Ensuring secure and compliant cloud app use with Symantec

Symantec™

CASB Best Practices Guide

Cloud Access Security Broker

Ensuring secure and compliant cloud app use with Symantec

Section Page

Introduction 01

Cloud Access Security Brokers (CASBs) serve as a critical control point to ensure the secure and compliant use of cloud apps and services. Cloud service providers typically maintain a shared responsibility policy for security—they guarantee the integrity of their service infrastructure, but the customer is responsible for securing actual app usage. In addition to the growing cloud security challenges organizations face to safeguard data and protect against threats in the cloud, total volume of cloud app adoption is accelerating, with most of it being done by business units and employees without approval or security oversight from the IT organization. As a result, CASB functionality has become so critical that by 2020 it is projected that 80% of enterprises will use a CASB solution. (Gartner)

A full-function CASB that covers the entire lifecycle of cloud app security must include:

1. **Cloud App Discovery and Analysis**
   Discover, rate, select, and control access to cloud apps and services
2. **Data Governance and Protection**
   Classify, manage, protect, and control access to and sharing of sensitive cloud data
3. **Threat Detection and Incident Response**
   Detect cloud threats such as account takeovers, data loss, data destruction, malware and content oversharing, and respond to incidents and compliance violations.

While many traditional CASBs address these three basic capabilities, they do have some blind spots and limitations you should be aware of. For example, what do you do when you need to apply consistent DLP policies to data in the cloud and on-prem? What are your options for encrypting confidential data? Can you safeguard against confidential data transfer to unsanctioned cloud apps or personal cloud accounts? Can your CASB automatically identify and respond when a user account has been compromised? Does your CASB automatically classify confidential data or do you have to build a system from scratch? Effective DLP requires more than basic regex capabilities and many solutions offer only rudimentary DLP capabilities. These and other issues should be considered when selecting a CASB.

CloudSOC™

Symantec offers CloudSOC™, a CASB solution that integrates seamlessly with Symantec DLP, Endpoint Security (SEP), Secure Web Gateways (ProxySG, WSS), authentication (VIP), field-level Tokenization/Encryption (CDP), and file-level encryption (ICE). Together, these integrated solutions bridge the gaps between your CASB and existing cloud and on-prem security solutions to protect your apps and data, no matter where they or your users reside.

About this guide

This document is designed to guide organizations through the complex process of Data Governance and Protection, plus Threat Detection and Incident Response. It also specifies which Symantec CASB features and integrations can be used to facilitate the process. **To learn best practices for Cloud App Discovery and Analysis, please refer to the *Shadow IT Discovery Best Practices Guide.***

Key Challenges

- Many IT departments fail to regularly include business units and executive staff when developing a cloud strategy, identifying business-critical cloud apps in use, mitigating cloud risk, and educating cloud users.
- Many enterprises aren't aware of all of the cloud services and data in use throughout the organization. Most have 20x more apps in use than they would estimate. (see the Symantec Shadow Data Report)
- Even when cloud services are known, most enterprises cannot identify, classify, granularly control access to, and manage the secure handling of sensitive, compliance-related data in these apps.
- CASBs provide a combination of user-centric and threat-centric capabilities as well as a range of deployment options, increasing the complexity of evaluation.
- Most enterprises have no way to detect cloud threats such as malware, account compromises, data theft, and data destruction.
- Most organizations attempt to apply the same controls to all cloud data, regardless of data type, compliance requirements, or data sensitivity.
- Focusing disproportionately on the prevention of cloud data loss, account compromise, and risky user behavior, many organizations overlook the critical need for threat detection, continuous monitoring, and post-incident response.

Recommendations

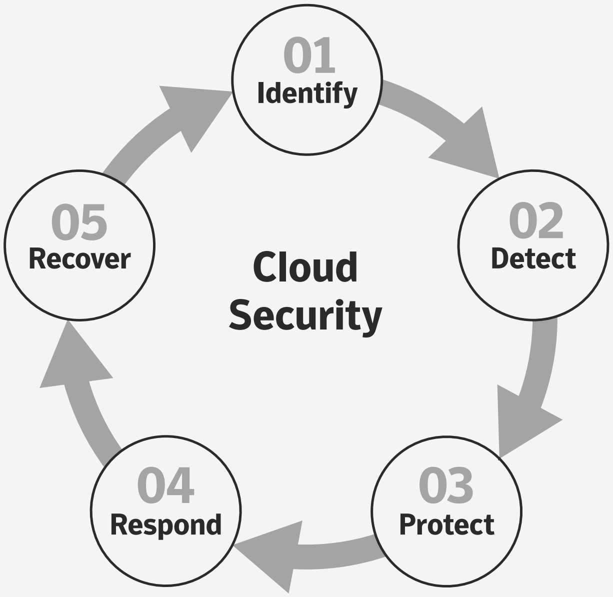
Our goal is to help organizations maximize the effectiveness of their cloud security investment by following six key guidelines:

1. Build a cloud security program aligned to both the organization's business and security requirements.
2. Integrate an authentication solution with your CASB to leverage device and behavior profiling to block risky login attempts.
3. Implement an integrated CASB solution that can discover and assess the risk of cloud apps, detect malicious activity in cloud accounts, and classify and control the data in them—no matter where the user or device resides. (For more details on cloud app discovery and risk assessment, see the *Shadow IT Discovery Best Practices Guide*)
4. Reorient the organization to take a security-first approach in the cloud and regularly include users in continual process enhancement.
5. Extend sensitive data monitoring policies and workflows to cloud-based services by integrating on-prem and cloud-based DLP.
6. When sensitive or regulated data needs to be stored and used in the cloud, use information protection techniques like encryption and tokenization to assist in compliance efforts.

Cloud Security Lifecycle 02

The cloud security lifecycle follows a series of repeatable steps that organizations can follow to drive awareness of the importance of security in the cloud with executive management and cloud users. By refining and repeating this process, organizations can begin to build this awareness. In addition, over time risky cloud 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 managing sensitive and compliance-related data, educating users on cloud data best practices, and including users as part of the solution. By alerting them to policy violations and educating them on cloud best practices, 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.



01 Identify

- Identify cloud apps
- Uncover & classify cloud data
- Identify risky data, activities, and users
- Plan cloud security strategy

02 Detect

- Monitor for policy violations
- Detect anomalous user behavior that could indicate account compromise, data destruction or data exfiltration
- Monitor/detect incidents, malware, and data loss

03 Protect

- Block non-secure apps
- Define cloud policy
- Set risk thresholds
- Communicate policy
- Enforce policy

04 Respond

- Quarantine data and users
- Encrypt and tokenize sensitive content
- Adjust login requirements when ThreatScore is elevated (MFA)
- Block downloading of sensitive content
- Remediate risky exposures in file shares
- Take appropriate action with HR or legal as necessary

05 Recover

- Investigate violations and exploits
- Revise Policy
- Educate users

Use Cases 03

Uncover and rate cloud apps

CIOs think they have 30-40 cloud apps on their network, when in reality the average organization has over 900. They need to be able to identify these apps, rate them according to their security risk, and select those that conform to the organizations' risk tolerance. For more info, refer to the *Shadow IT Discovery Best Practices Guide*.

Classify data

Compliance Officers often want to know what types of compliance-related data (PII, PCI, PHI, etc.) are being stored and shared in the cloud, and whether they are overexposed and at risk. In addition, other data types such as legal documents, engineering documents, source code, and IP need to be identified as well.

Identify over exposed data

Security Administrators need to identify which cloud data is at highest risk of leakage outside of the organization — either inadvertently due to user error, due to malicious use or hacker activity.

Extend on-prem DLP to the cloud

IT organizations with on-prem DLP often want to extend coverage to the cloud in a non-disruptive way that will enable them to use consistent dictionaries, policies, and workflows on-prem and in the cloud.

Identify risky users

CIOs often want to identify risky user behaviors such as file oversharing, data exfiltration/ destruction, and account takeovers.

Develop a cloud governance program

Effective cloud governance programs are not built in isolation. Including business units, management leadership, and compliance officers is critical to understanding the organization's cloud security, compliance, and data usage requirements, as well as understanding what types of data is most critical to the organization. Leveraging insights gathered during the data discovery and classification process, CIOs can knowledgeably lead the process of building the data governance regime.

Protect data

All CIOs need to protect the organization's data, but different methods and degrees of protection should be used to protect different types of data. Sensitive, regulated data may need to be controlled and in many cases encrypted or tokenized, depending on compliance requirements and potential impacts on app performance.

Ensure compliance & data privacy

Compliance Officers may want to continuously monitor how data is being accessed and shared by the organization and individual departments to make sure they meet compliance requirements.

Monitor cloud usage & detect threats

Security managers need to continually monitor data usage for possible policy violations, data leakage, malware attacks, and user access to unauthorized websites that could pose a risk to cloud accounts and data.

Remediate incidents

In the event that cloud accounts are compromised, files are infected with malware, or data is lost or stolen from cloud accounts, IT departments need the ability to initiate a post-event investigation to remediate the issue and to provide an audit trail.

Considerations When Defining a Cloud Security Strategy 04

You need to answer several questions as you step through the cloud app adoption process:

How can I build a Cloud Security Advisory Board? Do I need one? **(Hint? *Yes, you do!*)**

□ **Who should be included to cover the entire organization's security and business needs? Executive staff? Line of business managers? Compliance officers? End users?**

□ **What processes do I need to set up for: Selecting secure cloud apps, defining use policies, modifying policies, escalating issues, mitigating and responding to incidents, and educating users?**

What are my riskiest cloud apps and services?

□ **Do my apps conform to my organization's security requirements?**

□ **What are the business functionality and performance requirements for cloud apps identified by my users and business units?**

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

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

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

□ **Are there safer alternatives to my risky apps?**

What are the most critical data types in my organization?

□ **What types of data do my organization's business units find most valuable?**

□ **Is my organization heavily dependent on protecting PII? PCI? PHI? IP?**

□ **What are the data compliance regimes to which my organization is subject? Am I required to comply with the data regulations in the General Data Protection Regulation (GDPR)?**

□ **How much sensitive or compliance-related data are employees storing and sharing in the cloud?**

□ **What format are my documents in? Spreadsheets? Word Processing? PDFs?**

□ **Do I have compromising data in the cloud such as pornography, obscenity or files infected with malware?**

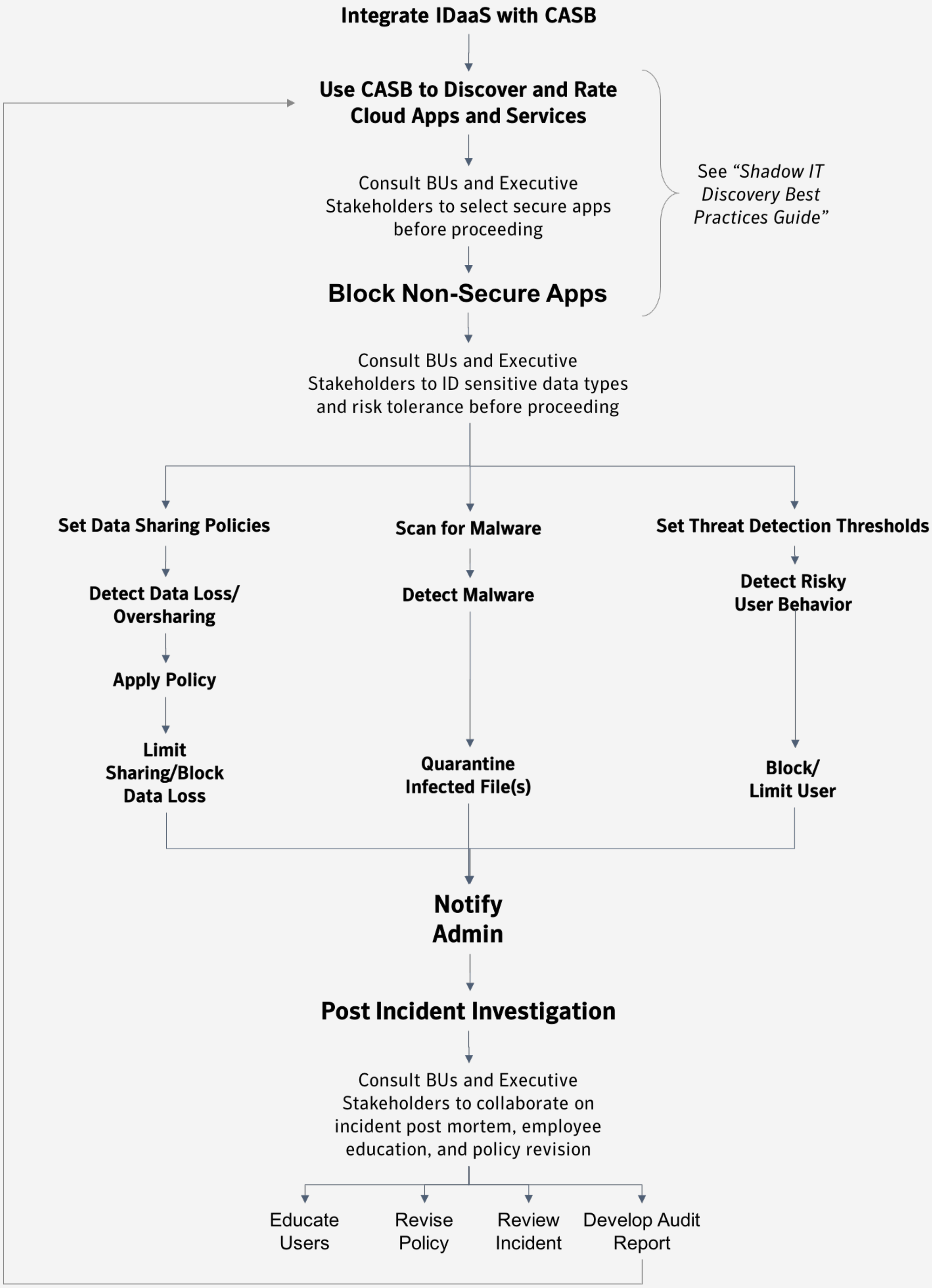
Who are my riskiest cloud users?

□ **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 Security Workflow 05



Integrate IDaaS with CASB

Use CASB to Discover and Rate Cloud Apps and Services

Consult BUs and Executive Stakeholders to select secure apps before proceeding

Block Non-Secure Apps

See *“Shadow IT Discovery Best Practices Guide”*

Consult BUs and Executive Stakeholders to ID sensitive data types and risk tolerance before proceeding

Set Data Sharing Policies

Detect Data Loss/ Oversharing

Apply Policy

Limit Sharing/Block Data Loss

Scan for Malware

Detect Malware

Quarantine Infected File(s)

Set Threat Detection Thresholds

Detect Risky User Behavior

Block/ Limit User

Notify Admin

Post Incident Investigation

Consult BUs and Executive Stakeholders to collaborate on incident post mortem, employee education, and policy revision

Educate Users

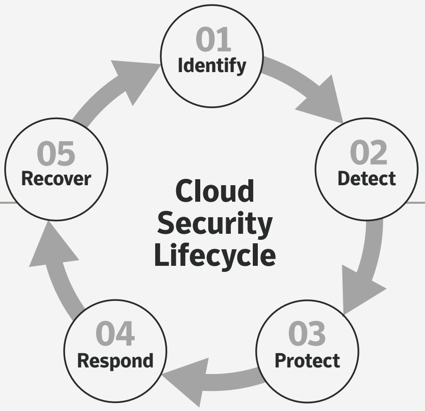
Revise Policy

Review Incident

Develop Audit Report

Cloud App Security Controls

06



Once you understand the cloud security lifecycle and workflow, you can adopt CASB and other cloud security solutions to provide full coverage for your cloud app usage.

01 Identify

CASB Audit
CASB Protect
Secure Web Gateway

02 Detect

CASB Detect

03 Protect

CASB Protect
Cloud DLP
Authentication
Encryption
Tokenization

04 Respond

Securlet Dashboard
CASB Investigate

05 Recover

CASB Investigate

Identifying and Protecting Sensitive Cloud Data

07

Adopt Adaptive Access Control

Category	Description	Mitigation Options
Manage Cloud Access	The first step in protecting cloud app usage is to integrate your CASB with an authentication service, preferably one that leverages device and behavior profiling to block risky login attempts.	Use Symantec VIP to provide secure access to sensitive data and applications anytime, anywhere, from any device. Includes risk-based intelligent authentication leveraging intelligence from CloudSOC.

Uncover and Rate Cloud Applications *(please refer to the Shadow IT Discovery Best Practices Guide for further details)*

Category	Description	Mitigation Options
Identify and Rate Cloud Apps	Use a CASB to: • uncover apps on your network • provide a security risk assessment on each app • assist in the process of determining which apps should be allowed, blocked, or replaced with safer alternatives	Use Symantec CloudSOC Audit to uncover Shadow IT from network log files and assign a Business Readiness Rating™ to thousands of apps and services. It also allows you to do a side-by-side comparison of cloud apps based on their security ratings.
Upload logfiles	Upload logfiles to CloudSOC Audit for Shadow IT Discovery.	CloudSOC's Flex Universal Log Format enables ingestion of almost any log file type (proxy, firewall, endpoint, malware, etc.) into CloudSOC Audit. Log ingestion modes include web uploads, SpanVA for continuous monitoring, SCP, SFTP, and S3
Anonymize Logfiles (optional)	Anonymize log files before uploading to Audit.	Tokenize user-identifiable information before it is sent to CloudSOC Audit using SpanVA, an optional virtual appliance.

Uncover and Rate Cloud Applications *(Cont.)* *(please refer to the Shadow IT Discovery Best Practices Guide for further details)*

Category	Description	Mitigation Options
Determine Corporate App Business Requirements	Consult with Executive stakeholders to: • Identify business-critical apps • Negotiate substitutes for non-secure apps • Look at policy exceptions for non-secure apps without alternatives	Consult with Executive stakeholders then document your policy decisions and communicate the new standards out to the organization.
Block Non-Secure Cloud Apps	Block access to cloud apps that don't meet your organization's risk tolerance.	Control/block cloud apps using Symantec SWG (ProxySG or WSS), leveraging the AppFeed from CloudSOC Audit.

Plan Data Governance Strategy

Category	Description	Mitigation Options
Determine Corporate Data Security Requirements	Prior to defining your cloud security strategy, consult with Executive stakeholders to identify: • Compliance requirements (HIPAA, PCI, FISMA, TRUSTe, Safe Harbor, GDPR, etc.) • Sensitive data types • Data loss risk tolerance, by data type	Meet with BUs, critical management leaders and users to determine what data is most critical, how it should be managed/ protected. Document your policy decisions and communicate the new standards out to the organization.
Define DLP Dictionaries	Based on discussions with stakeholders, define dictionaries for cloud DLP, i.e.: • Company Confidential • Gambling • Drugs/Medical • Obscenities • Violence	• Use the Protect app in Symantec CASB Gateway or Securlets™ to upload and manage DLP dictionaries. • Recommended: Integration of Symantec DLP with CloudSOC will enable you to apply your existing on-prem DLP dictionaries to the cloud.
Define Content Risk Security Profiles	Apply a risk severity rating to all data types that would be most damaging if leaked: • Critical • High • Medium • Low • Informational	Use Symantec CASB Gateway or Securlets to create ContentIQ™ profiles to tag critical data types by risk severity.

Conduct Shadow Data Risk Assessment

Category	Description	Mitigation Options
Classify Cloud Data	Classify data as: • Business • Health • Legal • Engineering • Design • Computing • Digital Certs. • Source Code	• Detect and classify all data using the ContentIQ function in Symantec CloudSOC Gateway or Securlets. • Leverage the already defined data types in CloudSOC ContentIQ. • Recommended: Integration of Symantec DLP and CloudSOC will enable you to use the same data classification engine on-prem and in the cloud.
Identify File Classes	Identify files as: • Word Processor • Spreadsheet • Database • Presentation • Encapsulation • Movie • Sound Raster Image • Other	• Detect and classify all data using the ContentIQ function in Symantec CloudSOC Gateway or Securlets. • Leverage the data science engine in CloudSOC ContentIQ to automatically identify sensitive data in different file types.
Identify Risk Types	Identify sensitive compliance data such as: • PII • PCI • PHI • GDPR • GLBA • External DLP • Virus/Malware • VBA Macros • FERPA	• Detect and classify sensitive data using the ContentIQ function in Symantec Securlets. • Leverage the data science engine in CloudSOC ContentIQ to automatically identify sensitive data for specific risk and compliance categories. • Recommended: when data should be blocked from cloud apps, integration of Symantec DLP and CloudSOC enables you to use the same data classification engine on-prem and in the cloud. • Recommended: when data requires additional protection in cloud apps, encrypt or tokenize all regulated information (SaaS data fields and file attachments) at rest, in motion, and during processing using Symantec Cloud Data Protection and CloudSOC file encryption.
Identify Over-exposed Sensitive Data	Categorize sensitive/risky data as: • Internally Exposed • Externally Exposed • Publicly Exposed	Use Symantec CloudSOC Gateway or Securlets with ContentIQ policies to identify which documents are overexposed.
Determine User Risk	Based on file sharing and cloud use behavior, categorize users as: • High risk • Medium risk • Low risk	Leverage CloudSOC Detect's dynamic user ThreatScore™ (1-100) to categorize users as high, medium or low risk based on their activity profile. Thresholds for each of the three categories can be customized.

Establish Data Use Policy

Category	Description	Mitigation Options
Validate Data Governance Strategy	Collaborate with Executive Management BUs, to finalize a data governance strategy.	Leverage the data from the Shadow Data Risk Assessment performed in the steps above to establish baseline requirements for data governance.
Set Cloud Data Policy with stand-alone CASB	Set policies based on: • Protecting your data from risky user behavior • Monitoring and controlling file uploads and downloads • Monitoring and controlling file sharing behavior • Monitoring and removing exposures of sensitive files • Monitoring and controlling user access and activities in Cloud services	Set granular policies using CloudSOC leveraging ContentIQ and UBA ThreatScore tracking: • ThreatScore based policies • File Transfer based policies • File Sharing based policies • Data Exposure based policies • Access Monitoring and Enforcement based policies
Alternate: Set Cloud Data Policy with integrated On-Prem DLP + CASB	The integrated DLP and CASB solution enables you to combine context, including UBA, from your CASB with Advanced Content Detection in DLP.	This functionality is available when you purchase Symantec DLP Cloud and Symantec CloudSOC CASB Gateway or Security for SaaS. It is the only CASB DLP solution where your data stays in the cloud rather than being transferred to on-prem and back to cloud via ICAP — a solution with high latency and limited functionality. Rules can be based on Six Contextual Dimensions: • User (User Threat Score, Internal/External) • Region (Country/Geo-Location of the device) • Cloud Application (Application Name/Sanctioned) • Activity (Upload/Download, Sharing) • Device Posture (Managed/Personal) • Document Meta-Data (Internal/External, File Type)
Encrypt/ Tokenize Sensitive Data **(File Level)**	Encrypt/tokenize compliance-related data at the file level, including: • PII • PCI • PCI • GLBA • CJIS	Use Symantec CloudSOC integrated with ICE to encrypt static file content in: • Office 365 OneDrive • Box Use Symantec CloudSOC integrated with SafeNet.
Encrypt/ Tokenize Sensitive Data **(Field Level)**	Encrypt/tokenize data at the field level only when required to satisfy highly stringent security requirement.	Use Symantec Cloud Data Protection (CDP) to tokenize or encrypt field level data, like PII or PHI, in SaaS applications such as Salesforce, ServiceNow, and Oracle.

Set Threat Detection Thresholds

Category	Description	Mitigation Options
Set **Threshold** Based Incident Detection Settings	Set duration (minutes) and importance of threshold-based activities (i.e., five invalid logins in 2 minutes) • Less Important • Important • Very Important • Critical	Set threshold-based detectors using the Detect app in CloudSOC Gateway or Securlets.
Set **Behavioral** Based Incident Detection Settings	Set confidence level (≥ x%) and Importance of Behavioral activities (i.e., Anomalous frequent user actions: ≥30% confidence) • Less Important • Important • Very Important • Critical	Set behavioral based detectors using the Detect app in CloudSOC Gateway or Securlets.
Set **Sequence** Based Incident Detection Settings	Create sequence based detectors: • # Steps • Duration • Importance	Set sequence based detectors using the Detect app in CloudSOC Gateway or Securlets.

Monitor Cloud Accounts for Violations & Threats

Category	Description	Mitigation Options
Respond to policy violations	Policy violation responses may include: • Email, text or ticket alert • Update file permissions • Remove shared link • Set link expiration	Set granular policies using Symantec CloudSOC or integrated ProxySG, WSS, or DLP Enforce.
Detect/Classify Risky Behavior	Classify/group threat incidents as: • Data Exfiltration • Data Destruction • Account Takeover	Use the StreamIQ™ functionality in Symantec CloudSOC Securlets or Gateway to extract granular events from real-time cloud app traffic leveraging machine learning to identify threats.
Rate Threat Incidents	Rate incidents as: • Low Risk • Medium Risk • High Risk	The Detect app will identify specific actions and their users as low, high or medium risk.
Detect/Block Malware	Identify and block: • Traditional malware	The CloudSOC Securlets and Gateway will run files through AV scanning upon onboarding and when any document is added or modified.
Export Data	Export data for offline analysis	Through CloudSOC you can readily export data for offline analysis and processing in CSV format or REST API.

Investigate Post Incident

Category	Description	Mitigation Options
Post Incident Investigation	Perform a deep dive analysis on historical cloud activity.	Use Symantec CloudSOC's Investigate to track: • Cloud services used • Risky activities & threats • High-risk users Export CloudSOC logs to your SIEM to correlate data with other systems.
Post Incident Response	Respond to incidents by: • Educating Users • Developing an audit report • Revising policy in consultation with Executive Management	Work with BUs and Executive Management to educate employees and revise policies based on the post-incident analysis.

Generate Reports

Category	Description	Mitigation Options
Create dashboards, reports and infographics	Create dashboards, reports and infographics for executive staff.	Through CloudSOC you can create dashboards with predefined and customizable widgets.
Schedule Reports	Schedule daily, weekly, monthly reports	CloudSOC enables you to schedule delivery of customized reports via email to critical stakeholders in the organization.

Next Steps 08

1. 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 the need to rewrite them, that can be managed from the Symantec DLP Enforce 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 words, perform a Shadow Data Risk Assessment). Leverage Symantec CASB 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 sharing will be restricted or given additional security protection via encryption or tokenization.

Enforce policies for sensitive data
Use 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.

2. Detect and Mitigate Threats

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. Use Symantec CloudSOC to detect malware in the cloud early to avoid a larger problem down the road.

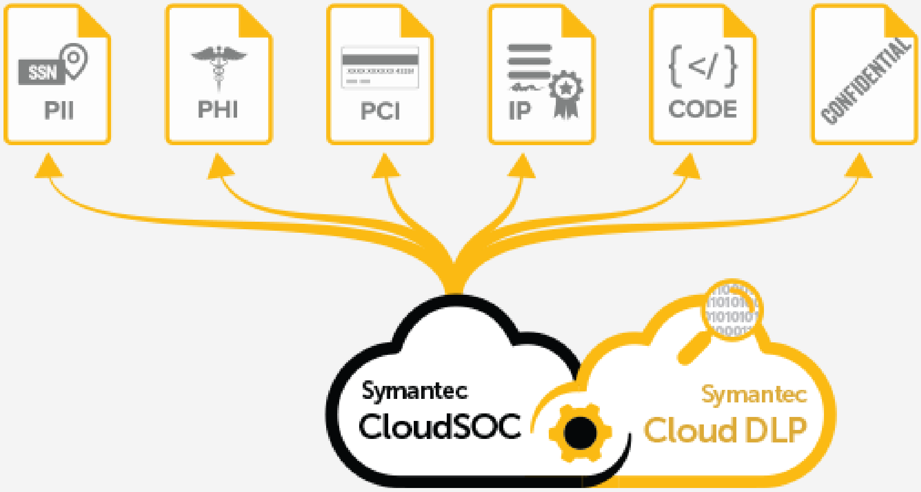
Implement strong incident analysis
The ongoing security life cycle is a practice that implements solutions, learns from real-world activity, and updates tools based on these learnings. Deploy strong analysis capabilities upfront to enable effective incident response and provide valuable insights that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

Recommended Integrations and Processes 09

Integrate CloudSOC with on-prem DLP to apply common data policies and workflows in the cloud

Steps:

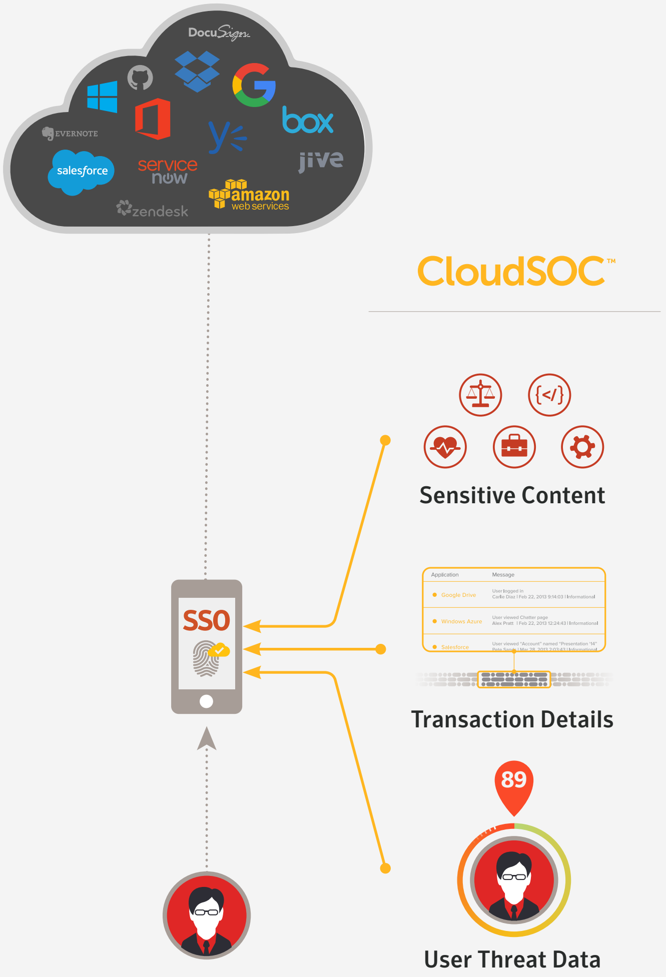
1. Symantec DLP customers subscribe to Symantec DLP cloud
2. Discover sensitive data in more than 60 cloud apps including Office 365, Box and Dropbox
3. Apply existing on-prem DLP policies and workflows to data stored and shared in cloud apps
4. Enforce DLP policies everywhere from one unified management console

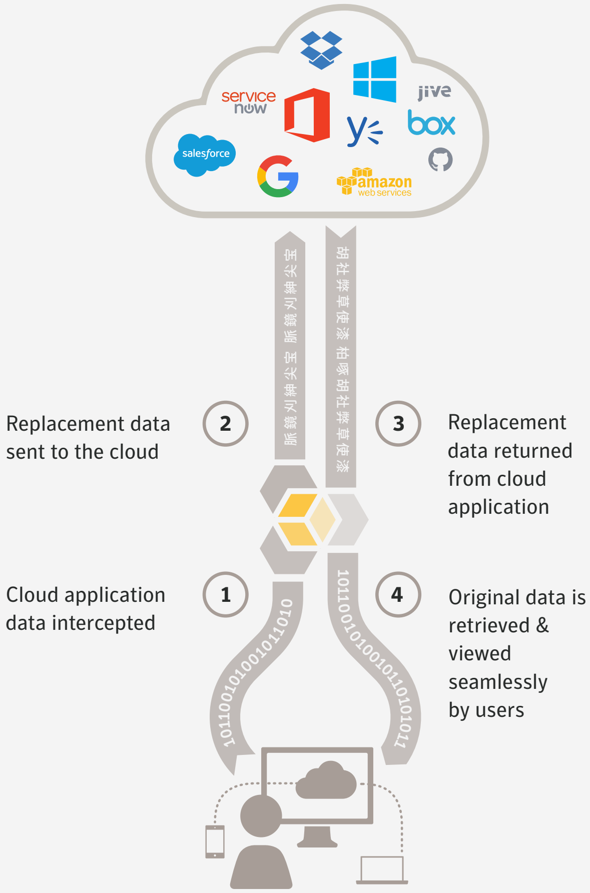


Manage cloud access by integrating CloudSOC with VIP Access Mgr & Adaptive Authentication

Steps:

1. Purchase Symantec VIP.
2. Leveraging intelligence from CloudSOC, Symantec VIP will provide secure access to sensitive data and applications anytime, anywhere, from any device using risk-based intelligent authentication.




service now
jive
box
salesforce
amazon web services
Replacement data sent to the cloud
2
3
Replacement data returned from cloud application
Cloud application data intercepted
1
4
Original data is retrieved & viewed seamlessly by users

If you have compliance policies that require it, perform field-level encryption or tokenization of business-critical and compliance-related data with Symantec Cloud Data Protection (CDP)

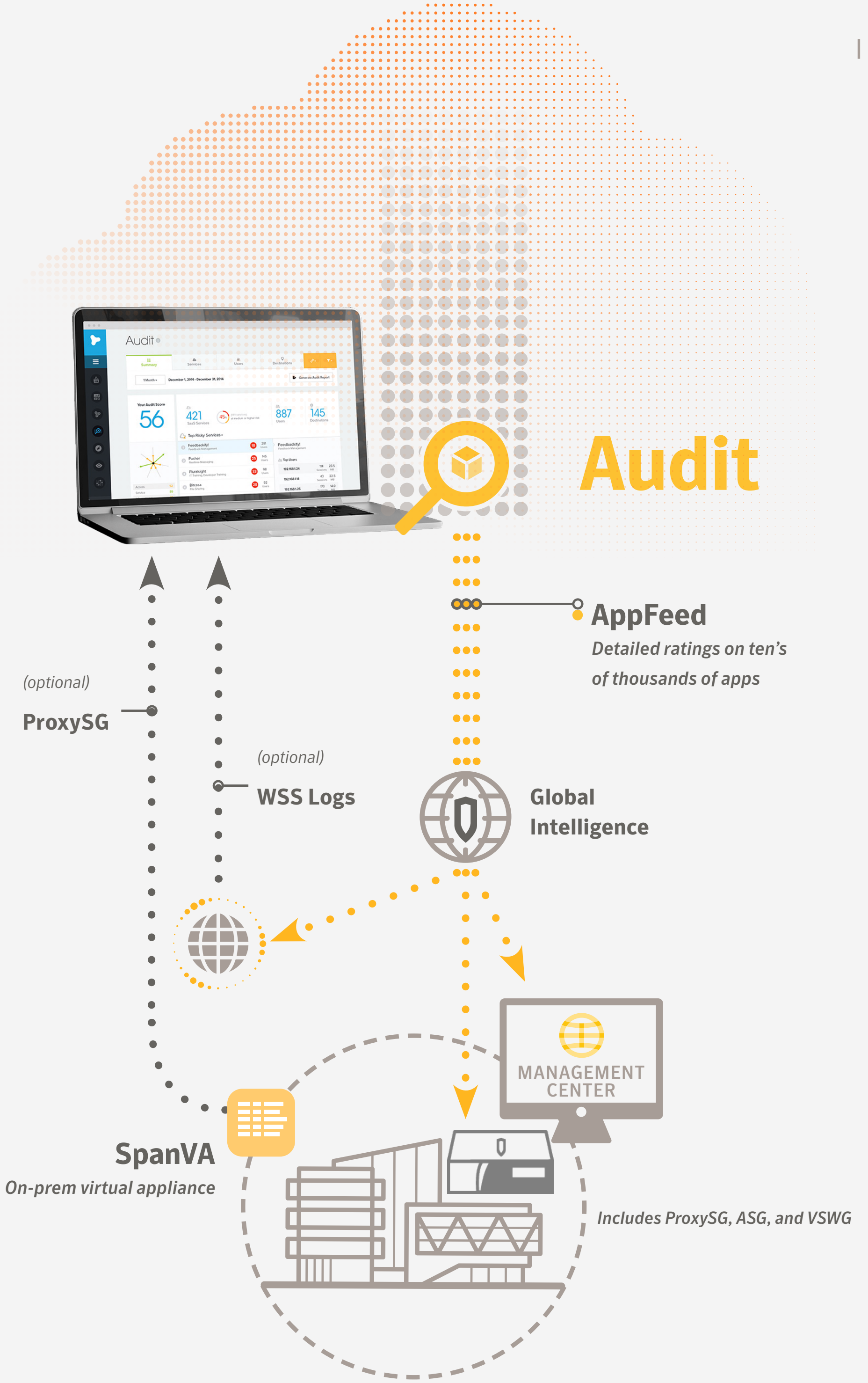
Steps:

1. Use CloudSOC to identify/classify compliance related and other sensitive data you want to tokenize/encrypt.
2. Cloud application traffic routes through CDP gateway and data protection policies are enforced (encrypted or tokenized value generated)
3. Replacement data is sent to the cloud application
4. Replacement data is retrieved from the cloud application
5. Information is brought back into the clear and presented to app user

Integrate CloudSOC with ProxySG to enforce policies based on rich cloud app data.

Steps:

1. ProxySG customers purchase the Audit AppFeed
2. Info on tens of thousands of cloud apps and services with their BRR ratings are automatically sent to the ProxySG
3. Set up policies in ProxySG based on an app's *Business Readiness Rating*, or risk attributes related to a set of apps (i.e., SOC-2 compliance, multifactor authentication)
4. Policies are enforced on all cloud traffic passing through the proxy.



Conclusion 10

When sanctioning cloud apps and adopting cloud and data usage policies, collaborating closely with line-of-business owners and key stakeholder management groups can help bring them into the cloud security decision-making process. This can add key process checkpoints specific to your organization to ensure that both business and security requirements are being considered when adopting cloud apps and services with Symantec CloudSOC. It can also be an opportunity to extend much-needed security awareness throughout the organization.

Insights provided by a Shadow IT Risk Assessment generated from Symantec CloudSOC Audit can uncover and assess both sanctioned and unsanctioned cloud apps and help in making the decision to adopt, block, or substitute those cloud apps. A Shadow Data Risk Assessment provides actionable insights into cloud data usage—information needed when collaborating with stakeholder management groups.

Subsequently, you can then secure your cloud app usage and data from any location, device, or user with a CASB solution that integrates seamlessly with your existing DLP, Endpoint, SWG, encryption, and authentication solutions, and ultimately close the gaps that would occur between a stand-alone CASB and the rest of your enterprise security.

About CloudSOC 11

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 capabilities on the 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.

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.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law, and are subject to change without notice.

+1 650-527-8000

symantec.com