1. Security and Data Privacy Overview – Hazman II

1.1 OVERVIEW

- Marico has now implemented a full Microsoft Azure managed platform for Hazman II delivery in the UK.
- It is on a Microsoft Server 2019 operating system.
- This incudes a SQL database with security and update managed directly by Microsoft.
- It includes continuous backup to secure servers also managed by the Microsoft system.
- Security monitoring is in place by with Microsoft Security Centre on Azure.
- There is implemented new sensitivity classifications in SQL Server to help with data compliance. These link to the GDPR requirements for data class.
- There is an Azure server based in the UK jurisdiction and a server based in NZ.

1.2 NZ SECURITY

There is no AZURE service in New Zealand. However, Microsoft have announced, in 2021, an NZ based Azure service and once this is established, the Hazman II platform will look to move over to full AZURE compliance in NZ. The NZ service operates on a server managed by Developer's EndGame, which ensures users data remains in the NZ jurisdiction and can thus be kept private to New Zealand privacy laws. The NZ server has exactly the same database structure as in the UK, but cannot be claimed to be GRDP compliant as there is no GRDP standard in NZ. However, Section 2.2, 2.2.1 and 3.0 (Data ownership policy) do apply to the NZ delivery server.

1.3 SECURITY COMPLIANCE BENEFITS - AZURE

Compliance

Hazman IIs use of Azure provides access to Microsoft's compliance program, which is well promulgated and understood by IT departments in a port of any size. Microsoft enterprise cloud services are independently validated through certifications and attestations, as well as third-party audits. In-scope services within the Microsoft Cloud meet key international and industry-specific compliance standards, such as:-

- ISO/IEC 27001;
- ISO/IEC 27018;
- FedRAMP;
- SOC 1;
- SOC 2.

Microsoft Azure also meets regional and country-specific standards and contractual commitments, including:-

- EU Model Clauses;
- UK G-Cloud;
- Singapore MTCS;
- Australia CCSL (IRAP).

Microsoft have stated they comply with the EU-US *Privacy Shield Framework* as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States. Microsoft has certified to the

Department of Commerce that it adheres to the Privacy Shield Principles. Marico have taken an Azure solution for the UK which retains data in the UK. The NZ and UK servers used to exchange data for backup, before the Azure solution was implemented, but no longer do so.

2. Detail

Hazman II is now delivered from a Microsoft Azure platform in the UK, and to any client whose site is delivered via the UK server. Marico administer the system, own the IPR for the software and retain responsibility for its design and the security of its delivery. The Hazman II application and infrastructure is presently supported under contract by EndGame in New Zealand. This includes Azure administration.

Hazman is an ASP.NET application which stores data in SQL Server and on a local filesystem. There are two delivery servers, one in the UK jurisdiction and one in the New Zealand Jurisdiction. In each case the data is stored adjacent to the application, which is more secure than a remote database location.

Within Azure, there are tools specifically to help in GDPR and data security.

- Search tools to easily find and link to any customer data that may be covered by security requirements subject to GDPR. Once potentially responsive documents are stored, you can perform one or more of the DSR actions to respond to the request.
- Personal data that resides in the Microsoft cloud (i.e. Azure) can be linked to ensure permanent deletion if requested. Equally a secure copy can be made available to the data user of that personal data.
- Using the Azure solution allows:-
    - Changes or implementation of requested actions on personal data to be guaranteed to occur;
    - Restrictions on the processing of personal data, either by removing licenses for various Azure services or turning off the desired services where possible;
    - Personal data can also be removed from the Microsoft cloud and retained at another location (physical);
    - Permanent deletion of personal data that resides in the Microsoft cloud;
    - Easy provision of an electronic copy (in a machine-readable format) of personal data or personal information to the data owner.

The UK Azure solution is hosted in the UK West region.

The systems use a common architecture, Figure 1:-

2.1 NETWORK ARCHITECTURE

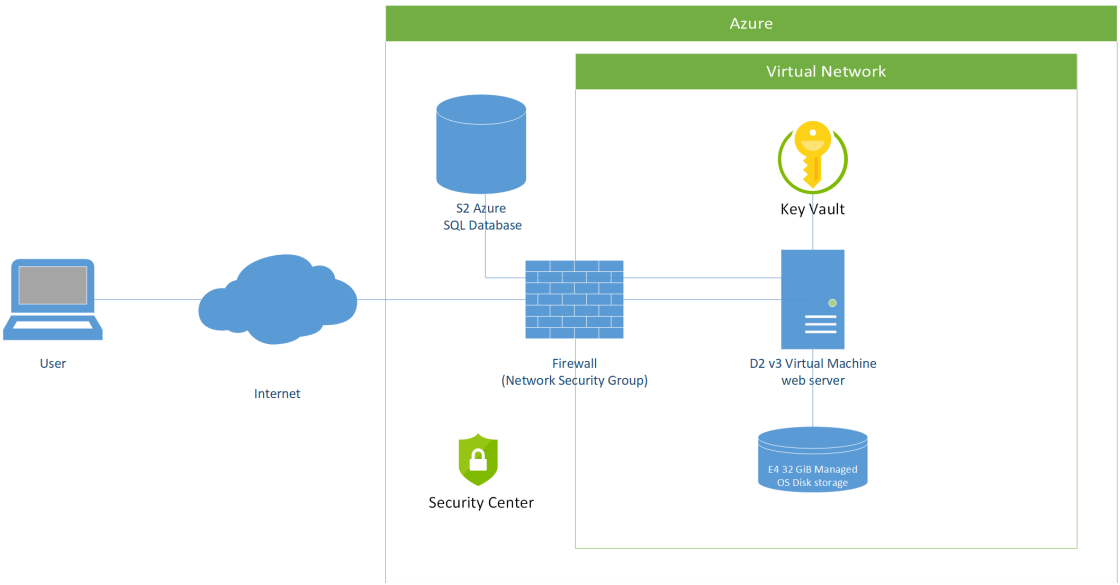

Figure 1 : Hazman II System Azure Network Architecture

2.2 KEY SECURITY FEATURES OF SYSTEM DESIGN IN AZURE

Hazman is hosted in Azure in its own virtual network. The virtual machine is running IIS on Windows Server 2019. All web traffic is encrypted using SSL. The shared Azure SQL Database is logically in the same virtual network. Its firewall is configured to only accept connections from within the virtual network and nowhere else. Data is encrypted at rest and in transit.

Direct access to the SQL Server from outside the virtual network is not permitted. Authorised users must first connect to the virtual machine. Access to the virtual machine is locked down by Marico requirement, to EndGame's jumpbox, which itself is only accessible by authorised EndGame staff via VPN.

A firewall is in place, based on the network security group feature of the Azure system networking. The storage directory on the local filesystem is backed up within the Azure domain, using Azure Recovery Services. The keys are managed using the Key Vault system.

The Azure Security Centre regularly monitors the infrastructure and suggests improvements that can be made. These automated suggestions are reviewed by EndGame's operations team and this is reported to Marico Marine who take the decision to implement if recommended by End Game.

2.2.1 AZURE WINDOWS DEFENDER CREDENTIAL

The system uses the Azure Windows Defender Credential Guard, deploying virtualization-based security to isolate credential information, preventing password hashes or Kerberos tickets from being intercepted. It uses an isolated Local Security Authority (LSA) process, which is not accessible to the rest of the operating system. All binaries used by the isolated LSA are signed with certificates that are validated before launching them in the protected environment, making Pass-the-Hash type attacks completely ineffective.

Windows Defender Credential Guard uses:

- Virtualization-based security (required), running on a:
  - 64-bit CPU Server;
  - CPU virtualization extensions, plus extended page tables;
  - Windows hypervisor.
- Secure boot (required);
- TPM 2.0 either discrete or firmware (preferred - provides binding to hardware)

2.2.2 CONTROL FLOW GUARD

Windows Server 2019 has a built-in protection (always on) against some classes of memory corruption attacks. Patching servers is important, but there is always a chance that malware could be developed for a vulnerability that has not yet been identified. Some of the most common methods for exploiting these vulnerabilities are to provide unusual or extreme data to a running program. For example, an attacker can exploit a buffer overflow vulnerability by providing more input to a program than expected and overrun the area reserved by the program to hold a response. This can corrupt adjacent memory that might hold a function pointer. This built in functionality is why Marico selected the MS server 2019 operating system, on the Microsoft Azure platform.

2.3 APPLICATION USER SECURITY

Hazman is multi-tenanted. Users are authenticated via username and password. Passwords are hashed using bcrypt. One user account is able to be assigned to multiple organisations. Within an organisation, role-based security is practiced. There are three organisation-level roles: administrator, manager and standard. Furthermore, standard users can be granted specific access to registers: read only, standard and full access.

Users can be invited by an administrator, at which point an invitation email is sent. The recipient accepts the invitation, before a password can be created.

3. GDPR Security and Data Ownership Policy

Under GDPR:-

- The Port is the data owner.
- Marico is the data processor.
- Endgame is the data processors agent and follows our requirements.

For the European General Data Protection Regulation 2016/679 (GDPR requirements), the port (Hazman II subscriber) user remains the data owner at all times. The data controller is Marico Marine Group Limited and Marico Marine (UK and or NZ) retains responsibly as the data processor and sets the standard of security for the system. Endgame deliver the support service against the requirements of Marico Marine.