HawkSight Software V3

Security White Paper

Introduction

HawkSight Software is a security risk assessment tool that delivers a single solution to strategic, operational and tactical risk assessment and tailored security planning. Customisable and scalable it is setting the benchmark for software in the sector.

Our security risk analysis software calculates risk based on ISO 31000 Risk Management Guidelines and the associated Australian New Zealand Standards, Security Risk Management Handbook 167 Guidelines. It does so in a fraction of the time it normally takes.

HawkSight Software is a unique security risk assessment tool, that is enabling our clients to save time and money by enabling the quantification of risk appetite in business terms, including financial exposure, and to best deploy resources to proactively and reactively mitigate risk.

The powerful reporting tools included in our risk assessment software bridge the gap between operational security personnel and business leaders, by translating the traditional language of security into that of enterprise risk.

Cloud-based access

The HawkSight Application is available as a Cloud-based SAAS (Software as a Service) product, which can be accessed by users from a wide variety of devices.

This Application has been using a microservices-based design methodology which can respond to elastic, on-demand usage, and can process and analyze millions of records in sub-seconds.

This is possible by using modern technologies like containers, and cloud-based servers, along with Managed Database as a Service. The application has been deployed on Amazon's AWS, which allows us to serve clients across the globe and enable us to expand as and when required on user-specific requirements.

The application has been developed using open standards, which allow us to connect to and use data from various GIS Services, such a MapBox, as well as ArcGIS Online Services. This allows us to serve users who have existing ArcGIS Online Accounts, as well as non-ArcGIS Users.

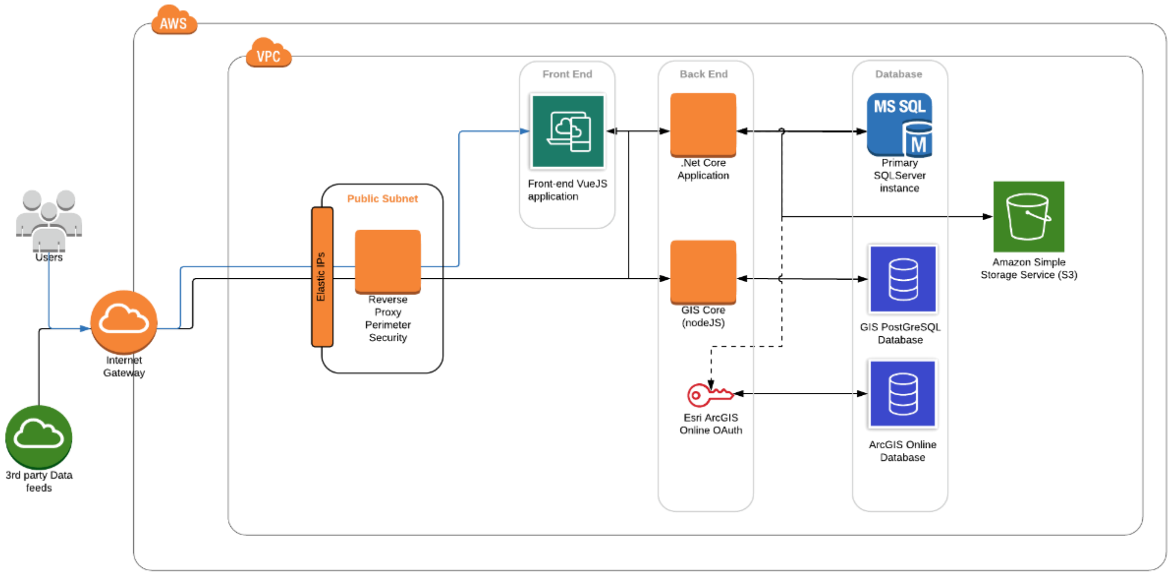

Figure 1: A simplified Architecture Diagram

On-Premise Deployment

There are many considerations to make when preparing to deploy HawkSight On-Premise. A successful and efficient HawkSight deployment has an architecture that has been designed with considerations for:

- The capabilities your organisation requires.
- How you anticipate your organisation will utilize HawkSight.
- The number and type of users you expect for your deployment.
- Clear expectations around service-level agreement (SLA) requirements.

A typical HawkSight deployment involves setting up the following components:

- The HawkSight Core
- The GIS Core
- 3rd Party data feeds

For the application to make use of the 3rd party feeds, the relevant access must be granted so that the app can access the internet to fetch the data.

Security

The Application has been developed using current best practices when it comes to security. This can be broken down into the following main categories:

Built Using Secure Design Principles

HawkSight's security strategy is based on an industry-standard, defence-in-depth approach that provides security controls at every level, for every user, including the application, network, and facilities. Adherence to these security principles helps ensure that HawkSight can provide confidentiality, integrity, and availability of data.

Platform Security

Whether deployed on the Cloud or On-Premise, HawkSight's core application uses the user level authentication to various resources that are used by the application to ensure that data level security is not breached, and only the application has access to the data.

Data Security

While HawkSight provides data to enable you to perform a security assessment, based on worldwide data sources, the data and the reports that you generate belong to you.

- Ownership-Customers retain intellectual property rights for data they publish on HawkSight.
- Multitenancy-Each data record within multitenant storage is stamped with the ID of the owning subscription to ensure organisation data is accessible only by the organisation's users. User's data cannot move across the organisation, which enable data security.
- Reliability-We have a robust backup policy, which creates regular backups, which gives us resilience and enables us to come back from unforeseen disasters.
- Security at Rest and Transfer-The application has been designed with these techniques in place, to protect your data, wherever it is.

Encrypted Communication

User identity is established through a login process that always takes place over HTTPS to ensure industry-standard encryption of sensitive information.

All subsequent requests and data storage also happens over HTTPS which prevents any other third-party from eavesdropping on this communication.

Add-Ons

AD integration

The standard application uses either ArcGIS Online based Logins or Application Logins. It is possible to integrate this Application with your own Microsoft AD account. This would require an API with either your on-premise AD controller or Microsoft's 365 based AD Service.

Single Sign-on & TFA

The application can also be configured to have User Authentication and Authorization based on your specific Single Sign-on provider. In case your provider supports Two-Factor Authentication, this too can be smoothly integrated into the Application's user flow.