

# 2018 Shadow Data Report



Symantec





## Contents

About the report	2
Executive summary	3
Shadow IT risks	4
Shadow data risks	6
Malicious account activity	10
Compromised cloud services	11
Cost of a cloud data breach	12
Where to start?	13

## 01

# About the Report

The Symantec 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. This edition of the report is based on the analysis of over **22K cloud apps** and services, **758M documents** and over **1.4B emails and attachments**.

All stats for this report are drawn from anonymized and aggregated customer activity on the CloudSOC CASB platform over the 12 months ending Feb 2018.

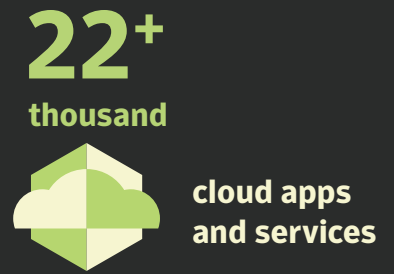
### Important note

Since many CloudSOC customers have already mitigated their cloud application risks and data exposures, the number and severity of risks identified in the report may be lower than what you could expect to find if you have not had a Cloud Access Security Broker (CASB) or cloud security strategy in place.

# EXECUTIVE SUMMARY

**The average enterprise uses 1,516 cloud apps, 40 times what they typically think.**

Up 23% (from 1,232) in the last report.



**13% of all files stored in the cloud are broadly shared, and 1% of these files contain compliance related data.**

The percentage of files containing compliance data has gone down from 2%, reflecting continuing improvement in mitigation efforts and employee training using the CloudSOC platform.

**18% of all PII, 13% of all PCI, and 56% of all PHI shared in the cloud is overexposed.**

Broadly shared PHI presents an elevated risk to organizations given such a large percentage is overexposed and that the cost of a PHI data breach is far higher than that of other types of data.



**32% of emails and attachments in the cloud are broadly shared, and 1% of these contain compliance-related data.**

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

**68% of organizations have some employees who exhibit high-risk behavior in their cloud accounts**

Up to 71% of employees in some cases. High-risk behavior includes activities that can indicate data destruction, data exfiltration, and account takeovers.



**The average cost to an organization for a breach of all compliance-related data is \$2.8M**

This goes up to \$11.5M in the healthcare industry.

# 03

## Shadow IT Risks



In the context of the cloud, Shadow IT refers to the adoption and use of SaaS apps without the IT department’s oversight or sanction. Proliferation of Shadow IT can result in users storing and sharing confidential data in apps with inherent security risks or that are unmanaged by the IT department, increasing the likelihood of data loss or destruction.

### The culprits—employees and business units

Shadow IT is typically adopted by your employees or business units, often using a credit card to fulfill immediate business needs without consideration of organizational security requirements—or consulting with IT.

### The challenge—your organization is using more apps than you think

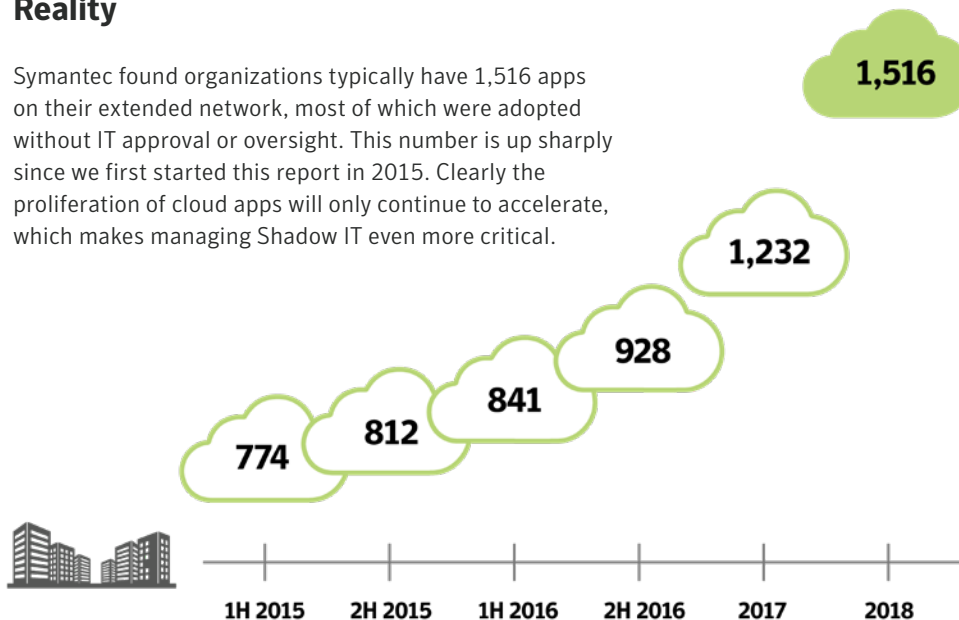
#### Perception

“My organization only uses about 30-40 cloud apps.”

We continue to find 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 40 times their best guess.

#### Reality





















Symantec found organizations typically have 1,516 apps on their extended network, most of which were adopted without IT approval or oversight. This number is up sharply since we first started this report in 2015. Clearly the proliferation of cloud apps will only continue to accelerate, which makes managing Shadow IT even more critical.



## Top used apps

Symantec looked at the top five apps in commonly used app categories: collaboration/file sharing, business enablement, consumer and, new to this report, messaging. While there has been very little change in the rankings for file sharing and business enablement, with Office 365, Google, and Salesforce continuing to dominate, we have seen a shift in consumer apps. LinkedIn and YouTube are overtaking Facebook and Twitter as corporate communication and marketing platforms of choice.

### Top 5 apps by category

File Sharing	Business Enablement	Consumer	Messaging
			
			
			
			
			

### Under-the-radar popular business apps

Most people are familiar with other common cloud apps like Asana or DocuSign, but have you heard of Smartsheet or Infogram? Here are some of the most used apps you may not have heard of, and are (statistically speaking) likely already housing some of your company's sensitive data.

BU Tools	Productivity	E-Commerce	Cloud/Platform
<b>SucessFactors</b>	<b>Smartsheet</b>	<b>WorldPay</b>	<b>Ning</b>
<b>Cvent</b>	<b>Infogram</b>	<b>Mobify</b>	<b>Firebase</b>
<b>Affinity.co</b>	<b>Ontraport</b>	<b>Stripe</b>	<b>NetSuite</b>
<b>Coveo</b>	<b>Trello</b>	<b>Volusion</b>	<b>Transifex</b>
<b>Mendeley</b>	<b>ShareFile</b>	<b>FoxyCart</b>	<b>Rackspace Cloud</b>



## The solution—gaining visibility and control over cloud apps

Sanctioning only those apps that have adequate security protocols in place and blocking or limiting access to the rest is a key first step in maintaining cloud security and compliance.

## Shadow Data Risks



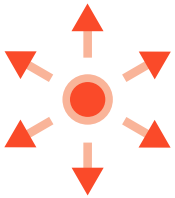
Shadow Data comprises all of the unmanaged content that users are uploading, storing, and sharing not only using unsanctioned cloud apps, but sanctioned ones as well. Even if an organization were to successfully limit employees to the use of secure file sharing apps, it would not mean they have fully mitigated the risks of data loss or compliance violations.

### The culprits—high-risk employees

The biggest risk to shadow data is high risk employees—those that do not have malicious intent, but may inadvertently overshare confidential data due to poor security, compliance, or data governance training, distracted use, or accidental misuse.

### The challenge—rampant oversharing of confidential files

Oversharing is particularly risky when files contain confidential data. Symantec found that of the 758M cloud-stored documents analyzed, 13% were broadly shared and at high risk of exposure, down from 20% in the last report.



#### *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

1% of broadly shared documents contain compliance-related data, including PII, PCI, and PHI. It is interesting to note that this is down from the 2% 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?*

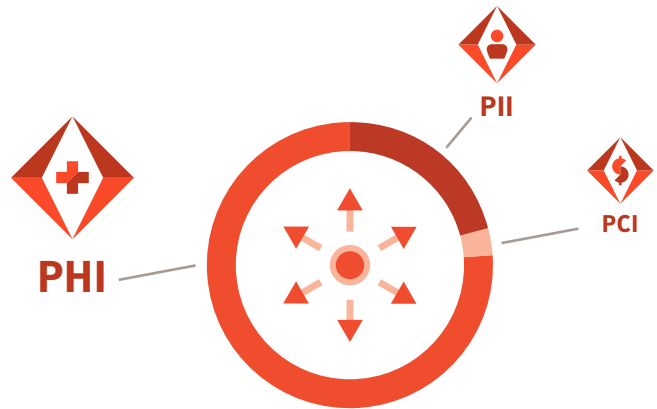
Not all documents stored in file sharing apps are sensitive. The majority are innocuous business files such as meeting notes, non-business critical files, etc. For the purposes of this report, we focus on the most sensitive data types: **Personally Identifiable Information (PII), Payment Card Information (PCI), and Protected Health Information (PHI)**

Of the 1% of broadly shared files containing confidential data:

21% contain PII

3% contain PCI

77% contain PHI

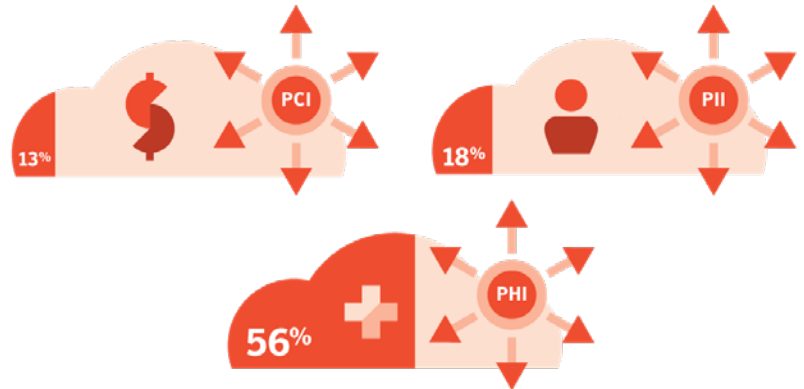


Looking at this another way:

18% of all PII in the cloud is overexposed.

13% of all PCI in the cloud is overexposed.

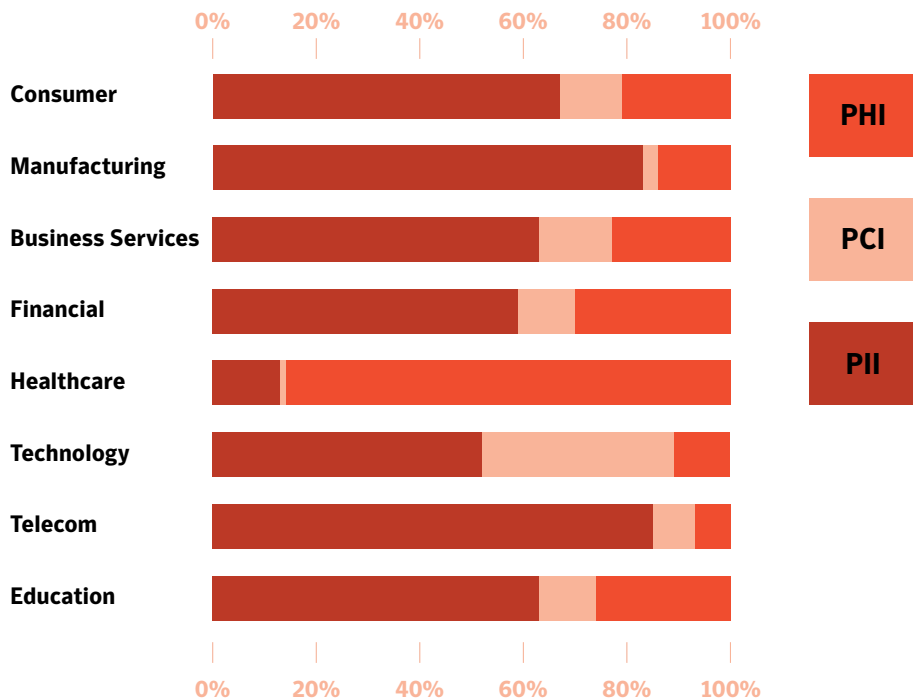
6% of all PHI in the cloud is overexposed.



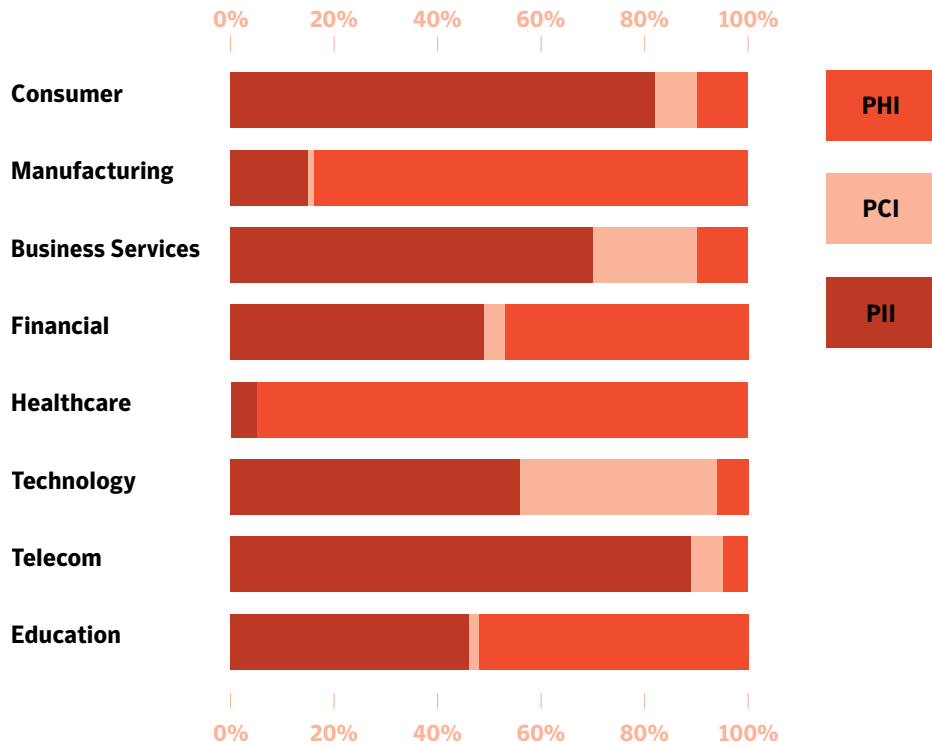
### Identifying confidential and compliance related content

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.

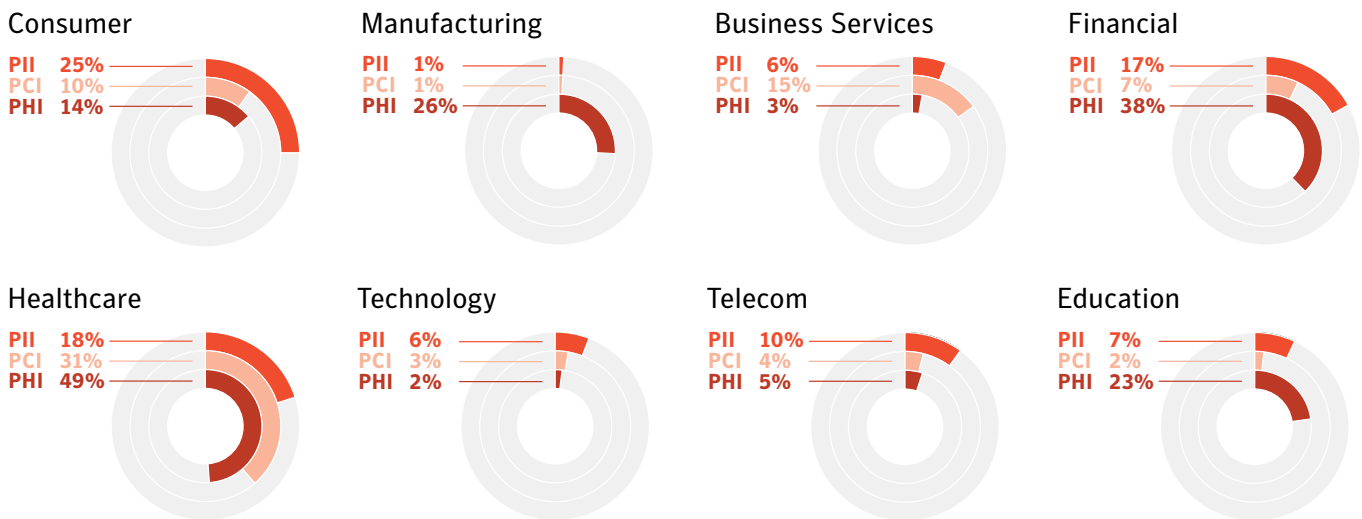
Here is the distribution of all cloud docs that contain compliance data, by industry:



Here is the distribution of all exposed cloud docs that contain compliance data, by industry:



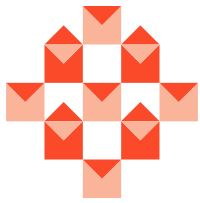
Looking at it another way, here is the percentage of each type of compliance doc that is exposed, by industry:



As you can see, for instance, the majority of compliance files in healthcare (86%) contain PHI, and 95% of exposed compliance docs contain PHI, which one would expect. However, what is concerning is that 49% of all healthcare PHI data is exposed, suggesting poor controls on PHI.

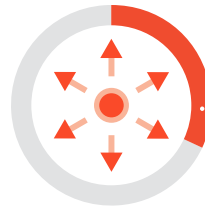
Alternately, in the technology industry, the majority (52%) of compliance files contain PII, and 55% of exposed compliance files contain PII. However, only 6% of PII overall is exposed, suggesting that industry has done a better job of securing its PII than healthcare has in securing PHI.





### Email Risks

**32% of emails and attachments are broadly shared**



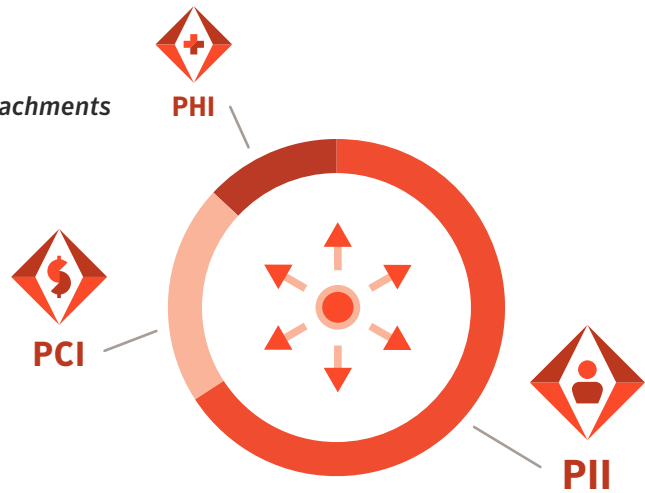
**1% contain PII, PCI or PHI** of 1.4 billion emails means that ~4.4 million emails contain compliance related data!

*Of all broadly shared emails and attachments containing confidential data:*

**66% contain PII**

**21% contain PCI**

**13% contain PHI**



### The solution—cloud data governance

Identifying and categorizing all confidential cloud data, then enforcing policies around its use, are the only way to prevent oversharing and the inadvertent leakage of business critical data.

*(continues next page)*

# Malicious account activity

Malicious activity includes intentional attempts to exfiltrate or destroy data or hack into user accounts.

## The culprit—malicious insiders and hackers

Disgruntled employees intent on destroying company data or exfiltrating customer data or IP pose a significant threat to your confidential data. And hackers, armed with sophisticated phishing exploits, brute force hacking tools, and social engineering techniques can compromise accounts to exfiltrate or destroy data, or inject ransomware.

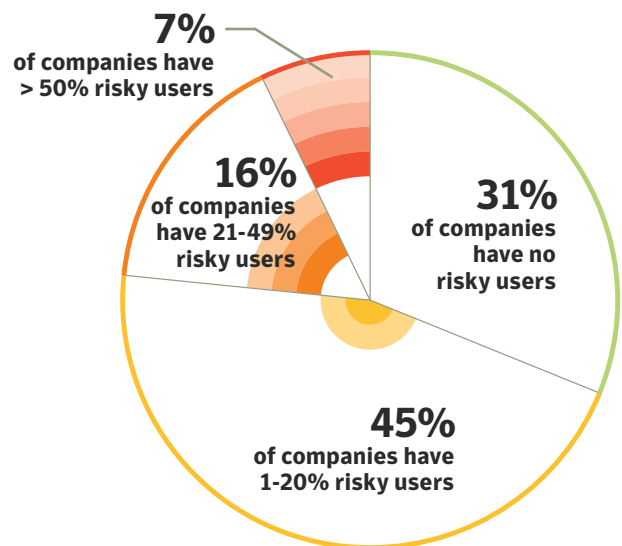
## The situation—data exfiltration, destruction, and account takeovers

*Of the risky behaviors seen in cloud accounts over the past twelve months:*



### High-risk users

The good and bad news is that high risk users are concentrated in 69% of companies. If you are among the 31% 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 69% of companies with active high-risk users, up to 71% of your employees may have demonstrated high risk activity.



## The solution—User Behavior Analytics (UBA)

Tracking malicious behaviors in cloud accounts through an analysis of user activities is critical to identifying and preventing exploits. It also gives you the insight needed to create and enforce policies that limit access and sharing of confidential data by high-risk users.

## Compromised Cloud Services

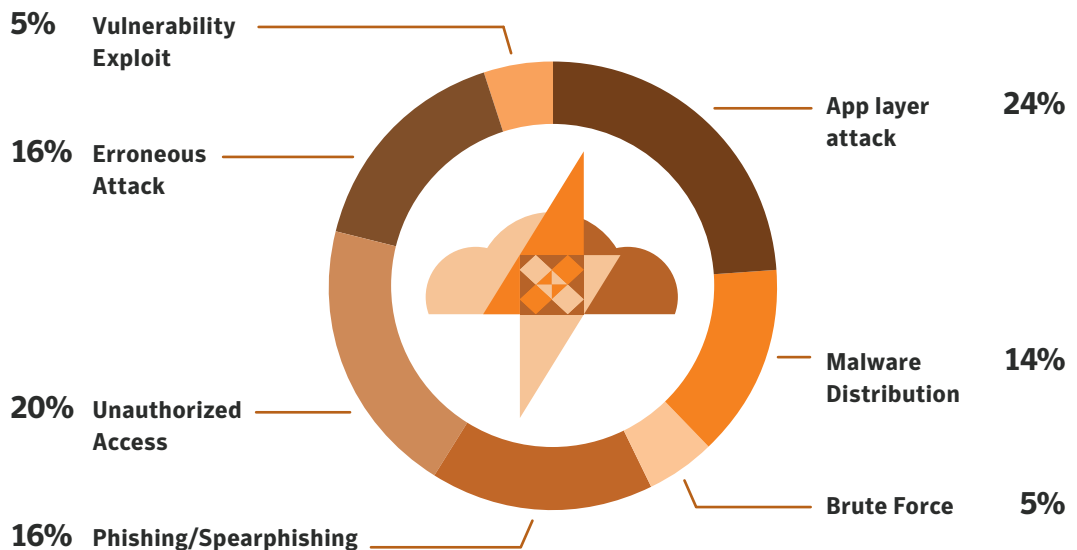
Symantec tracks recent major cloud service and web portal hacks and exploits, and then factor them into infected apps' Business Readiness Ratings (BRR) in CloudSOC Audit.

### The culprit—cloud service vendors themselves

Leading cloud service vendors maintain a shared responsibility for security. They ensure their infrastructure is secure, while the customer is responsible for ensuring secure app usage. However, many lesser-known apps do not even meet minimal security standards such as supporting MFA , encryption, and strong password enforcement, meaning that the entire security burden falls to the customer to ensure such non-secure apps are not used by employees.

### The situation—attacks on cloud services that reveal inherent security vulnerabilities in some apps

*Of the successfully damaging cloud exploits identified by Symantec during the past year:*



### The solution—ensuring business readiness of app sanctioned cloud apps

Cloud customers must perform a security evaluation on all apps before sanctioning them for use by employees. This evaluation should determine whether the app meets standards for important

compliance regimes, whether the app has controls in place to protect compliance related data, and whether effective access controls are in place. These attributes fall into the following broad categories:

COMPLIANCE                      DATA PROTECTION                      ADMINISTRATIVE CONTROLS  
ACCESS CONTROLS                      SERVICE AVAILABILITY                      BUSINESS STABILITY                      INFORMATIONAL

## 07

# Cost of a Cloud Data Breach

Healthcare and Financial 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 \$2.8M. The cost by industry varies substantially.

*Here is the average cost to an organization for a breach of confidential data by industry:*

	All Verticals	Consumer	Education	Biz Services	Financial	Health	Technology	Telecom
Non PHI Files	855,603	6,823	31,672	56,563	423,412	160,694	228,056	115,384
Cost of Non PHI leaked docs	\$135M	\$1M	\$5M	\$9M	\$67M	\$25M	\$36M	\$18,230,672
# PHI Files	1,232,283	1,850	10,981	16,687	184,852	999,802	4,522	9,345
Cost of PHI leaked docs	\$437M	\$657M	\$3.9M	\$6M	\$66M	\$355M	\$1.6M	\$3,317,475
Cost of all leaked docs	\$573M	\$1.7M	\$9M	\$15M	\$133M	\$380M	\$38M	\$21,548,147
Avg cost per company	\$2.8M	\$145K	\$1.5M	\$531K	\$2.3M	\$11.5M	\$523K	\$1.2M



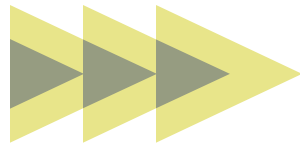
## The solution—CASB to the rescue

By providing organizations visibility and control over Shadow IT and Shadow Data, a full-featured CASB solution can help minimize the risk of incurring massive compliance fines, mitigation costs, and lost reputation due to a breach of compliance-related data.

## Where to start?

### *A free shadow IT risk assessment*

The first step towards securing your organization's cloud usage is to request a Shadow IT Risk Assessment to uncover all apps running on your extended network. This will also give you an opportunity to see the Symantec Audit in action through a 30-day free trial.



[go.symantec.com/shadow-it](https://go.symantec.com/shadow-it)

### *A free shadow data risk assessment*

The next step towards securing your organization's cloud usage is to request a Shadow Data Risk Assessment to uncover and classify all Shadow Data stored and shared within your selected cloud app. You will also get temporary access to the CloudSOC dashboard, which will give you an opportunity to see the Securlet in action.



[go.symantec.com/shadow-data](https://go.symantec.com/shadow-data)

### **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](https://www.symantec.com) or connect with us on [Facebook](#), [Twitter](#), and [LinkedIn](#).

350 Ellis St., Mountain View, CA 94043 USA

| +1 (650) 527 8000

| 1 (800) 721 3934

Copyright ©2018 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

[www.symantec.com](https://www.symantec.com)

SYMC\_IR\_SHADOWDATAREPORT-2018\_EN\_V1B