GDPR Compliance

Symantec

CloudSOC / CASB 2.0

Monitor and Control Shadow IT & Shadow Data for GDPR Compliance

Contents

What is GDPR?

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a new set of rules by which the European Union (EU) intends to standardize data protection requirements for all personal data for individuals within its borders. It also addresses the export of personal data outside the EU. GDPR will become enforceable as of May 25, 2018.

Sanctions for non-compliance can cost $20m Euros or 4% of gross worldwide turnover, whichever is higher.

Which recitals *(provisions)* apply to cloud applications and data?

GDPR requires enterprises to identify where all of their personal data resides, how it is protected, and how it is being used, including data shared and stored in cloud apps and services. Many GDPR recitals relate to not just technology, but an organization's policies, systems, and people behaviors. However, as the GDPR has a fundamental goal of ensuring that private data is kept secure, there are some key principles that will be common to any data protection plan with the goal of protecting data across its entire life cycle. These are:

- **Know your personal data**
  Understand what personal data you collect and any retention rules you have to store personal data.
- **Assess your data security**
  Assess whether the level of security offered by current policies and procedures is adequate to offer protection against unauthorized processing and data loss.
- **Embed Privacy**
  Ensure that the technologies embed privacy and the processes are built protecting the privacy of individuals.
- **Protect Personal Data**
  Ensure full risk management of personal data from who has access to it, where it is located, how it is used and that it is protected through strong information risk management and security.
- **Control transfers of personal data**
  Transferring personal data out of the European Economic Area—e.g., in the cloud—will be subject to increased regulatory scrutiny.
- **Review any breach notification processes**
  Ensure that your company has tools on hand to investigate the extent of any compromise within a 72-hour notification deadline.

Cloud Apps & Services
SaaS | IaaS | Web | Mobile

How do GDPR compliance requirements affect cloud applications and data?

Organizations will need to monitor and control cloud applications and services used by employees who may be sharing and storing the personal data of EU residents. They will also need to have data protection policies in place to protect the personal data itself.

These compliance requirements will apply to any company that processes EU residents' personal data, no matter where it is located.

What constitutes personal data under GDPR?

Personal data is broadly defined as any information relating to an identified or identifiable natural person such as an identification number or information specific to their physical, physiological, mental, economic, cultural, or social identity. Most significantly for cloud applications, it is also worth mentioning that user, network and device identifiers (i.e., IP addresses) in log files are also considered personal data if they can be traced back, even indirectly, to a particular individual (e.g., employee, consumer, customer contact person, system administrator, support agent, website visitor).

What are the specific compliance issues for cloud apps?

GDPR requirements are concerned with location, access, protection, handling, security, and encryption for personal data. This can be particularly challenging for an organization when the IT team may not be aware that a department or individual is using a certain cloud application or service. For those cases when IT is tracking the use of sanctioned SaaS and IaaS solutions, they may not have any visibility or control over how that service addresses these issues.

How can Symantec CloudSOC help address GDPR requirements?

CloudSOC Cloud Access Security Broker (CASB) addresses these GDPR compliance recitals for personal data stored and shared in the cloud with a full end-to-end cloud security life cycle:

01 Prepare

- Know where your personal data is in the cloud
- Check if your cloud apps fulfill key security attributes associated with GDPR
- Uncover and classify personal data

02 Detect

- Know what risky personal data you have and whether it is exposed
- Detect anomalous user behavior and malware

03 Protect

- Block apps that do not fulfill key security attributes associated with GDPR
- Define cloud data policies
- (Optional) Ensure you have consistent DLP policies both in the cloud and on-prem
- Identify risky users, activities and data
- Set risk detector thresholds

04 Respond

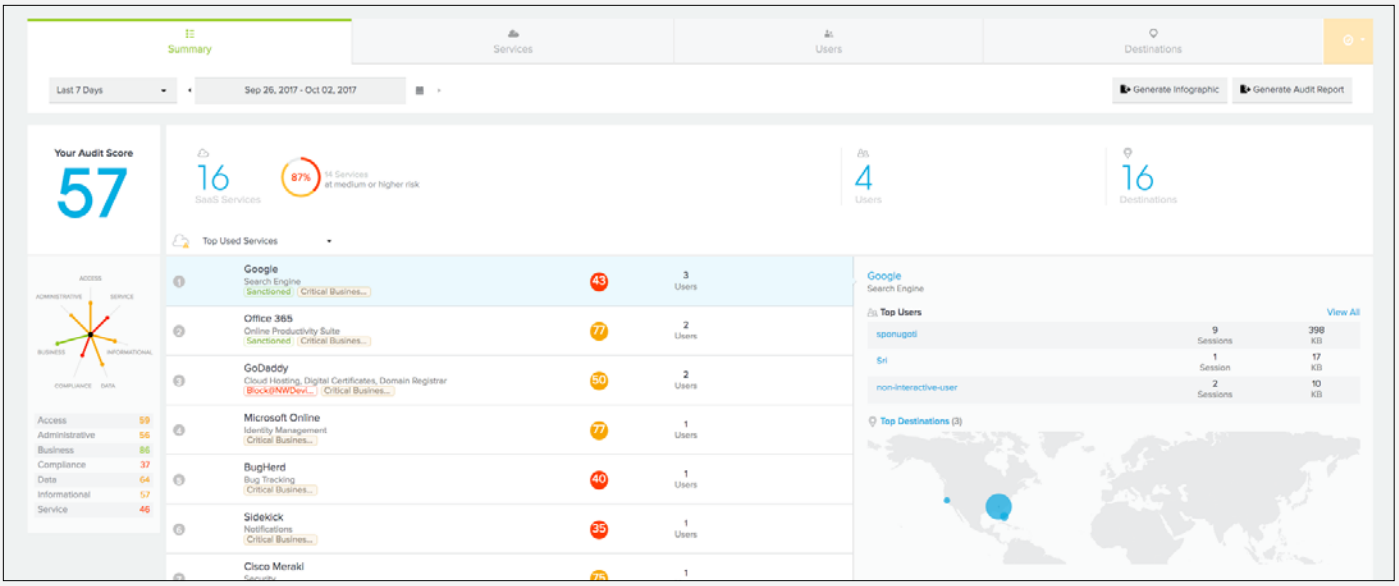
- Quarantine risky personal data and users
- Block uploading and downloading of personal data
- Remediate risky exposures in file shares
- Set up and send policy violation alerts to admins and users
- Provide post incident analysis and response within a 72-hour notification deadline
- Provide dashboards and reports that provide visibility into your GDPR compliance posture
- (optional) Tokenize or encrypt personal data either at the field or file level for added security

01 Prepare

You cannot control what you cannot see, so uncovering the cloud apps and services in which your personal data is stored, and identifying that personal data itself, is a prerequisite to setting GDPR-related policies and enforcing compliant cloud usage.

1. **Know where your personal data is in the cloud**
   The European Union General Data Protection Regulation requirement has significant implications for organizations using cloud apps. Shadow IT comprises cloud apps and services adopted by employees and business units, often without IT sanction or security oversight. More than 90% of cloud apps today do not exhibit key security attributes associated with GDPR. Uncovering these apps is a critical first step in helping to secure your personal data for GDPR compliance.[1]

   - CloudSOC Audit helps enable you to uncover and analyze all cloud applications on your network, including Shadow IT adopted by employees and business units without IT sanction or security oversight. CloudSOC can provide granular information on over 22,000 cloud apps and services, and then provide an overall cloud Risk Score on the cloud apps used by your organization.

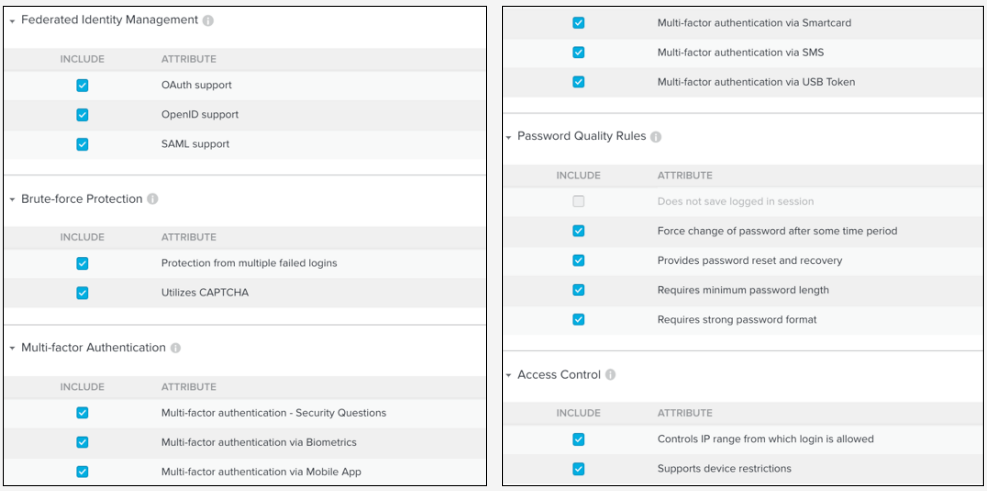


Screenshot: CloudSOC Audit screen showing apps in use, their Business Readiness Rating (BRR) and the sample organization's overall Audit Score (57)

2. **Ensure that usage of your apps is GDPR compliant**
   Performing the due diligence necessary to confirm cloud applications exhibit key security attribute requirements for GDPR compliance can be challenging, but this is a critical second step to ensuring your personal data is being handled according to GDPR requirements.

   - CloudSOC Audit provides a Business Readiness Rating (BRR) on a scale of 1-100 for each app based on over 100 risk attributes, including those associated with GDPR (See next page). This information can help you to make smart app choices. These attributes are used to compile the BRR for your cloud apps. You can customize the significance of each attribute to customize your app BRRs to match your security requirements.

1. *Symantec 1H 2016 Shadow Data Report*



Screenshot: Sample of the risk attributes tracked for cloud apps in CloudSOC. The importance of Risk Attributes, including GDPR relevant ones, can be customized to Must Have, Important, Nice to Have or Don't Care

List of cloud app GDPR relevant attributes in CloudSOC

GDPR requirements applicable to cloud usage	Attributes
Know the location where cloud apps are processing or storing personal data	Identify the locations of data centers where the app is hosting your personal data (based on current usage)
Take adequate security measures to protect personal data from loss, alteration or unauthorized processing	Password quality rules, brute-force protection, MFA, role based access control, IP and device based restriction
	Content security policies, policy configuration and enforcement
	Data sharing controls
	Admin, User Audit Trails
	Compliance and certs
	Encryption data at rest, keys in control of the enterprise? No known security vulnerabilities
	Encryption data in motion, SSL used for data in motion, key strength, cert strength
	Data not stored on mobile for offline access, offline data encrypted
Don't allow cloud apps to use personal data for unauthorized purposes (opt-in regulations)	Customer data not analyzed for ad targeting
	Customer data not analyzed for behavior mining
Take adequate security measures to protect personal data from loss, alteration or unauthorized processing	Does the service have backup data center for data redundancy and availability (disaster recovery and business continuity)
	Is the backup data encrypted?
	Restrict opening files in external apps on mobile (device security policy)
	Are user account credentials encrypted? If integrated with other 3rd party services, is password stored?
Don't allow cloud apps to use personal data for unauthorized purposes	Does the customer or SaaS vendor own the data?

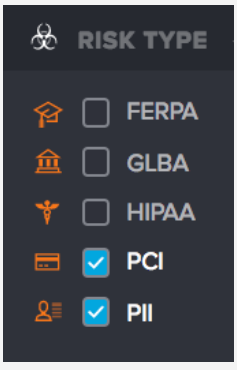
List of cloud app GDPR relevant attributes in CloudSOC *(cont.)*

GDPR requirements applicable to cloud usage	Attributes
Know the location where cloud apps are processing or storing personal data	Location of where data can be hosted for processing and storage (all data centers)
	Capability to restrict storage of personal data to specific regions
Ensure that you can erase the personal data when you stop using the app	Data erased upon termination of service by customer
Take adequate security measures to protect personal data from loss, alteration or unauthorized processing	Does a service have a published disaster recovery plan?
	How would a SaaS vendor handle personal data in case of merger/ acquisition/shut-down
Does my company have a formalized breach notification process?	Formal breach notification and incident response policies in place to identify, confirm, address and notify affected parties of breaches within 72 hours
Close a data processing agreement with the cloud apps you're using	Does the cloud vendor offer a data processing agreement?
Collect only necessary data and limit the processing of personal data	Only necessary data to perform the functions of app collected (i.e. per the data processing agreement, limits on the collection of personal data that reveal race, ethnicity, religion, political conviction, ...)

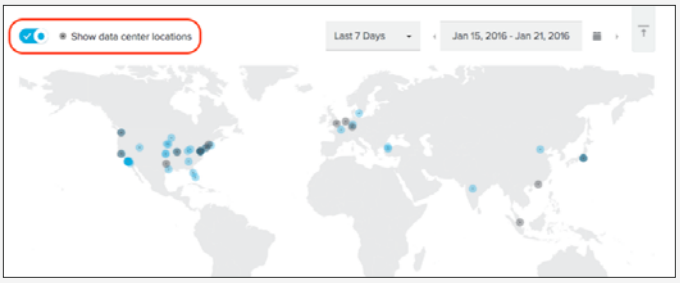
3. Uncover and classify personal cloud data

Once you understand where your personal data is being stored, it is necessary to identify which data stored and shared in them is personal and what retention rules you have relating to the storage of that data.

- **CloudSOC** uses **ContentIQ**, its data science driven content inspection engine, to provide native CASB data governance and DLP capabilities. You can quickly set up ContentIQ profiles to identify specific personal data types.
- **CloudSOC** then monitors and scans all cloud data to determine:
  - What types personal data is being stored in the cloud
  - Where the personal data resides



Screenshot: Some content types automatically identified in CloudSOC using the data science powered ContentIQ data classification engine.



Screenshot: Accurately track the locations where data associated with a specific cloud application may be found based on global application traffic flow analysis performed in CloudSOC. Unlike other solutions that rely solely on self-reported public data, CloudSOC leverages Symantec's global footprint to identify data locations through empirical analysis. This enables us to identify locations not found in general public sources.

02 Detect

Detecting threats in the cloud requires leveraging either real time gateway detection for unsanctioned and sanctioned cloud apps or APIs to get near real time detection of incidents in select sanctioned cloud apps:

- **CloudSOC Gateway** uses StreamIQ™ technology to extract granular events from real-time cloud application traffic. Its unique data science-powered technology enables deep visibility into transactions with a broad range of cloud applications.
- **CloudSOC Securlets** leverage APIs for a dozen top cloud apps such as Office 365, G Suite, Box, and Salesforce. It can inspect data at rest, even for cloud-to-cloud transactions or legacy data exposures not previously detected.
- **CloudSOC Audit** ingests log files from your proxy or firewall to uncover Shadow IT and audit use of cloud applications. It also enables you to evaluate which cloud services are business-ready and control their usage to keep your organization safe and compliant.
- **Cloud Data Protection (CDP)** selectively encrypts or tokenizes field-level information in SaaS applications to help achieve cloud data protection and compliance for personal data.

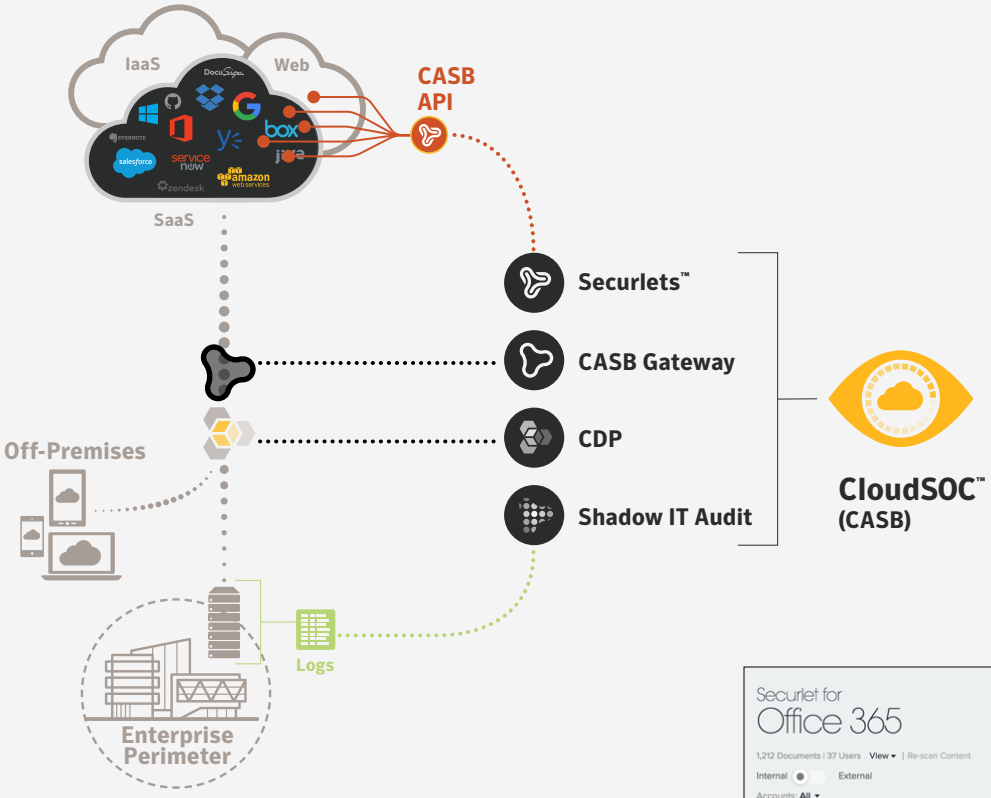
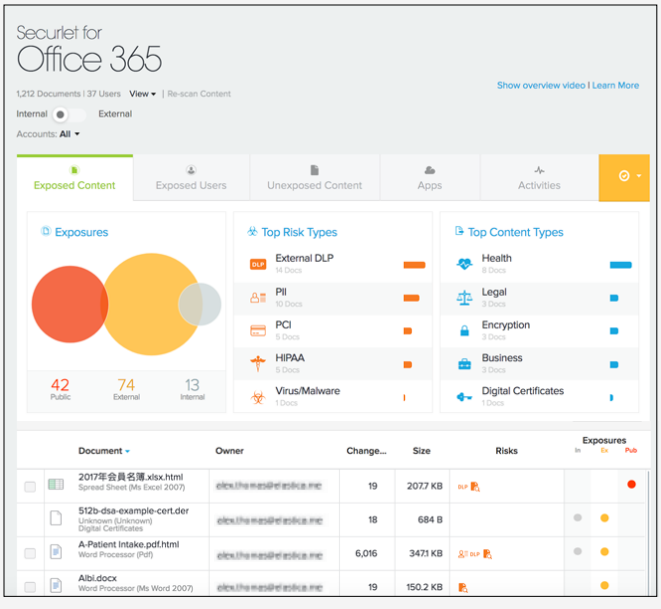


Diagram: This diagram shows the full suite of CloudSOC CASB solutions, including the API based Securlets and CASB Gateway

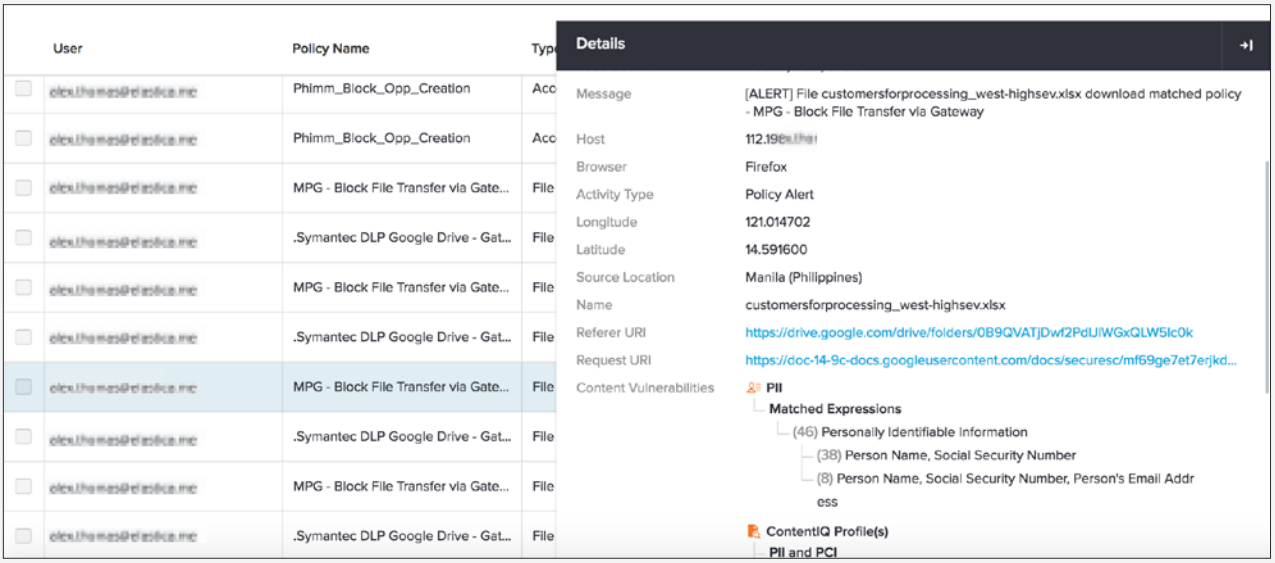
- **Know what personal data you have and whether it is exposed**

- **Detect Policy Violations**
  CloudSOC Protect allows you to identify when a ContentIQ/DLP policy has been violated, providing the intelligence needed to take action.



Screenshot: Securlet dashboard showing data exposures, top risk types, top exposed data and a list of all exposed document

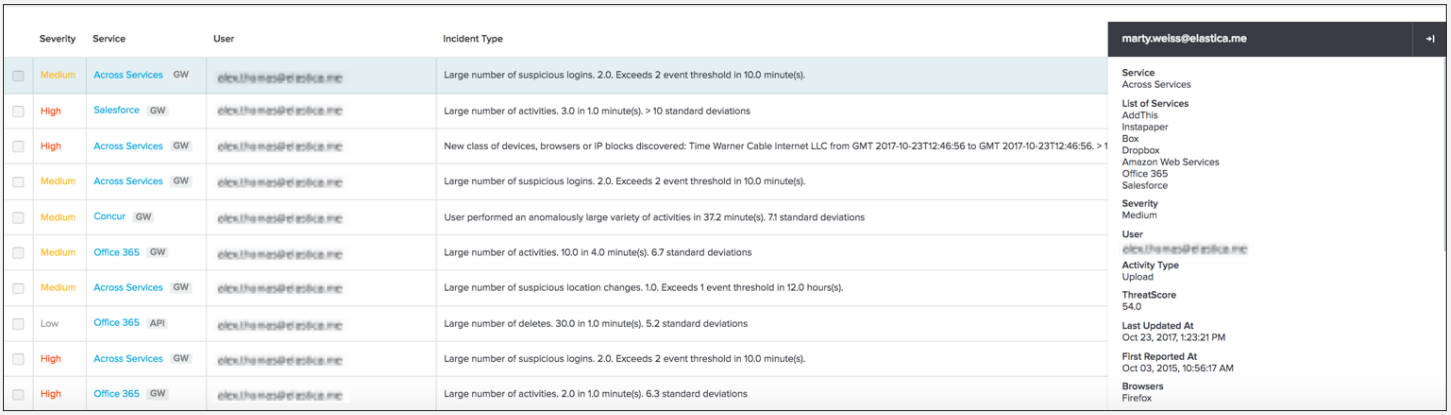
Symantec.



Screenshot: CloudSOC Protect Screen policy alerts, with a pop-up showing drill down event details for a user who's download of personal data has been blocked.

- **Detect anomalous user behavior and malware**
  CloudSOC Detect allows you to identify risky behaviors such as account compromises, data destruction, and data exfiltration as well as malware infected files. Detect ingests and correlates user behavior, applying data science to graphically identify issues. This enables you to:

  - Detect risky user behavior
  - Identify potential account take-overs or malware, etc.
  - Avert risks due to inadvertent exposures while educating users
  - Define new data protection strategies and fine tune policies



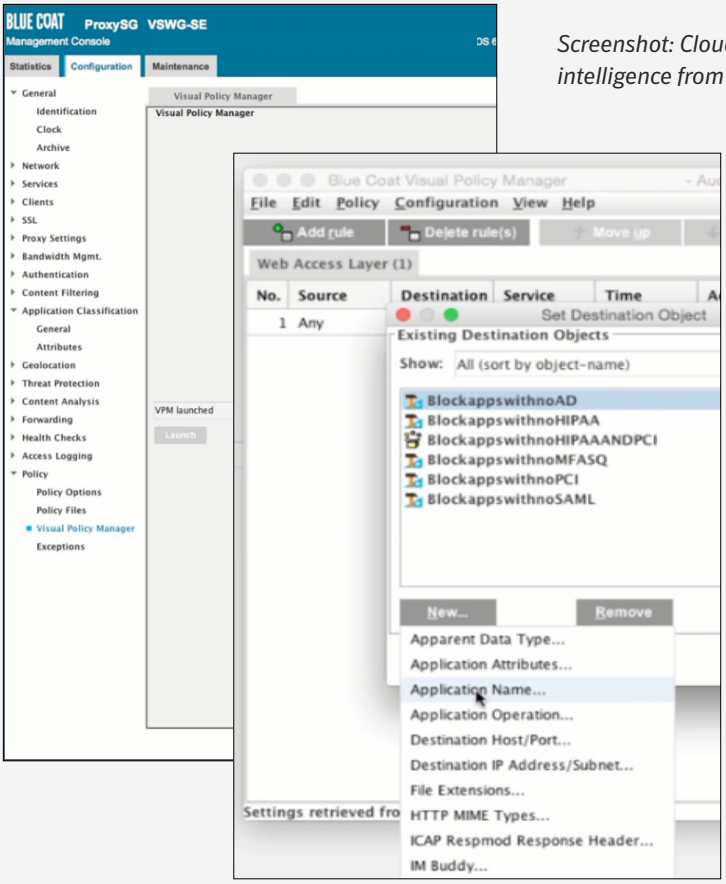
Screenshot: CloudSOC Detect Screen Showing incidents with a drill down into users, incident types, affected applications and other event details

03 Protect

Protection refers to the setting and enforcement of cloud application and data policies that ensure cloud usage adheres to GDPR guidelines.

1. **Block apps that do not exhibit key security attributes associated with GDPR compliance**
   Just uncovering Shadow IT is not sufficient for GDPR compliance; you also must be able to set policies to control access to apps likely to allow non-compliant behaviors and actions.

   - **Integrating CloudSOC and Symantec ProxySG or WSS** provides visibility and control over cloud apps directly through your proxy management console. This is achieved through an App Feed from CloudSOC to ProxySG and WSS. You can then apply policies based on GDPR-relevant attributes and geographic processing/ storage profiles directly in your Secure Web Gateway (SWG) based on this dynamic app intelligence.



Screenshot: Cloud app policy set up through the ProxySG management console using intelligence from CloudSOC App Feed via the Symantec Global Intelligence Network (GIN)

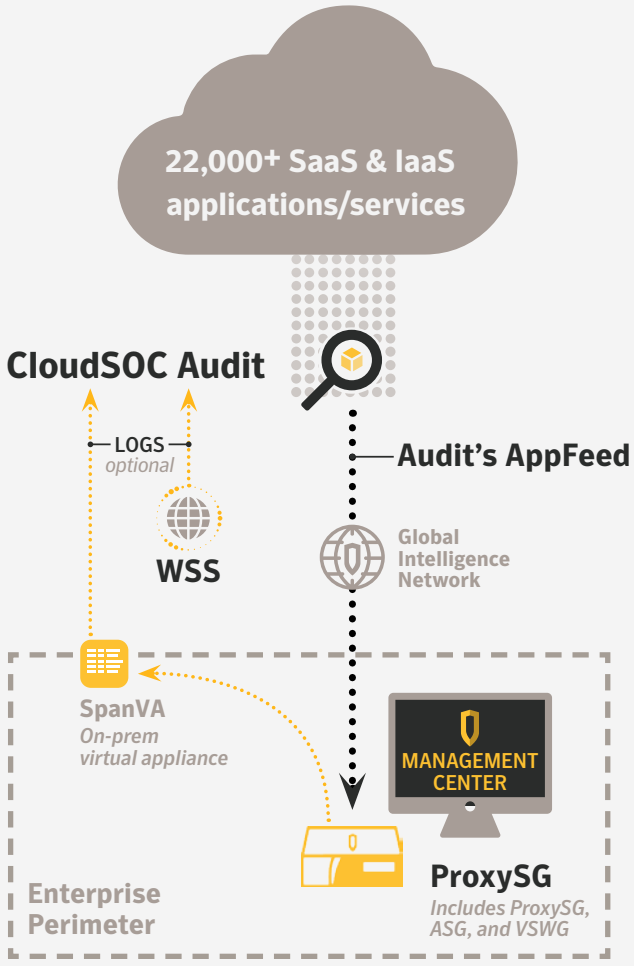
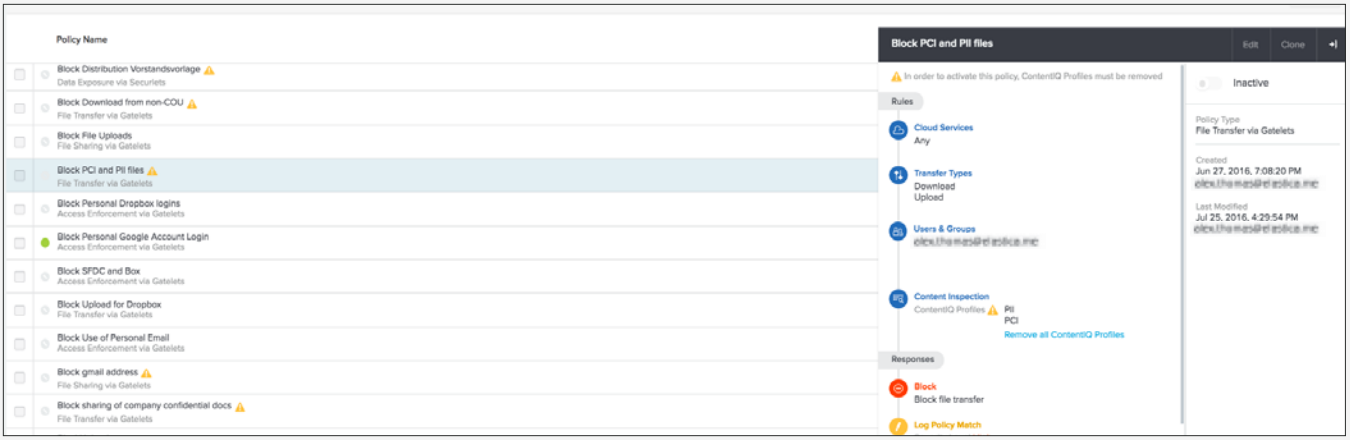


Diagram: CloudSOC Audit integration with ProxySG/WSS

2. **Define Cloud Data Policies**
   CloudSOC Protect enables you to apply GDPR-related privacy policies for both data-in-motion and data-at-rest using CloudSOC's native DLP, ContentIQ, or alternately through integration with Symantec DLP. (See section 3 below)

   - **Policies can be built using CloudSOC ContentIQ,** enabling you to block or alert on specific violations.



Screenshot: CoudSOC Protect policy screen showing drill down details into an example document with personal data or PCI policy

   - **Protect personal data**
     Ensure full risk management of personal data from who has access to it, where it is located, how it is used and that it is protected through strong information risk management and security.
   - **Control transfers of personal data**
     Transferring personal data out of the European Economic Area (e.g., in the cloud), will be subject to increased regulatory scrutiny. CloudSOC helps you to apply policies preventing such transfers.

3. **(Optional) Ensure you have consistent DLP policies both in the cloud and on-prem**
   Personal data travels between your on-prem network and the cloud. To avoid gaps in security caused by creating separate islands of DLP in the cloud, and inconsistent policies and workflows, you should integrate your on-prem DLP and CASB. Note that most solutions use ICAP, which wastes bandwidth and increases latency due to the need to reroute all traffic to the on-prem DLP engine. Only Symantec has a native REST API based solution (see next page) that doesn't rely on ICAP for integration—optimizing performance. It also empowers the DLP console with rich insights from CloudSOC such as new policy attributes, user ThreatScores and detailed cloud activity log information.

   - **CloudSOC Securlets and Gateway integrated with Symantec DLP**
     Extend your existing DLP policies and workflows to the cloud without having to recreate them for cloud stored and shared data, to gain consistent visibility and control over Shadow Data on-prem and in the cloud.

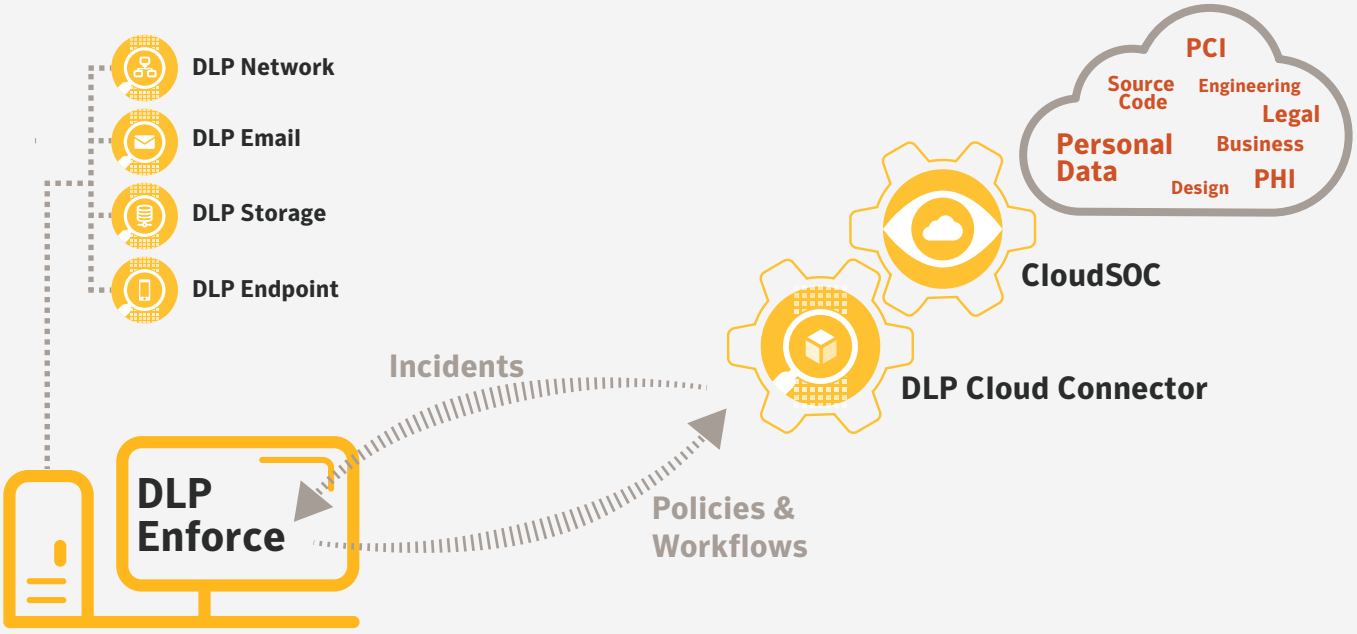
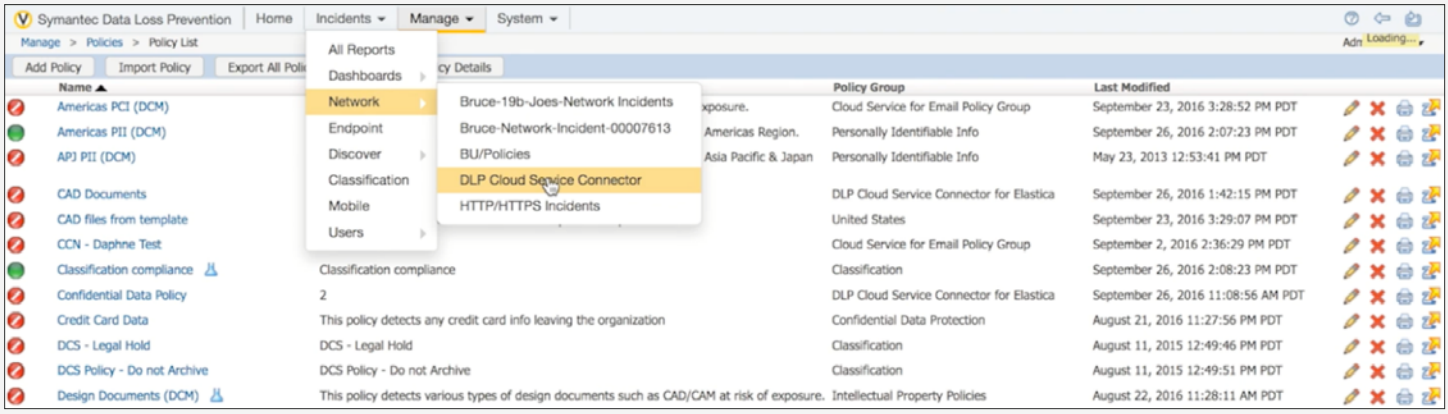


Diagram: CloudSOC Integrated with Symantec DLP



Screenshot: Symantec DLP Policy List Screen Showing Activation of DLP Cloud Service Connector

4. **Identify Risky Users, Cloud Activities and Data**
Once you know what GDPR relevant data is stored and where, you will need to track when classified data is placed at risk of account takeover, data destruction or data exfiltration.

- CloudSOC leverages User Behavior Analytics (UBA) to analyze cloud usage then assigns a dynamic ThreatScore to every user based on their cloud activities. This enables you to track and control access to personal data for high-risk users.
- If user behavior threatens to violate GDPR compliance requirements, you may choose additional user-education, step-up authentication, or restriction of risky users' actions to safeguard your data.

Screenshot: User Threat Tree. Note the user ThreatScore of 99 (high) on the left and the branches showing violations that contributed to that score.

5. **Set Risk Thresholds**
Set threshold, behavioral, and sequence based detectors for detection of risky behaviors. Threshold importance can be set to Less Important, Important, Very Important, or Critical based on your organization's threat posture.

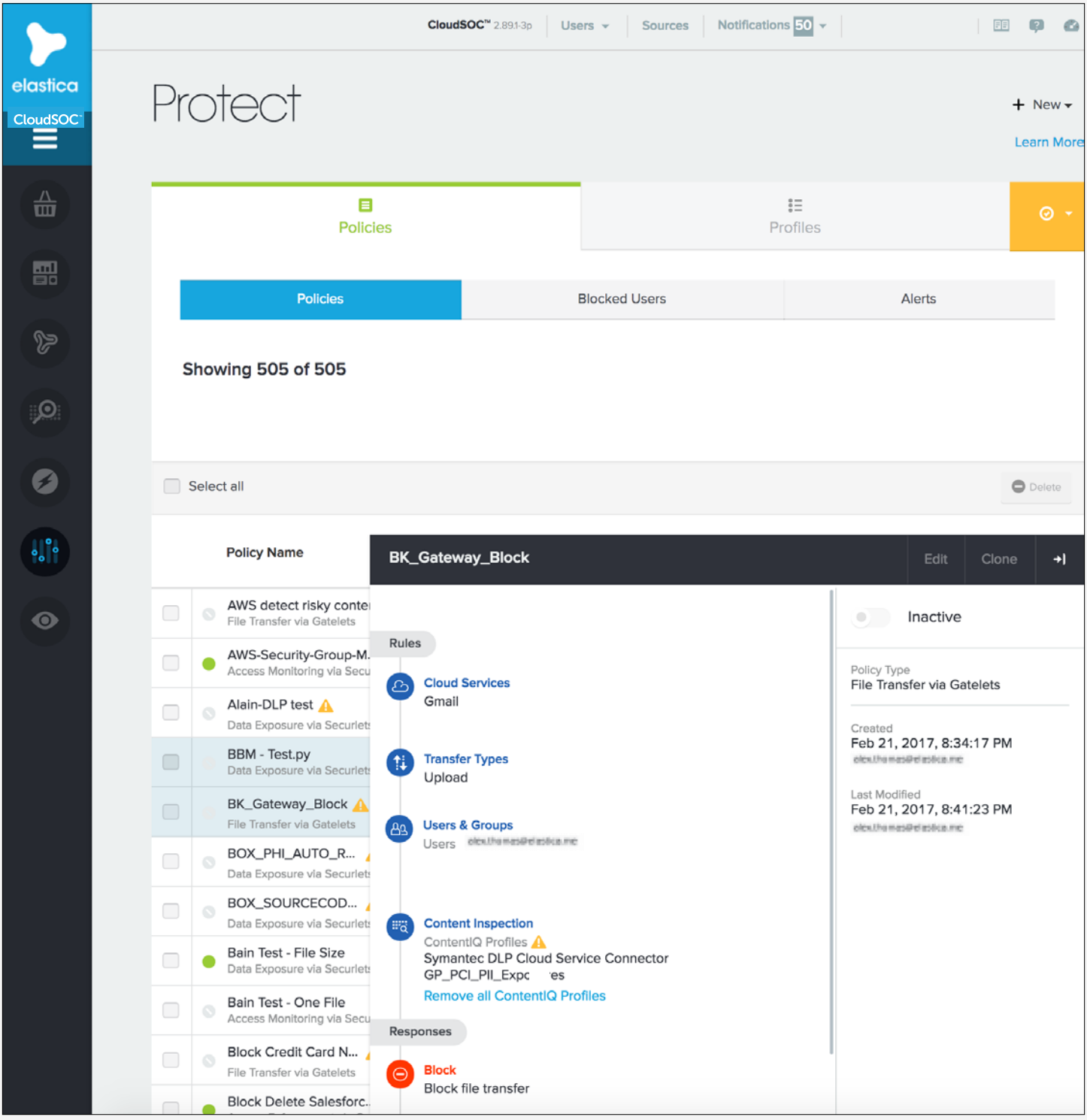
- **Threshold detectors**
Set duration (minutes) and importance of threshold-based activities (e.g., five invalid logins in 2 minutes)
- **Behavior detectors**
Set confidence level (≥ x%) and Importance of behavioral activities (e.g., Anomalous frequent user actions : ≥30% confidence)
- **Sequence based detectors**
Create multi-step sequence based detectors that identify a chain of activities within a set time-frame (e.g., a user copies, renames and downloads 10 spreadsheets in 1 hour)

04 Respond

Responding to policy violations and threats can include alerts to IT admins by email, text or ticket, or remediation activities such as updating file permissions, quarantining risky data and users, and blocking downloads of personal data.

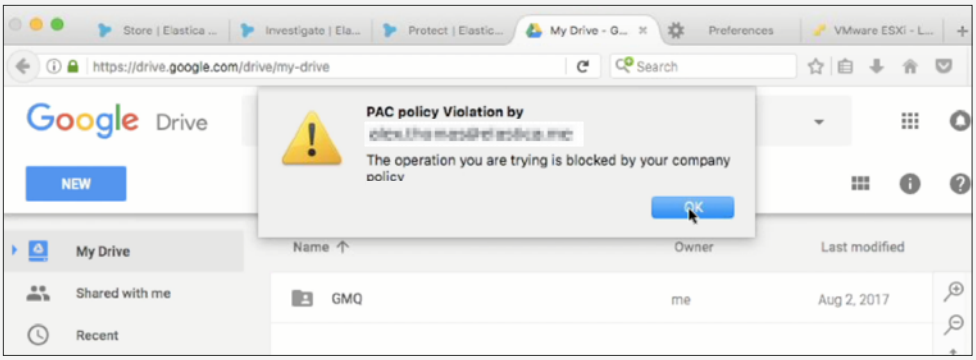
1. **Quarantine data and users**
When data has been overexposed or a user or group has violated a policy or performed a risky activity, you can remediate or block the activity, for example:

- Block uploads of files
- Quarantine files
- Unshare shared files
- Encrypt files



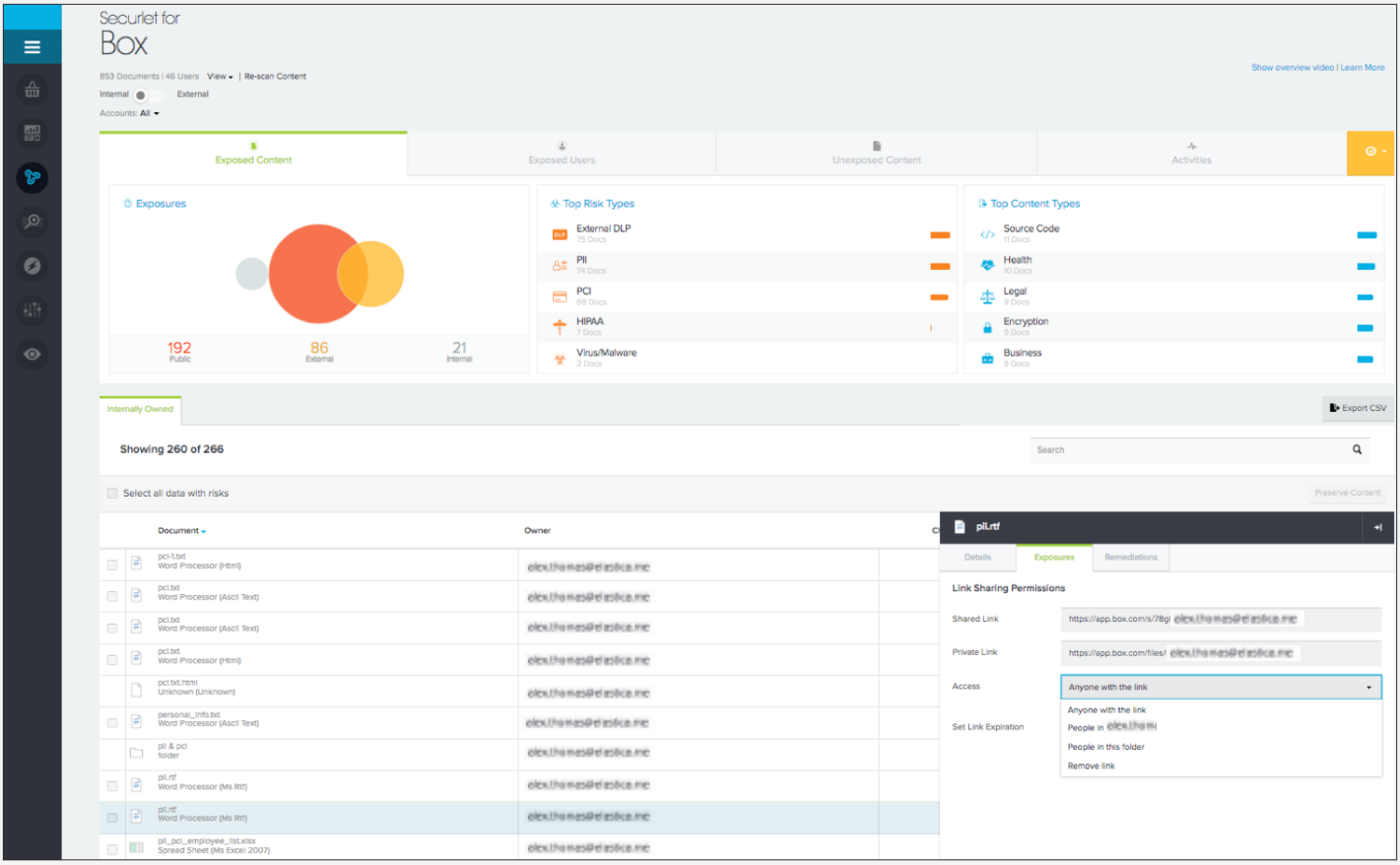
Screenshot: a drill down on a policy blocking uploads of GP, PCI, and documents containing personal data

2. **Block uploading and downloading of personal data**
   Once you set up a ContentIQ DLP policy to block uploads or downloads of personal data, the action is automatically blocked when users violate the policy.



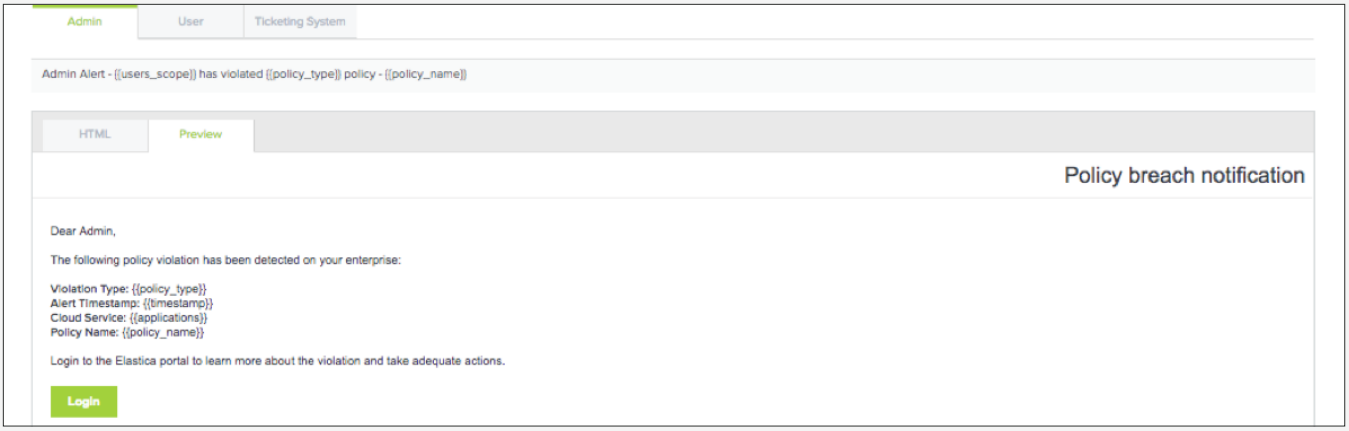
Screenshot: Policy violation notification when user attempts to upload personal data to a corporate Box account

3. **Remediate risky exposures in file shares**
   When personal data is found to be at risk (overshared), you should change the sharing permissions of that file.



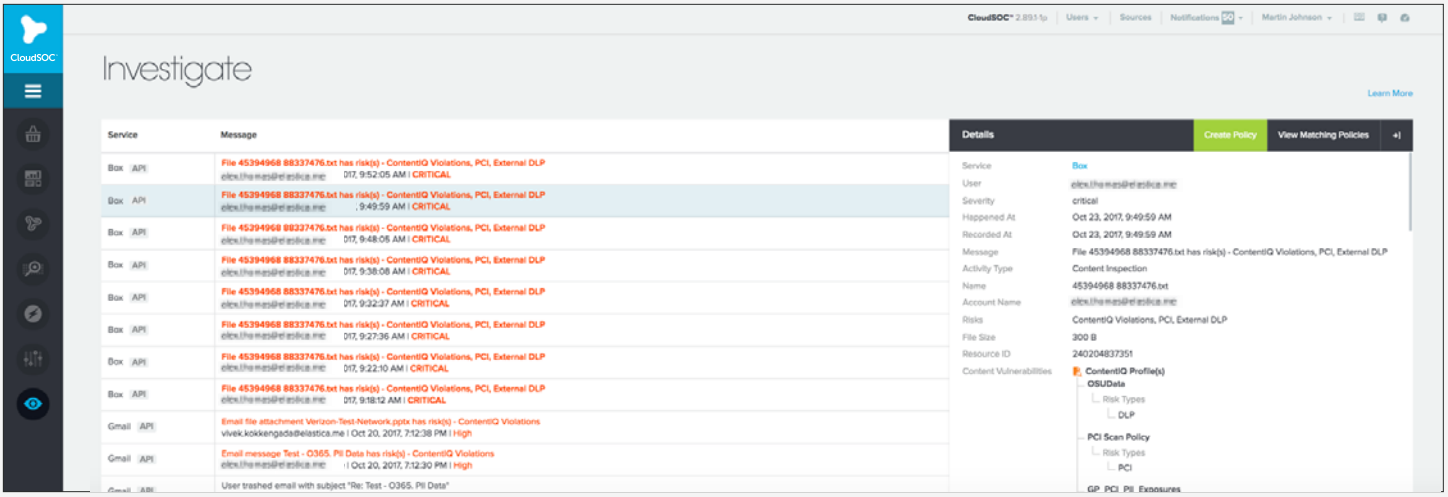
Screenshot: Box Securlet dashboard showing an overexposed document containing personal data and a pop-up screen enabling you to change sharing permissions

4. **Set up and send policy violation alerts to admins and users**
   CloudSOC Protect allows you to set up and customize alerts via email, text or ticket to system admins when policies are violated, and email alerts to users.



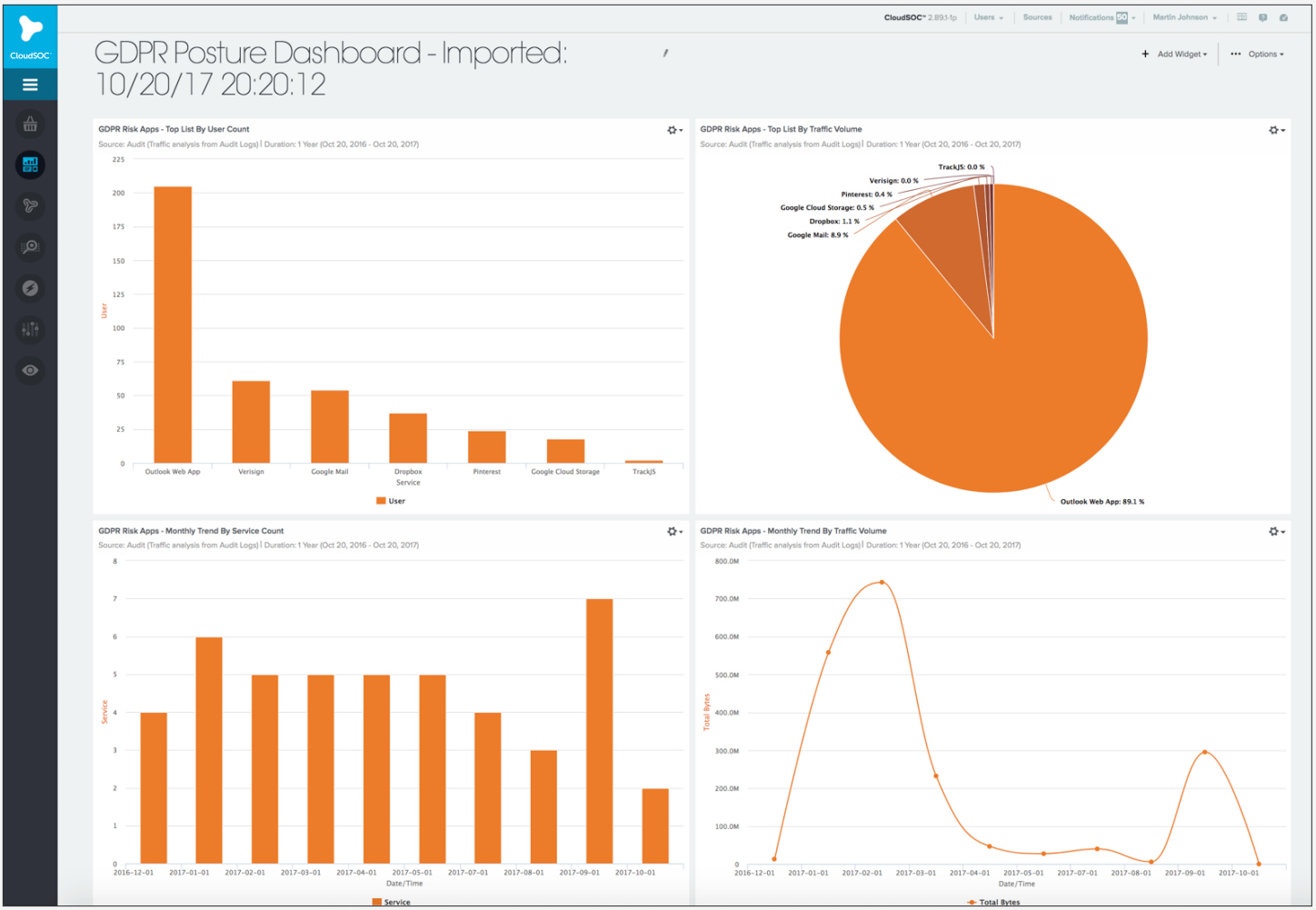
Screenshot: CloudSOC Protect response template screen, showing a customizable admin policy violation email alert template

5. **Provide post incident analysis and response within a 72-hour notification deadline as per GDPR Article 33 (1)**
   CloudSOC Investigate capability enables you to quickly investigate areas of concern in cloud accounts for fast reporting of data breaches to the Data Protection Authorities (DPA). CloudSOC collects granular data on transactions using machine learning-assisted StreamIQ technology. You can access that data through intuitive search and filtering functions and analyze it via powerful data visualizations and consolidated log reports.



Screenshot: CloudSOC Investigate Screen showing historical personal data policy violations with drill-down details on an example incident

6. **Provide dashboards & reports that give full visibility into the cloud portion of your GDPR compliance posture**
   CloudSOC's out of the box GDPR dashboards help you readily monitor GDPR compliance and potential risks. In addition, these dashboards can be regularly sent out through email distribution as regular reports, which are key to keeping an eye on your GDPR cloud posture on an ongoing basis.



Screenshot: Fully customizable GDPR dashboard in CloudSOC

7. **Tokenize or encrypt personal data**
Notification of each affected person after a data breach is a key GDPR requirement, but also a major burden. Tokenization and encryption of personal data at rest, in motion and in use can reduce this burden.

- **(Optional) CloudSOC Gateway integrated with Safenet** enables you to encrypt files when users upload them to cloud services, and to decrypt those files when they are downloaded. The Gateway:
  - Works across multiple SaaS apps with a single encryption solution.
  - Lets you control the encryption keys.
  - It is focused on encryption of static file content (for example, financial statements, medical records, etc.) when they are uploaded to the cloud.
  - Supports encryption/tokenization of data in Office 365 OneDrive, Google Drive, Salesforce, and Box

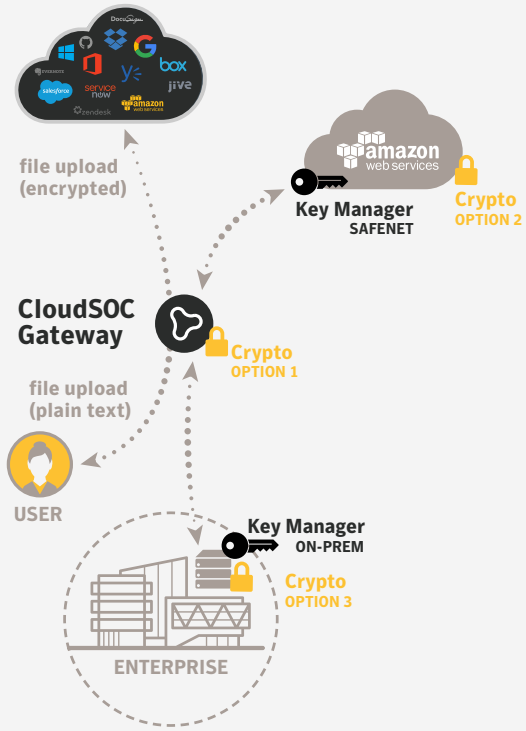


Diagram: The CloudSOC Gateway Encryption Process

- **(Optional) Symantec CDP, integrated with CloudSOC**
Selectively encrypts or tokenizes field-level information in SaaS applications to achieve cloud data protection and compliance for structured data.
  - Before any personal cloud data leaves an organization's control, it is replaced with a meaningless surrogate token or a strongly encrypted value to ensure it remains private to meet GDPR requirements.
  - Supports field-level encryption/tokenization in ServiceNOW, Salesforce, and Oracle.
  - Integrates with DLP to enable you to use DLP policies to trigger tokenization and encryption.

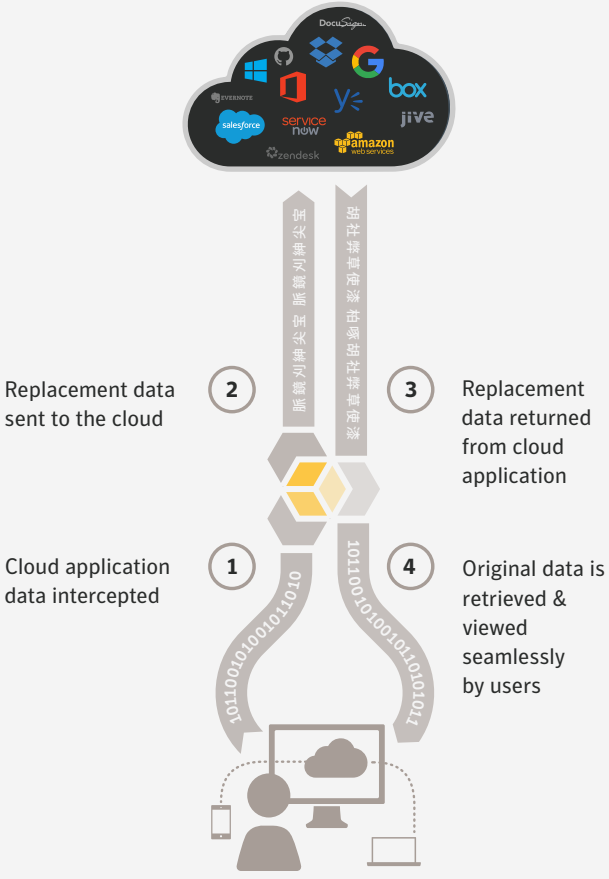


Diagram: The Cloud Data Protection Gateway encryption/Tokenization Process

- **(Optional) Symantec Information Centric Encryption (ICE) integrated with CloudSOC and DLP (recommended)**
  With ICE, you can encrypt entire files and keep data safe though monitoring and controlling access in real time, dynamically revoking user access or remotely wiping access to a document. With Symantec ICE you can:
  - Encrypt application data and personal data in a broad set of file formats
  - Revoke access to personal data if a malicious insider or hacker obtains it
  - Find and wipe copies of personal data accessed by an unauthorized user
  - Store your keys in a customer-managed Amazon Web Services account

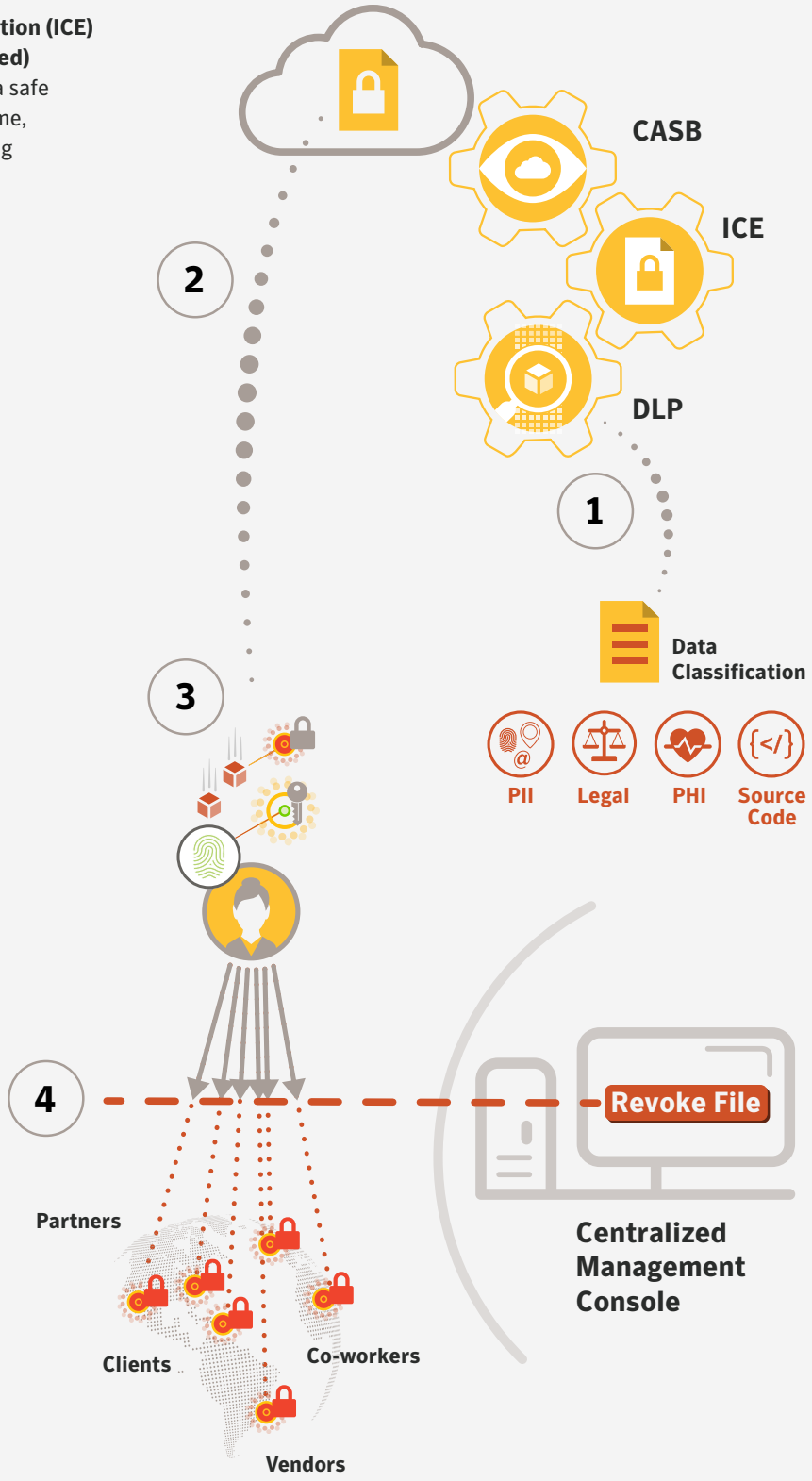


Diagram: ICE encryption process, a comprehensive Information Rights Management solution

1. Dynamically encrypt based on content classification.
2. Content stays encrypted, regardless of where it travels.
3. Granular control of who can access content.
4. Content is beaconized and may be revoked at any time.

How Can You Get Started on Becoming GDPR Compliant in the Cloud?

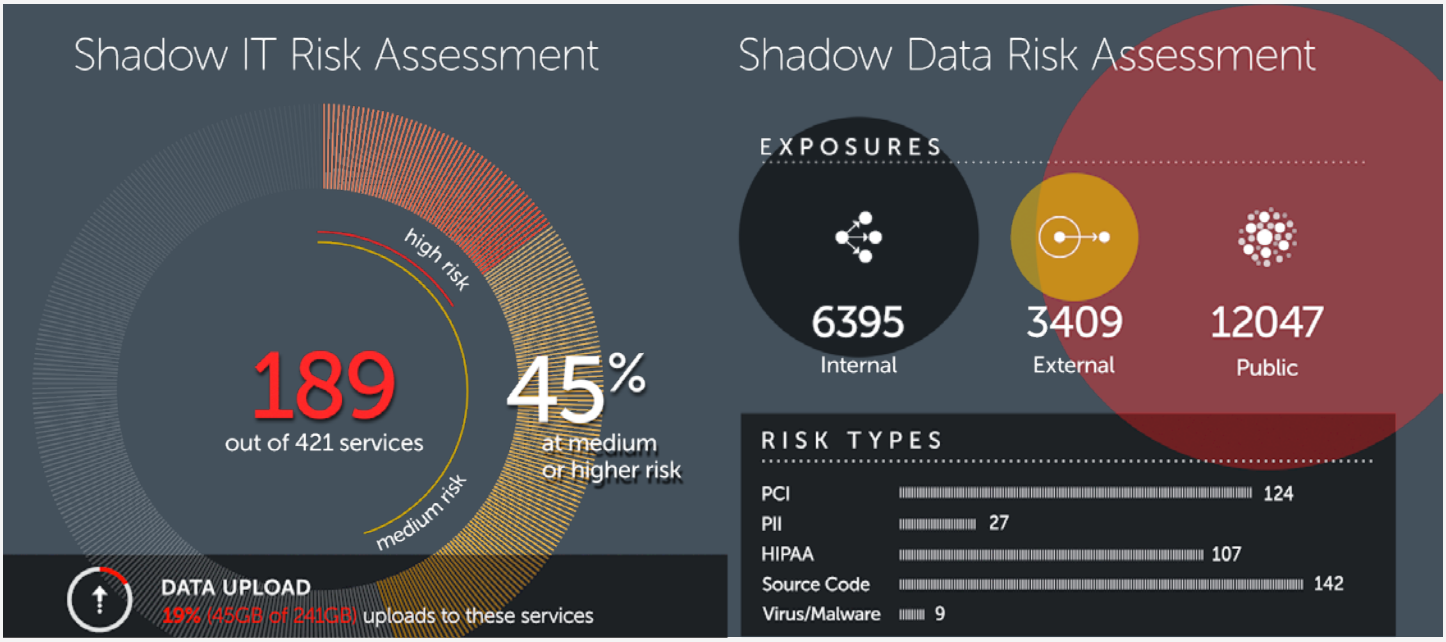
Contact Symantec for a free Shadow IT or Shadow Data Risk Assessment.

The Shadow IT Risk Assessment is a multi-page analysis of your cloud security posture that includes:

- Executive Summary of most used apps, new services added, most active cloud users, service categories, and service hosting locations
- List of all services by category
- List of all discovered services
- List of all users
- Security recommendations

The Shadow Data Risk Assessment is based on your organization's unique security requirements, but generally within a few days, your account rep will deliver a PowerPoint slide deck giving your organization a comprehensive overview of:

- The types and risk level of data stored and shared in the selected cloud app
- User activity and usage patterns in the selected cloud app
- The types of policies and controls that will be required to promote the cloud app to the business as the only approved file sharing drive
- The economic and productivity benefits from a successful and secure migration to the selected cloud app



go.symantec.com/shadow-it

go.symantec.com/shadow-data

In addition, through direct access to the CloudSOC dashboard, your organization will be able to gain real-time visibility into the following:

Exposure Risk
Visibility into files that are exposed publicly, externally, or internally.

Sensitive Content Risk
Patent-pending ContentIQ™ technology, based on computational linguistics and machine learning identifies sensitive/personal data in the cloud.

Compliance Risk
ContentIQ™ also automatically highlights possible compliance risks.

Usage Analytics
Filtering based on user, content type, and risk type is a breeze. You get a slick desktop style experience. Users responsible for data exposures are identified.

Users with Sensitive Content
Users with the most compliance risks are highlighted.

Users with Exposures
Users responsible for data exposures are identified.

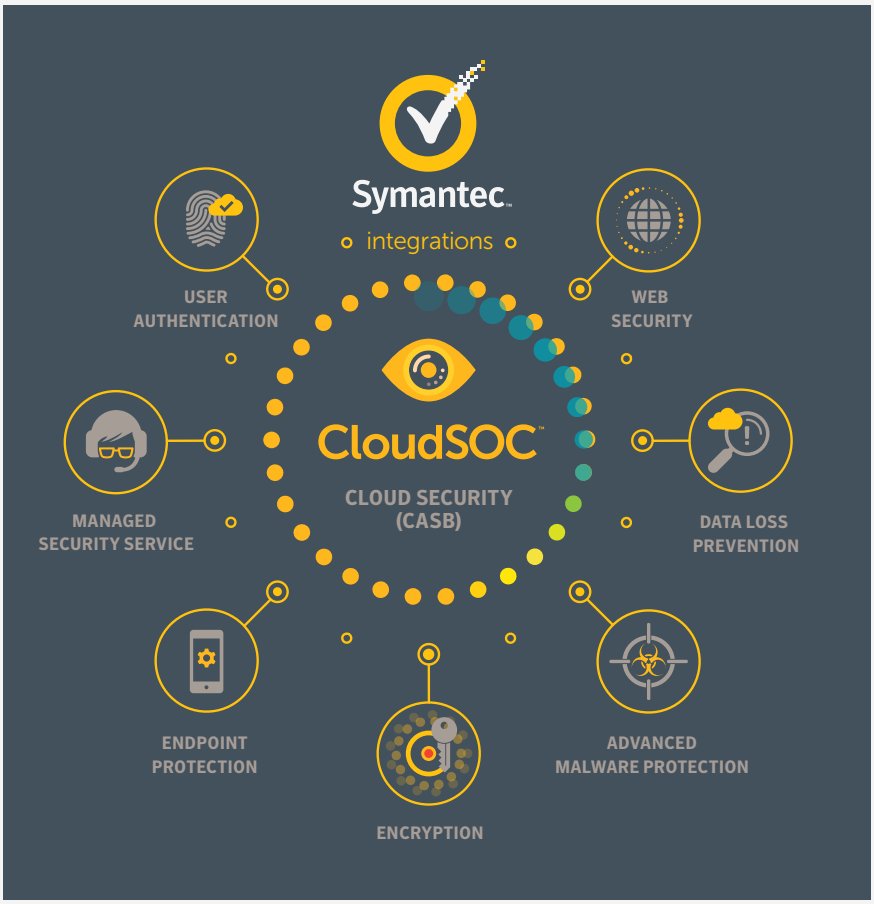
User Centric ThreatScore™
Identify users demonstrating risky behavior.

DISCLAIMER: Prudent companies should review their broad GDPR compliance PLAN with appropriate counsel.

Symantec

What is CASB 2.0?

CASB 2.0 refers to a next generation CASB solution that seamlessly integrates with a wide range of core security technologies including Data Loss Prevention (DLP), Secure Web Gateways (SWG), endpoint, encryption, access control, and Advanced Threat Protection (ATP). CloudSOC pioneered this technology by natively integrating with the full suite of Symantec Security solutions, enabling you to avoid creating an island of security in the cloud separate from your existing on-prem security investments.



Symantec CloudSOC Audit:
https://www.symantec.com/products/web-and-cloud-security/cloud-application-security-cloudsoc

Symantec ProxySG:
https://www.symantec.com/products/web-and-cloud-security/secure-web-gateway-proxy-sg-and-asg

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016:
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

Opinion 4/2007 on the concept of personal data, Article 29 Data Protection Working Party:
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | **www.symantec.com**

Symc_WP_CloudSOC_GDPR-Compliance_en_v1d

Symantec