DiligenceVault
Data Security Overview

2025

Layers of Data Security Control

ENHANCED
MONITORING

USER
CONTROLS

APPLICATION
CONTROLS

AZURE
CONTROLS
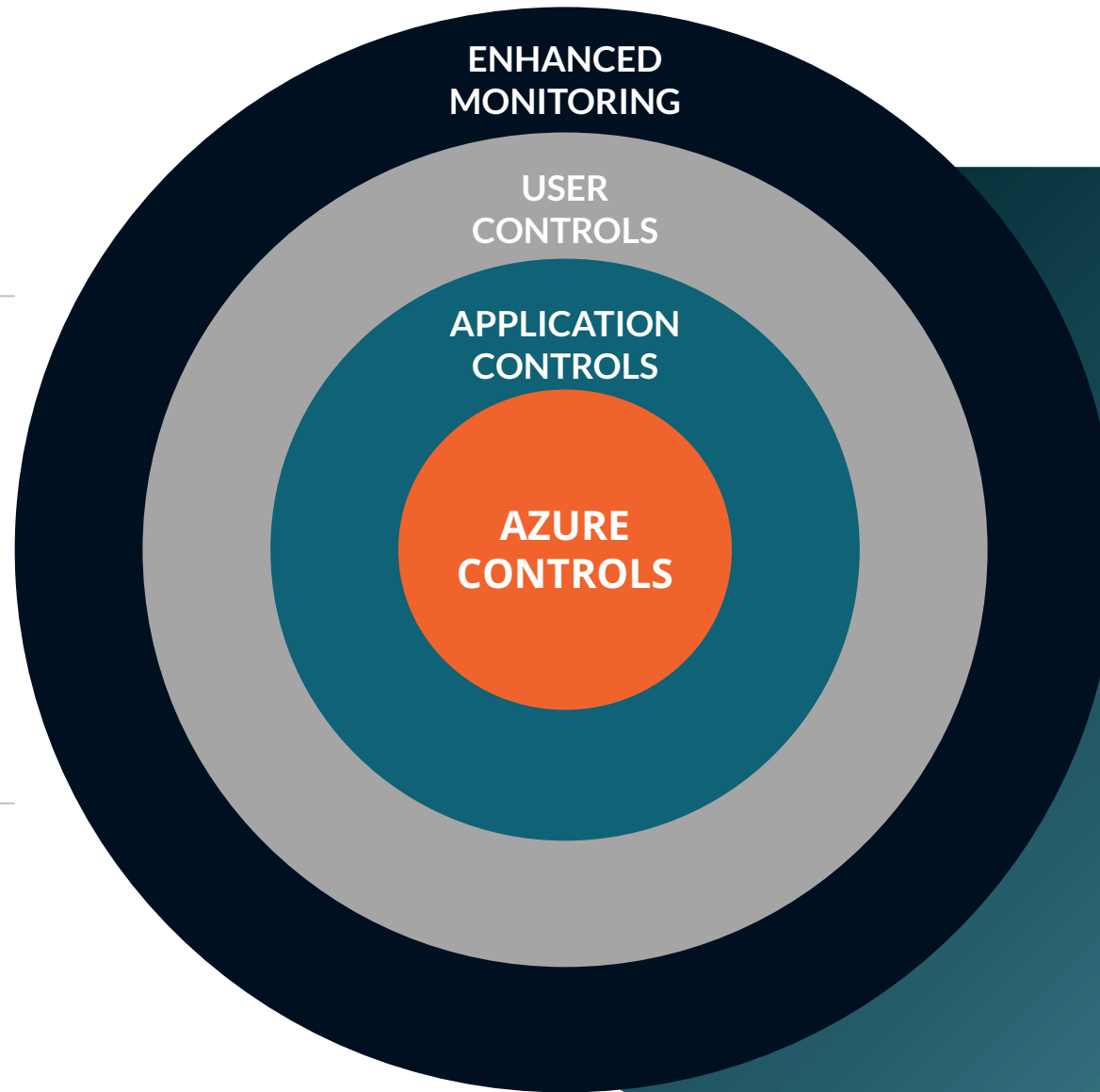
*Architecture leverages industry best practices and is designed with controls at each layer of data access*

Compliance and Data Privacy

ISO Certified for rigorous protection of organizational information assets.

SOC-2 compliance independently validated to ensure strong controls across security, availability, confidentiality, processing integrity, and privacy.

Data Privacy Framework (DPF) certification enabling compliant data transfers between the EU/UK/Switzerland and the U.S., underpinned by robust DPF Principles.

Complete GDPR alignment to uphold privacy rights and transparent data practices.

TX-RAMP authorized to meet Texas state government cloud security standards.
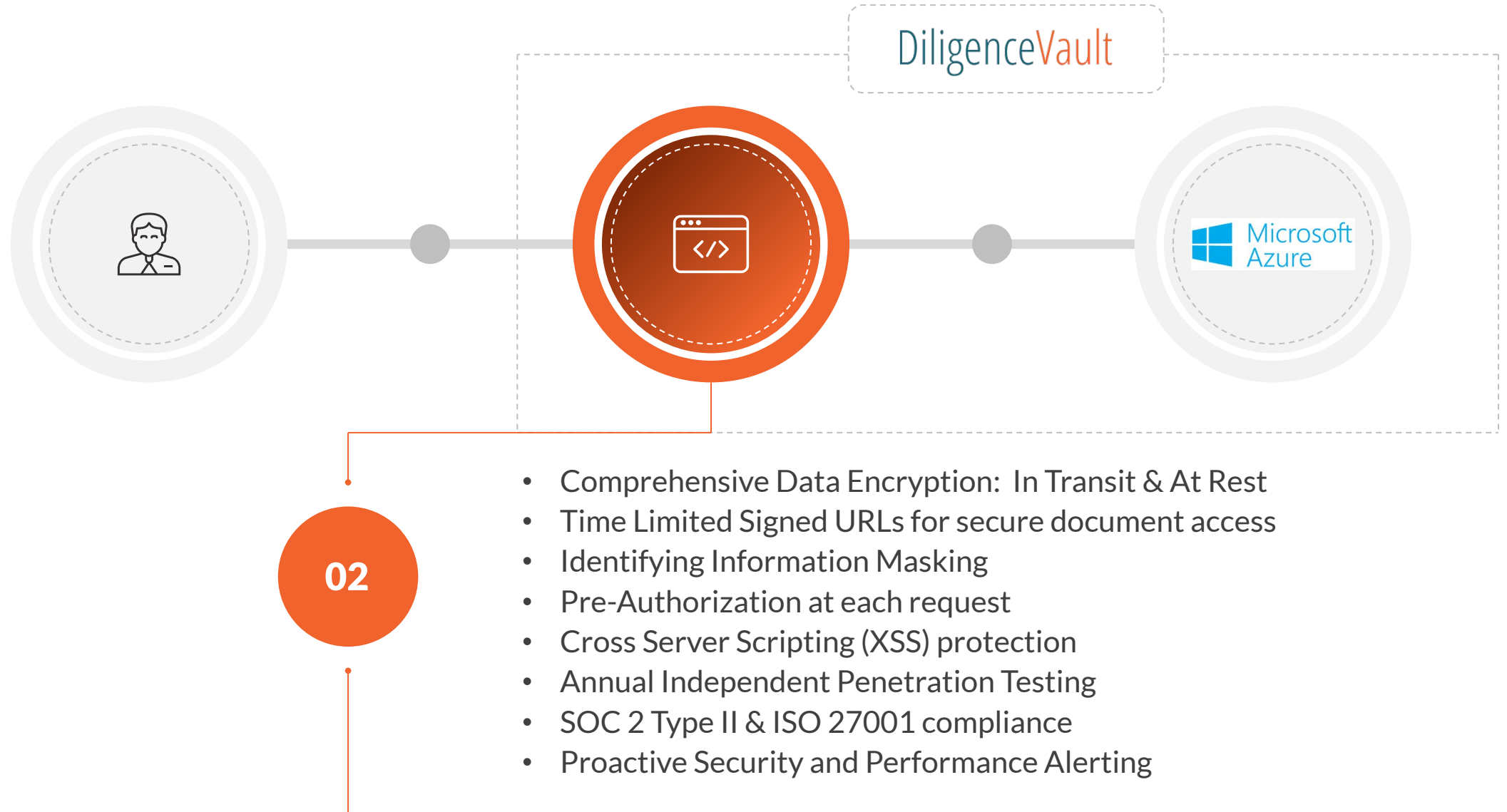
User Access Security & Controls

DiligenceVault

Microsoft Azure
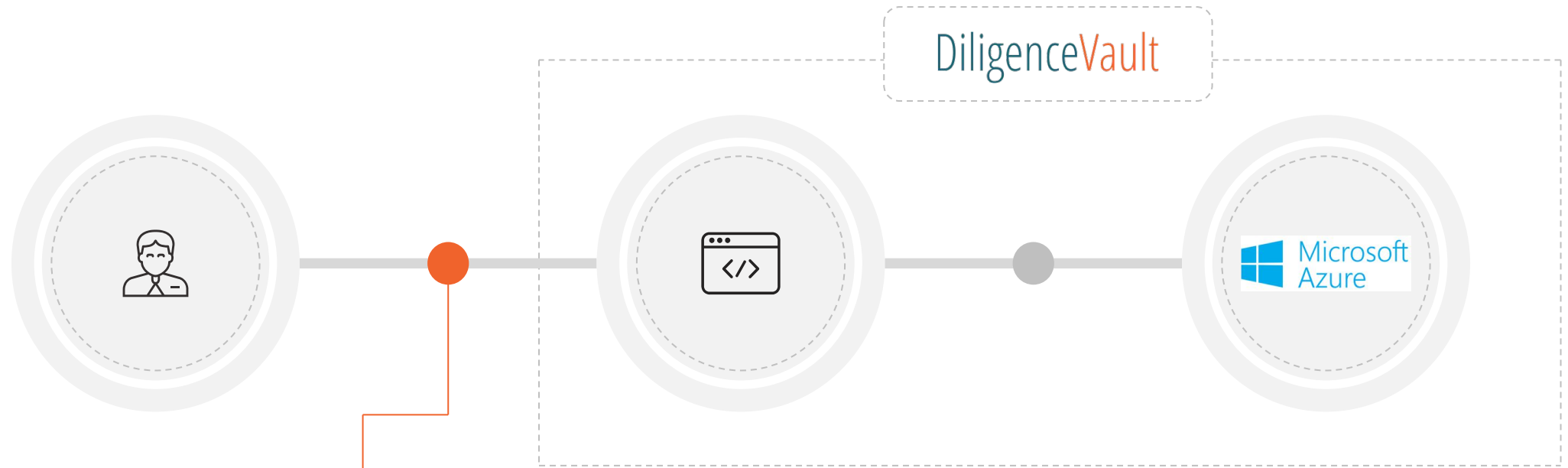
01

- Advanced Identity and Access management with multi-factor authentication
- Domain and IP address whitelisting
- Single Sign On
- Role-based Access controls
- Token-based session management
- Access Protection and Security Notifications
- Proactive Network Monitoring and Audit Trail
- Enhanced Email Security

Product Security & Controls

DiligenceVault

02

- Comprehensive Data Encryption: In Transit & At Rest
- Time Limited Signed URLs for secure document access
- Identifying Information Masking
- Pre-Authorization at each request
- Cross Server Scripting (XSS) protection
- Annual Independent Penetration Testing
- SOC 2 Type II & ISO 27001 compliance
- Proactive Security and Performance Alerting

Microsoft Azure

Data Security & Redundancy

DiligenceVault

Microsoft Azure

03

- Data Encryption
- Data Masking
- IP whitelisting for Secure Access Control
- 35 days Data Retention Policy
- Institutional Controls for Patch Management
- Periodic DR & BCP testing across Infrastructure, Application and Microservices, with respective RPO and RTO for each tier
- Threat Focussed Audit logging & Retention
- Real time Security and Performance Alerting

Infrastructure Security & Redundancy

DiligenceVault

Microsoft Azure

04

- Geo-Replicated Redundancy Across Regions
- Seamless and Efficient Scalability
- Real Time Security and Service Degradation Alerts
- Independent Penetration Testing for Azure IAAS and PAAS
- Azure IAAS & PAAS Security with SOC 1/2/3 & ISO 27001 certification
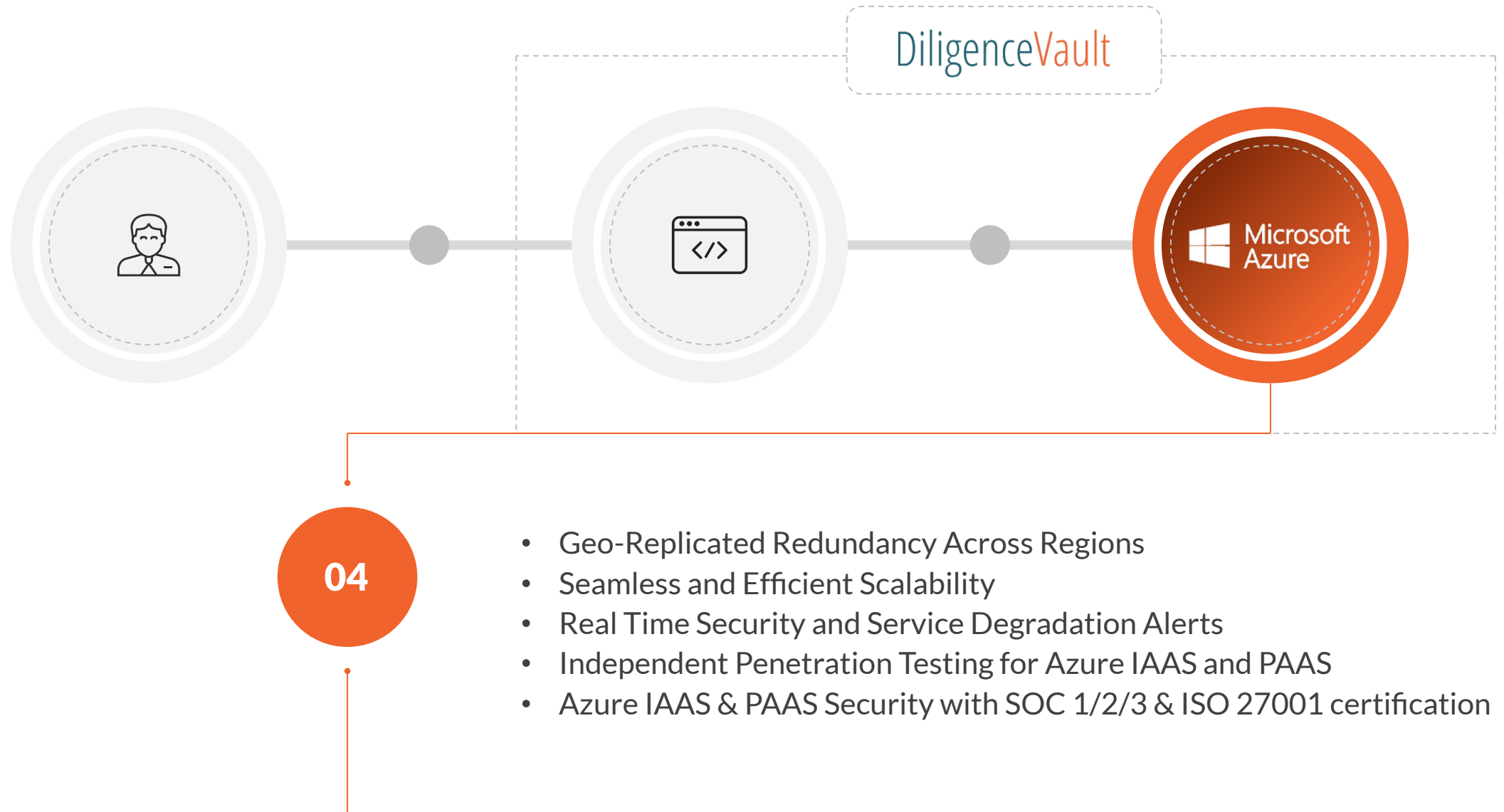
Diligence**Vault**'s Operational Controls

Our commitment and capacity towards providing the best-in-class services for our clients

Application Security Enforcement

Security aspects of the application are reviewed during peer reviews as well as there is periodic sharing of best practices. Application data subprocessor selection goes through security review and list can be found <u>here</u>

Change Management

There is a formal framework for change management to the production infrastructure and software. The process if tightly coupled with different environments to manage the change management process well documented in JIRA.

Training and Awareness

DiligenceVault enforces comprehensive, risk-based security trainings. Our training encompasses standards for confidentiality, privacy, physical and system security, acceptable use, social engineering, and more, ensuring full awareness and compliance.

Incident Management

Real-time alerts detect unauthorized access across both the application and infrastructure. A formal incident-management process ensures swift corrective actions and prompt client notification.

Thank You!

FOLLOW US ON LINKEDIN	https://www.linkedin.com/company/diligencevault
VISIT OUR WEBSITE	www.diligencevault.com
CHECK OUT OUR BLOG	https://diligencevault.com/blogs/

DiligenceVault