Threat Feed

Introducing all new cloud app threat feed data in this edition.

Recently added to **CloudSOC Audit,** cloud app threat feed provides deeper insight into global exploits (threats from hackers), especially attempts to compromise accounts and exfiltrate data that have been publicized in the media over the first six months of the year.

using Google
reatens Android
ng Malware Discove
Bug Exposes Data Of
ction Vulnerability in Ne
nt card data from 40 onli
care with Facebook Lite - it
mmers expose their entire o
laws Patched With Release
Injection Vulnerability in Ne
nfected Android Apps on Go
cyber attack: Travel trade g
onalds India is leaking 2.2 m
ram web HACK WARNING -
kers Personal Informatio
ner Network compromi
ld password manage
ums resets passwor
rns Coachella.co
rums Hacked

INDUSTRY REPORT

1H 2017 Shadow Data Report

Enterprise Cloud Applications & Services Adoption, Use, Content and Threats

Symantec™

CASB

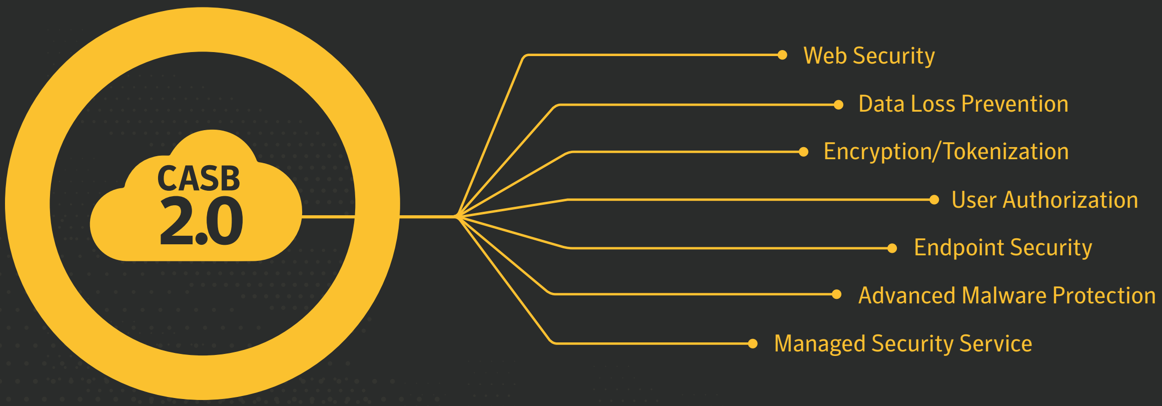
Cloud Access Security Broker

DATA AND ANALYSIS FROM

CloudSOC™

All stats for this report are drawn from anonymized customer activity on the CloudSOC platform, Symantec cloud application intelligence research and Symantec Cloud Threat Labs in the first six months of 2017.

CloudSOC is an industry-leading Cloud Access Security Broker (CASB) solution designed to enable you to securely adopt cloud apps and meet your regulatory compliance requirements through integration with the rest of your enterprise security investment. CloudSOC provides visibility, data security, and threat protection for today's cloud generation of users across a wide range of sanctioned and unsanctioned apps.



CASB 2.0

Web Security

Data Loss Prevention

Encryption/Tokenization

User Authorization

Endpoint Security

Advanced Malware Protection

Managed Security Service

CloudSOC pioneered the concept of CASB 2.0, 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).

Executive Summary

The average enterprise uses 1,232 cloud apps.

Up 33% (from 928) in the last report.

71% of risky user activity in the cloud indicates attempts to exfiltrate data.

17% of risky activity in the cloud indicates brute force attacks.

1% of users were responsible for all high risk data exfiltration, destruction and account takeover incidents.

20% of all files stored in the cloud are broadly shared, and 2% of these files contain compliance related data.

The percentage of files containing compliance data has gone down from 3%, reflecting continuing improvement in mitigation efforts and employee training using the CloudSOC platform.

29% of emails and attachments in the cloud are broadly shared, and 9% of these contain compliance related data.

This indicated a higher risk from emails than file sharing, especially given that the volume is much higher.

About the Report

The Symantec CloudSOC Shadow Data Report covers key trends and challenges organizations face when trying to ensure their sensitive data in cloud apps and services remains secure and compliant. Covering the first half of 2017, this report is based on the analysis of over 22K cloud apps and services, 465M documents and over 2.3B emails—nearly double the data from the last report. All data is anonymized and aggregated to protect Symantec CloudSOC customer confidentiality.

> 22 thousand *cloud apps and services*

> 465 million *documents*

> 2.3 billion *emails*

Cloud apps and services provide unprecedented levels of collaboration and business enablement that can help your employees and organization become more productive and efficient. And they can do this while keeping your sensitive data secure—if you take the proper steps to maintain security and compliance over the entire cloud security lifecycle.

PUBLISHED BY

Cloud Threat Labs & Symantec CloudSOC™

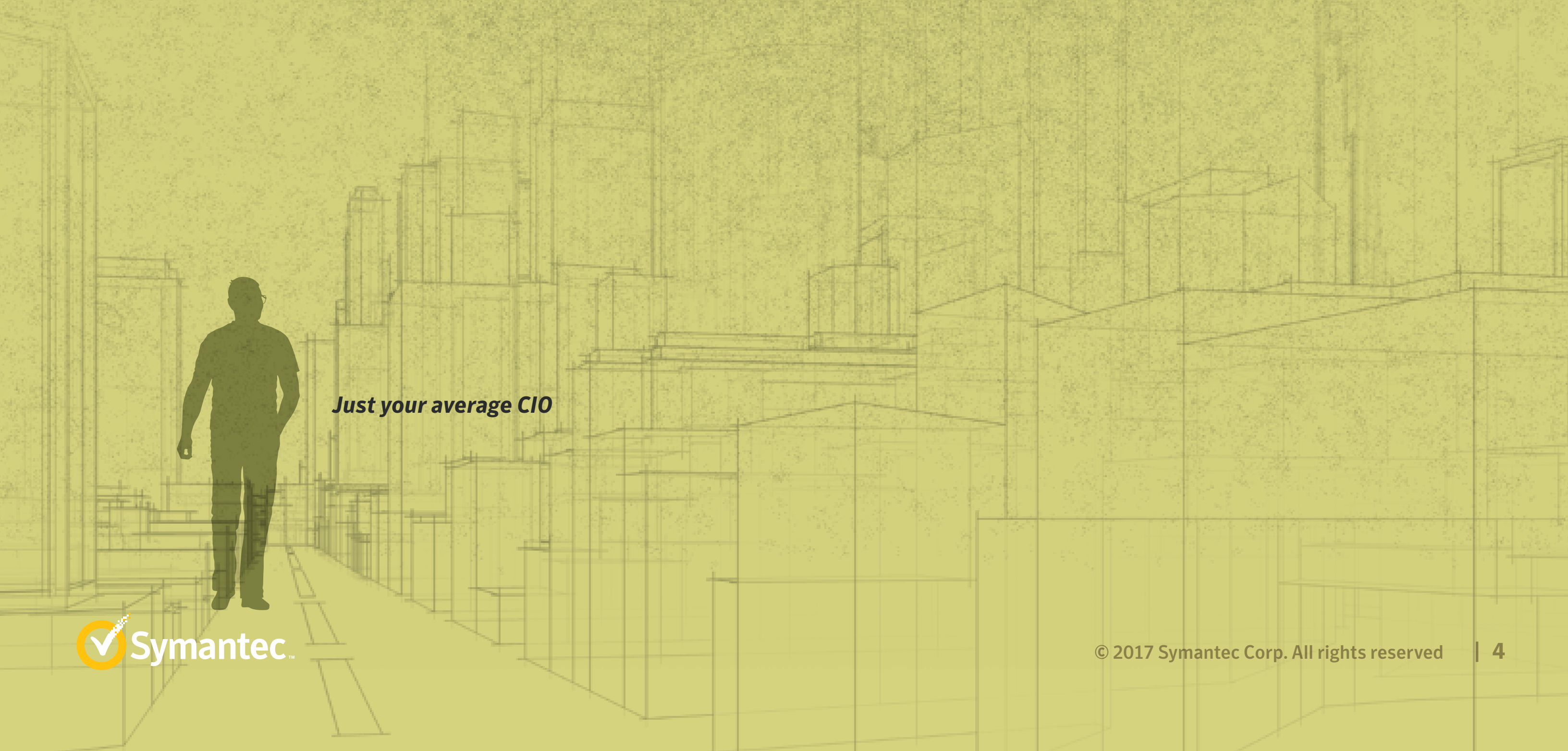
About cloud app threat feed

This report includes a special section focused on threats from hackers, especially attempts to compromise accounts and exfiltrate data that have been publicized in the media over the first six months of the year. While we have looked at threats impacting individual customers in the past, the cloud app threat feed recently added to CloudSOC Audit provides deeper insight into global exploits. It enables users to temporarily factor recent exploits into the Business Readiness Rating (BRR) of affected cloud apps and services. Identifying risks in the wild—before they have affected CloudSOC customers—is an important extension of our ability to keep our CloudSOC users secure and provide greater insight into the cloud threats they face.

Shadow IT perception

> "My organization only uses about 30-40 cloud apps."

In discussions with customers, we've found that the average CIO continues to think their organization is using between 30 and 40 cloud apps and services, when in reality, the number is ***30 times*** their best guess.



Just your average CIO

Symantec found **organizations typically have 1,232 apps on their extended network,** most of which were adopted without IT approval or oversight.

This number is up sharply from 928 in the last Shadow Data Report. Clearly the proliferation of cloud apps is not slowing down, but instead still expanding, which makes managing Shadow IT even more important.

What is Shadow IT?

In the context of the cloud, Shadow IT refers to the adoption and use of SaaS apps by employees and business units without the IT department's oversight or consideration of organizational security requirements. Gaining visibility and control over cloud apps is a key first step in maintaining cloud security and compliance.

Learn more about Shadow IT at
go.symantec.com/audit

Top Used Apps

Symantec looked at the top five apps in commonly used app categories: Collaboration/File Sharing, Business Enablement, and Consumer. While enterprise and consumer apps differ greatly in their functionality and their adherence to security best practices and relevant compliance regimes, the practical distinction is becoming less relevant as consumer apps are increasingly adopted for business use.

	Collaboration/File Sharing	Business Enablement	Consumer
①	Office 365	Salesforce	Facebook
②	Google	ServiceNow	Twitter
③	Box	GitHub	YouTube
④	Dropbox	Zendesk	Pinterest
⑤	Evernote	Amazon	LinkedIn

Shadow Data

Threats from Oversharing

Shadow Data poses a growing challenge to IT's ability to prevent the loss or non-compliant exposure of sensitive corporate data. It comprises all of the unmanaged content that users are uploading, storing, and sharing not only using unsanctioned cloud apps, but sanctioned ones as well. Even if an organization were to successfully limit employees to the use of secure file sharing apps, it would not mean they have fully mitigated the risks of data loss or compliance violations. Smart data governance practices such as identifying and categorizing all cloud data, then enforcing policies around its use, are the only way to prevent the leakage of business critical data.

Oversharing is particularly risky when files contain sensitive data. Symantec found that of the 465M cloud-stored documents analyzed, 20% were broadly shared and at high risk of exposure.

20% of all Shadow Data stored in the cloud is broadly shared

Broadly shared = high risk of exposure

Broadly shared refers to documents that are widely shared with employees within the organization, documents that have been shared externally with specific individuals such as contractors and partners, and documents shared to the public.

The added risk of exposing compliance related data

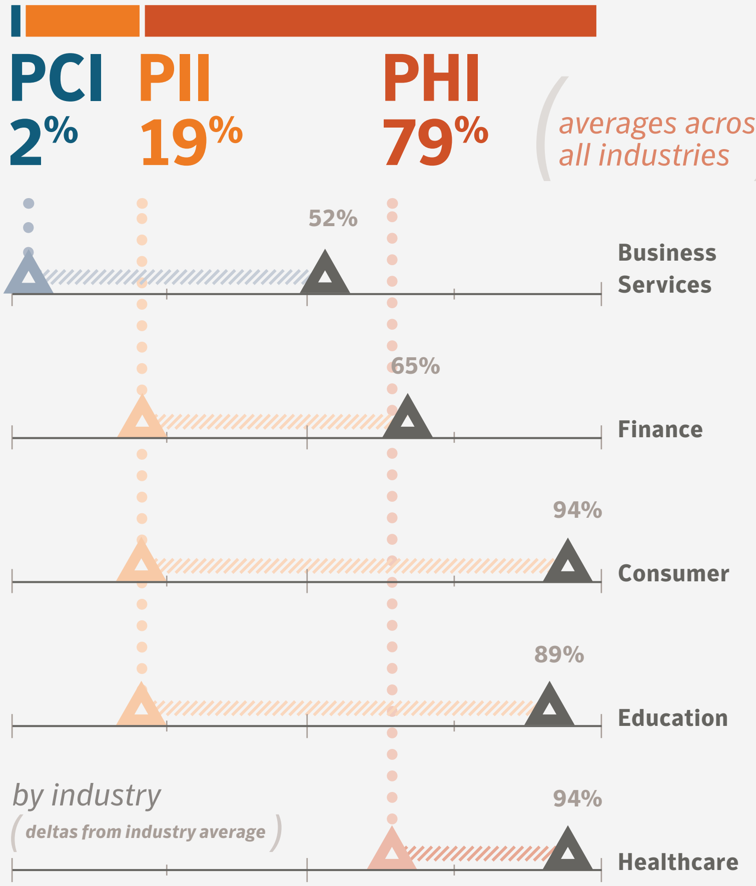
2% of broadly shared documents contain compliance related data, including PII, PCI and PHI. It is interesting to note that this is down from the 3% identified in the last report. It indicates that organizations are using Symantec CloudSOC to continually improve their security and educate users on the secure use of cloud apps. Companies not using CloudSOC may find this number to be much higher.

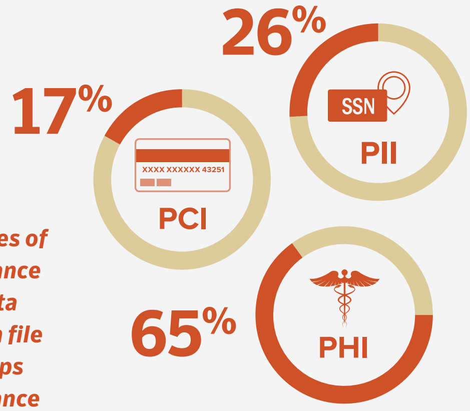
What is considered compliance-related data?

Not all documents stored in file sharing apps are sensitive. The majority are innocuous business files such as meeting notes, non-business critical files, etc. For the purposes of this report, we focus on the most sensitive data types:

Personally Identifiable Information (PII) **Payment Card Information (PCI)** **Protected Health Information (PHI)**

2% of broadly shared files that *do* contain sensitive data, are distributed as follows:





Percentages of all compliance related data exposed in file sharing apps by compliance violation type

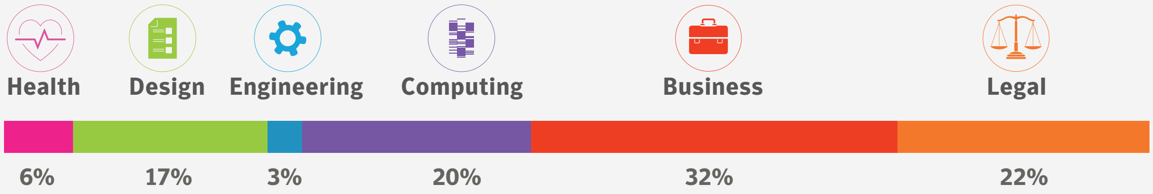
These statistics are quite alarming, especially with the vast majority of high value PHI being overexposed.

Identifying sensitive content—is there malicious activity going on?

Symantec uses machine learning and advanced computational linguistics for content analysis, not just regular expression matching, to more accurately classify documents by compliance type (PII, PHI, PCI) as well as category types such as legal, human resources, finance, source code, etc.

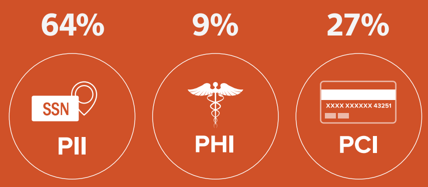
Potentially sensitive data also broadly shared

In addition to compliance related files and source code, organizations also want to classify and manage broad categories of documents, such as legal, business, computing, and health related files. The distribution across all industries is as follows:



What about Email Threats?

Symantec found that 29% of emails and attachments are broadly shared and at risk of leakage, with 9% of these emails containing compliance related data, distributed as follows:



Organizations need to be able to scan a broad range of apps, not just file sharing services, to provide end-to-end security for cloud content. For example, comprehensive security for Office 365 must cover not only One Drive, but also Email, Sites, Yammer, Teams, and Groups. This allows organizations to consistently enforce their policies regardless of the channel of communication.

Threats from Malicious Employees and Hackers

Threat Feed

featuring new data from cloud app threat feed

Beginning in January 2017, Symantec began tracking major cloud service and web portal hacks and exploits, which are now temporarily factored into infected apps' Business Readiness Ratings (BRR) in CloudSOC Audit. Of the succesfully damaging cloud exploits identified by Symantec during the first half of 2017:

46% targeted enterprise apps

52% targeted consumer apps

21% were malware distribution exploits

These attacks leverage a cloud service to distribute malware to unsuspecting users. For instance, through SQL injection attacks.

44% were application layer attacks

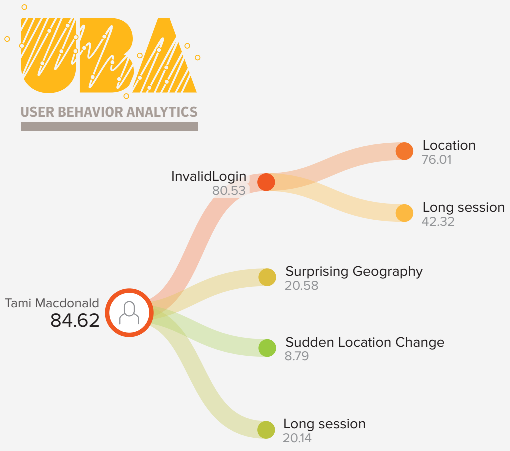
These include exploits where a web portal or cloud service provider's infrastructure was compromised due to a software bug or unseen vulnerability in their security protocols.

18% were phishing or spear phishing attacks

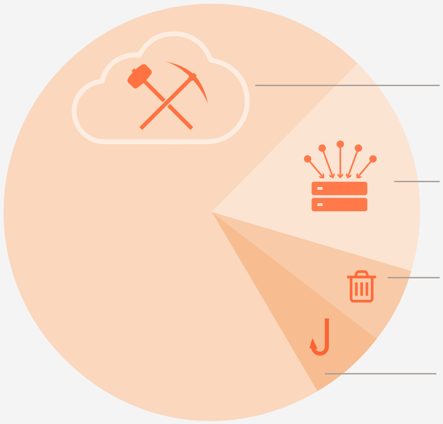
In most cases, these involved cloud email services that used social engineering to direct users to malicious websites.

Identifying threats: is a user account compromised?

Symantec takes a multilayered data science approach to identifying malicious cloud related activity, leveraging machine learning and computational analysis to detect suspicious user behavior. Symantec determines the relative risk of each cloud app user. This individualized risk profile updates dynamically and can provide early identification of malicious insiders or compromised user end-points and accounts. Automated policy controls can be set to trigger when a user passes certain thresholds for very fast response.



Of the risky behavior seen in cloud accounts over the past six months:



71% indicates attempts to exfiltrate data

17% indicates a brute force attack attempt

6% indicates attempts to destroy data

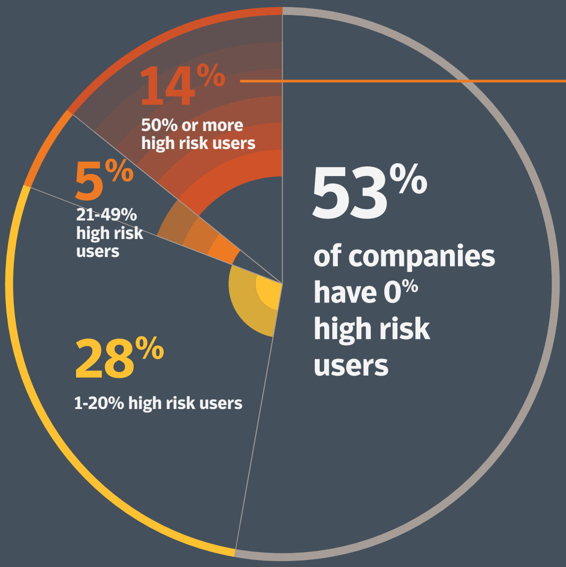
6% indicates attempts to hack into user cloud accounts

Exploits by App Type

If we look at exploited accounts for the top 5 app types we get:

Type	*% of top 5*
Instant Messaging	18%
Hosted Email	13%
File Share/Prod Suite	18%
Online Shopping	34%
Social Network	18%

Consumer apps (such as online shopping or social networking) experience over 50% of the exploits, but much of this risk is posed to individual users by placing their finances and personal accounts at risk, as well as potentially damaging the cloud service provider's reputation, business, and compliance posture. We see the highest risk posed to sensitive and compliance related corporate data among the many enterprise apps, especially IM, email, and file sharing.



An astonishing 14% of all organizations have 50% or more of their employees who are high risk users.

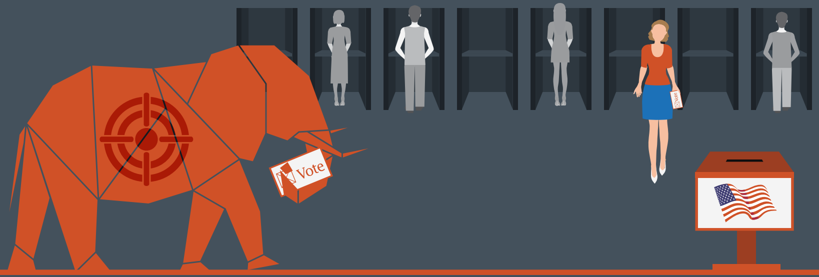
The good and bad news is that high risk users are concentrated, as mentioned earlier, in 47% of companies. If you are among the 53% of companies that currently have no users performing high-risk activities, then the risk to your business is reduced, though not eliminated. But, if you happen to be one of the 47% of companies with active high-risk users, up to 70% of your employees may have demonstrated high risk activity.

Please note that the population of data examined in this report comes from organizations who have already demonstrated a higher commitment than average to secure themselves against cloud risks. These risk statistics could easily be higher for businesses who haven't adopted cloud security that identifies suspicious user behavior, and haven't used that information to educate their users on safe cloud usage.

Alarming Cloud Threat for U.S. GOP in 1H 2017

One of the more shocking 2017 cloud exploits was in June when nearly 200M American voters' personal details (PII) were exposed via S3 buckets.

Internal GOP documents had been stored on a publicly accessible cloud server and contained ***US voter names, addresses, birth dates, last four digits of their Social Security Numbers, and voting sentiments.*** More than a terabyte of data was stored for twelve days without a password and could have been accessed by anyone who found the URL during that time. CloudSOC could have helped prevent this exposure!



What is considered a high risk user?

A high risk user is one whose account has shown high levels of compromise by one of the top three most serious security incidents: data exfiltration, data destruction, and account takeovers. Symantec tracks over 100 risky activities that fall into these three categories, such as anomalous frequent file previews, anomalous frequent file sharing, and anomalous frequent account logins.

Data Exfiltration

Anomalous frequent file previews

Anomalous frequent file downloads

Anomalous frequent emails sent

Anomalous frequent file sharing

Data Destruction

Anomalous frequent file edits

Anomalous frequent file deletions

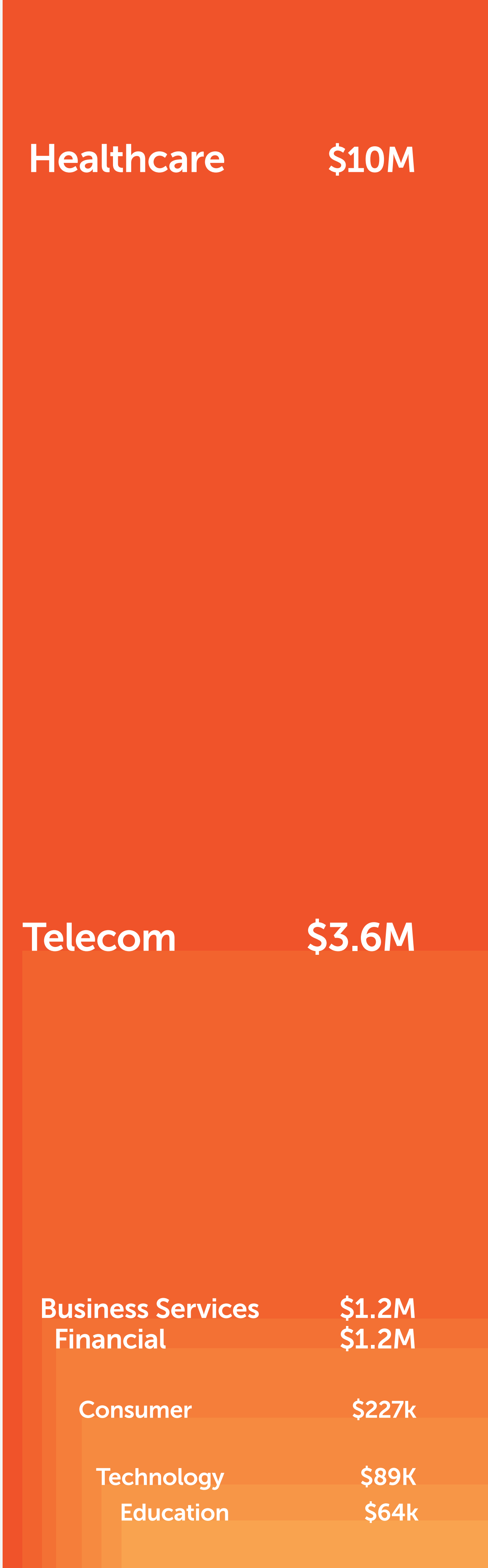
Account Takeover

Anomalous frequent account logins

Too many suspicious account logins

Cost of a Typical Data Breach

Healthcare and Telecom face the highest financial risk from the leakage of compliance related data Symantec calculated that the potential financial impact on the average organization over the past six months from the leakage of all of an organization's sensitive cloud data was just over $3.7M. The cost by industry varies substantially.



Conclusion

01 Upgrade to CASB 2.0

With the proliferation of cloud apps, and its accompanying risks, you need to look to protect your cloud apps and data from any device, any user, and any app—both on and off-prem—without having to build a separate island of security in the cloud. This requires a CASB 2.0 solution that natively integrates with your existing security investments to provide you with the same peace of mind in the cloud that you've come to trust from your on-prem security infrastructure.

02 Extend your existing DLP policies to the cloud

You should extend your on-prem Data Loss Prevention (DLP) to your cloud apps and services to ensure consistent policies and mitigation workflows are enforced no matter where your data resides. This will reduce the cost and complexity of building a separate instance of DLP in the cloud. The best way to achieve this is to select a CASB 2.0 solution that natively integrates with your on-prem DLP and can be managed through a single dashboard.

03 Don't just discover Shadow IT…control IT!

CASB 1.0 solutions are good at discovering Shadow IT, but don't enable you set policies to control it. You should select a single vendor CASB 2.0 solution that natively integrates your CASB functionality with your Secure Web Gateway (SWG) to provide automated SWG log file analysis for Shadow IT discovery, cloud policy control, and simplified deployment of CASB and SWG, in addition to deep shadow IT visibility.

04 Enable Information-Centric Encryption for your CASB

You should select a CASB 2.0 that automatically encrypt files from DLP policies and allow decryption with identity triggers, from anywhere. It should then monitor and change permissions in real time allowing you to dynamically protect information whether its on-prem or in the cloud.

05 Extend Advanced Threat Protection to cloud accounts

You should select a CASB 2.0 solution that can secure your cloud accounts and transactions against malware by natively integrating with an advanced threat protection solution that includes file reputation intelligence, A/V scanning, and sandboxing technologies. It should enable you to detect insider threats, block and neutralize malicious files, identify and eliminate malware, and detect zero-day threats in the cloud.

Request a free trial or

Shadow IT and Shadow Data Risk Assessment

Get a complimentary Shadow Data or Shadow IT risk assessment and start getting visibility and control over your cloud app usage.

get started

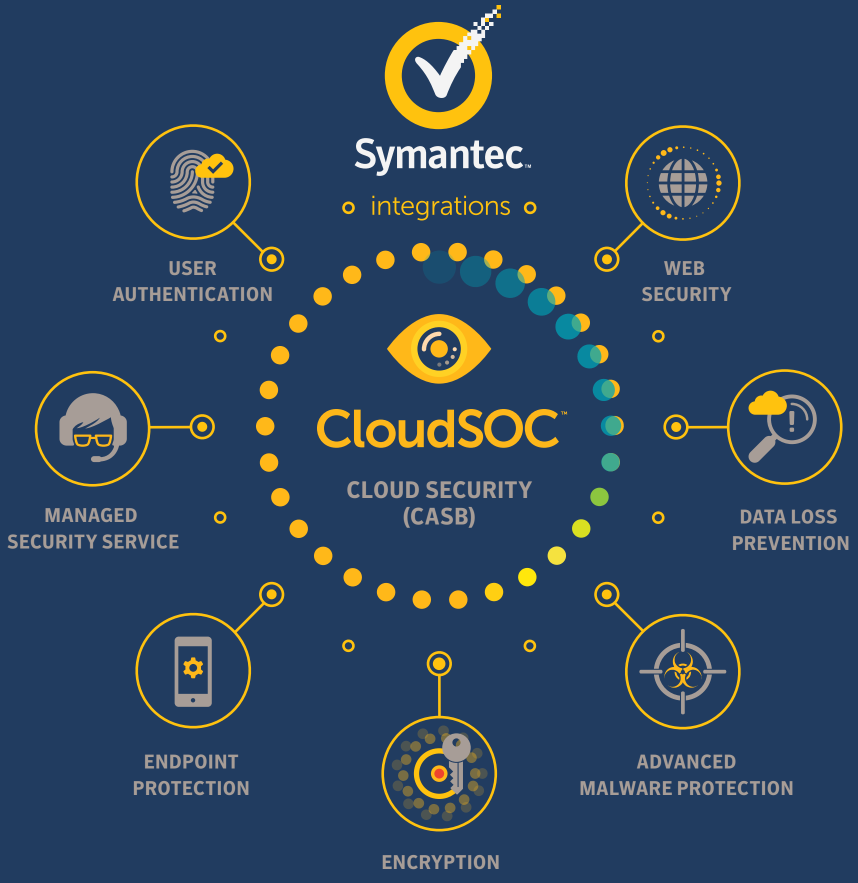
go.symantec.com/shadow-data

go.symantec.com/shadow-it

or visit **go.symantec.com/casb** to learn more

Get better security with 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.



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

Symantec.

symantec.com +1 650-527-8000

About CloudSOC

Data Science Powered™ Symantec CloudSOC platform empowers companies to confidently leverage cloud applications 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, real-time detection of intrusions and threats, protection against data loss 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.