System and Organization Controls (SOC) 3

Report on the Symantec CloudSOC Service Relevant to Security

For the Period
January 1, 2020 to June 30, 2020

Table of Contents

I. INDEPENDENT SERVICE AUDITORS' REPORT

INDEPENDENT SERVICE AUDITORS' REPORT

To the Management of Broadcom, Inc.
San Jose, California

Scope

We have examined management's assertion, contained within the accompanying "Assertion of Broadcom Inc. Management" (assertion) that Broadcom's controls over the Symantec CloudSOC Service (system) were effective throughout the period January 1, 2020 to June 30, 2020, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Service Organization's Responsibilities

Broadcom is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Broadcom's service commitments and system requirements were achieved. In Section II of this report, Broadcom has provided the accompanying assertion titled "Assertion of Broadcom Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Broadcom is responsible for preparing the description and assertion; including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Broadcom's relevant security policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Inherent Limitations

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that Broadcom's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, Broadcom's controls over the system were effective throughout the period January 1, 2020 to June 30, 2020, to provide reasonable assurance that its principle service commitments and system requirements were achieved based on the applicable trust services criteria.

JohansonGroup LLP

Colorado Springs, Colorado
September 1, 2020

II. ASSERTION OF BROADCOM, INC. MANAGEMENT

Assertion of Broadcom, Inc. Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Broadcom's Symantec CloudSOC service (system) throughout the period January 1, 2020 to June 30, 2020, to provide reasonable assurance that Broadcom's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Broadcom, Inc. Description of the System," (description) and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2020 to June 30, 2020, to provide reasonable assurance that Broadcom's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Broadcom's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the accompanying system description.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period January 1, 2020 to June 30, 2020, to provide reasonable assurance that Broadcom's service commitments and system requirements were achieved based on the applicable trust services criteria.

Broadcom, Inc. Management
September 1, 2020

III. BROADCOM, INC. DESCRIPTION OF THE SYSTEM

TYPES OF SERVICES PROVIDED

Symantec CloudSOC service ("CloudSOC" or "the Service") is a secure, shared cloud-based platform provided and operated by Symantec Enterprise Division, a division of Broadcom (hereafter "Symantec" or "SED"). CloudSOC enables organizations to extend their security policies and policy enforcement to their cloud applications. The primary components of the CloudSOC service are:

Audit

Audit allows an organization to get a summary report card for their organization about cloud app security. This report can be used to identify all Software as a Service ("SaaS") apps used across the organization, apps that pose medium or high risk, and top riskiest apps, as well as users and location of these apps. An Audit Score provides a top-level view of an organization's risk profile. Symantec CloudSOC's algorithms automatically assign a Business Readiness Rating™ to the cloud services that are discovered based on a comprehensive set of criteria. These ratings can be tailored to suit an organization's requirements, by customizing the importance of any of the criteria. Advanced visualization allows Audit users to instantly pivot on multiple parameters to view data from various perspectives. These views can be further refined with granular filters, enabling the organization to quickly gain insights into cloud app usage and take action. Audit allows organizations to easily compare and contrast existing cloud apps side-by-side with similar apps, enabling the organization to narrow in on which may be best suited for general adoption. This comparison is supported by an extensive database containing a detailed analysis of thousands of cloud services.

Detect

Detect uses advanced machine learning and data science to detect threatening activities and users in cloud services. This allows organizations to identify threats without sifting through large numbers of historical cloud service usage records. Detect helps organizations identify specialized malware threats to their cloud data in real-time, including Zeus-like malware, watering hole attacks or other sophisticated threats exposed by the use of cloud services. Symantec's data science algorithms assign a threat score to highlight the risk levels of all account activities on cloud services. By immediately identifying suspicious behavior, these scores enable the organization to define simpler and smarter policies and controls to protect data in the cloud.

Protect

Protect allows companies to implement global policies for use of cloud services in a way that hides the complexities associated with the technical enforcement of those policies on disparate cloud services platforms.

Investigate

Investigate allows organizations to perform post-incident investigations and forensic analysis across all historical transactions for cloud applications and services. Investigate can facilitate "deep dive" analysis for legal, compliance or human resource initiatives, ensuring cloud-based data is no longer outside the sphere of enterprise analysis. Investigate allows organizations to ingest data from multiple sources, including real-time traffic analytics, application programming interface ("API") data from cloud services and data from other security technologies to provide a comprehensive picture of cloud activity. Organizations can then cross-correlate this data to find relevant information and patterns to support investigations.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Commitments are declarations made by management to customers regarding the performance of Symantec CloudSOC. Commitments are communicated in written individualized agreements and standardized contracts.

System requirements are specifications regarding how the Symantec CloudSOC should function to meet Broadcom's principal commitments to user entities. System requirements are specified in Symantec CloudSOC's Service Agreement and its end user documentation, both of which are available internally to all employees and externally to all CloudSOC customers.

Trust Services Category	Service Commitments	System Requirements
Security	• Protection of data at rest and in transit. • Regular System updates. • Protection and security of the information system from unauthorized access, use, modification, disclosure, destruction, threats, or hazards.	• Logical and physical access standards • Access provisioning and deprovisioning standards • Access reviews • Encryption standards • Intrusion detection and prevention standards • Risk and vulnerability management standards • Configuration management • Incident response standards • Change management standards • Vendor management standards • System access is granted to authorized personnel only • Regular security assessments • Identification and remediation of security incidents • Perform risk assessments for both internal and external threats to the system and its information

THE COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICE

The boundaries of the system are the specific aspects of Broadcom's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the system.

The components that directly support the services provided to customers are as follows:

Infrastructure

The following is a summary of the Infrastructure that comprises the System and that which is used to address the security of the System:

- Data Center – AWS provides data center and Infrastructure-as-a-Service capabilities, physical and environmental security services. However, Broadcom is responsible for designing and configuring the CloudSOC architecture within AWS to ensure CloudSOC's security requirements are met.
- Servers – Virtualized Linux servers are used within the AWS environment in combination with AWS ELB for load balancing. AWS Security Groups provide perimeter firewall capabilities.
- Databases – MongoDB, ElasticSearch, AWS RDS and AWS Redshift are used to provide key data storage functionality for storing, searching, removing and otherwise processing live data used to support the System.
- Endpoint Computers – Broadcom supplies Apple MacBook and Dell Windows laptops for employees tasked with ensuring the security of the System. Okta software is used to provide multi-factor authentication.
- Source Code Repository – GitHub provides source code repository-as-a-service infrastructure.

Software

The application programs and information technology ("IT") system software that support the operating systems, middleware and utilities include:

- Configuration management (Salt)
- Remote administration (SSH)
- Two-factor authentication (Okta)
- Monitoring and logging utilities (Splunk, AWS CloudWatch and CloudTrail)
- Security monitoring and scanning (Amazon GuardDuty and Qualys)

- Data monitoring and visualization (Wavefront)
- Application Performance Monitoring (New Relic)

People

Symantec is a division of Broadcom. Symantec develops, manages, and secures Symantec CloudSOC via separate functional groups. The personnel involved in the governance, operation and use of the System are:

- Engineers – Write internally developed software for key System functionality.
- Quality Assurance ("QA") – Test the software written by the Engineers for security, availability, and confidentiality robustness.
- DevOps – Perform routine operational maintenance and monitoring of the System Infrastructure and facilitate software releases in order to improve the System.
- Security – Manage the overall security and security-related compliance of the System by defining policies, procedures and standards, and working with the Engineers, QA and DevOps teams to ensure that the foregoing items are implemented.
- Customer Support – Manage customer escalations and interactions.
- Human Resources (HR) – Manage the processes that support the employee lifecycle, to include: partnering with management on defining new roles/positions; performing background screening, onboarding new personnel, and facilitating the employee termination process.

Procedures

Procedures include the automated and manual procedures involved in the operation of Symantec CloudSOC. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, IT, human resources, etc. These procedures are drafted in alignment with the overall Broadcom Information Security Policies and are updated and approved as necessary for changes in the business, no less than annually.

- Logical and Physical Access - How Symantec restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
- System Operations - How Symantec manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.
- Change Management - How Symantec identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.

- Vulnerability and Risk Mitigation - How the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Data

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts. The Data relevant to the System is:

- Firewall and proxy logs received from the customer environments to audit cloud apps.
- Metadata related to actions performed by the users in the cloud apps such as uploading, downloading of files, etc.
- Processed data is stored in the databases such as MongoDB and ElasticSearch. Sensitive data, such as user identifiers, can be anonymized via specific application components.
- Data specific to the results obtained from content inspection of the files as part of the Cloud Data Loss Prevention solution, which contains file metadata such as filenames, timestamps, user identifiers, etc.

THE APPLICABLE TRUST SERVICE CRITERIA AND RELATED CONTROLS

Applicable Trust Service Criteria

The Trust Service Categories that are in scope for purposes of this report are as follows:

- Security: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the security of information or systems and affect the entity's ability to meet its objectives.

The criteria are organized as follows:

1. *Control environment:* The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values, and qualifications of personnel, and the environment in which they function.

2. *Communication and information:* The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system, and the obligations of those parties and users to the effective operation of the system.

3. *Risk assessment:* The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks, including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

4. *Monitoring activities:* The criteria relevant to how the entity monitors the system, including the suitability, and design and operating effectiveness of the controls, and acts to address deficiencies identified.

5. *Control activities:* The criteria relevant to the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.

6. *Logical and physical access controls:* The criteria relevant to how an entity restricts logical and physical access, provides, and removes that access, and prevents unauthorized access.

7. *System operations:* The criteria relevant to how an entity manages the operation of system(s) and detects and mitigates processing deviations, including logical and physical security deviations.

8. *Change management:* The criteria relevant to how an entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.

9. *Risk mitigation:* The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

This report is focused solely on the security category and Broadcom has elected to exclude the availability, confidentiality, processing integrity and privacy categories.

Controls Related to the Applicable Criteria

Broadcom's applicable controls supporting the security category and related criteria are included in Section IV of this report. Although the applicable criteria and related controls are included in Section IV, they are, nevertheless, an integral part of the organization's description of its system.

The five interrelated components of internal control at Symantec include:

- Control Environment – sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

- Communication and Information – are systems, both automated and manual, that support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.

- Risk Assessment – is the entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks can be managed.
- Monitoring – is a process that assesses the quality of internal control performance over time.
- Control Activities – are the policies and procedures that help make sure that management's directives are carried out.

Symantec CloudSOC's internal control components include controls that may have a pervasive effect on the organization, an effect on specific processes, account balances, disclosures, classes of transactions or applications, or both. Some of the components of internal control include controls that have more of an effect at the entity level, while other components include controls that are primarily related to specific processes or applications. When assessing internal control, Symantec CloudSOC considers the interrelationships among the five components.

Control Environment

Integrity and Ethical Values

Broadcom has developed a Code of Ethics and Business Conduct that addresses acceptable business practices, conflicts of interest, and expected standards of ethical and moral behavior. Broadcom has also developed employee Confidentiality Agreements that prohibit inappropriate use and disclosure of customer or Corporate information. These documents are provided to all new employees. All employees and contractors are required to sign a Confidentiality Agreement as well as acknowledge and agree to follow the Code of Conduct

Broadcom management performs annual performance evaluations of personnel to maintain compliance with Broadcom policies and codes of conduct. Employees and contractors who violate the code of conduct are subject to disciplinary actions.

Board of Directors

The Broadcom Board of Directors or a designated committee oversees and advises Broadcom's corporate governance, strategy, and risk oversight. The Board of Directors, composed of internal and external business executives, meets regularly to discuss matters pertinent to Broadcom business operations, financial results, and strategic planning.

Organizational Structure

Symantec Enterprise Division (SED) has established lines of reporting which facilitate the flow of information to personnel. Broadcom's HR system has a built-in organization chart that sets forth Symantec Enterprise Division's lines of reporting and which is updated automatically as organizational changes occur. The Executive Management Team empowers business functions to implement and manage functional policies, procedures, methods, and organization structure for increasing operational effectiveness and service delivery excellence. The Broadcom organization is structured to oversee the implementation and compliance of all required financial, business, and security controls. Roles and responsibilities are segregated based on functional requirements and to ensure separation of authority for key controls.

Management's Philosophy and Operating Style

Senior management of the Symantec Enterprise Division (SED) takes a "hands on" approach to running the business. Senior Management is heavily involved in all phases of the business operations. Management uses a top-down approach to establish or update specific business objectives for business units and functions, including information technology, within the organization. This process includes budgeting resources and establishing metrics for the achievement of the objectives.

Authority and Responsibility

Management and employees are assigned levels of authority and responsibility to facilitate effective internal control. The Chief Information Security Officer (CISO) is responsible for overseeing the control environment. The duties, responsibilities, and hierarchy of employees on the information security team are defined in a role matrix and form the foundation of Symantec's control environment. The CISO reports administratively to the CIO, with an escalation point to the CFO. As part of the development of specific business objectives, the General Manager for the Symantec Enterprise Division is responsible for executing the strategy and other decisions agreed upon by the executive management and the Board of Directors.

Human Resources

Broadcom maintains formal hiring and termination policies and procedures. Applicants with a role in the delivery of services are hired based on their ability to satisfy the job duties and responsibilities of the position and fulfill the goals and expectations of Broadcom. They are evaluated on their level of education, the merits of their experience, and their knowledge of relevant security controls and processes. All applicants must undergo a background check in accordance with local law; employment is contingent upon satisfactory results. Broadcom has a process to assign key processes and technology to authorized personnel.

Upon hiring and annually thereafter, all employees must successfully complete training courses covering Broadcom's code of conduct, data protection/privacy, and basic information security practices. The training courses are designed to assist employees in identifying and responding to social engineering attacks and in avoiding inappropriate security practices.

Contractors are required to follow the same onboarding process as employees and are contractually obligated to perform the same background checks and security awareness training requirements as employees. Employees' and contractors' compliance with security awareness training requirements is monitored on an annual basis by Digital Trust & Safety.

All employees go through an annual performance review cycle. At the beginning of each review period, employees and their immediate supervisors establish goals and expectations for their job performance over the upcoming year based on the job duties, priorities, and responsibilities described.

Employees receive an annual performance review from their supervisors that assesses the employees' performance against the agreed-upon goals and expectations. Employees whose performance is not in alignment with established goals and expectations for job performance, or who are not fulfilling their job

responsibilities, may be referred to human resources by their supervisor to develop a performance improvement plan. If an employee violates any Broadcom policies, or otherwise acts in a manner deemed contrary to the mission and objectives of Broadcom or in violation of the code of conduct, whether purposefully or not, the employee is subject to sanctions up to and including termination of employment.

Communication and Information

Broadcom has implemented information and communication mechanisms to make information available regarding its business practices.

Broadcom has a documented Information Security Policy and a suite of supporting policies. These documents are updated at least annually and are made available to all employees. The internal communication of cybersecurity information for employees is according to their role in the organization.

Broadcom has reporting mechanisms for employees to communicate potential security issues or concerns they have been involved in or witnessed (such as phishing attacks, malware, lost or stolen devices, and inappropriate information disclosure). One mechanism employee can use includes the anonymous EthicsLine, available 24/7 via phone, email, or website. SED also has established processes to accept and address reports of software vulnerabilities, including providing a means for external entities to contact the information security group.

SED obtains or generates and uses relevant information to support the functioning of internal control through the following:

- Control monitoring through periodic management review meetings, internal and external audits
- Vulnerability scans
- Penetration testing
- Log management tools and reviews

Broadcom limits communication of matters related to the functioning of internal systems to only those stakeholders and business partners who have a need to know such information. This information is communicated via mediums appropriate to the nature of the information and the urgency of the situation, and may include conference calls, electronic mail, memoranda, or in-person meetings. In the rare instance when public disclosure of such matters would be necessary or appropriate, Symantec's legal counsel and Corporate Communications team are responsible for jointly distributing and communicating such disclosure.

Broadcom provides customers with multiple channels to report and manage service issues. Dedicated support resources are responsible for keeping these Service Requests up to date and use available escalation and communication methods to keep customers informed about their requests.

Broadcom communicates its policies and business practices to its customers in the form of service contracts and user agreements, which must be accepted before services are rendered. These agreements

delineate customer and Broadcom responsibilities as they pertain to confidentiality, ownership, and other areas of liability. Broadcom's privacy policy is provided on the Broadcom website.

Risk Assessment and Mitigation

The Corporate Cyber Security team oversees Broadcom's risk assessment process to identify and manage risks that could affect Broadcom's ability to provide reliable services to its clients. This process requires management to identify significant risks in their areas of responsibility and to implement measures to address those risks. In designing its controls, Broadcom has considered the risks that could prevent it from effectively addressing the criteria under the security trust services principle.

Symantec Enterprise Division (SED) maintains a risk management framework designed to ensure risks are evaluated and that controls are reasonably designed, implemented, and operated to address all areas, as appropriate, to detect, respond to, mitigate, and recover from security events based on the assessed risks. Areas for consideration include compliance objectives, external laws and regulations, and risk appetite. Areas for evaluation include systems development, computer operations, program changes, and access to programs and data. Implemented controls include preventive and detective controls, such as manual, automated, or IT-dependent controls based on the environment in which the entity operates, the nature and scope of the entity's operations, and its specific characteristics. SED identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. SED's risk assessment process includes an analysis of possible threats and vulnerabilities relative to each of the objectives. The risk identification process includes consideration of both internal and external factors and their impact on the achievement of the objectives.

SED considers the potential for fraud in assessing risks to the achievement of objectives. The assessment of fraud risk considers fraudulent reporting, possible loss of assets, or data and corruption resulting from the various ways that fraud and misconduct can occur. It also considers opportunities for unauthorized acquisition, use or disposal of assets, altering of the entity's reporting records, or committing other inappropriate acts and how management and other personnel might engage in or justify inappropriate actions.

SED identifies and assesses changes that could significantly impact the system of internal control. The risk identification process considers changes to the regulatory, economic, and physical environment in which SED operates. SED considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations, rapid growth, and new technologies on the system of internal control.

Identified risks are analyzed through a process that includes estimating the potential significance of the risk. SED's risk assessment process includes considering how the risk should be managed and whether to accept, avoid, mitigate, or share the risk. SED determines mitigation strategies for the risks that have been identified and designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy.

Security risks related to external parties (such as contractors and vendors) are identified and addressed based on Symantec's procurement process. Designated responsibilities are defined in reviewing risks associated with external parties and establishing relevant agreements. Purchase orders to engage a third-party require a vendor agreement and signed NDA to be established.

Sensitive information is disclosed to a vendor or business partner only on an as-needed basis, and only if the vendor or business partner has enacted appropriate information security and privacy controls. All vendors and business partners with access to sensitive information are subject to confidentiality and privacy agreements and other contractual confidentiality provisions, which must be signed and acknowledged before access to Symantec's systems and data is granted.

Broadcom's Supplier Security Assurance program manages supply chain security risk throughout the lifecycle of the relationship and provides assurance that third parties who handle and process information and facilities on Symantec's behalf do so in accordance with legal, regulatory, and contractual requirements for security.

Adoption of a supplier's services has inherent information security risks, which are managed by adopting the following approach:

- Categorize: Third parties are categorized according to the nature, criticality, and likelihood of risk commensurate with the adoption of their services
- Assess: Third parties are security reviewed in accordance with their assigned risk category
- Respond: The Supplier Assurance team conducts risk assessments based upon information provided in completed questionnaires and audit findings
- Monitor: All risk remediation actions identified from risk assessments are tracked through to closure. Third parties are periodically re-assessed, according to their risk categorization

Information Security Policies

Broadcom has developed Company-wide Security policies, procedures, guidelines, templates, and checklists. The Company policies are reviewed by the management team. As a Division of Broadcom, Symantec workers are informed about their responsibilities with regard to implementing approved policies related to Security. The policy domains include Acceptable Encryption Use, Acceptable Use, Asset Management, Data Backup, Business Continuity & Disaster Recovery, Capacity Management, Change Management, Cybersecurity Incident Response, Data Classification, Access Control, Mobile Device Use, Personal Data Handling and Protection, Physical Security, Privacy and Data Protection, Privacy Incident Response, Risk Management, Secure Development, Supplier Risk Program, Vulnerability & Patch Management. Broadcom updates the policies based on changes to the Broadcom environment, the annual risk assessment, and because of evolving business and industry requirements.

Monitoring

Broadcom selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. Internal personnel conduct periodic assessments and tests of internal controls that include (a) working with process owners and IT support personnel to identify specific security threats and vulnerabilities and how the associated risk is being addressed and (b) tests of the design, implementation, and operating effectiveness of internal controls that address risks. Members of the internal assessment team have the requisite knowledge of and

experience with cybersecurity risks and controls. They also subscribe to industry standard bulletins and email alerts on security, delivered through Broadcom's Vulnerability Management Team.

Broadcom also uses external parties to independently evaluate the state of the control environment. Quarterly vulnerability assessments and annual penetration tests are performed by an external service provider to identify specific technical threats and vulnerabilities and to benchmark the environment against leading cybersecurity practices. Every year, Broadcom engages a service provider to perform an independent assessment of the system program to evaluate alignment with leading industry practices and consistency with company policies in order to identify gaps and potential opportunities for improvement.

Both internal and external evaluations are made using a risk-based approach that may vary in the nature, timing, and extent of testing. The criteria for such evaluations, including the nature and frequency of such evaluations, are reviewed during the annual risk assessment and modified as needed, with consideration for changes to Broadcom's operational processes, including changes to the size, scope, and operational nature of the business, recent security threats or incidents, new or emerging risks, and changes in industry standards.

The results of all monitoring activities, regardless of source, are entered into a vulnerability tracking system for evaluation and identification of remediation activities that may be needed. Identified vulnerabilities are assessed regarding the likelihood and magnitude of exploitation. All vulnerabilities evaluated are identified for remediation or additional monitoring. Responsibilities for corrective action plans are assigned and completion dates determined. The Information Security team reviews the list of open vulnerabilities monthly to monitor progress toward resolution and to identify trends and responses.

Control Activities

Symantec Enterprise Division's (SED) control activities are defined through its established policies and procedures. Policies are dictated through management or board member statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected, and procedures that put policies into action. A list of policies and procedures is documented in the above Procedures section.

Logical and Physical Access

Broadcom's Information Access Control Policy establishes the access control requirements for requesting and provisioning user access for the system. The policy requires that access be denied by default, following a least privilege principle, and be granted only upon business need. Broadcom uses centralized authentication and authorization to restrict access to the systems and services within the environment. Each user account is unique and is identifiable to an individual user. Segregation of duties is established on critical functions within the environment to minimize the risk of unauthorized changes to production systems.

Domain-account management requests are routed to the designated asset owner or associated employee according to established account provisioning and de-provisioning processes for approval. Typically, access is controlled through addition of individual user accounts to established domain security groups within the Active Directory (AD). Based on the configuration of a security group, any access requests

require explicit approval from the assigned security group owner. Requests are automatically forwarded to the security group owner for approval in the system.

Employee status data is used to facilitate the provisioning and removal of user accounts in the system. Account management processes prevent the creation of an account for individuals that do not have valid HR records. Select users can request removal of user accounts from the system. In addition, system owners can directly remove users from Security Groups. Upon termination, employees are required to return their badges and workstations to Symantec. Terminated employees are removed from the AD and thus all access is terminated.

Automated mechanisms have been implemented to manage the appropriateness of access granted to information systems. Manual periodic reviews of individual accounts and security group memberships on assets are performed by authorized individuals, as appropriate, to evaluate whether access is still required. Remediation action is taken, as necessary, based on the review.

Policies and standards have been established and implemented to enforce appropriate user account password expiration, length, complexity, and history. All personnel are required to follow Broadcom's password policy for all domains as well as local user accounts for all assets.

Access to the production environment is controlled through a designated set of access points and restricted to the product teams. Users are authenticated to access points using AD domain credentials depending on where the production assets are located. Virtual private network ("VPN") access also requires authentication. Personnel connect to servers in the production environment using encrypted administration protocols such as secure shell ("SSH"). Passwords, along with two-factor authentication used to access network devices are restricted to authorized individuals and system processes based on job responsibilities and are changed on a periodic basis.

Cryptographic controls and approved algorithms are used for information protection within the production environment and are implemented based on Broadcom's policies and standards. Cryptographic keys are managed throughout their lifecycle (e.g., ownership, generation, storage, distribution, periodic rotation and revocation) in accordance with key management procedures.

Symantec Enterprise Division (SED) maintains a detailed inventory of all information systems. All such assets are assigned ownership by a designated department or team within Symantec and prioritized based on the asset's business value and criticality to the organization. Information and data assets are subject to the data management policy that defines parameters for the ownership, classification, security, storage, and retention of data. Software and hardware assets are subject to the information systems management policy that defines parameters for the acquisition, development, maintenance, security, and disposal of information system assets. Steps are taken to protect assets commensurate with the respective asset's classification and its data sovereignty. Review of asset inventory, ownership, and classification is performed at least semi-annually.

The inventory of servers is monitored and maintained by the product team. On a monthly basis, the Broadcom Financial team checks for completeness and accuracy of the inventory to ensure that it represents the production environment appropriately. SED has created and implemented processes to control the delivery and removal of information assets through a centralized ticketing system. In addition, network architecture is maintained as part of the inventory process. Metadata of the assets are collected and maintained within the inventory that provides an overview and flow of the network.

Symantec CloudSOC's production environment is entirely contained within Amazon's hosted environment; as such, Symantec personnel do not have physical access to the production environment.

Physical access to the distributed production environment is a subservice control.

System Operations

Technical standards and baselines have been established and communicated for production system deployments. Automated mechanisms and periodic scanning have been deployed to detect and troubleshoot exceptions and / or deviations from the baseline in the production environment. Where applicable, mechanisms are in place for services to re-image production servers with the latest baseline configuration at least on a monthly frequency. Further, OS and product teams review and update configuration settings and baseline configurations at least annually.

Broadcom has implemented procedural and technical standards for the deployment of network devices. These standards include baseline configurations for network devices, network architecture, and approved protocols and ports. Broadcom regularly monitors network devices for compliance with technical standards and potential malicious activities.

Broadcom has implemented agent-based monitoring infrastructure and custom script-based monitoring within the environment to provide automated logging and alerting capabilities. The logging solutions are enabled on all production systems. The monitoring system detects potential unauthorized activity and security events such as the creation of unauthorized local users and local groups. The monitoring agents are responsible for monitoring a defined set of user and administrator events, aggregating log events and sending the aggregated log information to a centralized log repository at regular intervals.

Broadcom has established a policy which restricts the log and monitor access to only authorized staff with a business need to access such systems. Product teams determine the specific events that need to be captured in consideration with a baseline. Administrator, operator, and system activities performed, such as logon / logoff within the environment, are logged and monitored.

For network devices, Broadcom monitors, logs, and reports on critical / suspicious activities and deviations from established baseline security configurations for the network devices. Predefined events are reported, tracked, and followed up on and security data is available for forensic investigations. The logs are retained centrally for forensic related analysis and access to the logs follows the same procedures defined above.

Broadcom has implemented an alerting system to provide real-time alerting through automatic generation of emails and alarms based on the log information captured by the monitoring infrastructure. Product teams are responsible for configuring the events to be alerted. The event and warning logs are routinely examined for anomalous behavior and, when necessary, appropriate actions are taken in accordance with the incident handling procedures described in the Incident Management section. The product teams manage response to malicious events, including escalation to and engaging specialized support groups. In addition, Symantec monitors relevant external information to stay up-to-date with current threat scenarios and countermeasures.

Symantec Enterprise Division (SED) carries out internal and external scans to identify vulnerabilities and assess the effectiveness of the patch management process. These scans are used to ensure compliance with baseline configuration templates, validate that relevant patches are installed, and identify

vulnerabilities. The scanning reports are reviewed by the Product team, and remediation efforts are conducted in a timely manner.

Security patches are applied immediately or during a scheduled release to the environment based on the severity of the vulnerability. Processes are in place to evaluate patches and their applicability to the environment. Once patches have been reviewed and their criticality level determined, product teams determine the release cadence for implementing patches without service disruption.

Product teams follow a change process to modify the underlying OS within the platform. All changes are reviewed and tested, at a minimum, for their quality, performance, impact on other systems, recovery objectives and security features before they are moved into production using a defined release process. Test windows have been established for reviewing and testing of new features, and changes to existing features and patches.

Penetration testing (pen test) is performed at least annually on the system. The pen test scope is determined based on SED's areas of risk and compliance requirements.

Broadcom has implemented an Incident Management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation and response to incidents internally and to customers.

Broadcom has established Incident Response procedures and centralized tracking tools which consist of different channels for reporting production system incidents and weaknesses. Automated mechanisms include system monitoring processes for alerting security teams per defined and configured events, thresholds, or metric triggers. Customers are made aware of their responsibilities of reporting incidents that shall be investigated without any negative consequences. Broadcom's incident response provides 24x7 event / incident monitoring and response services. The teams assess the health of various components along with access to detailed information when issues are discovered. The infrastructure is designed for resilience and contingency plans are in place in case of service-impacting events. Symantec can deploy an entire copy of its production environment in any AWS region in the event of the loss of a single AWS region.

Additionally, Broadcom conducts yearly tests of the Incident Management SOPs and response capabilities. Reports related to information security events are provided to management on a quarterly basis.

Broadcom's product teams use the established incident classification, escalation, and notification process for assessing an incident's criticality and severity, and accordingly escalating to the appropriate groups for timely action. The security team documents, tracks, and coordinates responses to incidents. Where required, security incidents are escalated to the privacy, legal, or executive management team(s) following established forensic procedures to support potential legal action after an information security incident.

Post-mortem activities are conducted for customer impacting incidents or incidents with high-severity ratings. The post-mortems are reviewed by the security team during monthly review meetings with senior management. Incident and security post-mortem trends are reviewed and evaluated on a periodic basis and, where necessary, the platform or security program may be updated to incorporate improvements identified as a result of incidents.

Change Management

The Change Management process has been established to plan, schedule, approve, apply, distribute, and track changes to the production environment through designated responsibilities with the objective of minimizing risk and customer impact. It further controls the integrity and reliability of the environment while maintaining the pace of change required for business purposes.

Software, system, and configuration changes are managed through a formal change and release management procedure and tracked using a centralized ticketing system. The categorization of these changes is based on priority and risk associated with the change. Changes are requested, approved, tracked, and implemented throughout the release lifecycle, which includes product and engineering planning, release management, deployment, and post-deployment support phases. Change requests are documented, assessed for their risks, and evaluated / approved for acceptance by the designated personnel.

Patches are released through the periodic OS release cycle in accordance with change and release management procedures. Emergency out-of-band security patches are expedited for more immediate release.

Formal security and quality assurance testing are performed prior to the software release through each pre-production environment (i.e., development and test/sandbox) based on defined acceptance criteria. The results of the quality assurance testing are reviewed and approved by the appropriate personnel prior to moving the release to production. Changes are reviewed for their adherence to established change and release management procedures prior to closure. Once deployed, changes are monitored for success; failed implementations are immediately rolled back, and the change is not considered as completed until it is implemented and validated to operate as intended.

The Symantec CloudSOC product team's software development practices, outlined in its Software Development Lifecycle (SDLC) methodology, is aligned with Broadcom's Secure Software Development Lifecycle Standard. The Standard introduces security and privacy control specifications during the feature/component design and throughout the development process, which are reviewed through designated security roles.

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

Symantec CloudSOC was designed with the assumption that certain controls will be implemented by user organizations. Such controls are called complementary user entity controls. It is not feasible for all of the criteria related to the System to be solely achieved by Symantec's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Symantec.

The following complementary user entity controls should be implemented by user organizations to provide additional assurance that the control activities described within this report are met.

As these items represent only a part of the control considerations that might be pertinent at the user organizations' locations, user organizations' management and auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

Complementary User Entity Controls
User entities are responsible for:
• Notifying Symantec Enterprise Division (SED) in a timely manner when changes are made to technical, billing, or administrative contact information.
• Developing their own disaster recovery and business continuity plans that address the inability to access or utilize Symantec services
• Ensuring the confidentiality of any user accounts and passwords assigned to them for use with Symantec's CloudSOC.
• Notifying SED regarding new user accounts and terminated user accounts.
• Informing SED of any regulatory issues that may affect the services provided by SED.
• Understanding and complying with their contractual obligations to SED.
• Notifying SED of user account maintenance tasks (including the revocation of account access) in a timely manner.
• Immediately notifying SED of any actual or suspected information security breaches involving SED, including compromised user accounts.
• Ensuring that designated authorized points of contact are appropriate.
• Ensuring that changes to authorized personnel are communicated to SED in a timely manner.
• Accepting the terms and agreement for using the SED online application.

SUBSERVICE ORGANIZATIONS AND COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

Broadcom uses Amazon Web Services (AWS) as a subservice organization for data center colocation services. The Symantec CloudSOC controls related to the CloudSOC system cover only a portion of the overall internal control for each user entity of the Symantec CloudSOC. The description does not extend to the services provided by the subservice organization that provides colocation services for IT infrastructure. Section IV of this report and the description of the system only cover the Trust Services Criteria and related controls of Symantec and exclude the related controls of AWS.

Although the subservice organization has been carved out for the purposes of this report, certain Trust Services Criteria are intended to be met by controls at the subservice organization. CSOCs are expected to be in place at AWS related to physical security and environmental protection, as well as backup and

recovery. AWS' physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities.

Broadcom management receives and reviews the SOC 2 report of AWS at least annually. In addition, through its operational activities, Symantec CloudSOC management monitors the services performed by AWS to determine whether operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also has communication with the subservice organization to monitor compliance with the service agreement, stay abreast of changes planned at the hosting facility, and relay any issues or concerns to AWS management.

It is not feasible for the criteria related to the Symantec CloudSOC Service to be achieved solely by Symantec CloudSOC. Therefore, each user entity's internal control must be evaluated in conjunction with the Symantec CloudSOC's controls and related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Facilities Housing the System	
Applicable Trust Services Criteria	Types of Controls Expected at the Subservice Organization (CSOCs)
CC-6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
CC-6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

SPECIFIC CRITERION NOT RELEVANT TO THE SYSTEM

There were no specific security Trust Services Criterion as set forth in TSP Section 100 that were not relevant to the system as presented in this report.

REPORT USE

The description does not omit or distort information relevant to the Symantec CloudSOC Service, while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.