This whitepaper targets IT decision makers, security personnel & IT auditors, and assumes that the reader is familiar with basic security concepts in the area of data storage, networking, operating systems, data encryption, and operational controls in hybrid cloud environments.

Customers that have additional questions or comments regarding document can email Veritas Global Security Office (GSO) Customer Trust at DL-VTAS-GSO-CustomerTrustOffice@veritas.com stating the document title.
# Table of Contents

Executive Summary .............................................................................................................. 3

How Veritas Cloud Products are delivered........................................................................ 3

Governance and Organizational Design ........................................................................... 3

Monitoring and Reporting – Driving security maturity in products.................................. 4

Application Security Processes – from the ground up: ...................................................... 4

Physical Security................................................................................................................ 5

Infrastructure Security ...................................................................................................... 6

- Network Segmentation.................................................................................................. 6
- Firewalls ......................................................................................................................... 6
- Redundant load balancers ............................................................................................ 6
- Minimum system baselines .......................................................................................... 6
- Vulnerability scanning .................................................................................................. 6

Administrative security ...................................................................................................... 7

- Personnel security ........................................................................................................ 7
- Employee screening ....................................................................................................... 7
- Confidentiality NDAs ..................................................................................................... 7
- Ongoing training ............................................................................................................ 7
- Change management ...................................................................................................... 7
- Access management ...................................................................................................... 8
- Security and uptime monitoring .................................................................................... 8

Summary ................................................................................................................................. 9
Executive Summary

When it comes to cloud-based services, Veritas believes that information security and data privacy is of utmost importance to Veritas customers. Security is a core functional requirement that helps protect critical data assets from accidental or deliberate theft, leakage, integrity compromise, and deletion.

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

1. **Governance**: Organizational structure, policies and processes designed to support an environment of continuous improvement utilizing a risk based approach.

2. **Application Security Processes**: Cybersecurity resiliency through a secure development lifecycle (SDL) that drives application security maturity using a defense-in-depth approach.

3. **Physical security**: Security and resiliency of partner data-centers that are regularly certified and audited by third party audit organizations (3PAO).

4. **Infrastructure Security**: Layered technologies across infrastructure components in our hybrid cloud environments provide a defense-in-depth approach to technical security controls.

How Veritas Cloud Products are delivered.

In general, Veritas hosted cloud products currently reside in state-of-the-art Tier-1 public cloud data centers with Tier-4 networks, delivered with world leading cloud service providers (CSPs) to ensure best-in-class best-in-class security and compliance capabilities by design.

Governance and Organizational Design

Veritas utilizes a cross-functional organizational strategy and internal control framework (ICF) designed to drive continuous improvement throughout our global processes and systems. We utilize a risk-based approach to align security practices with organizational risk tolerance levels.

The Global Security Office (GSO), led by the Chief Security Officer (CSO), provides the enterprise corporate security framework for establishing policies, processes, training, and internal control guidelines that product-developing Business Units (BU’s) must align with. GSO sets the tone of security for the enterprise, with strong ‘tone at the top’. GSO is also responsible for global physical security, incident response, and Veritas Customer Trust engagement.

The Product Security Group (PSG), led by the Chief Product Security Officer (CPSO), works closely with GSO to drive security activities within the Central Products Office (CPO) to ensure products meet or exceed customer requirements. The PSG programs include the ‘Security Warrior’ and ‘PSG Presents’ training activities, administration of a Secure Development Lifecycle (SDL) driven by the Veritas Application Security Assurance Program (ASAP), third-party code, vulnerability and pen testing management, and risk and compliance activities that closely align with our Veritas legal teams to ensure data privacy goals are met.
Monitoring and Reporting – Driving security maturity in products.
PSG programs and product compliance metrics are monitored and reported through the ‘PSG Dashboard’ to senior CPO management on monthly and quarterly reporting cycles.

Additionally, the PSG utilizes the Building Security in Maturity Model (BSIMM) framework for aligning to, and measuring against, industry standard best practices in alignment with key strategic partners.

Application Security Processes – from the ground up:

• **Application Security Assurance Program (drives Secure Development Lifecycle)**
  - The Application Security Assurance Program provides a framework to ensure that our products are developed, delivered, and supported throughout their lifecycle in alignment with industry best practices.

• **Threat modeling and security checklist review by Architectural Review Board (ARB)**
  - The architectural process at Veritas includes threat modeling activity and security review checklists required for review by the ARB prior to greenlight.

• **Software security training for Architects, Engineers, and Product Managers**
  - The PSG ‘Security Warrior’ product security training and awareness program ensures that our Architects, Engineers, and Product Managers receive relevant and targeted role based training, at a minimum, on an annual basis. The ‘PSG Presents’ brown bag training activities and ‘PSG Bulletins’ provide timely awareness of current security news, events, and emerging regulations.

• **Static Application Security Testing (SAST)**
  - During the implementation phase of the Secure Development Lifecycle (SDL), product teams are required to perform static analysis on their code to catch coding vulnerabilities as early as possible.

• **Dynamic Application Security Testing (DAST)**
  - During the verification phase of the Secure Development Lifecycle (SDL), product teams are required to perform dynamic security testing to again identify vulnerabilities prior to release.

• **Open-source software management**
The PSG team actively manages third party and open-source software utilized within the Veritas cloud product service offerings to ensure utilization of the most up-to-date versions, and that vulnerabilities are identified, patched, and remediated in a timely manner according to Veritas GSO policies.

- **Cryptography reviews and adherence to standards**
  - The PSG team conducts regular and ad-hoc reviews of cryptographic modules and algorithms used in Veritas products to ensure that current standard and supported versions are utilized. Veritas products utilize FIPS 140-2 standards where applicable and appropriate.

- **Annual 3rd party penetration testing (red team) and versioned vulnerability scanning**
  - Veritas policy requires that products are pen tested by an independent third party red team at least once per year. The PSG also conducts internal scans whenever a new product version is released. PSG manages schedules for pen testing and internal vulnerability scans.

- **Vulnerability Management Policy covering all Veritas products**
  - Veritas product teams are required to adhere to the internally facing Veritas Product Vulnerability Management Policy, including resolving vulnerabilities within a target SLA window based on severity.

**Physical Security**

In general, the Veritas cloud environment for running Veritas hosted offerings is a Platform as a Service (PaaS) environment that runs on multiple cloud service providers in data centers designed for resiliency and compliance that are regularly audited by third party audit organizations (3PAO).

The Veritas cloud platform inherits the underlying security and standards of the cloud service provider that provides the hosting Infrastructure as a Service (IaaS). Our partner managed data centers provide multiple levels of physical security, are compliant with many standards such as ISO 27001, SOC2 Type II, and are regularly certified against U.S. National and International global standards. Veritas cloud data centers may also meet the US Government’s Federal Information Security Management Act (FISMA) and Federal Risk and Authorization Management Program (FedRAMP) standards where applicable.
Infrastructure Security

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

**Network Segmentation**

Veritas cloud managed services are isolated and protected from external access on Tier-4 networks using physical and logical segmentation, including use of Virtual Local Area Networks (VLANs), and Virtual Private (VPCs) where applicable. Strict security and network access controls restrict the traffic that can enter and leave the segmented VLANs and VPCs as well as who can access the networks to provide operational support. Veritas enforces separation of duties and the principle of least privilege for administrative management of our Tier-4 cloud networks.

**Firewalls**

Firewalls block Internet-based attacks and maintain high availability for the public-facing web application and Application Programming Interface (API) web service endpoints.

Veritas uses a Web Application Firewall (WAF) to audit activity against the web application and web service endpoints. Suspicious activity is automatically reported to the Security Information and Event Management (SIEM) system for monitoring and incident response, as well as blocked by the WAF Intrusion Prevention System (IPS).

**Redundant load balancers**

Availability zone in our hybrid cloud data centers are provisioned with multiple load balancers for performance and availability. The load balancers automatically ensure that traffic is evenly directed across servers based on geographic region, and spreads the load across servers in all logical availability zones.

**Minimum system baselines**

Our standard Operating System (OS) server build aligns to industry best practices; only the required services are enabled and OS 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 to acceptable risk tolerance levels. Veritas’ Global Security Office (GSO) uses standard industry processes and tools for assessment and notification of external threats.

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.
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
Employees must sign legally binding security agreements and receive mandatory security awareness training annually. Our administrative offices also feature controlled access and surveillance to ensure resource and employee safety.

The security policy requires comprehensive background checks for contingent employees and third-party service providers. Personnel who have access to offices or systems (e.g. contractors) are required under Veritas policy to adhere to the security standards and conduct background checks of their employees prior to beginning work.

Confidentiality NDAs
Employees are required to sign and agree to comprehensive confidentiality and non-disclosure agreements prior to beginning work. Employees who have access to any computer or network are required to acknowledge that any actions may be logged or monitored for acceptable use before logging in.

Ongoing training
Employees are required to take annual security training. Any changes to security policies are communicated in real time and employees must acknowledge receipt and adherence to the policies.

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 rigorous change and configuration management process.

Changes to production environments must have an associated Change Management Request. System changes require Change Management reviews and associated approvals.

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

- Management authorization of change requests.
- Tracking our production changes.
- Peer review of changes prior to implementation.
- Fully documenting changes in a system of record (SOR).
- 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 the Veritas Access Control Policy. Access, onboarding, change requests, or terminations can only be made by management. Access is provisioned based on the principles of least privilege, default deny, and separation of duties. Administrative or root super user accounts are unique and their use is logged for auditing and accountability purposes.

Remote administration access to cloud resources requires the use of Veritas’s VPN tunnels combined with multi-factor (MFA) authentication.

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

The GSO security team performs regular audit and monitoring of privileged account use, and cloud management console logs.

Veritas utilizes 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.

Additionally, accounts are regularly audited and disabled if inactive.

**Security and uptime monitoring**

Veritas’ Global Security Office (GSO) and Product Teams employ a variety of monitoring systems, which produce alerts for our Data Center Operations, Security Operations Center (SOC), Engineering and management teams via email and SMS, and other communication mechanisms. Security monitoring is done 24x7x365, with an on-call rotation model for incident response. On-call GSO staff are responsible for tracking alerts, identifying, and remediating issues and incidents via the Security Incident and Event Reporting (SIEM) system.

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

- Storage devices
- Network devices
- Servers
- Operating systems
- Databases
Summary
Veritas believes that 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 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.