Symantec

Symantec CloudSOC™ Data Science

Feature Brief Series 03

StreamIQ™ Automation

CloudSOC StreamIQ

New apps, custom apps, any apps with StreamIQ

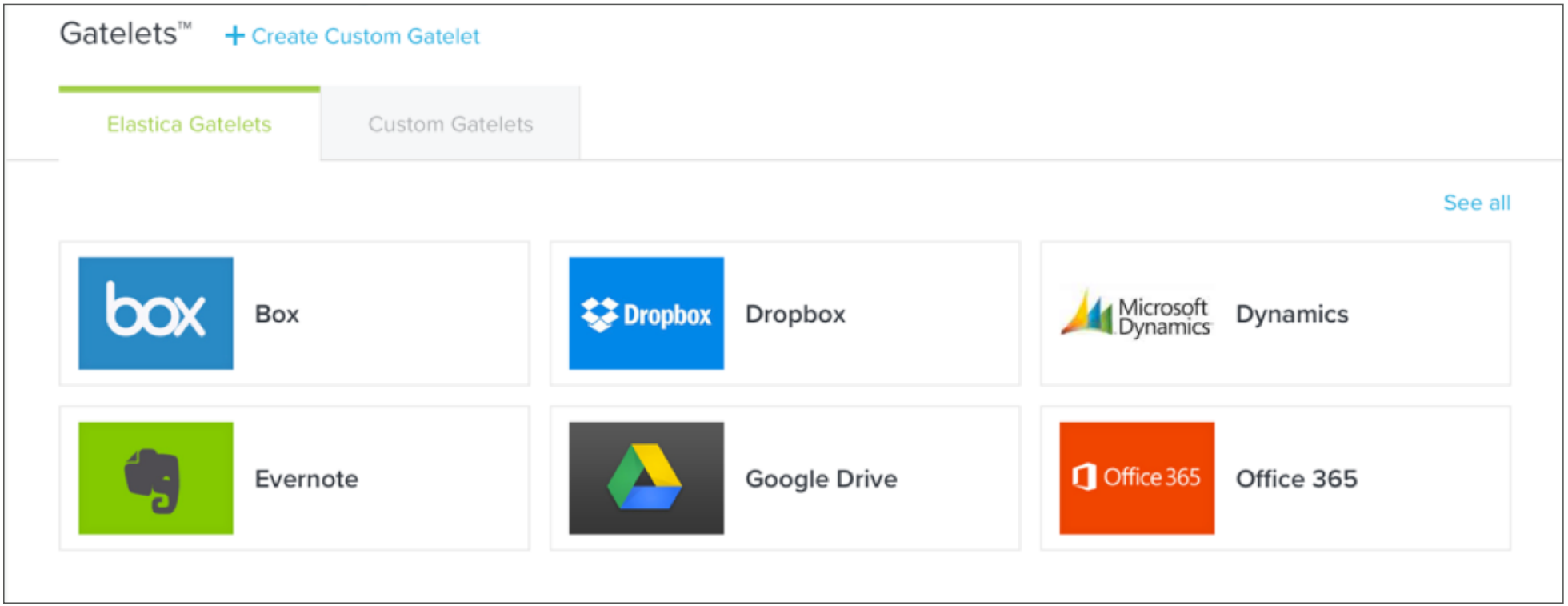
Can your CASB automatically safeguard transactions with any cloud app?

CloudSOC StreamIQ automates visibility and control for new and custom cloud apps

What is StreamIQ?

CloudSOC uses StreamIQ for visibility over how members of your organization are using cloud apps including granular data on the apps, actions, objects, and other characteristics of individual transactions. StreamIQ provides the intelligence and algorithms that fuel cloud app traffic analysis in CloudSOC. StreamIQ leverages multiple machine learning engines to deliver automated and accurate real-time activity tracking for any cloud app. As a result, CloudSOC delivers:

- **Granular detail on transactions in live traffic between users and cloud apps**
- **Analysis of traffic for more apps – for both sanctioned and unsanctioned accounts**
- **Visibility and control over transactions with new and custom apps**
- **Automatic ability to accommodate cloud app code changes to maintain accuracy**
- **More accurate risk analysis as a result of more extensive activity intelligence**
- **More granular policy controls over more apps, more actions, and more objects**
- **More useful data for successful incident response investigations**



Quickly Add New & Custom Apps

The CloudSOC CASB Gateway service uses StreamIQ for inline analysis of traffic with cloud apps. CloudSOC users can quickly activate new apps and custom apps directly from the CloudSOC platform. A data science built universal interpreter function in StreamIQ automatically enables CloudSOC to perform inline analysis of the new app traffic. Unlike other systems, StreamIQ can operate without requiring time consuming custom signature tuning by the end user.

The Data Science of StreamIQ

StreamIQ uses both unsupervised and supervised machine learning to analyze cloud app traffic. Significant characteristics associated with important traffic attributes are targeted and unsupervised machine learning identifies significant instructions in machine code. Supervised machine learning systems use knowledge of these instructions to build content and contextual intelligence. This knowledge powers StreamIQ algorithms that understand the unique machine code for individual cloud apps at a very granular level. Furthermore, aggregated analysis of machine code across a wide range of different cloud app transactions is used to create a universal interpreter function for StreamIQ, enabling CloudSOC to automatically recognize fundamental user actions in cloud transactions with new and custom cloud apps.

The Benefits of StreamIQ

Visibility and control over custom apps, new apps, and changing apps
StreamIQ enables CloudSOC to provide visibility, data security, and threat protection over nearly any cloud app. The automated engines of StreamIQ make it easy to add custom apps and new apps to the CloudSOC platform without having to build time consuming custom signatures.

Detect high risk users and compromised accounts
All that granular user transaction data analyzed by StreamIQ is fed to the CloudSOC User Behavior Analytics system. It fuels the creation of custom user behavior profiles and provides data for user activity threat maps and the user ThreatScore features of CloudSOC.

DLP for transactions with cloud apps
StreamIQ visibility enables CloudSOC to apply DLP to transactions with both sanctioned and unsanctioned cloud apps and accounts. This important inline CASB service helps prevent data loss.

Automated policy controls and protective responses
You can create policies in CloudSOC based on app, action, object, data classification, user, location, and more. StreamIQ 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 transaction data provided by StreamIQ greatly 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**

Symc_FB_CloudSOC_DataScienceSeries_en_v1d