Symantec

Symantec CloudSOC™ Data Science

Feature Brief Series 01

Cloud App Intelligence

Business Readiness Ratings™

Extensive, accurate, timely intelligence on thousands of cloud apps

What do you know about the cloud apps you use?

- Business readiness?
- Risk attributes?
- Data location?
- Breaches?

What if you had up-to-date intelligence for thousands of apps based on millions of data points whenever you needed it?

CloudSOC keeps you up-to-date with Business Readiness Ratings.

CloudSOC maintains a data science driven intelligence system to analyze and compare cloud apps for business use. CloudSOC intelligence covers thousands of cloud and mobile apps, tracks more than 120 significant risk attributes for each app, and uses this granular intelligence to assign a Business Readiness Rating to each app. This system enables customers to quickly perform a risk analysis of the cloud apps they use, confirm that cloud apps meet specific requirements, and compare cloud apps delivering similar services for security informed decision making. CloudSOC cloud app intelligence and Business Readiness Ratings are regularly checked and updated to keep this critical information fresh and accurate. As a result, CloudSOC delivers:

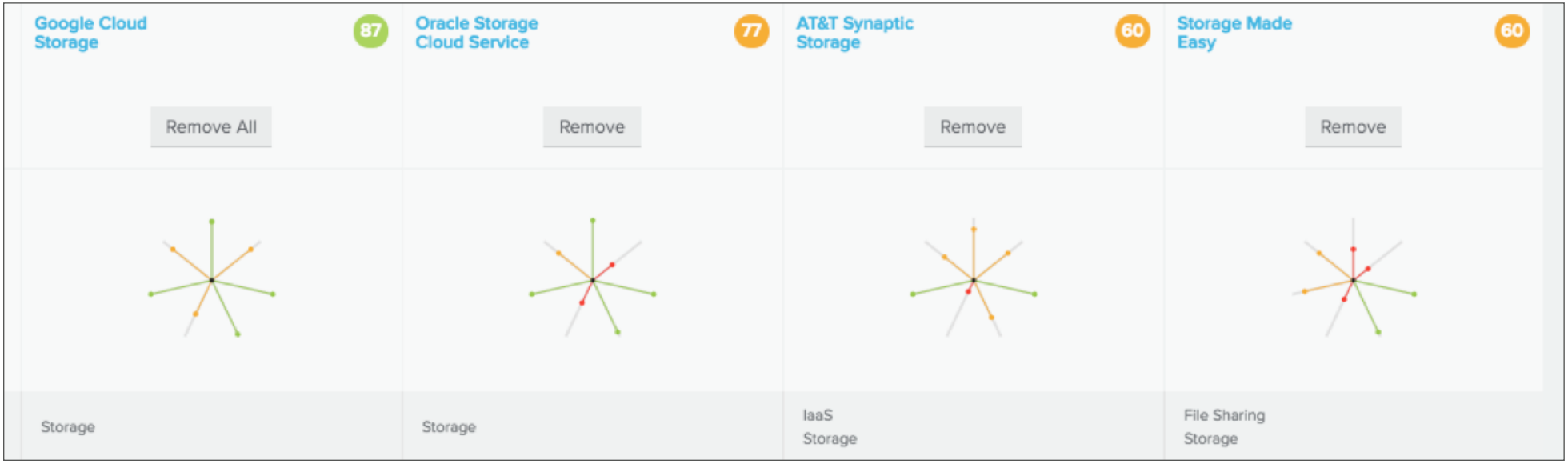
- **Automatic detection of thousands of cloud and mobile apps in CloudSOC Audit Shadow IT mwonitoring and in CloudSOC Securlets as integrated third party apps**
- **Granular data on risk and business attributes for thousands of cloud and mobile apps**
- **Individualized and customizable Business Readiness Ratings for fast identification of high risk apps**
- **Direct comparisons of similar cloud apps for analysis of respective risk attributes**
- **Automated reports on risky apps, risky users, and volume use of apps**
- **Integration via the Symantec Global Intelligence Network with Symantec Secure Web Gateway solutions ProxySG and Web Security Service for automated policies based on CloudSOC app intelligence and ratings**

Access	92	95	77
Federated Identity Management	100	100	100
OAuth support	✓	✓	×
OpenID support	×	×	×
SAML support	✓	✓	✓
Brute-force Protection	100	100	1
Protection from multiple failed logins	Account Lockout	Account Lockout	None
Utilizes CAPTCHA	✓	×	×
Multi-factor Authentication	100	100	100
Multi-factor authentication - Security Questions	×	✓	×
Multi-factor authentication via Biometrics	×	×	×
Multi-factor authentication via Mobile App	✓	✓	✓
Multi-factor authentication via Others	✓	×	×
Multi-factor authentication via secondary email	×	×	×
Multi-factor authentication via Smartcard	×	×	×
Multi-factor authentication via SMS	✓	✓	×
Multi-factor authentication via USB Token	✓	×	×
Password Quality Rules	80	100	80
Does not save logged in session	✓	✓	✓
Force change of password after some time period	×	✓	×
Provides password reset and recovery	✓	✓	✓
Requires minimum password length	✓	✓	✓
Requires strong password format	✓	✓	✓

Cloud service risk attributes

CloudSOC analysts use machine-learning to discover apps and analyze them for more than 100 different business and risk attributes including items associated with access controls, regulatory compliance, data security, business model, and security vulnerabilities. With this detailed data on the business and risk attributes of cloud apps at hand, if you identify a cloud app of interest, you can find out what specific risks might be associated with using that app and if there are attributes that make that app a particularly good or bad choice for your users.

By leveraging machine learning CloudSOC analysts can research and maintain an up-to-date databased with millions of data points for granular intelligence on thousands of cloud apps. Every app exposes attributes in a unique way, making it necessary to build smart discovery tools able to scan and identify critical attribute information from a cloud app based on source material that varies widely. This requires a system able to analyze expressions, keywords, and machine code details from multiple sources and then consider them in context to confidently identify that an app does or does not have a specific attribute and key details about that specific attribute. CloudSOC analysts are able to review extensive volumes of data associated with cloud apps by leveraging data science techniques such as supervised machine learning to explore and analyze many different sources of information.

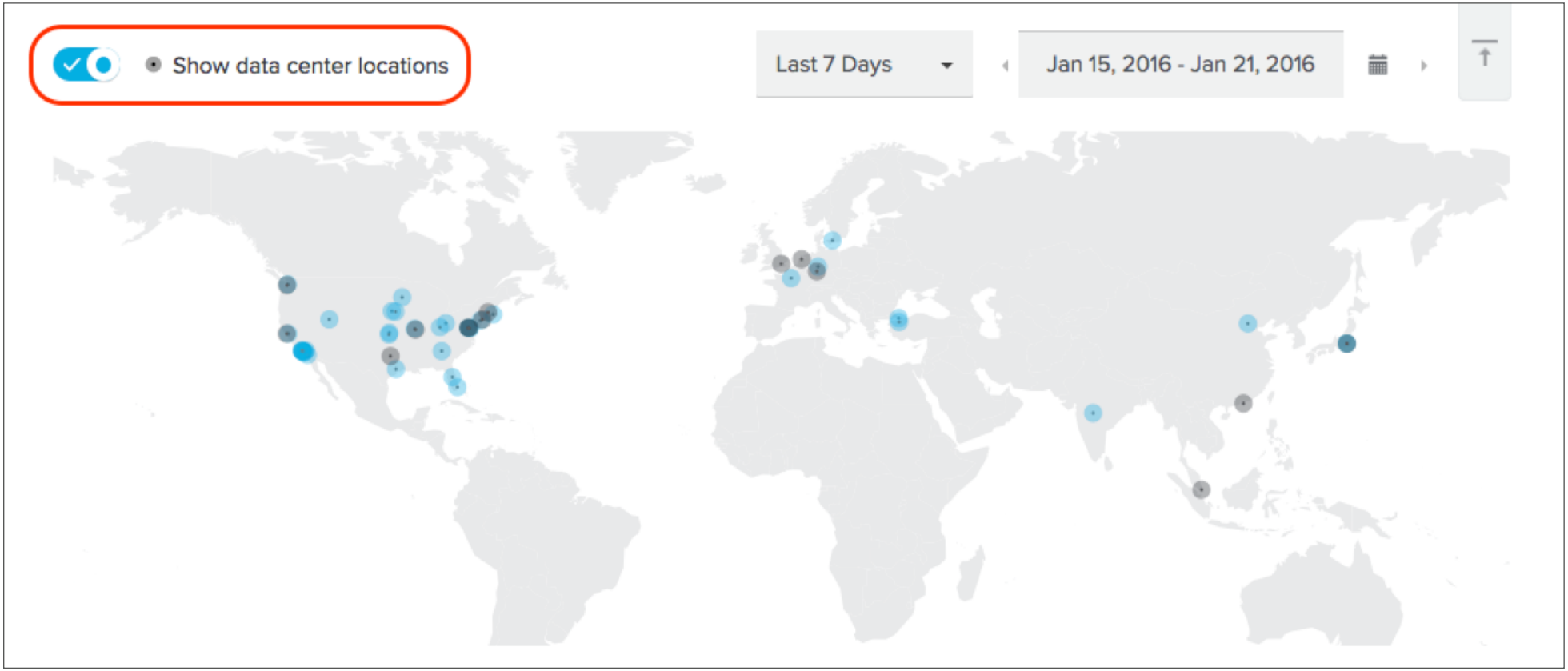


Business Readiness Ratings

Sometimes you need to make decisions fast. CloudSOC mines its extensive cloud app intelligence database to calculate a Business Readiness Rating for each app so you can make at-a-glance decisions and automate policy controls to enable or restrict the use of cloud apps that may not meet your security requirements. The CloudSOC system uses computational analysis and machine learning algorithms to analyze attribute findings, evaluate their overall significance based on customizable priorities, and dynamically generate numerical ratings on a scale of 1-99.

With these standardized numerical ratings that measure and compare relative risk levels you can:

- **Quickly identify apps with high ratings to review for sanctioned, strategic use,**
- **Quickly identify apps with low ratings that may pose a problem for your organization,**
- **Easily compare apps that perform similar functions to find the best one to standardize on for your**



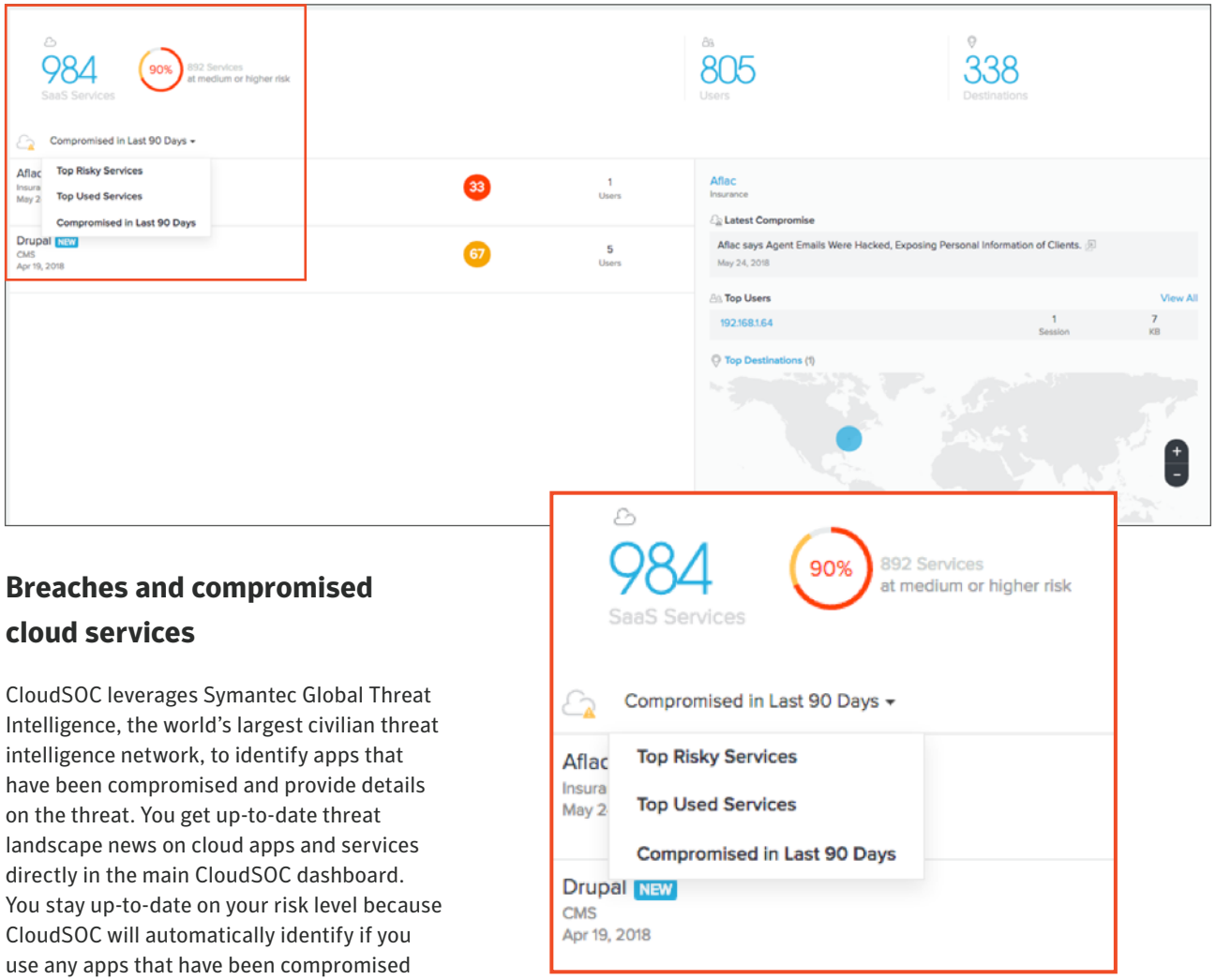
Accurate data locations

CloudSOC uses a unique method to track the location of datacenters for cloud apps. Unlike other solutions, CloudSOC monitors traffic in-motion that is associated with cloud apps and identifies datacenter locations based on patterns of data flow. The system uses a heuristics engine based on machine learning to identify and compile a record of associated GeoIP addresses. These records are then used by CloudSOC Audit to display an extensive list of datacenter locations associated with individual cloud apps.

Since CloudSOC relies on real traffic flow to identify locations, it delivers more accurate, more comprehensive, and more granular information on where data is located. Other CASB solutions rely on public records and self reporting by cloud applications to document datacenter locations. This methodology is good for identifying key data repositories but won't identify data that travels to secondary datacenter locations due to embedded first or third party services such as content syndication, ad services, traffic management, or other dynamic infrastructure services.

The benefits of cloud app intelligence

- Automatically detect shadow IT use of risky cloud apps
- Track risky apps integrated with cloud services such as Microsoft Office 365 and Google G Suite
- Perform a side-by-side risk analysis of cloud apps delivering similar services
- Regularly monitor, report, and respond to the use of risky or compromised cloud services
- Automate visibility and control over access to cloud apps based on risk attributes and ratings



Breaches and compromised cloud services

CloudSOC leverages Symantec Global Threat Intelligence, the world's largest civilian threat intelligence network, to identify apps that have been compromised and provide details on the threat. You get up-to-date threat landscape news on cloud apps and services directly in the main CloudSOC dashboard. You stay up-to-date on your risk level because CloudSOC will automatically identify if you use any apps that have been compromised and can alert you. CloudSOC can also automatically downgrade the Business Readiness Rating for cloud services that have been recently compromised to help you automate your response actions.

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