

1.1 Service name

Service name

TRUSTMARQUE SafeGUARD BACK-UP AS A SERVICE

1.2 About your service

Service description

Unifying Backup & Recovery, DR, Archiving and Search, SafeGUARD provides a highly secure data management service to protect all your data. Eliminating the burden of performing traditional local backups, the service offers centralised visibility of all data and allows you to stream your data on demand from backups and archives.

Service categories

- Archiving, backup and disaster recovery
- Search
- Block storage
- Object storage
- Other storage services

1.3 Service features and benefits

Service features and benefits

Service features

- Rapid restore and recovery
- Deduplication to reduce transmitted and stored data volumes
- Located in UK Data Centres
- Advanced Malware detection
- Encryption (AES-256) to secure your data in the cloud
- Archiving and search functionality
- Centralised management console for ease of management
- Automated reporting including exception-reporting
- SaaS Backup for Microsoft 365 and Salesforce
- Options for local copies of data

Service benefits

- Eliminate downtime. Instant Data provides on-demand access to data
- Reduced backup window through advanced data reduction techniques
- Reduced operation effort with simple 'set and forget' backups
- Reduced bandwidth and low system overhead via data reduction techniques
- Management console providing single point of view for all data
- Simple, transparent pricing, no bandwidth charges, no hidden costs
- Reduces primary storage requirements through automated archiving
- Reduced maintenance overhead through automatic software updates
- Recover anything, anywhere and at any time
- Supported by data management specialists with experience since 1988.

1.4 Service scope

Service constraints

An installed client software agent is used to protect devices running supported operating systems and applications. Please refer to the system requirements and compatibility matrix.

System requirements

- Internet connectivity
- Backup software client installed on a supported operating system
- Resource availability (low) on systems to be protected

1.5 Reselling

Supplier type

Supplier type

I'm a reseller providing extra support

Organisation whose services are being resold

Redstor - <https://www.redstor.com/>

1.6 User support

Email or ticketing support

Email or online ticketing support

Yes

Support response times

Subject to an agreed SLA.

User can manage status and priority of support tickets

Yes

Online ticketing support accessibility

WCAG 2.1 AA or EN 301 549

Phone support

Phone support

Yes

Phone support availability

9 to 5 (UK time), Monday to Friday

Web chat support

Web chat support

No

Onsite support

Yes, at extra cost

Support levels

Business hours support is included as part of the service. Please refer to the Service Definition Document and End User Agreement. Users can upgrade if required to Support Advantage, which offers 24/7 support, a

Technical Account Manager and agreed levels of on-site resource. Please contact Trustmarque for further information on Support Advantage.

Support available to third parties

No

1.7 How users work with your service

Web interface

Web browser interface

Yes

Using the web interface

A central management console allows IT departments to monitor and manage online backups, set-up schedules and automate administration and processes - true management by exception, reducing the time spent managing backups for data in hybrid or cloud storage. Reporting is a key function, with scheduled reports and information on online backup status, enabling IT departments to intimately track, administer and manage backups and restores.

Web interface accessibility standard

None or don't know

How the web interface is accessible

The management Console has full role based access security and audit logs.

Web interface accessibility testing

N/A

API

API

Yes

What users can and can't do using the API

The default graphical user interface of the SafeGUARD software can be replaced completely with customised branding and UX design through the

API whilst maintaining the full functionality of the software. SafeGUARD comes complete with a full reporting suite and centralised management console, all of which can be accessed through the extensive API.

API automation tools

Other

API documentation

Yes

API documentation formats

PDF

Command line interface

Command line interface

Yes

Command line interface compatibility

- Linux or Unix
- Windows

Using the command line interface

Backup and restore can be performed via the command line. This required that a backup selection has been performed via an installed client first.

1.8 Onboarding and offboarding

Getting started

A technical adviser from our dedicated Support team will provide the relevant advice as to the most efficient way to on-board the End User in pre-agreed and defined timeframes. All relevant software, training and support to run and maintain the Service will be provided by Trustmarque. For further information, please refer to the Service Definition Document.

Documentation

Service documentation

Yes

Documentation formats

- HTML
- ODF
- PDF

Documentation accessibility standard

WCAG 2.1 AA or EN 301 549

End-of-contract data extraction

All data is fully recoverable for up to 30-days after contract ends. Longer terms can be negotiated.

End-of-contract process

All data is fully recoverable for up to 30-days after contract ends. Longer terms can be negotiated.

1.9 Backups and recovery

Backup and recovery

Backup and recovery

Yes

What's backed up

- Files
- Virtual Machines
- Azure VM's and BLOB Storage
- Network Attached Storage (NAS)
- Laptops, PCs and Servers
- M365 including; Exchange, SharePoint, OneDrive, Teams and EntraID (Coming Soon)
- Google Workspace
- AWS and Azure Kubernetes
- Salesforce
- Applications

Backup controls

The SafeGUARD Backup Service provides an online storage platform which enables a Customer to back up a specified device. The associated software that is provided by Trustmarque to enable use of the Service allows automated or manual backup, as well as Customer initiated data recovery. Backups can be scheduled to run unattended at a particular time and at a frequency defined by the Customer. Different backup selections can be scheduled to run at different times and frequencies.

Datacentre setup

Multiple datacentres with disaster recovery

Scheduling backups

Users schedule backups through a web interface

Backup recovery

Users can recover backups themselves, for example through a web interface

1.10 Analytics

Metrics

Infrastructure or application metrics

Yes

Metrics types

Memory

Reporting types

Real-time dashboards

1.11 Scaling

Scaling

Scaling available

Yes

Scaling type

Scales automatically

Independence of resources

The service is underpinned by a scale out infrastructure which is scaled ahead of being needed so there is always availability to support demand. As the infrastructure scales, it scales in both performance and capacity. A comprehensive Service level Agreement (SLA) is offered to Customers.

Usage notifications

Usage notifications

Yes

Usage reporting

- API
- Other

Other usage reporting

Uses can see usage in the management interface.

1.12 Data-in-transit protection

Protection between networks

Data protection between buyer and supplier networks

- Private network or public sector network
- Legacy SSL and TLS (under 1.2)
- Other

Other protection between networks

The SafeGUARD software fully encrypts the Customer's data using 256-bit AES encryption and transfers the Customer's fully encrypted data via any TCP-IP enabled network connection over TCP port 443. Data is encrypted before leaving the Customer's device in relation to which the Service is provided and remains so until recovered by the Customer.

Protection within your network

Data protection within supplier network

Legacy SSL and TLS (under 1.2)

1.13 Asset protection

Data storage and processing locations

Knowledge of data storage and processing locations

Yes

Data storage and processing locations

United Kingdom

User control over data storage and processing locations

Yes

Datacentre security standards

Managed by a third party

Penetration testing

Penetration testing frequency

At least once a year

Penetration testing approach

Another external penetration testing organisation

Protection of data at rest

Protecting data at rest

- Physical access control, complying with another standard
- Encryption of all physical media

Data sanitisation process

Data sanitisation process

Yes

Data sanitisation type

Deleted data can't be directly accessed

Equipment disposal approach

A third-party destruction service

1.14 Availability and resilience

Guaranteed availability

Trustmarque uses reasonable endeavours to provide the Services in accordance with the Service Level Agreement which is that the Service is available at a minimum of 99.5% per month. In calculating availability, no account shall be taken of time the Service is unavailable due to any installation work or due to any maintenance in relation to the Service. If Trustmarque fails to achieve the Services Level targets specified for the Service, the End User may claim a credit (limited per month) based on the monthly recurring charge for the Service. Please refer to Schedule 3 - Service Level Agreement in the SafeGUARD End User Agreement for further details.

Approach to resilience

The data centres provide high levels of uptime. Ensuring electricity is always available, the primary data centre facility provides a minimum of N+1 power redundancy, meaning every mission-critical component has at least one backup power feed that kicks in when there's an outage. Data centres also have enough fuel on site to provide 24 to 48 hours of emergency power using backup generators with guaranteed fuel delivery.

Outage reporting

Any outages are reported to Customers via email alerts

1.15 Separation between users

Virtualisation

Virtualisation technology used to keep applications and users sharing the same infrastructure apart

No

1.16 Governance

Named board-level person responsible for service security

Yes

Security governance

Security governance certified

Yes

Security governance standards

ISO/IEC 27001

Information security policies and processes

S3 is ISO9001 and ISO27001 accredited and as such adheres to the policies and procedures set out under these schemes.

1.17 Operational security

Configuration and change management standard

Supplier-defined controls

Configuration and change management approach

Further information can be provided upon request.

Vulnerability management type

Supplier-defined controls

Vulnerability management approach

Further information can be provided upon request.

Protective monitoring type

Supplier-defined controls

Protective monitoring approach

Further information can be provided upon request.

Incident management type

Supplier-defined controls

Incident management approach

Further information can be provided upon request.

1.18 Staff security

Staff security clearance

Staff screening performed but doesn't conform with BS7858:2019

Government security clearance

Up to Security Clearance (SC)

1.19 Secure development

Approach to secure software development best practice

Supplier-defined process

1.20 Identity and authentication

User authentication

User authentication

- Username or password
- Other

Other user authentication

One set of security credentials (account name, password and encryption key) is required for each device, and the security credentials may not be shared between devices. Security credentials include an encryption key. The key can be combination of alphanumeric characters of the customer's choosing and is used when the encryption algorithm encrypts files to keep data confidential. Without the key, no one can access the data.

Access restrictions in management interfaces and support channels

The management interface offers role based access meaning you can restrict each user to allow only the functionality required. An audit trail allows tracking of changes made by different users.

Access restriction testing frequency

At least once a year

Management access

Management access authentication

Username or password

Devices users manage the service through

Directly from any device which may also be used for normal business (for example web browsing or viewing external email)

1.21 Audit information for users**Audit for buyers' users' actions**

Access to user activity audit information

Users have access to real-time audit information

How long user audit data is stored for

Less than 1 month

Audit for suppliers' users' actions

Access to supplier activity audit information

Users have access to real-time audit information

How long supplier audit data is stored for

Less than 1 month

How long system logs are stored for

Between 1 month and 6 months

1.22 Standards and certifications

ISO/IEC 27001 certification

ISO/IEC 27001 certification

Yes

Who accredited the ISO/IEC 27001

IMSM (International Management Systems Marketing)

ISO/IEC 27001 accreditation date

2024

What the ISO/IEC 27001 doesn't cover

N/A

ISO 28000:2007 certification

ISO 28000:2007 certification

No

CSA STAR certification

CSA STAR certification

No

PCI certification

PCI certification

No

Cyber essentials

Cyber essentials

Yes

Cyber essentials plus

Yes

Other security certifications

Other security certifications

Yes

Any other security certifications

- ISO 27001 certified for Information Security Management
- SOC 2 Type 1

1.23 Energy efficiency

Energy efficiency

Energy-efficient datacentres

Yes

Description of energy efficient datacentres

tbc

1.24 Social Value

Social Value

Social Value

Wellbeing

Wellbeing

Cloud backup services offer significant social value for businesses by fostering resilience and ensuring continuity of operations. In the event of a cyberattack, hardware failure, or natural disaster, a secure, off-site backup allows businesses to recover critical data quickly and minimize downtime. This translates to a reduced risk of lost revenue, maintains customer trust by protecting sensitive information, and safeguards jobs by ensuring employees can keep working. Overall, cloud backups contribute to a more stable and secure business environment, benefiting both the company and the wider community it serves.

1.25 Pricing

Price

£0.10 to £0.45 a gigabyte a month

Discount for educational organisations

Yes

Free or trial versions

Free trial available

Yes

Description of free trial

A 14-day unlimited, full version, free trial is available on request.