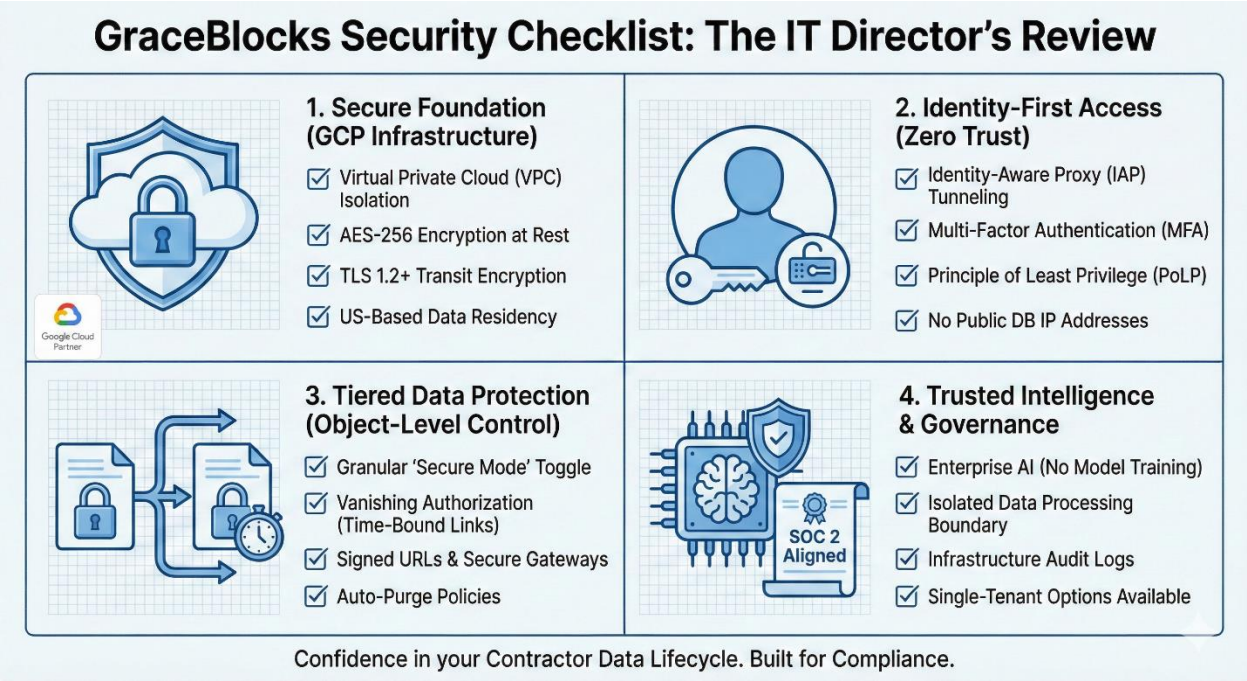
Security Architecture & Data Protection

Whitepaper | Version 1.1 Focus: Contractor Lifecycle & "Shadow HR" Data Sovereignty

---

1. Executive Summary: The "Secure Pull" Model

Traditional HR onboarding and contractor management rely on email—a fundamentally unencrypted protocol where sensitive data (W9s, NDAs, and PII) persists indefinitely in recipient inboxes. GraceBlocks (by GraceRock) replaces this with a **Secure Pull Architecture**. We treat document access as a temporary, validated permission rather than a permanent transmission, ensuring that your organization's most sensitive data remains under your control.



2. Infrastructure & Network Security

GraceBlocks is built on **Google Cloud Platform (GCP)**, utilizing the same security infrastructure that protects global enterprise data.

- **VPC Isolation:** Our production environment resides within a Private Virtual Private Cloud (VPC), logically isolated from the public internet.
- **Encrypted Storage:** All data is encrypted at rest using **AES-256** and in transit via **TLS 1.2+** (HTTPS).
- **Zero-Trust Access:** Administrative access to the database and infrastructure is restricted through **Identity-Aware Proxy (IAP)**, requiring multi-factor authentication (MFA) and individual IAM verification.
- **Regional Residency:** All data is stored and processed within Google's high-availability data centers in the United States.

---

3. Tiered Document Security (Object-Level Control)

GraceBlocks uniquely provides **Object-Level Security**. Rather than applying a single rule to an entire database column, we allow individual files to carry their own security "DNA." This enables workflows to automatically escalate security for sensitive documents like W9s while maintaining performance for standard assets.

Security Mode Comparison

Feature	**Standard Mode**	**Secure Mode**
Use Case	General assets (Headshots, bios)	PII & Legal (W9s, NDAs, Banking)
URL Type	High-entropy GUID (Obscurity)	**Signed URL** or **Node.js Gateway**
Access Window	Indefinite	**Temporary (e.g., 15 minutes)**
Authorization	Knowledge of URL	**Active Session Validation**

Feature	Standard Mode	Secure Mode
Vanishing Access	No	**Yes (Link expires automatically)**

---

4. AI Document Intelligence & Privacy

GraceBlocks leverages the **Google Gemini API** to automate the extraction and verification of contractor data. We prioritize compliance in every AI-assisted workflow:

- **Enterprise Compliance:** Our AI workloads run within Google's **Vertex AI** environment, which is covered under Google Cloud's **SOC 2 Type II** and **ISO 27001** reports.
- **No Model Training:** Consistent with Google's Enterprise Privacy commitments, neither your prompts nor the contents of analyzed documents (e.g., a W9) are used to train or improve Google's underlying Large Language Models (LLMs).
- **Data Boundary:** AI analysis is a transient operation; the data remains within the GraceBlocks security boundary and is never stored by the AI provider.

---

5. Access Governance & Compliance

As we align with **SOC 2 Trust Service Criteria**, GraceBlocks focuses on robust governance and logical access control.

- **Principle of Least Privilege (PoLP):** Permissions are granular. A user can only access documents if they have explicit permission for the specific record and field.
- **Infrastructure Logging:** We utilize **Google Cloud Audit Logs** to monitor infrastructure-level configuration changes, providing a tamper-evident record of administrative activity.
- **Single-Tenant Options:** For enterprise clients with extreme compliance requirements, GraceBlocks offers **Single-Tenant Database** isolation, ensuring your data is physically separated from all other platform tenants.

- **Data Minimization:** GraceBlocks supports automated purging rules, allowing organizations to delete sensitive contractor documents automatically after a set period (e.g., 30 days post-onboarding), reducing long-term data liability.

Appendix: Security FAQ for IT Directors

Q: Where is my data physically located? A: All data is stored in Google Cloud's US-CENTRAL region, benefiting from 99.9% availability and physical security.

Q: Can a GraceBlocks employee view my documents? A: Access is restricted via IAM roles. Employees have no access to customer data unless explicitly granted for a limited troubleshooting window under a "Break-Glass" protocol.

Q: What happens if a secure link is forwarded to an unauthorized person? A: For documents marked as "Secure," the link is tied to a specific session or is a short-lived Signed URL. If forwarded, the link will either expire within minutes or fail to open because the recipient does not have an active GraceBlocks session.