Brighter Days

Solar Workplace

Security Guidelines

1 April 2021

CONTENTS

1. Introduction

Solar Workplace is a framework that allows clients to have their own hosted Software as a Service (SaaS) product platform and has been designed with information security as the highest priority. The very nature of the modern network architecture that we use is designed to be robust and secure as a web host.

This document outlines the specific application security that is built into the Solar Workplace product.

2. Data Centre Security

Solar Workplace sites and applications are hosted with our Infrastructure Partner vBridge – specialist providers of high security & performance & hosted compute infrastructure, based in New Zealand.

vBridge recognise the importance of data integrity & security and with this in mind have adopted a multi-node, multi-datacentre approach. All vBridge staff have passed the Ministry of Justice vetting process and have signed a confidentiality agreement.

The vBridge platform has been designed with a minimum of N+1 resiliency across all components. The hosting platform provides separation of all customers' data and network traffic. vBridge control physical security and stability using Tier 3 and Tier 2+ New Zealand Department of Internal Affairs approved Datacentres. These provide robust entry and access control along with high levels of physical protection against unplanned events.

ISO 27001

vBridge is an ISO27001 certified organisation. This standard is widely recognised as the gold standard for information security. Their certification is maintained through ongoing auditing by an external ISO accredited provider along with their own regular internal audit processes.

vBridge maintains an Information Classification Matrix along with a Classified Information Handling Policy. All information stored by customers has a RESTRICTED classification.

FIREWALL SECURITY

vBridge Firewall as a Service (FWaaS) is a next generation firewall (NGFW) service enabling organisations to achieve best practice network security. This service is delivered from N+1 Fortigate Firewall Clusters. These next generation firewalls provide Full L4 to L7 configurable security policies along with industry leading IPS, SSL inspection and advanced threat protection.

GDPR COMPLIANCE

For customers that are required to work under the EU GDPR, vBridge can enter into a Data Processing Agreement to support all compliance needs.

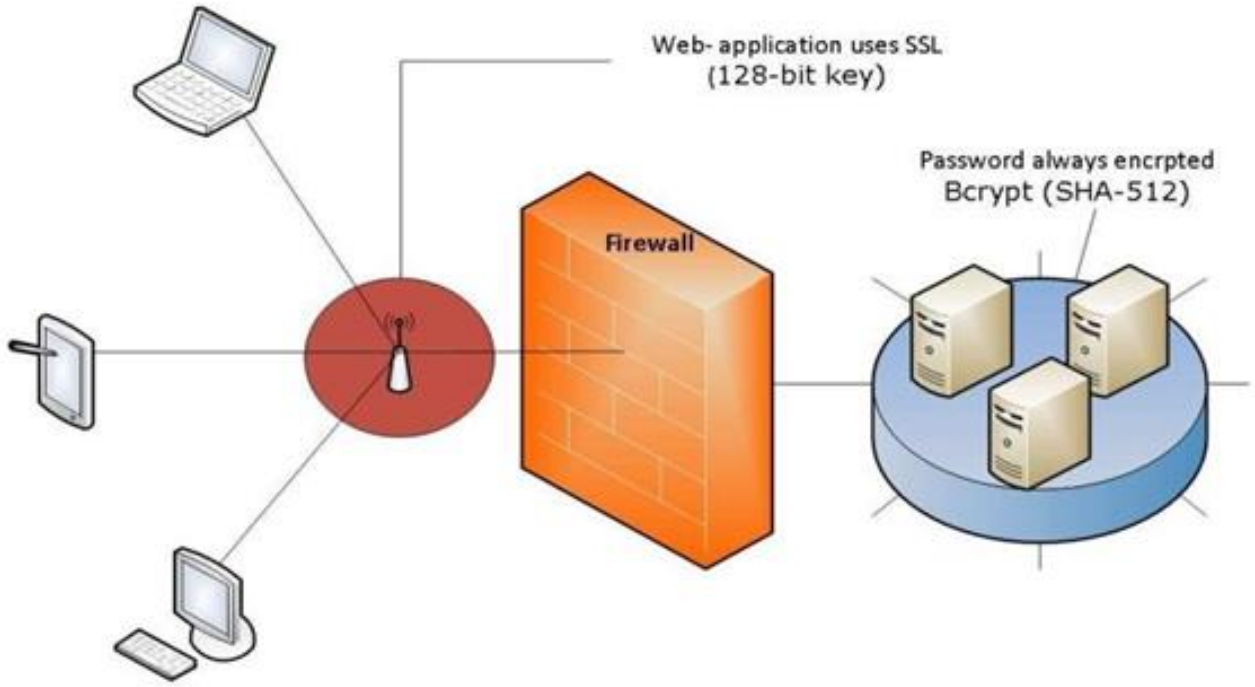
BACKUPS

Information is routinely retained in the format of Database Backups.

A full backup is taken daily, with incremental backups taking place hourly through the working day.

Backup Databases are stored on a secure server distinct from the Production ("Live") Server, with periodic transport to "off-site" Data Centres to aid in the event of Disaster Recovery. Backups are also routinely restored and tested to ensure a robust recovery plan is in place.

3. Application Security



The application and the web server technology have been specifically configured and designed to withstand the most prominent forms of attack. These include:

- URL interpretation
- Input validation
- SQL injection
- Buffer overflow attacks
- All passwords are encrypted using BCrypt (SHA-512), an algorithm designed to be strong even if the user chooses a simple password. It can also significantly delay attempts at brute force attacks.
- Passwords are never stored or transmitted in plain text.
- Users are automatically locked out after a failed login attempts – configurable to suit your business needs - making brute force attacks near impossible.

- Solar Workplace uses SSL certificates - web traffic between the user and the server is encrypted at all times using SSL (SHA-256 With RSA Encryption).
- All key user actions are logged along with their IP address. In the event of a breach (for example a user has their password on a sticky note attached to their monitor), the problem can be traced and mitigated. Logs can be produced, detailing information that may have been accessed or altered.
- Each client instance is also a separate web application with its own application pool and SQL database, this ensures complete segregation of client data for further protection.
- Solar Workplace has been developed as a full-stack Web Application leveraging the Microsoft .NET Framework, and deployed onto securely hosted servers.
- Solar Workplace is a single product that is deployed across multiple servers to give clients reassurance that no breaches of their data will occur. Each site is hosted within its own secure environment as a separate web application with data access to its own secured Sql Server Database.
- Monitoring is in place to track all external and internal access or attempted access.

4. Personnel & Training

All Brighter Days staff are recruited via trusted partners and services, including direct referrals.

Background checks are performed on all staff validating identity, references, experience, and education. Additionally, and where legally permissible, this also includes police background checks.

As part of the on-boarding process, all staff are required to read and acknowledge understanding and adherence to internal policies and standards.

All staff are subject to a Terms of Employment contract, that clearly lays out requirements and expectations around privacy and confidentiality terms.

DATA ACCESS

As part of routine maintenance, members of the Brighter Days teams may directly access the production ("Live") server to perform tasks including, but not limited to:

- Server Updates (software of configuration),
- Manual Database backups and transfers,
- Housekeeping tasks including archiving and optimisation.

No direct data access that might expose personal information is undertaken at any point during the above tasks.

DATA TRANSFER

On occasions – and at the client's request – data is required to be transferred between the client and the Solar Workplace servers, typically during the initial project phase (e.g., loading of employee profiles).

All data transfers take place over secure FTPS channel, with access permissions routinely reviewed.

SITE SECURITY

Client-facing access to the Montage Online web application has multiple layers, ensuring security at multiple points. From the initial login, users will only have access to view, modify, create, or delete what they have been granted access to.

Access to specific process, entity, or user records, can only be applied by designated Super Users.

INITIAL USER ACCESS – LOGGING IN

- Only those with an active, non-expired user account can log on to the Montage Online web application. From the initial login page, the user is prompted for their username and password.
- By default, there is a configurable three-strike lockout in place. If a user fails to enter their password correctly three times their account will be locked out and an email notification sent with password reset information.
- For additional security these is also a Single Sign-On (SSO) option to allow access only to users on your network.
- A user account can be expired by a designated super user. Users cannot be deleted from the client facing application.
- Requests to delete users can be done through our Support Portal.
- The password policy can be set to enforce complex passwords being a mix of upper-case, lower-case and numbers.
- The Solar Workplace application allows for the setting of cookie time-out intervals. If enabled, after a predefined period of inactivity the user will have to re-enter their username and password to continue using the software.

USER ACCESS LISTS

- User access lists govern access to confidential and non-confidential records in the Montage Online application.
- A user access list can be in the form of 'Groups' or 'Roles'.

ROLES

- Users can switch to a Role if they have been granted the required security access.

- Roles have customised access to specific records, such as certain processes and a certain area of employee records.
- When assigning security access, the Role can be given varying levels of view, modify, create, or delete.
- When a user switches to a Role, any access granted to the user at a user or group level becomes redundant.
- When in a Role, the Role security supersedes all other access.

GROUPS

- Groups are access lists given to specific types of users or a set list of users.
- An example of a user Group would be New Zealand Managers or All Active Employees. Groups are useful for granting access to processes and entities without having to switch Roles.
- When given access via a group, users will have access as soon as they log in.
- When assigning security access to Groups, varying levels of view, modify, create, or delete can be granted.

PROCESSES, ENTITIES AND USER RECORDS

- Processes, entities, and user records are granted specific access requirements through Roles and Groups.
- The same access rights can be applied at the user level, to ensure that security is as granular as needed.
- When assigning security access, varying levels of view, modify, create, or delete can be granted to specific Users, Roles or Groups to a detailed level.
- For example, at a specific step or part of a process flow the user may only have view and edit access when the user is assigned to or required to participate in the process (such as make comments and approve).

5. Questions

If you have any questions pertaining to any of the content in this document, please contact either of the following individuals listed below:

Paul White
Principal Consultant – Product
paul@brighterdays.co.nz

Lee Stevens
Principal
lee@brighterdays.co.nz