Wisenet Product Fact Sheet

Important details about Wisenet Architecture, Security & Business Continuity

Last Updated January 2024

Wisenet is an modern, cloud-native architected application. Beyond the use of primitive cloud infrastructure such as compute and storage, Wisenet exploits many advanced Amazon Web Services to deliver a truly distributed, scalable and secure application stack.

Personnel

It is a requirement that all Wisenet personnel and contractors are subject to the Wisenet Information Security Policy which is formulated and enforced as part of ISO 27001:2022 certification (The international standard for information security).

Infrastructure-as-Code

The vast majority of Wisenet virtual infrastructure is deployed as code. This enables granular deployment of specific infrastructure components, reducing the risk of conflicts or introduction of security vulnerabilities. Changes to infrastructure are managed under source code control enabling rollbacks, and automated provisioning just in time as part of continuous delivery.

Resources are mostly stateless and disposable with most compute resources fully replaced with a new fully patched, up-to-date image of the OS, on every deployment.

Separate Virtual Private Clouds (VPC)

Development, Staging and Production run in their own separate VPC with their own IAM roles. Developer access to production VPC is highly restricted with almost all functions performed through Cloud Formation code.

Zoning and Network Segmentation impose security controls within and between VPCs, and access to various resources and logs.

With elastic cloud infrastructure and automated deployment, Wisenet can apply the same security controls across all AWS regions. Repeatable and uniform deployments improve the overall security posture.

Automated Multi-Data-Centre Design

Wisenet is designed to operate in active-passive multi-datacenter configuration. Data is replicated between Availability Zones near real time. Infrastructure can be quickly deployed to any AWS data centre by running the appropriate Cloud Formation scripts that reside in the Source Code Repository.

Serverless Architecture

Serverless architectures can reduce the operational complexity of running applications. It is possible to build both event-driven and synchronous services for mobile, web, analytics, CDN business logic, and IoT without managing any server infrastructure.

Wisenet serverless architecture reduces the complexity involved in redundant systems.

IAM Roles

Each service runs under its own IAM Role to run at least privilege level and to prevent lateral access to other services.

Stateless Applications

When users or services interact with a Wisenet application they will often perform a series of interactions that form a session. A session is unique data for users that persists between requests while they use the application. A stateless application is an application that does not need knowledge of previous interactions and does not store session information.

For example, an application that, given the same input, provides the same response to any end user,

is a stateless application. Stateless applications can scale horizontally because any of the available compute resources (such as EC2 instances and AWS Lambda functions) can service any request. Without stored session data, Wisenet can simply add more compute resources as needed. When that capacity is no longer required, Wisenet can safely terminate those individual resources, after running tasks have been drained. Those resources do not need to be aware of the presence of their peers.

Distribute Load to Multiple Nodes

Wisenet implements distributed asynchronous event-driven architecture where tasks that need to be performed or data that needs to be processed can be stored as messages in a queue using Amazon Simple Queue Service (Amazon SQS) and as Amazon Kinesis.

Multiple compute resources can then pull and consume those messages, processing them in a distributed fashion.

Containerisation

Wisenet deploys Docker Containers - an open-source technology that allows you to build and deploy distributed applications inside software containers. Docker allows us to package a piece of software in a Docker image, which is a standardized unit for software development, containing everything the software needs to run: code, runtime, system tools, system libraries, etc.

2-Factor Authentication

All AWS resources are protected by 2-Factor authentication.

Alarms & Events

Wisenet makes extensive use of AWS Cloudwatch to provide self healing instructure, and critical alerts to our team. Automated monitoring is conducted via the Prometheus toolset.

3rd Party Monitoring

In addition to our own internal monitoring, we engage third party vendors to conduct monitoring of public facing systems.

Best Practice Bench

Wisenet engages Base2 Services in ongoing arrangement which provides additional expertise in AWS architecture. This provides our team with on-demand expertise in any AWS Service to ensure that we choose the best service for the task at hand, and that the design approach meets AWS best practice guidelines.

Data Encryption at Rest and in Transit

Amazon EBS and S3 encryption offers seamless encryption of EBS data volumes, boot volumes and snapshots, and S3 buckets, eliminating the need to build and manage a secure key management infrastructure. EBS encryption enables data at rest security by encrypting data volumes, boot volumes and snapshots using keys created with the AWS Key Management Service (KMS). In addition, the encryption occurs on the servers that host EC2 instances, providing encryption of data as it moves between EC2 instances and EBS data and boot volumes.

Wisenet APIs expose HTTPS endpoints only. Wisenet doesn't support unencrypted (HTTP) endpoints. The minimum Transport Layer Security (TLS) protocol version to be enforced for APIs is TLS version 1.2.

Data Retention Policy

Once a subscription is terminated by you or us, it is archived and the data submitted or created by you is no longer available to you. We retain it for a period of time consistent with our data retention policy, during which, as a subscriber, you can reactivate your subscription and once again access your data by paying the subscription fees. We retain data in case you need it as part of your record retention obligations, but you can get in touch with us to have your data removed completely if you wish.

Business Continuity

Wisenet is a Division of Adapt IT with offices globally. Wisenet teams are by design distributed geographically. Our technology platforms are built for resilience. Unlike a traditional Disaster Recovery model, where there is a backup office and facilities that are used only in the event of an emergency, Wisenet's normal mode of operation is distributed.

Wisenet is not dependent on any single geographic location (ie: office, data centre), network vendor (ie: connectivity), power supply, or telephony operator. We are very agile in our ability to work in an office or remotely, as this has been our standard operating procedure for more than two decades.

We maintain continuous commercial arrangements with third party vendors (eg: Dell, Base2, Vocus) to ensure that we have on demand access to a bench of expertise, reducing key person risk.

The Covid-19 Pandemic has been a true test of our preparedness for a disaster.

Since the beginning of the pandemic, Wisenet customers and staff have not experienced any adverse impact as a result of the lockdown measures imposed in various parts of Australia or globally. Even during the four month lockdown in Melbourne, the location of Wisenet's Australia office, our team continued to operate at normal levels without incident.

Security

Wisenet designs with security and durability of data as the highest priority in accordance with AWS Security Best Practices.

Wisenet's parent company, Adapt IT, has engaged leading third party security vendors in a full range of company wide cyber-security projects:

→ Payment Card Industry Compliance Consultancy
→ Payment Card Industry Forensic Investigations
→ Penetration Testing
→ Mobile Application Testing
→ Managed Security Services
→ Security Training
→ Threat Detection
→ Incident Response
→ DLM

About Wisenet

Established in 1997, Wisenet is the market leader in Cloud applications for the vocational training sector in the APEC region.

With over 4 million learners under management and Wisenet's integrated Cloud platform is designed to help training organisations manage risk and reputation, reduce business costs and grow revenues.

Wisenet was acquired by Adapt IT (JSE:ADI) in 2019 and has offices in Australia, Singapore, New Zealand and South Africa.

For more information, visit www.wisenet.co

About Adapt IT

Adapt IT is a South African company and a member of Volaris Group Inc. – a subsidiary of Constellation Software Inc. (CSI) a listed company on the Toronto Stock Exchange.

Adapt IT is a Level 1 Broad-Based Black Economic Empowerment (B-BBEE) contributor that provides leading specialised software and digitally-led business solutions that assist clients across targeted industries to Achieve more by improving their customer experience, core business operations, business administration, enterprise resource planning and public service delivery.

The organisation has deep sector knowledge and experience predominantly in the education, manufacturing, financial services, energy, technology expense management (multi-industries), telecommunications, consumer security and services, and hospitality industries including public sector.

Adapt IT serves over 10 000 global customers, with headquarters in Johannesburg, South Africa, and regional offices in Durban and Cape Town. To service international customers, Adapt IT focuses on the Pan African market, through a presence in Mauritius, Botswana, Kenya and Nigeria, as well as on the Asia Pacific market, where the group has a presence in Australia, New Zealand and Singapore. Through its presence in Ireland, Adapt IT is able to service customers in Europe.

For more information, visit www.adaptit.co