Ensuring safe cloud app adoption with Symantec CloudSOC™

Symantec™

Shadow IT Discovery Best Practices Guide

Ensuring safe cloud app adoption with Symantec CloudSOC

Introduction 01

Shadow IT Discovery with CloudSOC

CloudSOC can help you more easily determine which apps should be blocked and which should be allowed within your organization by assisting in identifying unsanctioned Shadow IT, providing customized Business Readiness Ratings™ for each cloud app tailored to your organization's risk profile, and applying User Behavior Analytics (UBA) to identify hackers and malicious usage. Here you'll learn how to guide your organization through the process of safely adopting cloud apps and services using Symantec CloudSOC.

CloudSOC™

About CloudSOC

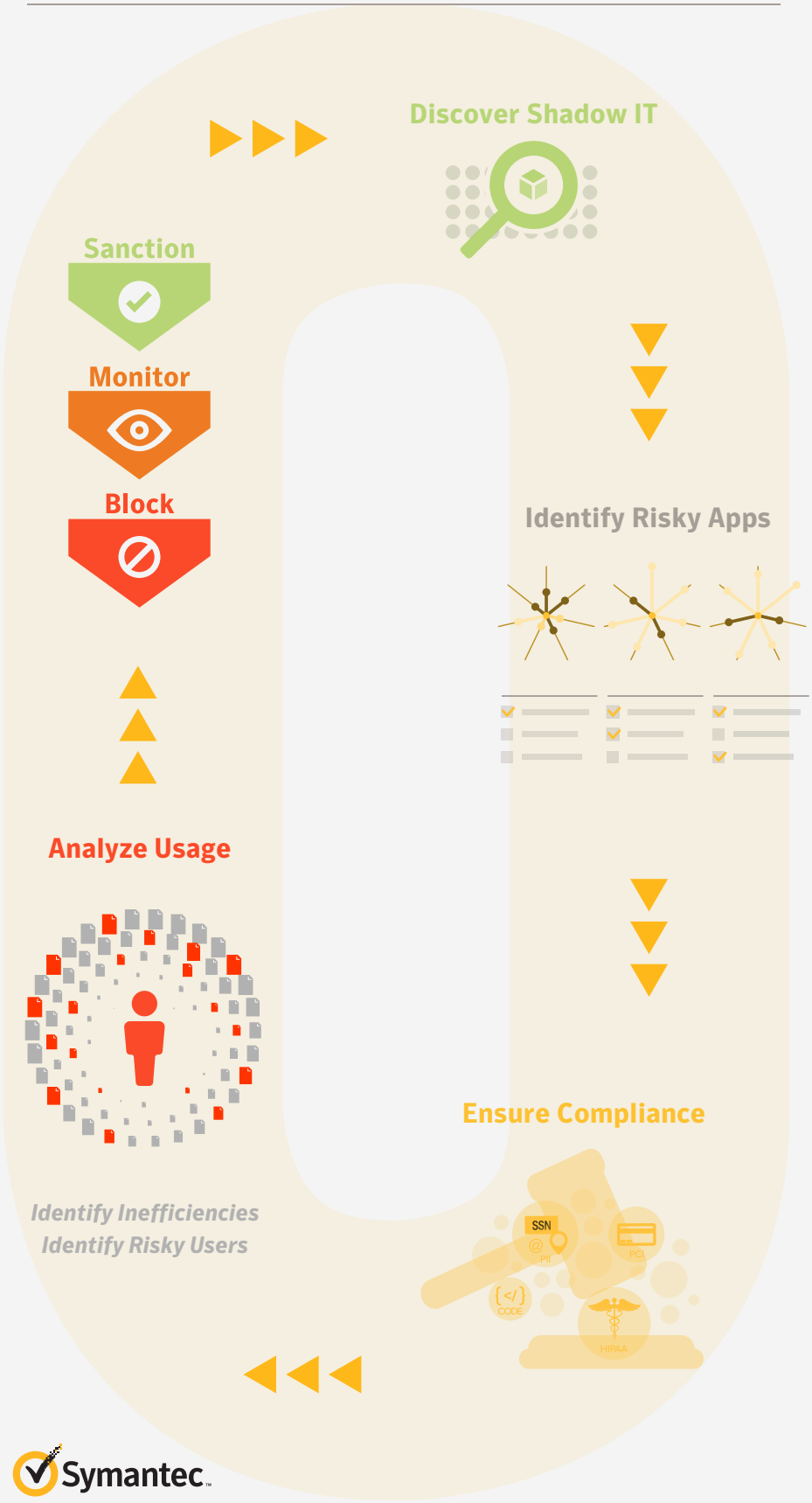
The Data Science Powered™ Symantec CloudSOC platform empowers companies to confidently leverage cloud applications and services while staying safe, secure and compliant. A range of Symantec security apps deployed on the extensible CloudSOC platform deliver the full life cycle of cloud application security, including auditing of shadow IT, real-time detection of intrusions and threats, protection against intrusions and compliance violations, and investigation of historical account activity for post-incident analysis.

Cloud discovery and safe adoption lifecycle 02

The cloud app adoption lifecycle follows a series of repeatable steps that organizations can follow to drive awareness with management and cloud users. By refining and repeating this process, organizations can begin to build this awareness. In addition, over time risky usage will decrease due to better controls and deeper understanding of how users can safely use cloud apps and services.

Regular consultation with business units and users throughout this lifecycle will enable organizations to gain greater insight into the business requirements they have for cloud apps, educate users on cloud use best practices, and include users as part of the solution. By alerting them to policy violations and redirecting them to use sanctioned apps, organizations can provide transparency into the cloud security decision making process. And by letting them report false positives organizations can gain valuable insight that will enable the process to be enhanced over time.

Safe adoption lifecycle



Discover Shadow IT
CIOs often need visibility into what cloud apps are being used organization-wide and who is using them. Governance groups may also mandate this information.

Identify risky apps
Security admins must identify SaaS apps posing a risk to their environments, such as understanding which have lax security controls, which can be conduits for data exfiltration, or which are hosted in rogue states.

Ensure compliance
Compliance officers may want to continuously monitor apps being used by the organization and individual departments to make sure apps have the appropriate certifications and meet compliance requirements.

Identify inefficiencies
Organizations may have many groups using a plethora of similar cloud applications. By identifying all apps in use and comparing functionality and security profiles, they can trim costs and simplify management.

Identify risky users
CIOs often want to identify how apps are being used and by whom, as well as risky user behaviors such as data exfiltration, data destruction, and account takeovers.

Block risky apps
Security administrators may want to enforce policies that prevent the riskiest apps from being used by their organizations.

Sanction secure apps
Organizations may want to examine current cloud app usage along with cloud app risk analysis to select sanctioned apps to be used by their employees.

Monitor business critical apps
Some apps may not match the organization's security requirements but are business critical or are used by many employees in the organization. Organizations can sanction these apps as an exception then monitor them for risk over time.

Considerations prior to defining sanctioned and unsanctioned apps 03

You need to keep in mind several questions as you step through the cloud app adoption process:

What are the business functionality and performance requirements identified by my users and business units?

- ☐ **What types of apps are my employees adopting? (i.e., file sharing apps CRMs and business analytics)**
- ☐ **Which users/departments are driving this usage?**

What is my company's tolerance for risk in cloud apps and services?

- ☐ **Are there compliance regimes that apply to my organization (HIPAA, GDPR, controls for PII and PCI, etc.)**
- ☐ **Does a business unit or department within the organization require waivers or exceptions due to critical business need for a particular app that may not meet security requirements?**

Which applications are my users and BUs adopting without IT sanction or oversight?

- ☐ **Do the apps align with the cloud services selected by the business?**
- ☐ **Do the categories of apps accessed align with the industries the business is active in?**
- ☐ **Are productivity metrics being met or will management need to effect change to improve?**
- ☐ **Do these apps have appropriate security controls?**
- ☐ **Do these apps align with compliance requirements?**
- ☐ **Can these apps operate as conduits for data exfiltration?**
- ☐ **If a large number of employees are using a particular risky app, will a broader discussion with executive stakeholders be required before replacing it with a more secure alternative or tagging it as an exception?**
- ☐ **Are there executive stakeholders who, for sensitive reasons must be consulted before blocking or replacing a risky cloud app?**
- ☐ **Have any new apps been added since last review?**

Are there any opportunities for consolidation or elimination of apps or accounts?

- ☐ **Are there multiple apps that provide similar or identical functionality?**
- ☐ **Are there multiple accounts for the same app?**

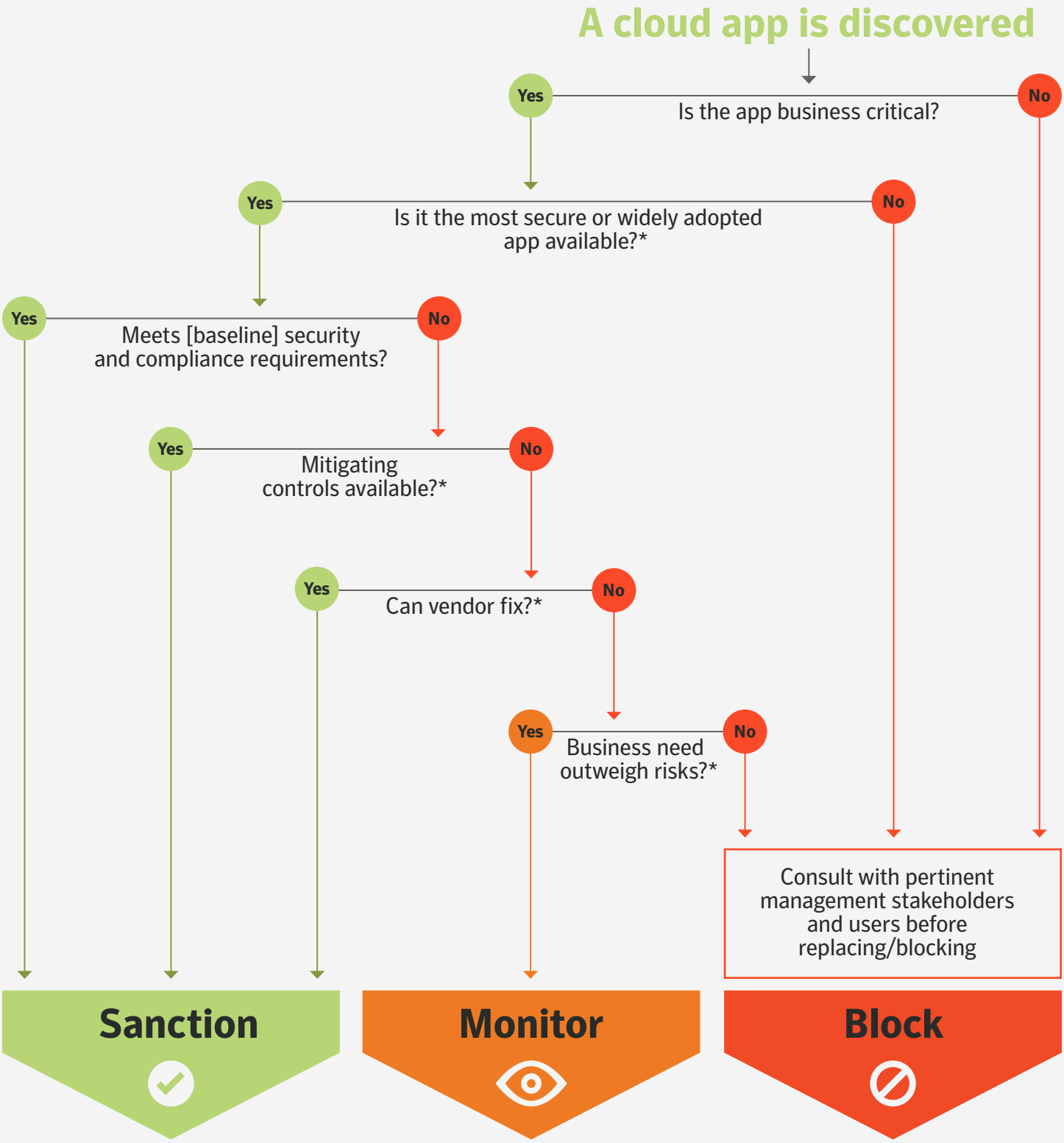
Who is accessing the riskiest apps?

- ☐ **How often are employees accessing these apps?**
- ☐ **Which locations are involved?**
- ☐ **Which browsers and platforms are employees using?**

Who are the riskiest users? Which users are exhibiting risky behavior, such as oversharing documents, downloading too many files, encrypting too many files?

- ☐ **Is the risky behavior due to intentional malicious activity on the part of the user, account takeover by a hacker, or misuse?**
- ☐ **If oversharing, misuse or other risky behavior occur, what processes does the organization have in place to provide coaching and training to high risk users?**

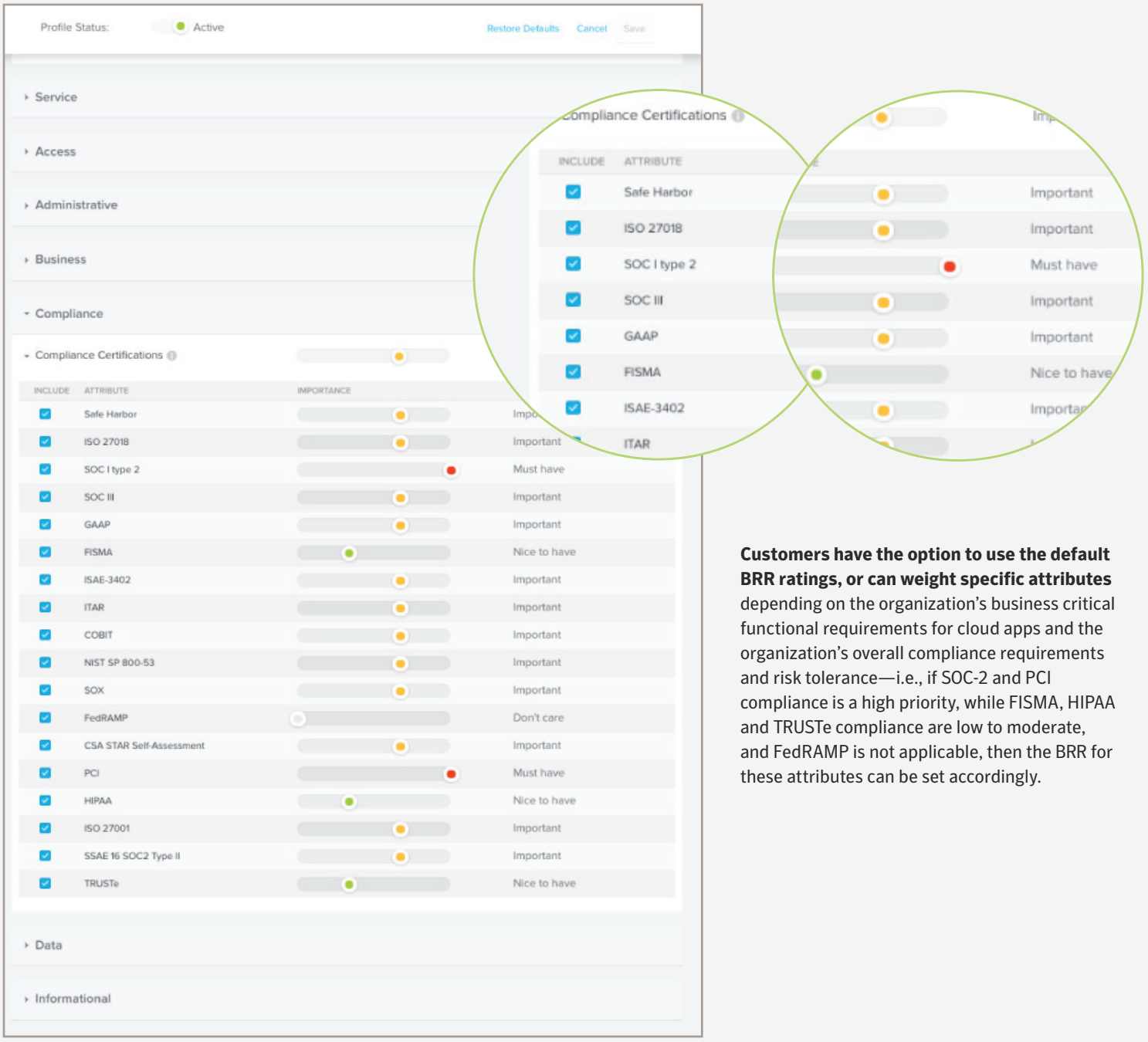
Cloud app adoption workflow 04



*Appropriate management stakeholders, governance and risk boards, and legal representatives should be consulted before proceeding to ensure that issues of business continuity and critical app functionality are taken into account before apps are blocked, replaced or approved.

Business Readiness Rating™, Determining security requirements 05

Symantec applies a Business Readiness Rating (BRR) to 20,000+ cloud apps and services classified and tracked on the CloudSOC platform. Business readiness is based on over 89 attributes, including whether the app meets standards for important compliance regimes, whether effective access controls are in place, and whether the app encrypts data. A cloud application is considered to be enterprise-ready if it rates above 80 (high or excellent).



Customers have the option to use the default BRR ratings, or can weight specific attributes depending on the organization's business critical functional requirements for cloud apps and the organization's overall compliance requirements and risk tolerance—i.e., if SOC-2 and PCI compliance is a high priority, while FISMA, HIPAA and TRUSTe compliance are low to moderate, and FedRAMP is not applicable, then the BRR for these attributes can be set accordingly.

Customer security requirements mapped to BRR 06

Category	Description		Mitigation Options
Compliance	Vendor should validate that SaaS services maintain compliance certifications with various compliance regimes	Compliance Certifications: i.e. HIPAA, ISO 27001, PCI-DSS and Safe Harbor	• Block app and select an alternative that complies with the necessary compliance regimes using the BRR rating.
Data Protection	Vendor should validate that there are data sharing policies with unauthorized third parties	Data Sharing Controls	• Enforce data sharing policy using the Symantec CASB Gateway
	Vendor should validate that the SaaS service encrypts data in the cloud—at rest, in motion, and in use—and how are encryption keys handled.	Data at Rest Encryption	• Encrypt sensitive content using Symantec CASB Gateway, PGP or CDP (tokenization) • Prevent sensitive or regulated data from upload to apps lacking encryption • Block app and select a secure alternative using the BRR rating.
		Data in Motion Encryption	• Encrypt sensitive content using Symantec CASB Gateway, PGP or CDP • Block app and select a secure alternative using the BRR rating
	Vendor should validate that HTTP security headers are supported	HTTP Security Headers	• Block app and select a secure alternative using the BRR rating.
Admin Controls	The vendor should support audit trails of administrators and users	Admin Audit Trail	• Audit admin and user activities and data access in all apps using the app using Symantec Shadow IT Audit service.
		User Audit Trail	
	The vendor should support administrative policy config-uration and enforcement	Policies	• Enforce granular policies using Symantec ProxySG, CASB Gateway or app-specific API based Securlets. • Block app and select a secure alternative using the BRR rating.

Customer security requirements mapped to BRR *(Cont.)*

Category	Description		Mitigation Options
Access Control	Vendor should validate the SaaS service supports strong password management controls, federated identity management, multi-factor authentication and integration with enterprise identity solutions such as LDAP and Active Directory	Brute-force protection	• Provide protection against brute force attacks using Symantec CASB Gateway. • Block app and select a secure alternative using the BRR rating.
		Enterprise Identity Integration	• Block app and select a secure alternative using the BRR rating.
		Federated Identity Management	• Block app and select a secure alternative using the BRR rating.
		Multi-factor Authentication	• Add SSO and tie into MFA • Block app and select a secure alternative using the BRR rating.
		Password Quality Rules	• Add Single Sign On • Block app and select a secure alternative using the BRR rating.
		Role Based Access Control	• Control admin privi-leges based on enterprise directory attributes
Service Characteristics	Vendor should validate the SaaS service employs a multi-tenant or a single-tenant architecture, and what policies are in place to address issues associated with multi-tenancy, including data cross pollination between customers and data retention rules	Hosting Service	• Block app and select an appropriate alternative.
		Multi-tenancy Support	• Ask vendor to switch to version of service that segregates customer data • Contractually indemnify vendor for data loss or downtime. • Buy cloud insurance. • Block app and select a secure alternative using the BRR rating.
Business Characteristics	The vendor should verify that the SaaS service is financially stable and has additional enterprise customers? Should also validate how long has the vendor been in business?	Financial Stability	• Ensure that the app vendor is financially secure and has been in business for a while. • Block app and select a secure alternative using the BRR rating.
Informational	Vendor should validate the general characteristics of the SaaS service such as client type support and type of service	SLA	• Contractually indemnify vendor for data loss or downtime. • Buy cloud insurance. • Block app and select a secure alternative using the BRR rating.
		Type of Clients	
		Type of Service	

Questions to ask a CASB vendor

- ☐ How many risk attributes are used to calculate risk readiness rating of apps?
- ☐ Is readiness rating customizable by assigning weights to risk attributes?
- ☐ Does the solution provide automated risk assessment reports?
- ☐ Is there an on-premises solution provided to automate uploading, anonymization, compression and caching of log data for Shadow IT analysis?
- ☐ Can risky cloud apps be blocked through integrations with secure web gateways or firewalls?

Identifying risky cloud usage and compensating controls 07

Risky Behavior	Examples	Typical Apps Used	Mitigation Options
Account Takeovers	• Anomalous frequent logins • Too many suspicious logins	All	Alert compromised users to change passwords. Monitor high risk employees for indicators of account compromise.
Data Exfiltration	• Anomalous frequent downloads • Anomalous frequent emails sent • Anomalous frequent file sharing • Anomalous frequent data previews	• BI • File Sharing • Cloud Storage • CRM • Document Management • Finance/Acct • HR • Software Development	Monitor high risk employees for indicators of account compromise.
Data Destruction	• Anomalous frequent deletes • Anomalous frequent edits		Monitor high risk employees for indicators of account compromise.

Identifying and protecting sensitive cloud data 08

Category	Description	Mitigation Options
Data Classification	Identify and classify sensitive data such as PII, PCO, PHI, source code, etc.	Detect and classify sensitive data using ContentIQ function in Symantec Gateway and/or Securlets.
Policy Enforcement	Sharing policies need to be set and enforced to prevent data from be overshared.	Set granular policies using the Symantec CASB Gateway or ProxySG
Data Protection	Many types of data such as PCI and PII should be encrypted before being uploaded to a cloud service	Tokenize or Encrypt PCI and other compliance related data (See data protection section above.)

Next steps 09

1. Mitigate Shadow IT Risk

Leveraging the powerful capabilities of a comprehensive CASB solution like Symantec CloudSOC, here is a summary of actions that information security professionals can take to mitigate risk from Shadow IT after initial application of web filtering policies using products such as Symantec ProxySG or Web Security Service (WSS):

Make smart app choices
Analyze what apps are appropriate for the company's environment, taking into consideration security controls, compliance regulations, and other important factors. Customize the rating to match the organization's policies and create a list of sanctioned apps. This information can be integrated with Symantec's Management Security Service (MSS) to be part of that overarching decision framework.

Review contracts with cloud providers
Read the fine print. Make sure to understand the liability and responsibility the cloud app provider is assuming with regard to security-related incidents. Ask how the service provider will support the organization in detecting and remediating security incidents. Know what security measures they have implemented.

Coach users
Identify users and departments leveraging inappropriate apps and work with them to find alternatives that fit their needs and the organization's security and compliance guidelines. Through CloudSOC, you can also inserting coaching messages automatically when users choose apps that are not sanctioned, and guide them to use the corporate standard.

Identify cost savings
Track apps with similar functionality or multiple instances of the same cloud app and explore opportunities for streamlining costs through eliminating redundant apps and consolidating subscriptions. CloudSOC enables organizations to compare apps side-by-side.

Block risky apps
Tune web proxy and firewall policies to block risky apps below a specified BRR rating that are inappropriate for the enterprise environment. In addition, any new app added that has a BRR rating below the threshold specified will be automatically blocked on day-one. This process can be streamlined via CloudSOC integration with web proxies.

Monitor continuously
Using CloudSOC, organizations can continually track cloud usage activity to monitor overall security risk profile, ensure compliance and look for trends and opportunities over time.

2. Mitigate Data Loss Exposure

Symantec CloudSOC CASB Gateway and Securlets provide the ability to classify risky data in cloud accounts and enable organizations to set policy to prevent its leakage. In addition, the CASB Gateway and Securlets can be integrated with Symantec DLP, providing the ability to leverage existing on-prem DLP policies and workflows in the cloud without need to rewrite them, can be managed from the Symantec DLP management console.

Identify and remediate risky exposures
Analyze existing cloud file sharing apps—such as Box, Google Drive, Dropbox, Salesforce or Office 365—to identify any sensitive or compliance-related content that may be shared inappropriately (in other terms, perform a Shadow Data Risk Assessment). Leverage Symantec CASB Gateway to remediate these exposures to align with security policies.

Define a data protection strategy
Develop a strategy to protect sensitive data and adhere to compliance regulations. Decide which types of content to allow in the cloud and if the sharing of such content will be restricted or given additional security protection via encryption or tokenization.

Enforce policies for sensitive data
Using Symantec CloudSOC to define and enforce appropriate policies that cover all cloud activity, including sanctioned and unsanctioned apps, business accounts and personal accounts, browser-based access and native apps, mobile devices and desktops, user-to-cloud and cloud-to-cloud. Ensure such policies can be enforced in real time to prevent data loss and compliance violations.

Coach users on appropriate behavior
Track users who are acting outside corporate guidelines, such as sharing inappropriate content or using outdated browsers and coach them with interactive messages.

Enforce compliance regulations
Use CloudSOC to perform continuous monitoring of user activity to ensure adherence to appropriate compliance regulations, such as HIPAA. Ensure data is handled with appropriate sharing restrictions and encryption or tokenization is applied as appropriate. Generate periodic reports to demonstrate compliance and maintain visibility.

3. Mitigate Risks from attacks

Manage identities and credentials
Given that most organizations are using multiple cloud apps and services, and that users' credentials represent new threat vectors for attack, consider an identity management solution to manage credentials centrally. Identity management should be tightly integrated with the Symantec CloudSOC solution to enable effective monitoring and control of cloud app usage.

Continuously monitor cloud activity for threats
This requires sophisticated analysis of anomalous behavior to help secure new threat vectors introduced by cloud apps and services. A comprehensive CASB solution like CloudSOC enables organizations to be on the lookout for malicious attackers that may try and steal user credentials, malware that may hijack sessions, or insiders with malicious intent.

Identify and prevent malware
Malicious attackers can harness the cloud for dissemination of malware, avoiding the scrutiny of traditional security. Using Symantec CloudSOC Gateway, detect malware in the cloud early to avoid a larger problem down the road.

Implement strong incident analysis
The ongoing security life cycle is a practice that implements solutions, learns from real-world activity, and updates tools based on these learnings. Deploy strong analysis capabilities upfront to enable effective incident response and provide valuable insights that will help improve your security solution over time.

Best Practices 10

Begin periodic application usage review within the security team.

Steps:

1. Schedule monthly review meeting with security tiger team
2. Run monthly audit report one week prior to the monthly review meeting
3. Review trends:
    a. New high volume applications
    b. Unusual user behavior
    c. Applications with shrinking risk score
4. Select top 3 concerns
5. Tiger Team addresses concerns over following month
6. Repeat process

Integrate CASB with ProxySG to reduce risky traffic seen in the cloud and streamline review process

Steps:

1. Subscribe to CASB AppFeed within ProxySG
2. Through established review process, identify apps (or application attributes/actions) as block or monitor candidates, including:
    a. Non-sanctioned apps
    b. Apps with compliance risk
    c. Expensive apps (i.e. bandwidth cost, service cost)
    d. Unnecessary functions within sanctioned applications

    If an app is business critical, mark it as an exception, monitor it over time for misuse or breach, and coach users on its safe usage.
3. Assess risk/consequences of blocking (i.e. any users, important functions).
4. Perform user notifications of intent to block applications
5. Collect feedback and identify hidden risks
6. Configure new block policy (bandwidth savings = cost savings)
7. Review CASB logs to ensure block policy is properly enforced
8. Monitor employee feedback for unforeseen consequences and revise policy as necessary

Inspect and automatically remediate cloud usage to ensure compliance with HIPAA, PII, regulations with Symantec CASB Gateway

Steps:

1. Identify risk types
2. Select canned ContentIQ profile or customize to specific requirements
3. Determine appropriate customer response for potential violations (comfort page /notice)
4. Apply policy via API connection to cloud services (Securlet)
5. Establish notifications to internal SOC team
6. Sample remediations with established review process

Conclusion 11

When sanctioning cloud apps with Symantec CloudSOC Audit, collaborate closely with line-of-business owners and key stakeholder management groups (such as those dealing with medical information, IP, financial information, credit card information, or customer PII) to include them in the cloud security decision making process. This can add key process checkpoints specific to your organization to ensure that both business needs and security requirements are being considered when adopting cloud apps and services. It also provides an opportunity to extend much-needed security awareness throughout the organization.

CloudSOC Audit generates a Shadow IT Risk Assessment report to provide the critical cloud app usage information and insights needed to effectively collaborate with stakeholder management groups.

Subsequently, with the full Symantec CASB gateway solution (Audit, Detect, Protect and Investigate), as well as integrations with Symantec DLP, Endpoint, ProxySG and WSS, you can also manage Shadow Data resident within cloud apps and services to prevent data loss and oversharing of sensitive data, detect malware and risky user behavior, set usage policy, and perform post incident analysis.

CASB Glossary 12

Cloud Access Security Broker (CASB)
Security policy enforcement points that sit between cloud service users and the cloud services they are accessing. These are designed to provide visibility and control over cloud apps used organization-wide and apply policies to protect cloud data from theft, loss or over-exposure.

CloudSOC™
Symantec's Cloud Access Security Broker (CASB) solution.

CloudSOC Gateway
Symantec's real-time security gateway that enables enterprises to continuously monitor cloud traffic and apply granular policies to control user activities in the cloud.

CloudSOC Securlet™
API-based security solutions that provide advanced security functionality for popular cloud apps and services such as Office 365, Google Drive, Salesforce, Box, and Dropbox. Currently 12+ cloud apps are supported.

ContentIQ™
CloudSOC feature that dynamically classifies content and identifies compliance-related and other sensitive content.

Gatelet™
A cloud app specific signature enabling deep analysis of that app by the Symantec CloudSOC Gateway. Currently 75+ cloud apps are supported.

Audit
CloudSOC feature that finds and monitors all the cloud apps being used in an organization and highlights any risks and compliance issues these may pose. Audit currently has the ability to identify and assess 20K+ cloud apps.

Detect
CloudSOC feature that identifies threats to an organization's cloud accounts and data such as account takeovers, data destruction, and data exfiltration attempts.

Protect
CloudSOC feature that enables the creation and enforcement of data security policies in the cloud.

Investigate
CloudSOC feature that supports analysis of historical cloud activity.

StreamIQ™
CloudSOC feature that extracts granular events from real-time cloud app-traffic.

ThreatScore™
CloudSOC feature that performs continuous User Behavioral Analysis to identify and rate threats to cloud apps.

Symantec™

+1 650-527-8000

symantec.com