Symantec CloudSOC™ Data Science

Feature Brief Series 02

ContentIQ™ DLP

ContentIQ™
Extremely accurate, automated DLP with ContentIQ

CloudSOC with ContentIQ automates high accuracy DLP for you

What if your cloud security automatically identified sensitive content in your cloud apps? What if it was so accurate you didn't worry about missing data or false positives?

What is ContentIQ?

CloudSOC uses ContentIQ to provide governance over the data you have in cloud apps. ContentIQ helps you know what files and accounts contain sensitive, confidential and/or compliance governed content; who has access to that content; which users are associated with that content; and if it is at risk of exposure. ContentIQ includes highly accurate DLP based on a data classification engine that can automatically and accurately identify risky and sensitive types of content. As a result, CloudSOC:

- **Automatically identifies compliance related content such as PII, HIPAA, and PCI with almost no false positives**
- **Automatically identifies sensitive content such as source code, design documents, and legal documents**
- **Tracks sensitive data stored in sanctioned cloud apps including in files, email, messages, databases and notes**
- **Identifies sensitive data in transactions with sanctioned and unsanctioned cloud apps and accounts**
- **Automatically delivers more accurate classification of risky content**
- **Identifies sensitive data at risk of exposure**
- **Enables accurate and granular data governance policies to control access and mitigate risk of exposure**
- **Provides useful data for incident response investigations**

How ContentIQ classifies content

Unlike other systems, ContentIQ can operate without requiring time consuming custom tuning because machine learning powers a sophisticated computational linguistics approach to content analysis to more accurately identify and classify sensitive data. The automated system classifies a robust range of data types covering confidential and regulated data such as personal information, healthcare information, payment card information, financial data, technical content such as source code and design documents, legal documents, etc. The automated classification function of ContentIQ also tracks content that could indicate a risk to your organization such as files that are encrypted or contain macros.

ContentIQ can examine a very broad range of file and field types including documents, data bases, sound and video, graphics, executables, custom forms, and more. It can examine structured, unstructured, and interactive content in emails, messages, notes, storage, and more in the cloud.

The Data Science of ContentIQ

ContentIQ uses data science to tackle DLP employing both unsupervised and supervised machine learning techniques as well as computational linguistics analysis to achieve more accurate content identification and classification.

To accurately identify and classify content you need to know a lot about characteristics that indicate specific types of data. ContentIQ uses newer machine learning techniques and large cloud-based computational resources to identify a far more extensive volume of content indicators than you find in most DLP systems. The ContentIQ classification algorithms use thousands of content indicators and will analyze those indicators in context using sophisticated relationship models to more accurately identify sensitive data.

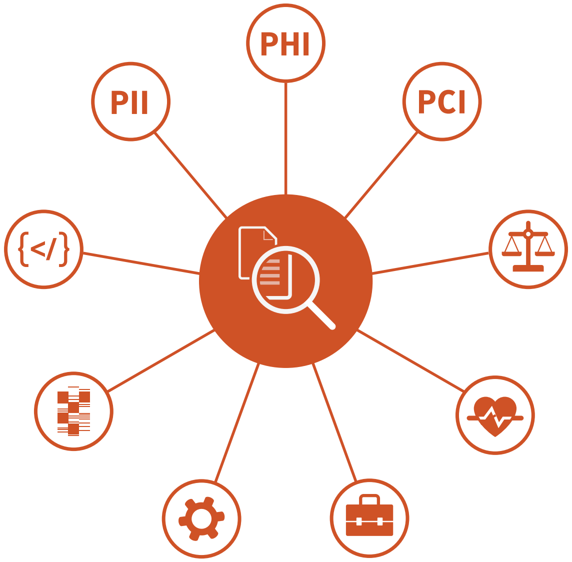
Custom forms and new content types

Some organizations use specific types of data in formats unique to their organization. The same machine learning capabilities used to discover content indicators in publicly available data sources can also be used to discover and leverage content indicators in forms unique to an organization. The ContentIQ learning system is smart enough to require only a few examples of a custom form specific to an organization to enable automatic classification of new types of content.

How ContentIQ handles content at risk

Once ContentIQ has classified a piece of content, CloudSOC identifies if that content is publicly accessible to anyone, shared to a user external to the company, or accessible to anyone in the company. Sensitive content and the user associated with that content is tracked in CloudSOC. Dashboards display what sensitive data is in the cloud and what content is at risk and if that risk of exposure is public, external, or broad across the company.

Policy controls can alert and automatically act to mitigate risk to the company by unsharing, quarantining, or deleting data; blocking data transfers, messages, or emails; or requiring additional levels of user authentication to complete an action.



The Benefits of CloudSOC ContentIQ

Automated visibility and control over confidential data in cloud apps

ContentIQ enables CloudSOC to provide visibility, data security, and threat protection over sensitive content in cloud apps. This API-based capability includes automated classification, monitoring, remediation actions to protect confidential data and mitigate proliferation of malicious files.

Automated DLP for transactions with cloud apps

StreamIQ enables CloudSOC to apply ContentIQ DLP to transactions with both sanctioned and unsanctioned cloud apps and accounts. This important inline CASB service helps prevent data loss by tracking or preventing users from sharing confidential content with unsanctioned cloud services or personal accounts.

Detection and mitigation for content at risk

CloudSOC identifies sensitive data at risk of exposure such as content that can be accessed by the general public, by users external to the company, or broadly by anyone in the company and offers the option to automatically remediate unsafe links and access permissions.

Identification of compromised accounts, malicious insiders, and risky users

CloudSOC User Behavior Analytics considers ContentIQ content analysis when analyzing user behavior. It includes DLP violations in user activity threat maps and when formulating a user ThreatScore. Further details on security incidents include ContentIQ details for incident response and investigations.

Visibility and control over custom forms and new content types

The automated engines of ContentIQ make it fast and easy to track custom forms and new content types with the CloudSOC platform.

Automated policy controls and protective responses

You can create policies in CloudSOC based on app, action, ContentIQ characteristics, user, location, and more. CloudSOC provides granular data on user transactions that can be used to define and trigger automated policies to control access, prevent unsafe uploads or file sharing, prevent proliferation of malware, and more.

Fast and accurate incident investigations

The granular data provided by ContentIQ expands the richness of incident records in the CloudSOC Investigate dashboard making it faster and easier to discover what has happened in order to successfully resolve an incident.

More from the CloudSOC Data Science Feature Brief Series

01

Cloud App Intelligence

CloudSOC Business Readiness Ratings™
Extensive, accurate, timely intelligence on thousands of cloud apps

02

ContentIQ™ DLP

CloudSOC ContentIQ™
Extremely accurate, automated DLP with ContentIQ

03

StreamIQ™ Automation

CloudSOC StreamIQ™
New apps, custom apps, any apps with StreamIQ

04

Detect with UBA

CloudSOC ThreatScore™
Catch attacks and high risk users fast

Better Security, Less Complexity

Deploy a cloud security solution that integrates with your existing security infrastructure. A Symantec solution with CloudSOC provides greater security coverage, reduces operational complexity, and provides an optimal user experience.

Explore Symantec CloudSOC CASB and its industry leading integrations with Symantec Enterprise Security Systems ❯ go.symantec.com/casb

About CloudSOC

The Data Science Powered™ CloudSOC platform empowers companies to confidently leverage cloud applications and s ervices while staying safe, secure and compliant. A range of capabilities delivers 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.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit **www.symantec.com** or connect with us on **Facebook**, **Twitter**, and **LinkedIn**.

Symantec™

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