SERVICE DESCRIPTION

DSPROTECT

Version: 1.10

Date: December 2021

Status: Released

Prepared by:

Dan Frith   Level 8, 300 Ann Street

Product Lead   Brisbane, QLD, 4000

1300 799 908

digitalsense.com.au

CONTENTS

TABLES

DOCUMENT RECORD

Document Information
Author: Dan Frith
Status: Released
Version: 1.10
Date Created: 2020.11.10
Date Issued: 2021.12.01
Location: DSProtect_ServiceDescription_v1.10.docx
ServiceNow:

Table 1 - Document Record

REVISION HISTORY

Revision Number	Author	Issue Purpose	Date
1.00	Luke McDougall	Final draft	2020.11.10
1.03	Luke McDougall	Minor updates	2020.12.01
1.04	Dan Frith	Release	2020.12.22
1.05	Dan Frith	New NAS policies added	2021.01.15
1.06	Dan Frith	Minor updates	2021.03.05
1.07	Dan Frith	DSProtect Edge, new template	2021.07.20
1.08	Dan Frith	Additional service operations	2021.08.20
1.09	Dan Frith	Minor Updates	2021.11.01
1.10	Dan Frith, Nigel Mearns	Minor Updates	2021.12.01

Table 2 - Revision History

RELEASE APPROVAL

This document is approved for release.

Version:

Name:

Position: , Digital Sense

Signature:

Date:

1   INTRODUCTION

DSProtect is Digital Sense's data protection service based on Rubrik Cloud Data Management (CDM)[1]. The service delivers a fully managed backup environment where the customer's data is completely protected and can be restored at any time according to specified service levels. DSProtect offers data protection across a variety of environments, including:

- Public clouds (Digital Sense operated and third-party);
- Dedicated customer environments; and
- Customer on-premises.

The solution supports a variety of workloads and can deliver multiple tiers of data protection and availability.

Data can be recovered on a VM-level, file-level and more granular level if required. The service offers enhanced support for physical resources and host systems, with agent-less integration. Additionally supported cluster configurations for application consistency. Data stored with DSProtect cannot be deleted or encrypted by malware attacks such as ransomware. Moreover, Digital Sense also provides fast recovery of an infected production environment. DSProtect also includes vendor-agnostic support for all NAS vendors that use NFS or SMB protocols.

In future releases of DSProtect, it's envisaged the solution offering will extend to:

- **Cloud Out** - automated archival to public and private cloud storage tiers.
- **Cloud Instantiate** - conversion of on-premises VMs to cloud instances in AWS and Microsoft Azure for cost-effective disaster recovery, application migration, and accelerated test / development.
- **Cloud Cluster** - users can deploy DSProtect as a software instance in a public cloud provider to orchestrate all critical functions.
- **AWS Native Data Protection** - DSProtect will integrate with native AWS APIs to deliver policy-driven and cloud-native data protection for AWS EC2.

1.1   KEY FEATURES

The solution currently supports multi-site availability across two physical Digital Sense Availability Zones (Kenmore and Polaris). Rubrik appliances provide cross-site protection of backup data, subsequently minimising any data unavailability due to either planned or unplanned outages. Erasure coding protection is used, along with archiving to DSObject. Other features include:

- Complete Data Protection as-a-Service (DPaaS) on a pay per month per GiB model – including backup service, software and off-site data storage in a fully redundant configuration;

---

[1] https://www.rubrik.com/en/products/cloud-data-management

- Self-service file restore functionality for virtual machines is available on-demand via VMware Cloud Director (VCD);

- Multiple data retention periods available ranging from 14 days to 7 years;

- Long-Term Retention – Meet compliance requirements with extended data retention rules in the cloud, or on-premises;

- Rapid Recovery – Reduced recovery time objective for VM recovery;

- Test and Development – Quickly provision VMs for test and/or development requirements in the cloud or on-premises; and

- Remote Office / Branch Office (RO / BO) – Support for replication of protected data from edge sites to the core, failover of protection jobs, and multiple fan-in configurations.

1.2 SUPPORTED WORKLOADS

The solution supports the following workload types:

- VMware VMs

- NAS storage (SMB and NFS)

- Physical machines - Windows, Linux

- Databases - Microsoft SQL, Oracle

- Public cloud workloads (AWS and Azure)

- RO / BO – via DSProtect Edge

In future releases, the following workloads will also be officially supported:

- Non-x86 (AIX, HP-UX, Sparc)

- Applications (SharePoint, Active Directory)

- Software as a Service (SaaS) - Microsoft 365, OneDrive

- NoSQL, MySQL, PostgreSQL workloads

- Microsoft Hyper-V VMs

- Nutanix AHV VMs

- Additional public cloud workloads (GCP)

1.3 RETENTION

The solution offers four levels of protection data retention.

Policy Name	Frequency	Local Retention on Brik (STR)	Second Copy (SC)	RTO	Remote Retention on Brik (SC)	Long Term Retention Archive Location (LTR)	RTO
Standard Policy	Daily backup	14 Days	No	8 hrs	Nil	None	24 hrs
Advanced Policy	Daily backup	14 Days	Yes	8 hrs	14 Days	None	24 hrs
Premium Policy	Daily backup	14 Days	Yes	8 hrs	14 Days	None	24 hrs
	Monthly Backup	14 Days	Yes	8 hrs	14 Days	77 Days	24 hrs
GFS Policy	Daily Backup	14 Days	Yes	8 hrs	14 Days	None	24 hrs
	Monthly Backup	14 Days	Yes	8 hrs	14 Days	12 Months	24 hrs
	Yearly Backup	14 Days	Yes	8 hrs	14 Days	7 Years	24 hrs

Table 3 - Standard Policy Retention

Policies are also available for database workloads. These are outlined in the table below.

Policy Name	Frequency	Local Retention on Brik (STR)	Second Copy (SC)	RTO	Remote Retention on Brik (SC)	Long Term Retention Archive Location (LTR)	RTO
SQL Advanced Policy	Daily backup	14 Days	Yes	8 hrs	14 Days	None	24 hrs
	TXLog Backup (Hourly)	7 Days	Yes	1 Hr	7 Days	None	N/A
SQL Premium Policy	Daily backup	14 Days	Yes	8 hrs	14 Days	None	24 hrs
	Monthly Backup	14 Days	Yes	8 hrs	14 Days	77 Days	24 hrs
	TXLog Backup (Hourly)	14 Days	Yes	1 Hr	14 Days	None	N/A
SQL GFS Policy	Daily Backup	14 Days	Yes	8 hrs	14 Days	None	24 hrs
	Monthly Backup	14 Days	Yes	8 hrs	14 Days	12 Months	24 hrs
	Yearly Backup	14 Days	Yes	8 hrs	14 Days	7 Years	24 hrs
	TXLog Backup (Hourly)	14 Days	Yes	1 Hr	14 Days	None	N/A

Table 4 - Database Policy Retention

Policies are also available for NAS workloads. These are outlined in the table below.

Policy Name	Frequency	Local Retention on Brik (STR)	Second Copy (SC)	RTO	Remote Retention on Brik (SC)	Long Term Retention Archive Location (LTR)	RTO
NAS DA Standard Policy	Daily backup	Meta Data Only	No	8 hrs	Nil	14 Days	24 hrs
NAS DA Advanced Policy	12 Hourly	Meta Data Only	No	8 hrs	Nil	14 Days	24 hrs

NAS DA Premium Policy	12 Hourly	Meta Data Only	No	8 hrs	Nil	30 Days	24 hrs
	Monthly Backup	Meta Data Only	No	8 hrs	Nil	3 Months	24 hrs

Table 5 - NAS Policy Retention

Note the following constraints relating to NAS workload protection:

- Frequency is Daily or 12 Hourly. If customers require more frequent protection, it is recommended that DSFile snapshots or DSProtect Availability (Zerto) be leveraged.

- The initial protection activity will take more time than the policy indicates. For example, a 100TB protection job will not complete with the expected policy window.

- NAS Direct Archive does not support replication of Archive locations. This is done by DSObject via StorageGRID's 3DC Erasure Coding.

- While Polaris Radar is supported with NAS Direct Archive workloads, Polaris Sonar is not.

1.4   BUSINESS BENEFITS

- Compliance with corporate frameworks around data storage, protection and integrity;

- Reduced risk of lost or corrupted data due to higher availability service offering;

- Data retrieval on demand for compliance or legal discovery;

- Complete DPaaS with 24x7 support reducing internal headcount and operational burden; and

- Peace of mind knowing that your data is protected with industry-leading SLAs.

2   SUBSCRIPTION

DSProtect is provided on a subscription basis, with 1, 3 or 5-year contract terms. There is no minimum commitment required in terms of capacity consumed. There are, however, commercial incentives available for customers committing to minimum capacities and contract duration.

The subscription is comprised of an upfront establishment charge coupled with a front-end, protected GiB pricing model. Beyond these basic subscription components, optional fee-based services may also be consumed. Please refer to the table below for service and feature pricing.

Policy	Usage	Cost AUD
Establish Service Offering	Initial Setup	$1,000.00
Add Virtual Machines	Per Virtual Machine	$8.72
Virtual Machine Standard	Per GiB	0.18

Virtual Machine Advanced	Per GiB	0.33
Virtual Machine Premium	Per GiB	0.36
Virtual Machine GFS	Per GiB	0.40
Long Term Retention S3 Archive	Per GiB	0.35
On-Demand Snapshot	Per Snapshot	$19.00
Configuration Guest Cluster	Per Virtual Guest Cluster	$495.00

Table 6 - DSProtect Service and Feature Pricing

Note the solution offers the following features:

- Policy based management;

- No API call charges;

- No ingress or egress charges; and

- No data retrieval charges.

2.1   SERVICE PORTALS

It is anticipated that in future releases of DSProtect, a service portal will be offered to consume and manage the service. The URL for this portal will be provided as part of the service handover. In the initial iteration of DSProtect, this feature will not be made available to customers. All service requests will be submitted via ServiceNow.

2.2   ADDITIONAL INFORMATION

The offering services customers who are seeking data protection with industry-leading service levels that are available across multiple DSCloud Availability Zones and / or third-party owned and operated data centres; including on-premises customer data centres.

- Backup and instant recovery;

- Data archival and compliance;

- Copy data management; and

- Cloud portability.

3   SERVICE OPERATIONS

The table below outlines Digital Sense's roles and responsibilities in the delivery of the service offerings. While specific roles and responsibilities have also been identified as being owned by the customer, any roles or responsibilities not contained in this Service Description are either not provided with the

service offering or are viewed to be the customer's responsibility. Digital Sense's service level commitments are outlined below.

Service Description	DS	Customer
Facilities		
Provide and maintain sufficient data centre floor space	✓	
Provide and maintain sufficient power and cooling within the Installation Sites	✓	
Provision and maintenance of Intra and Inter-site network connectivity required to support data replication and remote management including DSProtect platform and TCP/IP connectivity	✓	
Infrastructure Configuration		
Procurement of equipment	✓	
Physical installation of equipment	✓	
Supply / capacity increase and maintenance of network cabling required to support the environment including connectivity to Digital Sense or End Customer servers	✓	
Decommission of infrastructure	✓	
Removal of decommissioned hardware from Digital Sense sites	✓	
Installation and configuration of management software	✓	
Data Erasure on hardware	✓	
Configuration of features of DSProtect infrastructure	✓	
Enable features of DSProtect infrastructure	✓	
DSProtect Management		
Develop initial data protection and retention policies	✓	
Manage hardware and backup service software within the customer environment (patch and update etc.)	✓	
Proactively monitor and resolve incidents within the data protection environment	✓	
Forward automated events and alerts from proactive monitoring to customer	✓	
Maintain and manage data protection & retention policies	✓	
Maintain and store audit logs, deliver daily backup reports	✓	

Table 7 - Service Operations

3.1 SERVICE REQUESTS

Customers may request services from the standard DSProtect service catalogue. Service requests are executed based on the standard Digital Sense operational services for Service Requests. The following table details the service catalogue items for DSProtect.

Service Request Description	Included Quantity	Fee per SR[2]
New data protection policy	2/annum	$500.00
Modify existing data protection policy	6/annum	$250.00
Remove existing data protection policy	Unlimited	N/A
New data retention policy (time)	2/annum	$250.00
New data retention policy (instance)	2/annum	$250.00

---

[2] The fee per Service Request in excess of the included quantity.

Modify existing data retention policy	6/annum	$250.00
Remove existing data retention policy	Unlimited	N/A
Delete data from protected storage	Unlimited	N/A
Ad-Hoc backup - Digital Sense performed	4/month	$120.00
Data restoration – files or folders	10/month	$60.00
Data restoration – Virtual Machine	6/annum	$60.00
Data restorations – application data	4/annum	$60.00
Test restorations – file and folder level	1/quarter	$60.00
Test restorations – Virtual Machine level	1/quarter	$60.00
Test restorations – application data level	None	POA
Ad-Hoc Digital Sense generated simple reports	6/annum	$60.00
Ad-Hoc Digital Sense generated complex reports	None	POA
Portal Request – New User Account	20/annum	$30.00
Portal Request – Modify User Account	10/annum	$30.00
Portal Request – Delete User Account	unlimited	N/A
Portal Request – Reset Password	unlimited	N/A

Table 8 - Service Request Pricing

3.2   ACCOUNTS

A privileged user account will be required for Digital Sense to deliver data protection services for the customer's workloads. The details of this account will be provided as part of the detailed design phase.

3.3   SUPPORT

The service offering includes support for reported problems as they relate to DSProtect service availability.

Service Description	DS	Customer
Provide a fully managed data protection service including ensuring the service is "evergreen" (patching, software updates, hardware maintenance, firmware updates, security updates, hardware refresh etc.)	✓	
Develop initial network design (if DSProtect is accessed outside of DSCloud)	✓	✓
Deploy hardware and assets on-site where required	✓	
Provide suitable data centre facilities for onsite deployed hardware (including environmental aspects – rack space, power, UPS, air-con and security etc.)		✓
Provide elevated security accounts for operation, maintenance and customer environment support as required		✓
Proactively monitor and resolve incidents within the DSProtect environment	✓	
Forward automated events and alerts from proactive monitoring to customer[i]	✓	

Maintain and manage object storage resilience polices	✓	
Maintain and store audit logs	✓	
Provide data protection online user portals	✓	
Provide customer contact details for escalation		✓
Provide customer contact details for operational reports		✓
Provide customer contact details for alerting		✓

Table 9 - Support Responsibilities

3.4 TRANSITION ACTIVITIES

DSProtect is based on a standard configuration, however certain aspects of the service are tailored to match the customer's environment. For users of the DSProtect solution, a brief service initiation phase is required to ensure that the appropriate connectivity is in place. For Internet access, this is not required, but for users leveraging DSProtect via on-premises resources, some work is needed to ensure the appropriate connectivity solutions are in place. The Service Initiation phase includes design workshops and planning sessions with a detailed design document developed (if required).

Implementation of the service uses the design document and the Digital Sense Transition Methodology to ensure that the transition of services is executed successfully. The service initiation and transition phase includes:

- Understanding future data protection capacity and growth;

- Reviewing current security and encryption policies and aligning these with the standard Digital Sense design;

- Designing of the connectivity solution;

- Planning the timing and implementation of the service in line with the transition methodology;

- Presenting a transition plan for customer approval; and

- The implementation of the transition plan and design.

The cost of the service initiation could vary considerably depending on the complexity of the migration and transition. The cost of the service initiation will be based on the effort required for each implementation as detailed in the transition plan developed.

3.5 MONITORING

Digital Sense will provide the following monitoring services:

- Monitoring of the DSProtect solution at the physical, logical, and network layers and ensuring availability as per the agreed service levels.

The customer is responsible for the following monitoring activities:

- Monitoring of customer-operated endpoints, applications, and networks to ensure access to the DSProtect service is maintained.

Service Description	DS	Customer
Monitoring		
Configure the standard set of identified events, thresholds, and the required resources to be monitored for infrastructure services	✓	
DSProtect platform and related network fabric monitoring	✓	
Maintain monitoring tools and backup service software	✓	
Monitor in scope infrastructure housekeeping routines	✓	
Log events and notifications, including resource affected, specific event type, and time of detection	✓	
Notify the appropriate contact when an Incident has been detected in accordance with the notification procedures as defined in the incident and problem management section.	✓	
Respond to, and take appropriate action on alerts relating to the DSProtect environment	✓	
Document and maintain procedures to be followed in the event of a storage alert event	✓	
Provide monthly DSProtect storage usage reports	✓	

Table 10 - Monitoring

3.6 INCIDENT AND PROBLEM MANAGEMENT

Digital Sense will provide incident and problem management services aligned with ITIL recommended practices. These services will include detection, classification, escalation, and resolution, and will be recorded in Digital Sense's IT Service Management Tool (ServiceNow). These Incident and Problem Management services only relate to the provided service and covers:

- DSProtect solution availability, including software, hardware, and networks operated by Digital Sense to deliver the service.

The customer is responsible for incident and problem management activities including detection, classification, escalation, and resolution relating to:

- Customer-operated platforms, applications, or services leveraging the DSProtect service;

- Customer-operated endpoints (such as Internet browsers or web applications) that use DSProtect; and

- Customer-operated networks that the above-mentioned services used to access DSProtect.

Service Description	DS	Customer
Incident Management		
Maintain Digital Sense Incident Management processes and policies	✓	
Incident creation in Service Desk Tracking System. Each time an authorised person contacts the Service Desk and provide a unique reference number for each case	✓	
Provide logs and route support for incidents and service requests according to the escalation process	✓	

	✓	
Open incident tickets for genuine automated alerts	✓	
Assign incident priority to each incident	✓	
Perform incident notification according to the escalation management procedures	✓	
Evaluate incident impact to SLA	✓	
Resolve incidents, interface with third parties where required to assist in incident resolution	✓	
Close incidents upon confirmation of successful resolution	✓	
Problem Management		
Maintain customer Problem Management processes and policies		✓
Compile RCA post-incident	✓	
Review and present RCA Findings	✓	
Review incident and RCA information	✓	
Identify problems, diagnose root causes and initiate actions to improve or correct the problem including interface with third parties as required to resolve problems	✓	
Adopt RFC process for Problem Management to link with change control	✓	
Periodic trending analysis of problems based on a review of #, types and status	✓	
Report on problem management activity	✓	

Table 11 - Incident and Problem Management

3.7 SECURITY

The end-to-end security of the DSProtect solution is shared between Digital Sense and the customer. Digital Sense will provide the security for the aspects of DSProtect over which it has sole physical, logical and administrative level control. The customer is responsible for the aspects of the service over which it has administrative level access or control. The primary areas of responsibility between Digital Sense and the customer is detailed below:

Digital Sense will use commercially reasonable efforts to provide:

- Physical security of data centre locations hosting DSProtect;

- Information security of the DSProtect platform, including operating environment, account security, and security of supporting infrastructure;

- Network security of the DSProtect platform, including network transit under the control of Digital Sense;

- Security monitoring of the DSProtect platform, including intrusion detection and vulnerability prevention within Digital Sense operated networks; and

- Patching and vulnerability management of the DSProtect platform, including regular security patching of platform vulnerabilities.

The customer is responsible for:

- Information security of all applications, endpoints, and services accessing the DSProtect platform on the customer's behalf;

- Network security of all applications, endpoints, and services accessing the DSProtect platform; and

- Security monitoring of all applications, endpoints, and services accessing the DSProtect platform.

3.7.1 Compromised Infrastructure

Digital Sense reserves the right to suspend servers or any related elements or whole customer accounts if compromised servers are detected. This step is to ensure continued availability of the service and protect Digital Sense's infrastructure and business operations.

4 BUSINESS OPERATIONS

This section summarises the processes for ordering, scaling, renewing, suspending, and terminating the service.

4.1 ORDERING AND INVOICING

Details of ordering and invoicing are included in the standard Digital Sense Master Services Agreement (MSA), available from your Digital Sense account representative.

4.2 RENEWAL

Digital Sense reserves the right to not renew any service offering at the end of its subscription term. If this is the case, Digital Sense will notify you 30 days prior to the end of the subscription term.

4.2.1 Auto-Renewal

The service will be automatically renewed at the end of the subscription term unless you notify Digital Sense in writing 30 days prior to the end of the subscription term.

4.3 SUSPENSION AND RE-ENABLEMENT

If an account is suspended for non-payment or any other reason, Digital Sense will restrict access to all service components and block all traffic across its public IP addresses. Digital Sense will retain these service components with configurations and data intact until the issue is resolved or the subscription

expires or is terminated. Service re-enablement will be initiated immediately upon resolution of the account issues that led to the suspension. Public IP traffic blocks will also be removed.

4.4   TERMINATION

Upon termination of the contract, customer data will be retained on the DSProtect platform for 30 days. It is the responsibility of the customer to work with Digital Sense to obtain a copy of the data (if required) prior to its removal from the service.

5   GLOSSARY

The following table provides a brief glossary of terms used in this document.

Term	Definition
CDM	Cloud Data Management. Rubrik's platform for data protection and other data operations.
DA	Disaster Avoidance
DPaaS	Data Protection as a Service
DR	Disaster Recovery
LTR	Long-Term Retention
NAS	Network-Attached Storage
NFS	Network File System. A file protocol for accessing resources over a network.
Polaris	Rubrik's SaaS-based management tool.
RCA	Root Cause Analysis
RPO	Recovery Point Objective. Reflects the amount of data that potentially could be lost during a data loss event.
RO / BO	Remote Office / Branch Office. An office that is located in a different or remote geographical area to that of the company headquarters.
RTO	Recovery Time Objective. Refers to the amount of time it takes to recover from a data loss event and how long it takes to return to service.
SAN	Storage Area Network
SLA	Service Level Agreement
SMB	Server Message Block. A file protocol for accessing resources over a network.
STR	Short Term Retention
VCD	VMware Cloud Director
VLAN	Virtual Logical Area Network
VM	Virtual Machine

Table 12 - Glossary of Terms