Symantec Guide to Operationalizing a Cloud Governance Strategy

Symantec

Creating and Operating a Cloud Center of Excellence (CCoE)

Symantec Guide to Creating and Operating a Cloud Center of Excellence (CCoE)

Introduction 01

Gartner security industry analysts recommend the establishment of a Cloud Center of Excellence (CCoE) within every organization, represented by a cross-functional team of people responsible for developing and leading cloud strategy, governance, and best practices. The intent is to ensure cloud selections are made keeping in mind confidentiality, integrity, and availability. While Gartner and other sources offer high-level strategy ideas for organization, this guide is intended to be more tactical with real-world examples and suggestions for execution.

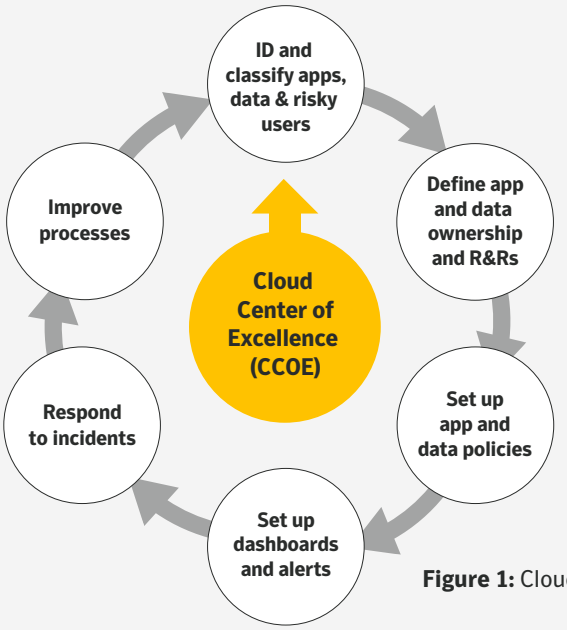


Figure 1: Cloud application governance lifecycle

This paper describes how to use CloudSOC and appropriate project management principles to set up and support your organization's CCoE which will then define, execute, and document your cloud governance plan.

CloudSOC is an indispensable tool that will help your CCoE uncover, classify, monitor, and secure your applications and documents. CloudSOC provides the intelligence to help your CCoE define policies for both current and future application adoption and usage as well as facilitating post-incident response.

While CASB is the primary solution discussed in this document and is core to your cloud application security strategy, your CCoE should be expanded over time to encompass your cloud security solutions beyond cloud apps; including web security, DLP, email security, workload protection, identity and access controls, software designed perimeter; to ensure you build an effective and integrated cloud cyber defense platform.

[1]Gartner: Developing Your SaaS Governance Framework

Step 1 – Establishing a CCoE 01

Assemble the Team

If you start small, you can make decisions quickly. Three to five people are sufficient to get your CCoE set up and running, and you can always add more as the responsibility for decision-making spreads out. It is critical to include business stakeholders from heavy app and data-using teams such as app developers, business units such as sales and marketing, sys admins, engineers, security teams, database admins – groups that are the primary culprits in generating Shadow IT. Each will have overlapping responsibility or input into everything from platform security to confidentiality, activity and data control, to regulatory and internal compliance.

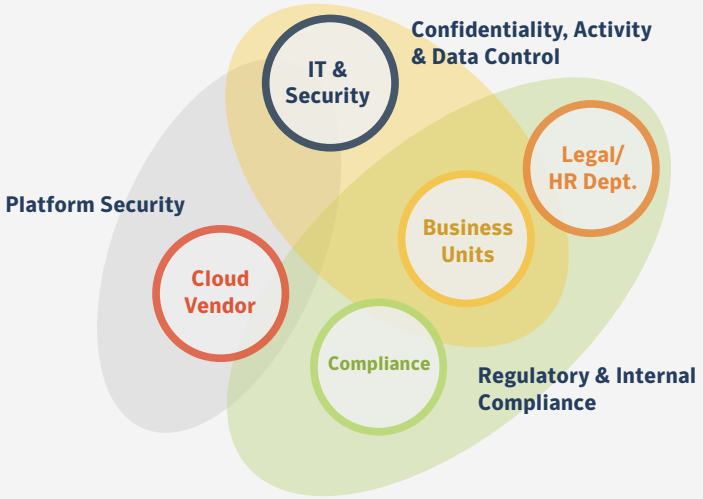


Figure 2: Overlapping responsibilities in cloud app and content ownership

What is Shadow IT?

Shadow IT is a collection of Systems, especially cloud applications, built and used within organizations without explicit organizational approval, and often without IT or Security awareness or review.

Ultimately, bringing a together a diverse group will give you a team with a broad range of perspectives on each of these areas of responsibility and lead to a more robust CCoE. This team's institutional knowledge of your existing products and processes will help inform CCoE decisions on how to create and govern the most fitting cloud best practices for your organization. Some groups to add to your CCoE over time include:

CCoE Representative	Primary Role	Example Titles
Functional departments (i.e. marketing, sales, engineering)	identify their business-critical cloud apps and the confidential content types. Educate users on policies and breaches.	CMO, CRO, VP Sales & Marketing
DevOps	Mandates sanctioned tools and repositories	VP Development, VP Engineering
HR	Decides fair internet and app usage and allowable exceptions	VP HR
Security/Legal/Data Privacy Officers	Selects security tools, investigates threats and breaches	CISO, Legal Counsel

Step 1 – Establishing a CCoE (Continued) 01

CCoE Representative	Primary Role	Example Titles
Compliance team	Ensures adherence to externally mandated regimes such as GDPR and HIPAA	Compliance Director
IT/Sys Admins	Own licensing to corporate apps, and set up log accesses, gateways, end-user administration, and help security investigate incidents	CIO, VP IT
CASB administrator (typically a member of IT or Security team)	Actively creates rules, policies, reports, and dashboards in CloudSOC that support all of the above, and reports back	SysAdmin

Table 1: Recommended individuals and groups for inclusion in your CCoE

Your CCoE is there to help find the safest way to achieve your organization's goals, not to provide a choke point of obstruction for business flow. Skeptics, who have concerns of cloud security, and champions, who advocate for cloud app usage, are both important points of view to represent for policies and baselines.

How Often Should the CCoE Meet?

The CCoE should meet frequently (weekly/biweekly) at first as you plan to get your cloud governance process up and running, then periodically (Monthly/Quarterly) to discuss system and process improvements, policy and compliance changes, and the addition of new apps, users, organizational changes, data types, etc.

Basic CloudSOC functionality should be turned on, with all settings out of the box when initiating your cloud app and data discovery, which will drive your initial CCoE meeting discussions and decisions.

What do we mean by data?

Data, as referred to in this guide, denotes informational logs ingested by CloudSOC Audit for Shadow IT discovery, as well as cloud traffic that is monitored and controlled via the CloudSOC Gateway and APIs. The term data is also used in this paper to refer to output from the CASB via logs, alerts, dashboards, and notifications.

What do we mean by content?

Your organization's documents and records, which are often referred to as data elsewhere, we'll call content for the purposes of this guide.

What do those other CloudSOC terms mean?

- When you see Securlet, think near real-time API-based security controls.
- When you see Gatelet, think inline, real-time cloud data traffic inspection and controls, as well as stand-alone cloud service that ingests proxy and firewall log files for Shadow IT discovery.

Early meeting agendas:

Your initial CCoE meeting agenda might include defining a workshop process with the following To Do list:

1. Review list of all apps identified by CloudSOC Audit through an initial Shadow IT Risk Assessment
2. Assign owners to each app, accountable for any misuse, compromise, or breach. Confirm the RACI matrix, and edit as appropriate
3. Confirm the RACI matrix (Table 2, page 7 below), and edit as appropriate
4. Where do escalations go? (Don't forget your executive sponsor!)
5. Decide how you will categorize apps – For illustration, we use Sanctioned/Official through Unsanctioned (see below for more)
6. Review at-risk confidential documents identified by CloudSOC and determine how you want to remediate exposures and control these documents going forward.
7. Establish a communication plan for changes – how are you going to inform employees about decisions?
8. Establish a communication plan for incidents – who needs to be informed and how will that communication proceed? How will you alert users to violations?

Later meeting agendas might include:

1. Review any new or changing traffic patterns or events; determine if there are new factors or cloud apps which have come into view and need ownership assigned
2. Review high-risk behaviors, decide on use policies, and communicate to users
3. Decide where to apply additional controls, such as authentication or blocking
4. Confirm data is ported out of redundant cloud apps to sanctioned apps
5. Confirm any changes in policy for personnel that need to be written, reviewed, and communicated
6. Integrate any new cloud security solutions (e.g. Email security, SWG, DLP, compliance posture, Workload Protection, etc.) into CCoE processes and documentation.
7. Create incident response templates. (More on this later.)

Executive Sponsorship

The most important part of your CCoE team is the executive sponsor. Without support and encouragement, policies can be neither officially sanctioned nor properly enforced. While they do not need to be included in all planning meetings, executives should receive regular reports on team progress as well as CloudSOC dashboard reports and infographics. Executive sponsors can either be high level members of the IT team such as the CIO or CISO, key functional leaders such as the CMO or CRO, or even the CEO – basically any leader who has organization-wide visibility and authority to help enforce policy changes.

RACI Matrix of CCoE Activities

Drawing out a RACI matrix for your team is a fine way to make sure that each initiative has all the support and input it needs for rolling out new cloud apps and putting in controls over the unofficial ones.

Role	Review App Lists	Determine App Ownership	Determine Content Guidelines	Formulate Policies	Create Policies and Reporting	Respond to Incidents (Technical)	Respond
Functional Manager	C	R	R	C	C	C	R
IT/Security Manager	A	A	A	A	C	R	C
HR/Legal/ Compliance	C	C	R	C	A	I	R
DevOps/Eng	C	R	R	C	C	C	I
CASB Admin	R	I	I	R	R	R	I
Executive Sponsor	I	I	I	C	I	I	A

Table 2: Sample RACI matrix for CCoE duties

Compliance

With the proliferation of new compliance policies and governance, it is important for the CCoE to have an open line in to your audit or compliance team to help you identify potential data and applications which need to be addressed as a priority. Data and compliance stakeholders will have a larger role in Step 3 - Data and Content Classification. (I.e. if your organization operates in or holds E.U. citizen data, GDPR compliance will be a concern, so you will need Data Protection and Compliance Officers' involvement with your CCoE both to inform and alert.)

RACI is a methodology for visually expressing the roles on a team to achieve its goals by function.

R = Responsible
A = Accountable
C = Consulted
I = Informed

Some of the most common and critical compliance guidelines that you might need to consider as part of your CCoE planning, depending on applicability, include:

- GDPR – General Data Protection Regulation
- CCPA – California Consumer Privacy Act
- HIPAA – Health Insurance Portability and Accountability Act
- PII – Personally identifiable information
- PCI – Payment Card Information
- FISMA – Federal Information Security Management Act
- FedRAMP – Federal Risk and Authorization Management Program

Step 2 – Planning and Scoping Cloud Applications

You can't manage what you can't see. While you plan for trusted services and service migrations, it's important to first uncover, classify and apply policy to the unknown services in use by your employees. While this is possible as a manual operation, CloudSOC helps automate and control the process.

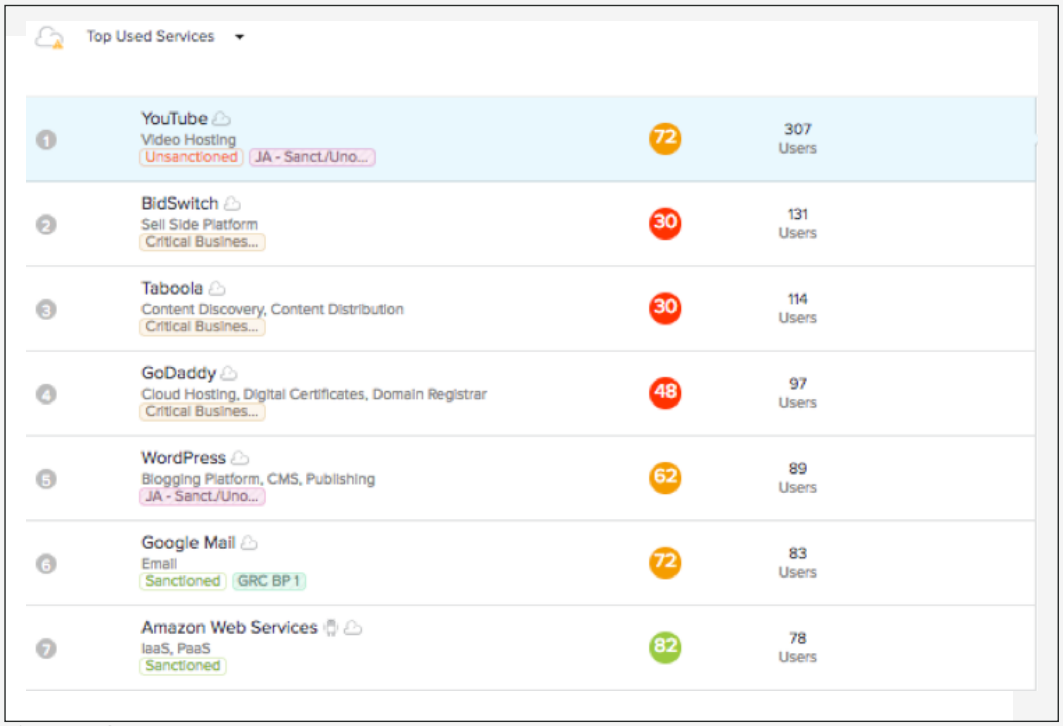


Figure 3: Sample top used apps with BRR Ratings

Classifying Apps

Your CCOE should use application intelligence from CloudSOC Audit to classify apps into 4 categories:

- Sanctioned/official services (business critical, typically have a business readiness rating (BRR) of 70 or above)
- Untrusted services (non-secure, redundant, or negatively impact productivity)
- Provisionally sanctioned services (unsecured but business-critical, no secure alternatives exist)
- Sanctioned/unofficial services (non-business apps that can be sanctioned, but only if the cost is negligible and use does not negatively impact productivity).

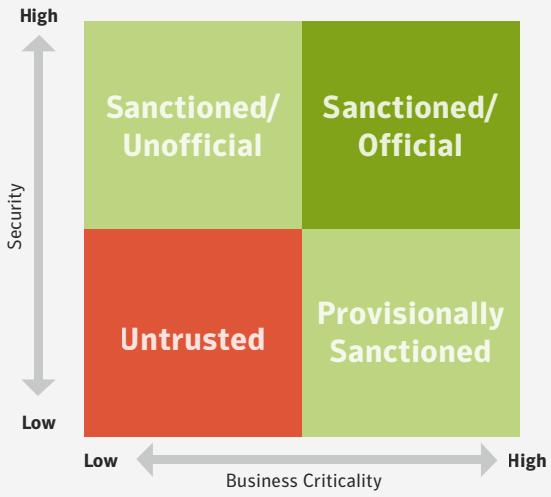


Figure 4: When to sanction a cloud app

Classifying Applications

Creating a worksheet can be helpful to organize your business application classifications. Use the BRR of all similar apps to find opportunities to reduce applications and cost – especially for cross-department collaboration tools such as project management, release controls, and change requests. Don't forget to include mobile applications!

App categorization is very useful in both list and graphical form, as shown in this sample table:

App List	Sanctioned/ Official	Sanctioned/ Unofficial	Provisionally Sanctioned	Untrusted	Redundant
App 1	X				
App 2		X		X	
App 3					X, prefer App 1
App 4, etc.			X		

Table 3: Sample App Categorization Worksheet

In all probability you have hundreds if not thousands of apps running on your network. Rather than trying to classify and control them all at once, which can be a daunting task, start with the top 25-50 apps that have the most users, as the vast majority of your corporate documents are likely being stored and shared through these.

Planning for Sanctioned/Official Apps

How is your CCoE going to determine what sanctioned or trusted services mean? You should first start with considering the vendor's app platform security. Most cloud apps come with documented security and privacy statements, and many have a market reputation as secure. Generally, the larger cloud service providers adhere to a shared responsibility model of security, where the provider agrees to provide a secure infrastructure that prevents account access without authorized account access credentials.

These cloud vendors do not, however, take responsibility for preventing accidental or malicious misuse of your company's user accounts, and often do not secure the files being stored and shared against data leakage.

This responsibility falls to your CCoE, and the cloud security products you use to enable governance and controls.

To complicating this part of the practice, every cloud customer has different security requirements, and therefore may have a different definition of a sanctioned or trusted app. While your organization may require app vendors to support MFA or encryption, for example, other organizations might not.

CloudSOC helps your CCoE define a Business Readiness Rating (BRR) customized to your organizations unique security requirements by adjusting the importance of specific security attributes that go into calculating the BRR.

Your CCoE, then, when selecting sanctioned/official apps, must fully understand each app's security posture, as well as your organization's security requirements.

Leveraging BRR generated for each app by CloudSOC Audit, your CCoE can more quickly and fully vet apps for sanctioned use. Note that on a scale of 1-100 a BRR above 70 typically denotes a trusted service.

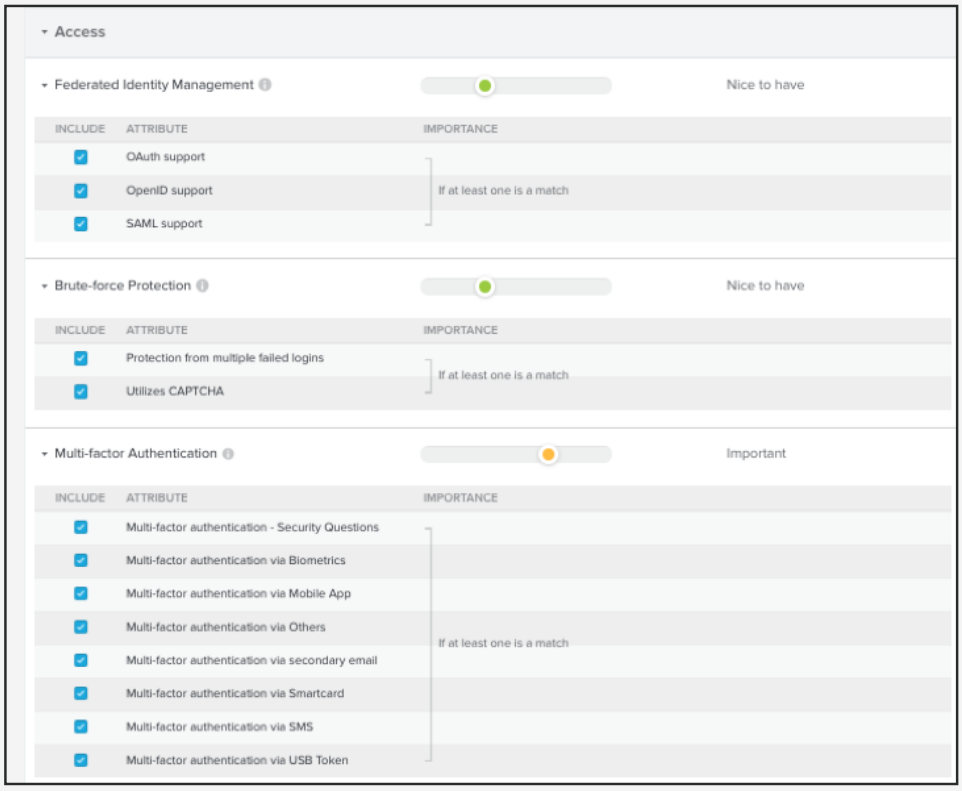


Figure 5: Sample of customizable attribute importance levels in CloudSOC

Sanctioned/official does not mean that you sanction it for use and then forget it. As with all apps, a designated owner, as we will discuss later, needs to be assigned to these apps and they will be responsible for any employee follow up, education, or reprimands that need to take place post incident. You will also need to periodically reevaluate apps as their security posture may change or even more secure alternatives may emerge.

Planning for Provisionally Sanctioned Apps

There may be instances where an application is provisionally sanctioned; e.g. negotiated or sanctioned because it is business critical, but is not 100 percent trusted or secure (having a BRR rating in CloudSOC Audit below 70) and for which there are no secure alternatives. The ability to compare apps side-by side is a powerful tool for identifying whether there are secure alternative apps with similar functionality:

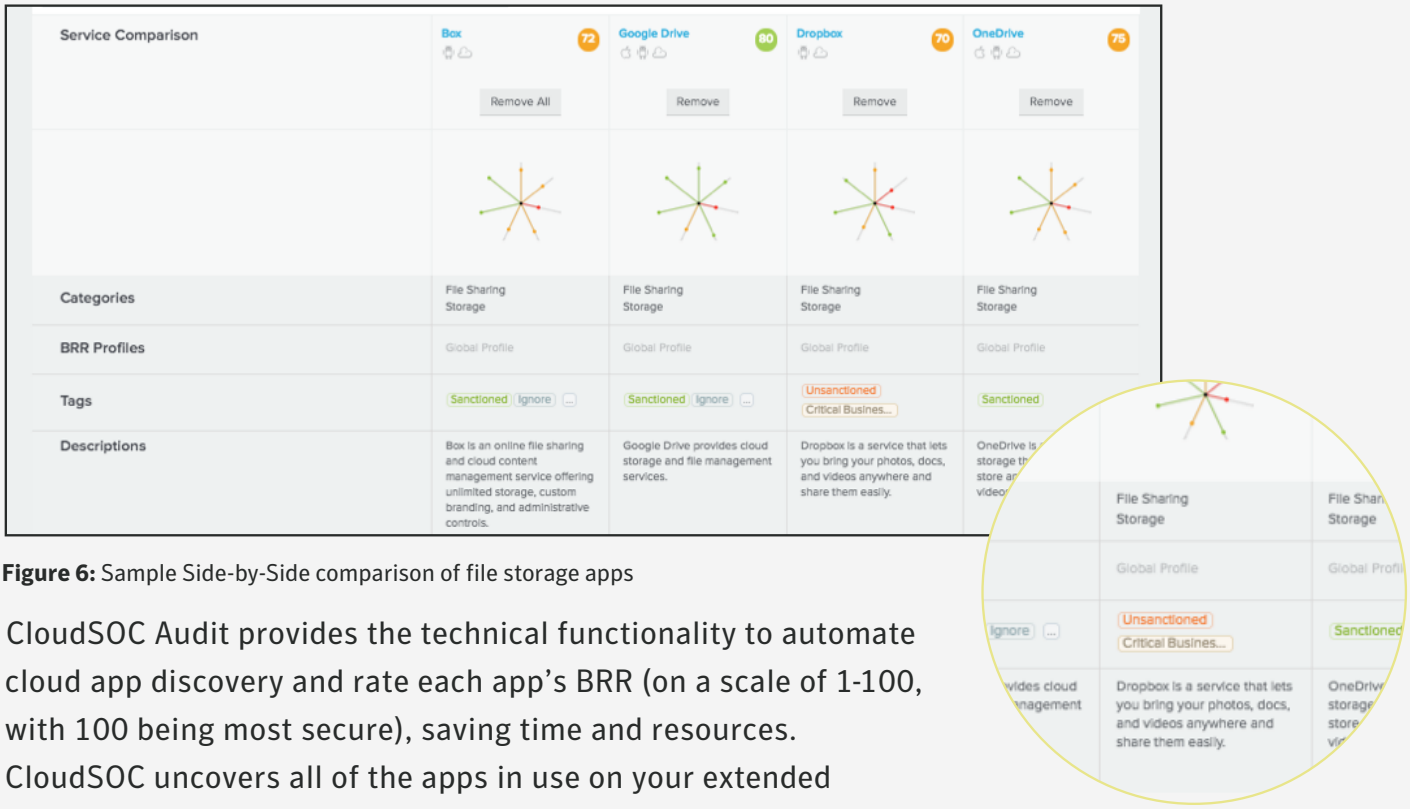


Figure 6: Sample Side-by-Side comparison of file storage apps

CloudSOC Audit provides the technical functionality to automate cloud app discovery and rate each app's BRR (on a scale of 1-100, with 100 being most secure), saving time and resources. CloudSOC uncovers all of the apps in use on your extended network, whether sanctioned or unsanctioned, and help inform CCoE decisions on cloud app and content usage.

Controlling these provisional apps does not mean simply blocking them as you would do with unsanctioned apps. Your cloud governance planning needs to consider this scenario especially carefully when reviewing what content should be shared via the app, and then when developing CloudSOC DLP policies which restrict access, sharing, and use of that content without impeding business productivity.

Allowing Sanctioned/Unofficial Apps

Most organizations have a large number of non-business critical apps running on their network. These run the gamut from niche business apps used by small groups or individuals, such as design apps, to consumer apps that employees may be using to do personal banking or shopping. While these apps must follow the same security requirements as sanctioned/official apps (with a BRR above 70), it will be incumbent upon the functional teams and HR to determine if these apps are appropriate for the company (i.e. no drugs, sex or violence) or are potentially a distraction or detrimental to employee productivity. This is where human judgment rather than technology plays the critical role.

Policies designed to control these types of apps should focus on secure access and use. However, it can be more important to focus on optimizing business productivity, such as restricting them from being used during business hours from company owned devices, than setting policies from your proxy.

Planning for Untrusted Apps

In most enterprises, there are hundreds (if not thousands) of untrusted, non-secure apps which don't guarantee the security of their infrastructures or don't have critical security features that your organization requires. These basic security vulnerabilities can be a lack of multi-factor authentication (MFA) to insecure logins and pose an extreme risk to users and data.

Of course, a straightforward solution already exists, especially for apps with an unacceptably low BRR rating – simply block employees from using such insecure services, especially as there are typically alternative services with better security that provide the same functionality. This is why it's important to identify non-secure apps which are being accessed, block them, and then replace them with comparable secure services.

In the event that you need to automatically block untrusted applications, you should do so through applying firewall rules or through integration with Symantec ProxySG or Web Security Services, which allow you to set policies from within the Secure Web Gateway (SWG) dashboard.

Alternatively you can set controls using the CloudSOC CASB Gateway by creating a custom Gatelet in Options on the cloud app detail page in audit.

Read the Symantec Web Security Service (WSS) Datasheet

Read the Symantec ProxySG Datasheet

Planning for No User Activity

As you review, categorize, allow and discard different cloud apps, there is an opportunity to review usage and user licenses. The CloudSOC administrator can review users which have zero activity in CloudSOC Detect. Ask the following: Is there an opportunity to remove users which have left the company, or are no longer in the covered work group? Do those cloud app licenses need to be reassigned to an active user? Are all the licensed applications still being used?

The CCoE can make recommendations for changes in licensing and volume to IT, which can save valuable resources and reduce expenditure.

App Ownership & Inventory

Every sanctioned app, once uncovered and classified as above, needs to have a designated owner who accepts the risks and consequences of its use – typically either IT or a business unit manager or department head who pays for the service. Any usage policy violation or data breach will ultimately fall to this owner.

At the conclusion of your initial app planning and scoping process, an official app inventory should be documented and registered with the IT team, which should include:

- App name
- App owner(s)
- Data type/sensitivity/compliance considerations
- App contract details
- Details on the app risk assessment and adoption process.

This will be a living document, which must be updated regularly as owners and compliance regimes change, applications are added or deleted, or risk scores and usage patterns change dramatically.

Keep in mind that application owners need to be:

- Expert in their business group on tools and usage
- Aware of the duties and activities of their team - all through the business processes
- Blessed by their management structure to represent the needs of the team
- Collaborative - they need to know how team activities meld with other teams in terms of conflicting business drivers
- Able to keep the high-level organization’s cloud security governance in mind
- Capable and willing to add to the body of knowledge/documentation for the CCoE

Step 3 – Planning for Data and Content Classification

Like the discussion above about the need to audit all cloud applications to help ensure your CCoE makes informed app security decisions, best practices dictate that companies and departments should also take the time to determine the confidentiality and data classification of their content so they can make smart data security decisions. This is, again, a time-consuming and ongoing project that will be always be in motion, as new content and files are constantly being created.

CloudSOC Gateway and Securlets provide the technical functionality to automate and speed up much of this classification, both through out-of-the-box settings as well creating the option for customization.

ContentIQ™ is the cloud-based Data Loss Prevention (DLP) system for CloudSOC. It scans documents hosted in a cloud service to classify their contents, determines if there are compliance violations, and runs custom content searches. ContentIQ can scan all common file formats and comes pre-configured to identify risk types relating to government and industry regulations on privacy and confidentiality.

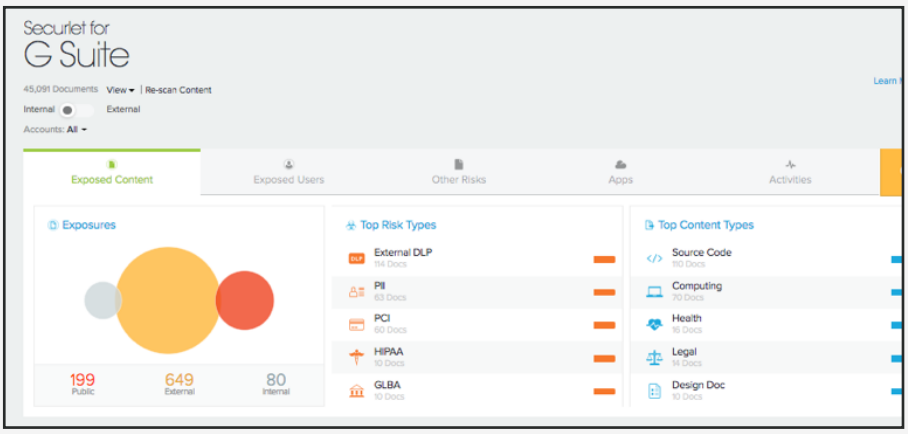


Figure 6: Detail of risks and potential exposures for Google Suite apps

For content without governance and compliance restrictions, the classification ownership resides with the data owner or creator. However, the CCoE can and should offer guidance for data and content owners in terms of how confidential or controlled the content should be both for the organization and for the customers.

If these discussions lead to the need to customize content not currently found under one of these predefined content types above, you can create a ContentIQ profile to customize alerting on content particular to your CCOE's needs.

For FERPA, GLBA, GDPR, HIPAA, PCI, and Personally Identifiable Information (PII), standard settings and queries already exist in CloudSOC. CloudSOC also checks for malware and viruses which indicate infection at an endpoint.

Once documents are classified, it can be valuable to create a table summarizing general rules for handling them. (See Table 4, next page.)

Document Type	Business Criticality	Stored in	Compliance Applies	Primary Owners
PII	High	SFDC, GSuite	Y	Sales/Marketing
PCI	High	SFDC, Zuora	Y	Accounting
PHI	NA	NA	NA	NA
Source Code	High	GDrive	N	Engineering
Computing	Medium	GDrive	N	Eng. & IT

Table 4: Tracking table created to show documents by type in GSuite and associated apps

If you are a current Symantec DLP customer and have already thought through your data protection policies, why expend precious CCoE time and effort rebuilding them in CloudSOC? By integrating Symantec DLP with CloudSOC you can extend your existing on-prem DLP policies into the cloud. Your current DLP/on-prem policies, dictionaries, and mitigation workflows can be automatically shared with CloudSOC to protect your data stored and shared through cloud apps.

Read the Symantec CloudSOC + DLP Integration Solution Guide

Read the Symantec DLP Datasheet

CloudSOC with Symantec DLP integration features:

1. **API vs. ICAP integration**
   a) Symantec DLP integrates with CloudSOC via a native RESTful API. This allows established policies from DLP to extend to content moved and stored in cloud apps. With the CloudSOC + DLP integration, your existing policies can be applied to a specific app, as well as adding rules and exceptions based on context.
   b) Policies can be different for each application. Box, Dropbox, and Microsoft O365 policies can all be unique as they each have different requirements. With API, you get context-based, granular enforcement options that ICAP cannot provide.
   c) Symantec DLP offers a cloud inspector with this integration, with local policies available for enforcement - unlike via ICAP where data must be inspected on premises.
   d) Symantec DLP Enforce has a section specific to cloud data within the incidents tab. You can see specific incident data for Data-in-Motion and Data-at-Rest both.
   e) When looking at incident data the more information and context that can be provided to the remediation team, the better. The User, File, Exposure, Response, and specific site information is being sent from CloudSOC to DLP to populate within the incident.

2. **Detection**
   a. Advanced DLP technologies including image recognition, vectored machine learning, described content matching and more, are all robust detection technologies which can be applied to data in the cloud.
   b. With the custom data identifier technology built into DLP, you can look at the regular expressions, then add/remove/modify existing to improve accuracy and lower false positives.
3. **Workflow**
   a. Existing workflows built into the DLP system can govern cloud data with easy management from a singular location.
   b. With the DLP/CloudSOC integration you can apply specific workflow rules and conditions based specifically on cloud apps.
   c. All incidents within the Symantec DLP console look the same (cloud or on-prem) so you don't have to retrain incident handlers on a new solution.
   d. Policy is stored in a single location, reporting is from a single location, and the response can be handled from a single location

Data Controls and Monitoring

Data and content can go astray in multiple ways. There is always accidental leakage, for example someone uploading a document that violates prescribed use. There are also bad actors and compromised accounts maliciously trying to exfiltrate data. No matter the motivation of the user/actor, the rules and policies in play should be shaped to control access, identify high-risk behavior, and make sure that data security policies are enforced.

Policies, controls, thresholds, and exceptions will help you determine the appropriate response – by content type, by application, and many other factors. (See Basic Policy Examples in Step 4.)

Keeping Your Content Safe

CloudSOC can show text excerpts of files which match ContentIQ profiles. These excerpts show you the actual content that matched the profile, making it easier to verify policy violations and take effective action to mitigate. To ensure the security of your sensitive information contained in the excerpts, these are stored on an Amazon Web Services S3 account you own and control. The data is accessed by CloudSOC and presented as excerpts but is never logged or saved elsewhere. You can revoke CloudSOC's access to this data at any time. See ContentIQ Violations in Figure 11 for a visual example.

Step 4 – Define Data Policies and Exceptions

What can a policy do?

Policies create automated security response and enforce compliance with process and guidelines to reinforce governing rules and principles. CloudSOC sits either between the user and the cloud application vendors (Gatelets) or as an API (Securlet) to monitor activity and enforce threshold, risk, and content-level rules based on all the contextual factors that make up a cloud transaction.

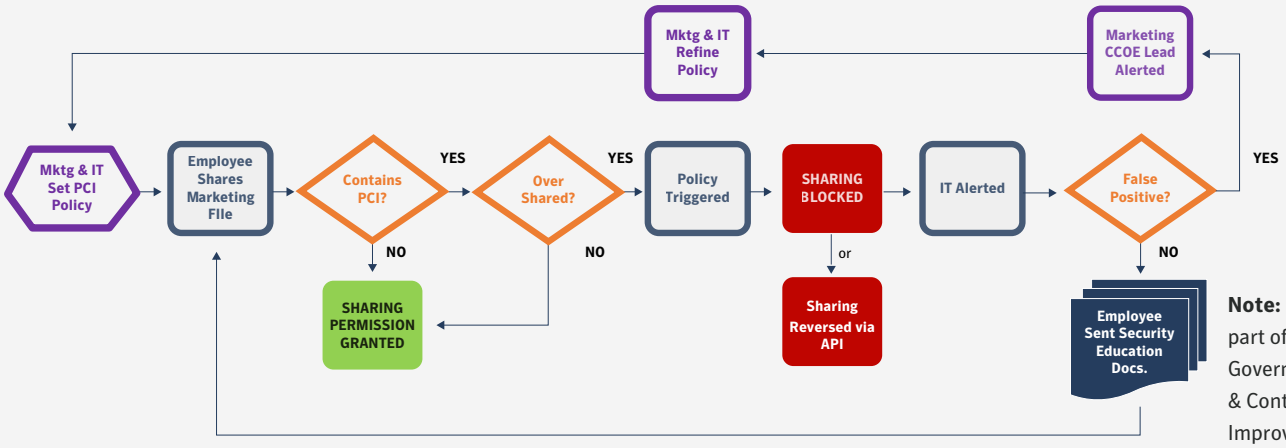


Figure 8: Example PCI policy and response flow.

Prior to building policies in CloudSOC, it can be valuable to create a table defining the policies in advance:

Data Type	Cloud Service	Transfer type	Users/ Groups	Location	Device Type	Require 2FA?	Encrypt?	Block?	Alert	Response Message
PII	SFDC, GSuite	Download/ upload	All	Europe	All	Y	Y	Y	Txt: 555-555-5555	GDPR Compliance
PCI	SFDC, Zuora	Download/ upload	All	All	All	Y	Y	N	AcctVP@ company. com	PCI Compliance
PHI	NA	NA	NA	NA	NA	NA		NA	NA	
Source Code	GDrive	Download	All	All	Unmanaged	N	N	Y	EngVP@ company. com	IP Warning
Computing	GDrive	Download	ALL	US	Managed	N	N	Y	ITDir@ company. com	IP Warning

Table 5: Sample data transfer policy planning spreadsheet

You will want to replicate the spreadsheet above, with modifications to the 3rd column from the left, for file sharing, data exposure, user ThreatScore, and Access enforcement/monitoring based policies.

Building polices help you do things like:

- Detect classified content in motion or at rest in apps
- See and control usage of applications according to the preferred, trusted, and sanctioned lists
- Describe that action – was it an upload or download? A share via URL? Preview?
- Recognize and enforce different policies; for instance, the same doc being shared via a Trusted App vs Sanctioned App – do you need to add a second level of Multi-Factor Authentication?
- Integrate with the Active Directory to customize application use and controls by user, group, etc.
- Decrypt SSL to understand the transactions for forward proxy

Basic Policy Examples

1. **Activity or App Policy Blocking**
   a. No one visits Hulu or Netflix at work – or
   b. Employees can surf the sites, but streaming media is throttled and disallowed
   c. Alert on inactive users
2. **Data Movement Policies and Blocking**
   a. Downloads are okay, but uploads to unsanctioned Apps are not
   b. Even downloads are not okay
   c. Certain content is allowed, but needs to be checked
   d. Data needs encryption while in movement, or at rest in the cloud
   e. Data moved to a sanctioned but untrusted app needs a second MFA step
   f. Throttling uploads/downloads by size
3. **Basic Threshold Policies**
   a. No more than 5 failed login attempts (Prevent brute force attacks)
   b. No more than five encrypted files to be uploaded
   c. No more than two simultaneous logins from different physical locations
4. User ThreatScore Policies
   a. User ThreatScore abruptly jumps above a threshold - like 85
   b. Unshare documents uploaded which contain malware or secure content

Beyond Basics - A Layered Policy Example: “Hooray!”

A semi-imaginary organization we’ll call “Hooray!” creates marketing content. Hooray develops high-end animation for motion pictures and commercials. Hooray uses G Suite and email to store and collaborate on artists’ creations. While Hooray could allow G Suite and Gmail but block everything else at the perimeter, it’s not an effective strategy because their artists could upload – either inadvertently or intentionally – proprietary content to personal versions of Google Drive or another file-sharing app. Moreover, Hooray wants to allow its users to access and download files and images from other Cloud Storage and Collaboration services without being concerned about data leakage.

Hooray creates a policy that identifies its corporate version of G Suite and mail, and allows content upload to that. For other (personal) versions of Google Drive, as well as other Cloud Storage services, the organization enforces a “no upload” policy while allowing “view,” “edit,” and “download” from those services.

Step 5 – Tracking and Managing Human Behavior

When we talk about bad behavior it includes multiple scenarios. Consider the following two categories of human misuse in the Cloud:

Accidental Misuse

- Employee uses an unsanctioned or forbidden cloud application for convenience or 'work-around' the limits of standard corporate applications
- Employee violates best practices for PCI, GDPR, or other IP information by uploading confidential files
- Employee mails files to themselves for home or remote work against policy or uploads files to a personal Google or O365 account.

Malicious Behavior

- Disgruntled employee shares information to an external cloud account, or uploads into a public sharing location
- Corporate credentials of an employee have been compromised, and an external hacker is using them to exfiltrate data
- An employee's online credentials of a cloud application have been compromised by a third party, allowing malicious viewing, downloading, sharing of confidential data

Whether accidental or malicious, employees can divulge or expose private information in the Cloud.
Some applications have vulnerabilities in their authentication or authorization schemas which can be exploited by external hackers. CloudSOC examines user behavior in the cloud, both from on-premise locations, mobile, or remote, to create a picture and audit trail illustrating what data is being accessed and shared, and by whom. Usage policies are critical to securing your logins, apps and data in the cloud.

Figure 9: Sample High-Risk Employee Threat Tree with a 99 ThreatScore

Within the CloudSOC Detect module, you can quickly identify high-risk users and examine the behaviors that defined that high-risk score.

In the threat tree you can dig further into the source of this risky behavior by clicking on any red circle to investigate, for example the Invalid Login 'branch'. Here, the user may have become compromised through a Brute Force attack (next page). In response, the credentials may need to be revoked, or at least have a password reset.

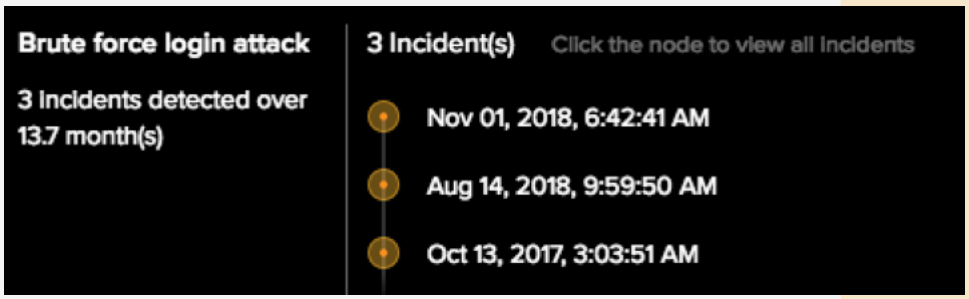


Figure 10: Example of the dates and times of a Brute force login attack

CloudSOC's machine learning reviews peer groups against individual behavior profiles, looking for abnormal behavior and elevating ThreatScores which can trigger a policy to block or quarantine content or users alike. Events like this brute force attack can be exported into your SIEM for correlation against network activity.

Data in Context of User Risk

ContentIQ can automatically classify data with highly accurate machine learning engines. These are fed by classifications of 1000+ file formats, and tens of thousands of keywords in predefined dictionaries plus PII data elements for over 50 countries. These include high-level classes such as "business", "computing", and "legal", but also include more challenging classifications such as engineering and design documents, as well as regulatory violations such as HIPAA, GLBA, PII, etc. These classifications are based on a combination of content analysis with adaptive learning and computational linguistics.

The content of the data directly applies to the ThreatScore of a user, as the movement of sensitive data is a direct input to risk calculations.

When a user creates or uploads a document, ContentIQ immediately scans the document to assess its contents. Whenever a user modifies the document, ContentIQ automatically re-scans it. If a user attempts to download or share the document, ContentIQ information about it is made available to Protect, which can alert your information security team, or automatically block the action if the document contains sensitive information.

In summary, CloudSOC tracks content identified by ContentIQ, so you can track where that content is kept in your cloud apps.

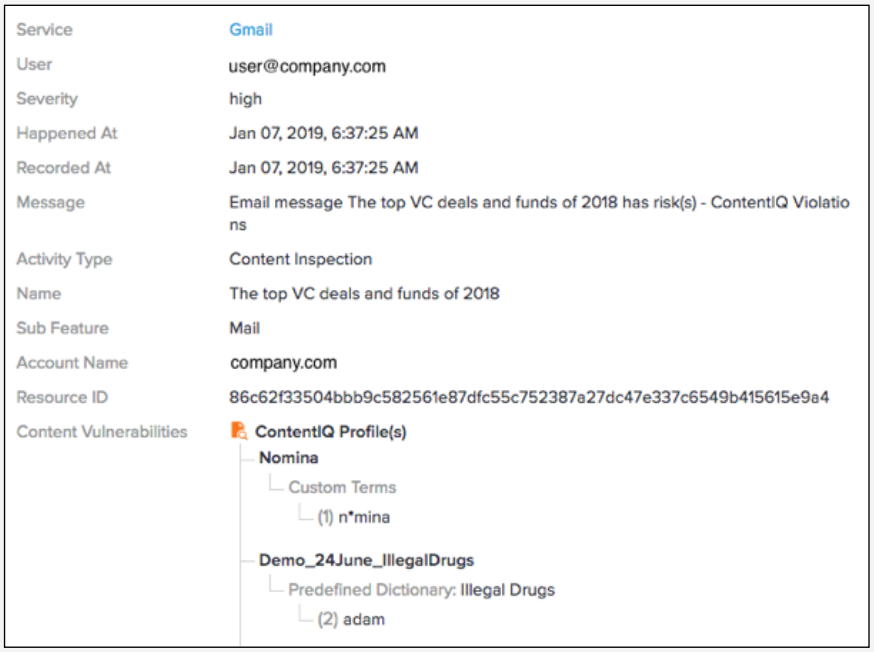


Figure 11: Sample CloudSOC Investigate screenshot of a ContentIQ violation

Decision Making for Policies

You now have information about the cloud applications and services in use, the data and content types, and can construct rules for best practices in usage for your organization. Your CCoE team as a group needs to bring expertise to the table in terms of answering the following questions:

- Who is the person who can make a decision that a user behavior is appropriate, acceptable, and low risk?
- Who can decide when to block versus simply note activity?
- How can these decisions be changed if they are wrong or block major productivity?
- Who needs to be notified if an incident occurs?
- What kind of follow up – education, HR action, correction of policy – will be considered?
- What is the escalation chain for issues, if one of the CCoE members is not available? Where does the buck stop?

The CCoE may need to enforce policies in a way that involves a "base" policy (applies to everyone) and one or more "exception" policies based on user identities, groups, devices, or a host of other contextual factors. These layered policies can work in tandem to create an "else-if" logic to control cloud access, activities, and data in a granular manner. You can train ContentIQ to recognize your organization's words, content, or document types by providing sample documents, which become part of the data element lists scanned for by CloudSOC.

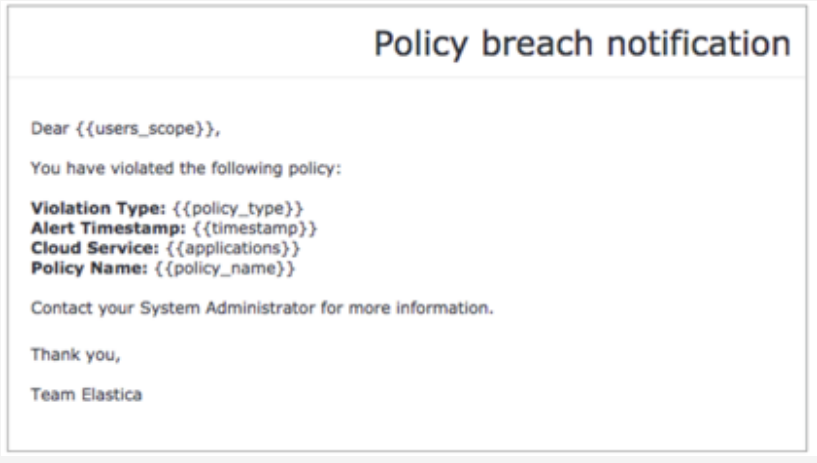
Step 6 – Alerts and Communications

Communications Planning

Once you've defined your policies it's best to set up guidelines for how your CASB will support reports and alerting, and to whom the alerts and reports will go. If you can establish your baseline, define 'normal' and accepted use early, you can very quickly set up a regular cadence of reporting and communicating out the findings of your CASB solution.

User Response Messages

User response messages are responses that you can customize to alert cloud app users to potential policy violations. These can either be simple alerts to the admin or CCoE members, or can include educational.


Policy breach notification

Dear {{users_scope}},

You have violated the following policy:

Violation Type: {{policy_type}}
Alert Timestamp: {{timestamp}}
Cloud Service: {{applications}}
Policy Name: {{policy_name}}

Contact your System Administrator for more information.

Thank you,

Team Elastica

Figure 12: Sample Violation Alert Email to Cloud App User

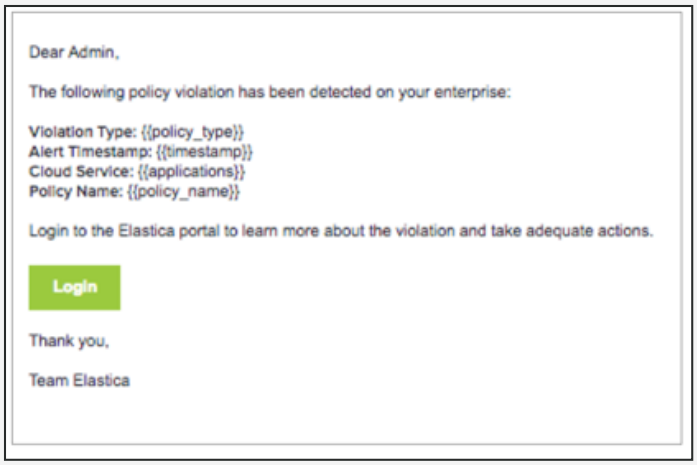


Figure 13: Sample Violation Alert Email to Admin

Admin Alerts

Administrator alerts are messages sent to the person or group designated to respond to policy violations as soon as they occur. You will want to create a custom email or IM alert for each violation type. I.e. An alert emailed to both the CloudSOC SysAdmin and Compliance officer whenever a violation regarding the inappropriate sharing of PCI or HIPAA data occurs.

Dashboard Reports

Dashboard reports are helpful to give CCoE members high level insights into cloud activity. But don't flood people with reports, or the wrong data. By the wrong data, I mean that if a user cannot change the process or habits involved in a rule violation, they are not an appropriate audience for an email or communication/report.

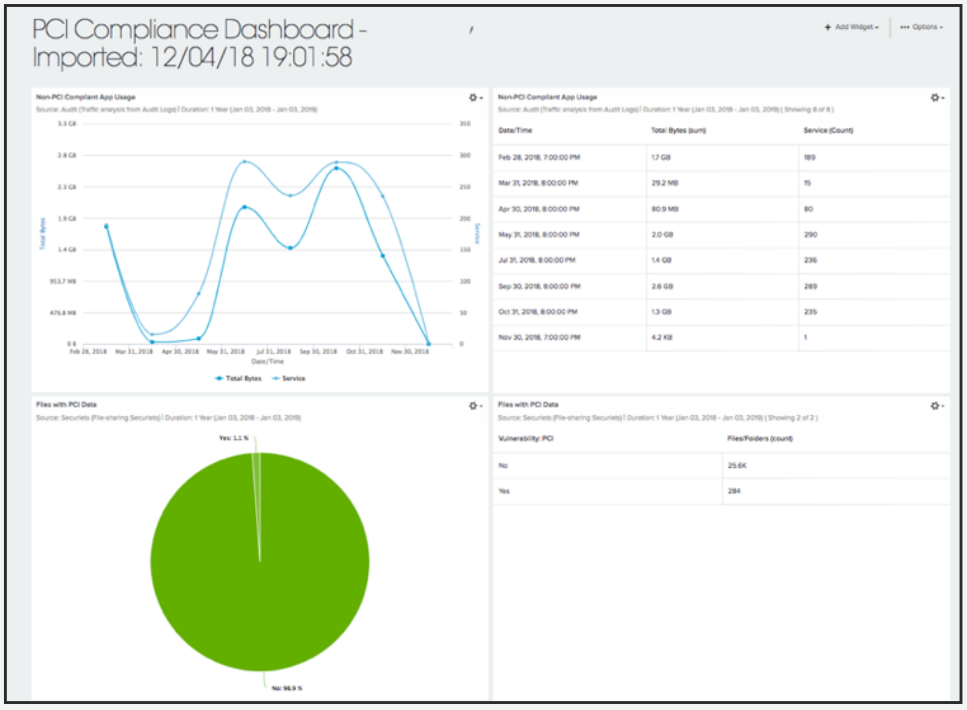


Figure 14: Sample PCI Compliance Dashboard Report

It is best practice to make sure that your IT Security team receives alerts and summaries of anomalies, the compliance team gets insights into compliance violations, and the CCoE team should review the findings early and often to curate what kind of data they can absorb and use.

When you first set up your CASB, you'll have a flood of data and information, especially if you combine with Auditing, API-based securelets and CASB Gateway. A few well-chosen policies implemented early will help reduce the flood to a manageable level and help the decision process for what new or layered policies are needed.

Feedback Loops for Success

If a team or a department needs access to a particular cloud app which has been cut off or restricted to a point where usage is perceived as unnecessarily painful, there needs to be a clear and quick method for communication back to the CCoE, along with engaging, deliberating the request, and timely decision making. Remember, the CCoE exists to make the transition to the cloud both safe and convenient.

When security incidents happen, you need a clear escalation path for how to provide inside (or outside) requests for information. This will also help your compliance officer or data privacy officer fulfil both their documentation and answer audit requests in non-emergency ways.

Metrics – Determining what's Important and measuring success

You'll need to figure out the required metrics for monthly reporting on the status of your cloud ecosystem, including the big picture metrics that can inform buying decisions as well as Cloud App Vendor relationship management. Useful data includes having dashboards and reports on:

- The number of cloud apps in use, including type and security profile.
- The types of data being shared, and where it's flowing.
- Policy violations – who, what, where
- Post-incident analysis, if incidents occur
- Post-incident analysis, if incidents occur

Step 7: Planning Post-Incident Response

It is most likely that your organization already has some form of Incident Response plan. Your CCoE should inform sections with answers to questions like the following:

If verified and confirmed data breach:

- User ID(s) involved in the breach
- Date, time, physical location of the user
- What types of data and files were exfiltrated or exposed?
- Where/App/URL was the information sent?

CloudSOC incident alerting can provide valuable and timely input to the context behind firewall, web application firewall (WAF), secure web gateway (SWG), or other log sources. The technical details of the CloudSOC Critical and High alerts should be routed to incident response teams, or (if available) even imported into a SIEM solution.

During the discovery period (first 1-3 months) your CCoE may want to concentrate on reviewing dashboards and reports at the meetings. After you have baselined normal usage and started to create policies which enforce best practices, you'll need to determine how to communicate violations of these policies so that appropriate actions are taken not only on the product side to mitigate the exploit, but also to ensure proper compliance notifications, employee education, or disciplinary action against disgruntled employees through the Human Resources department.

Source	Type	Alert				
		HR Team	App Owner	Account Admin	Compliance Team	Tech Support
Employee Misuse	Data Breach		√	√	√	
	Malware		√			√
	Risky App Use		√	√		
Internal Bad Actor	Data Breach	√	√	√	√	
	Malware	√	√	√		√
External Hacker	Data Breach		√	√	√	
	Malware		√	√		√
	Acct Takeover		√	√		

Figure 15: Cloud exploit alert plan

Basic notification lists

Remember the first rule of security: Automated security is better than manual security. This includes notification and responses, wherever possible. CloudSOC provides response templates for all of these in Protect module. Here are some basics to consider writing and enabling.

1. Your CloudSOC Admin will be the one who creates response templates. They can decide if they need to be aware of every instance or violation where a response is issued vs reading summary reports.
2. In the event of a customer information or PCI breach, or other critical finding via one of the governance dashboards, you will also want to include your executive sponsor, as well as possible contracts management. This should also include your designated Data Privacy Officer or their equivalent.
3. High-risk user activity, if not found to have caused data exfiltration, will need to alert to the management chain of the user. Most teams divide this between generalities such as "all users in engineering/dev/IT" versus "all sales/marketing/SE/non-technical" users.
    a. In these cases, the CCoE should have some sort of recommended action that can become automatic.
    b. You can store an email notification of the policy which was violated and send it automatically to the users as well as their managers.
    c. Consider how many warnings of inappropriate activity over time need to involve HR retraining (or possible HR policy creation.)

Step 8 – Documenting a Cloud Governance Plan and Educating your Organization

What does success look like?

While security will always advocate for the best scores and least privilege, and Marketing will advocate for ease of use and 'fewest hoops', and Engineering has limits on logical tool sets and DevOps release schedules, you can still come up with success criteria for your CCoE:

- Your daily business needs and standard productivity are met.
- The advantages of cloud services, especially cost and scale, are being delivered.
- Risks are being managed and minimized and documented in your risk register.
- Stakeholders are engaged – everyone understands what you're trying to do and agrees on the process to get there.
- Performance targets are being met.

With this general success criteria, let's talk about KPIs.

KPIs for measuring success

Your CCoE will have to decide how to measure the success of your cloud security, application expenditures, and solution. Like most other projects, it is best to try to measure what you value, rather than just valuing what you think you can measure.

Think of the criteria for a successful CCoE the same way you would each individual app, which is a combination of asking a question and applying values:

- Is the risk score across your organization below the threshold of high business risk? i.e. no App with a BRR score under 70 in use?
- Do you have a clear incident response plan in place for anomalies and incidents?
- Have you determined how to communicate with users who exceed thresholds, violate policies, and generally have a higher risk score?
- Have you started this communication, and reviewed responses?
- Were any HR policy updates required?
- Have you achieved buy in and executive support, so that the entire organization accepts that you are moving toward a more secure cloud posture?
- Does everyone understand their roles, including WHY they need to keep to sanctioned apps, and keep provisional apps strictly for a rigidly-defined use case?
- Are the number of daily violations going up or down over time? Do you need to consider new rules?

You can create KPIs on policies such as:

- What kind of data can now be shared in the cloud
- What enforcement is allowed? Blocking, unsharing, encryption, multi-factor authentication, etc.
- Do you have false positives, and how do you handle them?
- Are the number of policy violations going down over time?
- What kind of input have you been able to provide to incident response teams, if needed?

Step 9 – Cloud Governance Checklist

The most important part of your CCoE team is the executive sponsor. Without executive support and encouragement, policies can be neither officially sanctioned nor properly enforced. While they do not need to be regularly included in planning meetings, they should receive regular reports on team progress as well as executive CloudSOC dashboard reports. Executive sponsors can either be high level members of the IT team such as the CIO or CISO, key functional leaders such as the CMO or CRO, or even the CEO – basically any leader who has organization-wide visibility and authority to help enforce policy changes.

Action Item	Complete?
CCoE Launch	
Selected CCoE members	
CCoE planning meetings	
App Discovery, Classification & Control	
Identified all cloud apps in use	
Analyzed all apps for business criticality and security	
Assigned owners for all business critical cloud apps	
Sanctioned all business critical/secure apps	
Placed controls on business critical/partially-secure apps	
Blocked all non-secure apps	
Compared/consolidated similar apps	
Eliminated redundant cloud and user accounts	
Cloud Data Classification & Control	
Uncovered and categorized all confidential and compliance documents	
Identified sources of compliance docs (BUs, individuals)	
Identified all risky cloud data users	
Set policies controlling sharing of confidential documents	
Set threat detection thresholds-threshold, behavioral, and sequence	
Developed post incident escalation paths	
Deployed incident response notifications for app users	
Deployed incident response notifications for CCoE stakeholders	
Measuring Success	
Developed and began tracking CCoE KPIs	
Documenting Processes	
Developed RACI matrix	
Documented Policies	
Provided Cloud App Inventory Report to IT	

Summary

Remember, as you form your CCoE, that organizational change in processes need to be incremental. No organization can create all their useful policies, thresholds, and responses in a day, a week, even a month. Finding your baselines and learning what normal traffic looks like can take 1-3 months. Making snap decisions that alter traffic patterns quickly can lead to problems.

For example, the moment you determine that one location will NEVER need to send a type of file to a certain location or application, you may get an executive that tells you this behavior is mandatory and quarterly. There will be continuous policy and process improvement as your CCoE matures. Building time into your project to establish a baseline of observed activity and traffic is important before you start to impose multiple complex rules or strict thresholds with blocking.

Look for iterative successes and opportunities for improved lines of communication as well as improved security posture. Automate as much as possible:

- ✓ Auto detect high-risk users
- ✓ Auto classify data types
- ✓ Auto policy enforcement actions
- ✓ Automate incident response and follow-on actions

Symantec

+1 650-527-8000

symantec.com

Keeping Your CCoE Up to-Date on CloudSOC Information

Symantec provides a number of technical and semi-technical resources to keep customers up-to-date on CloudSOC. These resources include:

- **Technical and release notes** available from within the CloudSOC portal. These give some insight into existing and newly released functionality.
- **Periodic product newsletters** sent to your CloudSOC Admin. These include links to best practices documents, informational best practices webcasts, and new product feature updates.
- **The Symantec CASB Best Practices Guide**
- **The Symantec Shadow IT Discovery Best Practices Guide**

Other Symantec Cloud Security Products your CCoE may want to consider include:

- Secure Access Cloud
- Cloud Workload Protection
- Web Security Services
- DLP
- Email Security
- IAM/VIP