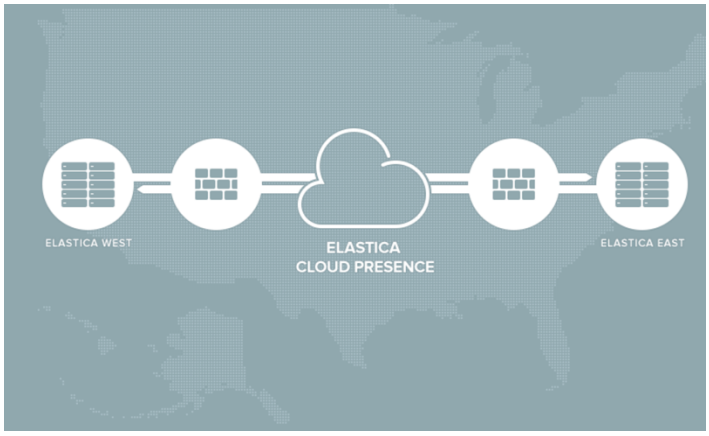
Symantec CloudSOC
Compliance



The Symantec Cloud
Business-Ready and Secure

The Symantec Cloud – A Commitment to Uptime, Performance and Security
We developed the Symantec cloud platform from the ground-up, leveraging multiple data centers to ensure high redundancy and availability and meet our customer commitment to uptime and performance.

Symantec uses best-in-industry commercial security products for daily scanning of its environment and services. We also engage professional security vendors to perform third party penetration tests and audits of our environment on an annual and bi-annual basis, respectively, while internal system scans are performed daily.
Symantec uses multiple data centers to provide redundancy. The Symantec data centers are in geographically distributed regions and are highly redundant in themselves.

Compliance and Internal Controls: SOC 2 Type-2

Symantec CloudSOC platform meets the criteria for the trust services principles set forth by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles (AICPA's) under the Service Organization Controls 2 (SOC-2) standards. The trust services principles' described in the AICPA's guidelines define the essential practice controls relevant to availability, security, confidentiality, privacy, and integrity that are pertinent to service organization such as Symantec. The security, availability, and processing integrity criteria are related to the controls system, and the confidentiality and privacy criteria are related to the information processed by the system. SOC-2 report validates the operating effectiveness of all the system controls related to service design by providing independent assurance regarding compliance and internal controls. The SOC-2 report demonstrates our commitment to protect customer data by implementing the operational controls in accordance with trust services principles and assurance criteria thereby providing a transparency into organization control environment by articulating information in a structured manner.

Secure Data Handling and Destruction
Symantec has taken a simple, no nonsense approach to security: no device capable of holding data may ever leave a data center intact – it must be physically destroyed following the techniques detailed in the DoD 5220.22-M (National Industrial Security Program Operating Manual) or NIST 800-88 (Guidelines for Media Sanitization).

Customer Responsibilities

“IT TAKES A VILLAGE...”

Symantec CloudSOC™ (“CloudSOC”) security operations service (“Service”) provides broad functionality for enabling organizations in securing the cloud services adopted as part of their “Extended Enterprise Infrastructure”. Elastic’s CloudSOC is provided as a multi-tenant, cloud-based service, accessible on the Internet via popular web browsers such as Internet Explorer, Chrome, and FireFox.

As a member of the Symantec CloudSOC community, subscribers should be proactive in recognizing the value, sensitivity, and need to safeguard the information provided by the service and access to the policy enforcement capabilities.

This document details CloudSOC user and customer responsibilities as they relate to acceptable usage of Symantec’s CloudSOC security operations service. It is the responsibility of Symantec customers and CloudSOC users to familiarise themselves with the information and procedures set forth below and comply with the service usage and notification requirements which are intended to maximize protection of CloudSOC users information assets and cloud service security posture.

SAFEGUARDING OF ASSETS AND INFORMATION

“Keep your doors and windows locked...”

To safeguard information assets and policy enforcement capabilities available in the Symantec CloudSOC service, the subscribers’ IT governance processes should include end-user training regarding appropriate use and awareness of the need for securing access to their CloudSOC service account credentials.

As with most cloud services, access to Symantec’s CloudSOC service requires a login ID and password. When an organization subscribes to the Symantec CloudSOC cloud service, it is the client’s responsibility to manage which end users should be given access. Clients should also define when access should be taken away from the end users. For example, access must be revoked upon end users’ separation from employment or as part of departmental changes that result in change of duties or responsibilities. Only valid account credentials should be used by authorized users to access the Symantec CloudSOC service.

Symantec’s CloudSOC service should be considered sensitive and confidential by CloudSOC users. Users should follow information security best practices in ensuring access to their account credentials is appropriately limited, as well as ensuring that the information and functionality provided by the Symantec CloudSOC service is protected and restricted from unauthorized use.

Symantec CloudSOC service users are responsible for maintaining the security and confidentiality of their user credentials (e.g., Login ID and Password), and are responsible for all activities and uses performed under their account credentials whether authorized by them or not.
By establishing user credentials and accessing the CloudSOC environment, end users of the CloudSOC service agree to comply with these requirements to safeguard assets and account information.

PASSWORD MANAGEMENT

“Change the locks...”

Cloud-based services are accessible to the global Internet public, as a result, great care must be exercised by Symantec CloudSOC service users in protecting their CloudSOC subscriptions against unauthorized access and use of their credentials.
By establishing user credentials and accessing the CloudSOC environment, service end users agree to proactively protect the security and confidentiality of their user credentials and never share service account credentials, disclose any passwords or user identifications to any unauthorized persons, or permit any unauthorized person to use or access their Symantec CloudSOC accounts.

Any loss of control of passwords or user identifications could result in the loss of "Personally Identifiable Data (PII)" and the culpable account owner(s) may be liable for the actions taken under their service account credentials whether they authorized the activity or not.

Additionally, when establishing CloudSOC account credentials, end users are required to establish strong passwords following password strength and complexity best practices; passwords should not be easily guessable.

PROCESS FOR REPORTING OPERATIONAL ISSUES

"Participate in Neighborhood Watch..."

On the occasion that Symantec CloudSOC users observe performances issues, problems, or service outages, users should contact Symantec immediately. Proactive reporting of operational issues provides "fixed for one, fixed for all" benefit for the entire Symantec CloudSOC community.

INCIDENTS AND BREACHES

"Call the authorities..."

By establishing CloudSOC account credentials or accessing Symantec's CloudSOC service, end users of the service agree to notify Symantec immediately of any security incident, including any suspected or confirmed breach of security. Also, users of the service agree to logout or exit the service immediately at the end of each session to provide further protection against unauthorized use and intrusion.

Symantec CloudSOC users should also notify Symantec immediately if they observe any activity or communications in other forums that may indicate that other Symantec customers have had their CloudSOC accounts compromised.

Lastly, Symantec encourages users to practice responsible disclosure by notifying Symantec of any identified security vulnerabilities. Symantec is dedicated to providing secure services to clients, and will triage all security vulnerabilities that are reported. Furthermore, Symantec will prioritize and fix security vulnerabilities in accordance with the risk that they pose.

COMPLAINTS AND OTHER CONCERNS

Symantec customers and CloudSOC end users are encouraged to communicate any complaints and concerns related to the Symantec CloudSOC solution. To facilitate thorough investigation and appropriate response, compliance should be provided in writing and provided via email or fax and contain as much detailed information as possible including:

- Summary description of the issue
- Contact details for all participants related to the complaint
  - Including company, full name, telephone numbers, email addresses, address
- Date and time of complaint submissions
  - As well as related activities, observations, and events
- Origin of the complaint
  - Including Symantec website information, function, mail headers, relevant CloudSOC module, function, effect, etc.
- Any additional detail or information useful for understanding and investigation

Symantec encourages complainants to supply names and contact details and will not release this information except were required by legal mandate. Symantec will review all submitted complaints where sufficient detail has been provided but cannot commit to managing or resolving all complaints reported anonymously or submitted by individuals that are not current Symantec customers, or do not have active service contracts, or for issues that have been created by other networks, cloud service providers, technology vendors, or other contributing factors outside of Symantec control.

If Symantec CloudSOC users have other concerns they would like to discuss, please contact Symantec using the information below.

CONTACT INFORMATION
To notify the appropriate Symantec incident response or support personnel, please use the contact information listed below:

Symantec Address and Contact Information:

- 350 Ellis St.
- Mountain View, CA 94043
- https://support.symantec.com/en_US/contact-support.html
- Phone: 650-527-8000

If you do not agree with these terms, please do not use this site.

COMPLIANCE ISSUES
“Obey the law…”
Regulatory requirements and industry mandates are continuously increasing in scope & depth and can vary from industry to industry. Symantec CloudSOC users agree to abide by the regulatory requirements, industry mandates, and other compliance requirements imposed on their organizations and understand that use of cloud-based services does not exclude the organizations from responsibilities for restricting access to application information and functionality.

Responsible Disclosure Policy

Symantec is dedicated to keeping its cloud platform safe from all types of security issues thereby providing a safe and secure environment to our customers. Data security is a matter of utmost importance and top priority for us. If you are a dedicated security researcher or vulnerability hunter and have discovered a security flaw in the Symantec CloudSOC platform including the cloud application and infrastructure, we appreciate your support in disclosing the issue to us in a responsible manner.

Our responsible disclosure process is managed by security team at Symantec. We are always ready to recognize the efforts of security researchers by rewarding them with a token of appreciation, provided the reported security issue is of high severity and not known to us.

While reporting the security vulnerability to Symantec Security, please refrain disclosing the vulnerability details to public outside of this process without explicit permission. Please provide the complete details. We determine the impact of vulnerability by looking into the ease of exploitation and business risks associated with the vulnerability.

Response

As a security researcher, if you identify or discover a security vulnerability in compliance with the responsible disclosure guidelines, Symantec security commits to:

- acknowledge the receipt of reported security vulnerability in a timely fashion
- notify you when the vulnerability is remediated
- extend our gratitude by providing a token of appreciation in supporting us to make our customers safe and secure

Please send the details of the discovered vulnerability or any security issue to : security@symantec.com.