Architecting Trust: The Security and Compliance Framework of Doc-Scribe.ai

A comprehensive overview of our multi-layered defence model for protecting your most valuable digital assets.

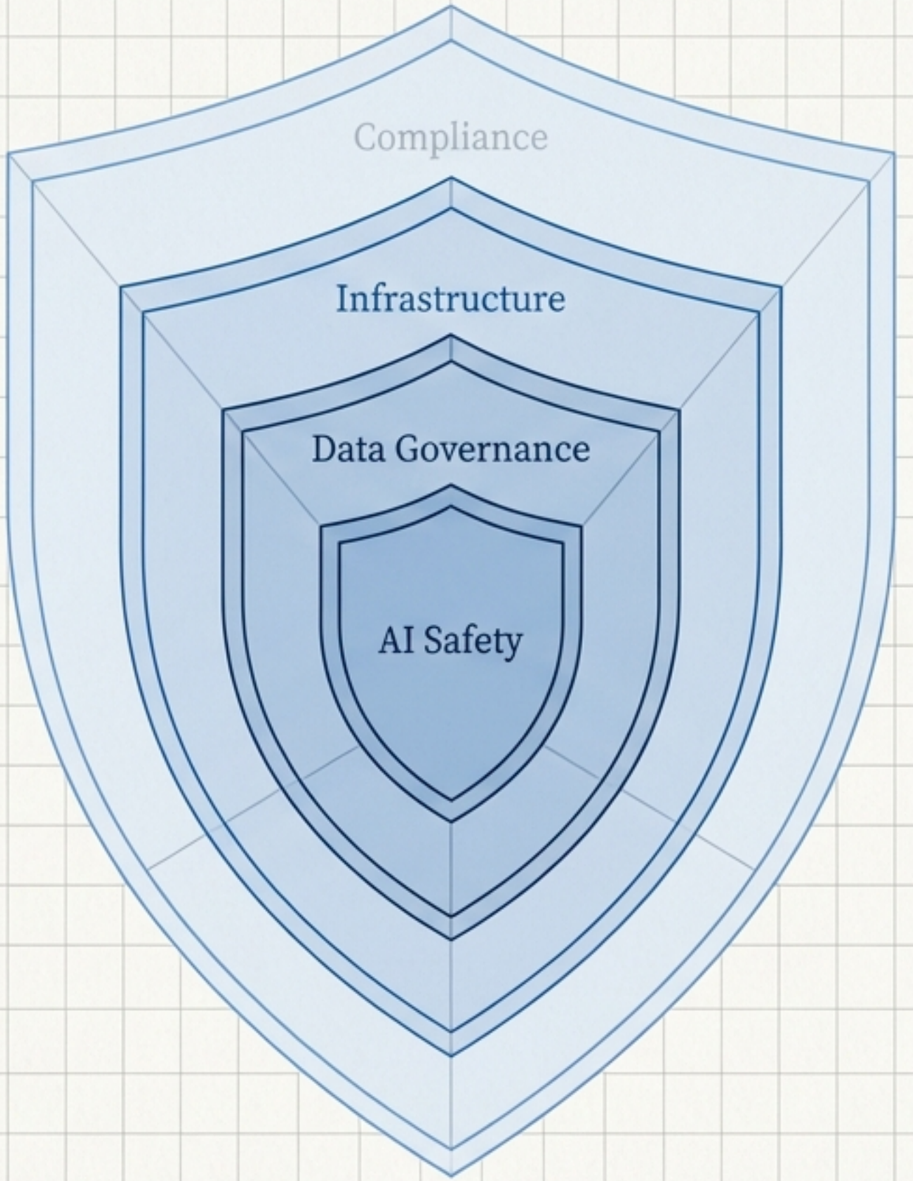
Doc-Scribe.ai

January 2026

Our Foundational Principle: Security is Architected, Not Added.

> “At Doc-Scribe.ai, security and trust are not features—they are the foundational principles of our Digital Management System (DMS).”

We understand that the integrity, confidentiality, and availability of your documents are paramount. Our comprehensive security framework is built upon a **Layered Defense Model**, integrating proprietary architecture with the global compliance of our infrastructure partner, Amazon Web Services (AWS), (AWS), to protect data across its entire lifecycle.



Built on Bedrock: Our Exclusive AWS Foundation

Doc-Scribe.ai is hosted exclusively on Amazon Web Services (AWS), the industry leader in cloud infrastructure. This partnership allows us to inherit a globally-validated security foundation, designed to meet the rigorous requirements of the world's most risk-sensitive organizations.

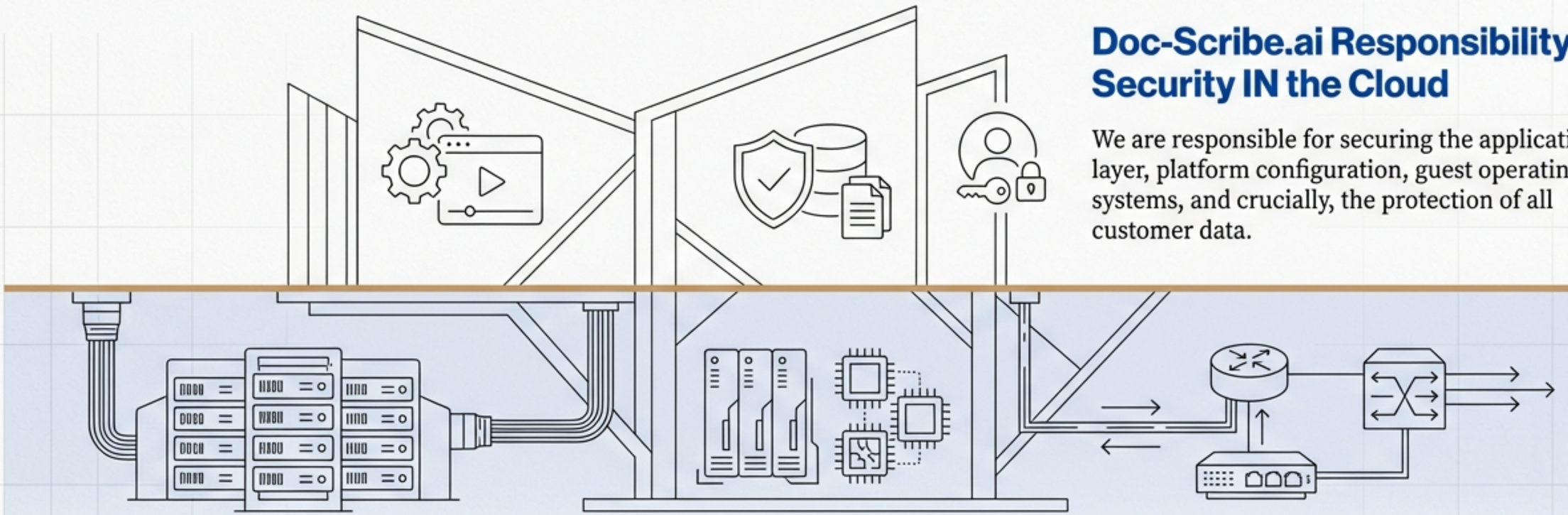
Global Scale: Leveraging AWS's secure, resilient global data centres.

Validated Compliance: Inheriting a platform attested by major standards including **SOC 1/2/3, ISO 27001, and PCI DSS Level 1.**

Serverless Security: Our architecture is secured using **AWS Firecracker micro-VM isolation**, ensuring every process executes within a secure, hardware-virtualized sandbox.

A Clear Partnership: The AWS Shared Responsibility Model

Our security posture is optimally managed by clearly defining responsibilities. This ensures comprehensive protection with no gaps.



Doc-Scribe.ai Responsibility: Security IN the Cloud

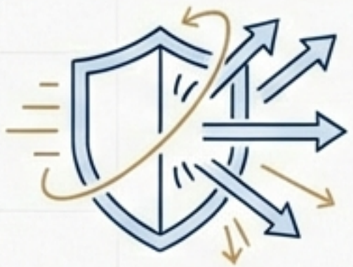
We are responsible for securing the application layer, platform configuration, guest operating systems, and crucially, the protection of all customer data.

AWS Responsibility: Security OF the Cloud

AWS manages and secures the underlying infrastructure, including physical data centres, networking hardware, and the virtualization layer.

The Fortress Perimeter: A Zero Trust Network Architecture

We implement a rigorous **Zero Trust Architecture** where no user or request is trusted by default. Every single request must be authenticated and authorized before gaining access to any resource, regardless of its origin.

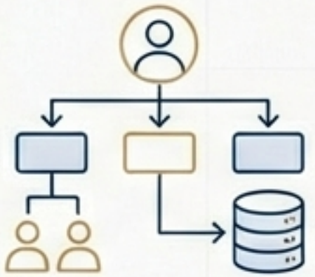


Global DDoS Protection

Utilising **AWS Shield** and advanced edge security services for comprehensive protection against Distributed Denial of Service (DDoS) attacks.

Standardised Identity Protocols

Every request is authenticated and authorized using enterprise-standard identity protocols such as **OIDC/SAML**.



Granular Access Control

Role-Based Access Control (RBAC) ensures access is strictly governed by permissions you assign, enforcing the principle of least privilege.

Securing The Gates: Advanced Authentication and Session Integrity

1. Secure Remote Password (SRP) Protocol

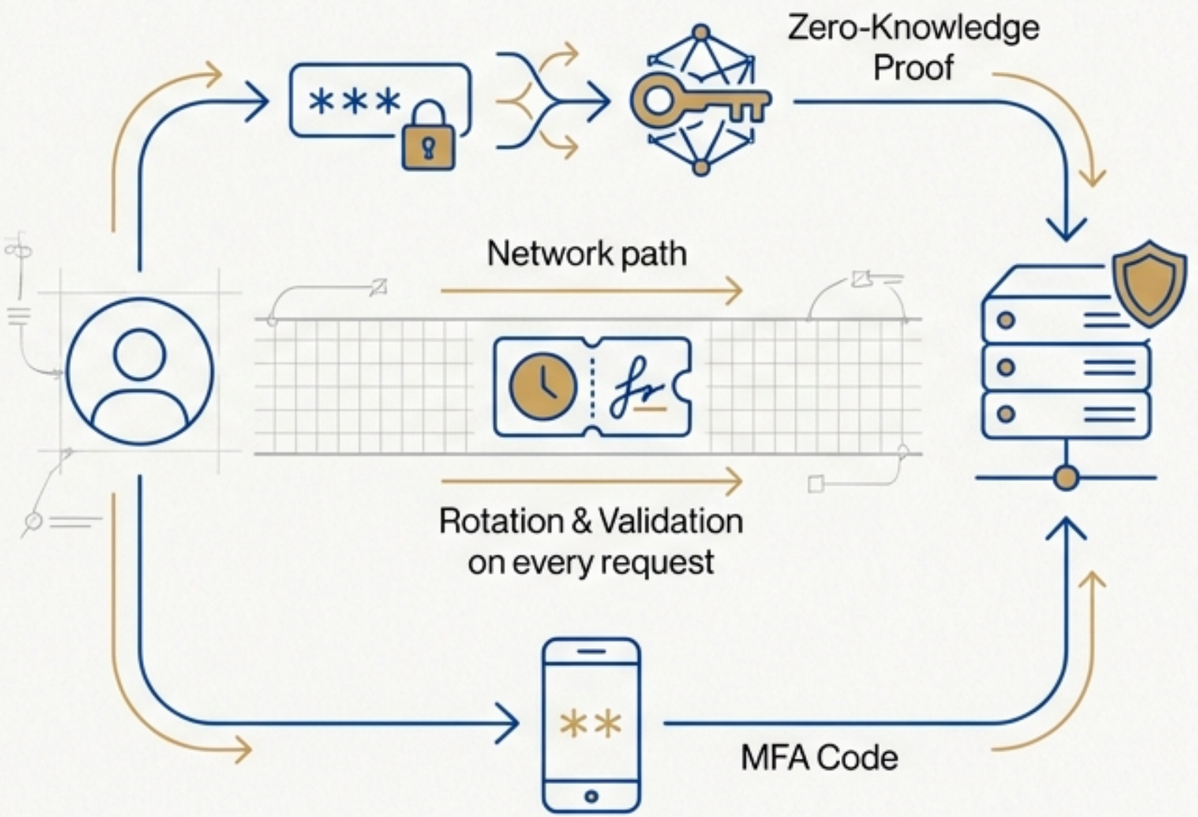
Protects primary authentication. Your password is never transmitted across the network, even encrypted. SRP uses a zero-knowledge proof to verify identity, defending against Man-in-the-Middle and replay attacks.

2. JWT-Based Session Security

Post-login, sessions are managed by **short-lived, cryptographically signed JSON Web Tokens (JWT).** These tokens are automatically rotated and validated on every request to maintain session integrity and minimise risk.

3. Multi-Factor Authentication (MFA)

Enterprise-grade MFA is fully supported, providing an essential second layer of defence beyond traditional credentials.



Your Data is Yours. Exclusively and Absolutely.

“Customer Data is Sacred.”

You maintain **full and exclusive ownership** of all documents and associated metadata uploaded to the Doc-Scribe.ai platform.

Our platform guarantees **Strict Tenant Isolation**.

We use native AWS controls to ensure your organisation’s data is logically, physically, and computationally separated from all other customers at both the storage and compute levels.

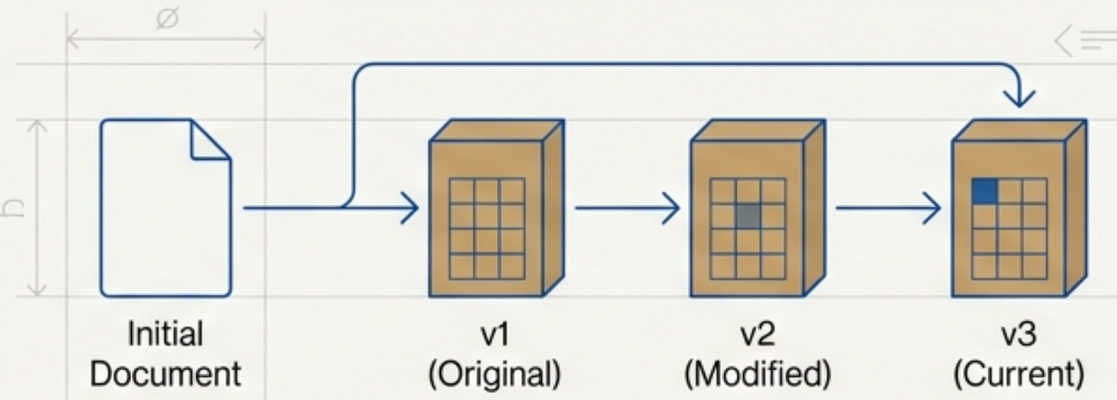
This creates **Zero Cross-Tenant Visibility**.

Preserving the Archives: Guarantees of Data Integrity and Immutability

The integrity of your stored documents is guaranteed through continuous verification and robust versioning.

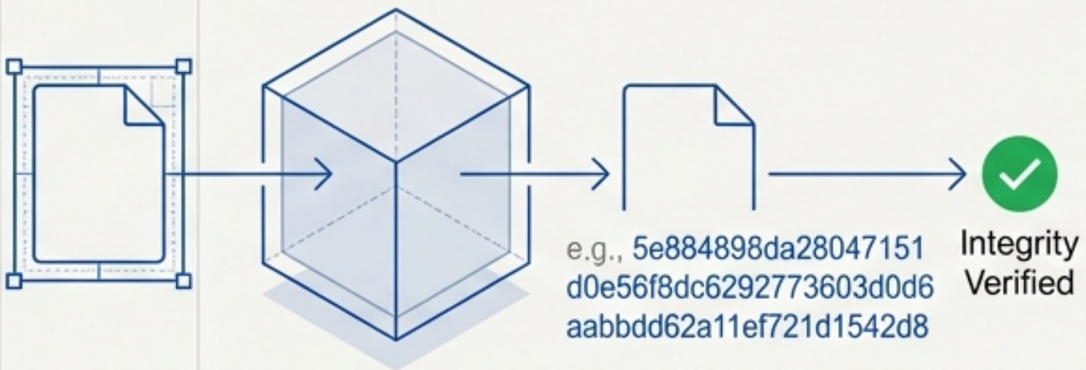
1. Immutable Versioning

Our storage layer implements **Versioned Objects**. Every modification to a document is tracked as a new, immutable version. This provides a complete history, enabling reliable forensic analysis and instantaneous rollback to any previous state.



2. Cryptographic Checksums

We use **SHA-256 integrity checks** during both data transit and storage. This cryptographically verifies that documents remain exactly as they were uploaded, with zero corruption or unauthorised modification.



The Intelligent Command Centre: Enterprise-Grade AI Safety

Our integrated AI features are built on **Amazon Bedrock** and designed from the ground up to be enterprise-safe. We address the most critical business privacy and data security concerns head-on.

Our approach provides a contractually binding guarantee that your data is never used for training third-party models.

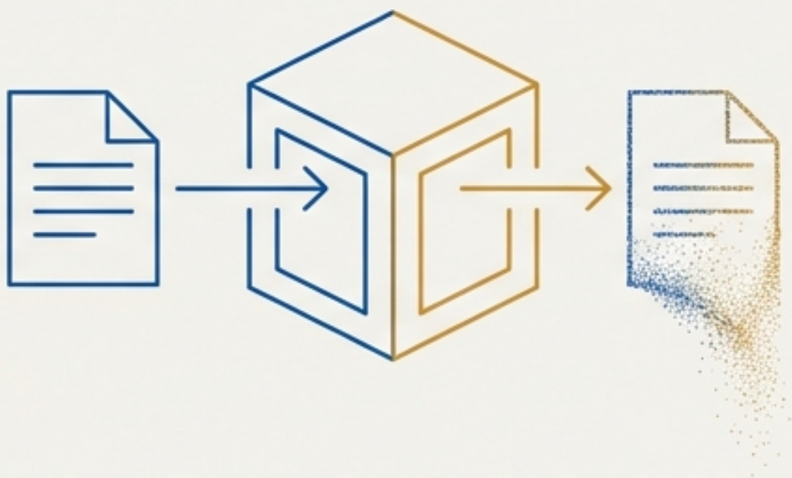
Our Ironclad AI Guarantee: No Training & Zero Persistence

No Data Usage for Training

Amazon Bedrock contractually assures that your input prompts and AI-generated completions are **never** used to train or improve any underlying foundational models. Your data is never shared with third-party model providers.

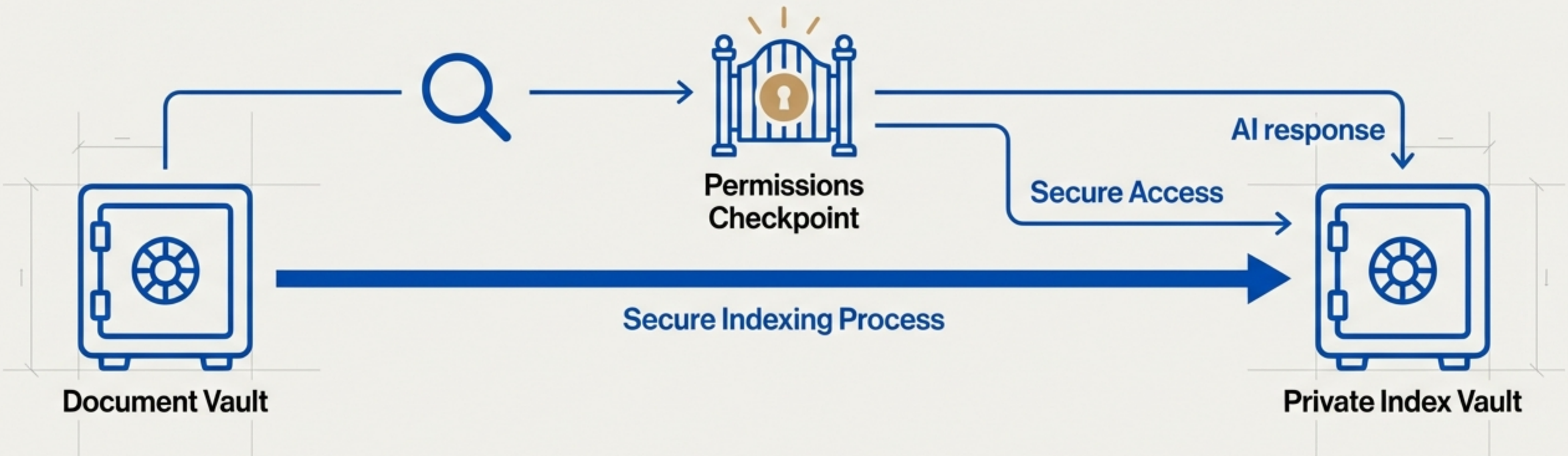
Zero-Persistence Guarantee

All prompts and AI responses are **ephemeral**. They are not logged or retained by the underlying AI infrastructure for model improvement or any other permanent storage purpose.



Your Private Knowledge Base, Secured to the Core

To power our AI features, your documents are indexed into a dedicated, isolated knowledge base created exclusively for your organisation.



Identical Security Controls: This index is secured with the identical, robust **AWS-grade security controls** that protect your primary document store.

Permission-Driven Access: Access to AI-generated summaries and search results is strictly governed by the **document-level permissions** you have already assigned to your users via RBAC. An AI query can never surface data a user is not authorised to see.

The Blueprint for Trust: Validated by Global Compliance Frameworks

Our security controls are not just claims; they are continuously validated and audited. Doc-Scribe.ai operates within an environment designed to meet the world's most rigorous compliance standards.

General Data Protection Regulation

Service Organization Control 2

International Organization for Standardization

Health Insurance Portability and Accountability Act

The Unblinking Sentry: Comprehensive and Immutable Audit Trails

For your compliance and forensic review, every single action performed within your Doc-Scribe.ai environment is logged and secured.

- **Complete Record:** All actions are captured, from user logins to document modifications and AI queries.
- **Tamper-Proof Logs:** We use **AWS CloudTrail and CloudWatch** to create immutable logs. Once written, these records cannot be altered or deleted.
- **Forensic Readiness:** This provides a comprehensive and unchangeable record essential for security audits and incident investigation.

Verifiable Foundations: Resources for Your Due Diligence

We encourage you to review the official security and compliance documentation from our infrastructure partner, Amazon Web Services.

AWS Cloud Security Foundation
https://aws.amazon.com/security/

Amazon Bedrock Data Privacy & Security
https://aws.amazon.com/bedrock/security-compliance/

AWS Compliance Programs
https://aws.amazon.com/compliance/programs/

Continue Your Security Review

Our dedicated security team is available to support your organisation's due diligence process. We are committed to complete transparency and partnership.

For further details, to initiate a security review, or to request our latest compliance certifications, please contact our team directly.

Email
security@doc-scribe.ai