VERITAS

Veritas Alta Backup as a Service Security Overview

This whitepaper is intended for IT professionals, IT managers, and IT security and risk management personnel.

White Paper | March 2023

VERITAS ALTA™

Revision History

Version	Date	Changes
1.0	March 2023	Initial release

Contents

Contents

Executive Summary

Veritas Alta™ Backup as a Service is a hosted service that helps enterprise IT organizations deal with data sprawl from the migration of applications to the cloud. It provides comprehensive, highly performant, scalable, and secure backup as a service without the burden, complexity, and cost of managing backup hardware and infrastructure.

When it comes to cloud-based services, security is a key consideration. A big question that many organizations ask is: *if we let our data reside outside my own controls and processes, how secure is it?* Any uncertainty can keep an IT management and professionals up at night.

With Veritas Alta Backup as a Service, we plan the security of our cloud-based service around three core areas:

1. Physical Security: Security and resiliency of hosting datacenter buildings and facilities.
2. Technical Security: Security of customer data, our systems, networks and applications.
3. Administrative Security: Secure processes across every level of an organization.

This white paper takes an in-depth look at our security along with the systems and processes that support it.

Veritas Alta Backup as a Service Overview

Key Capabilities of Veritas Alta Backup as a Service

- Effortless: Increase agility and time-to-value with the simplicity and ease of a flexible, cloud-optimized service
- Cost-Efficient: Optimize cost investments without sacrificing quality and function
- Secure: Assure business availability and continuity with comprehensive, intelligent cyber resiliency

How is it Delivered?

As a hosted service—Veritas Alta Backup as a Service is hosted under Veritas management, offering a high level of security and availability and the big data capabilities of its underlying technology platform.

Architecture

Veritas Alta Backup as a Service comprises two main components; the management plane and the control plane plus data plane.

- The management plane is a central portal where customers manage their service from
- The control plane orchestrates protection and recovery of assets. The data plane is co-located with the control plane, and secures the backup data

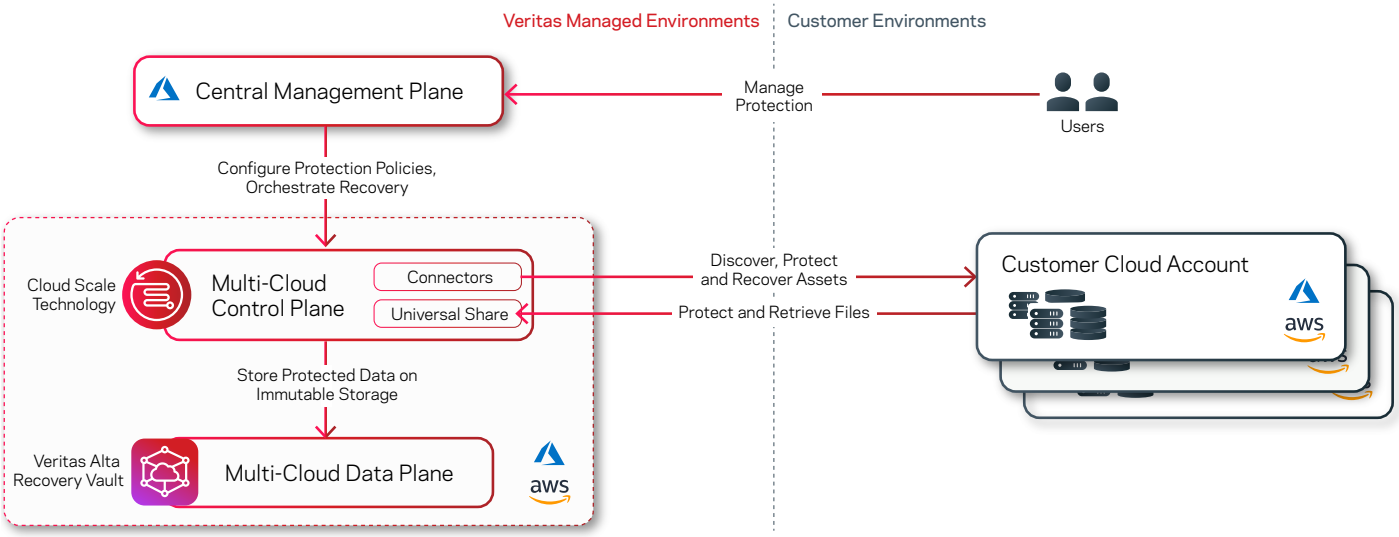

Figure 1. Veritas Alta Backup as a Service main components

Application Administration

Centralized administration is offered through the cloud-hosted Veritas Alta management portal.

- **Secure Sign-On:** Administrative and end-user accounts can be managed either with the Veritas identity provider or customers can integrate with their existing identity provider. See Identity Management for more details.
- **Role-Based Administration:** Ensures you can segregate your administrators from your Veritas Alta Backup as a Service users.

Physical Security

Veritas operates Veritas Alta Backup as a Service in the cloud. The Veritas cloud platform leverages the underlying security and standards of the cloud service provider. As an example, Microsoft Azure provides multiple levels of physical security and is compliant with many standards such as ISO 27001, ISO 9001, SOC, the PCI Data Security Standard and the US Government's Federal Risk and Authorization Management Program (FedRAMP). Details on Azure's security and compliance can be found here:

azure.microsoft.com/en-us/explore/trusted-cloud/compliance/

learn.microsoft.com/en-us/azure/compliance/

Azure's Certificates, Regulations and Standards reports:

Service Trust Portal Home Page (microsoft.com)

Data Isolation and Residency

The management plane is a multi-tenant services that provides customers administrative access to configure protection of assets and recovery. The management plane stores configuration information provided by the customer and metadata about the assets that are discovered and protected.

Each customer is provisioned as a separate tenant within the management plane service and each tenant is logically isolated in different database schemas. Access controls to ensure only authorized identities can access each tenant. The management plane is currently hosted in the United States of America.

The control plane orchestrates protection and recovery of assets, storing metadata and managing the backup data. Veritas deploys a separate control and data plane for each customer in each of their cloud service provider regions that they wish to protect. All data from protected assets is stored in the same region as the asset itself; the data does not leave the region or the cloud service provider network.

In the example diagram, Acme and GloboCorp are protecting assets in two regions in Azure and AWS. Veritas provisions both customers with a separate control plane and data plane in a matching region to their assets. This ensures that data never leaves the cloud service provider for security purposes and stays in-region to help with any data residency requirements.

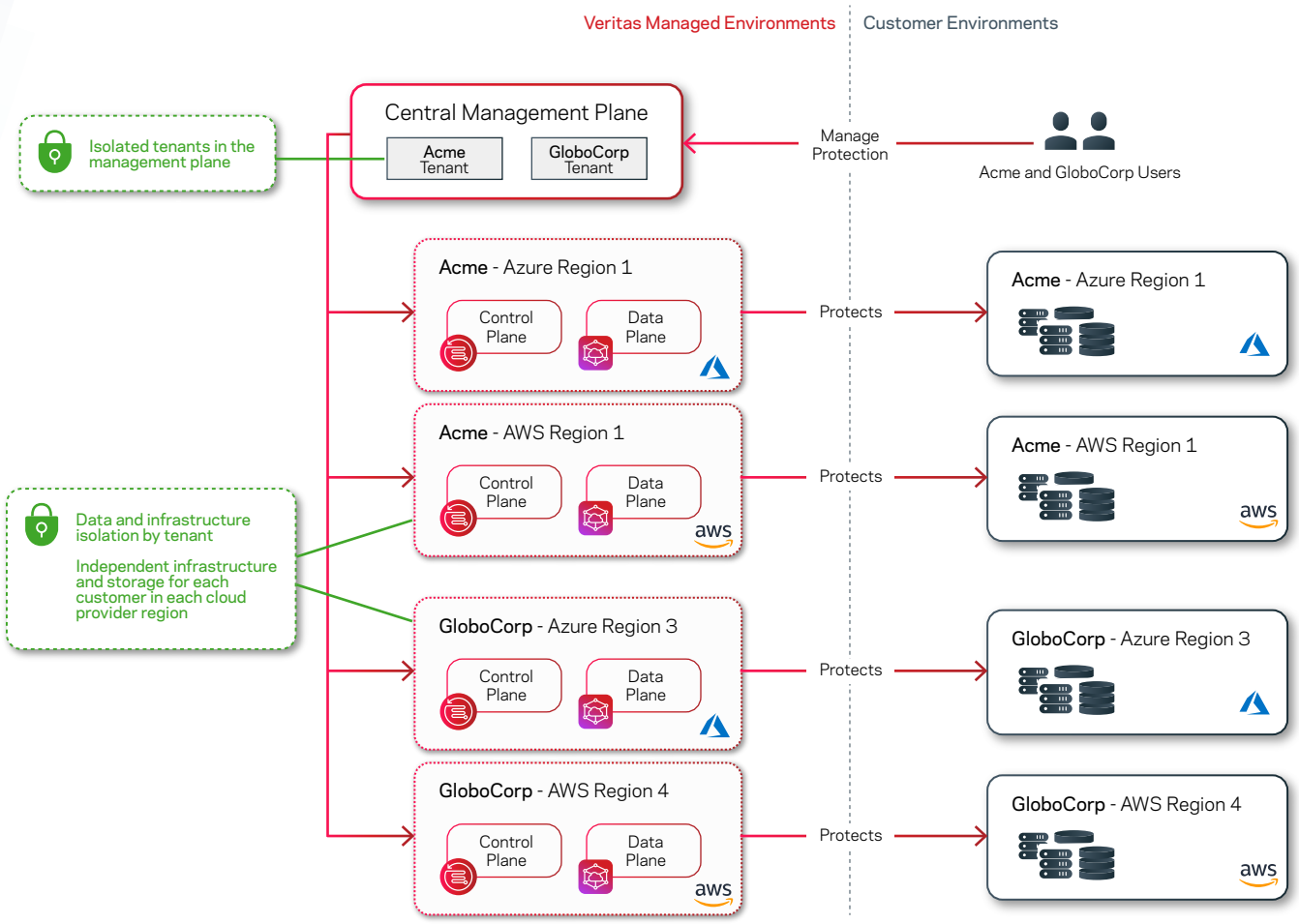

Figure 2 – Veritas Alta Backup as a Service – data isolation

As Veritas deploys new instances of the management plane in locations such as Europe and Asia Pacific, customers will be able to choose the location where they would like to manage the service. Note that the location of the management plane does not restrict where assets can be protected; control plane instances can be deployed in any supported region worldwide.

Technical Security

The following technical controls support our infrastructure, application, and data security policies:

Infrastructure Security

Virtual Private Cloud

The Veritas Alta Backup as a Service management plane, deployed in Azure, is isolated and protected from external access using Azure's Virtual Networks and Web Application firewall. Strict security and network access controls restrict the traffic that can enter and leave the network as well as who can access the services for operational reasons.

The control plane, which is deployed in Azure or AWS depending on the assets to protect is strictly isolated using Azure and AWS network security mechanisms. The control plane cannot be remotely accessed from the public internet; the only outgoing connections allowed are to the management plane and the customer's environment. An outbound-initiated connection to the management plane is used to report status and control asset protection. An outbound-initiated connection to a customer's AWS or Azure account is used to protect assets; the control plane uses a private link service to ensure that data flows only over the AWS and Azure private network and not the internet.

Firewalls

Firewalls are used to block internet-based attacks and maintain high availability for the public-facing web application and API web service endpoints. This performs traffic inspection including OWASP and BadBot protocols. Suspicious activity is automatically detected and blocked.

Minimum System Baselines

Our standard Linux-based container images and services align to industry best practices; only the required services are enabled and system hardening measures are applied. Automated configuration analysis tools help ensure continuous baseline compliance.

Vulnerability Scanning

Veritas conducts regular vulnerability scanning using internal tools and third-party assessment of security, with penetration testing in pre-production and production. These periodic tests help ensure that Veritas Alta Backup as a Service remains secure.

Veritas uses standard industry processes and tools for assessment and notification of external threats and software vulnerabilities discovered by other trusted security sources.

Patches are applied and/or risk mitigation measures put in place in a timely manner based on the severity and exploitability of the scored vulnerability.

For more information about vulnerability scanning, please see the System Security section.

Application Security

The Veritas Application Security Assurance Program (ASAP) is a risk-based software assurance process that includes comprehensive and rigorous software development processes and procedures that are consistent with Building Security in Maturity Model (BSIMM) industry standards. The ASAP scrutinizes products across different categories, including:

1) Training (application security specific);

2) Requirements (data classification);

3) Design (threat modeling and cryptography);

4) Implementation (static and dynamic analysis security testing);

5) Verification (vulnerability scan and third-party pen testing);

6) Deployment (third-party software review and readiness); and

7) Operations (customer support for security and vulnerability management).

Role-Based Access Controls

Role-based access control (RBAC) is provided to support a separation of duties within the product. Veritas Alta Backup as a Service provides predefined roles that customers can assign to application users. New roles can be created to support business processes and granular delegation of responsibilities.

Identity Management

Customers can choose to integrate their own identity provider (IDP) with Veritas Alta Backup as a Service, or use Veritas as the IDP. Veritas recommends that customers use their own IDP to better manage identity lifecycle and make use of existing controls from their IDP such as multifactor authentication (MFA), conditional access policies and device checks, etc. Veritas offers its own IDP to help get started quickly, with the ability to switch over to an external IDP at any point.

Each user can additionally obtain an API key which allows programmatic access to the Veritas Alta Backup as a Service REST APIs in the context of that user and the roles they have been assigned.

Using the Veritas Identity Provider

The Veritas IDP works by creating user accounts based on a user's organizational email address. Strong password policies with historical checks are enforced, and enrollment for MFA is mandatory. The Veritas IDP is powered by Okta Cloud, which provides MFA options via mobile authenticator apps. Email and SMS factors are explicitly disabled since they are less secure.

Password Policy for Veritas IDP

These restrictions apply only to user accounts created in the Veritas IDP:

- Minimum of eight characters in length
- No more than two identical characters in a row
- Contain at least three of the following four types of characters
  - Special characters (!@#$%^&*)
  - Lower case (a-z)
  - Upper case (A-Z)
  - Numbers (0-9)
- Do not allow re-use of the previous 10 passwords
- Prevent use of passwords containing parts of a user's email address or name
- Do not allow passwords that are part of 10,000+ commonly used passwords

Using an External Identity Provider

The Veritas Identity Service supports single sign-on (SSO) through federated authentication to other IDPs with SAML 2.0. This enables customers to use their own IDP for user management and authentication.

In this mode, the customer manages their user accounts, credentials, and password policies in their own IDP. Veritas Alta Backup as a Service then securely brokers the authentication process with the IDP and receives the authenticated user's identity such as their email address. Note that in this mode, role-based access controls are still defined and managed within Veritas Alta Backup as a Service.

Attack Protection

Veritas enables various mechanisms to protect against user account attacks such as suspicious IP throttling and brute force protection.

Session Management

After users have authenticated, a session is created for them in Veritas Alta Backup as a Service. The session expires after 15 minutes of inactivity, and has a hard limit of six hours; after six hours, the user must re-authenticate. Shortly before reaching the inactivity limit, users are informed within the web application that they will be logged out, and have a choice to extend an inactive session.

Veritas Alta Backup as a Service and each user session ID control sessions is stored in a secure cookie on the browser for the duration of the session. The cookie is a temporary session cookie which is deleted by the browser when it is closed, even if the user does not select the Sign-out option in the application. This means that when the browser is re-opened, the user must sign-in again.

Audit History

All end-user logins, in-application activity and API client activity is audited and available as read only to customer's administrators through the Administration Console.

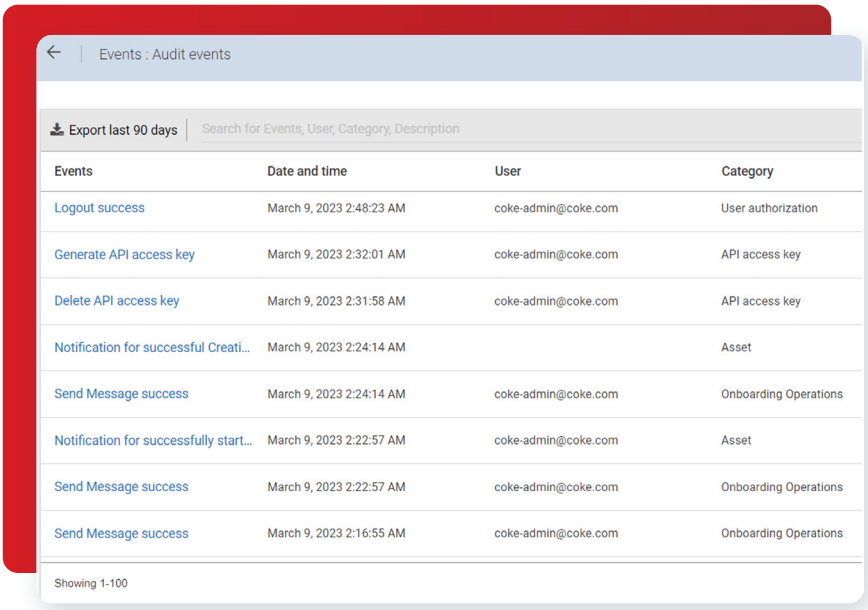

Figure 3. Veritas Alta Backup as a Service audit events

Data Security

Veritas employs a variety of security measures to ensure the security of data-in-transit and at-rest within the cloud platform.

Data Isolation and Segregation

The Veritas Alta Backup as a Service management plane is a multitenant solution that uses application security and logical boundaries to segregate and protect customer metadata.

For asset protection using the control plane, each customer is serviced with at least one independent, isolated backup infrastructure dedicated to them. Backup data is stored in logically separate locations for each customer within Recovery Vaults. A recovery vault is created for each control plane instance and access to that recovery vault is only granted to that single control plane instance.

Encryption of Data-in-Transit

All data sent to or retrieved from Veritas Alta Backup as a Service is over HTTPS; secured using an encrypted Transport Layer Security (TLS) channel.

Public endpoints exposed by the management plane for portal access only allow connections over TLS v1.2 and TLS v1.3 using the most secure cipher suites.

The Universal Share feature can be enabled to expose a protected file share using NFS and SMB protocols. To secure data in transit, Stunnel is used to add TLS v1.2 encryption for data sent to and received from a Universal Share. Stunnel is an open-source network relay, and is installed on the control plane and the client that mounts the file share. Mutual authentication and encryption in Stunnel uses a pre-shared key.

Encryption of Data-at-Rest

Veritas Alta Backup as a Service utilizes Veritas Alta Recovery Vault as target for customer-initiated backups. Data stored in Veritas Alta Recovery Vault is encrypted with AES 256-bit encryption and is FIPS 140-2 validated.

All metadata stored in the management plane is encrypted at rest using AES 256-bit encryption.

Encryption Key Management

Veritas manages encryption keys for Veritas Alta Backup as a Service management plane using Azure Key Vault. All customer metadata at rest in the management plane is encrypted using keys derived from a primary key that never leaves Azure Key Vault.

Veritas manages encryption keys for Veritas Alta Backup as a Service control plane and data plane which is used to encrypt the backup data.

Immutable/Write Once, Read Many (WORM) Storage

Immutable/WORM (Write Once Read Many) storage for backup data is supported and enabled by default by Veritas Alta Backup as a Service.

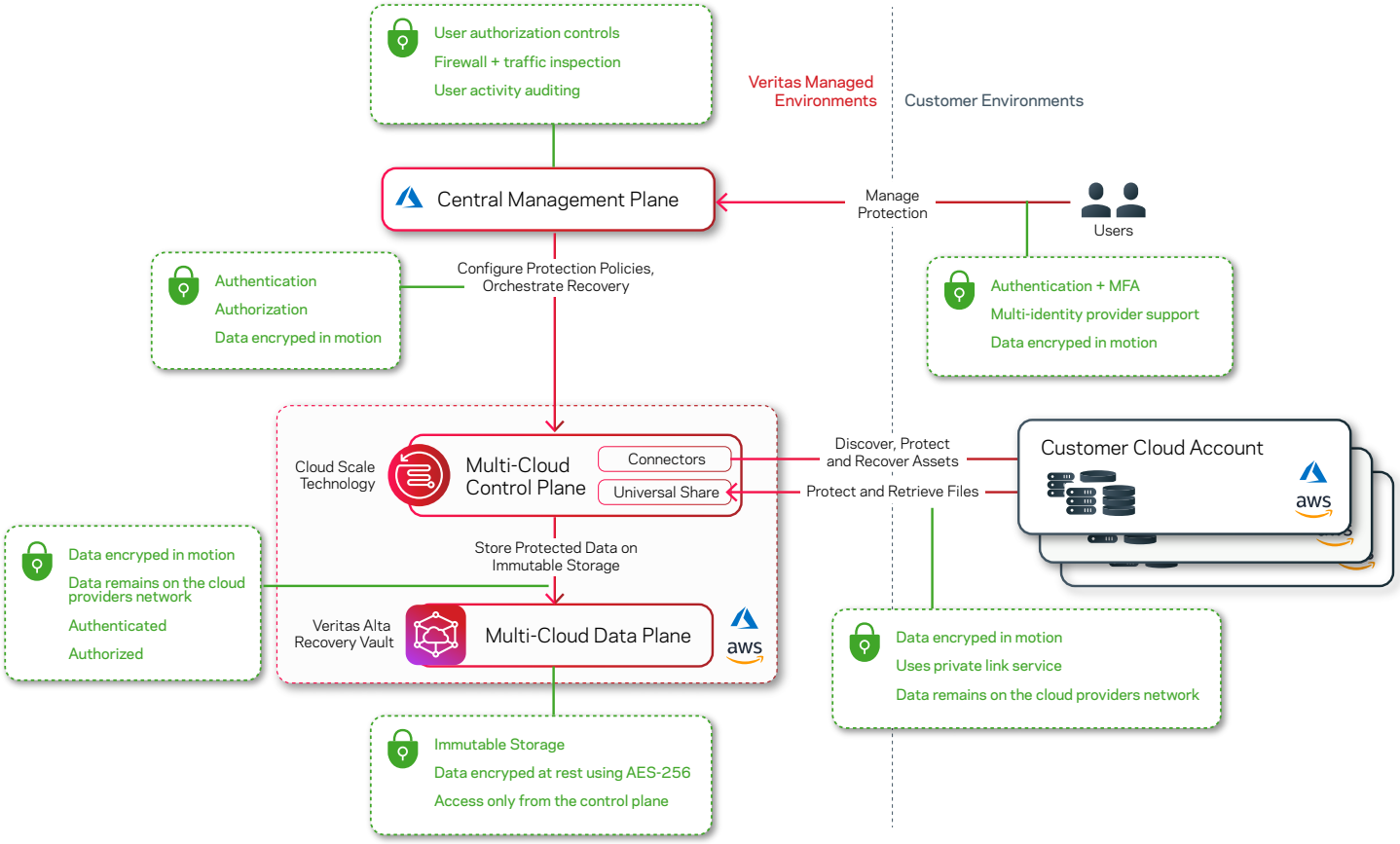

Figure 4. Veritas Alta Backup as a Service—data security

Deletion of Data on Service Termination

Upon request to terminate the service, all data that resides in the cloud platform managed by Veritas is deleted and a Certificate of Destruction is then issued to the customer. The customer's unique encryption key is also removed from the service. The timeframe to complete data deletion is covered in the Service Agreement.

Administrative Security

Veritas has several administrative controls in place to help ensure defense-in-depth security through a layered security strategy. Administrative control measures are enforced through a combination of policies and processes.

Process Security

Change Management

Veritas releases a variety of enhancements and fixes on a regular basis to improve the performance and security of our services. To minimize security risk and maximize service uptime, we follow a strict change and configuration management process.

Any changes to production environments must have an associated Change Management Request. Changes cannot be implemented without a Change Management Request and the associated approvals.

Proposed changes are reviewed by a Change Review Board (CRB). The major benefits of implementing formalized Change Management are:

- Tracking production changes
- Peer- and management-level review of changes prior to implementation
- Fully documenting changes
- Centralized knowledgebase on what/where/when changes are being made
- Documenting processes for executing change, post-change testing, and fallback procedures if the change does not occur as planned
- Performing a security review to assess impact to existing security posture
- Testing of changes in a dev/test environment prior to going live in production

The CRB can approve, reject, or place a change request on hold based on the details available in a change ticket or possible conflicts with other approved/scheduled changes.

Access Management

User access management practices exist to support our Access Control Policy. Access, onboarding, change requests, or terminations can only be made by a Veritas employee at a manager level (or higher). Access is provisioned based on the principles of least privilege, default deny, and separation of duties. Privileged administrative users also have unique accounts for non-administrative duties, and both are logged for auditing and accountability purposes.

All remote administration access to cloud resources requires the use of Veritas VPN tunnels combined with two-factor authentication. This authentication includes strong passwords and tokens.

Remote access to the cloud management consoles is restricted to key employees whose duties are to ensure the service is operational.

The security team performs regular audits of privileged account use, cloud management console audit trails.

Ninety-day inactive accounts are audited on a quarterly basis and disabled upon discovery.

We follow a controlled, repeatable, and documented process when an employee leaves the company. This ensures that our security policies are met, including returning keycards and other company equipment and disabling user accounts. Access to systems is promptly revoked following termination of employment.

Access Policy for Customer Data

Veritas does not require access to your customers' encrypted content stored in the disk. By default, Veritas does not grant employees access to customer data. Veritas will not sign on to the Veritas Alta Backup as a Service customer portal unless access is provided via a customer for a support case.

However, events such as diagnosing issues may require limited access to data in the cloud service, such as:

- Service-wide degradation or failure that impacts multiple customers
- Diagnosis or remediation of a customer-raised issue in the cloud service or on-premises software
- Customer request for access to bespoke user or application audit events

Uptime Monitoring

Veritas employs a variety of monitoring systems, which produce alerts for our data center operations, engineering, and management teams via alert systems in the event of system availability concerns and/or performance issues. Our operations staff have an around-the-clock on-call rotation model. On-call Veritas staff are responsible for tracking alerts and identifying potential issues.

Systems Monitoring

Veritas uses multiple IT management software frameworks for monitoring of core systems, including:

- Storage devices
- Network devices
- Servers
- Operating systems
- Databases
- Key application processes/services

Application Monitoring

Customized monitoring and metric tracking are used to monitor critical components and data flows for deviations from trends and abnormal response times.

External Monitoring

Veritas Alta Backup as a Service uses a third party to monitor our services externally from the internet to simulate customer access. The service has points of presence around the world, and performs availability monitoring on an automated, regular basis.

Uptrends is configured to perform many tests, including the following tests every five minutes from every POP:

- Veritas alta portal connectivity
- Web service API connectivity

Application Response Monitoring

Veritas tracks and monitors metrics to help maintain a responsive interactive experience and ensure the responsiveness of the web service APIs.

System Security

Vulnerability Testing

Veritas uses multiple tools to monitor infrastructure and application resources.

Veritas System Auditing

Audits are key to our overall security strategy, providing a thorough evaluation of our threat exposure. This information allows us to proactively address any potential vulnerability. Using third-party tools and independent third-party penetration testing also allows us to confirm remediation efforts are successful and security baselines are maintained. Frequent audits include automated and manual penetration testing including critical risks identified by the OWASP Top 10 project and other industry-standard best practices for security configuration and control.

Independent third-party penetration tests include review of internal systems, providing a complete evaluation of the environment. Once we receive the report, our security team works aggressively to address any potential vulnerability. Identified vulnerabilities are resolved following a risk-based approach using thorough testing of proposed solutions.

Conclusion

Veritas Alta Backup as a Service is a secure platform. Veritas is committed to the security of your data by following industry best practices. Rest assured that safeguards are in place to help secure your data within the Veritas Alta portal, and communications in and out of Veritas Alta Backup as a Service. Veritas Alta Backup as a Service provides a highly performant, scalable, and secure platform to meet the highest data protection requirements to support any company's journey to the cloud.

Related Documentation

Veritas Alta Recovery Vault Security Profile:

veritas.com/content/dam/www/en_us/documents/white-papers/WP_recovery_vault_security_V1537.pdf

Veritas Privacy Policy:

www.veritas.com/company/privacy

Veritas Data Processing Terms and Conditions (GDPR):

www.veritas.com/content/dam/Veritas/docs/policies/Veritas%20Data%20Processing%20Terms%20and%20Conditions%20and%20new%20SCCs.pdf

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V1864 03/23