Pivolt Global

FINANCIAL INTELLIGENCE

CLOUD INFRASTRUCTURE AND SECURITY TECHNICAL PAPER

2023

Infrastructure - Europe

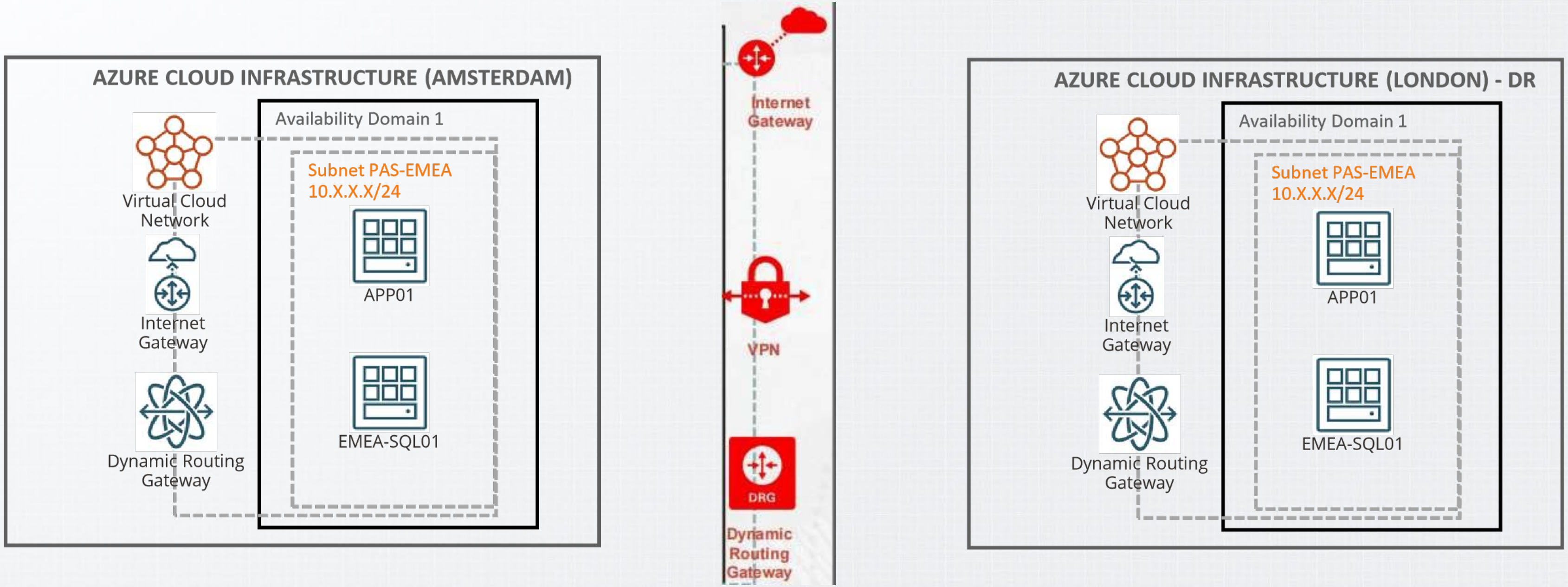
A SaaS company focused on Investment Management. It operates on 4 fundamental pillars in the delivery of solutions for investment management: experience, technology, productivity and excellence.

Pivolt Platform Systems offered in SaaS mode are hosted in a secure environment that uses a firewall and other technologies to prevent interference or intruder access.

The entire physical infrastructure is hosted in data centers located in Netherlands. The data center follows the ITIL guidelines and has its quality assured by an ISO 9001:27001 certified management system, continuously valuing the safety and quality of its services. It undergoes periodic assessments to ensure compliance with industry safety standards.

The data centers where our SaaS Solution is hosted have certifications (SSAE16, SAS70 type II, ISO) that meet international standards including SOX.

Infrastructure - Europe



Infrastructure – Azure Europe

Effective security management to restrict access and segregate operational responsibilities. Logs and security analytics that allow auditing and monitoring of customer assets.

Fault-tolerant data centers that enable high-availability, attack-resilient scale-out architectures. Transparent internal security processes and controls in a third-party audited and certified framework.

Resilience and Performance: 100% SSD Storage, Optimized VM sizing according to Mission Critical Application Workload.

Observability: Monitoring, Logging, Notifications, Events, Alarms. Service security, access controls, monitoring and audits, DDoS, WAF.

Security - Pivolt

AUTHENTICATION

Chinese wall rules for accessing system data and modules
Audit trail recording all operations
Configurable session expiration time

PASSWORD POLICY

Passwords stored in encrypted form
Possibility of setting the minimum size, presence of special characters, etc.
Setting the number of incorrect attempts before login is blocked
Password history control preventing its reuse

SECURITY IN SOFTWARE AS A SERVICE

No sensitive data traveling as URL parameters
Encrypted Connection via SSL
Running daily website vulnerability tests

Security - Database

Access to production bases is restricted to a limited number of points and production bases do not share a master password.

Pivolt employees do not have direct access to the production environment, except when necessary for system maintenance, monitoring and backups.

Data backups are performed daily, according to previously defined policies.

Security - SSL

SSL Digital Certificate

Encrypted electronic file containing the public key.

The information entered in forms (such as usernames and passwords) is encrypted before being sent via the internet and is only decrypted by the server that hosts the website.

If the information is “intercepted” along the way by hackers, it cannot be deciphered.

Security – Application URL

Daily Vulnerability Scan.

More than 32,000 tests are carried out divided into 17 categories in which most of these categories are aligned with the OWASPTOPTEN.

The other scanners:
At least once a week, tests that we consider the most critical are:

1. SQL Disclosure
2. SQL Error Message
3. Blind SQL Injection
4. Cross Site Scripting
5. Check http Method

Security – Server IP

Server Scan (IP)

More than 11,000+ vulnerability tests are performed on hundreds of applications and operating systems. We maintain a comprehensive Vulnerability Knowledgebase. Almost daily, new subscriptions are added to this database.

Each scan starts with a pre-scan module which are fingerprints. The fingerprint is done by sending a series of packages specially created for the reception and interpretation of the results.

This scan is capable of identifying the machine's operating system, running services and open ports (0-65535). Once this information has been captured, the scanning engine selects only the appropriate vulnerabilities and interprets the results.

In addition to testing network services, they are able to check for any type of malicious code using your server, SNMP, existing firewall identification on the Server, denial of service (Dos) vulnerability, remote database vulnerabilities, among others. tests.

Security – PenTest

Penetration Test (Pentest)

It identifies basic vulnerabilities that are not analyzed by automated tools, given their particular characteristics. Through the tests developed by Pivolt's security team, the adherence of the web application to seven specific points that often have their protection neglected are scored and can be exploited to identify failures and carry out attacks. Are they:

1. Allowed HTTP methods - Checks which methods are active on the Server (TRACE, PUT, DELETE, COPY);
2. Cross Site Scripting – Complementary tests to automated tests are performed;
3. Blind SQL Injection – Complementary tests are performed to the automated ones;
4. SQL Error – Complementary tests are performed to the automated ones;
5. SSL– Checks if even installed the certificate is able to enter without HTTPS;
6. Administration area – Checks if the client's administration area is easily located;
7. Discovered Directories - Checks if there are application directories that are copyable.

Backup Policy

Database
Full backups are generated every 24 hours and kept for at least 6 months. Incremental backups are generated every 4 hours.

Environment
Even considering that all relevant data are restricted to each client database, a Full environment backup is generated weekly and kept for at least 6 months.

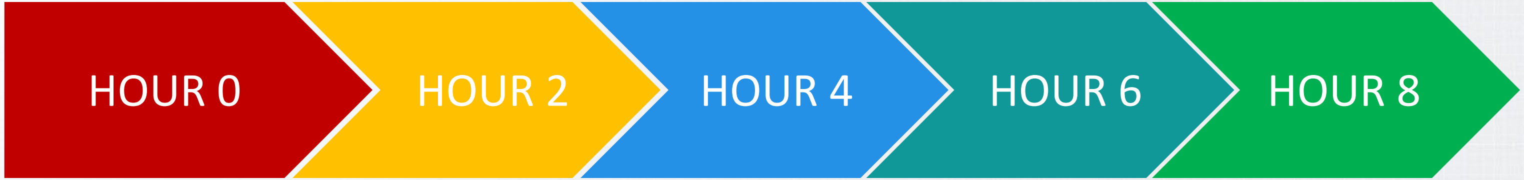
Storage locations
Backup are stored across Azure´s Netherland and London locations.
All backups are mirrored to Google Cloud storage with location restricted to Europe datacenters (Ireland, Netherlands, Denmark, Finland and Belgium)

Disaster recovery

Europe disaster recovery site are provisioned in London location.

Default RTO is defined to 8 hours and RPO to 4 hours, lower objectives can be arranged upon client request.

Recovery timeline:



HOUR 0

Disaster Occurs

The disaster occurs and your primary server becomes unavailable.

HOUR 2

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.

HOUR 4

Failover and Restoration

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

HOUR 6

Data Restoration

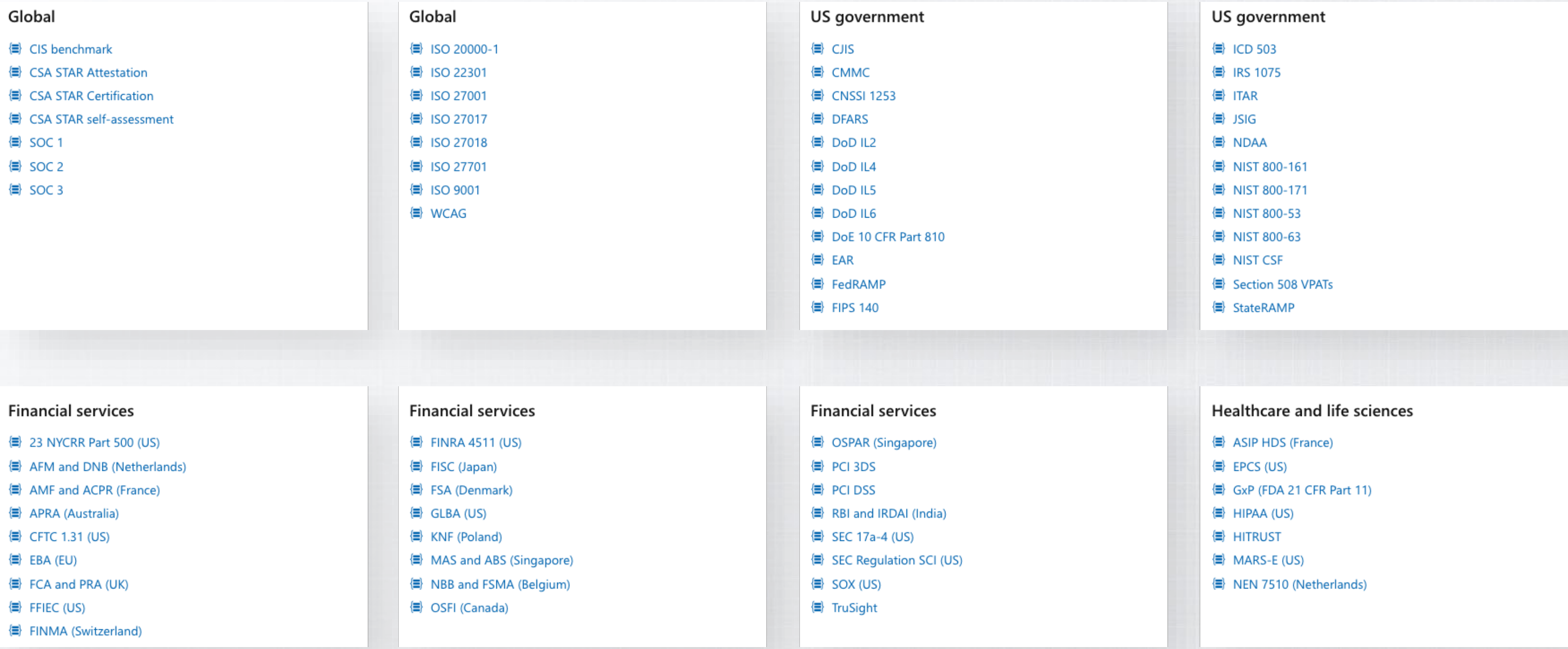
Once VMs are verified, backup restoration is initiated and validation tests are deployed.

HOUR 8

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)

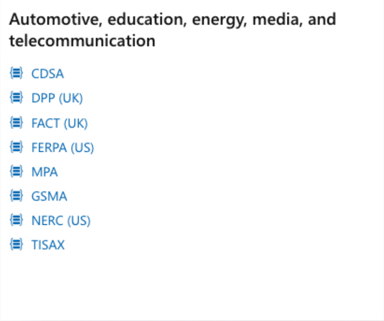
Financial services

- 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

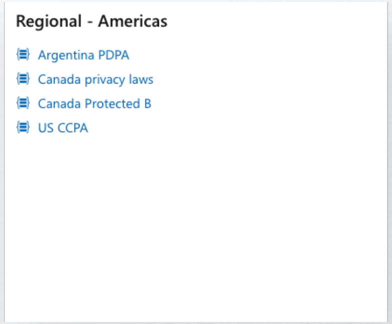
- ASIP HDS (France)
- EPCS (US)
- GxP (FDA 21 CFR Part 11)
- HIPAA (US)
- HITRUST
- MARS-E (US)
- NEN 7510 (Netherlands)

Azure compliance



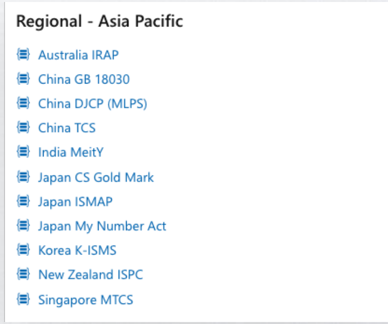
Automotive, education, energy, media, and telecommunication

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



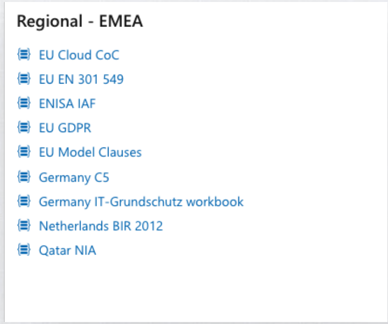
Regional - Americas

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



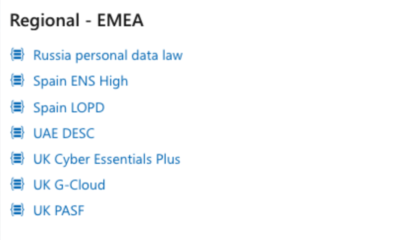
Regional - Asia Pacific

- 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/