BackupSimple

Security Whitepaper

Version 1.3

1 Document Control

1.1 Classification

Classification		Restriction groups
Internal		
Restricted Internal		
Restricted External	X	Provided on specific Customer request
External		

1.2 Version History

Version	Date	Author	Comments
1.0	18 January 2018	Dominic Banister	Initial document
1.1	16 April 2018	Dominic Banister	Updated to add additional audit notes
1.2	30 April 2018	Dominic Banister	Additional encryption details
1.3	14 May 2018	Dominic Banister	Added information on encryption at source and re-aligned encryption headlines for continuity

2 Contents

3 Introduction

Information Security is of paramount importance to BackupSimple.

This whitepaper provides a view of the security position across the technical components of BackupSimple, and that of the customer data protected by the solution.

4 Architecture

BackupSimple is an Enterprise grade backup system which offers customers the ability to protect their entire data landscape with a single comprehensive tool, hosted by SoftwareONE.

BackupSimple has been architected from the ground up to deliver against two key security principles:

1. Ensure customers retain full control of their environment
    - BackupSimple's hosted infrastructure requires no inbound connectivity to any customer environment. BackupSimple Agents initiate communications outbound-only, ensuring customers retain full control of all traffic traversing their environment.
    - Customer retain the ability to administer the entire data protection lifecycle, from deploying agents and selecting the scope and policies of backup, to fully controlling the scope and schedule of data restorations.
    - Customers manage all credentials required to protect their data. At no point are any credentials shared with any BackupSimple operations staff.
2. Customers retain full ownership of their data
    - All data is stored at rest in the customer's own, dedicated storage repository. To ensure this requirements is met, BackupSimple is able to directly leverage the largest selection of both Private and Public cloud storage solutions on the market.
    - Customers are able to encrypt all data at rest with their own encryption keys, or can utilise keys from their own preferred storage provider.
    - Customers are able to migrate away from BackupSimple quickly and effectively.

To deliver these principles across multiple customers and multiple environment types, BackupSimple utilises a highly componentised architecture. The key components across the architecture are as follows:

- *CommCell* : A CommCell is the logical grouping of all software components that protect, move, store, and manage data and information. BackupSimple's Commcell's is a secure multi-tenant environment.
- *CommServe* : The CommServe hosts coordinate and execute all CommCell operations, maintaining Microsoft SQL Server databases that contain all configuration, security, and operational history for the CommCell environment.
- *Web Console*: The Web Console is a web-based portal that allows end-users to manage their data, as well as to perform other useful operations such as reporting, downloading software packages, and managing virtual machines.
- Proxy gateways: The Proxy gateways, hosted by SoftwareONE, are used to surface the CommServe environment to the Internet consistently and securely.
- Media Agents: The Media Agent is the data transmission manager in the CommCell environment. It provides high performance data movement and manages the data storage libraries. Dedicated Media

Agents are installed within each customer environment and hold customer specific Deduplication & Index databases

- iData Agents: A software module that is installed on a client computer to protect a specific type of data, e.g. SQL iData agent specifically protects Microsoft SQL databases.
- Backup Target : The data set being protected by an iData agent
- Storage Target : The final resting location for all protected data.

The following diagram gives an overview of the BackupSimple technical architecture

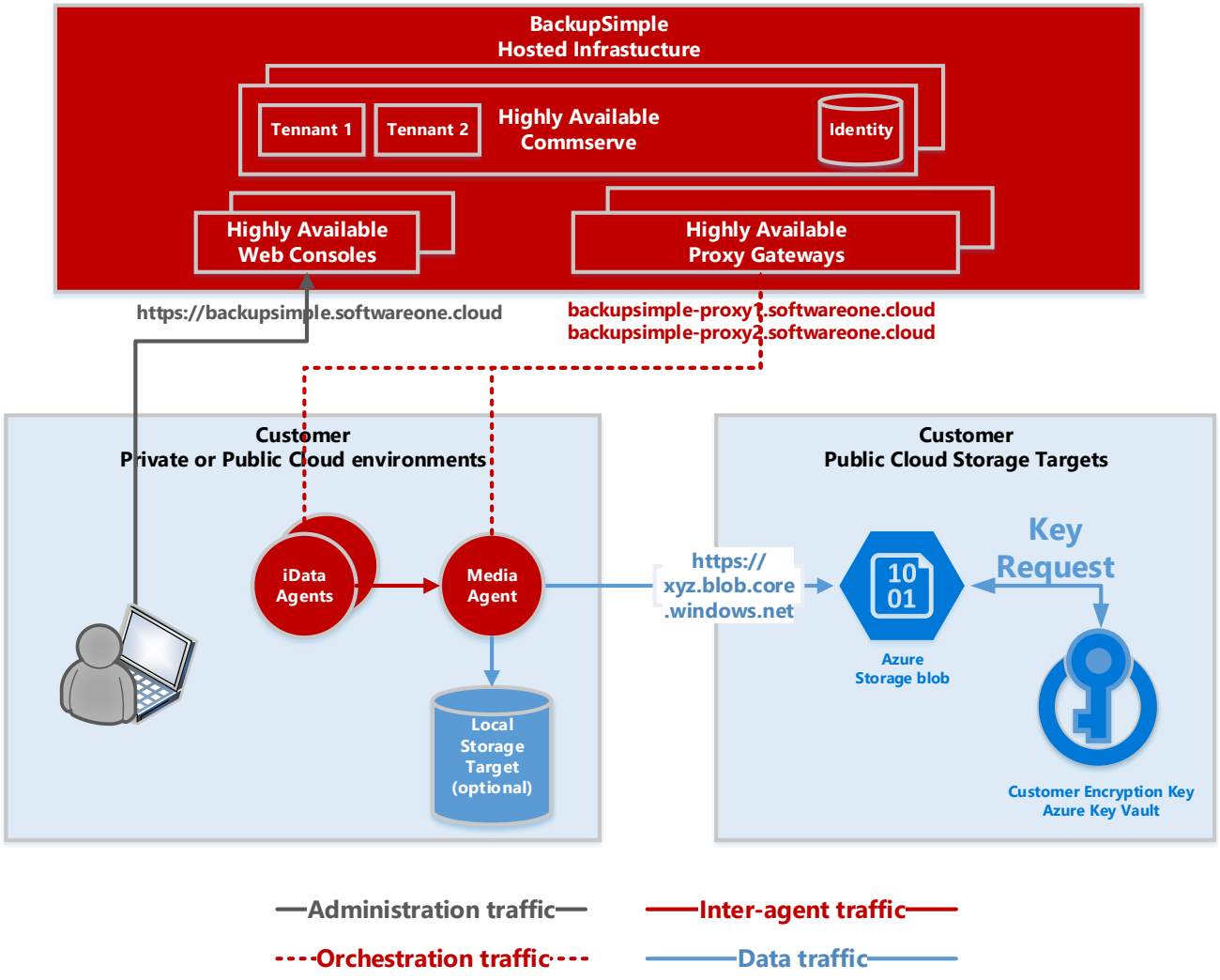

Figure 1 BackupSimple High Level Architecture

5 Service security

BackupSimple leverages Commvault, the Enterprise backup solution which consistently occupies the top right position of Gartner's magic quadrant. Gartner say *"Commvault has the most expansive list of supported public cloud providers, hypervisors, big data support and database protection, providing technological liberty for future procurement decisions".*

BackupSimple infrastructure is entirely hosted on Microsoft Azure and as a result we are able to offer a market leading 99.9% uptime SLA across the entire service stack.

Each component of the hosted infrastructure is delivered across a highly available platform architecture and is geo-replicated between two Azure regions for Disaster recovery

SoftwareONE ensure the highest security and functionality from our managed services by applying minor updates and patches with 3 months of a major Software Vendor's release, and major upgrades within 6 months.

All nodes within the BackupSimple environment are patched and have antivirus deployed to meet SoftwareONE's Managed Services internal policies.

SoftwareONE entirely segregate Production, Test, Development and any other lifecycle environments. Operations teams access all lifecycle environments from a dedicated Management environment. This ensure there's is no cross-lifecycle environment traffic, including that required for management.

6 Perimeter & Network security

Web Application firewalls utilising rules from the OWASP ModSecurity Core Rule Set protect the perimeter of the BackupSimple hosted infrastructure.

SoftwareONE operate an n-tiered networking structure with monitored highly resilient firewalling between each tier.

6.1.1 Vulnerability scans

SoftwareONE leverage industry standard tools to run weekly scans for externally-facing security vulnerabilities.

Level 4 and level 5 vulnerabilities are entered into the Change Management System by the IT Services Coordinator. Definitions for level 4 and level 5 vulnerabilities are as follows:

Level 4 - Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host. All Level 4 known vulnerabilities will be researched and resolved within 30 days.

Level 5 - Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors. All Level 5 known vulnerabilities will be researched and resolved within 5 days.

Scan can be made available upon specific request from customer security teams.

6.1.2 Intrusion Detection Systems

All internet facing network segments are monitored by Azure's Intrusion Detection Systems (IDS).

7 Data security

7.1 Data Sovereignty

BackupSimple's hosted infrastructure is based in West Europe (Netherlands) and is continuously, asynchronously, replicated to North Europe (Ireland).

The BackupSimple hosted infrastructure holds zero customer data, nor does any customer data traverse the BackupSimple hosted infrastructure. Only the following *metadata* is held on the hosted infrastructure:

- Server / Agent names
- Backup Schedules
- Backup Retention Policies
- Backup Scope (e.g. drivename\foldername\filename)
- Backup/Restore History
- Customer's BackupSimple Identity

Customer data is held at rest at the Customer's preferred storage provider, and therefore, by definition in the customer's preferred storage geographies.

At no point does BackupSimple, restore, copy or move any customer data without specific request from customer.

7.2 Data Encryption

BackupSimple offers three key encryption methods:

1. **Inline encryption** –Secures data during the data protection job and takes place on the client or Media Agent. By default Data is encrypted at source, on the client, before network transmission providing complete end-to-end security.
    - **Note:** Encryption at source can be disabled for customers preferring to rely solely on their own Hardware encryption keys.
2. **Offline encryption** – Secures data during auxiliary copy jobs (for example, when copying data from one storage repository to another). Takes place on the source Media Agent.
3. **Hardware encryption** – takes place on the storage device. Encrypts data at rest with additional encryption keys, e.g. those owned by Customer.

BackupSimple's Inline and Offline encryption keys are maintained in the BackupSimple database and scrambled using a proprietary algorithm.

During restore operations Inline and Offline decryption always occurs on the destination client. Hardware decryption always occurs on the storage hardware.

7.2.1 Encryption in transit

All BackupSimple communications, including administration, orchestration and data traffic are encrypted in transit.

- Administration traffic is outbound-only on port 443 and is encrypted using 2048 bit, TLS 1.2 encryption to https://backupsimple.softwareone.cloud.
- Orchestration traffic is outbound from iData agents to the following addresses
    - Backupsimple-proxy1.softwareone.cloud
    - Backupsimple-proxy2.softwareone.cloud

  All orchestration traffic is encrypted using TLS 1.2 protocol with the AES 256-GCM-SHA384 cipher suite
- Inter-agent traffic is outbound-only from iData agent to Media agent. The default port is 8403 although this can be changed upon request. Traffic is encrypted using TLS 1.2 protocol with the AES 256-GCM-SHA384 cipher suite
- Traffic to Azure Blob storage is encrypted in transit per the configuration preferred by customer. BackupSimple recommend ensuring "Secure transfer required " is enabled per Microsoft's documentation here: https://docs.microsoft.com/en-us/azure/storage/common/storage-require-secure-transfer

7.2.2 Deduplicated data encryption

A unique feature of BackupSimple is the ability to encrypt deduplicated data. The software accomplishes this by encrypting the data after the hash signature has been generated. The full process, including compression is:

- **Object backups** : Compress, Hash, Encrypt
- **Database backups** : Hash, Compress, Encrypt

Traditional methods of deduplicating encrypted data hash the encrypted data; every time the block is encrypted a different hash is generated. As a result, it is not possible to achieve efficient deduplication ratios. Since BackupSimple software hashes the block prior to encryption, the hash is always consistent even if the encryption key changes resulting in efficient deduplication ratios.

7.2.3 Encryption at Rest

The data held in BackupSimple Storage Targets, a.k.a Storage Repositories, can be encrypted in one of two ways:

1. Using BackupSimple's native encryption features as described above, i.e. encrypted at source prior to transmission and at rest in the Storage Target.
2. Utilising the Storage Repository provider's own Keys.
    - BackupSimple leverages Azure Blob Storage as the standard long term data Storage Repository.

      Azure Bob offers Storage Service Encryption (SSE) which utilizes 256-bit AES encryption for all data at rest.

      Note that Azure Blob customers are able to utilize their own encryption keys for SSE. More information is available on the requirements for uploading and managing Customer's own keys here: https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption-customer-managed-keys.

      The BackupSimple Support team will assist Customer with utilizing SSE with Azure Key Vault

- Customer's using their own storage repositories should refer to the Storage Vendor's documentation for enabling encryption

Note that customers can utilize both BackupSimple's native encryption and their Storage providers encryption in tandem if preferred.

By leveraging BackupSimple's native encryption with a third party storage provider, such as Microsoft Azure, BackupSimple customers are able to ensure security through segregation of duties across providers, i.e. BackupSimple have no access to the Customer's Storage and the Storage Provider has no access to the Backup's Data encryption keys.

7.3 Data Disposal

Microsoft Azure securely erase or destroy drives used for storage that suffer hardware failure. When such devices are decommissioned, they are purged or destroyed according to NIST 800-88 Guidelines for Media Sanitation. Further details can be found here: https://www.microsoft.com/en-us/trustcenter/privacy/you-own-your-data

SoftwareONE utilize industry standard software to erase data drives to DoD 5220.22-M data sanitation standards before handing them back to Microsoft.

7.4 Data Portability

BackupSimple data is stored in a proprietary format.

For customer's wanting to exit the BackupSimple environment a simple request to BackupSimple Support will initiate a 'MetaData Export' from the BackupSimple database.

Due to the unique Storage Architecture, i.e. each customer leveraging their own dedicated storage, the MetaData export takes minutes to complete and can be dropped onto your own Storage Repository enabling your local team, or new service provider, to stand up a new Commserve environment to restore all data from the repository. At specific request this can be scheduled on a regular basis for a simplified exit strategy.

Further information on importing the Metadata can be found here:
http://documentation.commvault.com/commvault/v11/article?p=5101.htm

Note that Commserve license their product on Front End Terrabyte or Number of Nodes being protected. In the scenario above there would be no license fees from Commserve as they do not charge for restoring data.

8 Identity

8.1.1 Client Identity

Client's register with BackupSimple during installation by using a unique, customer-specific, alpha-numeric authorisation code appended to the end of the installation commands as shown below

```
Win64-AC_Windows-x64.exe /silent /install /silent /authcode 37986BA0
```

After initial authorization has completed, and connectivity to the BackupSimple orchestration engine has completed, an internal Commserve Certificate Authority is used for all future authentications.

- BackupSimple generates client certificates based on 2048-bit RSA keys.
- Matching RSA private keys are stored on the clients in 3DES-encrypted envelopes and are never transmitted across the network.
- Client certificates authenticate all tunnel connections using the TLS 1.2 protocol.
- Commvault implements its own Certificate Authority (CA) service running on the CommServe host.
- Client Certificates are rotated every 6 months
- The BackupSimple Certificate Authority (CA) is renewed every 5 years

8.1.2 Users

BackupSimple hosts a dedicated identity database, provided by Commserve.

Two Factor Authentication is enabled for all users, including BackupSimple operations staff.

9 Auditability

BackupSimple's hosted infrastructure resides entirely on Microsoft Azure and leverages Azure's own audit trails for infrastructure-level change and management logging.

The BackupSimple application also monitors all activity across the customer tenant. This information is available to the customer Tenant Admins through the BackupSimple web portal. The following table gives a high level view of the audited operations and their retention periods

Severity Level	Type of Operations Included	Examples	Default Retention days
Critical	Operations that delete data.	Deleting a backup set; reconfiguring an agent.	365 days
High	Operations that might delete data.	Changing client encryption properties or media management configuration.	365 days
Medium	Operations that change the general configuration of one or more entities in the CommCell,	Exporting media; killing a job.	240 days

	which may produce unintended results.		
Low	Operations that change status, add entities, and other operations that have minimal impact on existing CommCell functions.	Compliance searches; setting container information for Vault Tracker actions. See Operations Recorded for Audit Trail for a list of operations.	120 days

Backup and Restore job summaries are also available to all Tenant Administrators through the BackupSimple web portal. These reports show all information regards the restore including the source and destination agent that committed the restore.

10 Human Resources

SoftwareONE employees involved in the administration of Cloud systems or customer data are screened by SoftwareONE's Human Resource departments, including an external background check and criminal history review.

All permanent employees are required to agree to a confidentiality agreement covering all SoftwareONE and customer information.

SoftwareONE employs a yearly employee performance review process, provides training opportunities to employees, and has a fully documented Employee Resources website that details the terms of employment and identifies the relationship between SoftwareONE and its employees.

10.1 Security Awareness Training

All SoftwareONE employees are required to complete annual security awareness training to ensure that employees remain vigilant and utilize safe computing practices.

Training covers such topics as social engineering, email and instant messaging, general web browsing, password security, use of encryption, and data security as well as awareness of SoftwareONE own internal security policies.