we don't process protected health information (PHI), our platform filters out such data, thus safeguarding sensitive data.
- Encryption: All data is encrypted at rest (AES-256) and in transit (TLS 1.2 or higher).
- Multi-Tenancy: We enforce multi-tenancy at multiple levels to maintain strong data isolation. Your data is logically separated and securely stored, preventing unauthorized access.



System Access

Knownwell offers flexible and secure access options:

- **Single Sign-On (SSO):** We support SSO via SAML or OAuth 2.0, allowing your users to access Knownwell with their existing credentials.
- **Multi-Factor Authentication (MFA):** MFA is enforced for all administrative and privileged actions, adding an extra layer of protection.
- **Role-Based Access Control (RBAC):** RBAC ensures users only see and interact with data necessary for their role.
- **Identify and Access Management:** We utilize advanced Identity and Access Management (IAM) systems to manage access controls to the cloud platform and perform access reviews to ensure the principle of least privilege is followed.

Data Access and Governance

We prioritize data privacy and adhere to the following principles:

- **Data Minimization:** We collect and process only the minimum necessary data.
- **Purpose Limitation:** Data is used solely for its intended purpose.
- **Data Retention:** Data is retained per our retention policy and/or is as required by law.
- **Data Destruction:** Data that is no longer needed is securely destroyed following NIST compliant processes.
- **Data Subject Rights:** We respect data subject rights and provide mechanisms to exercise those rights.
- **Data Backups:** Data is securely backed up daily and stored for 90 days. Point-in-time recovery allows for data to be restored to the minute within the last 7-day window.

Infrastructure

- **Cloud Provider:** We are fully deployed in Google Cloud Platform (GCP). These data centers maintain industry-leading certifications (ISO 27001, SOC 2, etc.) and high physical security standards.
- **Reliability:** Data and workloads are distributed across multiple zones (data centers) within GCP to ensure availability, durability, and data consistency in response to disaster scenarios.
- **Logical Segmentation:** Production environments are logically separated from development and testing.
- **Network Security:** Firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) guard the production network perimeter.

Key Considerations

- **AI Model Usage:** Knownwell does not train or improve third-party AI models using your data. All AI features protect your data from unauthorized use or sharing.
- **Vulnerability Management:** Regular automated scans (SAST/DAST) and annual third-party penetration tests ensure code integrity.
- **Logging and Monitoring:** System logs are maintained with real-time detection of suspicious or anomalous behavior.
- **Incident Response:** We maintain a formal Incident Response Plan, which is tested semi-annually. Notifications are sent within 72 hours (or faster if the law requires) for incidents impacting customer data.

Next Steps

We are standing by to answer any questions you may have about Knownwell. Please do not hesitate to reach out to us if you have questions at knownwell@knownwell.com.

Additional information regarding Knownwell's Security program and controls is available on our Trust Center: trustcenter.knownwell.com/

Installation Procedures

Overview

Knownwell synthesizes your organization's natural communications, enterprise data, and public information into actionable client intelligence. Instantly know your portfolio's health, understand your clients inside and out, and get the intel you need to retain, delight, and grow your best clients.

Connecting your Email and CRM

Using admin-consent OAuth scopes, Knownwell connects securely with Google Workspace, Microsoft 365, Salesforce, and HubSpot. This allows us to access only the data needed to deliver insights, always with your permission and control.

Our application will guide you step-by-step through the connection process. It's quick, secure, and requires admin authorization to ensure compliance with your organization's access policies.

To configure your clients via a CSV file, the platform will guide you through the upload process.

Our **Customer Success team** is here to help if you have any questions.

Frequently Asked Questions

1. Describe your security posture?

Security is embedded into every stage of our product development, from initial design to release. We follow industry best practices (OWASP, NIST, ISO) to proactively mitigate risks.

Every Knownwell employee undergoes background checks, signs confidentiality agreements, and completes mandatory annual security training.

2. How do I find out more about your security and privacy policies?

We believe in transparency regarding security and privacy. Upon request, we provide access to our Trust and Security portal, which offers detailed information about our security practices, compliance certifications, privacy policies, and ongoing efforts to safeguard your data. This portal is a testament to our commitment to security and privacy, providing the assurance you need to trust us with your sensitive information.

3. What Artificial Intelligence Models do you use?

Knownwell currently uses Google's Gemini models.

4. Who oversees your security program?

Our Chief Information Security Officer oversees our security capability and maintains policies and controls. This team regularly collaborates with product, engineering, and compliance to ensure alignment with regulatory requirements and emerging threats.

5. How do I receive security updates?

We provide quarterly security briefings via email or the customer success team, covering material updates, if any.

6. How do I learn more about your product roadmap?

Major platform releases are accompanied by clear release notes outlining new features, bug fixes, and any security-related enhancements..

7. Why should we trust your Artificial Intelligence?

At Knownwell, we are committed to the responsible and ethical use of artificial intelligence (AI). Our core purpose is “To elevate the dignity of human work through the application of AI.” We firmly believe that AI has immense potential to transform industries and society when developed and applied thoughtfully, positively and humanely.

Our dedication to Responsible AI is exemplified through our commitment to transparency and explainability. We prioritize making our AI systems as transparent and explainable as possible. We provide clear information about their functionality and decision-making processes. Importantly, we show the source communications from which insights are drawn, enabling users to understand the basis of the AI’s outputs.

By surfacing the original data and communications that inform the AI’s insights, we empower users to assess the validity and context of the information. This transparency builds trust in our AI systems and allows users to make informed decisions based on the insights provided.

At Knownwell, Responsible AI is deeply ingrained in our purpose and practices. By integrating transparency and explainability into the core of our AI systems, we aim to create solutions that users can understand and trust, ultimately elevating the dignity of human work and contributing to a more equitable and prosperous future for all.

8. Who owns the data once accessed?

Knownwell customers retain full ownership of their data.

9. Who has access to your data?

Your team’s access to the Knownwell platform is determined by you. Knownwell team access is on a need-only basis and limited to select staff who require access to support or manage the platform. All data is encrypted at motion and rest.

10. Can we limit the types of data that Knownwell ingests?

Yes! Firstly, Knownwell will only ingest data from platforms and accounts that you specify. Knownwell can limit ingestion to specific email addresses, groups, and channels.

Knownwell

Act on what matters