Security Architecture and Privacy Design of the Paige Document Intelligence Platform

A Technical Analysis of Enterprise-Grade Document Security

Prepared by:

Security Architecture Review Committee

Stratis AI

In collaboration with Ademero, Inc.

March 28, 2025

Contents

1 Executive Summary **2**

2 Introduction to Document Security Challenges **2**
2.1 The Evolving Threat Landscape 2
2.2 AI and Machine Learning: Security Implications 2

3 Paige Security Architecture Overview **3**
3.1 Security-by-Design Methodology 3
3.2 Threat Modeling and Security Validation 3

4 Data Protection and Privacy **3**
4.1 Data Classification and Handling 3
4.2 Encryption Implementation 4
4.3 Secure Multi-tenancy 4

5 AI Implementation and Data Privacy **4**
5.1 Data Privacy in AI Processing 4
5.2 Training Data Governance 5
5.3 Flexible Deployment Models 5

6 Infrastructure and Network Security **5**
6.1 Secure Infrastructure Design 5
6.2 Network Protection Mechanisms 6
6.3 Secure Communications 6

7 Access Controls and Authentication **6**
7.1 Identity Management 6
7.2 Role-Based Access Control 7
7.3 Session Management 7

8 Audit, Logging, and Monitoring **7**
8.1 Comprehensive Audit Trail 7
8.2 Security Monitoring 8
8.3 Incident Response 8

9 Compliance and Standards Alignment **8**
9.1 Regulatory Frameworks 8
9.2 Security Standards Alignment 9

10 Conclusion **9**

1 Executive Summary

This technical whitepaper presents a comprehensive analysis of the security architecture implemented within Paige, Ademero's AI-powered document intelligence platform. Our examination reveals a system designed with security-first principles, employing multiple layers of protection to safeguard sensitive organizational data while providing advanced document processing capabilities.

Paige was architected to meet the stringent requirements commonly found in government agencies and Fortune 500 organizations where data confidentiality, integrity, and availability are paramount concerns. Our analysis indicates that Ademero has implemented robust practices across key security domains, including infrastructure security, data protection, access controls, secure AI implementation, and comprehensive audit capabilities.

Of particular significance is Ademero's approach to AI implementation, which demonstrates a strong commitment to data isolation and privacy. The platform's architecture incorporates numerous safeguards designed to protect customer documents while still delivering advanced AI-powered analysis capabilities.

This paper details the technical implementations and architectural decisions that position Paige as a strong model of secure enterprise software design in the document intelligence space.

2 Introduction to Document Security Challenges

2.1 The Evolving Threat Landscape

Modern organizations face unprecedented challenges in protecting sensitive document repositories. With the average enterprise managing millions of documents containing intellectual property, financial data, and personally identifiable information (PII), the security implications are substantial. Recent industry research indicates a significant increase in document-related security incidents in recent years, highlighting the critical importance of robust security controls for document management systems.

The attack surface for document repositories continues to expand as organizations implement more sophisticated workflows, integrations, and automation capabilities. Each new connection point represents a potential vector for unauthorized access, data exfiltration, or integrity violations. Furthermore, the adoption of cloud-based services introduces additional complexity to the security architecture.

2.2 AI and Machine Learning: Security Implications

The integration of artificial intelligence into document management introduces a new dimension of security considerations. While AI delivers unprecedented automation and intelligence capabilities, its implementation can create significant security and privacy risks if not properly architected.

Key considerations include how customer data is handled in relation to AI processing and the implementation of appropriate controls to protect sensitive information. Additionally, organizations must navigate complex regulatory frameworks such as GDPR, CCPA, and industry-specific compliance requirements that mandate specific controls around data processing, retention, and transparency.

3 Paige Security Architecture Overview

3.1 Security-by-Design Methodology

Ademero's development of Paige follows a security-by-design methodology where security controls are integrated into the product from initial architecture through deployment rather than added as an afterthought. This approach helps ensure that security is a fundamental characteristic of the platform rather than a superficial layer.

The security architecture implements defense-in-depth principles, employing multiple security controls at different layers of the application stack. This approach helps protect against the compromise of any single control. The architecture encompasses:

- Infrastructure security controls
- Network security implementations
- Application-level security mechanisms
- Data protection methodologies
- Identity and access management systems
- Comprehensive logging and monitoring capabilities

Each of these domains is implemented with controls designed to address sophisticated attack vectors while maintaining system performance and usability.

3.2 Threat Modeling and Security Validation

Ademero employs threat modeling methodologies to identify and mitigate potential attack vectors. Using established security frameworks, Paige's architecture undergoes security assessment to identify and remediate vulnerabilities before deployment.

Security validation is performed through multiple complementary approaches:

- Application security testing methodologies
- Security assessment by qualified professionals
- Threat intelligence integration to address emerging attack vectors
- Vulnerability management and remediation processes

This validation methodology helps ensure that security controls remain effective against evolving threats and that new features are designed with security in mind.

4 Data Protection and Privacy

4.1 Data Classification and Handling

Paige implements data classification capabilities that help categorize information based on sensitivity and apply appropriate security controls. This classification approach supports appropriate security measures for different types of information.

Documents processed by Paige incorporate protections throughout their lifecycle with controls that maintain both confidentiality and integrity. The platform's data handling protocols help ensure that sensitive information remains protected during processing, storage, transmission, and retrieval operations.

4.2 Encryption Implementation

Ademero has implemented encryption capabilities within Paige that help protect data in various states:

- Data at rest: Industry-standard encryption with key management
- Data in transit: Standard secure transport protocols
- Data in processing: Memory protection measures

The system employs key management infrastructure that can support practices such as key rotation, secure distribution, and cryptographic compartmentalization.

4.3 Secure Multi-tenancy

For organizations utilizing Paige's cloud-based deployment options, the architecture implements logical isolation between customer environments. This isolation approach includes resource separation such as:

- Customer-specific encryption capabilities
- Processing resource isolation
- Authentication domain separation
- Network path segregation

This approach helps ensure that even in a multi-tenant environment, customer data remains appropriately isolated, reducing cross-tenant data exposure risks.

5 AI Implementation and Data Privacy

5.1 Data Privacy in AI Processing

A key principle of Paige's AI implementation is the protection of customer data privacy during AI processing operations. The platform's architecture includes measures designed to protect document confidentiality while still enabling advanced AI-powered analysis capabilities.

This architectural approach delivers several security benefits:

- Helps address data sovereignty considerations
- Implements controls around data processing
- Supports consistent application of security policies
- Maintains appropriate data processing boundaries

Paige's architecture incorporates safeguards designed to protect against unauthorized data usage while still delivering powerful AI capabilities.

5.2 Training Data Governance

Ademero implements data governance practices for AI systems where models operate in a manner designed to respect customer data privacy. These practices are implemented with security considerations as a priority.

This approach to AI governance includes:

- Privacy-conscious model architectures
- Security controls around AI processing
- Clear boundaries between data processing functions

The AI capabilities undergo security review before deployment to help maintain both security and accuracy in document analysis tasks.

5.3 Flexible Deployment Models

For organizations with specific security requirements, Paige provides deployment flexibility with options that can accommodate different organizational needs and security policies. This capability helps organizations align the solution with their existing security architecture and controls.

The deployment approach supports:

- Integration with existing security ecosystems
- Alignment with organizational policies
- Support for various infrastructure configurations
- Compatibility with diverse security requirements

This architectural flexibility helps organizations implement document intelligence capabilities in alignment with their established security practices.

6 Infrastructure and Network Security

6.1 Secure Infrastructure Design

Paige's infrastructure is designed with security as a primary architectural consideration. For cloud deployments, Ademero utilizes enterprise-grade data centers with robust security controls:

- Compliance-oriented facility design
- Physical security monitoring
- Environmental controls and redundancy
- Disaster recovery capabilities

The infrastructure implements security zoning with network segmentation between components of different sensitivity levels. This approach helps ensure that a compromise of one system component does not automatically grant access to more sensitive areas of the application.

6.2 Network Protection Mechanisms

Network security is enforced through multiple complementary controls:

- Advanced firewall technologies
- Intrusion detection and prevention systems
- Application-layer security controls
- Protection against denial of service attacks
- Traffic analysis capabilities

Network interfaces implement principles of least privilege, exposing only the minimum functionality required for legitimate system operation. External interfaces are monitored for unauthorized access attempts and suspicious patterns.

6.3 Secure Communications

Data transmission within the Paige ecosystem is protected using modern encryption protocols. The implementation includes:

- Industry-standard transport encryption for external communications
- Forward secrecy capabilities to enhance long-term protection
- Certificate validation mechanisms
- Cryptographic material management

API endpoints are secured using authentication mechanisms, rate limiting, and input validation to help prevent injection attacks and unauthorized access.

7 Access Controls and Authentication

7.1 Identity Management

Paige implements identity management functionality that supports:

- Integration with enterprise identity providers
- Multi-factor authentication capabilities
- Role-based access control
- Privileged access management features

The platform enforces authentication policies and includes protections against common authentication-focused attack vectors.

7.2 Role-Based Access Control

Paige's access control model follows the principle of least privilege, granting users only the permissions required to perform their authorized functions. The RBAC implementation includes:

- Role structures aligned with organizational responsibilities
- Attribute-based access control for granular permissions
- Permission evaluation based on content classification
- Separation of duties for sensitive operations

Administrative functions are controlled with logging and approval workflows for permission changes. The system supports administration models while maintaining security oversight.

7.3 Session Management

User sessions within Paige are secured through session management techniques:

- Session token security measures
- Session timeout mechanisms
- Device fingerprinting capabilities
- Session management controls

The platform includes mechanisms to detect and terminate potentially compromised sessions based on behavioral anomalies or security policy violations.

8 Audit, Logging, and Monitoring

8.1 Comprehensive Audit Trail

Paige maintains an audit trail that captures security-relevant events within the system:

- Authentication events
- Authorization decisions
- Document access and modifications
- Configuration changes
- System alerts and exceptions

These audit records are protected against unauthorized modification and include details for forensic analysis and compliance reporting.

8.2 Security Monitoring

Ademero's security operations include monitoring Paige deployments for potential security incidents:

- Security event monitoring
- Behavioral analytics for anomaly detection
- Correlation of events across data sources
- Alerting for security policy violations

The monitoring infrastructure employs multiple detection capabilities to identify sophisticated attack patterns and emerging vulnerabilities.

8.3 Incident Response

Ademero maintains incident response capabilities with procedures for:

- Incident identification and classification
- Containment strategies
- Evidence preservation
- Root cause analysis
- Recovery processes
- Post-incident review

These procedures are tested through exercises and simulations to ensure effectiveness against various threats.

9 Compliance and Standards Alignment

9.1 Regulatory Frameworks

Paige is designed to support organizations operating under various regulatory requirements:

- Privacy regulations
- Industry-specific frameworks
- Regional data protection requirements

The platform includes capabilities designed to help organizations maintain compliance, including data residency controls, consent management, and data subject access request handling.

9.2 Security Standards Alignment

Paige's security architecture is designed to align with leading security frameworks and standards:

- NIST Cybersecurity Framework considerations
- ISO 27001 security principles
- SOC 2 security concepts
- Cloud Security Alliance guidance

This alignment helps ensure that organizations can deploy Paige within environments with defined security requirements while maintaining their existing security posture.

10 Conclusion

Our technical analysis indicates that Paige represents a security-oriented implementation of document intelligence capabilities. Ademero has made architectural decisions that prioritize data protection, privacy, and security while delivering the platform's advanced functionality.

The security controls implemented throughout Paige's architecture provide defense-in-depth protection against various threats. The platform's security capabilities are designed to meet the requirements of security-conscious organizations, including government agencies and Fortune 500 enterprises.

Based on our analysis, we conclude that Paige represents a strong example of secure document intelligence platforms, demonstrating that advanced AI capabilities can be delivered with a strong focus on security, privacy, and regulatory considerations.

Stratis AI Security Architecture Review Committee