CASB

Cloud Access Security Broker

Symantec

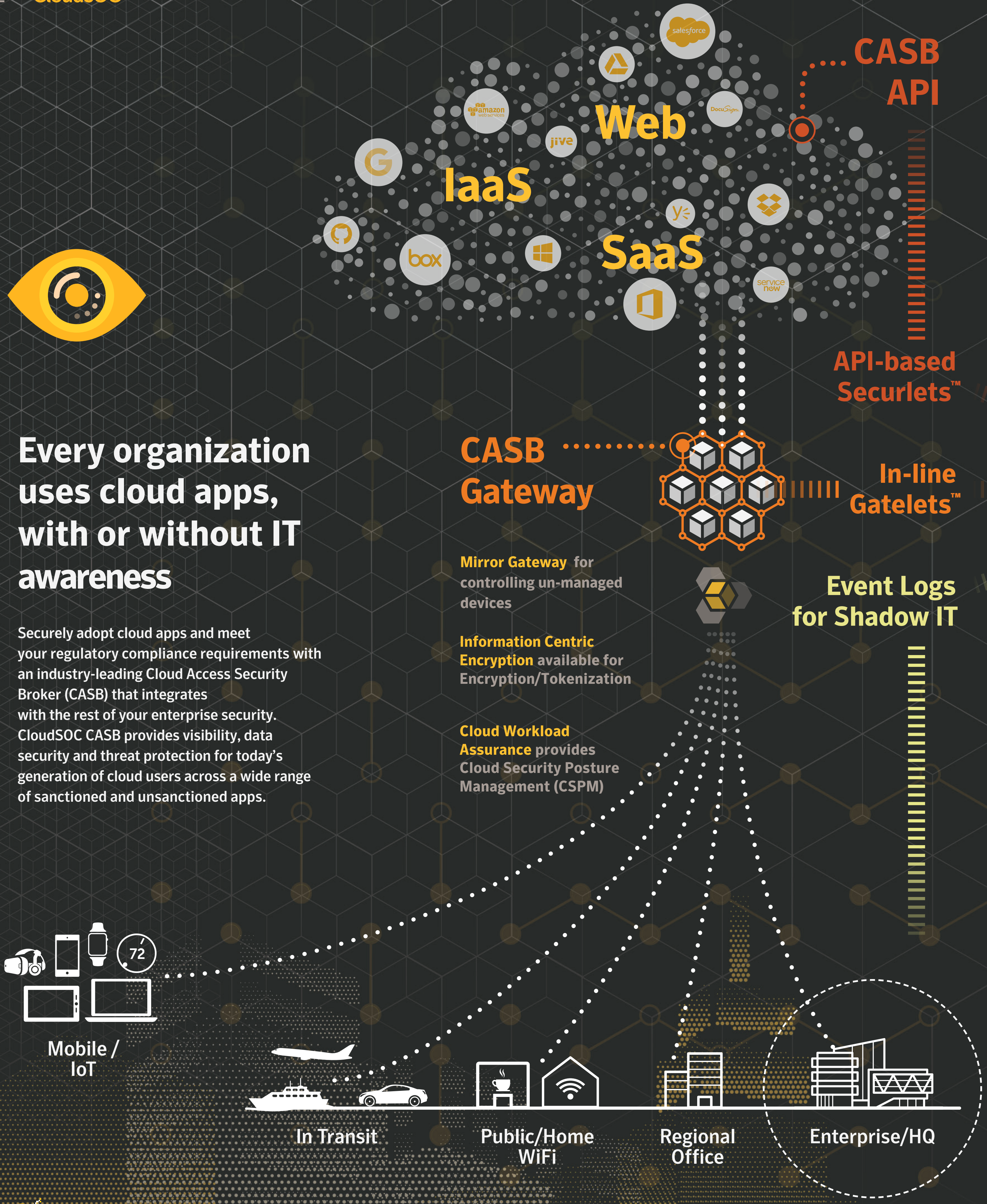
Secure use of cloud apps & services

CloudSOC

visibilty. control. protection.

Every organization uses cloud apps, with or without IT awareness

Securely adopt cloud apps and meet your regulatory compliance requirements with an industry-leading Cloud Access Security Broker (CASB) that integrates with the rest of your enterprise security. CloudSOC CASB provides visibility, data security and threat protection for today's generation of cloud users across a wide range of sanctioned and unsanctioned apps.



Mirror Gateway for controlling un-managed devices

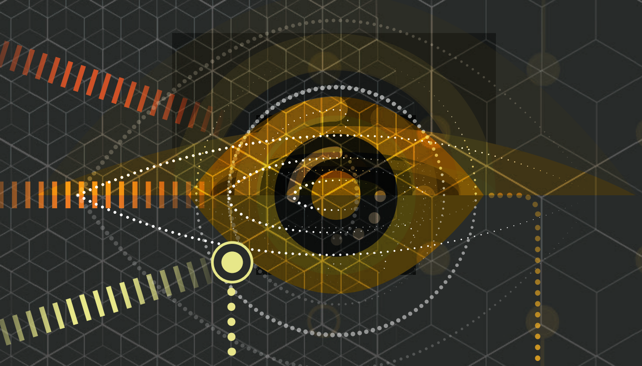
Information Centric Encryption available for Encryption/Tokenization

Cloud Workload Assurance provides Cloud Security Posture Management (CSPM)

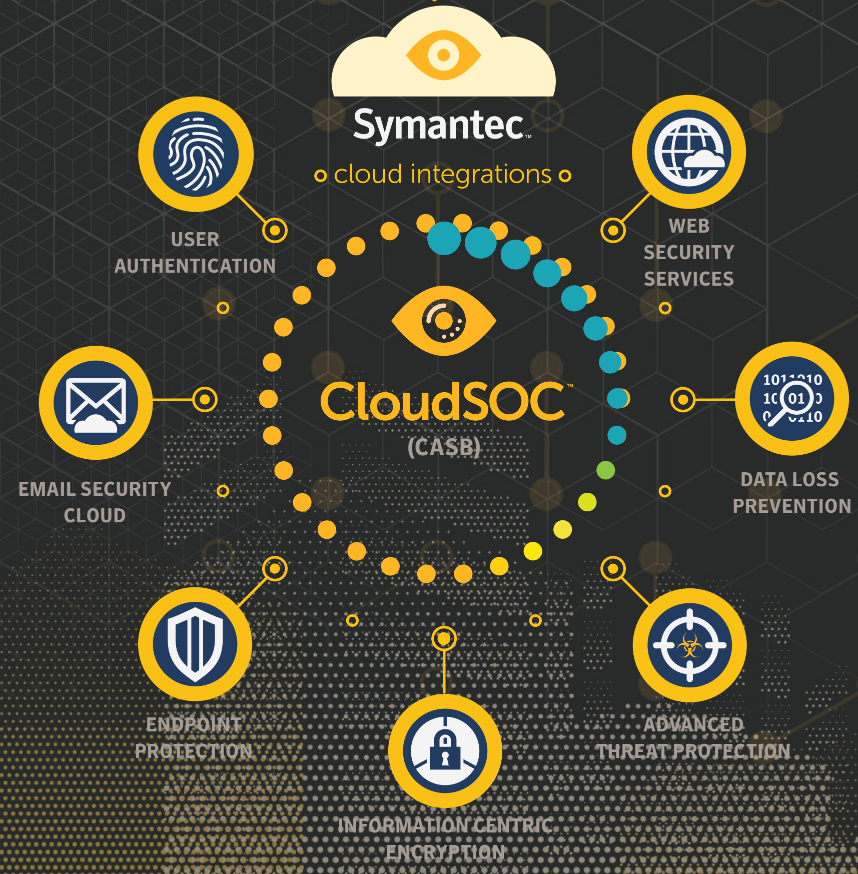
Symantec.

CloudSOC™

visibilty. control. protection.



CASB Audit



Symantec.
cloud integrations

CloudSOC™
(CASB)

USER AUTHENTICATION

WEB SECURITY SERVICES

EMAIL SECURITY CLOUD

DATA LOSS PREVENTION

ENDPOINT PROTECTION

ADVANCED THREAT PROTECTION

INFORMATION CENTRIC ENCRYPTION

Cloud App Visibility

Discovers and controls the use of Shadow IT.

Data Security

Identifies, classifies and controls sensitive, compliance-related and confidential data at risk of exposure in the cloud.

Threat Protection

Identifies high-risk user behavior and controls threats in cloud apps.

Incident Response

Quickly investigate areas of concern in cloud accounts with rich log-based intelligence.

Cloud App Visibility

Analyze risk attributes and the business readiness of individual cloud apps

Identify cost savings through optimizing cloud subscriptions

Track use of cloud apps, risky users, and risky activity

Coach users to adhere to corporate policies for cloud usage

Deliver regular reports on cloud activity for security and compliance

Discover and control use of Shadow IT with CloudSOC Audit

SITUATION

Shadow IT use of cloud apps introduces compliance and security risk. Typical enterprises find hundreds of cloud apps in use, but most of these services are not business ready, do not meet compliance requirements, and have zero security oversight.

SOLUTION

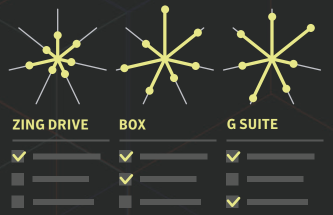
Gain visibility over all the cloud services used in your organization and identify risk and compliance issues. Make smart decisions on what apps to sanction, subscriptions to streamline, and controls to enforce on the use of risky apps.

Know Your Cloud Apps

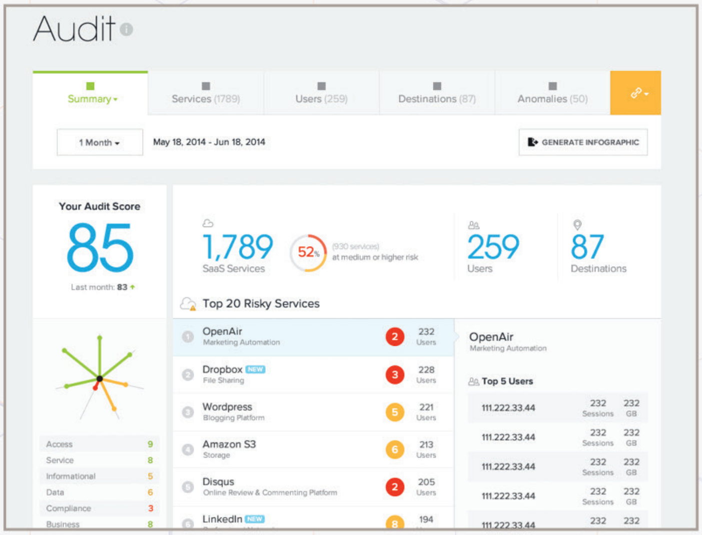
Extensive Cloud App Intelligence

The cloud app intelligence in Audit makes it easy to compare similar cloud services, identify and standardize on the best platforms for your business, and automate controls to mitigate the risk of using unsanctioned cloud apps.

- Extensive identification and research for ten's of thousands of cloud apps
- Detailed intelligence on more than 100 different risk attributes for each cloud service



- Automatic and customizable Business Readiness Ratings™ for each application



Audit

May 18, 2014 - Jun 18, 2014

Your Audit Score 85

Last month: 83

1,789 SaaS Services

52% (930 services) at medium or higher risk

259 Users

87 Destinations

Access	9
Service	8
Informational	5
Data	6
Compliance	3
Business	8

Top 20 Risky Services

1	OpenAir Marketing Automation	2	232 Users
2	Dropbox NEW File Sharing	3	228 Users
3	Wordpress Blogging Platform	5	221 Users
4	Amazon S3 Storage	6	213 Users
5	Disqus Online Review & Commenting Platform	2	205 Users
6	LinkedIn NEW	8	194

OpenAir
Marketing Automation

Top 5 Users

111.222.33.44	232 Sessions	232 GB
111.222.33.44	232 Sessions	232 GB
111.222.33.44	232 Sessions	232 GB
111.222.33.44	232 Sessions	232 GB
111.222.33.44	232	232

How CloudSOC Analyzes Cloud App Usage

- Discovers Shadow IT by analyzing event logs from firewalls, proxies, and other systems
- Analyzes Shadow IT in use with intelligence on the risks associated with individual cloud services
- Monitors Shadow IT usage through intuitive dashboards and reports
- Generates risk assessments on demand—a key requirement for most compliance regulations
- Automates control over use of cloud apps through integration with Symantec secure web gateways

Request a free Cloud Services Risk Assesment Report.

An Integrated Security System

Get Unique Shadow IT Control with SWG Integration

Audit integrates with Symantec's ProxySG and Web Security Service (WSS) to add app visibility to your SWG, and enable dynamic policy enforcement based on risk metrics governing the use of cloud apps by members of your organization.

Get Greater Visibility with SEP Integration

Audit integration with Symantec Endpoint Protection adds visibility of Shadow IT usage by remote employees in addition to the visibility provided by enterprise firewall and proxy logs.

Streamline Management with Integrated Policies & Architecture

Automate and coordinate visibility and control over Shadow IT use with integrated cloud app intelligence, universal secure web gateway policies, and an architecture designed to support a web and cloud security system.

Data Security

Classify and track compliance-related and confidential data such as PII, PHI, source code, legal, health, and more automatically

Identify users associated with sensitive data at risk

Monitor and mitigate risk of exposure for sensitive data

Apply global policies to control access to data and transactions with cloud apps

Encrypt sensitive content being uploaded to the cloud

Protect your data in the cloud with CloudSOC

SITUATION

Cloud services make it easy to collaborate.
They also make it easy to expose or lose sensitive, confidential, or compliance-related data. A typical organization broadly shares more than 20% of files in cloud apps—either to the public, to the entire organization or to an external party.[1] Some of these files will contain confidential data.

SOLUTION

Prevent Data Loss in the Cloud with CloudSOC
by identifying sensitive data, monitoring data at risk, encrypting sensitive content, and enforcing policy controls to prevent data breach.

Know Your Cloud Data

SSN PII

PHI

PCI

ContentIQ™

Data Science Engine for DLP

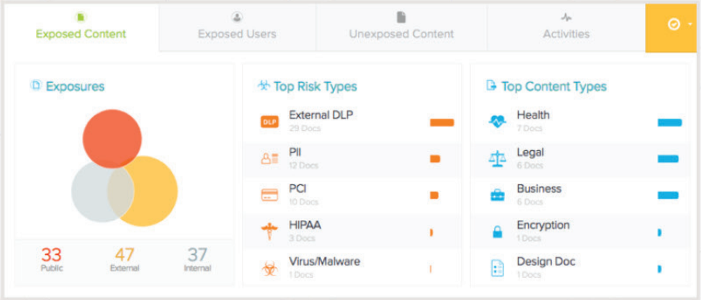
- Highly accurate data classification powered by a machine-learning system
- Contextual-analysis and computational linguistics identify more content without false positives than simple Regex matching alone
- Automatic classification of data and file types
- Extensive dictionaries—automated and customizable
- Self-training system learns to identify custom documents

[1] *Source: 2H 2016 Shadow Data Report, Symantec*

Symantec.

How CloudSOC Secures Data in the Cloud

- Scans content and automatically classifies data with highly accurate DLP
- Monitors sensitive data and remediates risky exposures identified in cloud apps
- Leverages both API-based Securlets™ for sanctioned SaaS and IaaS accounts and CASB Gateway for real-time traffic between users and cloud apps
- Enforces rich content-aware and context-aware policies to govern transactions, including encryption of sensitive content
- Integrates with Symantec DLP to extend central enterprise DLP policies and workflows to cloud apps



Exposures

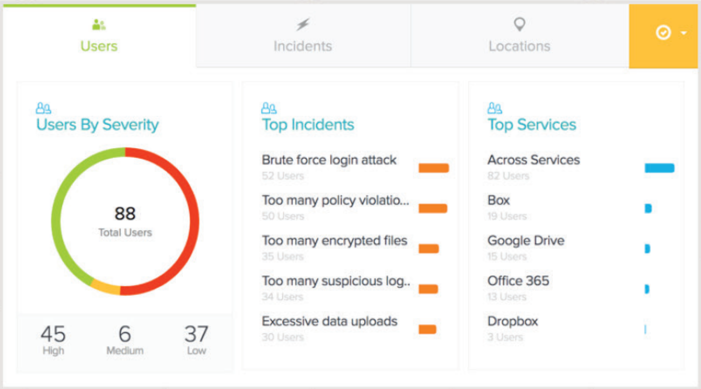
33 Public · 47 External · 37 Internal

Top Risk Types

- External DLP — 29 Docs
- PII — 12 Docs
- PCI — 10 Docs
- HIPAA — 3 Docs
- Virus/Malware — 1 Docs

Top Content Types

- Health — 7 Docs
- Legal — 6 Docs
- Business — 6 Docs
- Encryption — 1 Docs
- Design Doc — 1 Docs



Users By Severity

88 Total Users

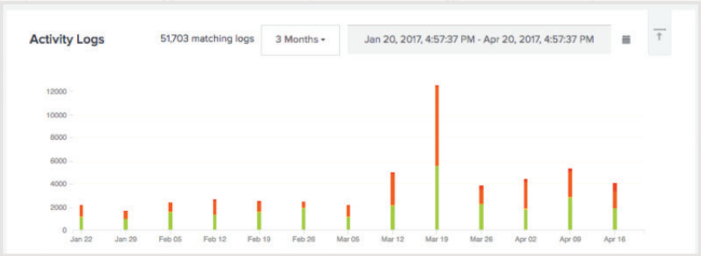
45 High · 6 Medium · 37 Low

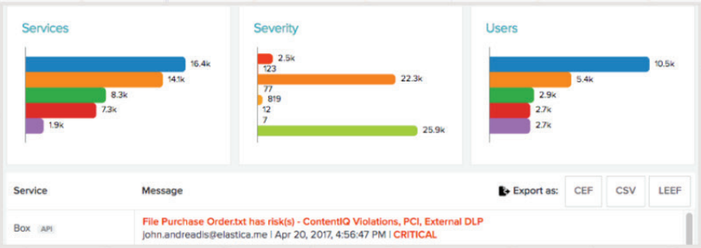
Top Incidents

- Brute force login attack — 52 Users
- Too many policy violatio... — 50 Users
- Too many encrypted files — 35 Users
- Too many suspicious log.. — 34 Users
- Excessive data uploads — 30 Users

Top Services

- Across Services — 82 Users
- Box — 19 Users
- Google Drive — 15 Users
- Office 365 — 13 Users
- Dropbox — 3 Users


Activity Logs 51,703 matching logs 3 Months ▾ Jan 20, 2017, 4:57:37 PM - Apr 20, 2017, 4:57:37 PM



Service	Message
Box API	File Purchase Order.txt has risk(s) - ContentIQ Violations, PCI, External DLP john.andreadis@elastica.me I Apr 20, 2017, 4:56:47 PM I CRITICAL

An Integrated Security System

Data Loss Prevention with integrated CloudSOC and Symantec DLP

Safeguard data in cloud apps with the same DLP policies and response workflows you use for your endpoints, networks, and data centers by using CloudSOC integration with Symantec DLP in the cloud.

Protect Confidential Data with integrated CloudSOC and Symantec Encryption

Automatically encrypt sensitive files in cloud apps and manage access to those files with integrated Symantec Encryption by PGP or SafeNet.

Protect Data in Motion and Resting with Symantec Information Centric Encryption

Content is beaconized, allowing you to track wherever it travels. At any point in time, you can revoke the file so that nobody can access it, regardless of how many copies exist.

Threat Protection

- Detect malicious user activity in context with one or more cloud apps
- Identify and enforce policies based on elevated threat levels and high risk activity
- Mitigate malware and advanced threat attacks
- Block or quarantine compromised accounts

Detect and remediate threats in cloud apps with CloudSOC

SITUATION

Cloud accounts are often accessible directly from the internet, introducing a new threat vector. Bad actors target user accounts to gain direct access to sensitive content and infiltrate an organization. In addition, users connecting to accounts with malware infected devices can inadvertently infect the broader organization or cause a data breach.

SOLUTION

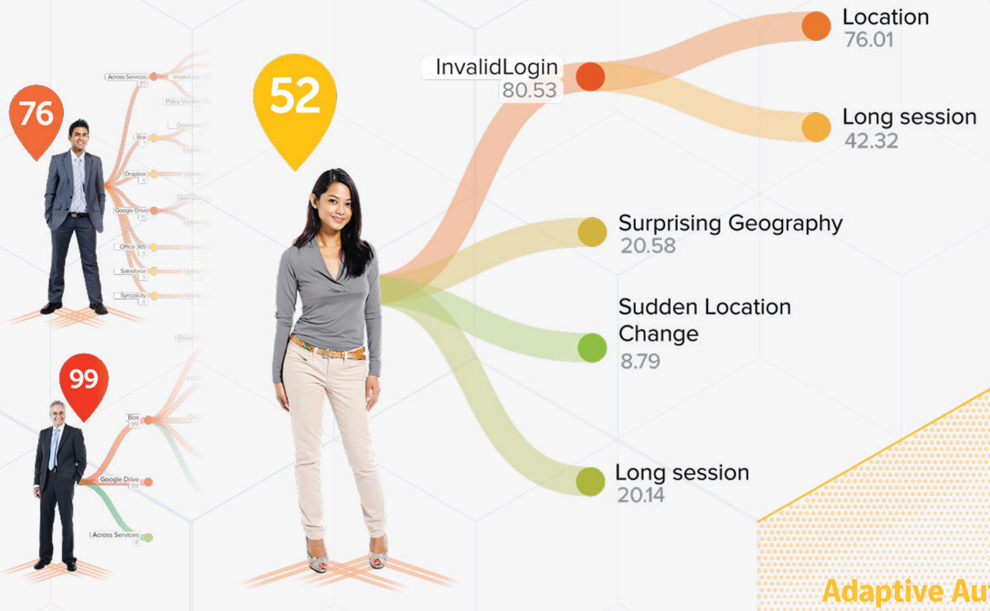
Protect your organization from threats in cloud account with controls based on data science powered User Behavior Analytics (UBA) and integrated malware protection.

Know Your Cloud Risk

User Behavior Analytics and ThreatScore™

The risk level of a user's behavior is quantified with a numerical ThreatScore. A high ThreatScore indicates risky and potentially malicious activity. You can identify the risk level for a user at-a-glance, trigger an alert, or enforce a policy control with this useful system.

- Individualized and contextualized user behavior profiles based on machine-learning
- Highly accurate data science driven identification of abnormal user activity
- Visual maps of user actions, policy violations, and threats across services
- Track complex sequence of events indicative of data exfiltration



How CloudSOC Protects Against Threats

- Identifies, logs and maps abnormal and high risk activity
- Tracks individual user activity and assigns a real-time user ThreatScore
- Enforces policies based on ThreatScore to alert, quarantine or block activity
- Scans content in cloud apps for malware and remediates
- Leverages both API-based Securlets for sanctioned SaaS and IaaS accounts and CASB Gateway for real-time traffic between users and cloud apps

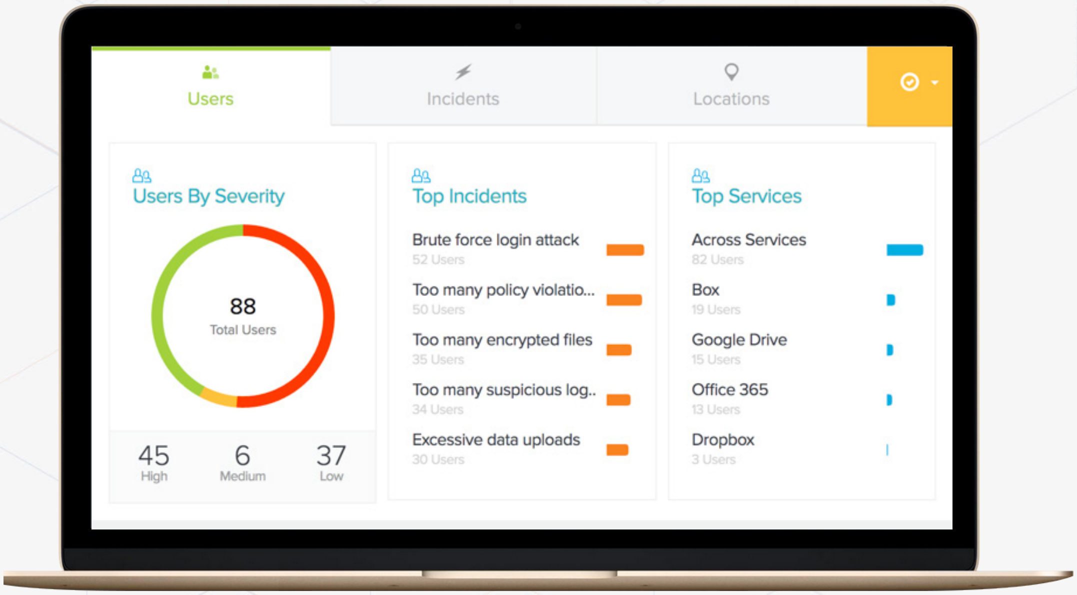
An Integrated Security System

Adaptive Authentication with integration of Symantec VIP

Control access to cloud accounts with identity management, single sign-on, and multifactor authentication solutions. CloudSOC offers deeper integration with Symantec VIP to apply adaptive multi-factor authentication to prevent bad actors from accessing cloud accounts even if login credentials are stolen or hacked.

Malware & Threat Protection with integrated Symantec ATP

CloudSOC offers flexible integration with anti-malware and advanced threat protection solutions to identify and remediate malware infections. Integration with Symantec ATP delivers file reputation analysis, A/V scanning and advanced threat sandboxing to all your cloud content.



Users By Severity

88 Total Users

45 High | 6 Medium | 37 Low

Top Incidents

Brute force login attack	52 Users
Too many policy violatio...	50 Users
Too many encrypted files	35 Users
Too many suspicious log..	34 Users
Excessive data uploads	30 Users

Top Services

Across Services	82 Users
Box	19 Users
Google Drive	15 Users
Office 365	13 Users
Dropbox	3 Users

Incident Response

Use granular insights into cloud activity for post-incident analysis

Quickly find critical information with free-form search, extensive filters and pivot tables

Monitor activity with customizable dashboards and reports

Integrate with SIEM products for additional analysis

Symantec.

Investigate and respond to incidents with CloudSOC

SITUATION

Security incidents happen.

The more you know about your activity in the cloud, the more you can do to protect your organization.

SOLUTION

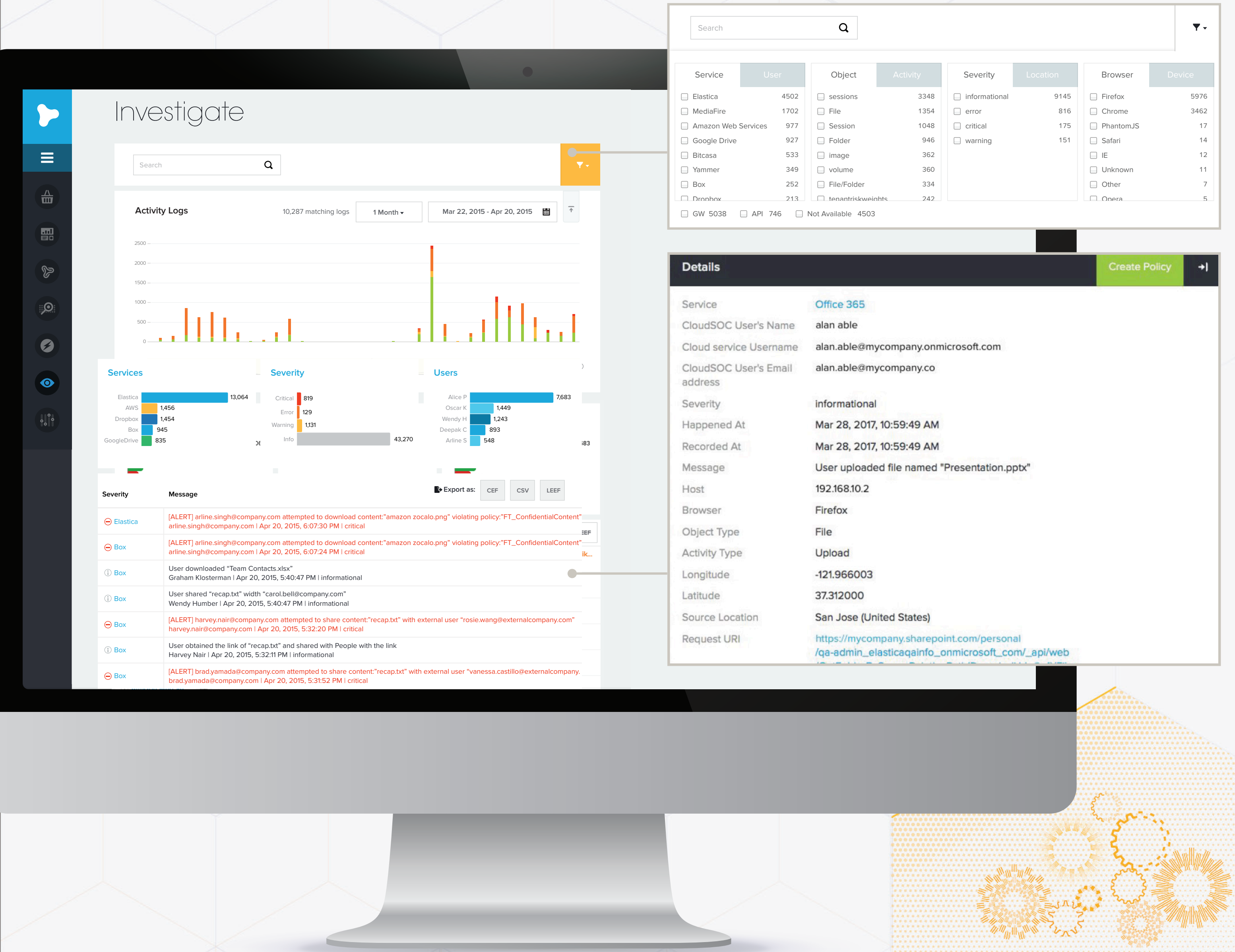
Quickly investigate areas of concern with rich log-based intelligence.

The Investigate function makes the intelligence of CloudSOC accessible to you through easily searched and filtered logs documenting cloud transactions based on users, files, apps, actions, and more. Investigate presents data graphically for fast analysis and offers consolidated summary logs for an instant review of relevant activity.

Know Your Cloud History

StreamIQ™ *delivers granular transaction details*

- Data science driven engine that translates real-time traffic and API data into granular log data that's easy to understand and act on
- Covers unlimited cloud apps in granular detail
- Granular details on what actions were taken (upload, download, share, delete, etc)
- Identification of which user, what objects, and what content was involved



Service	User	Object	Activity	Severity	Location	Browser	Device
□ Elastica	4502	□ sessions	3348	□ informational	9145	□ Firefox	5976
□ MediaFire	1702	□ File	1354	□ error	816	□ Chrome	3462
□ Amazon Web Services	977	□ Session	1048	□ critical	175	□ PhantomJS	17
□ Google Drive	927	□ Folder	946	□ warning	151	□ Safari	14
□ Bitcasa	533	□ image	362			□ IE	12
□ Yammer	349	□ volume	360			□ Unknown	11
□ Box	252	□ File/Folder	334			□ Other	7
□ Dropbox	213	□ tenantriskweights	242			□ Opera	5

□ GW 5038 □ API 746 □ Not Available 4503

Severity	Message
⊖ Elastica	[ALERT] arline.singh@company.com attempted to download content:”amazon zocalo.png” violating policy:”FT_ConfidentialContent” arline.singh@company.com I Apr 20, 2015, 6:07:30 PM I critical
⊖ Box	[ALERT] arline.singh@company.com attempted to download content:”amazon zocalo.png” violating policy:”FT_ConfidentialContent” arline.singh@company.com I Apr 20, 2015, 6:07:24 PM I critical
ⓘ Box	User downloaded “Team Contacts.xlsx” Graham Klosterman I Apr 20, 2015, 5:40:47 PM I informational
ⓘ Box	User shared “recap.txt” width “carol.bell@company.com” Wendy Humber I Apr 20, 2015, 5:40:47 PM I informational
⊖ Box	[ALERT] harvey.nair@company.com attempted to share content:”recap.txt” with external user “rosie.wang@externalcompany.com” harvey.nair@company.com I Apr 20, 2015, 5:32:20 PM I critical
ⓘ Box	User obtained the link of “recap.txt” and shared with People with the link Harvey Nair I Apr 20, 2015, 5:32:11 PM I informational
⊖ Box	[ALERT] brad.yamada@company.com attempted to share content:”recap.txt” with external user “vanessa.castillo@externalcompany. brad.yamada@company.com I Apr 20, 2015, 5:31:52 PM I critical

Details

Service	Office 365
CloudSOC User's Name	alan able
Cloud service Username	alan.able@mycompany.onmicrosoft.com
CloudSOC User's Email address	alan.able@mycompany.co
Severity	informational
Happened At	Mar 28, 2017, 10:59:49 AM
Recorded At	Mar 28, 2017, 10:59:49 AM
Message	User uploaded file named "Presentation.pptx"
Host	192.168.10.2
Browser	Firefox
Object Type	File
Activity Type	Upload
Longitude	-121.966003
Latitude	37.312000
Source Location	San Jose (United States)
Request URI	https://mycompany.sharepoint.com/personal /qa-admin_elasticaqainfo_onmicrosoft_com/_api/web

An Integrated Security System

How CloudSOC Investigates Incidents

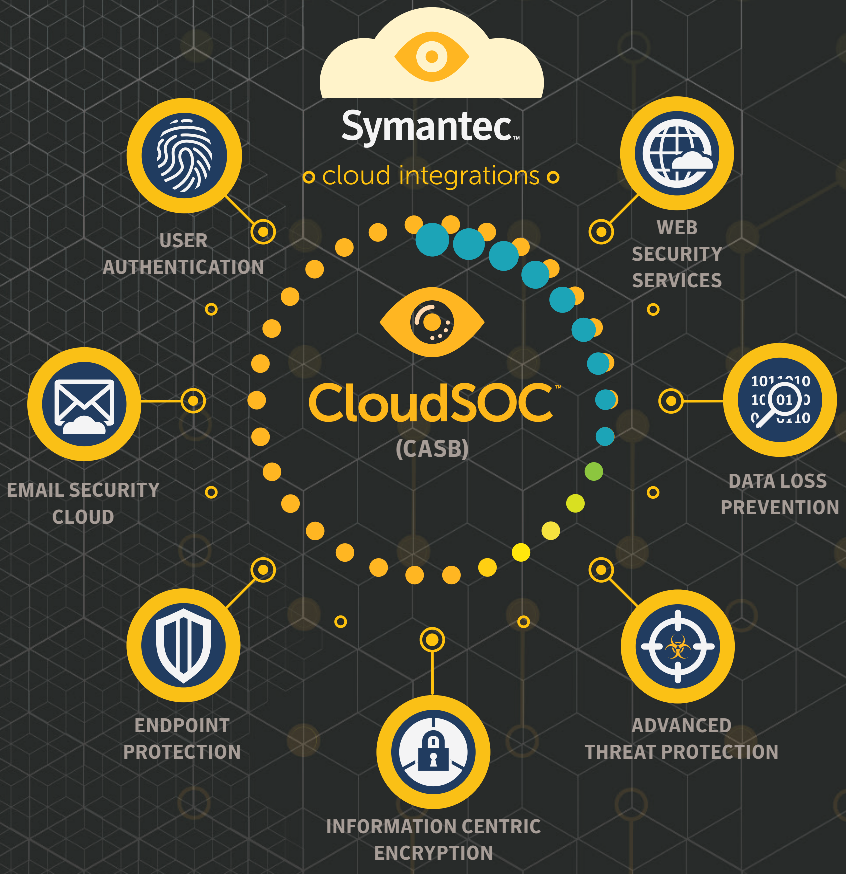
- Logs user activity in traffic between users and cloud apps via CASB Gateway and via API-based Securlets for sanctioned SaaS and IaaS accounts
- Displays graphs and consolidated log reports based on free-form search and filters
- Expands to share detailed log data on users, files, apps and actions
- Exports data to your favorite SIEM for further analysis

Incident Response with SIEMs

Log files from Investigate are easily exported to your SIEM for further analysis.

Secure your entire enterprise

The cloud is part of your organization's infrastructure. Solve your cloud security needs with a system that integrates with the rest of your enterprise security.



For more info on Symantec CloudSOC CASB and its industry leading integrations with Symantec Enterprise Security Systems, visit **go.symantec.com/casb**

About CloudSOC

Data Science-Powered™ Symantec CloudSOC CASB platform lets organizations confidently engage cloud apps and services while staying safe, secure and compliant. A range of capabilities on the CloudSOC platform deliver the full life cycle of cloud application security, including auditing of shadow IT, user behavior detection, real-time detection of intrusions and threats, protection against data loss, as well as examination and prevention of compliance violations and 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.

symantec.com +1 650-527-8000