VERITAS

Veritas Enterprise Vault.cloud™ Security In-Depth

Who should read this paper?

This white paper is intended for IT professionals, including Enterprise Email/Messaging Administrators, IT managers, Archiving Managers, as well as IT security and Risk Management personnel.

January 2016

Table of Contents

Executive Summary

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

With Veritas Enterprise Vault.cloud™, we plan the security of our cloud-based archiving services around three core areas:

1. **Physical security:** Security of our buildings and collocation facilities.
2. **Technical security:** Security of 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.

Physical Security

We implement the following physical controls to keep our network, applications, and data safe.

Data Center Security and Redundancy

SSAE 16 Type II /ISAE 3402 Type II-Compliant Data Centers

Statement on Standards for Attestation Engagements No. 16 (SSAE 16) and International Standard on Assurance Engagements 3402 (ISAE 3402) are internationally recognized auditing standards developed by the American Institute of Certified Public Accountants (AICPA) and the International Auditing and Assurance Standards Board (IAASB). A Type II audit means that a third-party performs an in-depth audit of the data center's control activities, which generally include controls over information technology and related processes.

Our co-located North American data centers have been SSAE 16 Type II certified and a service auditor's report is available upon request.

Our co-located European data centers comply with ISAE 3402 standards, which specify requirements for the implementation of security controls. International Auditing and Assurance Standards Board members specify the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented Information Security Management System within the context of the organization's overall business risks. It is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

Tier-4 Data Centers

Tier-4 data centers ensure the highest level of physical security and reliability for clients' data. The Uptime Institute uses a four-tier rating system to more fairly evaluate a data center's underlying infrastructure. The simplest is a Tier-1 data center, which is basically a computer room. The most stringent level is a Tier-4 data center, which is designed to host mission-critical data with the highest levels of physical security and controlled access, 24 hours a day, seven days a week, 365 days a year server monitoring, video surveillance, and uninterruptible power supplies with on-site generators.

Tier-1 networks

Our data centers feature multiple, redundant high-speed fiber routes for maximum network flexibility and reliability. These top-level private networks allow users to transfer data securely through settlement-free peering (i.e., no added cost to transfer data between Tier-1 networks).

A Tier-1 network is the highest level out of a total of three tiers. Tier-2 networks peer with some networks without fees, but require fees to reach a large portion of the Internet. Tier-3 networks always pay fees to obtain access to the larger backbones.

Power/cooling/network

Our data centers use high-capacity, redundant generators that ensure power availability—even during metro-wide power outages. They also feature multiple uninterruptible power source (UPS) systems to reduce fluctuations and provide clean, continuous power to our critical systems.

The climate is regulated in data centers to provide optimal temperature for the equipment. Our data centers are also outfitted with pre-action fire detection and suppression safeguards to protect equipment and data.

As noted in the previous section, our data centers leverage multiple, redundant routes to the Internet.

Geographically Dispersed

In the U.S. and Europe, the primary and backup data centers are located at least 300 miles apart to ensure a regional incident or disaster does not impact our primary and backup data centers in a single region.

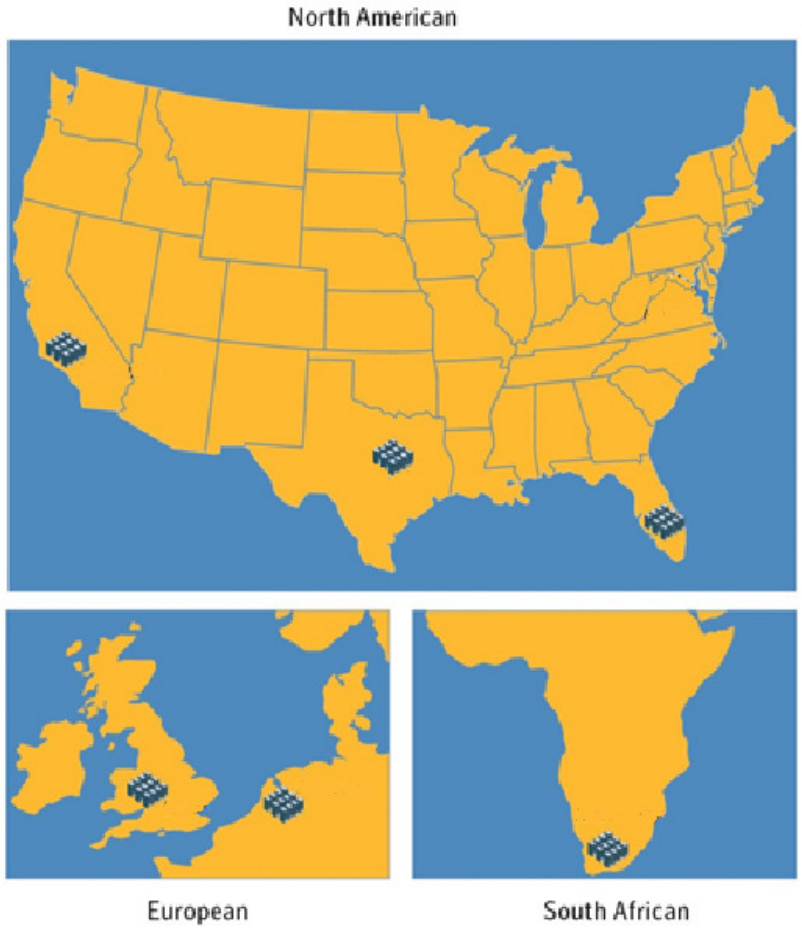

Figure 1. Worldwide locations for Enterprise Vault.cloud data centers.

Data replication

Clients' data is replicated from the primary service location to the appropriate in-region secondary service location, using disk-to-disk replication technology. Data is replicated over dedicated IPsec VPN tunnels using 256-bit AES and SHA2 algorithms. In addition, storage technology replicates data across multiple drives and nodes in the primary and secondary storage clusters to protect data in the event of drive failures or other sources of data corruption.

We leverage VMware® server virtualization for primary and backup operating server environments. VMware is a key element in helping to scale systems, allowing us to rapidly grow the infrastructure as email volumes grow.

Site security

Biometric access control

Biometric information, such as hand or fingerprint scanning, is required at all the data center entryways as part of the multifactor authentication process.

Security surveillance/closed-circuit television (CCTV)

Each point of access to our data centers is monitored with security cameras and CCTV.

24 hours a day, seven days a week guard service

The data centers reside in secure, unmarked buildings. Guards are on duty 24 hours a day, seven days a week, 365 days a year.

Guest access

Guests are required to sign in and a log is kept of every visit. Guests must also be escorted by authorized personnel once on the premises. In addition, data center employees are required to have a keycard to access the facilities, and they cannot enter restricted areas without the proper clearance.

The data centers also leverage weight-sensing mantraps (commonly found in bank vaults), which feature a set of doors and require visitors to enter the first door before receiving security clearance for the next one.

Technical Security

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

Infrastructure security

Redundant firewalls

Enterprise Vault.cloud uses best-of-breed, redundant firewalls to block Internet-based attacks on our network and maintain high availability.

Redundant load balancers

Data centers are outfitted with redundant top-of-the line, high-traffic throughput load balancers for performance and availability.

Minimum system baselines

The standard server builds align to industry best practices, i.e., CIS and NIST benchmarks. Only the required services are enabled on a server. Our malware protection and patch management agents ensure continuous security protection from external threats and software vulnerabilities. Vulnerability scanning and log event agents ensure continuous baseline compliance.

Application Security

Role-Based Access Controls (RBAC)

Our cloud-based email archiving solutions contain a number of granular permissions; we provide pre-defined built-in roles and allow customers to generate custom roles based on these permissions.

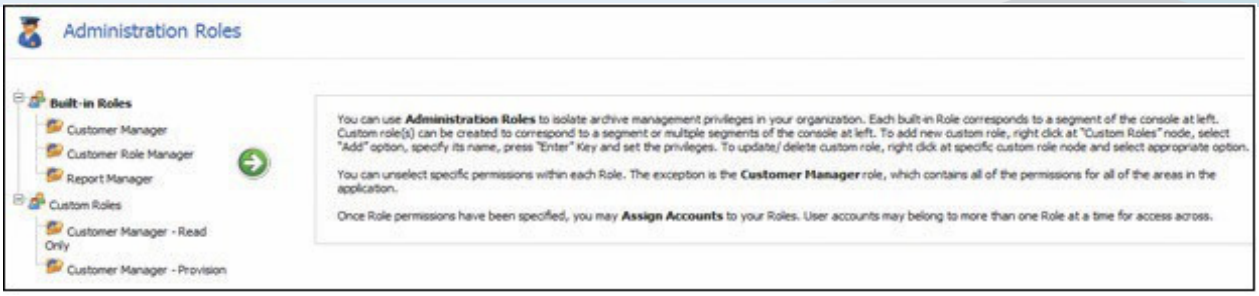

Figure 2. A screenshot of the roles-based access controls available to administrators in Enterprise Vault.cloud.

The following built-in roles are included with Enterprise Vault.cloud:

- **User:** Archive users can be granted access to their own personal archives, which gives them the ability to search their historical emails.
- **Account Manager:** This role can setup new accounts and reset passwords.
- **Policy Manager:** The Policy Manager can view and update policy settings (e.g., set time zones, specify storage of emails based on email direction).
- **Role Manager:** The Role Manager can view and modify the privileges of other users.
- **Administrator:** The Administrator role has each of the above privileges and other available

permissions. Clients can create any custom role in addition to the above built-in roles.

Administrators can use specialized eDiscovery roles in Veritas Enterprise Vault™ Discovery.cloud to control which reviewers can execute specified eDiscovery tasks, like running searches, reviewing search results, and performing exports.

The following built-in roles are included by default with Veritas AdvisorMail:

- **Auditor:** Auditors supervise and review an assigned group of end-user mailboxes to meet FINRA/SEC compliance requirements for U.S.- based companies.
- **Administrator:** The Administrator assigns auditors mailboxes to oversee and controls other privileges.

Trusted network authentication

By default, users access our services with a username and password, which are verified through an encrypted HTTPS login page. If a user chooses, "This is a private computer," an access token is cached in an encrypted cookie, ensuring that they do not have to enter login credentials for future logins for 10 hours.

With our "Trusted Networks" capability, companies can choose to "lockdown" access for Personal and Discovery users, so only users logging in from specified IP address ranges are permitted to login to the archive. In addition, every login is captured and logged, including the source IP address, for security tracking and forensic analysis.

In either authentication method, if a user attempts three incorrect logins in a row, he or she is prompted with a "captcha" (which requires the user to enter text seen in an image) to prevent automated login attacks. If the user then attempts two more failed logins, they are locked out of their account, which can only be reset by an administrator.

We leverage Active Directory Federation Services and the Security Assertion Markup Language (SAML) 2.0 standard to enable single sign-on for federated authentication. We provide a secure, standards-based solution for exchanging user security information between a service provider (Veritas) and an identity provider (Customer). SAML 2.0 ensures that a user's credentials are maintained by the client organization (not Veritas), and that a token is securely transmitted for authentication. Less secure methods, including LDAP-S, are inherently less secure because the vendor receives the user credentials, may require multiple trips for authentication and may even require companies to open additional firewall ports, which is a significant security threat for most enterprises

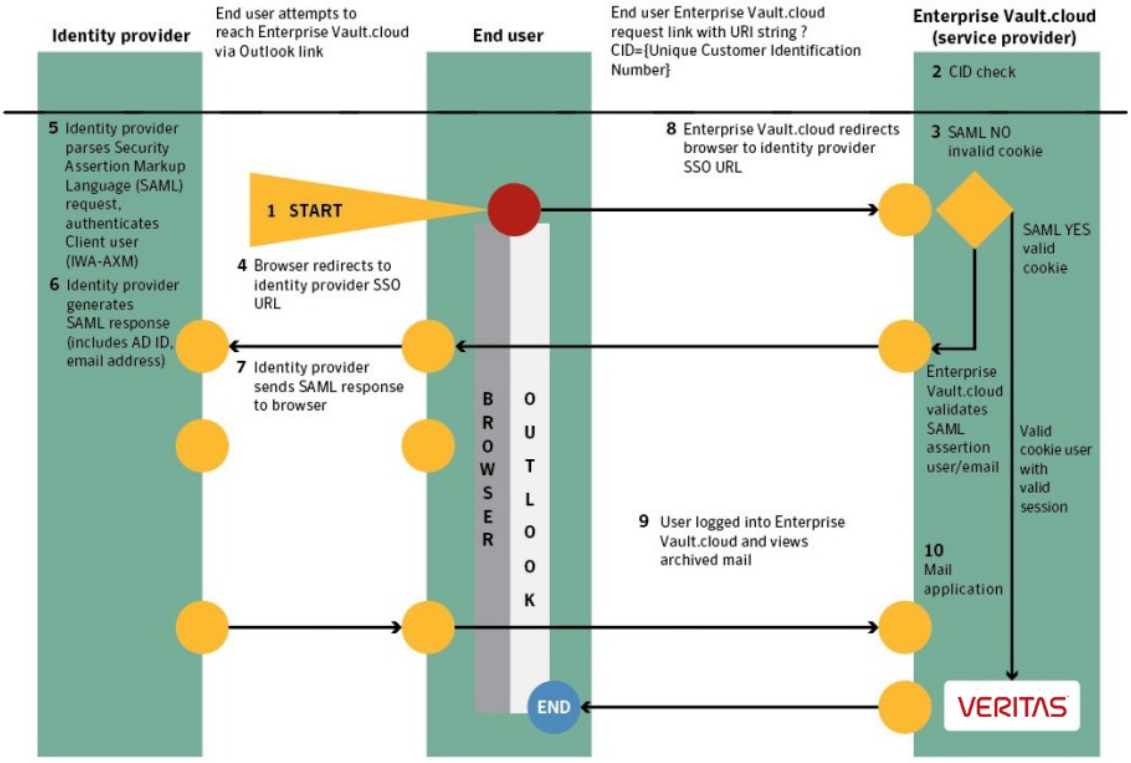

Figure 3. SAML 2.0 Single Sign-On experience for Enterprise Vault.cloud users.

Audit history

Administrators can conduct audits and review the history of Enterprise Vault.cloud to review important statistics and user actions, including total mail volumes (by day or week), user logins, search history, password resets, individual user activity, exports, and management changes. In addition, they can setup email alerts to receive notification of any new hits to active surveillance searches, eDiscovery downloads, or other areas of concern.

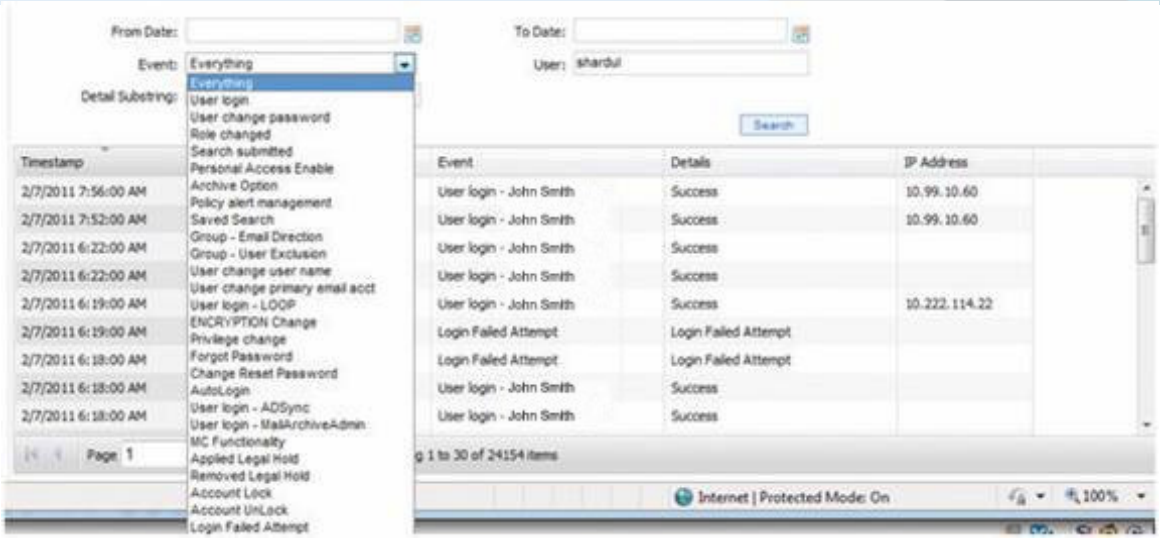

Figure 4. Screenshot of reporting functionality in Enterprise Vault.cloud.

Data security

Enterprise Vault.cloud employs a variety of security measures to ensure databases and data are secure.

Encryption in transit

When clients send data to us for archiving, they typically use a Transport Layer Security (TLS)-encrypted tunnel. TLS is an encryption protocol that provides security for communications sent via the Internet as well as other types of data transfers. TLS encryption maintains the confidentiality and integrity of emails, so they can't be modified, intercepted, or viewed while in transit.

User access

When a client uses our applications to access their information, they are required to provide credentials (login and password), and a secure SSL connection is used to access messages for search and review. SSL encrypts the data being transmitted between a server and a computer, so a third-party cannot "eavesdrop" on the transmission and view the data being transmitted. Only the user's computer and our secure servers are able to access the data.

Physical data security

We use the industry-leading Isilon clustered Network Attached Storage (NAS) solution to store data. Isilon's proprietary OneFS clustered file system technology stripes (also known as sharding) data across every hard drive and node in a given Isilon cluster. This means any given email message or file is spread across the drives and nodes in the system. As a result, any malicious actor gaining access to the physical hard drives or nodes in an Isilon cluster is not able to read or reconstruct any client data. Through a combination of hardware and software technologies, we also hash messages upon archiving to ensure that they are not later modified prior to search or production.

Encryption at rest

In addition, our innovative data at rest architecture uses 256-bit Advanced Encryption Standard (AES) encryption, while using unique symmetric encryption keys for each customer company. We encrypt and store customer keys separately from the physical data.

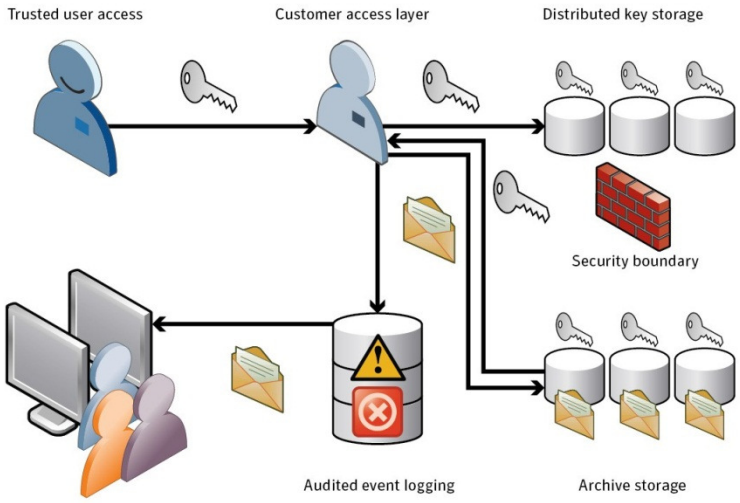

Figure 5. Diagram of encryption at rest.

If clients choose to authenticate via our services, we hash any stored user passwords using the SHA2 hashing algorithm with random salts. This is important in the unlikely event that the database is compromised. Password hashing also ensures that none of our employees are able to login to a customer's archive without the customer's permission.

Secure virtual client domains

Our archiving solutions are physically multitenant solutions but use application security and logical boundaries to protect client data. Client data segregation in the archive is controlled across multiple layers, including a unique client journal address, unique database IDs, and logical partitions. Each client's data is stored in a company-unique folder on a common/shared storage cluster infrastructure. In order to access data, company and user IDs are validated against archived items to ensure that a given client's email messages are only accessible to that client and the appropriate users at their company. In each case, we maintain an activity log, which is available for review (per the Audit History section on page 5).

Administrative security

We have 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

A strict security process is in place for new hires. Prior to beginning work at any of the Enterprise Vault.cloud offices, new employees must pass a thorough background check. Current background checks consist of a criminal check for the past seven years, a Department of Motor Vehicles check, a credit check, and validation of degrees and certifications. In addition, 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 (i.e., temps, contractors, data center employees) is 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

Enterprise Vault.cloud releases a variety of enhancements and fixes on a regular basis to improve the performance and security of our services. In order 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 our Change Review Board (CRB) Monday through Thursday. 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.

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.
The CRB is complimented by our Security Review Board (SRB). This board consists of security and engineering experts and is tasked with maintaining and improving our security baselines. The SRB provides guidance during the Software Development Lifecycle (SDLC), conducts regular penetration tests and ensures activities comply with Veritas's policies, procedures and standards.

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 requires the use of Veritas's VPN tunnels combined with two-factor authentication. This authentication includes strong passwords and Veritas's VIP soft tokens.

The security team performs quarterly audits of privileged account use, VPN gateways access lists, and data center facilities access logs. 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 revoked promptly following termination of employment.

Uptime monitoring

Enterprise Vault.cloud 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 Data Center Operations staff has an around-the-clock on-call rotation model. On-call Veritas staff are responsible for tracking alerts and identifying potential issues.

Systems monitoring

Enterprise Vault.cloud uses a variety of IT management software platforms to monitor core systems, including:

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

Application monitoring

Internally developed tools are used to monitor our archiving processes. We have dashboards that track the process of emails across the archive and reports that are used by staff to identify clients whose journaling traffic may have dropped off abnormally (versus previous trends) due to an issue on the client side or in the network.

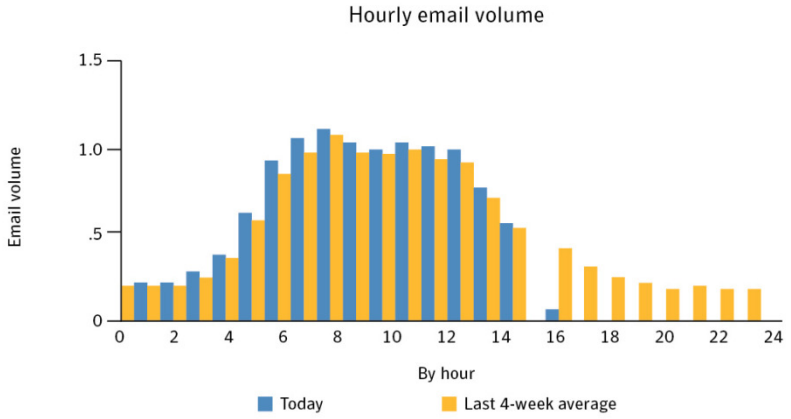

Figure 6. This report is used to trend overall journaling traffic to identify system-wide anomalies.

Internet monitoring

Enterprise Vault.cloud uses a 3rd party monitoring service provider to maintain external awareness of our services from the Internet. This monitoring service provider has Points of Presence (POP) throughout the world and performs availability and transaction monitoring from each POP on an automated, regular basis.

Figure 7. Map of Global POPs.

Our monitoring service provider performs many tests, including the following tests every five minutes from every POP:

Veritas AdvisorMail

- Test SMTP connection to Veritas AdvisorMail journaling interface.
- Test SMTP connection to Veritas AdvisorMail inbound routing interface.
- Test SMTP connection to Veritas AdvisorMail outbound routing interface.
- Test HTTPS connection to Veritas AdvisorMail Web application.

Veritas Enterprise Vault.cloud

- Test SMTP connection to Enterprise Vault.cloud journaling interface.
- Test HTTPS access to Web applications.
- Test HTTPS synthetic login to Enterprise Vault.cloud.

User interface monitoring

Enterprise Vault.cloud also monitors systems at the application level. A 3rd party service monitors our systems from the end user's perspective in real-time to ensure responsive systems are maintained.

Incident response process

The Internet security threat landscape is constantly evolving. Relying on the Internet to deliver services, an organized and controlled incident response process is critical to quickly responding and containing threats. A step-by-step process is in place to investigate and respond to any incidents.

The goals of our Incident Response Team are to:

1. Identify threats and contain incidents.
2. Maintain or restore business continuity.
3. Defend against further attacks.
4. Deter attackers through continuous monitoring, investigation, and prosecution.
5. Perform continuous counter-threat and security intelligence activities.

If a client-facing issue is detected with the infrastructure, or if an issue is reported by clients, a standard Network Incident is employed:

- Staff member opens a ticket in our internal ticketing system.
- Staff member escalates critical issues to on-call Data Center Operations staff member.
- Data Center Operations team member escalates for advanced Network and Security Operations or Engineering resources as needed.
- Client Services team notifies clients via the status page, email, text, or phone, where appropriate; Enterprise Vault.cloud can leverage an automated alerting service (MIR3) that clients can subscribe to for these notifications.
- Once the issue is resolved, the internal Network Incident ticket is closed and customers are notified.
- If appropriate, a root cause analysis of the incident is produced.

System security

Symantec™ Endpoint Protection and host intrusion prevention system (Endpoint Protection and HIPS) technology to provide malware protection for servers. Agents are centrally controlled by the security team and alerting functions have been enabled to support our security monitoring and incident response process.

Finally, we leverage a variety of tools to proactively manage patches and software updates by automating the collection, analysis, and delivery of patches across our production server environment. These systems provide information on each software bulletin, such as technical details, severity ratings, and number of updates. These tools also provide detailed reports and alerts on patch updates and distribution status.

Intrusion detection systems

For an additional layer of protection, we use Intrusion Detection/Prevention Systems (IDS/IPS) to detect malicious network traffic and computer usage that often cannot be caught by a conventional firewall. We partner with Managed Security Services to support a comprehensive IDS/IPS security event management system.

Enterprise Vault.cloud uses the most popular and widely supported open source network intrusion prevention and detection system (IDS/IPS). Our IDS/IPS platform can perform protocol analysis and content searching/matching. It can be used to detect a variety of attacks and probes, including buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts. It uses a flexible rules language to describe traffic that it should collect or pass, in addition to a detection engine that uses a modular plug-in architecture. Our IDS/IPS system has real-time alerting capabilities, incorporating alerting mechanisms for syslog, a user specified file, a UNIX® socket, or WinPopup messages to Windows clients.

Qualys vulnerability testing

Qualys proactively monitors all data center endpoints. 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 vulnerabilities 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 endpoint, 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 9. Qualys vulnerability testing process.

Independent third party system auditing

Our environments are reviewed annually by independent third party auditors. Independent 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 vulnerabilities.

Independent audits also allow us to confirm remediation efforts are successful and security baselines are maintained. Annual audits include automated and manual penetration testing.

Auditors target the most recent OWASP Top 10 vulnerabilities (Open Web Application Security Project) as part of their overall review. The OWASP Top 10 includes:

- Injection
- Cross-Site Scripting (XSS)
- 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

Please see the following link for more information regarding the OWASP Top 10:
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Annual 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 vulnerabilities. Identified vulnerabilities are typically resolved within 30 days of discovery, following thorough testing of proposed solutions.

Security seals of approval

In addition to the investments made to our physical, technical, and administrative security, Enterprise Vault.cloud has also sought the endorsement of leading security organizations to vet security policies and help ensure that we continue to follow and establish industry best practices.

Our co-located U.S. data centers are SSAE 16 Type II certified annually, which means that they conform to industry best practices in terms of security and internal controls.

Our co-located European data centers are audited annually for ISAE 3402 Type II compliance to ensure they meet security and control requirements defined by the IAASB.

We are a member of the Cloud Security Alliance, a non-profit organization formed to promote the use of best practices for providing security assurance in cloud computing.

We are a member of EuroCloud, a pan European cloud computing business network designed to build relationships with the European authorities and to promote technological relationships between member firms.

Conclusion

Security is a continuous process. Providing a high level of security and privacy protection for our SaaS clients 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.

About Veritas Technologies LLC

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.

For specific country offices and contact numbers, please visit our website.

Veritas World Headquarters
500 East Middlefield Road
Mountain View, CA 94043
+1 (650) 933 1000
www.veritas.com