PIVOLT

CLOUD INFRASTRUCTURE AND SECURITY TECHNICAL PAPER

2025

Infrastructure – Global Presence

Pivolt is a SaaS platform designed for Investment Management, built on four fundamental pillars: experience, technology, productivity, and excellence. Our systems are hosted in secure, firewall-protected environments, preventing unauthorized access or interference.

Pivolt's physical infrastructure is hosted across **global data centers**, with primary deployments in:

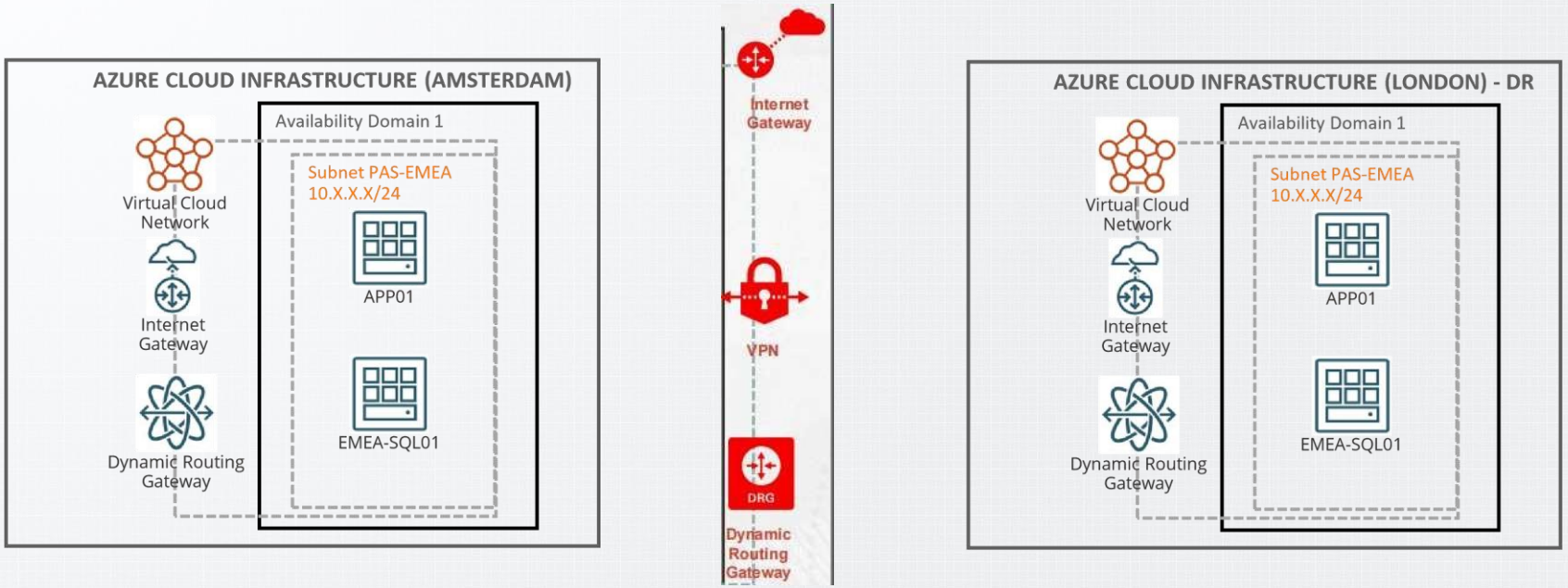
- **Europe** (Netherlands and London)
- **North America**
- **Asia-Pacific**
- **South America**

These data centers follow ITIL guidelines and operate under ISO 27001-certified management systems, ensuring continuous service quality and security. They undergo periodic assessments to maintain compliance with industry safety standards.

The data centers have certifications such as **SSAE16**, **SAS70 Type II**, and **ISO**, meeting international standards, including SOX compliance.

Pivolt also offers an **on-premise deployment option**, where clients can host the Pivolt solution within their own cloud environment or infrastructure. This provides clients with greater control over their data while benefiting from Pivolt's robust security features.

Infrastructure - Europe



Data Privacy and GDPR Compliance

Pivolt is committed to safeguarding personal data and complies with the General Data Protection Regulation (GDPR). Our GDPR compliance framework includes:

1. **Legal Basis and Consent:** Data is collected and processed based on legitimate interests, contractual necessity, or explicit consent.
2. **Data Subject Rights:** We provide mechanisms for users to exercise their rights, including access, rectification, data portability, and deletion requests.
3. **Data Retention Policy:** Personal data is retained only as long as necessary to fulfill contractual obligations and legal requirements, after which it is securely deleted unless otherwise requested.
4. **Sub processors and Data Transfers:** Data transfers between regions follow EU-approved Standard Contractual Clauses (SCCs) to ensure equivalent levels of protection when working with sub processors such as Microsoft Azure.
5. **Incident Response:** In the event of a data breach, Pivolt follows a comprehensive incident response plan that includes timely notifications to affected parties and mitigation measures.
6. **Data Security:** Encryption, access controls, and regular security audits are conducted to ensure the highest levels of data protection.
7. **Transparency and Contact Point:** Our privacy policy outlines how data is processed, and our Data Protection Officer (DPO) is available for any privacy-related inquiries at [contact details].

Infrastructure – Azure

Pivolt leverages Microsoft Azure's global data centers to ensure enterprise-grade security, with:

- Access restrictions and segregated operational responsibilities.
- Detailed logs for auditing and monitoring customer assets.
- Fault-tolerant data centers supporting high availability and resilience against attacks.

Security - Pivolt

1. Authentication:
    - Segregation of roles based on “Chinese Wall” rules to restrict data access.
    - Full audit trails for tracking operations.
    - Configurable session expiration for enhanced security.

2. Password Policy:
    - Encrypted storage of passwords.
    - Customizable password complexity rules.
    - Blocking after multiple incorrect attempts.
    - Password history control to prevent reuse.

Security - Database

- Access to production databases is restricted to limited entry points.
- Production databases use unique credentials, and no master passwords are shared.
- Pivolt employees do not have direct access to production environments, except for system maintenance, monitoring, or backups.

Security - SSL

- SSL certificates encrypt sensitive data (e.g., usernames and passwords), ensuring secure transmission.
- Encrypted data is only decrypted by authorized servers, preventing interception.

Security – Application URL

- Daily vulnerability scans perform over **32,000** tests across **17 categories**, aligned with OWASP Top Ten.
- Critical tests include:
    - SQL injection detection.
    - Cross-site scripting (XSS) prevention.
    - HTTP method checks.

Security – Server IP

- Server scans perform over **11,000 vulnerability tests** on operating systems and applications.
- Scans detect malicious code, identify open ports, and verify firewall protection.

Security – Penetration Testing (Pentest)

- Penetration testing identifies vulnerabilities that automated tools may miss.
- The security team tests for:
    - Allowed HTTP methods.
    - XSS vulnerabilities.
    - SQL injection risks.
    - SSL validation and administration area access.

Backup Policy

- **Database Backups**: Full backups are generated every **24 hours** and stored for at least **6 months**.
- **Incremental Backups**: Performed every **4 hours** to minimize data loss risks.
- **Environment Backups**: Weekly full environment backups, stored for **6 months**.

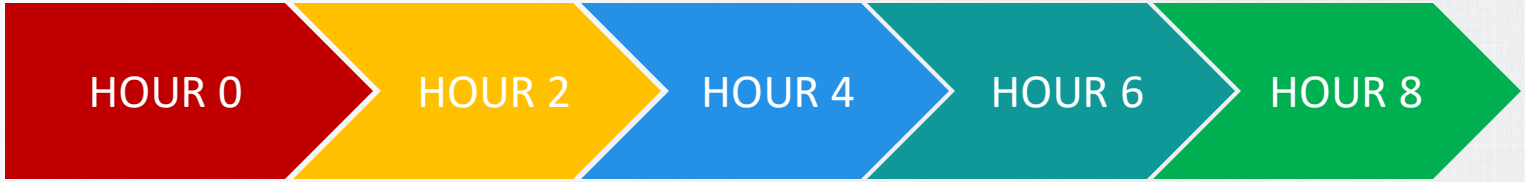
Storage locations

Backups are stored in secure Azure and Google Cloud data centers across key global regions, ensuring data redundancy and compliance with regional regulatory requirements. Clients may also request specific regions for backup storage, based on operational needs.

Disaster recovery

Pivolt's disaster recovery sites are provisioned in key regions, with default Recovery Time Objectives (RTO) of 8 hours and Recovery Point Objectives (RPO) of 4 hours. Clients can request alternative locations or lower recovery objectives to meet specific operational and regulatory requirements..

Recovery timeline:



Disaster Occurs
The disaster occurs and your primary server becomes unavailable.

Notification and Assessment
Monitoring system detects the issue and sends a notification to IT team.
IT team begins assessing the situation and determines that the primary server is not recoverable.

Failover and Restoration
IT team initiates failover procedures.
Clients receive notification that DR status is effective.
Provisioned VMs are started, and backup are copied.

Data Restoration
Once VMs are verified, backup restoration is initiated, and validation tests are deployed.

Services Restored
Restoration is finished and application access is enabled.
Clients are notified that DR environment is available.

Azure compliance

Global

- CIS benchmark
- CSA STAR Attestation
- CSA STAR Certification
- CSA STAR self-assessment
- SOC 1
- SOC 2
- SOC 3

Global

- ISO 20000-1
- ISO 22301
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 27701
- ISO 9001
- WCAG

US government

- CJIS
- CMMC
- CNSSI 1253
- DFARS
- DoD IL2
- DoD IL4
- DoD IL5
- DoD IL6
- DoE 10 CFR Part 810
- EAR
- FedRAMP
- FIPS 140

US government

- ICD 503
- IRS 1075
- ITAR
- JSIG
- NDAA
- NIST 800-161
- NIST 800-171
- NIST 800-53
- NIST 800-63
- NIST CSF
- Section 508 VPATs
- StateRAMP

Financial services

- 23 NYCRR Part 500 (US)
- AFM and DNB (Netherlands)
- AMF and ACPR (France)
- APRA (Australia)
- CFTC 1.31 (US)
- EBA (EU)
- FCA and PRA (UK)
- FFIEC (US)
- FINMA (Switzerland)

Financial services

- FINRA 4511 (US)
- FISC (Japan)
- FSA (Denmark)
- GLBA (US)
- KNF (Poland)
- MAS and ABS (Singapore)
- NBB and FSMA (Belgium)
- OSFI (Canada)

Financial services

- OSPAR (Singapore)
- PCI 3DS
- PCI DSS
- RBI and IRDAI (India)
- SEC 17a-4 (US)
- SEC Regulation SCI (US)
- SOX (US)
- TruSight

Healthcare and life sciences

- ASIP HDS (France)
- EPCS (US)
- GxP (FDA 21 CFR Part 11)
- HIPAA (US)
- HITRUST
- MARS-E (US)
- NEN 7510 (Netherlands)

Azure compliance

Automotive, education, energy, media, and telecommunication

- CDSA
- DPP (UK)
- FACT (UK)
- FERPA (US)
- MPA
- GSMA
- NERC (US)
- TISAX

Regional - Americas

- Argentina PDPA
- Canada privacy laws
- Canada Protected B
- US CCPA

Regional - Asia Pacific

- Australia IRAP
- China GB 18030
- China DJCP (MLPS)
- China TCS
- India MeitY
- Japan CS Gold Mark
- Japan ISMAP
- Japan My Number Act
- Korea K-ISMS
- New Zealand ISPC
- Singapore MTCS

Regional - EMEA

- EU Cloud CoC
- EU EN 301 549
- ENISA IAF
- EU GDPR
- EU Model Clauses
- Germany C5
- Germany IT-Grundschutz workbook
- Netherlands BIR 2012
- Qatar NIA

Regional - EMEA

- Russia personal data law
- Spain ENS High
- Spain LOPD
- UAE DESC
- UK Cyber Essentials Plus
- UK G-Cloud
- UK PASF

https://learn.microsoft.com/en-us/azure/compliance/