Information Map Whitepaper

Security In-Depth

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

If you have any feedback or questions about this document, please email them to II-TEC@veritas.com stating the document title.

© 2017 Veritas Technologies LLC. All rights reserved. Veritas and the Veritas Logo are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

Document Control

Contributors

Name	Contribution
Stuart Carter	Author

Revision History

Version	Date	Changes
1.0	July 2015	Initial release
1.1	October 2015	Updated user authentication and data security
1.2	June 2016	Updated TLS support
1.3	Sep 2017	Added data residency options, WAF & cloud endpoints

Related Documents

Document Title	Version / Date

Table of Contents

Executive Summary 1

Information Map Overview 1

What is Information Map? 1

Key capabilities of the Information Map 1

How is it delivered? 2

Key capabilities of the technology platform 2

Application administration 3

Requirements 3

Metadata Stored by Information Map 4

Metadata entered by a customer 4

Metadata collected by the Information Map Agent 4

Physical Security 6

Data Residency 6

Data Center Redundancy 6

Physical isolation & availability 6

Data replication 7

Technical Security 8

Infrastructure security 8

Virtual Private Cloud 8

Firewalls 8

Redundant load balancers 8

Minimum system baselines 8

Vulnerability scanning 8

Application security 8

Role-based access controls 8

User authentication 10

User session persistence & use of cookies 11

Audit history 11

Data security 11

Encryption of data in transit 11

Encryption of data at rest 12

Encryption key management 12

Secure virtual customer domains 12

On-premise agent security 12

On-premise credential encryption 13
Deletion of Data 13
Administrative security 14
Personnel security 14
Employee screening 14
Confidentiality NDAs 14
Ongoing certifications 14
Process security 14
Change management 14
Access management 15
Access policy for customer data 15
Uptime monitoring 15
Systems monitoring 15
Application monitoring 16
Internet monitoring 16
Application Response Monitoring 16
System security 16
Qualys vulnerability testing 16
Veritas System auditing 17
Conclusion 18
Appendix A – Browser Support for TLS 1.2 19
Appendix B – External endpoints used by Information Map 20

Executive Summary

The Veritas™ Information Map is a hosted service that delivers visibility into an organization's information, orienting it in context to make decisions that reduce the risks and costs of storing information over time. The information map serves as the access point to, and control panel for, the information aggregated into the information fabric technology platform.

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 our datacenters, how secure is it?" Any uncertainty can keep an IT manager up at night.

With Veritas Information Map, we plan the security of our cloud-based service around three core areas:

1. **Physical security**: Security and resiliency of datacentre 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.

Information Map Overview

What is Information Map?

The Veritas™ Information Map delivers visibility into an organization's information, orienting it in context to make decisions that reduce the risks and costs of storing information over time. The information map serves as the access point to, and control panel for, the information aggregated into the information fabric technology platform.

Key capabilities of the Information Map

- Visibility into unstructured data: The Information Map provides an immersive visual experience for end-users to gain insight into your organizations unstructured information environment.
- Once users have filtered, navigated or searched their way to a dataset of interest, the Information Map allows you to export the list of items in the dataset to a CSV file.

  Using the list of files and the Information Map visuals themselves, customers can pursue a number of use cases with new decision criteria available to them.

  - Intelligent storage use cases like decommissioning unused shares and addressing stale and orphaned data.
  - Retention management use cases like identifying Outlook Personal Storage Folders (PSTs) for migration.
  - Legal and compliance use cases like focusing eDiscovery collections on custodian datasets, or prioritizing high activity shares for extra protection.

How is it delivered?

As a hosted service - the Information Map is hosted on the Veritas™ cloud, offering a high level of security and availability and the big data capabilities of its underlying information fabric technology platform.

The information fabric technology platform aggregates and stores the metadata characteristics of an organization's global unstructured information environment. The insights represented in the Information Map are provided by the information fabric technology.

Key capabilities of the technology platform

- *Scalability:* Being built with big data technology, information fabric technology is designed to handle 10's or 100's of billions of meta-data objects.

- *Efficient data collection:* The information fabric technology platform collects file system meta-data via NetBackup. As part of its daily backup job, NetBackup collects metadata from electronically stored information, including files recently created, modified or deleted. The platform uses NetBackup as a proxy to understand what is happening on a file server. As no scanning of the file systems is required, vast volumes of file system metadata can be quickly collected and will be as up-to-date as your backup cadence permits.

- *Content Source Support:* The information fabric technology collects file system metadata from Veritas NetBackup for Windows file servers, Linux/Unix file servers and Network Attached Storage (NAS) devices. File servers are automatically mapped to their data center though IP to subnet matching.

- *Data Security:* All communications and data in motion are encrypted using industry standard encryption protocols. All customer data stored at rest is encrypted with a unique encryption key per customer.

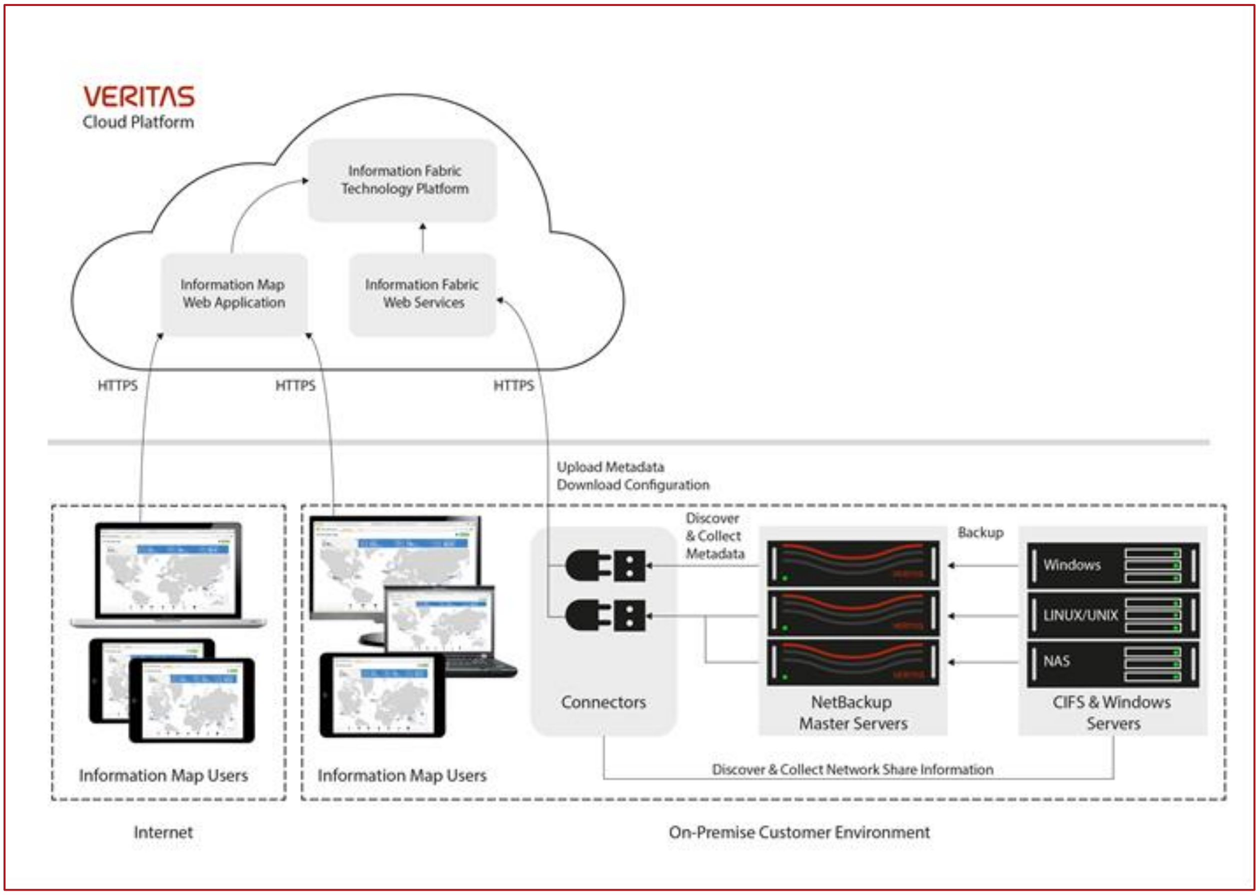


Figure 1 – Information Map Main Components

Application administration

Centralized administration is offered through the cloud-hosted Information Map administration web application.

- *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 such as ADFS. See ‘User authentication’ on page 10 for more details.

- *Roles Based Administration:* Ensures you can segregate your administrators from your Information Map users.

Requirements

Veritas NetBackup for Windows file servers, Linux/Unix file servers or Network Attached Storage (NAS) devices. NetBackup version 7.5 or later. NetBackup Appliances version 2.5 or later.

The on-premise agent requires a Windows 2012 or 2012R2, physical or virtual server for the on-premise collection processes.

External connectivity to Information Map endpoints. Please see Appendix B for the endpoints and protocols required.

Metadata Stored by Information Map

The following tables describe the metadata which is stored in the Information Map service.

Metadata entered by a customer

The table below lists the metadata entered by the customer's Information Map administrator in order to configure the application.

Category	Attribute	Example
Locations (data centers)	Display name	Tuscon
Locations (data centers)	Subnets	10.2.2.x, 10.2.3.x
Locations (data centers)	Longitude/Latitude	47.365824, 8.546017
Locations (data centers)	Address	Utoquai 15
Locations (data centers)	Region	EMEA
Locations (data centers)	Admin display name	Jane Doe
Locations (data centers)	Admin email address	jane_doe@acme.com
Locations (data centers)	Admin contact number	+41 111 22 33 44
Application User	Display Name	Jim Smith
Application User	Email address/username	jim_smith@acme.com
NetBackup Task	NetBackup Master Server hostname or IP address	acme-nbumaster01.acme.com
On-premise credentials	Display name	File Server Connection Credentials
On-premise credentials	Service account	acme\svc-infomap-agent
On-premise credentials	Service account password	<encrypted using customers private key> See section 'On-premise credential encryption' on page 13 for details.

Metadata collected by the Information Map Agent

This table lists all the metadata which can be collected from NetBackup, file servers and Cloud or SaaS services by Veritas software (agents). Collection of file share metadata is optional and depends on how the customer has configured Information Map.

Category	Attribute	Example
Agent Server	Host name	acme-infomap-agent01.acme.com

Agent Server	IP address(es)	10.2.2.50
Content Source	Host name	acmefiler05.acme.com
Content Source	IP address(es)	10.2.2.52, 10.2.2.53
Content Source	Type	Windows
File Share	Display Name	HomeShares
File Share	Local path of an exported share	c:\usershares
Item	File path	c:\usershares\john_doe\budget
Item	File name	FY15_Headcount_planning.xlsx
Item	File extension	.xlsx
Item	File size	1500
Item	Owner Account	acme\john_doe
Item	Owner Account SID	S-1-5-21-354581543--686939313--1299471892-39246
Item	Created date/time	2014-01-15T13:45:30.0000000Z
Item	Last modified date/time	2014-03-06T09:30:15.0000000Z
Item	Last accessed date/time	2014-08-27T18:05:25.0000000Z

Physical Security

Veritas operates the Information Map service in the Veritas cloud. The Veritas cloud is a Platform as a Service (PaaS) that runs on multiple cloud service providers including Amazon Web Services (AWS).

The Veritas cloud platform inherits the underlying security and standards of the cloud service provider. As an example, AWS 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 AWS security and compliance can be found here:

- Security - http://aws.amazon.com/security/
- Compliance - http://aws.amazon.com/compliance/

Note that while AWS conforms to the stated standards, Information Map as a product has not been certified to these standards.

Data Residency

For data residency reasons, Information Map is available in two standalone locations - one in Germany and one in the United States.

Customers choose the location where they would like their data to be stored during the provisioning process. Thereafter, all data is sent to and stored solely within that location; it is not stored or replicated anywhere else.

The choice of location makes no difference to where the service can be accessed from; both locations are globally accessible.

Data Center Redundancy

Physical isolation & availability

The Information Map service is deployed across 3 availability zones within each location.

An Availability Zone is a logical datacenter, composed of physical datacenters, each with their own redundant power, cooling and networking. Availability Zones are in distinct physical locations and engineered to isolate failure from each other so that a local incident does not impact the availability of other zones.

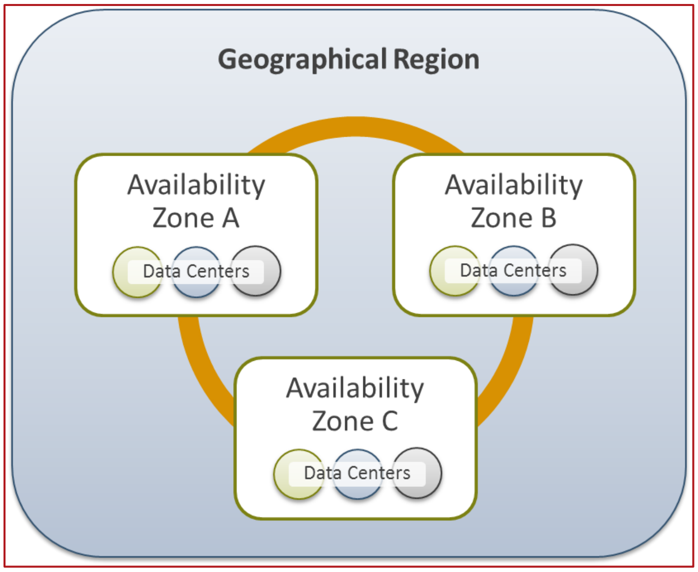


Figure 2 – Availability Zone Model

Data replication

Customer data is replicated across all 3 availability zones such that it is available and protected even in the event of another zone becoming unavailable.

Technical Security

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

Infrastructure security

Virtual Private Cloud

The Information Map service is isolated and protected from external access using a Virtual Private Cloud network (VPC). Strict security and network access controls restrict the traffic that can enter and leave the VPC as well as who can access the VPC for operational reasons.

Firewalls

Firewalls are used to block Internet-based attacks and maintain high availability for the public-facing web application and API web service endpoints.

Veritas uses a Web Application Firewall to audit activity against the web application and web service endpoints. Any suspicious activity is automatically detected and blocked.

Note that customers do not need to open any special ports on their firewall. All traffic from on-premise agents and browsers is outbound-initiated on the standard HTTPS port 443. The cloud service will not be able to directly reach in to a customer's data center. See the 'Encryption of data in transit' section (on page 11) for more details on encryption of data sent between the cloud and on-premise agents and browsers.

Redundant load balancers

Each availability zone is provisioned with multiple load balancers for performance and availability. The load balancers automatically ensure that traffic is directed to healthy servers and spread the load across servers in all 3 availability zones.

Minimum system baselines

Our standard Linux server build aligns to industry best practices; only the required services are enabled and system hardening measures are applied. Automated configuration enforcement agents ensure continuous baseline compliance.

Vulnerability scanning

Frequent vulnerability scanning and penetration tests help ensure that both internal and external threats are minimized. Veritas uses standard industry processes and tools for assessment and also 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 security level assessment of any advisory or vulnerability.

For more information on vulnerability scanning, please see the 'System Security' section (page 16).

Application security

Role-based access controls

The Information Map application provides pre-defined roles which customers can assign to application users. A user can be assigned one or more of the following roles:

- Information Map User

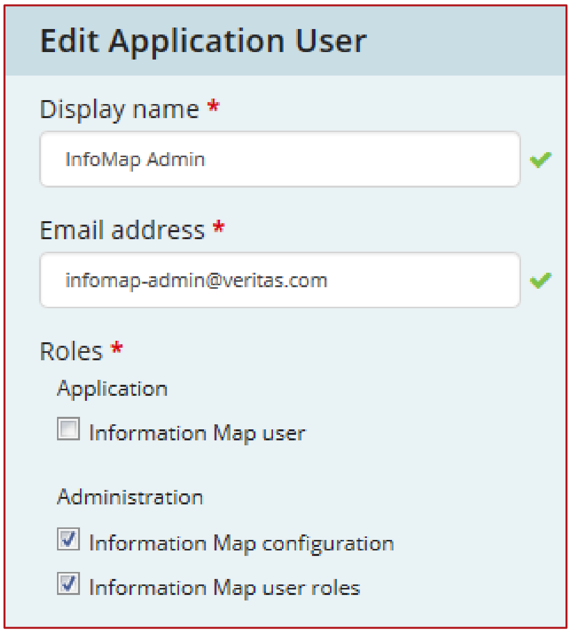
  Access to the Information Map for analysis, reporting and export of item metadata.

- Role Assignment

  Add and remove application users and assign roles.

- Application Administration

  Grants permission to configure most aspects of the application including on-premise agent management and application settings. This role does not provide the ability to perform 'Role assignment' to assist with delegation of responsibilities.



Edit Application User

Display name *

InfoMap Admin ✓

Email address *

infomap-admin@veritas.com ✓

Roles *

Application

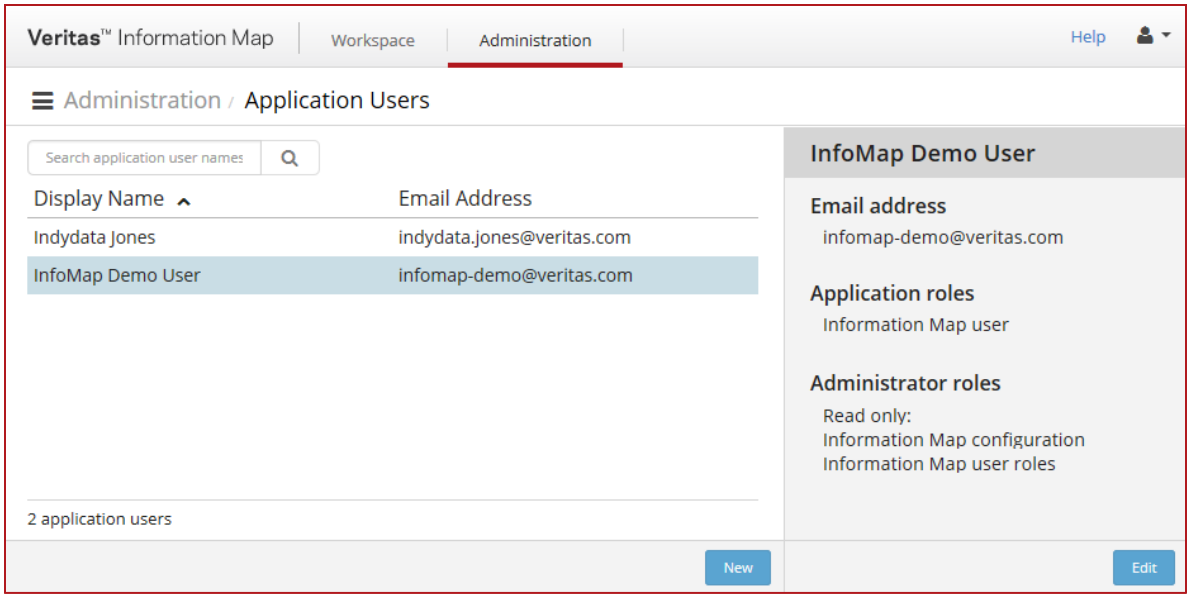
□ Information Map user

Administration

☑ Information Map configuration

☑ Information Map user roles

Figure 3 – Adding a new Application User



Administration / Application Users

Display Name ^	Email Address
Indydata Jones	indydata.jones@veritas.com
InfoMap Demo User	infomap-demo@veritas.com

2 application users

InfoMap Demo User

Email address
infomap-demo@veritas.com

Application roles
Information Map user

Administrator roles
Read only:
Information Map configuration
Information Map user roles

Figure 4 – List of Application Users

User authentication

Information Map uses a secure, highly available Veritas identity and authentication service to manage and authenticate application users.

When provisioning user access to Information Map, customers can choose whether to create and manage users using the Veritas Identity Provider (IDP) or integrate with their own IDP such as Active Directory Federated Services (ADFS), Okta or Ping Identity.

Using the Veritas Identity Provider

Information Map user accounts are created and managed through the Veritas Application Portal. Each new account is validated with the user through an email confirmation process before they can sign-on.

The Veritas IDP provides the ability for users to specify and change their own passwords through an email based password creation & reset workflow. All account passwords must meet the following complexity rules:

- Be different from the user ID
- Be between 8 to 15 characters long
- Contain at least one lower case and one upper case letter
- Contain at least one number

Using an external Identity Provider

The Veritas Identity Service supports Single Sign On 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. Information Map 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 Information Map.

User session persistence & use of cookies

Information Map uses non-persistent, ‘session-cookies’ that ensure the user is logged out of the application as soon as they close the browser, even if they don’t select the ‘Sign-out’ option in the application. This means that when the browser is re-opened, the user must sign-in again.

The cookie stored in the user’s browser contains a signed globally unique (GUID) session identification token that the Information Map Web Server uses to lookup the user. This token is included in every request the application makes to the Web Server.

Audit history

Information Map currently audits the following events and event properties for security tracking and forensic analysis:

Category	Audited Events	Event Properties
Authentication	• Sign-in • Sign-out • Failed sign-in (user has no role)	• Timestamp • User identity IP of the user’s device
Session Management	• Session creation • Session termination • Session expiry	• Timestamp • User identity • Session Identifier
User Management	• Add, remove, change application user • Modify role assignment	• Timestamp • User identity being modified • Admin user identity • IP of the admin’s device • List of roles assigned/changed
Resource Access	• Create • Read • Update • Delete	• Timestamp • User identity • Audit category • IP of the admin’s device • Success / failure • Resource Type & Identity

Table 1 – Auditable events

Customers can obtain these audit logs by submitting a request to Veritas.

Data security

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

Encryption of data in transit

All data sent to or retrieved from the cloud service is over HTTPS; encrypted and secured using Transport Layer Security (TLS). This security mechanism covers Information Map users interacting with the service through a browser as well as the on-premise agent which uploads metadata and retrieves configuration information.

TLS is a standard encryption protocol that provides security for communications sent over private networks and the Internet. TLS encryption maintains the integrity and confidentiality of data so that it can't be modified, intercepted, or viewed while in transit.

Information Map supports only TLS version 1.2, which is the most recently approved version. TLS versions 1.0, 1.1 and SSL are not supported due to known security vulnerabilities.

Please see Appendix A for TLS support by browser and guidance if you using Microsoft Internet Explorer 10.

Encryption of data at rest
All customer data in the Veritas cloud is encrypted at rest Advanced Encryption Standard (AES) encryption. This applies to all customer data whether uploaded, entered via the web application or generated data such as exports.

Each customer is randomly allocated a unique 256-bit AES master key which is used to encrypt and protect the keys used for actual data encryption, which are 128-bit AES keys. The master key is generated by and stored within a physical Key Management System. The master key can never leave the KMS and hence is kept separate from the encrypted data.

Multiple 128-bit AES keys are used to encrypt data within different repositories, such as databases and Object Storage. For example, each batch of metadata uploaded from the on-premise agent is assigned a new, randomly generated 128-bit AES key. The batch is then encrypted before being stored in Object Storage for subsequent processing.

Encryption key management
Encrypted data encryption keys (128-bit keys encrypted with the 256-bit master key) are stored alongside the data. The encrypted data encryption keys can only be decrypted by the customer's master key which is in a separate, secured Key Management Service.

Each customer's master key is rotated once a year.

Secure virtual customer domains
The Information Map service is a multitenant solution that uses application security and logical boundaries to segregate and protect customer data.

Data segregation is enforced across multiple layers by using a unique customer ID, logical database partitions, and logical partitions for all other data such as different folders on disk and different buckets within Object Storage.

In order to access data, customer and user IDs are validated to ensure that data is only accessible to that customer and the appropriate users.

On-premise agent security
The on-premise Information Map agent acquires metadata from Veritas NetBackup. It does this using a dedicated port (1556).

NetBackup Security Configuration
Each on-premise agent server must be authorised to connect to NetBackup master server(s) by adding the agent's IP address to a NetBackup policy configuration on each NetBackup master server.

File Server Security Configuration
In addition to connecting to NetBackup, the on-premise agent can be configured to automatically discover share and export details from primary file servers. These details help users in analysing data in the Information Map. To connect to file servers, the agent requires an account with a minimum set of read-only permissions.

The Information Map Administrators Guide contains more information on configuring NetBackup and access to file servers.

On-premise credential encryption

Information Map collects metadata from on-premise content sources, specifically NetBackup. In order to connect to file servers and discover useful information on shares and exports, a customer can optionally provide credentials (username and password) for use by the on-premise agent. This usually is a dedicated service account created in Active Directory and configured with the minimum privileges required for the agent.

Information Map stores the username and password in the cloud service to simplify the management and distribution of credentials to multiple agents.

The password is secured by encrypting it using public key cryptography (also known as asymmetric cryptography). The cloud service has the public key and the private key remains on-premise.

This means that the password can only be decrypted by the on-premise agent; no-one who could gain access to data in the cloud can view the password or decrypt it since the private key never leaves the customer's premises.

When the first agent is installed, it automatically creates a new RSA 2048-bit public/private key pair and sends the public key to the cloud during the registration process. The private key used to decrypt the credentials is secured locally on the agent server using the Microsoft Windows Protected Storage service.

When credentials are entered into the Information Map web application, they are encrypted with the RSA 2048-bit public key before being sent to the cloud for storage.

When an on-premise agent needs the credentials to access a file server, it retrieves the encrypted version from the cloud service and then using its local private key, decrypts them. The password is never stored in un-encrypted form in the cloud or on-premise.

Additional agent installations use the same key-pair that was generated the first time.

Deletion of Data

Upon request to terminate the service, the customer's master key will be disabled and in parallel, all of the customer's data that resides in the cloud platform will be deleted. A Certificate of Destruction will then be issued.

Administrative security

Veritas has a number of administrative controls in place to ensure defense-in-depth security through a layered security strategy. Administrative control measures are enforced through a combination of policies and processes. We implement the following controls, where applicable.

Personnel security

Employee screening

Every employee must sign legally binding security agreements and receive mandatory security awareness training annually. Our administrative offices also feature controlled access and camera surveillance at each ingress and egress point to monitor employee activities 24 hours a day, seven days a week, 365 days a year.

The security policy requires comprehensive background checks for every contingent employee and third-party service provider. Anyone who has access to offices or systems (e.g. contractors) are required to adhere to the security standards and/or conduct background checks of their employees prior to beginning work.

Confidentiality NDAs

Every employee is required to sign and agree to comprehensive confidentiality and non-disclosure agreements prior to beginning work. Any employee who has access to any computer or network is required to acknowledge that any actions may be logged or monitored for acceptable use before logging in.

Ongoing certifications

Every employee is required to renew their security certifications annually. Any changes to security policies are communicated in real time and employees must acknowledge receipt and adherence to them.

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 detailed 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 our 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 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. Powerful accounts are unique and their use is logged for auditing and accountability purposes.

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

Remote access to the cloud management consoles is also restricted to key employees.

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

Ninety-day inactive accounts are also 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, changing passwords, rerouting email, and voicemail, etc. Access to systems is promptly revoked following termination of employment.

Access policy for customer data
By default Veritas does not grant employees access to customer data. Veritas will not sign-on to the Information Map Web Application 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 an customer-raised issue in the cloud service or on-premise software
- Customer request for access to user and 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 email and SMS 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 is used to monitor critical components and data flows for deviations from trends and abnormal response times.

Internet monitoring
Information Map uses Uptrends (http://www.uptrends.com) to monitor our services externally from the Internet. Uptrends is a monitoring service provider that has Points of Presence (POP) throughout the world and performs availability and transaction monitoring from each POP on an automated, regular basis.

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

- Information Map Web Application Connectivity
- Information Map synthetic user login and information map queries to test the service is functional
- Web Service API connectivity

Application Response Monitoring
Veritas tracks and monitors metrics to help maintain a responsive interactive experience as well as ensuring the responsiveness of the Web Service APIs.

System security

Qualys vulnerability testing
Qualys proactively monitors every data center network access point. Driven by the most comprehensive vulnerability knowledgebase in the industry, QualysGuard delivers continuous protection against the latest worms and security threats without the substantial cost, resource, and deployment issues associated with traditional software. It enables users to effectively manage any vulnerability and maintain control over network security with centralized reports, verified remedies, and full remediation workflow capabilities with trouble tickets.

QualysGuard provides comprehensive reports on vulnerabilities, including severity levels, time to fix estimates, and impact on business, plus trend analysis on security issues. By proactively monitoring every network access point, this safeguard dramatically reduces the time spent researching, scanning, and fixing network exposures and enables us to eliminate network vulnerabilities before they can be exploited. All systems are scanned on a weekly basis to ensure security baselines are maintained.

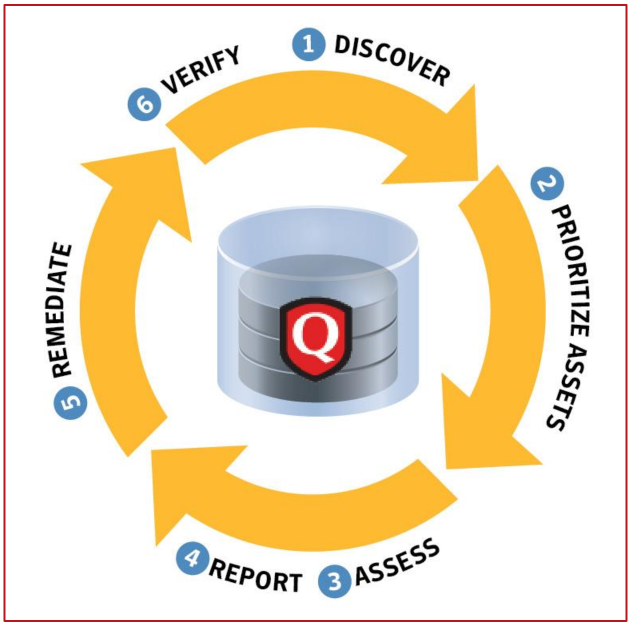


Figure 5 – Qualys vulnerability testing process

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. Independent audits also allow us to confirm remediation efforts are successful and security baselines are maintained. Frequent audits include automated and manual penetration testing for the following:

- Cross-Site Scripting (XSS)
- Injection
- Broken Authentication and Session Management
- Insecure Direct Object References
- Cross-Site Request Forgery (CSRF)
- Security Misconfiguration
- Insecure Cryptographic Storage
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Unvalidated Redirects and Forwards

Audits include review of internal systems, providing a complete evaluation of the environment. Once we receive the audit report, our security team works aggressively to address any potential vulnerability. Identified vulnerabilities are typically resolved within 30 days of discovery, following thorough testing of proposed solutions.

Conclusion

Security is a continuous process. Providing a high level of security and privacy protection for our customers means that we are continually adjusting the overall security control landscape to minimize risk to the changing business threat environment. While physical security, technical security, and administrative security remain constant, we are always re-evaluating our individual security measures to ensure our controls scale to meet business requirements and to combat constantly evolving Internet threats.

Appendix A – Browser Support for TLS 1.2

The table below shows the Information Map supported browsers that support TLS 1.2 and have it enabled *by default*. If you are using a browser from the table other than IE 10, no action is required.

Browser	Versions	TLS 1.2 Supported?	TLS 1.2 enabled by default?
Google Chrome	43 and later	Yes	Yes
Mozilla Firefox	34 and later	Yes	Yes
Microsoft Internet Explorer	10*	Yes	**No** Please see guidance below
	11	Yes	Yes
Apple Safari OS X	7 and later	Yes	Yes

Enabling TLS 1.2 for Microsoft Internet Explorer 10

If you are using Internet Explorer 10, TLS 1.2 must be enabled in order to use the Information Map application and configure the on-premise agent.

TLS 1.2 may already be enabled via your IT policies, but if you are unable to connect to the service when using IE 10, please refer to the following Veritas support article for guidance on how to proceed - https://www.veritas.com/support/en_US/article.000109445

*Note that at the time of writing, Internet Explorer 10 is only supported by Microsoft on Windows Server 2012. The supported Windows versions for the Information Map Agent are 2012 and 2012R2

Microsoft's Support Lifecycle Policies can be found here - https://support.microsoft.com/en-us/lifecycle

Appendix B – External endpoints used by Information Map

These are the HTTPS endpoints that are used for the Web Application and by the on-premise agent to connect to the Information Map service and must be accessible. This may involve configuration of proxy servers or firewalls depending on the environment.

Region	External endpoints	Outbound Port
Germany	apps.emea.veritas.com infomap.emea.apps.veritas.com infofabric-api.emea.apps.veritas.com	443 (HTTPS)
United States	apps.emeaveritas.com infomap.apps.veritas.com infofabric-api.apps.veritas.com	443 (HTTPS)

Notes

- All connections from a customer environment to the service are outbound; no inbound access is necessary.
- The region is selected by the customer during provisioning of the service and data remains in that region.
- More information on the connectivity requirements can be found in the support article here: https://www.veritas.com/support/en_US/article.000114451

About Veritas
Veritas Technologies LLC enables organizations to harness the power of their information, with solutions designed to serve the world's largest and most complex heterogeneous environments. Veritas works with 86 percent of Fortune 500 companies today, improving data availability and revealing insights to drive competitive advantage. More information is available at www.veritas.com.

For specific country offices and contact numbers, please visit our Web site: **www.veritas.com**

Veritas World Headquarters
500 East Middlefield Road
Mountain View, CA 94043 USA

+1 (650) 933 1000

© 2017 Veritas Technologies LLC. All rights reserved. Veritas and the Veritas Logo are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.