

PROACT

G-Cloud 15

Proact Backup as a Service
(BaaS) Service Definition

Document control

Document type	Public - Freely Distributable		
Company	Proact IT UK		
Address	Proact IT UK Grayson House, Venture Way, Chesterfield, Derbyshire, S41 8NE		
Telephone	01246 266 300		
Primary contact	bids@proact.oc.uk	Role	N/A

Revision history

Issue date	Author	Version	Revision description
25/11/2025	Colin Abram	V1	Document Upload

Proact Backup as a Service (BaaS) Service Definition

Proact provide a range of backup services to provide data protection for customer's data and systems. The service includes the provision of compute, storage and network resources to facilitate the backup of customer data offsite to Proact's data centre. The Backup services provided include:

- Backup as a Service Enterprise – Heterogenous data protection for customer's systems and data
- Backup as a Service Virtual – Data protection for virtual infrastructure
- Backup as a Service O365 – Data protection for customer's Microsoft 365 subscriptions
- Backup as a Service Secure Storage Vault – Data protection for customer's NetApp storage systems

Backup as a Service provides the following deliverables:

- Compute, storage and networking resources required to provide data protection, hosted in a Proact data centre. Where required Proact will provide an onsite disk repository for short term backup retention at the customer's data centre.
- Provision of software including management to protect data
- Managed backup and recovery
- 24x7x365 Proact Service desk
- 24x7x365 automated monitoring
- Self-service support and self-service monitoring portals
- Management, including break-fix activities, on underlying hardware
- Incident management and resolution
- Problem management
- Change and configuration management
- A named Service delivery manager to co-ordinate deliver and provide regular customer reports

This document contains the following appendices detailing the service definitions for the Backup services:

- [Appendix 1 – Backup as a Service - Enterprise](#)
- [Appendix 2 – Backup as a Service – Virtual](#)
- [Appendix 3 – Backup as a Service – O365](#)
- [Appendix 4 – Backup as a Service – Secure Storage Vault](#)

Appendix 1 - Backup as a Service – Enterprise Service Definition

1.1 - Service Overview

BaaS-E is a backup solution which suits environments with data to be backed up from; physical servers, virtual servers, storage arrays, Office 365 and hyperscale public cloud environments.

With BaaS-E a customer may backup data from one of multiple 'Source' locations and keep one or more copies of that data at, one or more, defined 'Targets'. This design allows for multiple copies of the customer's data to be retained to meet the customer's retention and resilience requirements. The service support two Immutable Targets held within Proact datacentres, one called Immutable Shared Data Vault (which is a feature of BaaS-E) and also utilising Proact's Object Storage as Service product, to provide an Immutable Object Vault. The customer can also utilise an external Public Cloud Object Store with Immutable functionality if they prefer.

Source – This is the data the customer wishes to backup. Source data may will be held on the CIs in scope for the service and can exist in a single location or multiple locations – such as; one or more customer datacentres, satellite sites, Proact's Hybrid Cloud (PHC), cloud environments (such as AWS and Azure) and Office365.

Target – Is a destination for a backup copy of the customers source CI data. Proact BaaS-E supports storing data in multiple target destinations so a customer can have multiple copies for resilience. Targets represent either 'on-site' copies 'off-site' copies or 'extended retention' copies of the backup data as defined below.

BaaS-E requires that at least one 'Off-Site' target be included in the solution:

On-Site

- A customer's datacentre with a Dedicated Data Vault (DDV) appliance
- A customer's PHC environment with a DDV appliance
- A customer's cloud environment with a Public Cloud Dedicated Data Vault (PCDDV) instance

Off-Site

- Proact's primary BaaS DC, with a Shared Data Vault (SDV)
- Proact's secondary BaaS DC, with an Immutable Shared Data Vault (ISDV)
- Proact's secondary BaaS DC, with a Shared Data Vault
- Proact's secondary BaaS DC, with a Proact OSTaaS Immutable Object Vault

Extended Retention

- Public Cloud Object Vault (PCOV) - AWS S3/Azure Blob
- Proact's secondary BaaS DC, with a Proact OSTaaS Object Vault

1.2 - Service Types

The Backup as a Service – Enterprise (BaaS-E) is delivered with a single service type:

Service type	Service type summary
BaaS-E	Proact provide a fully monitored and managed backup solution for a customer source data. BaaS-E supports multiple copies of a customer's data held at multiple target locations and is suited to environments where data will be backed up from; physical servers, virtual servers, storage arrays, hyperscale public cloud environments and Office 365. This is a pay-as-you-use service, sized based upon the servers, agents and instances backed up, the data transferred and the storage consumed at Proact for the customer's required retention periods.

1.3 - Service Options

The table below sets out the service options available within BaaS-E.

The services provided by Proact will be referenced in the charging tables in section 3 of the Service Specification Document.

Option name	Option description
BaaS Enterprise Virtual Agent	The number of Virtual Machine OS/File System backups in scope. The method of backup (i.e. agent or agentless) is not relevant.
BaaS Enterprise Application Agent	The number of servers (virtual or physical) that require Application Consistent backups to be taken (i.e. Microsoft SQL, MS Exchange, Oracle DB, etc.). Where the application is split across multiple servers (i.e. a Cluster), each server will require it's own agent.
BaaS Enterprise File System/NAS Agent	The number of physical file servers, or NAS controller backups in scope. This is based upon IP address, not controller or server hardware. Where a NAS Controller hosts multiple IP addresses for file services, a separate agent is required for each IP.
BaaS Enterprise O365 User	The number of Microsoft Office365 Active User subscriptions that require protection. A single user license will protect Exchange Online, SharePoint, Teams and OneDrive for Business for that user.
BaaS Enterprise Capacity	The backup storage consumed within one (or more) Proact Shared Data Vault/s. Where data is stored at both Proact's primary and Proact's secondary SDVs, the storage for both vaults will be combined.
BaaS Enterprise Immutable Capacity	The backup storage consumed within Proact Immutable Shared Data Vault.
BaaS Enterprise Managed Dedicated Vault	The number and tier of DDVs required to store the customer's backup data. DDVs are installed at the customers site for dedicated backup use.
Direct Internet Access	The daily internet bandwidth consumed by backup replication during the customers defined backup replication window. This figure is for data copied to Proact (via the internet) or from Proact's SDV to the customer's public cloud environment for extended retention (PCOV).
MPLS	The inter-site bandwidth consumed by backup replication between Proact's primary SDV and secondary SDV, to provide dual site resilience for backup data.



1.4 - Specific Architecture

This appendix covers detail on deliverables that are specific to this service. This service also includes the deliverables defined in the **Common Service Deliverables** labelled as 'Managed' (MAN).

The responsibility for each deliverable is defined below and colour-keyed for easy review:

Proact Responsibility

Customer Responsibility

Joint Responsibility

1.4.1 - Platform

Deliverable	Description and content summary	Responsibility
Platform	A secure multi-tenant platform for the backup of data held on physical servers, virtual servers, storage arrays, within hyperscale public cloud environments and within Office 365.	Proact
Storage (Proact's datacentre)	Where data is stored within Proact's datacentre, backup data is stored on high-capacity, low-performance multi-tenanted storage provided as a Shared Data Vault (SDV). Proact can store data within two SDVs, one at Proact's primary datacentre and one within Proact's secondary datacentre.	Proact
BaaS Immutable Storage	Immutable Shared Data Vault (ISDV) storage is stored on high-capacity, low-performance multi-tenanted storage, and time locked to prevent modification or deletion of the data, by Proact or the customer, until the assigned time lock has expired. Where possible ISDV data will be stored in a different datacentre to the customer's SDV. The data held in the ISDV is short term and is a duplicate copy of the data held within the SDV.	Proact
OSTaaS Immutable Storage	Where available BaaS-E can combine with Proact's Object Storage as a Service solution to create Immutable Object Vault (OSTaaS-IOV). OSTaaS will be used to provide a storage area (bucket) which will be time locked to prevent modification or deletion of the data, by Proact or the customer, until the assigned time lock has expired. Where possible – OSTaaS-IOV data will be stored in a different datacentre to the customer's SDV. The data held in the OSTaaS-IOV is short term and is a duplicate copy of the data held within the SDV.	Proact
Storage (Customer's datacentre)	Where data is stored within the customer's datacentre, backup data is stored on high-capacity Dedicated Data Vault (DDV) server hardware. The DDV operating system is provided, managed and updated by Proact.	Proact
Customer's datacentre	The customer will be responsible for the providing rack space, redundant power, UPS, network connectivity (including optical cables) and physical security for this hardware for the length of the contract.	Customer
Customer's domain	Proact will not join any DDV OSs into the customer's Windows Active Directory Domain for security and isolation.	Proact

Deliverable	Description and content summary	Responsibility
Storage (Public Cloud)	Public Cloud Block Storage Where data is to be stored within the customer's cloud environment on block-based cloud storage (such as AWS EC2 or Azure Compute), backup data is stored on a Public Cloud Dedicated Data Vault (PCDDV) VM instance running in the customer's cloud environment. Public Cloud Object Storage Bucket Where extended retention data is stored with the customer's cloud environment within an Object Storage service (such as AWS S3/Glacier, Azure BLOB), backup data is stored within a Public Cloud Object Vault (PCOV) which is held within the customer's dedicated object storage 'bucket/s'. All cloud infrastructure provided for BaaS-E by the customer will be maintained for the length of the contract. The customer will take responsibility for the provision, management, maintenance and security of these systems.	Customer

1.4.2 - Components

Deliverable	Description and content summary	Responsibility
Master backup server	A multi-tenanted master backup server deployed by Proact within Proact's datacentre to manage backup jobs and offload the backup process to backup agents and proxies. The master backup server will host and maintain the backup database service. This service will log backup jobs that copy the customer's data from the customer's source CIs, via backup agents and proxies to the backup media agents. The master backup server is replicated to a second Proact datacentre for redundancy.	Proact
Backup agents and proxies	Backup agent and proxy software will be used to perform backup operations on the customer's source CIs and allow for the backup solution to address multiple types business data, for example: Backup Agents - Physical server file systems (Windows/Linux) - SQL Databases - Oracle Databases - Exchange Server Backup Proxies - VMware or Hyper-V VMs - Cloud VMs/Instances - Office365 (Email, SharePoint and OneDrive) - NAS/SAN Storage Arrays The listed above not exhaustive and provided for example. The agents used will vary according to the CIs contracted. Proact will provide the backup agent & proxy software and licenses to deliver the BaaS-E service. The customer will allow for the installation of the required agents/proxies and for the provision of servers/VM/resources for proxy use, for the contract term. The customer is responsible for providing Operating System licenses and Anti-Virus software for any proxy VMs or PCDDV's required.	Joint



Deliverable	Description and content summary	Responsibility
Backup media agents	Media agent servers will be used during the backup tasks. These servers act as the backup engine, transferring data from backup agents/proxies and storing data within dedicated or shared backup storage targets. Proact may use one or more backup media agent servers to enable backup operations, depending on source data location, quantity and complexity. Where required the customer will allow for the installation of the required media agent software and for the provision of servers/VM/resources for media agent use, for the contract term.	Joint
Data storage vaults (Proact)	Backup agents and proxies will copy backup data to one of two targets types. Both these targets types are provided and managed by Proact: Dedicated Data Vaults (DDV) ▪ Installed on the same LAN as the customer's source CIs (on-site) ▪ Performs de-duplication to reduce storage usage ▪ Agents/proxies can backup directly to a DDV ▪ Replicates backups to SDVs to protect off-site ▪ Customers may have multiple DDVs at multiple sites, or multiple DDVs at a single site Shared Data Vaults (SDV) ▪ SDVs provide off-site storage for backup data ▪ Proact provide up to two SDVs, held at geographically different sites for resilience ▪ Performs de-duplication to reduce storage usage ▪ Agents/proxies can backup directly to SDVs to protect off-site ▪ Customer DDV backups can be replicated to SDVs to protect off-site ▪ SDVs can inter-replicate backups for resilience (primary SDV to secondary SDV and vice-versa) ▪ Can replicate to Public Cloud Object Vault (PCOV) for extended retention NOTE: DDV capacity is based upon standard building blocks and allow for stepped expansion. Should additional capacity be required, beyond the initial DDV sizing, further DDVs can be provided at any point during the contract term under a contract change.	Proact
Data storage vault (Customer)	Backup agents/proxies will copy public cloud backup data to a Public Cloud based backup target, provided and managed by the customer: Public Cloud Dedicated Data Vault (PCDDV) ▪ Installed as a Cloud Instance/VM in the customer Public Cloud environment on the same network as the customer's source cloud-based CIs ▪ Agents/proxies can backup directly to a PCDDV ▪ Performs de-duplication to reduce cloud storage usage ▪ Reduces egress from the public cloud ▪ Replicates cloud backups to SDV to protect off-cloud ▪ Customers may have multiple PCDDVs to balance load and capacity	Customer



Deliverable	Description and content summary	Responsibility
Data storage vault (Long term)	For extended retention the following target type can be used: Public Cloud Object Vault (PCOV) ▪ Utilises Public Cloud Object Storage provided by the customer ▪ Performs de-duplication to reduce storage usage (optional) ▪ Replication target for SDV backups for off-site protection ▪ Replication target for DDV backups for off-site protection ▪ For extended retention ▪ Not recommended where large restores could be required.	Customer

1.4.3 - Connectivity

Deliverable	Description and content summary	Responsibility
Customer firewalls	The customer will be required to open specific firewall ports to allow for secure backup data transfer and maintain this configuration for the contract term. Detailed requirements will be provided by Proact during service transition. The customer is required to provide an administrator to perform the firewall configuration.	Customer
Proact firewalls	All internet communication will be performed using Proact's existing firewall infrastructure. Proact manage this centralised firewall, which defines the open ports and blocks unwanted traffic for the entire service.	Proact
Throttling	By default, Proact will not impose throttling on backup traffic to maximise backup throughput. Throttling can be imposed at the customer's request, where there is contention on low bandwidth connections or additional traffic is considered higher priority (such as DR replication). The customer may request that throttling be applied to backup traffic, at any time during the contract period.	Customer
Management Traffic (Proact)	To connect for management of the DDV(s)/PCDDV(s) at the customer site(s), Proact will configure and operate an TLS encrypted tunnel over the Public Internet for management traffic unless a dedicated link or VPN is in place	Proact
Management Traffic (Customer)	The customer is required to provide appropriate technical resource to assist Proact with the initial configuration and any subsequent troubleshooting of the TLS tunnel.	Customer
Self-service restore access	For customers who wish to use self-service restore; two options are available: Self Service Portal – A web-based portal hosted at Proact. Self Service Console – A GUI available for the customer to install. This portal requires install on the customer's administrator's PC. Proact will provide and manage the portal and console software within the operating parameters of the product used. The customer will provide firewall access to the portal and an administrator's PC for console installation, as required.	Joint



Deliverable	Description and content summary	Responsibility
Bandwidth usage	Internet bandwidth is required for all data seeding backup, replication and retrieval activities involving the SDV, unless a dedicated link is in place. The customer is responsible for providing sufficient bandwidth between their site and the SDV for efficient replication. If sufficient bandwidth is not available, having an up to date off-site backup copy will not be achievable. Data change rates and the customer's available bandwidth will dictate the time required for backup /replication/restore tasks and Proact will work with the customer to minimise potential monopolisation of bandwidth by spreading data seeding activities and scheduled backup runs over customer-defined periods of time	Customer
Public cloud transfer usage charges (Customer)	Data transfers related to Public Cloud providers are subject to ingress, egress and other usage charges. Costs for the public cloud environment, whether providing the source for backup or hosting PCOV, will be billed by the customer's Public Cloud provider and are the customer's responsibility.	Customer
Public cloud transfer usage charges (Proact)	Proact will work with the customer to minimise usage charges through the use of compression, de-duplication and bandwidth throttling, to assist the customer in managing usage costs.	Joint
SaaS provider configuration change	Where a SaaS provider used by the service or customer, requires a configuration update from the customer and the lack of update leaves Proact unable to effectively complete operational activities, the customer is responsible for making the required configuration update to re-instate the service.	Customer
Microsoft bandwidth throttling	Microsoft may apply bandwidth throttling to the customer's M365 (O365) service and this may impact the time required to perform a backup each day. If sufficient Microsoft bandwidth is not available to perform the backup, Proact will not be responsible for backups not being completed.	Out of Scope
Interoperability with customer-managed systems	Where this service interacts with any system, application or environment not managed by Proact, it is the customer's responsibility to ensure that it remains compatible with any Proact-managed systems/applications at the hardware, firmware, OS, and application version level – as recommended by Proact or its vendors as best practice.	Customer
Customer credentials	During service start-up, the customer will provide one or more 'service accounts' and their attached passwords with sufficient privileges to allow backup of the CIs in scope. These accounts will be maintained for the length of the agreement. The customer must inform Proact prior to changing the passwords for these service accounts and provide Proact with the new passwords.	Customer
Proact bandwidth capacity	Proact will maintain sufficient bandwidth to accommodate BaaS-E backup traffic	Proact



1.4.4 - Security

Deliverable	Description and content summary	Responsibility
Data encryption	Encryption is applied to all data connections between Proact and their customers. Within all backup targets, backup data is stored in an encrypted format (using a Proact generated passphrase) to ensure security whether data is at-rest or in-flight.	Proact
Anti-virus (Proact)	Proact's BaaS-E platform, incorporates anti-virus protection. The anti-virus protection will not scan any of the customer's data. Proact will provide anti-virus software for physical DDV appliances installed within the customers environment.	Proact
Anti-virus (Customer)	Proact do not provide anti-virus protection for hardware or VMs running within a customer's environment (Proxy VMs or PCDDV cloud VM instances). The customer will be responsible for providing anti-virus protection for these systems. Proact will provide exclusion recommendations for the AV software.	Joint
Audit capability	Proact provide regular reports confirming the status of backup jobs, which together form an audit trail of job success or failure.	Proact
Application consistency	Where requested by the customer, Proact will provide agents that offer application consistent backups for supported applications. It is the customer's responsibility, through the use of test restores, to ensure that this functionality is working as designed and that data consistency is being achieved.	Customer
Data Immutability	Proact will ensure that data held within a ISDV or OSTaaS-IOV will be immutable and both Proact and the customer will not be able to modify, overwrite or delete data stored within these storage areas.	Proact

1.4.5 - Continuity

Deliverable	Description and content summary	Responsibility
Master server redundancy	Proact will replicate the master backup server from Proact's primary datacentre to Proact's secondary datacentre for redundancy. In the event of primary datacentre or master server failure, the replica will be used to re-instate the backup service.	Proact
Backup data redundancy	Proact provides the option to replicate customer backup data from the SDV at Proact's primary datacentre to the SDV at Proact's secondary datacentre or vice versa, for redundancy. In the event of the loss of one site/SDV, the peer SDV can be used for backup and restoration. Where the customer requires redundant backup data, it is their responsibility to request this option. Data held in a single SDV and not replicated will be lost should the SDV or its host site be lost. SDV replication can be introduced to the service at any point during the contract term. The ISDV and OSTaaS-IOV will also keep a redundant copy of the customer's SDV data, but this will be for short term storage only.	Customer



1.4.6 - Licensing

Deliverable	Description and content summary	Responsibility
Service licensing	Proact include the agent/proxy licenses requested for CIs in scope, within the operating parameters of the product used. This licensing includes, but is not limited to: ▪ OS/File data backup for VM or cloud instance ▪ Application backup ▪ NAS/Physical server backup ▪ CIFS/File data backup ▪ Office365 user backup Licenses for additional supported products or applications can be added during the contract term at the customer's request.	Proact
Customers licensing	Where the BaaS-E interacts with any licensed system, application or environment not managed by Proact, it is the customer's responsibility to ensure that licenses for these systems, services and environments are maintained and assigned to the correct CIs to allow for BaaS-E to function. These licenses include, but are not limited to: ▪ VMware Licenses for VMware backup ▪ MS Office Subscriptions for Office365 backup ▪ Amazon Web Service subscriptions ▪ Microsoft Azure subscriptions	Customer

1.5 - Configuration

1.5.1 - Service Capabilities

Deliverable	Description and content summary	Responsibility
Backup source support	The products capable of being protected by this solution are subject to change if the underlying product support changes. The current supported products are set out in Proact's BaaS-E Support Matrix which is available upon request.	Proact
Backup policies	Proact offer flexible policies, configurable per backup target, to meet the customer's contracted requirements, within the operating parameters of the product used. The default policies provide: ▪ Server/VM/Instance & Application Backup – a weekly synthetic full backup plus six daily incremental backups ▪ Storage/Office 365 Backup – initial full backup plus daily incremental forever backups The customer may request modification to the default backup policies, within the operating parameters of the product used, to better meet their needs. These modifications can be made during service transition or from time to time.	Proact
Backup retention	Proact configure and maintain a flexible retention policy to meet the customer's contracted retention requirements, within the operating parameters of the product and consistent with the contract term.	Proact
Immutable retention	Proact configure and maintain a time lock for a copy of the customer's data held within immutable storage (ISDV, OSTaaS-IOV). The time lock will be set to a default of 2 weeks (14 days), the customer can choose, at service commencement, to extend this to a maximum of 63 days(9 weeks). Time lock retention can be adjusted during the contract term, subject to any time lock currently in place. Proact will also configure immutable time locks on customer provided, Public Cloud Object Storage, where required.	Proact



Deliverable	Description and content summary	Responsibility
Backup replication	Proact will replicate backup data between backup targets (DDV, PCDDV and SDV) to meet a customer's retention and resilience requirements. For replication of backups between targets (DDV to SDV, SDV to SDV etc.), de-duplication will be performed to minimise inter-site bandwidth.	Proact
De-duplication	BaaS-E supports de-duplication during backup tasks and during replication of backups between targets. For backup tasks, the use of de-duplication within the source agent/proxy is used to reduce network bandwidth usage and may increase CPU load on the backup source. Proact will work with the customer to optimise the use of de-duplication to best meet the customer's needs during transition. Data held on DDVs, SDV and PCDDVs will be stored in a de-duplicated format (where supported) to save storage space, unless specifically changed at the customer's request.	Proact
De-duplication cache	Where de-duplication is performed by the source in-server agent, a local cache will be required which will consume disk space on the source server. The customer will ensure sufficient disk capacity is available on the source server to retain this cache.	Customer
GDPR Right to Erasure / Be Forgotten	Proact will not undertake the restoration of data from backup for the purposes of data removal under the GDPR right to erasure/ be forgotten requests, where they require: ▪ Restoration of existing backup data to separate storage ▪ Removal of the data to be Erased/Forgotten ▪ Re-backup of that data to be retained ▪ Deletion of the original backup data Under a separate project, Proact can offer professional services to undertake planning and implementation of the above process as per customer reasonable requirements and within the operating parameters of the product used. Prior to commencement of such a project, the customer and Proact will agree the specification and charges for this separate project.	Out of Scope
GDPR Right to Erasure / Be Forgotten requests	It is the customer's responsibility to maintain a register of all data erasure requests and use this to ensure such data is removed again if restored as a result of subsequent data restore requests.	Customer



1.5.2 - Backup Service Methods

Deliverable	Description and content summary	Responsibility
Backup approach	The solution provides two main backup approaches, agent based, and proxy based. Where possible an 'proxy' approach will be used to minimise customer disruption: Proxy based backups (default approach) This approach includes the following methods ▪ Hypervisor VM ▪ Public Cloud Instances/VM ▪ Storage Array backup ▪ Public Cloud Object Storage ▪ Public Cloud Database ▪ Office365 Agent based backups ▪ This approach includes the following methods ▪ Physical servers ▪ Applications servers, requiring application consistency	Proact
Hypervisor VM backup method (Proact)	Hypervisor backup method will protect the VMs at the hypervisor layer, providing OS consistent backups, granular file restore and allowing for the VM estate to be backed up as a single managed entity. With this option agents are not required within each VM. OS consistent backups for Hyper-V VMs where the Hypervisor is connected to the storage array using the SMB protocol and the VMs resides directly on the SMB share are excluded from this method.	Proact
Hypervisor VM backup method (Customers)	Where VMware is used, VMware tools must be installed and up to date, on the VMs running within the environment. If VMware tools is out of date, or not available, VM backups will be only crash consistent. Where a DDV is not installed at the customers site, the customer will be required to host one or more Proxy VMs.	Customer
Public Cloud instances/VM method	Public Cloud proxy backup method will protect Instances/VMs running within a Public Cloud compute infrastructure (e.g. AWS EC2, Microsoft Azure Compute). Backups will be performed at the cloud hypervisor layer, providing crash consistent backups. With this option agents are not required within each Instance/VM. The customer will be required to host one or more Public Cloud Proxy Instances/VMs within their cloud infrastructure. Where application or OS consistency is required, an in-server agent should be used.	Proact
Public Cloud database method	Public Cloud database backup method will protect database services running within a Public Cloud (e.g. AWS RDS, Microsoft Azure SQL). Backups will be performed at the database layer, providing application consistency. Each backup will be a 'full' database dump. The customer will be required to host one or more Public Cloud Proxy Instances/VMs within their cloud infrastructure.	Proact
Public Cloud Object Storage method	Public Cloud Object Storage backup method will protect cloud based object storage services (e.g. AWS S3, Microsoft Azure Blob). Backups will be performed at the object layer, providing file consistency. The initial backup will be a full backup with subsequent backups being incremental forever. The customer will be required to host one or more Public Cloud Proxy Instances/VMs within their cloud infrastructure.	Proact



Deliverable	Description and content summary	Responsibility
Public Cloud O365 method	The Public Cloud M365 (O365) Backup will backup business data held in Microsoft Office 365. The service will cover the primary O365 services that retain business data: - Exchange Online - SharePoint Online (Including Teams) - OneDrive for Business Backups will provide file consistency. The initial backup will be a full backup with subsequent backups being incremental forever.	Proact
In-server agent method	In-Server agents are used to backup physical servers and application servers. The in-server agent method requires that an agent be installed into the OS of the physical server or VM to be protected. This method will provide OS consistent and application consistent backup of the customer's source CIs. There is a limited number of applications, and application versions that support application consistent backup. Details of the applications supported are available in Proact's BaaS-E Support Matrix upon request. Any applications/versions not listed as 'supported' in the support matrix are explicitly excluded. The support matrix is subject to change during the life of the agreement. Where an in-server agent is installed a 'file system' agent will also be installed to protect the server's Operating System (OS)	Proact
Storage Array backup (Proact)	BaaS-E is able to backup storage arrays using two methods: NAS - Used to backup CIFS and NFS data stored on compatible NAS devices. NFS data backup is only supported in <i>mixed-mode</i> when the CIFS protocol can be used to access the file data. Neither LUNs or VMDKs are supported. SAN - Used to backup servers with their storage held on a SAN (for example, NetApp). A SAN proxy will be installed on the SAN attached server and configured to communicate with the storage array.	Proact
Storage Array backup (Customer)	NAS Backup - Where anti-virus (AV) is configured, a duplicate set of shares must be created with AV disabled to increase backup performance. - If the NAS device is configured with file archiving, data backup may trigger a recall. The customer will ensure that the archive program will be configured to exclude recalls from either a certain IP address or certain users - Where a DDV is not installed at the customers site, or the customer has more than two controllers, the customer will be required to host one or more NAS Proxy VMs. SAN backup - Where a DDV is not installed at the customers site, or the customer has more than two controllers, the customer will be required to host one or more SAN Proxy VMs. - Where the SAN method is required, the backup server/proxy will require access to the same storage network as the source servers.	Customer
Flat file dumps	Proact does not support flat file dumps of application data. Performing dumps is both bandwidth and storage intensive for backup data and can impact backup and restore performance and scheduling.	Out of Scope
Agent conflicts	To avoid potential conflict between backup applications, the customer will remove any existing backup agents from each backup source CI in scope.	Customer



Deliverable	Description and content summary	Responsibility
Existing replication	Where a customer is using Storage Array backup and a storage vendor's application consistency backup tools are used for disaster recovery (DR), the customer must: ▪ Configure the vendor's tools to perform application consistent backups that do not truncate the logs, update the applications catalogue or otherwise interfere with Proact's backup process. ▪ Ensure that the backup process and the DR snapshot/replication never run at the same time.	Customer

1.5.3 - Restore Service Methods

Deliverable	Description and content summary	Responsibility
Restore requests	The customer may request that a restore is initiated through a service request to Proact's service desk.	Customer
Restore approach	Multiple restore methods are available. For each restore request the method used will vary based upon: ▪ The backup method used ▪ The source CI backed up ▪ The customer's requirements from the restore Proact and the customer will agree on the best method for the restore during response to the restore request. The restore methods are: Hypervisor Proxy Backup ▪ File/Folder Restore ▪ Single-Item Restore ▪ Volume Restore ▪ VM Restore Public Cloud Proxy Backup ▪ File/Folder Restore ▪ Volume Restore ▪ VM Restore In-Server Agent Backup ▪ File/Folder Restore ▪ Single-Item Restore ▪ Volume Restore Storage Array Backup NAS ▪ File/Folder Restore Storage Array Backup SAN ▪ SAN Restore Public Cloud Office 365 Backup ▪ Single-Item Restore	Proact
Bare metal restore	Proact does not support bare metal restores (Restoring a physical machine back to new physical or virtual hardware). If a bare metal restore is required, Proact can offer standalone Professional Services to undertake planning and implementation of the recovery in-line with the customer's needs.	Out of Scope
Self-service restore	Self-service restore is performed by the customer and without Proact's interaction or knowledge and is not bound by Response Time SLAs, as Proact is not involved in the restore process.	Customer



Deliverable	Description and content summary	Responsibility
File/Folder restore method	The File/Folder restore method will return individual files, groups of files and folders from the backup copy, back to the original source CI or to a different source CI within the operating parameters of the product used.	Proact
Single-Item restore method	The Single-Item restore method will return application data and metadata from the backup copy, back to the original source CI or to a different compatible source CI within the operating parameters of the product used. This method will also be used for restoration of all Office365 data held in Exchange Online, OneDrive for Business, SharePoint Online and Teams.	Proact
Office 365 customer transfer	When requested to perform an Office 365 restore the customer and Proact will review the restore options, within the operating parameters of the product used and define the location of the restore and if the current O365 data should be overwritten, or if the data should be transferred to the customer directly. Data returned to the customer will first be placed within a password protected zip archive. The zip archive will be returned to the customer in one of two ways: ▪ Zip archives of up to 50MB can be returned via email to an existing account within the customer's Office365 environment. ▪ Zip archives of up to 1TB will be made available via an 'out of band' restore method that provide encrypted file transfer (such as OneDriveFB or DropBox). The customer will define and supply the file transferred method to be used for this option. The password for the zip archive will be sent via SMS to the receiving customer's pre-recorded contact mobile number. This process will ensure two factor authentication for the restored data regardless of the restore process chosen. Proact will not be responsible for the speed of the restore process, or the transfer time from Proact to the customer's environment during a restore.	Proact
Volume restore method	The Volume Restore method will return entire volumes/disks from the backup copy, back to the original source CI or to a different source CI within the operating parameters of the product used.	Proact
VM restore method	The VM Restore method will return an entire VM from the backup copy, either overwriting the existing VM or restoring to a new VM. The VM can also be restored to a separate public cloud/hypervisor environment within the operating parameters of the product used.	Proact
Storage Array SAN restore method	The SAN Restore method will restore data back to the source SAN storage array. Restoration of data from a SAN backup is always to a pre-existing LUN. If the entire LUN is lost from the array, the customer must enable restore by creating and mounting an empty LUN for restoration.	Joint
Service best practice	It is the customer's responsibility to act upon Proact best practice recommendations delivered during service review meetings or from time to time, to minimise the possibility of exceptional restore delays/failures.	Customer



Deliverable	Description and content summary	Responsibility
Exceptional restore delays/failures	Where the restore of an individual source takes over 48 hours to complete, or fails due to one or more of the below: - Storage performance - Available bandwidth - Application configuration - Customer source environment state Proact Professional Services will offer to undertake planning and implementation of the recovery in-line with the customer's needs, as a separate project. Prior to commencement, the customer and Proact will agree the charges for this separate project.	Out of Scope
Restore space	The customer will ensure that there is sufficient storage space available to restore their CIs.	Customer

1.6 - Service Deliverables

1.6.1 - Service Monitoring

The following provides an overview of the specific monitoring provided for the service. Proact's standard monitoring deliverables are provided in the Common Service Deliverables appendix.

Deliverable	Description and content summary	Responsibility
Monitored items	- Backup job status, including failed backups - The quantity of source servers/systems protected for licensing purposes. Proact do not actively monitor agent software, proxy VMs or client devices, customer server/applications as part of this service.	Proact

1.6.1.1 - Operational Activities

Deliverable	Description and content summary	Responsibility
Job failure response	Proact monitor the success state of backup jobs using the monitoring platform, which: - Generates alerts for failed backup jobs - Forwards alerts to the Proact service desk Proact will ensure that any jobs which have failed are investigated and where appropriate, re-run.	Proact
Job failure troubleshooting	For repeat failures, Proact will contact the customer and both parties will jointly troubleshoot the problem.	Joint
Backup reporting	Proact provide reports confirming the status of backup jobs.	Proact
Restore testing account	The customer will provide one or more user accounts that can be used for restore testing for the CIs in scope. These accounts will be agreed by the customer at service start-up and documented within the SOM.	Customer



Deliverable	Description and content summary	Responsibility
Restore testing (Proact)	Proact will undertake two scheduled restore tests in each twelve-month period (dated from the service commencement). Where a Dedicated Data Vault is installed at the customer's site, Proact will restore, from that vault, up to a maximum of 100GB of business data per source during each test. Where the data is held off-site, restore size will be limited by bandwidth availability. Where there is insufficient bandwidth, or bandwidth contention, for a 2 hour restore task then a subset of the customer's data will be restored in the test and this may require a different restore method, such as 'File/Folder' or 'Single Item' restore. All test restores will be performed out of place, not overwriting the customer's existing data. Proact will undertake initial restore tests during the service transition phase. These tests will represent one of the two tests allowed in the first 12-month period.	Proact
Restore testing (Customer)	The customer will nominate 3 data sources for each scheduled restore test. Proact recommend that these restore tests be taken from different restore approaches and methods where multiple restore approaches and methods are in use by the customer. Where a successful restore has been performed within two months of a scheduled restore test of a defined approach/method, that successful restore shall constitute a successful test for a given approach/method and Proact recommends this approach/method not be repeated in the next scheduled test.	Customer
Restore testing (Bare metal)	Proact does not support restore testing of complete bare metal restores (Restoring a physical machine back to new physical or virtual hardware) as part of restore testing. This process is both time and resource intensive. Restoration of a subset of the physical server backup data such as 'File/Folder' or 'Single Item' is supported for testing, as defined above. Where a complete bare metal restore is required, Proact Professional Services will offer to undertake planning and implementation of the recovery in-line with the customer's needs, as a separate project. Prior to commencement, the customer and Proact will agree the charges for this separate project. The customer will be responsible for providing the restore target hardware.	Out of Scope
Restore validation	The customer will confirm that restored data works as expected.	Customer

1.7 - Service Upgrades

Deliverable	Description and content summary	Responsibility
Upgrades and new features	This service is a multi-tenant platform provided by Proact. All upgrades, or enablement of new features, is at the sole discretion of Proact.	Proact



1.8 - Service Specific Reporting

Deliverable	Description and content summary	Responsible
Backup reporting	Proact will provide automated reports, within the operating parameters of the product used, confirming the status of backup jobs, at the customer's request.	Proact
Service review report (BaaS-E)	Within the service review report, Proact will include technical statistics, observations and recommendations regarding the service, in relation to: ▪ Backup service capacity ▪ Backup CI usage ▪ Bandwidth usage Note: The content listed above is an example and is subject to change.	Proact
Service review meeting	Proact will organise service review meetings, by teleconference, at a schedule agreed between both parties, but no more than once per quarter. These meetings will discuss the service review report content.	Proact

1.9 - Acceptance Criteria

Below are the defined service acceptance criteria for this service. Invoicing for the service(s) will commence once the following criteria have been met:

Associated Deliverable	Description and content summary	Responsibility
Storage (Customer's Datacentre)	Proact have deployed all the Local Vaults in scope of the customer's source site(s), or, by mutual agreement, a subset of those, and each deployed vault can successfully communicate with Proact's BaaS-E platform.	Proact
Storage (Proact's Datacentre)	Proact have deployed all SDVs in scope in a Proact datacenter, and the SDVs can successfully communicate with Proact's BaaS-E platform	Proact
Backup approach	Successful initial full backup (with no errors) and at least one subsequent scheduled incremental backup to the initial backup target of one of each of the following backup approaches, where appropriate and in scope, and to a maximum size of 100GB in total: ▪ Proxy based backup ▪ Agent based backup	Proact
Backup replication	Where a DDV or PCDDV is installed at the customers source site(s) and the initial full backup, from the 'Backup approach' deliverable, have been successfully replicated from the initial backup target to a second backup target.	Proact
Restore testing (Proact)	Proact have confirmed that data has been successfully restored from the initial backup target, using one of each of the restore approaches available that are applicable to the customer's backup and within the capabilities of the product. Each backup will always be restored to a separate location on the customer's source site.	Proact
Restore testing (Shared Data Vault)	For data held in the 'off-site' in an SDV, Proact have confirmed that restore data is successfully transferred from the SDV to the customers site once a restore task is started. Where bandwidth is limited, or contended, the restore task can be cancelled once data is evident at the customer's site. Each backup will always be restored to a separate location on the customer's source site.	Proact



Associated Deliverable	Description and content summary	Responsibility
Vault Monitoring	Where a DDV or a PCDDV are deployed, Proact are monitoring successfully the state of each vault, and monitoring alerts for these are being sent to Proact's Service Desk for investigation.	Proact
Job Monitoring	Proact are monitoring successfully the state of scheduled backup jobs, and monitoring alerts for failed jobs are being sent to Proact's Service Desk for investigation.	Proact
Self-service portal access	The customer has at least one administrator account (and associated password) that has access to the Self-service portal to view job configuration and status and to initiate restores	Proact
Backup reporting	Proact have scheduled reports confirming the status of backup jobs internally, and where requested, at least one report has been delivered to the customer	Proact

1.10 - Vendor Terms

The services described in this Services Specification will be subject to the vendor terms set out in the table below.

These terms are available in full at <https://www.proact.eu/en/about-us/terms-and-conditions/vendor-terms/>.

Vendor Name
Commvault

1.11 - Service Level Agreement

The below tables show the service levels Proact will endeavour to provide for this service. These levels relate to this specific service and are in addition to the Common Service Levels detailed in 1.12. Where a service level provided here is comparable with the Common Service Levels detailed in 1.12, the level stated here will take precedence for this service.

1.11.1 - Availability Service Levels

Service	SLA	Monthly SLA Description	Measurement
BaaS-E	99.5%	The service will be available for at least 99.5% of each month	The BaaS Platform will be available if the Shared Data Vault and any associated Backup Software located in Proact's data centre responds to Proact's monitoring software
Comms – Internet	99.95%	The internet connectivity will be available for at least 99.95% of each month	The internet connectivity will be available if Proact's monitoring software can access commonly available web pages using the communications link.
BaaS-E Public Cloud Object Vault	N/A	Availability for this service will be dictated by the service level agreement provided by the customer's own Public Cloud provider	The service availability will be measured according to the Public Cloud provider described measurement. Proact is not accountable for the SLA of the selected Public Cloud provider.



Appendix 2 - Backup as a Service – Virtual Service Definition

2.1 - Service Overview

Proact's Backup as a Service Virtual (BaaS-V) offering provides backup solution within Proact's DC, for customers to store their backup data. BaaS-V is provided in two separate product types:

- Managed Backup
- Unmanaged Remote Vault.

In both product types the solution

- Stores customer data encrypted in a dedicated backup vault in accordance with customer protection requirements
- Transfers data using encrypted links
- Employs de-duplication and compression for efficiency

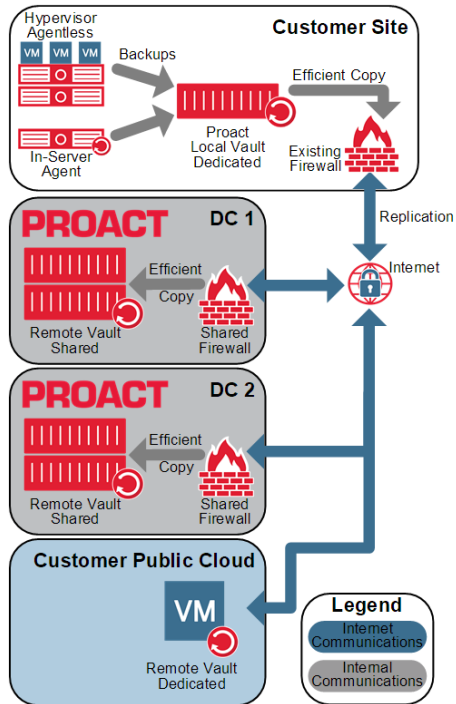
Managed Backup is a fully managed service, designed to replace an existing legacy backup application or replace a cloud-based backup offering. Managed Backup is suited to environments with data to be backed up from; physical servers, virtual servers and hyperscale public cloud environments. Proact will provide, where required, managed hardware appliances (Local Vaults), which will be installed within the customer's environment. These vaults store local backups of the customer's data and provide fast restore capabilities.

With Unmanaged Backup, the customer will license, run and manage their own 'Veeam Backup and Replication Solution', within Proact's DC providing an off-site location that the customer will use to store either short-term or long-term backup data. With Unmanaged Backup, the customer will monitor and manage the backup solution and perform any restores.

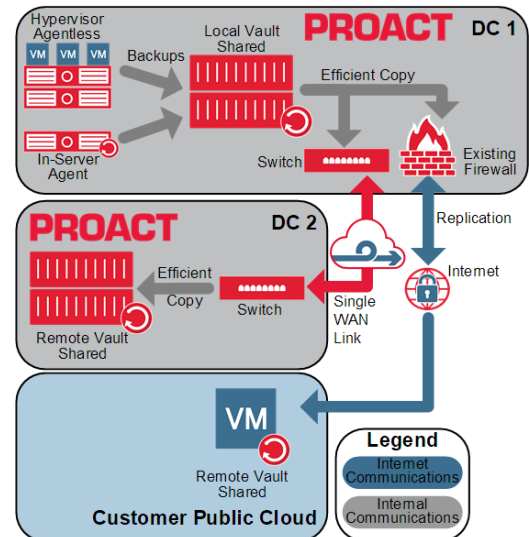
2.1.1 - Service Diagrams

The diagrams below provide solution overviews for each architecture option of the **Managed Backup** package and for the **Unmanaged Remote Vault** package. Each diagram includes all possible data vaults. The actual data vaults available will vary depending on the selected deployment.

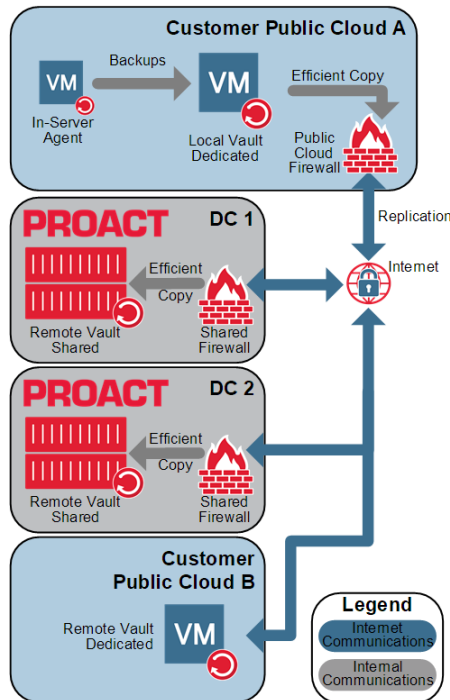
Managed Backup - Customer Datacentre



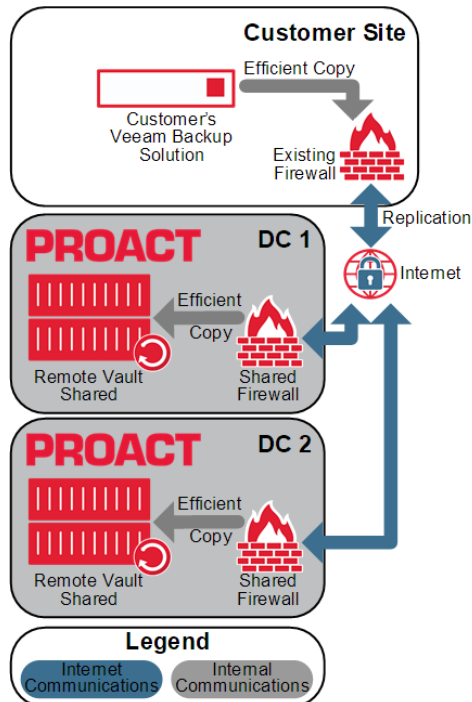
Managed Backup – Proact Datacentre



Managed Backup - Public Cloud



Unmanaged Remote Vault



2.2 - Service Types

The Backup as a Service – Virtual (BaaS-V) is delivered with two mutually exclusive service types:

Service type	Type number	Service type summary
BaaS-V Managed Backup	1	Proact provide a managed backup solution for source data residing in the customer's datacentre, Proact Hybrid Cloud or Public Cloud. The solution supports multiple copies of a customer's data held in a Local Vault, in the same location as the source data, and in shared Remote Vaults held within multiple Proact DCs. Where requested, Proact will provide dedicated backup storage hardware (Local Vaults) which will be installed within the customer's environment to provide faster backup and restore. This is a pay-as-you-use service, sized based upon the servers, agents backed up, Local Vault hardware installed, the data transferred (bandwidth), and the Remote Vault storage consumed for the customer's required retention periods.
BaaS-V Unmanaged Remote Vault	2	Proact allows customers with existing Veeam Backup & Replication (VBR) or Veeam Agent for Windows (VAW) software in their own datacentres to create additional off-site copies of backup data in shared Remote Vaults in up to two Proact datacentres (in the form of Veeam Cloud Connect repositories). The repositories are provided as unmanaged storage containers, where the customer retains full responsibility for management and operation of their own Veeam deployments, and for all backup and restore operations This is a pay-as-you-use service, sold on the data transferred (bandwidth), and the storage consumed at Proact for the customer's required retention periods.

1.1 - Service Options

The table below sets out the service options available within BaaS-V.

The services provided by Proact will be referenced in the charging tables in section 3 of the Service Specification Document.

Option name	Type	Option description
BaaS Virtual Physical Agent	1	The number of physical servers that require backups to be taken. A separate agent is required for each physical server.
BaaS Virtual Virtual Agent	1	The number of virtual machines that require backups to be taken (i.e. VMware or Hyper-V VMs). A separate agent is required for each VM.
BaaS Virtual Public Cloud Virtual Agent	1	The number of virtual machines that require backups to be taken that currently reside with a Public Cloud provider (i.e. AWS EC2, Microsoft Azure). A separate agent is required for each VM.
BaaS Virtual Cloud Connect Physical Agent	2	The number of customer physical servers that will have their backup data replicated to the Unmanaged Remote Vault. A separate agent is required for each physical server.
BaaS Virtual Cloud Connect Virtual Agent	2	The number of customer virtual machines that will have their backup data replicated to the Unmanaged Remote Vault. A separate agent is required for each virtual machine.
BaaS Virtual Cloud Connect Public Cloud Virtual Agent	2	The number of customer virtual machines that reside in the Public Cloud (i.e. AWS EC2 and Azure Compute) that will have their backup data replicated to the Unmanaged Remote Vault. A separate agent is required for each cloud virtual machine.
BaaS Virtual Capacity	ALL	The backup storage consumed within one (or more) Proact remote vaults. The storage consumed will include any configured storage efficiencies (de-duplication and compression) to reduce the overall storage required. Where data is stored at both Proact's primary and Proact's secondary remote vaults, the storage for both vaults will be combined.
BaaS Virtual Managed Dedicated Vault	1	The number and tier of local vaults required to store the customer's backup data. Local vaults are installed at the customers site for dedicated backup use.
Direct Internet Access	ALL	The daily internet bandwidth consumed by backup data replicating to Proact's remote vault, during the customers defined backup replication window.
MPLS	ALL	The inter-site bandwidth consumed by backup replication between Proact's primary remote vault and secondary remote vault, to provide dual site resilience for backup data.



2.3 - Specific Architecture

This appendix covers detail on deliverables that are specific to this service. This service also includes the deliverables defined in the **Common Service Deliverables** labelled as 'Managed' (**MAN**).

The responsibility for each deliverable is defined below and colour-keyed for easy review:

Proact Responsibility	Customer Responsibility	Joint Responsibility
-----------------------	-------------------------	----------------------

2.3.1 - Platform

Deliverable	Type	Description and content summary	Responsibility
Platform	ALL	A secure multi-tenant platform for the backup of data held on physical servers, virtual servers and within hyperscale public cloud environments.	Proact
Storage (Proact's datacentre)	ALL	Where data is stored within Proact's datacentre, backup data is stored on high-capacity, low-performance multi-tenanted storage systems called Remote Vaults. Proact can store data within two Remote Vaults, one at Proact's primary datacentre and one within Proact's secondary datacentre.	Proact
Storage (Customer's datacentre)	1	Where data is stored within the customer's datacentre, backup data is stored on high-capacity Local Vault server hardware and operating system, provided, supported and managed by Proact.	Proact
Customer's datacentre	1	Where a Local Vault is requested, the customer will be responsible for the providing rack space, redundant power, UPS, network connectivity (including optical cables) and physically security for this hardware for the length of the contract.	Customer
Storage (Public Cloud)	1	Public Cloud Block Storage Where data is to be stored within the customer's cloud environment on block-based cloud storage (such as AWS EC2 or Azure Compute), backup data is stored on a Public Cloud Local Vault instance running in the customer's cloud environment. All cloud infrastructure provided for BaaS-V by the customer will be maintained for the length of the contract. The customer will take responsibility for the provision, management, maintenance and security of these systems.	Customer



2.3.2 - Components

Deliverable	Type	Description and content summary	Responsibility
Master backup server (Proact)	1	Where Hypervisor Agentless Backup is performed a master backup server will be deployed by Proact at each of the customers geographically separate sites. The master backup server will manage backup jobs and offload the backup process to backup agents and proxies. The master backup server will host and maintain the backup database service. This service will log backup jobs that copy the customer's data from the customer's source CIs to the backup storage vaults. Proact will backup the configuration of the Master Backup Server on a regular basis. By default, this backup will contain all encryption keys, and itself be encrypted. The Customer may elect to exclude encryption keys from the configuration backup A master backup server is not required where In-Server Agent Backup only is to be performed.	Proact
Master backup server (Customer)	1	The master backup server will be located on a virtual machine (VM) running on the customer's source Hypervisor environment. The customer will provide the required master backup server VM, and required hypervisor resources, for the term of the contract. The customer is responsible for providing Operating System licenses and anti-virus protection for the master backup server.	Customer
Backup server database (Proact)	1	The master backup server requires a Microsoft SQL Server database as a store for the configuration information. By default, the Microsoft SQL Server will run on the same Master Backup Server VM, although the customer can choose to run the Microsoft SQL Server on a separate 'customer managed' SQL server. Microsoft SQL Server Express 2017 will be used as the database by default and is appropriate for environments where there are 500 VMs to backup or 50TB of source data.	Proact
Backup server database (Customer)	1	For larger environments, Microsoft SQL Server Standard/Enterprise will be required for performance reasons. The customer will provide a Microsoft SQL Server Standard/Enterprise environment or license, for the term of the contract, where the following conditions are met: - More than 500 VMs to be backed up - The SQL Server database is 10GB or larger - The customer requires 'SQL Server' encryption - The customer requires SQL table partitioning	Customer
Backup proxy server (Proact)	1	Where the Hypervisor Agentless Backup approach is used, backup data will be retrieved from the Hypervisor using a proxy server role which is configured on the Local Vault server (if selected) or on the master backup server. Proact will provide the backup agent software and licenses to deliver the BaaS-V service	Proact



Deliverable	Type	Description and content summary	Responsibility
Backup proxy server (Customer)	1	Proact may recommend that additional proxy servers be created within the customer's environment, to balance the backup load. If this is requested, the customer will provide the proxy server/s, and the required hypervisor resources, for the term of the contract. The customer is responsible for providing Operating System licenses and anti-virus protection the proxy servers.	Customer
Backup agents	1	Where the In-Server Agent Backup approach is used, a backup agent, installed on the customer source CI will be used to perform backup operations. This allows for backups to be performed for servers which are not running on a Hypervisor farm such a physical servers or Public Cloud servers/instances. Proact will provide the backup agent software and licenses to deliver the BaaS-V service. The customer will allow for the installation and upgrade of the required agents for the contract term.	Joint
Data storage vaults (Proact)	1	Backup agents and proxies will copy backup data to one of two vault types. Both these vault types are provided and managed by Proact: Local Vault ▪ Dedicated backup hardware, installed within the same environment as the customer's source CIs (on-site) ▪ Performs de-duplication to reduce storage usage ▪ Agents/proxies can backup directly to a Local Vault ▪ Replicates backups to one or more Remote Vaults to protect off-site ▪ Customers may have multiple Local Vaults at multiple sites, or multiple Local Vaults at a single site Remote Vault ▪ High capacity storage systems, held at Proact and providing off-site storage for backup data ▪ Proact provide up to two Remote Vaults, held at geographically different sites for resilience ▪ Performs de-duplication to reduce storage usage ▪ Agents/proxies can backup directly to Remote Vaults to protect off-site ▪ Customer Local Vault backups can be replicated to Remote Vaults to protect off-site ▪ Remote Vaults can inter-replicate backups for resilience (primary Remote Vault to secondary Remote Vault and vice-versa) Local Vault capacity is based upon standard building blocks and allow for stepped expansion. Should additional capacity be required, beyond the initial Local Vault sizing, further Local Vaults can be provided at any point during the contract term under a contract change.	Proact



Deliverable	Type	Description and content summary	Responsibility
Data storage vault customer cloud (Customer)	1	Backup agents/proxies can copy public cloud backup data to a Public Cloud based backup vault, rather than a Remote Vault. This cloud-based backup vault will reside on a server/instance created by the customer, via their cloud provider: Public Cloud Local Vault (PCLV) - Installed as a Public Cloud server/instance in the customer Public Cloud environment on the same network as the customer's source cloud-based CIs - Agents/proxies can backup directly to a PCLV - Performs de-duplication to reduce cloud storage usage - Reduces egress from the public cloud - Replicates cloud backups to Remote Vault to protect off-cloud - Customers may have multiple PCLVs to balance load and capacity The customer will be responsible for the creation, configuration and management of the server/instance(s) and OS within the customer's cloud environment.	Customer
Data storage vault customer cloud (Proact)	1	Where backup agents/proxies are deployed in the public cloud within a PCLV. Proact will install and manage the backup software running on the server/instance to enable the backup process.	Proact
Cloud Connect Remote Vault	2	For customers taking Unmanaged Remote Vault, Proact provide Remote Vault storage. These Remote Vaults: - Provide high capacity, low performance storage from Proact's shared platform - Are located in both Proact's primary and secondary datacentres - Store replicated copies of the customer's source VBR backup datasets - VAW can backup directly to Remote Vaults to protect off-site - Any backup data deleted is held in a recycle bin for 3 days prior to permanent deletion, to protect against accidental or malicious deletion VBR supports duplicating data on two separate Remote Vaults, whereas VAW supports backup to a single Remote Vault	Proact
Unmanaged Remote Vault customer environment	2	For customers taking Unmanaged Remote Vault: - The customer existing VBR and/or VAW solution will be used at source - The customer will configure Proact's Remote Vault as an off-site backup repository and use this repository as a target for a backup copy job - The customer will be responsible for configuring the backup job and data retention - The customer will be responsible for ensuring the Veeam components deployed within their environment have sufficient resources to deal with any additional load While the customer may run a different version of VBR and/or VAW to Proact. The customer must not upgrade to a version that is newer than Proact, or more than two major versions behind Proact.	Customer



2.3.3 - Connectivity

Deliverable	Type	Description and content summary	Responsibility
Customer firewalls	ALL	The customer will be required to open specific firewall ports to allow for secure backup data transfer and maintain this configuration for the contract term. Detailed requirements will be provided by Proact during service transition. The customer is required to provide an administrator to perform the firewall configuration.	Customer
Proact firewalls	ALL	All internet communication will be performed using Proact's existing firewall infrastructure. Proact manage this centralised firewall, which defines the open ports and blocks unwanted traffic for the entire service.	Proact
Throttling	1	By default, Proact will not impose throttling on backup traffic to maximise backup throughput. Throttling can be imposed at the customer's request, where there is contention on low bandwidth connections or additional traffic is considered higher priority (such as DR replication). The customer may request that throttling be applied to Hypervisor Agentless Backup traffic, at any time during the contract period.	Customer
Management Traffic	1	To connect for management of the backup solution and Local Vaults at the customer site(s), Proact will: ▪ Configure and operate an IPsec VPN over the Public Internet for management traffic unless a dedicated link is in place ▪ Establish the VPN between Proact's shared-platform firewalls and the customer's dedicated firewall or other shared or tenant firewall in a third-party or Public Cloud environment The customer is required to provide the following: ▪ Appropriate technical resource to assist Proact with the configuration of VPNs ▪ A dedicated public IP address for the VPN connection ▪ In the event of VPN failure, the customer will provide appropriate technical resource to assist, in a remote support session	Joint
Self-service restore access	1	For managed customers who wish to use self-service restore; two options are available: ▪ Self-Service Console for Hypervisor Agentless Backup Accessible via a client which can be installed on the Customer administrators' PC(s) or on a management server provided by the Customer. Alternatively, can be provided as a Web Console Plug-In where the customer uses VMware vCenter. ▪ Veeam Agent for Windows GUI for In-Server Agent Backup Accessed directly through the Operating System of the server(s) on which the agent is installed. Proact will provide and manage the agent and console software within the operating parameters of the product used. The customer will provide an administrator's PC for console installation, as required.	Joint



Deliverable	Type	Description and content summary	Responsibility
Bandwidth usage	ALL	Internet bandwidth is required for all data seeding backup, replication and retrieval activities involving the Remote Vault, unless a dedicated link is in place. The customer is responsible for providing sufficient bandwidth between their site and the Remote Vault for efficient replication. If sufficient bandwidth is not available, having an up-to-date off-site backup copy will not be achievable. Data change rates and the customer's available bandwidth will dictate the time required for backup /replication/restore tasks and Proact will work with the customer to minimise potential monopolisation of bandwidth by spreading data seeding activities and scheduled backup runs over customer-defined periods of time	Customer
Public cloud transfer usage charges (Customer)	ALL	Data transfers related to Public Cloud providers are subject to ingress, egress and other usage charges. Costs for the public cloud environment, whether providing the source for VAW backup or hosting a PCLV, will be billed by the customer's Public Cloud provider and are the customer's responsibility.	Customer
Public cloud transfer usage charges (Proact)	ALL	Proact will work with the customer to minimise usage charges through the use of compression, de-duplication and bandwidth throttling, to assist the customer in managing usage costs.	Joint
SaaS provider configuration change	1	Where a SaaS provider used by the service or customer, requires a configuration update from the customer and the lack of update leaves Proact unable to effectively complete operational activities, the customer is responsible for making the required configuration update to re-instate the service.	Customer
Interoperability with customer-managed systems	ALL	Where this service interacts with any system, application or environment not managed by Proact, it is the customer's responsibility to ensure that it remains compatible with any Proact-managed systems/applications at the hardware, firmware, OS, and application version level – as recommended by Proact or its vendors as best practice.	Customer
Customer credentials	1	During service start-up, the customer will provide one or more 'service accounts' and their attached passwords with sufficient privileges to allow backup of the CIs in scope. These accounts will be maintained for the length of the agreement. The customer must inform Proact prior to changing the passwords for these service accounts and provide Proact with the new passwords.	Customer
Proact bandwidth capacity	ALL	Proact will maintain sufficient bandwidth to accommodate BaaS-V backup traffic	Proact

2.3.4 - Security

Deliverable	Type	Description and content summary	Responsibility
Unmanaged Remote Vault access (Proact)	2	For customers using Unmanaged Remote Vault, Proact will provide a secure 'username and password' to provide the customer with access to their dedicated storage area within the 'Cloud Connect' shared environment.	Proact



Deliverable	Type	Description and content summary	Responsibility
Unmanaged Remote Vault (Customer)	2	The customer is responsible for entering the username and password into their VBR or VAW GUIs to gain access to their Remote Vault. The customer is also responsible for securing the username and password within their environment as this secures access to their Remote Vault	Customer
Data encryption	1	Encryption is applied to all management and backup transfer connections between Proact and their customers. Within all backup vaults, backup data is stored in an encrypted format (using a passphrase which is unique to the customer) to ensure security whether data is at-rest or in-flight.	Proact
Encryption key management	1	Encryption keys are per customer and stored in the VBR master backup server or on the VAW server located within the customer's site. To prevent the loss of the customer's backup environment from making the backup data unreadable, the passwords for the encryption keys will be stored in one of the following locations, decided by the customer prior to service commencement: ▪ Proact Password Safe – The default and recommend method, Proact store the encryption keys in Proact's password safe in-case of loss of the customer's site. ▪ 3rd Party Guardianship – If the customer would prefer for Proact to have no copy of the encryption key password, the customer can setup and send the keys to a 3rd party guardianship, which would allow Proact or the customer to access the password in-case of loss of the customer's site. ▪ Configuration Backup – A configuration backup is taken and stored in Proact's Remote Vault. The configuration backup will contain the encryption keys and will be secured by a single password. If the customer site is lost, Proact will restore the configuration backup and the customer will be required to enter the configuration backup password. This method is only supported for Hypervisor Agentless Backup.	Joint
Backup encryption (Customer)	2	Proact recommends that all data copied into an Unmanaged Remote Vault is encrypted by the customer. The customer will be responsible for configuring the encryption and ensuring the passwords used to create any encryption keys are stored in a safe location. If the customer loses their backup environment (e.g. VAW server or VBR master server), the customer must provide the encryption key passwords to be able to recover any of the data which has been encrypted in Proact's Unmanaged Remote Vault.	Customer
Anti-virus (Proact)	ALL	BaaS-V platform components held within Proact's DC's incorporate anti-virus protection. The anti-virus protection will not scan any of the customer's data.	Proact
Anti-virus (Customer)	ALL	The customer is responsible for antivirus protection for hardware or VMs running within a customer's environment (Master Server, Agent Server, Proxy servers, Local Vault server or PCLV instances). Proact will provide exclusion recommendations for the AV software.	Joint
Audit capability	1	Proact provide regular reports confirming the status of backup jobs, which together form an audit trail of job success or failure.	Proact



2.3.5 - Continuity

Deliverable	Type	Description and content summary	Responsibility
Master server redundancy	1	Proact will replicate the master backup server configuration the customers site to a Remote Vault for redundancy. In the event of failure or loss of a Master Backup Server, the Customer will deploy a new Virtual Machine, and Proact will restore the most recent configuration backup.	Joint
Backup data redundancy	ALL	Proact provides the option to replicate customer backup data from the Remote Vault at Proact's primary datacentre to the Remote Vault at Proact's secondary datacentre or vice versa, for redundancy. In the event of the loss of one site/Remote Vault, the peer Remote Vault can be used for backup and restoration. Where the customer requires redundant backup data, it is their responsibility to request this option. Data held in a single Remote Vault and not replicated will be lost should the Remote Vault or its host site be lost. Remote Vault replication can be introduced to the service at any point during the contract term.	Customer

2.3.6 - Licensing

Deliverable	Type	Description and content summary	Responsibility
Managed Backup licensing	1	Proact include the licenses requested for CIs in scope, within the operating parameters of the product used. This licensing includes, but is not limited to: Hypervisor Agentless Backup ▪ Hypervisor VM Backup Licenses In-Server Agent Backup ▪ Server Agent Licenses (Physical or Public Cloud server) Licenses for additional supported products or applications can be added during the contract term at the customer's request.	Proact
Unmanaged Remote Vault licensing (Proact)	2	Proact will provide an Unmanaged Data Vault license which is required to store the customer's data in a Remote Vault hosted in Proact's DC. A license is required per server backed up and per Proact Remote Vault utilised.	Proact
Unmanaged Remote Vault licensing (Customer)	2	The customer will provide the appropriate Veeam Backup & Replication (VBR) License (known as a perpetual license) to be able to store VBR data in Proact's Remote Vault(s). VBR can store the data in two Proact DC locations. The customer must provide the appropriate Veeam Agent for Windows (VAW) (known as a Subscription license) to be able to store data in Proact's shared Remote Vault(s). Veeam Agents can only store the data in one Proact DC location.	Customer



Deliverable	Type	Description and content summary	Responsibility
Customer licensing	ALL	Where the BaaS-V interacts with any licensed system, application or environment not managed by Proact, it is the customer's responsibility to ensure that licenses for these systems, services and environments are maintained and assigned to the correct CIs to allow for BaaS-V to function. These licenses include, but are not limited to: ▪ VMware Licenses for VMware backup ▪ Amazon Web Service subscriptions ▪ Microsoft Azure subscriptions	Customer

2.4 - Configuration

2.4.1 - Service Capabilities

Deliverable	Type	Description and content summary	Responsibility
Backup source support	1	The products capable of being protected by this solution are subject to change if the underlying product support changes. The current supported products are set out in Proact's <i>BaaS-V Support Matrix</i> which is available upon request.	Proact
Unmanaged backup retention	2	Customers taking Unmanaged Remote Vault , are responsible for managing retention for all backup data, held within the Remote Vault, within the operating parameters of the product used.	Customer
Backup policies	1	Proact offer flexible backup policies, configurable per backup job, to meet the customer's contracted requirements, within the operating parameters of the product used. The default backup policy provides: ▪ Server/VM/Instance & Application Backup – a weekly synthetic full backup plus six daily incremental backups The customer may request modification to the default backup policy, within the operating parameters of the product used, to better meet their needs. These modifications can be made during service transition or from time to time.	Proact
Backup retention	1	Proact configure and maintain a retention policy to meet the customer's contracted retention requirements, within the operating parameters of the product and consistent with the contract term.	Proact



Deliverable	Type	Description and content summary	Responsibility
Flexible retention	1	The retention period in different vaults can be different from each other (e.g. 2 weeks in a Local Vault and 13 weeks in a Remote Vault). ▪ Hypervisor Agentless Backup is used, up to three copies of backup data are supported. A copy in the customers Local Vault (where installed) with the second and third in Proact's primary and secondary Remote Vaults. ▪ Where In-Server Agent Backup is used alongside Hypervisor Agentless Backup, then two copies of the backup data are supported. A copy in the customers Local Vault (where installed) with the second in the Remote Vault. ▪ Where In-Server Agent Backup only is used, then one copy of the backup data, held at a Remote Vault is supported. The copies of data retained can modified and added, within the operating parameters of the product, during the contract term at the customer's request.	Proact
Backup replication	1	Proact will replicate backup data between backup vaults (Local Vault/PCLV and Remote Vault) to meet a customer's retention and resilience requirements. Replication is supported between: ▪ Local Vault to Remote Vault ▪ PCLV to Remote Vault ▪ Remote Vault to Remote Vault	Proact
Storage efficiencies	1	BaaS-V supports de-duplication and compression during backup tasks. For backup tasks, de-duplication and compression is used to reduce network bandwidth and storage usage but may increase CPU load on the backup source. Proact will work with the customer to optimise the use of de-duplication and compression to best meet the customer's needs during transition. Data held on Local Vaults/PCLV and Remote Vaults will be stored, by default, in a de-duplicated and compressed format (where supported) to reduce storage consumption, unless specifically changed at the customer's request.	Proact
GDPR Right to Erasure / Be Forgotten	1	Proact will not undertake the restoration of data from backup for the purposes of data removal under the GDPR right to erasure/ be forgotten requests, where they require: ▪ Restoration of existing backup data to separate storage ▪ Removal of the data to be Erased/Forgotten ▪ Re-backup of that data to be retained ▪ Deletion of the original backup data Under a separate project, Proact can offer professional services to undertake planning and implementation of the above process as per customer reasonable requirements and within the operating parameters of the product used. Prior to commencement of such a project, the customer and Proact will agree the specification and charges for this separate project.	Out of Scope



Deliverable	Type	Description and content summary	Responsibility
GDPR Right to Erasure / Be Forgotten requests	1	It is the customer's responsibility to maintain a register of all data erasure requests and use this to ensure such data is removed again if restored as a result of subsequent data restore requests.	Customer

2.4.2 - Backup Service Methods

Deliverable	Type	Description and content summary	Responsibility
Unmanaged backup	2	Customers taking Unmanaged Remote Vault , are responsible for the creation and administration of VBR and VAW backup jobs and copy jobs within the operating parameters of the product used.	Customer
Backup approach	1	The solution provides two main backup approaches, which will be used depending on the type of data the customer will be protecting: ▪ Hypervisor Agentless Backup: Virtual Machines are backed up by interacting directly with the Hypervisor via either: ▪ Storage Array Backup (VMware Only) ▪ Hypervisor Storage Backup ▪ Hypervisor Network Backup and with either: ▪ Application Consistent Backup ▪ Operating System Consistent Backup ▪ Crash Consistent Backup ▪ In-Server Agent Backup: A server can be backed up by sending data directly from an installed agent, with either: ▪ Application Consistent Backup ▪ Operating System (OS) Consistent Backup By default, all backups will be indexed/catalogued so that individual files can be retrieved from within the OS of the server.	Proact
VMware tools (Customer)	1	Where the Hypervisor Agentless Backup approach and VMware are used, VMware tools must be installed and up to date, on the VMs running within the environment. If VMware tools is out of date, or not available, VM backups will be only crash consistent. Where a Local Vault is not installed at the customer's site, the customer will be required to host one or more Proxy VMs.	Customer
Hypervisor Storage Backup method (Proact)	1	Hypervisor Storage Backup is performed by a backup proxy role running on either a Local Vault or a Proxy server provided by the Customer. Backup data is accessed by taking a Hypervisor-based snapshot and retrieving the backup data from that snapshot on the storage controllers directly. This reduces network traffic and the load on the Hypervisor hosts network cards.	Proact



Deliverable	Type	Description and content summary	Responsibility
Hypervisor Network Backup method (Proact)	1	Hypervisor Network Backup is performed by either the Local Vault (if selected) or the Master Backup Server. Backup data is accessed by taking a Hypervisor-based snapshot and retrieving the backup data from that snapshot via the network cards of the Hypervisor hosts. The Hypervisor Network Backup is only supported with VMware based Hypervisors. For Hyper-V, the Hypervisor Storage Backup method will be used instead.	Proact
In-server agent method	1	Where In-Server Agents Backups are used to backup physical servers or public cloud servers. The in-server agent method requires that an agent be installed into the OS of the physical server or Public Cloud server/instance to be protected. This method will provide OS consistent and application consistent backup of the customer's source CIs.	Proact
Storage Array backup (Proact)	1	BaaS-V is able to backup VM data directly from the storage arrays where VMware is the running hypervisor and VMware Storage Array Integration within the customers array is supported. The Storage Array Backup will be performed by the Local Vault or Master Backup Server. Backup data is retrieved directly from the storage array used by the VMware Hypervisor host, which reduces the load on the Hypervisor. Storage Array Backup is supported via iSCSI or NFS protocols. Linux VM Operating System Consistent backup is only supported with the iSCSI protocol.	Proact
Storage Array backup (Customer)	1	Where the SAN or NAS method is required, the Local Vault/Master Backup Server will require access to the same storage network as the hypervisor servers. Where the storage array uses the NFS protocol, the use of manually created VMware Snapshots by the customer's administrator or by other Snapshot integrated applications (e.g. NetApp SnapManager) is not recommended, because the presence of a pre-existing VMware Snapshots will prevent the backup job from starting. Where other Snapshot integrated applications are used, the BaaS-V and Snapshot integrated application scheduling should not overlap, to ensure that no pre-existing VMware Snapshot is present when BaaS-V is scheduled to take a backup.	Customer
Flat file dumps	1	Proact does not support flat file dumps of application data. Performing dumps is both bandwidth and storage intensive for backup data and can impact backup and restore performance and scheduling.	Out of Scope
Agent conflicts	1	To avoid potential conflict between backup applications, the customer will remove any existing backup agents from each backup source CI in scope.	Customer



Deliverable	Type	Description and content summary	Responsibility
Existing replication	1	Where a customer is using Storage Array backup and a storage vendor's application consistency backup tools are used for disaster recovery (DR), the customer must: ▪ Configure the vendor's tools to perform application consistent backups that do not truncate the logs, update the applications catalogue or otherwise interfere with Proact's backup process. ▪ Ensure that the backup process and the DR snapshot/replication never run at the same time.	Customer
Unmanaged backup consistency	2	Customers taking Unmanaged Remote Vault, are responsible for both managing and testing application consistency and operating system consistency within the operating parameters of the product used.	Customer
Application consistency (Proact)	1	Where requested by the customer, Proact will configure the service to provide application consistent backups for supported applications, within the operating parameters of the product used. Application consistency is available for supported applications with both the Hypervisor Agentless Backup and In-Server Agent Backup approaches.	Proact
Application consistency (Customer)	1	It is the customer's responsibility, through the use of test restores, to ensure that application consistent functionality is working as designed and that data consistency is being achieved.	Customer
Operating System consistency	1	Where supported by the operating parameters of the product used, Proact will perform an OS consistent backup. OS consistency is available for supported operating systems with both the Hypervisor Agentless Backup and In-Server Agent Backup approaches.	Proact
Crash consistency	1	Crash Consistent Backups take the backup without the VM (or the application within it) being aware that a backup is being performed. This method of backup will be quicker but there is a risk that some of the underlying files/data may be inconsistent or corrupt. If an entire VM is restored, an OS based disk check (i.e. Windows chkdsk) may be required. Crash Consistent Backup is only supported with Hypervisor Agentless Backup and will be used where the VM does not have any Hypervisor Integration Tools installed (for example a virtual appliance).	Proact

2.4.3 - Restore Service Methods

Deliverable	Type	Description and content summary	Responsibility
Unmanaged restore	2	Customers taking Unmanaged Remote Vault, are responsible for restoration of VBR and VAW backup data held within the Remote Vault, within the operating parameters of the product used. Restore tasks performed by the customer will be without Proact's interaction or knowledge and are not bound by Response Time SLAs.	Customer



Deliverable	Type	Description and content summary	Responsibility
Recycle bin	ALL	Backup data or restore points deleted are held in a recycle bin for 3 days prior to permanent deletion, within the operating parameters of the product used, to protect against accidental or malicious deletion. This data is available for restore, upon customer request.	Proact
Restore requests	1	The customer may request that a restore is initiated through a service request to Proact's service desk.	Customer
Restore approaches	1	The following restore methods are applicable to the available backup approaches: Hypervisor Agentless Backup: The VM is restored by interacting with the VM via the hypervisor via either: ▪ File/Folder Restore ▪ Single-Item Restore ▪ Volume Restore ▪ VM Restore In-Server Agent Backup: The server is restored by sending data to the agent via either: ▪ File/Folder Restore ▪ Single-Item Restore ▪ Volume Restore To provide the best restore performance, the restore will be performed from the vault which is closest to the destination server (i.e. the Local Vault), if the data required is not on the Local Vault, a Remote Vault will be used.	Proact
Restore process	1	With Hypervisor Agentless Backup, restoration of the data will be by remotely accessing the master backup server. In all-cases, the data is restored from the backup vault to the server using the network. With the In-Server Agent Backup, restoration of the data will be by remote access to the server via an Internet Site-to-Site VPN. In all-cases, the data is restored from the backup vault to the server using the network.	Proact
Self-service restore	1	Self-service restore is performed by the customer and without Proact's interaction or knowledge and is not bound by Response Time SLAs, as Proact is not involved in the restore process. With Hypervisor Agentless Backup, the restore process is performed by the self-service console which is run from an administrator's PC. With the In-Server Agent Backup, the restore process is performed by the agent GUI installed on each source server.	Customer
File/Folder restore method	1	The File/Folder restore method will return individual files, groups of files and folders from the backup copy, back to the original source CI or to a different source CI within the operating parameters of the product used.	Proact



Deliverable	Type	Description and content summary	Responsibility
Single-Item restore method	1	The Single-Item restore method will return application data and metadata from the backup copy, back to the original source CI or to a different compatible source CI within the operating parameters of the product used. Application data can be restored for the following applications: ▪ Microsoft Active Directory ▪ Microsoft Exchange ▪ Microsoft SharePoint ▪ Microsoft SQL Server ▪ Oracle RDBMS	Proact
Volume restore method (Proact)	1	The Volume Restore method will return entire volumes/disks from the backup copy, back to the original source CI or to a different source CI within the operating parameters of the product used.	Proact
Volume restore method (Customer)	1	With the In-Server Agent Backup approach all volumes (including the system drive) can be restored but system drives will only be restored to a new disk/mapping as the server will be powered-on when the volume is restored. Where physical servers are protected, the customer and Proact will agree a volume restore approach for any physical systems being protected, should a system drive fail. This approach will be agreed during service transition or from time to time.	Joint
VM restore method	1	The VM Restore method will return an entire VM from the backup copy, either overwriting the existing VM or restoring to a new VM. The VM can also be restored to a separate public cloud/hypervisor environment within the operating parameters of the product used.	Proact
Service best practice	1	It is the customer's responsibility to act upon Proact best practice recommendations delivered during service review meetings or from time to time, to minimise the possibility of exceptional restore delays/failures.	Customer
Exceptional restore delays/failures	1	Where the restore of an individual source takes over 48 hours to complete, or fails due to one or more of the below: ▪ Storage performance ▪ Available bandwidth ▪ Application configuration ▪ Customer source environment state Proact Professional Services will offer to undertake planning and implementation of the recovery in-line with the customer's needs, as a separate project. Prior to commencement, the customer and Proact will agree the charges for this separate project.	Out of Scope
Restore space	1	The customer will ensure that there is sufficient storage space available to restore their CIs.	Customer



2.5 - Service Deliverables

2.5.1 - Service Monitoring

The following provides an overview of the specific monitoring provided for the service. Proact's standard monitoring deliverables are provided in the Common Service Deliverables appendix.

Deliverable	Type	Description and content summary	Responsibility
Monitored items	1	- Backup job status, including failed backups - The quantity of source servers/systems protected for licensing purposes. Proact do not actively monitor agent software or customer server/applications, as part of this service.	Proact

2.5.2 - Operational Activities

Deliverable	Type	Description and content summary	Responsibility
Job failure response	1	Proact monitor the success state of backup jobs using the monitoring platform, which: - Generates alerts for failed backup jobs - Forwards alerts to the Proact service desk Proact will ensure that any jobs which have failed are investigated and where appropriate, re-run.	Proact
Job failure troubleshooting	1	For repeat failures, Proact will contact the customer and both parties will jointly troubleshoot the problem.	Joint
Restore testing account	1	The customer will provide one or more user accounts that can be used for restore testing for the CIs in scope. These accounts will be agreed by the customer at service start-up and documented within the SOM.	Customer
Restore testing (Proact)	1	Proact will undertake two scheduled restore tests in each twelve-month period (dated from the service commencement). Where a Local Vault is installed at the customer's site, Proact will restore, from that vault, up to a maximum of 100GB of business data per source during each test. Where the data is held off-site, restore size will be limited by bandwidth availability. Where there is insufficient bandwidth, or bandwidth contention, for a 2 hour restore task then a subset of the customer's data will be restored in the test and this may require a different restore method, such as 'File/Folder' or 'Single Item' restore. All test restores will be performed out of place, not overwriting the customer's existing data. Proact will undertake initial restore tests during the service transition phase. These tests will represent one of the two tests allowed in the first 12-month period.	Proact



Deliverable	Type	Description and content summary	Responsibility
Restore testing (Customer)	1	The customer will nominate 3 data sources for each scheduled restore test. Proact recommend that these restore tests be taken from different restore approaches and methods where multiple restore approaches and methods are in use by the customer. Where a successful restore has been performed within two months of a scheduled restore test of a defined approach/method, that successful restore shall constitute a successful test for a given approach/method and Proact recommends this approach/method not be repeated in the next scheduled test.	Customer
Restore validation	1	The customer will confirm that restored data works as expected.	Customer

2.6 - Service Upgrades

Deliverable	Type	Description and content summary	Responsibility
Upgrades and new features	ALL	This service is a multi-tenant platform provided by Proact. All upgrades, or enablement of new features, is at the sole discretion of Proact.	Proact

2.7 - Service Specific Reporting

Deliverable	Type	Description and content summary	Responsible
Backup reporting	ALL	Proact will provide automated reports, within the operating parameters of the product used, confirming the status of backup jobs, at the customer's request.	Proact
Service review report (BaaS-V)	1	Within the service review report, Proact will include technical statistics, observations and recommendations regarding the service, in relation to: - Backup service capacity - Backup CI usage - Bandwidth usage Note: The content listed above is an example and is subject to change.	Proact
Service review meeting	ALL	Proact will organise service review meetings, by teleconference, at a schedule agreed between both parties, but no more than once per quarter. These meetings will discuss the service review report content.	Proact

2.8 - Acceptance Criteria

Below are the defined service acceptance criteria for this service. Invoicing for the service(s) will commence once the following criteria have been met:



Associated Deliverable	Type	Description and content summary	Responsibility
Storage (Proact's Datacentre)	ALL	Proact have deployed a Remote Vault in a Proact datacentre, and the vault can successfully communicate with Proact's BaaS-V platform.	Proact
Unmanaged storage access	2	Proact have provided to the customer the credentials and address required to connect their local Veeam Backup and Recovery environment to Proact's shared Remote Vault.	Proact
Storage (Customer's Datacentre)	1	Proact has deployed all the Local Vaults in scope of the customer's source site(s), or, by mutual agreement, a subset of those, and each deployed vault can successfully communicate with Proact's BaaS-V platform.	Proact
Backup approach	1	Successful initial full backup (with no errors) and at least one subsequent scheduled incremental backup to the primary Remote Vault of one of each of the following, where appropriate and in scope, and to a maximum size of 100GB in total: - Virtual machine - Physical server - Public Cloud server/instance.	Proact
Backup replication	1	The initial full backups from the 'Backup approach' deliverable have been successfully replicated from the Local Vault to each Remote Vault in scope.	Proact
Restore testing (Local Vault)	1	Where a Local Vault is installed, Proact have confirmed that data has been successfully restored from backup on the Local Vault of one of each of the restore approaches available that are applicable to the customer's backup and within the capabilities of the product. Each backup will always be restored to a separate location on the customer's source site.	Proact
Restore testing (Remote Vault)	1	Proact have confirmed that data has been successfully restored from backup on the Remote Vault of one of each of the restore approaches available that are applicable to the customer's backup and within the capabilities of the product. Each backup will always be restored to a separate location on the customer's source site.	Proact
Monitoring (platform)	1	Proact are monitoring successfully the state of each deployed Local Vault, PCLV, master backup server and backup proxy server and monitoring alerts for these are being sent to Proact's Service Desk for investigation.	Proact
Monitoring (jobs)	1	Proact are monitoring successfully the state of scheduled backup jobs, and monitoring alerts for failed jobs are being sent to Proact's Service Desk for investigation.	Proact
Backup reporting	1	Proact have scheduled reports confirming the status of backup jobs internally, and where requested, at least one report has been delivered to the customer	Proact



2.9 - Vendor Terms

The services described in this Services Specification will be subject to the vendor terms set out in the table below.

These terms are available in full at <https://www.proact.eu/en/about-us/terms-and-conditions/vendor-terms/>.

Vendor Name
Veeam

2.10 - Service Level Agreement

2.10.1 - Availability Service Levels

This service level agreement sets out what levels of uptime availability Proact will endeavour to provide. Availability is monitored using Proact's software platform. Availability is measured continuously, for the purposes of the SLAs will be measured in units of a month. Service reports will be provided to the customer quarterly.

Service	SLA	Monthly SLA Description	Measurement
BaaS-V	99.5%	The service will be available for at least 99.5% of each month	The BaaS Platform will be available if the Remote Vault and any associated Backup Software located in Proact's data centre responds to Proact's monitoring software
Comms – Internet	99.95%	The internet connectivity will be available for at least 99.95% of each month	The internet connectivity will be available if Proact's monitoring software can access commonly available web pages using the communications link.



Appendix 3 - BaaS-O365 Service Definition

2.11 - Service Overview

Proact's Backup as a Service for Office365 solution (BaaS-O365) provides a backup solution for business data running within Microsoft O365 Cloud SaaS Service. Proact will deliver a fully managed service that will integrate with O365 and provide an independent backup of business data external to O365, to allow for point in time data protection, as well as recovering business data in the event that O365 services are not available.

2.12 - Service Types

The Backup as a Service - O365 is delivered with a single service type:

Service type	Service type summary
BaaS-O365	Proact provide a managed backup solution for source data residing in Microsoft's Office365 Cloud SaaS Service. The backup is billed based upon 'User Count' with the customer defining which O365 users require protection. All backup data will be copied to Proact's Primary DC daily and retained in line with the customer's retention requirements. This solution will provide an off-site copy of business data and historic granular restore for data deleted from Office365.

2.13 - Service Options

The table below sets out the service options available within BaaS-O365.

The services provided by Proact will be referenced in the charging tables in section 3 of the Service Specification Document.

Option name	Option description
BaaS O365 User	The number of Microsoft Office365 Active User subscriptions that require protection. A single user license will protect Exchange Online, SharePoint, Teams and OneDrive for Business for that user.

2.14 - Specific Architecture

2.14.1 - Platform

Deliverable	Description and content summary	Responsibility
Platform	A secure multi-tenant platform for the backup of Office365 Email, SharePoint and OneDrive for Business (OneDriveFB) data	Proact
Storage	Backup data is stored on high-capacity, low-performance storage provided as shared data vaults in Proact's datacentre. Each customers data will be stored in dedicated repositories within the shared data vaults.	Proact



Deliverable	Description and content summary	Responsibility
Self Service Restore Components	For customers who wish to use self-service restore; the customer will be either: ▪ Already a Veeam Backup and Replication customer with VBR installed and active. The version of VBR being used must be compatible with BaaS-O365 ▪ Or able to install a BaaS-O365 compatible version of 'Veeam Backup and Replication Community Edition'. This infrastructure will be maintained for the length of time that the self service restore feature is required. The customer will take responsibility for the provision and maintenance of these systems.	Customer

2.14.2 - Components

Deliverable	Description and content summary	Responsibility
Master backup server	A multi-tenanted master backup server is deployed by Proact within Proact's datacentre and will manage backup jobs and offload the backup process to backup proxy servers The master backup server will host and maintain the backup database service. This service will log backup jobs and provide indexing for the restore process.	Proact
Backup proxy server	Multi-tenanted proxy servers will perform the backup tasks for multiple customers, backing up data from within O365 and storing that data within the customer's dedicated repositories within the shared data vaults in Proact's datacentre. Proact may use one or more backup proxy servers to perform backup operations, depending on the size and complexity of the customer's environment.	Proact
Shared data vault & dedicated repositories	Each customer's O365 backup data will be stored within one or more shared data vaults on, one or more backup proxy servers. Customer's data will be held within one or more dedicated repositories, within a shared data vault to securely isolate the customer's data and provide differing retention periods.	Proact
Self Service Restore Connection	For customer who wish to use self-service restore; during service start-up, Proact and the Customer will configure a secure connection between the customers Veeam infrastructure into Proact's BaaS-O365 environment to enable secure restore communication.	Joint

2.14.3 - Connectivity

Deliverable	Description and content summary	Responsibility
Backup traffic	Connectivity for the solution will be via the internet. All backup traffic will be copied directly from the customer's O365 account to Proact's DC without passing through the customer's network.	Proact
Firewalls	All internet communication will be performed using Proact's existing firewall infrastructure.	Proact
Customer credentials	During service start-up, the customer will provide a 'service account' and its attached password with sufficient privileges to allow the Office365 backup process to be performed. This account will be maintained for the length of the agreement. The customer must inform Proact prior to changing the password for this service account and provide Proact with the new password.	Customer



Deliverable	Description and content summary	Responsibility
Bandwidth usage	Proact will maintain sufficient internet bandwidth to accommodate the O365 backup traffic.	Proact
Microsoft bandwidth throttling	Microsoft may apply bandwidth throttling to the customer's O365 service and this may impact the time required to perform a backup each day. If sufficient Microsoft bandwidth is not available to perform the backup, Proact will not be responsible for backups not being completed.	Out of Scope
Self Service Restore	For customers who wish to use self-service restore; during service start-up, Proact and the Customer will configure a secure connection between the customer's Veeam infrastructure into Proact's BaaS-O365 environment to enable secure restore communication. The customer will be responsible for version compatibility of VBR environment and BaaS-O365.	Customer
SaaS provider configuration change	Where a SaaS provider used by the service or customer, requires a configuration update from the customer and the lack of update leaves Proact unable to effectively complete operational activities, the customer is responsible for making the required configuration update to re-instate the service.	Customer

2.14.4 - Security

Deliverable	Description and content summary	Responsibility
Data encryption	All Backup data will be encrypted in-flight using Microsoft's standard Office365 security protocols (TLS encryption).	Proact
Anti-virus protection	Proact's BaaS-O365 service platform, including all shared data vaults incorporates enterprise level anti-virus protection. The anti-virus protection will not scan any of the customer's backup data.	Proact

2.14.5 - Licensing

Deliverable	Description and content summary	Responsibility
Office 365 licensing	This service is available to customers of Microsoft Office365. The customer must have a valid Office365 subscription and maintain this for the period of the contract.	Customer
Removal of O365 User License	The customer is responsible for the assignment of O365 licenses for users being backed up by the service. All users that require BaaS-O365 protection must be assigned an Office365 User license. Should a customer revoke/remove an Office365 User License from a user, protection of that user will no longer be protected by BaaS-O365.	Customer



2.15 - Configuration

2.15.1 - Backup Service Methods

Deliverable	Description and content summary	Responsibility
Job schedule types	Proact offer flexible backup policies to meet the customer's contracted requirements, within the operating parameters of the product used. Details of the Office365 services protected by this solution are available in Proact's BaaS-O365 Support Matrix upon request. Any services not listed as 'supported' in the support matrix are explicitly excluded. The support matrix is subject to change during the life of the agreement. Individual backup jobs will be performed for OneDriveFB, Exchange Online, Teams and SharePoint. These backups can be further subdivided based upon customer retention requirements.	Proact
Backup types	Backups will be taken as Synthetic Full backups, which means that after the initial full backup, all future backups will only consume the additional space for daily changed data but will have the advantage of being catalogued as a full backup which will allow for faster restores. All backups will be indexed/catalogued so that individual emails, files and SharePoint objects can be retrieved	Proact
Retention policy	Proact configure and maintain a flexible retention policy configuration to meet the customer's contracted retention requirements (within the operating parameters of the product used and consistent with the contract term).	Proact
Data consistency	Data copied from O365 will be retrieved using Microsoft's data transfer protocols and therefore will provide a consistent copy of the data at a file/email/SharePoint object level.	Proact
Exchange Public Folders	Public folders are not supported by Microsoft. Where a customer has Public Folders that require protection. The customer will convert these folders to Microsoft 365 Groups and inform Proact that backup of these groups is required.	Customer

2.15.2 - Restore Service Methods

Deliverable	Description and content summary	Responsibility
Restore requests	The customer may request that a restore is initiated through a service request to Proact's service desk.	Customer



Deliverable	Description and content summary	Responsibility
Standard restore process	Data can be restored by Proact to two locations: - Restored back to Office365 - Restored to the customer directly via email. Data 'restored to Office365' will be returned to the customers Office365 environment. At the time of the restore, the customer and Proact will review the restore options, within the operating parameters of the product used, and define the location of the restore and if the current O365 data should be overwritten. Data returned to the customer via email will first be placed within a password protected zip archive. The zip archive will be returned to the customer in one of two ways: - Zip archives of up to 50MB can be returned via email to an existing account within the customer's Office365 environment. - Zip archives of up to 1TB will be made available via an 'out of band' restore method that provide encrypted file transfer (such as OneDriveFB or DropBox). The customer will define and supply the file transferred method to be used for this option. The password for the zip archive will be sent via SMS to the receiving customer's pre-recorded contact mobile number. This process will ensure two factor authentication for the restored data regardless of the restore process chosen. Proact will not be responsible for the speed of the restore process, or the transfer time from Proact to the customer's environment during a restore.	Proact
High capacity restore process	With larger restores (in excess of 1TB of data) a viable restore process will depend upon a number of factors: - Reason for the restore - Customer bandwidth limitations - Recovery time objective - O365 environment state - Physical hardware (or IaaS) to act as the restore target For these restores Proact Professional Services will undertake planning and implementation of the recovery in-line with the customer's needs, as a separate project. Prior to commencement the customer and Proact will agree the charges for this separate project.	Joint
O365 two factor authentication	When 'modern authentication' is used with 'security defaults' the customer will provide a member of staff with the required two factor authentication, to assist Proact in performing the restore process.	Customer
Self Service Restore	For customer who wish to use self service restore; customers have to option to restore data without Proact's assistance. With 'self service restore', Data can be restore to Office365 directly or downloaded to the customers environment. This process is performed by the customer and without Proact's interaction of knowledge. Self service restore is not bound by SLAs, as Proact is not involved in the restore process.	Customer



2.16 - Service Deliverables

2.16.1 - Service Monitoring

The following provides an overview of the specific monitoring provided for BaaS-O365. Proact's standard monitoring deliverables are provided in the Common Service Deliverables appendix.

Deliverable	Description and content summary	Responsibility
Monitored items	- Backup job status, including failed backups - O365 user count	Proact

2.16.2 - Operational Activities

Deliverable	Description and content summary	Responsibility
Job failure response	Proact monitor the success state of backup jobs using the monitoring platform, which: - Generates alerts for failed backup jobs - Forwards alerts to the Proact service desk Proact will ensure that any jobs which have failed are investigated and where appropriate, re-run.	Proact
Job failure trouble-shooting	For repeat failures, Proact will contact the customer and both parties will jointly troubleshoot the problem.	Joint
Storage capacity management	Proact will extend storage capacity for backup data where storage vaults reach certain thresholds, to ensure that they do not run out of space. Proact may, where appropriate, move a customer's repository between shared data vaults to balance storage capacity. This will not impact the customer's backup process or ability to restore.	Proact
Backup reporting	Proact provide reports confirming the status of backup jobs.	Proact
Restore testing account	The customer will provide a user account that can be used for restore testing. This account will be agreed by the customer at service start-up and documented within the SOM.	Customer
Restore testing	Proact will undertake two scheduled restore tests in each twelve-month period (dated from the service commencement). Where a successful restore has been performed within two months of a scheduled restore test, that successful restore shall constitute a successful test, and Proact shall not run that next scheduled test. The restore test will be performed with the agreed restore testing account. Proact will confirm that a test restoration is successful for each O365 service the restore testing account is protecting, with three services being the maximum (OneDriveFB, Exchange, Teams and SharePoint). Proact will restore up to a maximum of 5 items or 2MB of business data during the restore test. The data will be restored by the Proact engineer and returned to the customer via email in line with the standard restore process. Proact will conduct the initial restore test during the service transition phase, and this test represents one of the two tests allowed in the first 12-month period.	Proact



Deliverable	Description and content summary	Responsibility
GDPR Right to Erasure / Be Forgotten	Proact will not undertake the restoration of data from backup for the purposes of data removal under the GDPR right to erasure/ be forgotten requests, where they require: ▪ Restoration of existing backup data to separate storage ▪ Removal of the data to be Erased/Forgotten ▪ Re-backup of that data to be retained ▪ Deletion of the original backup data Under a separate project, Proact can offer professional services to undertake planning and implementation of the above process as per customer reasonable requirements and within the operating parameters of the product used. Prior to commencement of such a project, the customer and Proact will agree the specification and charges for this separate project.	Out of Scope
GDPR Right to Erasure / Be Forgotten requests	It is the customer's responsibility to maintain a register of all data erasure requests and use this to ensure such data is removed again if restored as a result of subsequent data restore requests.	Customer

2.17 - Service Upgrades

Deliverable	Description and content summary	Responsibility
Upgrades and new features	This service is a multi-tenant platform provided by Proact. All upgrades, or enablement of new features, is at the sole discretion of Proact.	Proact

2.18 - Service Specific Reporting

Deliverable	Description and content summary	Responsible
Backup reporting	Proact will provide automated reports, within the operating parameters of the product used, confirming the status of backup jobs, at the customer's request.	Proact
Service review report (BaaS- O365)	Within the service review report, Proact will include technical statistics, observations and recommendations regarding the service, in relation to: ▪ Backup service capacity ▪ Backup CI usage ▪ Bandwidth usage Note: The content listed above is an example and is subject to change.	Proact
Service review meeting	Proact will organise service review meetings, by teleconference, at a schedule agreed between both parties, but no more than once per quarter. These meetings will discuss the service review report content.	Proact

2.19 - Acceptance Criteria

Below are the defined service acceptance criteria for BaaS-O365. Invoicing for the service(s) will commence once the following criteria have been met:



Deliverable	Description and content summary	Responsibility
Backup target vaults	Proact have provided one or more backup vaults for the customer's O365 data and commenced the backup process for each O365 service the customer is protecting.	Proact
Running backup process	The backup process will be running and protecting 10% of the customer's users, or a minimum of 5 users, whichever is the smaller.	Proact
Restore testing	Proact have confirmed that data has been successfully restored from the backup for two different customer user accounts. Proact have confirmed that a test restoration is successful for each O365 service the customer is protecting, with three services being the maximum (OneDriveFB, Exchange, Teams and SharePoint).	Proact

2.20 - Vendor Terms

The services described in this Services Specification will be subject to the vendor terms set out in the table below.

These terms are available in full at <https://www.proact.eu/en/about-us/terms-and-conditions/vendor-terms/>.

Vendor Name
Veeam

2.21 - Service Level Agreement

2.21.1 - Availability Service Levels

This service level agreement sets out what levels of uptime availability Proact will endeavour to provide. Availability is monitored using Proact's software platform. Availability is measured continuously, for the purposes of the SLAs will be measured in units of a month. Service reports will be provided to the customer quarterly.

Service	SLA	Monthly SLA Description	Measurement
BaaS-O365	99.5%	The service will be available for at least 99.5% of each month	The service will be available if the shared data vault and any associated master server located in Proact's data centre responds to Proact's monitoring software and if Proact's monitoring software can access commonly available web pages using the communications link.



Appendix 4 - Backup as a Service – Secure Storage Vault Service Definition

3.1 - Service Overview

Proact Backup as a Service - Secure Storage Vault (BaaS-SSV) is an offsite backup vault for customers who have NetApp ONTAP storage, run ONTAP storage in the cloud, or utilise ONTAP storage within Proact's Datacentres.

The offsite backup vault is hosted in a Proact datacentre and acts as a replication target for volumes, LUNs, and Storage Virtual Machines (SVMs) hosted on the customer's existing ONTAP storage. Where the ONTAP storage is also hosted within a Proact datacentre or within an existing Proact managed service (such as PHC or PMCP), BaaS-SSV will replicate to an alternate Proact datacentre to ensure the data is offsite. Replication will be performed using either NetApp SnapMirror or SnapVault technology. Proact will monitor all backups being sent to the Secure Storage Vault and perform restore tasks on behalf of the customer.

Access is provided to the Proact *Customer Service Portal*. This portal allows customers to view alerts produced by the BaaS-SSV replication relationships (i.e., usage, lag times etc.). The *Customer Service Portal* provides the ability to open and update support cases (i.e., restore request) as well as view the catalogue information held for the volumes/LUNs/SVMs being backed up.

For SSV replication, no additional onsite equipment is required. All backups are held locally on the source array as ONTAP Snapshots, and are replicated and stored remotely at Proact, to provide both an onsite and offsite backup.

3.2 - Service Types

The Backup as a Service – Secure Storage Vault (BaaS-SSV) is delivered with a single service type:

Service type	Service type summary
BaaS-SSV	Proact provide a monitored and managed offsite backup vault for customers who utilise NetApp ONTAP storage. The backup vault is held on Proact's shared ONTAP platform, with each customer assigned a dedicated ONTAP Storage Virtual Machine (SVM), to allow segregation of the data from other customers. BaaS-SSV supports replication of ONTAP Volumes, LUNs and SVMs. This is a pay-as-you-use service, sized based upon the quantity of data transferred, and the storage consumed at Proact for the customer's required retention periods.

3.3 - Service Options

The table below sets out the service options available within BaaS-SSV.

The services provided by Proact will be referenced in the charging tables in the contract.

Option name	Option description
BaaS Secure Storage Vault Capacity	The backup storage consumed within Proact BaaS-SSV Platform. Capacity Storage will be consumed by default.
Direct Internet Access	The daily Internet bandwidth consumed by backup replication during the customers defined backup replication window. This figure is for data copied to Proact (via the Internet).
MPLS - Primary to DR Data Centre	The daily inter-site bandwidth consumed by backup replication during the customers defined backup replication window. This figure is for data copied between Proact datacentres, on Proact's inter-site links.

3.4 - Specific Architecture

This appendix covers detail on deliverables that are specific to this service. This service also includes the deliverables defined in the **Common Service Deliverables** labelled as 'Managed' (**MAN**).

The responsibility for each deliverable is defined below and colour-keyed for easy review:

Proact Responsibility	Customer Responsibility	Joint Responsibility
-----------------------	-------------------------	----------------------

3.4.1 - Platform

Deliverable	Description and content summary	Responsibility
BaaS-SSV Platform	A secure multi-tenant NetApp ONTAP storage array platform. This platform is provided as a target for the SnapMirror and SnapVault replication of data held within the Source ONTAP Storage.	Proact
Platform Storage (Proact's datacentre)	Proact provide sufficient storage to support backup replication of the customer's Protected Volumes, LUNs and storage virtual machines (SVMs) to the BaaS-SSV Platform. The disk performance tier used for the customer's data, by default will be 'Capacity Storage', but can be varied according to customer's requirements. Available disk performance tiers are: ■ Ultra Performance Storage – SSD high performance, low latency storage ■ Performance Storage – SAS performance storage ■ Capacity Storage (Default) – NL-SAS/SATA low performance, high-capacity storage	Proact



Deliverable	Description and content summary	Responsibility
Source's ONTAP Storage	Backup replication will be performed from the Source ONTAP Storage installation. This installation can be: - Physical ONTAP storage array controller(s) - ONTAP Select storage software running on a VM or physical server - Cloud Volumes ONTAP - ONTAP storage array controllers running within a Proact DC - A Proact managed Service The customer will be responsible for the management, maintenance and administration of the Source ONTAP storage, unless Proact provide the ONTAP SVM within an existing Proact managed service (such as PHC, or PMCP), or Proact are contracted to provide Service Management for the source array.	Customer

3.4.2 - Components

Deliverable	Description and content summary	Responsibility
BaaS-SSV Cluster	A multi-tenanted ONTAP cluster deployed by Proact within Proact's datacentre to be the backup replication target for customer data.	Proact
Secure Storage Vault (SSV)	Proact will assign an ONTAP Storage Virtual Machine (SVM), called a Secure Storage Vault (SSV). This SSV is dedicated to the customer and will provide segregation of the data from other tenants within the BaaS-SSV Platform. Each SSV is managed as a separate entity. The SSV will host and maintain the backup data for the customer and instigate backup replication tasks from the Source ONTAP Storage through 'pull' replication. This SSV provides a dedicated IP network for backup replication.	Proact
Source ONTAP Storage	The Source ONTAP Storage will act as the source for the backup replication. For data to be replicated, ONTAP Snapshots will be used to capture each 'point in time' for volumes to be replicated.	Customer
Protected Volume	The customer will define which volumes, LUNs and SVMs that require protection. The customer can choose to protect all volumes or a subset of volumes as required. These volumes will be agreed by the customer at service start-up and documented within the <i>SOM</i>. Modifications to the list of Protected Volumes can be made during service transition or from time to time by logging requests through the Proact <i>Customer Service Portal</i>.	Customer
Target Volume	Backup replication is performed between the source Protected Volumes and Target Volumes created by Proact. Target Volumes are held within the customer's SSV at Proact.	Proact
Site to Site VPN (StS VPN)	Where internet replication is required and a dedicated link is not provided, a Site to Site (StS) VPN is used to provide the customer with secure access to their dedicated SSV IP Network over the public Internet. The StS VPN encrypts the backup Replication Traffic between the Source ONTAP installation and Proact's BaaS-SSV Platform.	Proact



Deliverable	Description and content summary	Responsibility
Replication Pairing	The Source ONTAP installation and Proacts SSV IP network are paired to allow storage backup replication between the systems. The pairing process is performed over the StS VPN tunnel, a dedicated link, or over Proact's internal network. Once paired, Snapshots created on the customer's Protected Volumes are marked for backup replication and will be replicated once the next scheduled backup replication is initiated. Proact and the customer will configure replication pairing during service transition.	Joint
Application Consistency (Proact)	All backup replications performed are crash consistent and not application consistent. Where an application requires data consistency (i.e., SQL database) then NetApp SnapCenter products can be used to ensure consistency. The customer is free to install and manage these products and Snapshots created by these products are supported by the replication process. The customer is required to discuss application consistency with Proact's IT team to ensure the replication schedule meets the customer's requirements.	Customer
Application Consistency (Customer)	The customer's installation, configuration, or management of the SnapCenter application, or its agents, is not included with BaaS-SSV.	Out of Scope
Disaster Recovery	The BaaS-SSV replica is not suitable for presentation of storage in a DR failover scenario. In the event that the source storage array is lost, and its Protected Volumes become unavailable, the network hosting the source ONTAP storage will not have access directly to the BaaS-SSV environment and, therefore, cannot access the BaaS-SSV data. The BaaS-SSV data must be restored to a compatible ONTAP array on the source network before it can be addressed. Proact provide a DRaaS product to deal with disaster recovery. This product should be considered where recovery from a disaster is required.	Out of Scope

3.4.3 - Connectivity

Deliverable	Description and content summary	Responsibility
Replication Traffic	Where the Source ONTAP Storage is hosted remotely and a dedicated link is not provided, all communication between the customer's site(s) and the BaaS-SSV Platform is performed securely over the public Internet through the StS VPN. The customer must ensure Internet access is available for the term of the agreement. Where the Source ONTAP Storage is hosted within a Proact Datacentre, Replication traffic to the BaaS-SSV platform will use Proact's internal network.	Customer
Proact Firewalls	All Internet and VPN communication will be performed using Proact's existing firewall infrastructure. Proact manage this centralised firewall, which defines open ports and blocks unwanted traffic for the entire service. These firewalls are used to allow Proact to provision a StS VPN for management and backup Replication Traffic for the BaaS-SSV service.	Proact



Deliverable	Description and content summary	Responsibility
Customer Firewalls	Where used, the customer's firewall infrastructure must support IPsec StS VPN, for the contract term: - The customer must provide a static public IP address to facilitate the establishment and ongoing operation of a StS VPN, for the contract term - The customer is required to open specific firewall ports to allow for backup data transfer and maintain this configuration for the contract term. Detailed requirements are provided by Proact during service transition. The customer is required to provide an administrator to perform the firewall configuration.	Customer
Utility Session	In the event of StS VPN failure, a customer-assisted remote support utility session is used to connect to the customer's site and to troubleshoot the failure. The customer is required to provide an administrator to assist in the troubleshooting process.	Customer
Throttling	By default, Proact will not impose restrictions on backup Replication Traffic to maximise backup throughput. Restrictions can be imposed at the customer's request, where there is contention on low bandwidth connections or additional traffic is considered higher priority. The customer may request that a throttle be applied to backup Replication Traffic, at any time during the contract period by logging requests through the Proact <i>Customer Service Portal</i>.	Customer
Bandwidth Capacity (Proact)	Proact will maintain sufficient bandwidth to accommodate management and backup Replication Traffic.	Proact
Bandwidth Capacity (Customer)	Where the Source ONTAP Storage is hosted remotely and a dedicated link is not provided, Internet bandwidth is required for all data seeding, backup replication and management activities involving BaaS-SSV. Data change rates and the customer's available bandwidth will dictate the time required for backup replication tasks. The customer is responsible for providing sufficient bandwidth between the site holding their ONTAP storage and Proact for efficient backup replication. If sufficient bandwidth is not available, having up to date backup data will not be achievable.	Customer
Bandwidth Capacity (Joint)	Proact will work with the customer to minimise potential monopolisation of bandwidth by Throttling and spreading backup replication activities over customer-defined periods of time.	Joint
Public Cloud Transfer Charges (Customer)	Data transfers related to public cloud providers are subject to ingress, egress and other usage charges. Where the Source ONTAP Storage is hosted by a public cloud provider, the costs for the public cloud environment, will be billed to customer, by the customer's public cloud provider and are the customer's responsibility.	Customer
Public Cloud Transfer Charges (Proact)	Proact will work with the customer to attempt to minimise public cloud transfer charges, through the use of compression and Throttling, within the operating parameters of the product used, to assist the customer in managing usage costs.	Joint
Interoperability with Customer-Managed Systems	Where this service interacts with any system, application or environment not managed by Proact, it is the customer's responsibility to ensure that it remains compatible with any Proact-managed systems/applications at the hardware, firmware, OS, and application version level – as recommended by Proact or its vendors as best practice.	Customer



Deliverable	Description and content summary	Responsibility
ONTAP Version (Customer)	The customer must ensure that they are on the same major release of ONTAP as utilised on the BaaS-SSV Platform. The customer must confirm the major ONTAP release in use by Proact prior to upgrading the source storage system.	Customer
ONTAP Version (Proact)	When using BaaS-SSV, the Source ONTAP Storage and Proact's BaaS-SSV Platform, must remain with-in the same ONTAP major version. Therefore, when Proact upgrade the BaaS-SSV Platform version, and Proact do not manage the Source ONTAP Storage, the customer is expected to upgrade their ONTAP storage with in-line with the ONTAP upgrade. This only applies to major version upgrades (i.e., 9.8.x to 9.9.x) and not to minor ONTAP upgrades (i.e., 9.8.P1 to 9.8.P3).	Customer

3.4.4 - Security

Deliverable	Description and content summary	Responsibility
Data Encryption in Flight	Encryption is applied, via the StS VPN, to all Internet backup replications between Proact and their customers.	Proact
Data Encryption at Rest (Proact)	By default, data held within the Target Volumes will not be encrypted. Where a customer has NetApp Volume Encryption (NVE) encryption applied to a Protected Volume, data held on the Target Volume will not be encrypted, as it will not have access to the customer's NVE encryption key.	Proact
Data Encryption at Rest (Customer)	The customer can choose to apply encryption to Target Volumes. When performed, Proact will hold the encryption keys within the BaaS-SSV Platform. The customer can choose to apply encryption to Target Volumes during service transition or from time to time by logging requests through the Proact <i>Customer Service Portal</i> .	Customer

3.4.5 - Continuity

Deliverable	Description and content summary	Responsibility
Single Site Resilience (Proact)	The BaaS-SSV Platform is architected with N+X redundancy to provide resilience against component hardware failure within the BaaS-SSV Platform.	Proact
Internet Redundancy	Internet access into the BaaS-SSV Platform is provided by redundant firewalls and delivered over diversely routed circuits to provide highly resilient Internet connectivity.	Proact
Backup Data Redundancy	Proact provides the option to replicate customer backup data from the customer's SSV at Proact's primary datacentre to a second SSV at an alternate Proact datacentre, for redundancy. In the event of the loss of the primary Secure Storage Vault platform, the replica SSV can be re-configured to receive backup data and perform restoration. Where the customer requires redundant backup data, it is their responsibility to request this option. Data held in a single SSV will be lost should the BaaS-SSV Platform or its host site be lost. Replication between Proact's datacentres can be introduced to the service at any point during the contract term.	Customer



3.4.6 - Licensing

Deliverable	Description and content summary	Responsibility
ONTAP Storage Licensing (Proact)	Proact will provide the replication software licenses (SnapMirror) for the BaaS-SSV Platform and any Source ONTAP Storage provided by a Proact managed service.	Proact
ONTAP Storage Licensing (Customer)	The customer will provide the replication software licenses (SnapMirror) for their Source ONTAP Storage, where it is not a Proact managed service. Proact are able to provide licenses, at an additional cost, if required.	Customer

3.5 - Configuration

3.5.1 - Backup Service Methods

Deliverable	Description and content summary	Responsibility
Backup Replication	Proact will work with the customer's internal team to initiate backup replication between the Source ONTAP Storage, and their SSV held at Proact.	Joint
Backup Schedule (Proact)	Proact offer flexible backup schedules, configurable per Protected Volume, to meet the customer's protection requirements, within the operating parameters of the product used. The default schedule provides: ▪ Backup replication performed once per day ▪ Backup replication initiated by the SSV hosted at Proact	Proact
Backup Schedule (Customer)	The customer may request modification to the default Backup Schedule, within the operating parameters of the product used. These modifications can be made during service transition or from time to time by logging requests through the Proact <i>Customer Service Portal</i> .	Customer



Deliverable	Description and content summary	Responsibility
Backup Replication Methods	The service provides two backup replication methods: Volume SnapMirror The backup replication includes the data and all incremental Snapshots, existing on the source volume. This provides a mirror of the source volume, meaning the retention period of the source Protected Volume and Target Volume are the same (i.e., source 14 days and target 14 days). ▪ Snapshots created within a Protected Volume are backup replicated to the Target Volume when replication is next initiated ▪ Snapshots deleted from within a Protected Volume are deleted from the Target Volume when replication is next initiated Volume SnapVault The backup replication includes the data and all incremental Snapshots, existing on the source volume. However, with SnapVault, the Target Volume can retain Snapshots for an extended retention period. This means that the retention period of the source and target can be different (i.e., source 14 days and target 24 days). ▪ Snapshots created within a Protected Volume are backup replicated to the Target Volume when replication is next initiated ▪ Snapshots deleted from within a Protected Volume are NOT deleted from the Target Volume when replication is next initiated until the Backup Retention Policy for the Target Volume is reached The customer and Proact will define the backup replication method for each Protected Volume during service transition. The customer may choose to change the backup replication method from time to time by logging requests through the Proact <i>Customer Service Portal</i>. This process will involve deleting the existing Target Volume and reseeding the replication with the new method.	Proact
Backup Retention Policy	Proact configure and maintain a retention policy for each Protected Volume to meet the customer's data retention requirements, within the operating parameters of the product used. The customer and Proact will define the backup retention policy for each Protected Volume during service transition. The customer may choose to modify this policy from time to time by logging requests through the Proact <i>Customer Service Portal</i>.	Joint
De-duplication & Compression	BaaS-SSV will maintain the volume settings between the Protected Volume and the Target Volume. Therefore, de-duplication and compression efficiencies will be replicated between volumes.	Proact
Snapshot Creation	Proact will work with the customer to configure scheduled snapshot creation, as defined with the Backup Schedule. Replication cannot take place if no Snapshots are created. The customer is responsible for ongoing snapshot creation within the Source ONTAP Storage Protected Volumes. All Snapshots created on a Protected Volume will be replicated to the customer's SSV, therefore – where additional Snapshots are created, additional storage may be consumed.	Customer
Snapshot Storage	Snapshots created on the Protected Volumes will consume ONTAP aggregate storage. Where the customer is responsible for management of the Source ONTAP Storage, the Customer will ensure there is sufficient storage capacity available to each Protected Volume to allow for Snapshot Creation and for retention for the required Backup Retention Policy.	Customer



Deliverable	Description and content summary	Responsibility
ONTAP Changes (Customer)	Where the customer makes a configuration change that impacts the replication or Snapshot Creation process, the customer is responsible for monitoring and managing these changes. Where such changes impact the backup service, Proact will not be responsible for the impact on the Backup Schedule or Backup Retention Policy.	Customer

3.5.2 - Restore Service Methods

Deliverable	Description and content summary	Responsibility
Restore Request	The customer may request that a restore is initiated by logging requests through the Proact <i>Customer Service Portal</i> .	Customer
Restore Methods	Restore Requests can be performed to one of two locations: ▪ Out of Place - Copied to the Source ONTAP Storage into a different location to the original data for the customer's administration team to distribute to the user or attach to a server as required ▪ In Place - Copied to the Source ONTAP Storage into the same location as the source data, overwriting the original Multiple restore methods are available. For each Restore Request the method used will vary based upon: ▪ The backup replication method used ▪ The type/format of data backed up ▪ The customer's requirements from the restore ▪ The quantity of customer data to restore Proact and the customer will agree on the best location and method for the restore during response to the Restore Request. The restore methods are: Volume SnapMirror/SnapVault – Out of place ▪ Small restore – CIFS share restore method ▪ Large restore – FlexClone method ▪ Full restore – New replication method Volume SnapMirror/SnapVault– In place ▪ Large restore – NDMPCopy method ▪ Full restore – Reverse mirror method	Proact
CIFS Share Restore Method	▪ Data is copied from the Target Volume via CIFS Share ▪ Data copied to a Restore Area on the customer site ▪ The Restore Area is then shared via CIFS with the customer's IT team	Proact
FlexClone Method	▪ A FlexClone of the Target Volume is made within the SSV ▪ Unwanted data from the FlexCloned volume is deleted ▪ The FlexClone volume is replicated to a new Restore Area volume on the customer site ▪ Once replication is complete, the customer accesses the Restore Area volume to access the data	Proact
New Replication Method	▪ A new SnapMirror relationship is initialised from the Target Volume to a new Restore Area volume created on the Source ONTAP Storage ▪ The Target Volume is replicated back to the customer to allow out of place access ▪ Once replication is complete, the customer accesses the newly replicated Restore Area volume to access the data	Proact



Deliverable	Description and content summary	Responsibility
NDMPCopy Method	- Data is copied from the SSV Target Volume back to the Source ONTAP Storage volume using NDMPcopy - Where required, data is copied to a sub-directory of the original volume to ensure data is out of place	Proact
Reverse Mirror Method	- The existing Protected Volume SnapMirror relationship is reversed - All data is replicated from the Target Volume at Proact to the original Protected Volume on the customer site, overwriting the volume	Proact
Restore Customer Transfer	When requested to perform a restore, Proact will engage with the customer to review the restore method options, within the operating parameters of the product used and define the preferred method.	Joint
Restore Area	Where the customer is responsible for the management of the Source ONTAP Storage, the customer will provide Restore Areas, such as Target Volumes and CIFS shares. The customer will also work with Proact to make replication configuration changes within their ONTAP storage, where required by the chosen restore method.	Customer
Service Best Practice	Where the customer is responsible for the management of the Source ONTAP Storage, it is the customer's responsibility to act upon Proact best practice recommendations delivered during service review meetings or from time to time, to minimise the possibility of exceptional restore delays/failures.	Customer
Exceptional Restore Delays/Failures	Where the customer is responsible for the management of the Source ONTAP Storage and an individual restore task takes over 48 hours to complete, or fails due to one or more of the below: - Storage performance - Available bandwidth - Application configuration - Customer source environment state Proact Professional Services will offer to undertake planning and implementation of the recovery in-line with the customer's needs, as a separate project. Prior to commencement, the customer and Proact will agree the charges for this separate project.	Out of Scope
Restore Space	Where the customer is responsible for the management of the Source ONTAP Storage, the customer will ensure that there is sufficient storage space available to restore their Protected Volumes. To perform an out of place, full restore, the customer must ensure that sufficient free space is available to restore the entire Protected Volume.	Customer

3.6 - Service Deliverables

3.6.1 - Service Monitoring

The following provides an overview of the specific monitoring provided for the service. Proact's standard monitoring deliverables are provided in the Common Service Deliverables appendix.

Deliverable	Description and content summary	Responsibility
Monitored Items	- Backup replication relationship status - Backup replication lag times Proact do not actively monitor the Source ONTAP Storage or servers/applications as part of this service.	Proact



3.6.2 - Operational Activities

Deliverable	Description and content summary	Responsibility
Job Failure Response	Proact monitor the backup replication lag time within the SSV to determine if an issue occurs. When an issue is found, an incident will be created, and the customer will be notified by email. Proact's helpdesk team will investigate the incident. Incident detail will be available in the in the Proact <i>Customer Service Portal</i> .	Proact
Job Failure Troubleshooting	For repeat failures, Proact will contact the customer and both parties will jointly troubleshoot the problem.	Joint
Restore Test(s) (Proact)	Proact will undertake two scheduled restore tests in each twelve-month period (dated from the service commencement). As the data is held off-site within the SSV, restore size will be limited by bandwidth availability. Where there is insufficient bandwidth, or bandwidth contention, for a 2 hour restore task then a subset of the customer's data will be restored in the test and this may require a different restore method, such as 'CIFS share method' or 'FlexClone method'. All test restores will be performed out of place, not overwriting the customer's existing data, and submitted to the Restore Testing Area. Proact will undertake initial restore tests during the service transition phase. These tests will represent one of the two tests allowed in the first 12-month period.	Proact
Restore Testing Area	Where the customer is responsible for the management of the Source ONTAP Storage, the customer will provide restore volumes and CIFS shares that can be used as a test restore target. The customer will agree to work with Proact to make replication configuration changes within their ONTAP storage, where required by the chosen restore testing method. These resources will be agreed by the customer at service start-up and documented within the SOM.	Customer
Restore Testing (Customer)	Where the customer is responsible for the management of the Source ONTAP Storage, the customer will nominate up to 2 data sources for each scheduled Restore Test. Proact recommend that these tests be taken from different restore methods where multiple restore approaches and methods are in use by the customer. Where a successful Restore Request has been performed within two months of a scheduled Restore Test, that successful restore shall constitute a successful test for the given method and Proact recommends this method not be repeated in the next scheduled test.	Customer
GDPR - Right to Erasure / Be Forgotten	BaaS-SSV does not support GDPR's Right to Erasure / Be Forgotten, as ONTAP Storage does not permit the removal of individual files/folders from a Target Volume. The customer can choose to erase an entire Target Volume if required. This will erase all data held within the Target Volume.	Out of Scope
Restore Validation	The customer will confirm that restored data works as expected.	Customer



3.7 - Service Specific Reporting

Deliverable	Description and content summary	Responsible
Service review report (BaaS-SSV)	Within the service review report, Proact will include technical statistics, observations and recommendations regarding the service, in relation to: - Backup service capacity - Protected Volumes - Bandwidth usage Note: The content listed above is an example and is subject to change.	Proact
Service review meeting	Proact will organise service review meetings, by teleconference, at a schedule agreed between both parties, but no more than once per quarter. These meetings will discuss the service review report content.	Proact

3.8 - Acceptance Criteria

Below are the defined service acceptance criteria. Invoicing for the service(s) will commence once the following criteria have been met:

Associated Deliverable	Description and content summary	Responsibility
Secure Storage Vault	Proact have deployed a Secure Storage Vault for the customer in a Proact datacentre.	Proact
Running Backup Process	Proact have performed a successful initial full backup (with no errors) and at least one subsequent scheduled incremental backup of one Protected Volume at one of the customer's source sites, up to a maximum size of 100GB.	Proact
Restore Testing	Proact have confirmed that data has been successfully restored from the SSV backup, for one of each of the following, where appropriate and in scope, and to a maximum size of 100GB in total: - Full volume - Selected files within a volume Each backup will always be restored out of place on the Source ONTAP Storage.	Proact
Monitoring	Proact are successfully monitoring the state of the SSV, and monitoring alerts for these are being sent to Proact's Service Desk for investigation.	Proact

3.9 - Vendor Terms

The services described in this Services Specification will be subject to the vendor terms set out in the table below.

These terms are available in full at <https://www.proact.eu/en/about-us/terms-and-conditions/vendor-terms/>.

Vendor Name
NetApp

3.10 - Service Level Agreement

3.10.1 - Availability Service Levels

This service level agreement sets out what levels of uptime availability Proact will endeavour to provide. Availability is monitored using Proact's software platform. Availability is measured continuously, for the

purposes of the SLAs will be measured in units of a month. Service reports will be provided to the customer quarterly.

Service	SLA	Monthly SLA Description	Measurement
BaaS-SSV	99.5%	The service will be available for at least 99.5% of each month	The BaaS-SSV Platform will be available if the Shared Data Vault and any associated Backup Software located in Proact's data centre responds to Proact's monitoring software
Comms – Internet	99.95%	The Internet connectivity will be available for at least 99.95% of each month	The Internet connectivity will be available if Proact's monitoring software can access commonly available web pages using the communications link.

