

# Veritas NetBackup SaaS Protection

Security overview.

# Contents

---

|   |     |
|---|-----|
| Introduction to NetBackup SaaS Protection . . . . .       | 3   |
| NetBackup SaaS Protection Security Fundamentals . . . . . | 3   |
| Application Security . . . . .                            | 5   |
| Identity Awareness. . . . .                               | 8   |
| Entitlements and Data Ownership Mapping. . . . .          | 8   |
| Shadow Users . . . . .                                    | 9   |
| NetBackup SaaS Protection Sharing . . . . .               | 9   |
| Encryption . . . . .                                      | 9   |
| Storage Account Security and Data Integrity . . . . .     | .10 |
| Auditing . . . . .  | .11 |
| Storage Tiering Security. . . . .                         | .11 |
| Deployment Security . . . . .                             | .12 |
| Operational Security . . . . .                            | .14 |
| Additional Security and Compliance Matters . . . . .      | .18 |
| Security Contacts . . . . .                               | .20 |
| Other Reading . . . . .                                   | .21 |
| Frequently Asked Questions . . . . .                      | .21 |



## Introduction to Veritas NetBackup SaaS Protection

NetBackup SaaS Protection is a cloud-based secondary storage platform for enterprise organizations to centrally protect, analyze, search, and manage all types of SaaS application data at any scale.

NetBackup SaaS Protection customers successfully protect their Software-as-a-Service (SaaS) application data. This is essential now that most SaaS providers have adopted a “shared responsibility model” which makes it clear that the providers will not take any action to protect customers’ data and the responsibility for doing so is completely the sole responsibility of the customer. The need is real. Customers who adopt NetBackup SaaS Protection are seeing the following results: complete backup and archiving of all of their SaaS application data, fast and flexible data recovery, decoupling of data from the storage layer as well as from the SaaS provider’s platform, and a data management engine that supports legal discovery, compliance, and data privacy.

The Veritas solution consists of a cloud-native backbone that runs in Microsoft Azure data centers as a fully-managed software-as-a-service (SaaS) deployment. NetBackup SaaS Protection uses the SaaS providers’ native APIs to seamlessly work to enable backup, archive, migration, tiering, and recovery of data stored on the providers’ platform.

### NetBackup SaaS Protection Security Fundamentals

A primer on the security fundamentals of NetBackup SaaS Protection follows.

- **SOC compliance** – Veritas maintains SOC 2 Type II compliance with security and availability trust service principles for NetBackup SaaS Protection.
- **Single-instance deployment architecture** – By default, the SaaS backbone of your NetBackup SaaS Protection tenant is provisioned as a single-tenant, providing the best possible foundation for a secure environment since your tenant is isolated and running on dedicated resources (no commingling of your data as in multi-tenant SaaS or competition for resources with other customers)
- **Flexible account hosting** – As a single-tenant architecture, NetBackup SaaS Protection offers the flexibility of hosting in your account or Veritas’, and your tenant can reside in any Azure region around the globe (with the exception of China regions when Veritas is hosting)
- **SaaS model** – Veritas always has full responsibility to deploy, manage, monitor, and upgrade your NetBackup SaaS Protection tenant, regardless of whose account is hosting
- **Azure AD identity provider** – Veritas relies on Azure Active Directory (AD) as its identity provider for authentication. For greater clarity, Veritas does not manage passwords of the users signing into the service. With Azure AD handling all sign-in to your NetBackup SaaS Protection tenant, features such as multi-factor authentication (MFA) and single sign-on (SSO) can be enabled to work for your instance
- **Directory synchronization option** – For a completely integrated identity and access experience, Veritas offers the option of directory synchronization with your own Azure AD (see Directory synchronization)
- **Limited attack surface** – While your NetBackup SaaS Protection tenant can consist of multiple cloud resources, there is only one entry point to the tenant for any user or application requests to the NetBackup SaaS Protection App Service (also referred to as the Web App). We’ll explore closely how the Web App security is configured. For now, the key takeaway is that all virtual machines, Azure SQL instances, and other resources within the NetBackup SaaS Protection tenant configuration are not externally accessible, except for blob storage accounts in certain circumstances where security is restricted via time-limited SAS tokens issued after authentication and authorization to specific items for a specific operation



- **Installable components** – Depending on the location of data sources, any necessary NetBackup SaaS Protection installable services can run on-premises, at the edge, or in the cloud. For example, any required installable components might run on customer-owned infrastructure (and are operated by the customer). Requirements such as drive shipping (i.e., Azure Data Box), message journaling, and backup of SaaS applications (e.g., Microsoft 365) typically have Veritas-managed instances of the installable components in the cloud. Your NetBackup SaaS Protection subscription includes usage rights to run any needed Veritas installable components on any number of machines.

## Architectural elements

These are terms used to describe core aspects of the NetBackup SaaS Protection topology:

**Hub** – Each NetBackup SaaS Protection tenant has a top-level configurable element referred to as a Hub which has an associated Hub database (the “HubDB”).

**StorSite** – Within each Hub is one or multiple StorSites which represent an Azure region consisting of at least an App Service instance and at least one blob storage account (a “Stor”). A Hub will have multiple StorSites when the customer organization is geographically distributed and requires localization of compute and storage for network efficiency or data residency.

**Stor** – Within each StorSite is one or multiple Stors which represent an Azure Blob Storage account and its associated Azure SQL database instance (a “StorDB”). A StorSite will have multiple Stors when there are different workload types, or if capacity requirements exceed the limits of a single storage account (i.e., 2 PB for the US and Europe, 500 TB for all other regions, including the UK).



*Deploying NetBackup SaaS Protection on Azure afforded us the agility needed to respond to our engineers with a speed only surpassed by our own hyperloop pod.”*

**Dawn Armstrong, VP of IT**  
Virgin Hyperloop

The following list of elements are in Veritas’ SaaS backbone:

**Azure App Service** – The App Service handles all user and application requests, supports all ingress and egress data flow, and runs Web Jobs to manage data in cloud storage.

**Azure SQL Database** – NetBackup SaaS Protection has an Azure SQL instance for its HubDB which stores configuration and directory synchronization data. Veritas also has an Azure SQL instance for its StorDB(s) which pair with each production Azure Blob Storage account (i.e., a “Stor”) to store certain metadata relating to statistics, auditing, permissions, folders, and items for dashboards, reports, policies, and query optimization.

**Azure Blob Storage** – Azure Blob Storage is where Veritas stores the original data along with metadata manifests and, if content indexing is present, the rendered text of items. A single NetBackup SaaS Protection instance can have multiple Stors – typically one for each SaaS workload being protected.

**Azure Active Directory** – Veritas leverages Azure Active Directory for authentication and, optionally, an identity awareness of all users and groups so that data ownership and access rights fully illuminate for any data in NetBackup SaaS Protection.

**Azure VPN Gateway** – A VPN gateway is used to create a private VNet for certain cloud resources used in the NetBackup SaaS Protection tenant.

**Azure Windows Virtual Machine** – In some deployments, a NSP Connector Service (NSPCS) instance will run on Windows VMs to capture information from target data sources and submit it to NetBackup SaaS Protection for ingestion.

**Azure Ubuntu Linux Virtual Machine** – In most deployments, Veritas runs Elasticsearch on Linux. The NetBackup SaaS Protection search cluster performs content indexing, PII detection, and search. For environments that include message journaling, Linux VMs are also used to host SMTP servers that receive and deliver mail for Veritas.

Any NetBackup SaaS Protection subscription includes access to Veritas' suite of installable app services which consist of the following elements:

**NetBackup SaaS Protection Connector Services (NSPCS)** - The NSPCS is lightweight software that runs as a service on a Windows physical or virtual host. It includes a suite of native connectors to various data source targets (e.g., file directories, OneDrive for Business, Exchange Online mailboxes), which enable simple capture, backup, tiering, synchronization, and migration of data, folders, and access rights to a Veritas tenant. The NSPCS can run on- premises, at the edge, or in any cloud, and you can install any number of NSPCS instances that connect to your NetBackup SaaS Protection tenant.

**NetBackup SaaS Protection Retrieval Service** - The Retrieval Service is a Windows filter driver component that runs as a service on a Windows physical or virtual host. It supports cloud tiering with a seamless recall of data within Windows shares, as well as linked-based stubbing for any SMB or NFS-based presentation.

**NetBackup SaaS Protection Export Utility** - The Export Utility is a lightweight software that runs on Windows to support on-demand, bulk export, and recovery scenarios.

**NetBackup SaaS Protection Export Service** - The Export Service is lightweight software that runs as a service on a Windows physical or virtual host to support background bulk egress requests that are initiated by a user in either the Web-based Admin Portal or User Portal.

**NetBackup SaaS Protection File Copy Utility** - The File Copy Utility is a standalone utility for migrating file data.

Other elements of the NetBackup SaaS Protection architecture are as follows:

**NetBackup SaaS Protection Admin Portal** - Veritas includes a Web-based user interface for IT administrators and other privileged users, supported by the App Service.

**NetBackup SaaS Protection User Portal** - Veritas includes a Web-based user interface for knowledge workers, supported by the App Service.

**NetBackup SaaS Protection Software Development Kit (SDK)** - The NetBackup SaaS Protection SDK offers a .Net client code library that wraps the NSP API. It includes code samples and documentation. All NetBackup SaaS Protection installable software uses the same API that is available in the SDK. The SDK requires a separate NetBackup SaaS Protection SDK Agreement and is available in the Enterprise or Enterprise Plus packages.

**Azure Data Box** - To expedite data ingestion to your NetBackup SaaS Protection tenant, Microsoft offers various form factors to facilitate drive-shipping your data to the cloud. Azure Data Box is a standard Azure service operated by Microsoft that is compatible with Veritas.

## Application Security

### Authentication

Veritas relies on your organization's Azure Active Directory (AD) as its trusted identity provider for all authentication to your NetBackup SaaS Protection. Veritas' claims-based authentication with Azure AD uses OpenID, an industry-standard authentication interface built on OAuth 2 for authenticating via one or more trusted identity providers.

Your NetBackup SaaS Protection tenant can work with multiple Azure AD domains, which is beneficial in merger and acquisition

scenarios. Azure AD enforces password policies and provides rich auditing of authentication-related events. Azure AD's Multi-Factor Authentication (MFA) and Single-Sign-On (SSO) options work with your NetBackup SaaS Protection tenant. If

you do not have an Azure AD domain provider, one will be installed and configured as part of your NetBackup SaaS Protection tenant.

By default, Veritas does not enable non-work accounts to authenticate (e.g., outlook.com, msn.com, and other such accounts), but this can be enabled if desired.

## Authorization

### Role-based access control (RBAC).

NetBackup SaaS Protection includes an RBAC layer that offers the flexibility to manage permissions by AD users and groups, along with the concept of customizable roles.

Access to NetBackup SaaS Protection is account-based and must pass Veritas' authorization layer, including all requests from users and applications, including any of the NetBackup SaaS Protection installable software components that may connect to your tenant, and any application that leverages NetBackup SaaS Protection APIs.

Four permission types exist in Veritas' RBAC layer:

- 1 Feature permissions** – Determine the capabilities that are available with feature-level permissions. For example, you can authorize access to the NetBackup SaaS Protection Admin Portal but restrict access to the Discovery and Content apps only. Likewise, you can authorize access to the NetBackup SaaS Protection User Portal but disable link-based sharing to external users.
- 2 Stor administration permissions** – Define the storage accounts (Stors) that an administration user of NetBackup SaaS Protection can manage with Stor permissions. For example, an administrator with access to the NetBackup SaaS Protection Admin Portal can be allowed to manage retention and deletion policies, but on a particular Stor only.
- 3 Case permissions** – Set which cases a Discovery user can access, including unique case-level permissions. For example, a user with access to the Discovery app in the NetBackup SaaS Protection Admin Portal can participate in several cases but is authorized to export data from a select one only.
- 4 Location permissions** – Restrict all other authorizations to certain folders (locations) within the storage. For instance, a user may be authorized to perform Discovery, view data in the Content app, and perform admin-level exports; however, these capabilities can be restricted to a subset of the organization's data.

Users can belong to one or multiple roles, be granted additional permissions explicitly, and be removed from roles individually or in bulk.

AD groups can be leveraged in NetBackup SaaS Protection's RBAC permissions, directly or in roles, with the advantage of authorizations updating automatically as NetBackup SaaS Protection synchronizes group memberships daily.

NetBackup SaaS Protection's RBAC model includes the concept of a 'default role' which all users belong to automatically. The default role offers a simple way to administer the base level of access globally because it is a single role that can be configured and managed to establish default access for a large end-user community with little effort. The default role can provide any configuration of NetBackup SaaS Protection permissions that you desire. Generally, the default role is configured to allow access to core features in the NetBackup SaaS Protection User Portal only, which, after authenticating, provides users with the ability to view and retrieve their own content.

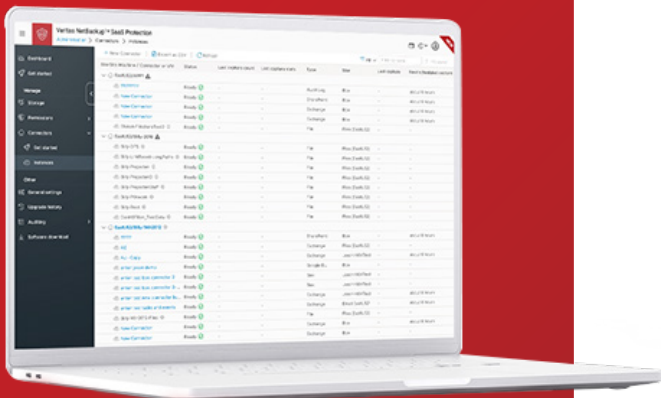
## Directory synchronization

Your NetBackup SaaS Protection tenant may synchronize user information from your organization's Azure Active Directory. Access is read-only and optional, but necessary for certain features in NetBackup SaaS Protection to work fully.

NetBackup SaaS Protection can synchronize with multiple domains/directory providers. Directory synchronization provides NetBackup SaaS Protection awareness of the users and groups that exist in your domain, along with an understanding of the following details:

- ✓ Group memberships (to any level)
- ✓ Account status (enabled/disabled)
- ✓ Extended directory attributes (i.e., Department, Job Title, PreferredDataLocation, etc.)

To allow directory synchronization, you will need to configure an Azure AD application within the target AD instance and provide its Application ID and key to Veritas. Instructions to configure directory synchronization are available in the Veritas knowledge base: <https://helpdesk.hubstor.net/portal/kb/articles/configuring-the-azure-active-directory-synchronization-app>.



The following NetBackup SaaS Protection features require directory synchronization:

- End-user portal
- Link-based storage tiering
- Location mapping policies
- Exchange connectors that use extended AD attributes to filter in-scope mailboxes
- SharePoint connectors that use extended AD attributes to filter in-scope OneDrive for Business site collections

When directory synchronization is not enabled, the features listed above will not be available, and the following NetBackup SaaS Protection features will have the following limitations:

- 1 Custodian-scoped searches in the Admin Portal's Discovery app will yield the result of explicit user permissions only. In other words, access rights via group memberships will not be in the result. Likewise, targeting a Group object will not yield results since, without directory synchronization, NetBackup SaaS Protection is unaware of group memberships.
- 2 Policies in the Admin Portal that use Custodian inclusion/exclusion clauses will yield the result of explicit user permissions only (no access via group memberships).

Policies in the Admin Portal that use Custodian Attribute inclusion/exclusion clauses will not yield a result.

If you opt-out of directory synchronization, Veritas will provision an Azure AD instance within your NetBackup SaaS Protection tenant configuration to act as the dedicated identity provider for your deployment.

## Identity Awareness

### Access rights inheritance

Typically, NetBackup SaaS Protection will inherit the security access control lists (ACLs) of the target data source from which it is capturing data.

In the case of file systems, ACL inheritance is configurable per connector in the NSPCS. Folder-level and item-level ACL options exist. Each time a file connector runs, it synchronizes the latest ACLs, including allow, deny, and inheritance for both user and group objects.

In the case of SharePoint, Teams, and OneDrive for Business, NetBackup SaaS Protection inherits the unique SharePoint permissions model similar to how it works for file systems.

For email, there are several scenarios by which email capture can occur. In general, there are two primary ways that access control inheritance works:

1. The mailbox owner is used to create a security ACL in NetBackup SaaS Protection for all folders and items within the mailbox, or
2. For each message, the sender and recipients list are used to create an item-level security ACL. Item-level ACLs are more expensive on system resources, especially with large object counts, so the preference is to avoid creating ACLs from email sender/recipients wherever possible. However, in certain cases such as email journaling, there is no mailbox context, so sender/recipient-based ACL creation is required.

Likewise, other connectors generally try to inherit data-level permissions from their target source, and any integrated applications using the NetBackup SaaS Protection SDK have methods available to set permissions on items and folders.

**Multiple security identifiers per custodian** In the NetBackup SaaS Protection Admin Portal, there are multiple custodian-related features. (Custodian being synonymous with a user or group object and the data they can access.) When you create a policy or perform a search that uses custodian clauses/filters, you target one or multiple users or groups.

NetBackup SaaS Protection can have multiple security identifiers per custodian. For example, permissions to file system data within a domain will have a unique SID per user/group. If you have multiple domains connecting file shares to your NetBackup SaaS Protection tenant, users can have multiple SIDs across the global dataset. If the different security identifiers of a user are mapped, NetBackup SaaS Protection will return a federated result set.

An SMTP address is another type of security identifier used by NetBackup SaaS Protection for authorization to Microsoft 365 and other email-related data sources. Users can have multiple SMTP addresses within an organization.

NetBackup SaaS Protection provides a federated result when a user or group has multiple security identifiers.

NetBackup SaaS Protection obtains security identifiers from Azure AD for each user and group object during directory synchronization and can also accept load files that provide security identifier mappings.

## Entitlements and Data Ownership Mapping

NetBackup SaaS Protection maintains a query-optimized mapping of access rights and data ownership and the ACL information is persisted into the search cluster.

When any user accesses NetBackup SaaS Protection, its authorization layer performs a union of their direct and role permissions at both the user and group level.

Similarly, when a custodian-based policy or search runs, NetBackup SaaS Protection performs a union of the direct and group-based access rights to trim the results.



## Shadow Users

When security identifiers are present in the data that do not resolve to any user or group found in the directory provider, NetBackup SaaS Protection creates a shadow user profile automatically. A shadow user is a placeholder account that illuminates an identity present in the data but not in the directory. Shadow users will display in NetBackup SaaS Protection as an external user that is not enabled in the directory provider. However, using any of the custodian-based policies or search capabilities in NetBackup SaaS Protection will allow you to specify shadow users.

If a shadow user is later discovered in the directory provider, NetBackup SaaS Protection automatically resolves its pre-existing access rights mapping for the identity.

## NetBackup SaaS Protection Sharing

In addition to the inheritance of source ACLs, NetBackup SaaS Protection has the concept of sharing ACLs. Likewise, items and folders in NetBackup SaaS Protection can be shared internally and externally. The capabilities are controllable in NetBackup SaaS Protection's RBAC model.

Sharing from NetBackup SaaS Protection can be initiated in both the User Portal and Admin Portal.

Auditing of all sharing activity records the grantor, grantee(s), Date/Time, and the specific item or folder that was shared.

In the User Portal, shares can be reviewed and revoked.

In the Admin Portal, settings allow control over the following:

- ✓ Who can share
- ✓ Whether they can share internally and/or externally
- ✓ Whether to allow external users to authenticate
- ✓ Whether to expire shares by default
- ✓ The default share length (in days)
- ✓ Whether to send sharing invitation emails by default

In addition to the inheritance of source ACLs, NetBackup SaaS Protection has the concept of sharing ACLs. Likewise, items and folders in NetBackup SaaS Protection can be shared internally and externally. The capabilities are controllable in NetBackup SaaS Protection's RBAC model.

## Encryption

### In-transit encryption

NetBackup SaaS Protection uses transport layer security (HTTPS / TLS) on all communications between users and apps, and within your NetBackup SaaS Protection tenant running in Azure, with one minor exception relating to a configuration within the search VM (see Search cluster security levels).

### At-rest encryption

NetBackup SaaS Protection provides two approaches for encrypting data-at-rest:

- 1 The first method is the built-in encryption of Microsoft Azure in the cloud known as Azure Storage Service Encryption (SSE) for Data at Rest which is enabled by default on each Stor. Encrypting data at rest in this manner has the advantage of ensuring all data in the Stor has protection. Since data is AES 256-bit encrypted in storage by Microsoft after it arrives in the cloud, functionality such as full-text search and Web-based retrieval work as expected because the keys to decrypt the data are contained within the Azure blob storage security framework of the isolated tenant.
- 2 The second method is the option to encrypt data before sending it to the cloud, which ensures only you can read your data. NetBackup SaaS Protection's pre-ingest encryption option requires both that the target Stor has the Supports Pre-ingest Encryption option enabled, and that the specific connector in the NSPCS has the Pre-Ingest Encrypt option enabled. Thus, it is possible to pre-ingest encrypt a subset of the data that you manage in NetBackup SaaS Protection since multiple connectors can write data to the Stor and connectors may or may not have the pre-ingest encryption option enabled. All data captured by a connector equipped with pre-ingest encryption will be encrypted before going through the ingestion process into your NetBackup SaaS Protection tenant.

When using the pre-ingest encryption capabilities, please note the following:

- The cipher is 256-bit AES encryption
- The key you provide in the NSPCS will be stored on the NSPCS host machine using Microsoft Data Protection API encryption (it will not be stored anywhere else)
- NetBackup SaaS Protection cloud-based features such as full-text indexing for search and any browser-based retrieval from the User Portal and Admin Portal will not be supported since these functions are not able to open the encrypted files
- Other NetBackup SaaS Protection installable software such as the Retrieval Service and Export Service can hold the pre-ingest encryption key(s) so that data accessed through these services can be seamlessly decrypted within your domain

## Storage Account Security and Data Integrity

A chief concern with any cloud storage technology should be the security surrounding the cloud storage accounts. In particular, standard practice for applications writing to cloud storage involves the application having the authentication key and password information for the target cloud storage account. Of course, the app will cache these credentials and the API security information locally, which it should store with encryption. However, regardless of local security measures by the calling application, this model has the sensitive storage account keys distributed to multiple machines outside of the tenant private network, creating a security governance challenge and risk exposure. For example, any compromise of this information would mean exposure of raw access to all the data in the storage account(s).

NetBackup SaaS Protection's unique design ensures the API key and credentials for your storage accounts are never known outside of the secure tenant configuration in the cloud. The NSPCS instances, along with all other NetBackup SaaS Protection installable components and any applications that use the NetBackup SaaS Protection SDK have no knowledge of the destination storage accounts, nor do they have any means of accessing them directly.

For data with a file size of less than one terabyte, Veritas sends data to a staging storage account. After authentication and authorization checks, the NSPCS or writing application are giving time- limited SAS tokens to the staging account. The data is then verified and deduplicated, copied into the final storage account, and then cleaned up from staging.

For large files, NetBackup SaaS Protection optimizes for performance by allowing direct writes and reads into the final storage account. When writing, the NSPCS is given a time-limited write- only SAS token. For any reads of such large files, the requestor is given a timelimited read-only SAS token. NetBackup SaaS Protection supports huge files sizes, much larger than Azure's 4.75 TB limit, which involves chunking files. In the case of chunked files, SAS tokens are issued for each chunk.

Veritas' ingestion methodology always performs inline deduplication, compression, and data integrity checking, and regardless of the ingestion approach (staging or direct), the credentials and API key for your storage accounts are never known or externalized.

## Auditing

All user activity is audited in NetBackup SaaS Protection to maintain a detailed history of all actions taken by users. This includes:

- Activities by end-users such as retrieval and sharing
- System activities that involve data manipulation (e.g., deletion)
- Administrative actions, such as modifying the configuration settings or creating or removing a policy
- Actions taken by privileged users in NetBackup SaaS Protection's data governance applications, such as removing a legal hold in a discovery case

Activity intelligence data can be filtered by date ranges, locations, and/or users and groups. At any time, activity data can be exported from NetBackup SaaS Protection for further analysis.

## Storage Tiering Security

NetBackup SaaS Protection offers multiple methods for storage tiering from target data sources, as follows:

For Windows-based or Windows front-ended file storage:

- Seamless shortcuts
- Link-based shortcuts
- HTML shortcuts

For Windows and any non-Windows (i.e., SMB and NFS) file storage:

- Link-based shortcuts
- HTML shortcuts

For NetApp filers, symbolic link-based tiering is coming soon. For SharePoint, OneDrive for Business, and Teams document libraries:

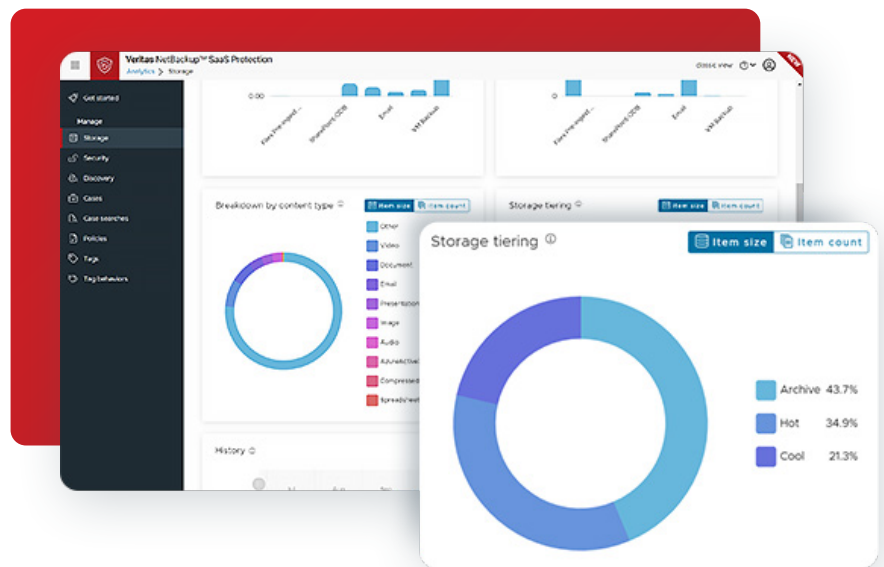
- URL shortcuts

The following is an overview of how authorization security works for each method of storage tiering:

- **Seamless shortcuts** – The default security for seamless shortcuts employs a unique NetBackup SaaS Protection tenant key along with an encoded key that is embedded within each seamless shortcut file. Upon retrieval, the key pairs are evaluated to determine authorization. In this model, the effective ACLs on the source file system remain authoritative. Alternatively, the NetBackup SaaS Protection Retrieval Service has an advanced setting, Require Authorization for Stub Retrieval, which will use the inherited ACL in NetBackup SaaS Protection to perform authorization. Using the advanced setting is viewed as more secure.

However, it has several usability drawbacks since the inherited ACL in NetBackup SaaS Protection consists of domain accounts only. Thus, a user performing the retrieval request from an account logged in as a local user will not pass authorization. Likewise, neither will a user granted access through a local or special built-in group such as domain admins.

- **Link-based shortcuts** – Links point back to a central instance of the Retrieval Service which maintains a corresponding seamless shortcut to recall the file from the Retrieval Service's local cache or the NetBackup SaaS Protection tenant. Link-based shortcuts require authorization checks against the ACLs in NetBackup SaaS Protection, so directory synchronization is a prerequisite. Users



are not able to obtain any directory listing of the Retrieval Service's local cache or its cohort of seamless shortcuts, and the names of seamless shortcuts in the Retrieval Service directory are impossible to guess.

- **HTML and URL shortcuts** – Shortcuts that are a URL to the item, when clicked, open the User Portal in the default browser, requiring the user to authenticate and pass authorization before the item opens. As the authorization checks evaluate the ACLs in NetBackup SaaS Protection, directory synchronization is a prerequisite.
- **Symbolic links** – Security of symbolic link-based tiering will be the same as it is for NetBackup SaaS Protection's current linkbased shortcuts when support is available.

## Penetration testing

Veritas contracts with a third-party to perform application penetration testing.

## Deployment Security

While some multi-tenant scenarios exist, NetBackup SaaS Protection's standard deployment model and architecture is a single tenant.

A single-tenant architecture of the cloud-based resources and software provides the following advantages:

- Isolation for security and performance assurances
- Flexibility for tuning to meet budget, performance, and scalability requirements
- Flexibility to select the hosting cloud data center(s)
- Flexibility to select the account host

## Logical organization of deployed cloud resources

In the cloud, resources dedicated to NetBackup SaaS Protection are deployed and managed within a logical boundary which is typically a dedicated subscription. There are two or three resource groups that serve as logical groupings of the different resource types used by NetBackup SaaS Protection. While deploying into an existing subscription is possible, a new and dedicated subscription is superior because it is better for maintaining a least-privileged authorization posture.

## Hosting configuration

### Veritas-hosted

If your NetBackup SaaS Protection tenant is hosted under Veritas' account, your dedicated NetBackup SaaS Protection resources will be configured in dedicated resource groups.

### Customer-hosted

If you host your NetBackup SaaS Protection tenant, there are several configuration steps required to provide access to NetBackup SaaS Protection's Customer Operations System (COPS). The following list summarizes the requirements:

1. Create a new Azure subscription that will be dedicated to NetBackup SaaS Protection
2. Create a user account that will be dedicated to NetBackup SaaS Protection in your default Azure AD
3. Assign the NetBackup SaaS Protection user account to have the required access to the NetBackup SaaS Protection subscription
4. Create an Azure AD application that will permit NetBackup SaaS Protection's provisioning and monitoring

Instructions to configure the above requirements are available in the NetBackup SaaS Protection knowledge base: [https://www.veritas.com/content/support/en\\_US/article.100050142](https://www.veritas.com/content/support/en_US/article.100050142).

It is important to note that NetBackup SaaS Protection prefers a dedicated subscription because this offers better access control. However, we understand that you may prefer to deploy inside an existing subscription, in which case NetBackup SaaS Protection requires the creation of dedicated resource groups (RG) with a specific naming convention. Such details are coordinated during the kickoff call for your deployment. Either way, it's crucial that you adhere to the following principles when hosting NetBackup SaaS Protection in your account:

- 1 The NetBackup SaaS Protection-dedicated subscription (or RGs) will be for NetBackup SaaS Protection resources only. If you provision other resources here, it will inflate your NetBackup SaaS Protection costs because NetBackup SaaS Protection uses the metered Azure consumption within the boundary to determine your monthly pricing.
- 2 Veritas will be solely responsible for any configuration changes to resources in the NetBackup SaaS Protection-dedicated subscription (or RGs).
- 3 You will maintain least-privileged access to the NetBackup SaaS Protection-dedicated subscription (or RGs) because any accidental or malicious tampering of the resources therein may cause irreversible damage to your NetBackup SaaS Protection tenant. Due to this risk when in your account, Veritas recommends additional safeguards such as:
  - a. Resource locks, and
  - b. NetBackup SaaS Protection backup for Azure Blob Storage accounts

### Vulnerability scanning

To monitor the security posture of your NetBackup SaaS Protection tenant, vulnerability scanning is an option via Azure Security Center.

Given that the App Service is the only external-facing component of a NetBackup SaaS Protection tenant, customers do not typically opt for enablement of Azure Security Center monitoring within their NetBackup SaaS Protection tenant. However, it is available if you want additional assurances. NetBackup SaaS Protection supports Azure Security Center enablement on the App Service(s), Azure SQL instances, and any Windows or Linux virtual machines in your tenant configuration. While Azure Security Center does support monitoring of Azure Blob Storage, Veritas does not support monitoring of this resource type because of false positives resulting from normal batch operations within NetBackup SaaS Protection (i.e., ingesting new data, bulk exports, indexing jobs, etc.).

When enabled, Azure Security Center introduces an additional cost per node enrolled in monitoring. Given the NetBackup SaaS Protection cloud architecture, a valid approach that is cost-efficient is to enroll the App Service instance(s) only.

### App Service security options

The App Service is the only external-facing component of your NetBackup SaaS Protection tenant. By default, the following App Service security characteristics are true:

- All communications and data transfers are encrypted in motion with TLS 1.2
- Any connection is forced to authenticate with your Azure AD directory provider, which can support MFA and SSO options
- Each NetBackup SaaS Protection tenant has dedicated App Service instances
- Within the NetBackup SaaS Protection tenant, a VPN gateway encrypts traffic between your App Service, Azure SQL instances, and search cluster VMs

Enhanced security options are available for your App Service instance(s), as follows:

- For additional isolation within Azure, the App Service Environment (ASE) feature can be enabled
- IP allow lists are supported
- Azure VPN Gateway and Express Route is an option for dedicated network connectivity

## Search cluster security levels

Each search cluster configuration is deployed in what we call a High-Security Model by default.

During indexing of data, the NetBackup SaaS Protection action executor passes BLOBs through a Tika filter engine for text rendering, a step involving potentially large internal data transfers. The rendered text is returned as much smaller data size and submitted to the Elasticsearch engine for indexing and search. The Tika engine runs on the same Linux VM(s) as Elasticsearch which reside(s) in the private VNET. However, to avoid networking performance bottlenecks in the indexing process, communication to the Tika engine does not travel through the private VNet (optional).

This configuration is regarded as highly secure because the Linux VMs and their indexing elements are not externally accessible.

## Billing data

NetBackup SaaS Protection's pricing is based on the number of users whose data is being protected. If your organization grows to have more users than the number you are licensed for, the pricing will be changed to a new level once you have exceeded the initial number in your contract.

If you host your NetBackup SaaS Protection tenant, then Veritas requires access to billing data from your Azure account. An Azure billing API key must be created and shared with Veritas. The key expires every 90 days. Veritas will notify you when the key needs refreshing. The billing API key is an all-or-nothing authorization at the account level. When Veritas queries for billing data, the query result is pruned in memory so that NetBackup SaaS Protection fetches billing data from the specific subscription(s) or resource groups relevant to your NetBackup SaaS Protection tenant exclusively. Veritas does not store, process, or view billing data that is outside of your NetBackup SaaS Protection tenant.

## Operational Security

### SOC compliance

Veritas maintains SOC 2 Type II compliance with security and availability trust service principles. A redacted version of Veritas' SOC 2 audit report is available upon request under a signed non-disclosure agreement.

### The Veritas Customer Operations System (COPS)

NetBackup SaaS Protection uses a custom-built SaaS operations security framework known as the Customer Operations System (COPS) for tenant automation and security. COPS also serves as an abstraction and governance layer so that any and all SaaS administration activity by Veritas does not require direct access to the Microsoft Azure portal. Instead, COPS forces multi-factor authentication, obfuscation, auditing, strict role-based access, and privileged identity management approval workflows.

With COPS, Veritas can attest that personnel in Veritas' DevOps and Customer Success teams do not have the ability to directly access any of the underlying cloud resources, nor can they maliciously or accidentally delete or access your data or resources.

COPS is used by Veritas in the following areas of Software-as-a-Service (SaaS) operation:

- Provisioning and de-provisioning of a NetBackup SaaS Protection tenant or the tenant's resources
- Manual and automatic upgrades
- Health monitoring, maintenance, and diagnostics
- NetBackup SaaS Protection administration activity auditing
- Manage authorizations, including privileged identity management security workflows
- Billing

At all times, COPS is working to obfuscate credentials, API keys, and identifiers associated with your NetBackup SaaS Protection tenant and its underlying cloud resources.

## Privileged admins of COPS

As with any system, there are administrators that have privileged access to COPS and customer resources. This group is known as the NetBackup SaaS Protection Privileged Admin Group. Technically, these users have super-user access to bypass the COPS framework. However, given their roles within the company, they have a vested interest in the success and security of this solution. It is an extremely low risk that these individuals would violate trust or accidentally breach security and risk protocols. Any access by these individuals is audited.

## Privileged identity authorization workflows

Veritas operates authorization workflows facilitated by COPS for privileged users. A NetBackup SaaS Protection tenant can operate one of two modes for approvals: standard or enhanced. For standard security, all authorization grant levels requiring approval have one or more of the members of the NetBackup SaaS Protection Privileged Admin Group at Veritas as the approver.

For enhanced security, a contact designated by the customer organization is the final approver of any authorization grants.

In both models, the following features are true:

- ✓ There are no shared accounts – Veritas personnel must authenticate to COPS through their veritas.com Azure AD account
- ✓ The grantee of the access approval initiates the workflow by logging a request which includes the authorization level type, purpose, and duration
- ✓ All approval workflow requests and grants are audited wherein the audit log is immutable and stored with indefinite retention
- ✓ Authorization grants are time-limited (usually in days)
- ✓ All Admin Portal access is audited (including page views if the relevant setting is enabled)

A self-grant authorization level exists by default to provide Veritas personnel with view-only access to the Admin Portal of your NetBackup SaaS Protection tenant. View-only access never exposes the information stored within your NetBackup SaaS Protection tenant in any way because the user cannot access the Discovery and Content apps (i.e., the individual does not see file and folder names). The view-only authorization still requires the logging of an access request, auditing of user activity, and does not expose your tenant to any risk of data access or tampering by a Veritas employee.

## Executive-privilege tenants

Veritas understands that some organizations require the utmost privacy. To accommodate customers wishing to keep their organization's name a secret, Veritas offers an executive privilege option that ensures that members of the NetBackup SaaS Protection Privileged Admin Group are the only users that can see and manage your tenant. With executive-privilege status, your company's name is hidden within COPS from the DevOps and Customer Success teams at Veritas.

COPS as a protection mechanism against potential rogue behavior COPS uniquely protects clients and Veritas from accidental or malicious insiders. With the exception of the members of the NetBackup SaaS Protection Privileged Admin Group, the COPS security framework ensures that all personnel at Veritas have no ability to accidentally or maliciously access, read, or delete your data or tenant resources.

The COPS framework ensures the following is true for all Veritas personnel (other than the privileged admins) without a time-limited authorization approval:

- They (Veritas personnel) do not need to know, and cannot access, the subscription ID, API keys, or any credentials to any subscription or underlying resource
- They are not able to access Azure resources directly (no view through Azure Portal)
- They cannot accidentally or maliciously:
  - Delete the subscription or any resources therein
  - Delete the NetBackup SaaS Protection tenant configuration
  - Access or delete BLOBs, either as operations directly against a storage account or through any of the NetBackup SaaS Protection interfaces
  - Read metadata of customer data (i.e., file names, folder names)

### **NetBackup SaaS Protection upgrades**

Veritas offers automatic and manual upgrade options for your NetBackup SaaS Protection tenant to stay current on the latest version of the NetBackup SaaS Protection software. When an upgrade occurs, it typically involves no more than three to five minutes of downtime and upgrades generally occur in the off-hours.

With the NetBackup SaaS Protection tenant upgrade complete, the latest version of the installable Veritas software components is downloaded from the Admin Portal. Veritas ensures that new versions of the NetBackup SaaS Protection tenant software are compatible with prior versions of the installable software.

However, it is a recommended best practice to update the installable software versions whenever the tenant software upgrades. In the future, Veritas plans to have the NetBackup SaaS Protection installable components upgrade automatically.

For manual upgrades of the tenant software, Veritas coordinates with you before any upgrade. If you prefer, you can have a dev/test NetBackup SaaS Protection tenant that upgrades first, allowing you to perform any quality control and user acceptance testing before the upgrade of your production tenant.

For most customers, upgrades of their NetBackup SaaS Protection tenant execute automatically. Veritas' auto-upgrade provides you with email notification in advance, and email notification upon completion. The emails include a release notes summary of what is new, and the Admin Portal includes an audit trail of all upgrade activity with a link to the release notes for each version.

The auto-upgrade is flexible in the following ways:

- Each customer enjoys a unique auto-upgrade configuration that suits their preference
- Notification emails can be sent to as many recipients as you desire, and the number of days in advance is also configurable. You can have multiple notification emails (up to five) sent at different configurable times before the actual upgrade.
- The default day and time of the upgrade event is configurable (i.e., Saturday at 6 AM)
- By default, the upgrade interval is every 90 days at an off-hours time. However, the upgrade interval can be more aggressive or more relaxed (i.e., weekly)

Regarding the default auto-upgrade interval, please note the following:

- In the Admin Portal, you will see the date of the next upgrade which you can change if you like. You can always advance or delay the next upgrade
- Veritas publishes a new version about every two weeks. When your tenant upgrades, it will always upgrade to the latest version at the time of your upgrade, and this will be a rollup of everything new since the last version of your NetBackup SaaS Protection tenant
- When set to run on automatic upgrade, if there is ever an urgent update you wish to receive, Veritas can coordinate a manual upgrade at any time



## Software development and release process security

Veritas maintains strict points of control within its development team and software release process.

Veritas uses BitBucket for source control, and Veritas' methodology for managing code changes involves a strict set of principles that are pushed down and managed by Veritas senior leadership.

For all check-ins, Veritas maintains a central point of control. Code changes go through one or multiple review and approval cycles before ultimately being reviewed by the central point of control, which is the Head of NetBackup SaaS Protection DevOps. Thus, this individual has the responsibility of performing a final approval on any code change before it goes into a release stream. For greater clarity, no one in Veritas can check in any code to master anywhere in Veritas' source control without passing the approval workflows which always include the final approval of the Head of NSP DevOps as the central control point. For business continuity, the senior leadership will assume the role of central control point in the event the Head of NSP DevOps is unable to for any reason.

Regarding Veritas' overall release process, for code changes that will go into the mainline code and eventually out to all customers, there is first a prioritization that happens within product strategy. All development items are tracked and prioritized in Jira. Features and fixes are targeted to a sprint per developer. Each developer branches off to make their specific changes. The changes will be staged and enter the approval workflow, which generally has two approvers on any given change. When the change has approval and passes through unit testing, it will go into a release candidate build. The release candidate build will deploy into multiple test tenants automatically where smoke testing and other types of testing occur. When Veritas is satisfied that the changes pass quality control measures, the change goes out with the next release.

## Identity verification for technical assistance

Veritas maintains strict security in its customer success group which is part of the NetBackup SaaS Protection team. Security starts with the concept of named support users – individuals that you have identified to Veritas as being approved to contact us for technical assistance with your NetBackup SaaS Protection tenant.

Veritas will not provide information or assistance to individuals without identity verification. For email inquiries, we require that the sender's email address match what we have on record. For phone inquiries, we require the individual calling to demonstrate their ability to successfully sign-in to the NetBackup SaaS Protection tenant, which requires successful authentication with your Azure AD.

As an additional security measure, you can arrange a security question and answer with Veritas so that any individual requesting support for your organization will have to answer a security question in addition to signing in.

## De-provisioning

Veritas maintains a cancel-any-time subscription model with all customers.

Before de-provisioning a NetBackup SaaS Protection tenant, or any component therein, notification of the request will go to the Veritas NetBackup SaaS Protection Privileged Admin Group through access grant approval workflows in COPS. Approval is required from two NSP Privileged Admins as well as a written authorization from a verified customer admin before a resource or tenant can be deprovisioned.

NetBackup SaaS Protection software includes bulk data extraction capabilities. If your organization decides to cancel, you can export your data from NetBackup SaaS Protection on a self-service basis. Once you are satisfied with the data extraction, simply provide written notification to Veritas of your need to cancel. Veritas will ask for double confirmation. If at any time you require assistance with data extraction, please contact our Help Desk: <https://www.veritas.com/content/support/contact-us>.

## Additional Security and Compliance Matters

### Confidentiality

Veritas maintains strict confidentiality requirements internally and observes all confidentiality obligations defined between our organizations

### Government / law enforcement data requests

Veritas will not disclose your data to government or law enforcement agencies except as you direct or where we must by law Veritas will not entertain unlawful requests Unless Veritas is legally prohibited from doing so, we will promptly notify you of any such demand with a copy of the court order or subpoena

### GDPR and other data privacy compliance

Veritas' Master Subscription Agreement (MSA) includes a schedule dealing with Veritas' obligations as the data processor under the

### GDPR

Neither Veritas nor Microsoft use your data or derive information from it for advertising or data mining This policy is backed by Veritas' MSA (Microsoft supports their similar policy in their enterprise cloud service agreements) Veritas generates anonymized pattern data but never accesses your data without your written permission There is generally no need for Veritas to access your data However, the authorization process does exist for scenarios where a customer requests us to do so for testing, or for regulatory compliance reasons (e.g., a designated third party under the SEA Rules)

In addition to day-to-day operations, Veritas support and services personnel may access diagnostic or pattern data of your NetBackup SaaS Protection tenant to provide customer support or optimize the service

### Microsoft security and compliance

NetBackup SaaS Protection runs in Microsoft Azure exclusively, a leading cloud infrastructure that meets a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2 Information about Microsoft Azure security, privacy, and compliance can be reviewed on the Microsoft website: <https://www.microsoft.com/en-us/trustcenter/>.

### NetBackup SaaS Protection data management features

The following describes the advanced data management capabilities that are found in the NetBackup SaaS Protection Admin Portal

All data that you manage in NetBackup SaaS Protection can be understood through file analysis capabilities By default, attributes such as file size, file type, last accessed date, and last modified date will have statistical aggregation computed automatically on a nearreal-time basis NetBackup SaaS Protection provides visualization of the data in each storage account Policies and searches can be used to isolate specific data sets, producing a dashboard visualization and a content browser view of the query results. Queries into the storage footprint can leverage combinations of the following clause types:

- Include Locations
- Exclude Locations
- Include Location Tags
- Exclude Location Tags
- Include Custodians
- Exclude Custodians
- Include Custodians by Extended AD Attribute
- Exclude Custodians by Extended AD Attribute

- Include Tags
- Exclude Tags
- Include Tag Behaviors
- Exclude Tag Behaviors
- Include Item Names
- Exclude Item Names
- Removed From Source
- Removed From Source At
- Item-level WORM Retention
- TotalBlobSizeKB
- LastModified
- LastAccessed
- ItemType
- DataOwner
- StorageTier
- CapturedAt
- And any list of item-level attributes that are specified in the metadata definition of the Stor configuration



*NetBackup SaaS Protection has been a reliable solution, delivering protection of our Office 365 data and supporting our litigation and GDPR requirements.*

**Steven Menmuir, Solutions Architect**  
Repsol Sinopec Resources UK

### Data classification

NetBackup SaaS Protection includes personally identifiable information (PII) and other sensitive data detection and tagging capabilities. Standing queries and regular expressions can be configured and will evaluate against all data that is in the scope of full-text indexing.

Customizable tags can apply to data containing PII or other things of interest, and be used for tracking, reporting, and to apply litigation holds or retrieval blocking.

### Discovery

NetBackup SaaS Protection is equipped with discovery features that can assist you in an audit, investigation, legal claim, or GDPR response.

You can create and manage cases, perform federated searches across storage accounts, save queries, report on search results, save results to a case, and export a case's saved searches.

All discovery search and export activity are audited. Search audit records include query parameters, users, and Date/Time.

Discovery capabilities in NetBackup SaaS Protection: [https://www.veritas.com/content/support/en\\_US/article.100050111](https://www.veritas.com/content/support/en_US/article.100050111)

### Litigation hold

NetBackup SaaS Protection provides multiple methods of applying litigation holds to your data, as follows:

1. By search added to a case
2. By user holds within a case
3. By tagging policy where the applied tag has the associated legal hold tag behavior

Items on hold are exempt from deletion by any NetBackup SaaS Protection deletion policies. NetBackup SaaS Protection provides insight into data that is on hold with dashboards and the content browser found in the Admin Portal.

Litigation holds in NetBackup SaaS Protection: [https://www.veritas.com/content/support/en\\_US/article.100050115](https://www.veritas.com/content/support/en_US/article.100050115).

## Immutability

NetBackup SaaS Protection is built upon a read-only object storage technology. In the service, there is one way to perform deletion: deletion policies found in the Admin Portal. For this reason, NetBackup SaaS Protection includes legal hold and Write-Once-Read-Many (WORM) retention periods to optionally prevent data from destruction.

When data is on legal hold or has a WORM retention period, it will not fall in the scope of any deletion policies and the deletion action executor performs item-level checks to verify that each item in scope of a deletion policy is eligible for deletion before executing any deletion.

NetBackup SaaS Protection also integrates with the Azure Immutable Blob Storage capabilities to enforce immutability at the cloud provider level.

## NetBackup SaaS Protection backup and disaster recovery

Many customers preserve data in their NetBackup SaaS Protection tenant, and NetBackup SaaS Protection becomes the master copy of the information. As such, a backup and disaster recovery strategy for your data in NetBackup SaaS Protection is paramount.

While data in your NetBackup SaaS Protection tenant is stored with synchronous replication within an Azure region by default, such redundancy is not a true backup of your information. Enabling Azure's geo-redundant storage options provides replication to a secondary Azure region. However, the secondary account is not a true backup. For this reason, NetBackup SaaS Protection provides a fully-managed cloud backup option that makes a true secondary copy of your NetBackup SaaS Protection Azure Blob Storage account(s).

NetBackup SaaS Protection's cloud backup option typically negates the value of Azure geo-redundant storage (GRS) or Azure read access geo-redundant storage (RA-GRS) since it can accomplish the same result (an asynchronous Azure locally redundant storage (LRS) copy of the primary in a second Azure data center for a total of six copies). However, NetBackup SaaS Protection's cloud backup approach offers distinct advantages over Azure's GRS storage. For example, NetBackup SaaS Protection's cloud backup is decoupled from the primary storage account (it is purely additive in the secondary storage account). With GRS, a malicious or accidental deletion of BLOBs in the primary would synchronize to the secondary. Whereas, with cloud backup, the data in the secondary account would not be deleted.

NetBackup SaaS Protection's cloud backup also provides greater flexibility regarding the Azure data center that hosts the secondary storage account. The storage tier of the backup account does not have to match that of primary (meaning all backup data can costefficiently reside in the Archive tier). In a regional failover scenario, we have complete control over the timing of the failover wherein both writes and reads can occur against the secondary account.

The backup storage account can and should be in a separate subscription. Veritas offers the flexibility for the backup account to exist in any Azure region (including the same as your primary if you wish to avoid egress bandwidth costs). Cloud backup is not a default feature of the service. It must be requested.

## Security Contacts

### Report a security incident

If you believe there's a security incident related to NetBackup SaaS Protection, or that may have any relation to Veritas, please report it to the Customer Success Help Desk. There are three ways to report an incident:

- Submit a ticket online via the Help Desk (you may need to register as a user if you are new to using the Help Desk).  
<https://www.veritas.com/support/>
- Call us toll-free at +1 (866) 837 4827

## NetBackup SaaS Protection Security Contacts

If you have any security issues or questions, please reach out to the NetBackup SaaS Protection team either by opening a support ticket at <https://www.veritas.com/support/>, or if it's not an urgent question, contact us here: <https://www.veritas.com/content/support/contact-us>

## Other Reading

How to Enable Directory Synchronization: [https://www.veritas.com/content/support/en\\_US/article.100050221](https://www.veritas.com/content/support/en_US/article.100050221)

Prepare Microsoft Office 365 for NetBackup SaaS Protection: [https://www.veritas.com/support/en\\_US/article.100050145](https://www.veritas.com/support/en_US/article.100050145)

NetBackup SaaS Protection Pre-deployment Requirements - Veritas Hosted: [https://www.veritas.com/content/support/en\\_US/article.100050144.html](https://www.veritas.com/content/support/en_US/article.100050144.html)

NetBackup SaaS Protection Pre-deployment Requirements - Customer Hosted: [https://www.veritas.com/content/support/en\\_US/article.100050142.html](https://www.veritas.com/content/support/en_US/article.100050142.html)

## Frequently Asked Questions

Q: Does NetBackup SaaS Protection support deployment into Azure Government regions?

A: Yes.

Q: Does NetBackup SaaS Protection support deployment into Azure China regions?

A: Yes, but only under a customer-hosted account. NetBackup SaaS Protection does not support deployment into Azure regions in China when hosting under Veritas.

Q: Is NetBackup SaaS Protection SOC 2 compliant?

A: Yes. Veritas maintains SOC 2 Type II compliance with Security and Availability TSPs.

Q: Does Veritas perform background checks on its employees?

A: Yes, as part of the hiring process, new employees must pass an international background check prior to their start date.

Q: Does Veritas have an insurance policy covering cyber threats liability?

A: Yes.

Q: Does Veritas use multi-factor authentication and single sign-on for all employees?

A: Yes. Both MFA and SSO are enabled for all employees.

## About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at [www.veritas.com](http://www.veritas.com). Follow us on Twitter at [@veritastechllc](https://twitter.com/veritastechllc).

# VERITAS™

2625 Augustine Drive  
Santa Clara, CA 95054  
+1 (866) 837 4827  
[veritas.com](http://veritas.com)

For global contact  
information visit:  
[veritas.com/company/contact](http://veritas.com/company/contact)