Shadow Data Report vs. Reality

Perception vs. Reality

Businesses are increasingly embracing the benefits of cloud—using 841 apps per organization on average.

99% of all business cloud apps are not business ready.

Organizations use 20 times more cloud apps than they assume.

Enterprise Cloud Applications & Services Adoption, Use, and Threats

Published by Elastica Cloud Threat Labs
The Shadow Data Report published by Elastica Cloud Threat Labs, addresses key trends and challenges faced by enterprises securing data stored and shared via cloud apps and services. Covering the first half of 2016, this report is based on the analysis of over fifteen thousand cloud apps and 108M documents. All data is anonymized and aggregated to protect customer confidentiality.

Cloud apps and services provide unprecedented levels of collaboration and business enablement that can empower employees and organizations to be more productive and efficient. And they can do this while keeping sensitive data secure—as long as they take steps to maintain adequate visibility and control over the entire cloud security lifecycle.

This report is focused on the potential risks enterprises may encounter whenever they adopt insecure or non-compliant apps, implement insufficient policies around data governance, allow the accidental sharing of files, or become exposed to malicious insiders and hackers. In addition, this report covers the potential repercussions of data leakage, including compliance and mitigation costs.

Most IT experts are aware of the risk posed by Shadow IT. In the context of the cloud, it refers to the adoption and use of SaaS apps by employees and business units without the knowledge or explicit consent of an organization’s IT department. Gaining visibility and control over cloud apps is a key first step in maintaining cloud security. Shadow Data, however, poses a much greater challenge to IT’s ability to prevent the loss or non-compliant exposure of sensitive corporate data.

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 enterprise-grade file sharing apps like Box or Office 365, it would not mean they have fully mitigated the risks of data loss or compliance violations. Even with sanctioned apps, it is challenging for organizations to identify and track how their users are using these apps, and what sort of sensitive data they may be uploading and sharing inappropriately. This lack of visibility into Shadow Data may result in risky exposures or compliance violations.
Executive Summary

**20 x**

Organizations use 20 times more cloud apps than they think.

**841**

An enterprise has 841 cloud apps in use (average).

| 63% of risky user activity in the cloud indicates attempts to exfiltrate data |
| 37% of suspicious cloud activity indicates attempts to hack into user cloud accounts |
| 2% of user accounts show signs of malicious activity due to compromised credentials |
| 11% of business cloud apps are still vulnerable to exploits such as FREAK, Logjam, Heartbleed, Poodle SSLv3, Poodle TLS, and CRIME |
| More than 98% of cloud apps are not GDPR ready |
| 95% of enterprise-class cloud apps are not SOC 2 compliant |
| While many popular enterprise apps are business ready, 99% of all business apps are not. |

23% of all files stored in the cloud are broadly shared.

12% contain compliance related data or confidential data.
The business-oriented cloud applications and services tracked by the Elastica data science team include popular file sharing services like Box, business productivity apps like Office 365, and sales enablement tools such as Salesforce. But while these popular apps are typically appropriate for business use, over 99% of all other business apps are not. Of those apps, 10% are partially business ready, meaning they may be suitable for limited business use, at least within companies with minimal sensitive data or compliance requirements. The rest are typically too risky for most businesses to adopt. Simply put—given that the average company has 30–40 known enterprise apps running on their network (not counting shadow IT, more on that later), chances are a number of them are not secure enough for business use—especially in industries where data governance and compliance are critical.

Threats Posed by Cloud App Security Vulnerabilities

Elastica determines the business readiness of 15,000+ cloud apps and services classified and tracked on the CloudSOC platform. Business readiness is based on multiple attributes, including whether the app meets standards for important compliance regimes, whether effective access controls are in place, and whether the app encrypts data. These attributes fall into the following broad categories:

- Compliance
- Data Protection
- Administrative Controls
- Access Controls
- Service Availability
- Business Stability
- Informational

Measuring Risk — How Business Ready Is That Cloud App?
Protection against common security vulnerabilities is another important attribute. 11% of apps are vulnerable to one or more of the following exploits: FREAK, Logjam, Heartbleed, Poodle SSLv3, Poodle TLS, and CRIME, even though these exploits are several years old.

Demanding SOC 2 compliance for any cloud app should be table stakes for any company looking to migrate to the cloud as it stipulates that applications need basic controls for security, availability, processing integrity, confidentiality, and privacy.

Another key attribute is whether an app has adequate access controls in place. Again, this should be a mandatory requirement for security conscious organizations, but 71% of enterprise apps do not provide Multi Factor Authentication (MFA).

Organizations use about 20 times more cloud apps than they think.

While the average IT department thinks their organization is using only thirty to forty cloud apps and services, the reality is that they typically have 841 apps on their extended network, up from 812 in the last Shadow Data Report.
Elastica tracks 15,000+ cloud apps and services shown here in 12 broad groups of app categories, by number of various apps within each category. Circles show the relative distribution of apps across category groups as well as nested subcategories. Marketing, business and financial groups have higher number of apps by category, but IT dominates with over half of all apps in its group. Take Project Management as an example, with over 480 different apps in its category, chances are that within an organization various apps are deployed serving the same function, and would be a smart target group to examine the potential for consolidation and cost savings.
50% of all business cloud apps do not adequately protect PHI according to HIPAA guidelines

For certain industries, preventing the leakage of specific types of sensitive data is critical. In the healthcare industry, for example, Protected Health Information (PHI) poses a high risk to the organization if exposed, with fines and remediation costs for a lost or stolen record being double that of other document types. This translates into an average cost of a PHI data breach to an organization of $10M. However, the cost can go much higher. The 2015 Anthem data breach where 80M unencrypted PHI records were leaked was a result of a data exfiltration exploit leveraging a popular file sharing application. The remediation costs and compliance fines could exceed $100M.

Not surprisingly, 52% of all health care industry documents contain PHI. But given that 50% of enterprise apps do not adequately protect PHI, healthcare organizations need to be highly selective when adopting cloud apps.

87% of cloud apps do not adequately encrypt data

Of all business apps, 13% encrypt data at rest, and 85% use SSL to secure data in motion. But for sensitive data like PII to be fully secured, a business app must have both, and only 3% of apps meet these criteria.

This poses a considerable problem for the finance industry, for example, where 85% of its sensitive cloud-stored data contains PCI. Telecom (71% PII) and Education (45% PII) are also at increased risk.

In addition, the Finance, Telecom and Education sectors face higher than average financial costs if compliance data is leaked or breached, especially since the US SEC is getting more aggressive about assigning PII penalties. For example, in February of this year the FCC released PII violation orders to six different telecom organizations with penalties ranging from $1.7M to $9.6M.

98% of cloud apps don’t come close to being GDPR ready

GDPR is a regulation by which the European Commission intends to strengthen data protection for individuals within the European Union (EU). It also addresses the export of personal data outside the EU. As a result, doing business in the EU can pose added regulatory challenges—a risk that is dramatically increased with the introduction of cloud services, many of which are hosted outside of the EU.

Elastica has analyzed business apps for GDPR readiness, covering fifteen key attributes. These include such requirements as access control, brute force protection, encryption of data at rest and in motion, and admin audit trails.

Across all enterprise oriented cloud apps tracked by Elastica CloudSOC, just 2% are GDPR ready. Popular apps such as Office 365, Google Drive, Salesforce, Box, and Dropbox are all GDPR ready. A further 25% of business apps meet some of the GDPR requirements for usage within the EU, but have a ways to go before being considered fully compliant.
Most Popular Cloud Apps Used in the Enterprise

For the sake of an apples-to-apples comparison, Elastica has compiled the top 5 apps in commonly used app categories: Collaboration and 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, as is shown below.

### TOP 5 APPS BY CATEGORY

<table>
<thead>
<tr>
<th>Collaboration Apps by Users</th>
<th>Business Enablement Apps by Users</th>
<th>Consumer Apps by Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>2H 2015</td>
<td>1H 2016</td>
<td>2H 2015</td>
</tr>
<tr>
<td>Office 365</td>
<td>Office 365</td>
<td>Facebook</td>
</tr>
<tr>
<td>2H 2015</td>
<td>1H 2016</td>
<td>2H 2015</td>
</tr>
<tr>
<td>Google</td>
<td>Google</td>
<td>GitHub</td>
</tr>
<tr>
<td>2H 2015</td>
<td>1H 2016</td>
<td>2H 2015</td>
</tr>
<tr>
<td>Dropbox</td>
<td>Dropbox</td>
<td>LinkedIn</td>
</tr>
<tr>
<td>2H 2015</td>
<td>1H 2016</td>
<td>2H 2015</td>
</tr>
<tr>
<td>Box</td>
<td>Box</td>
<td>YouTube</td>
</tr>
<tr>
<td>2H 2015</td>
<td>1H 2016</td>
<td>2H 2015</td>
</tr>
<tr>
<td>Evernote</td>
<td>Evernote</td>
<td>Pinterest</td>
</tr>
</tbody>
</table>

Important note: with the exception of Youtube, all of the most popular consumer apps listed above are not Business Ready although they are being used in nearly every enterprise.
Threats from Malicious Employees & Hackers

All organizations have experienced a minor to moderate security incident in the last year. However, according to the Elastica threat detection team, 12% of companies have high risk users and experienced one or more serious security incidents during that time. Of the common, most destructive activities, four stand out: anomalous frequent downloads, anomalous frequent sharing, too many suspicious logins (i.e., simultaneous logins from different locations), and anomalous frequent logins. These security incidents are related to risky user behavior indicative of malicious activity, whether it is the user’s own activity or that of an outside bad actor who has gained access to the account.

What is considered a security incident?
Security incidents can be broadly categorized as data exfiltration, data destruction, and account takeovers by hackers. Elastica tracks dozens of cloud activities within these three categories, but the most critical of these are as follows:

**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
63% of risky user activity in the cloud indicates attempts to exfiltrate data

37% of suspicious cloud activity indicates attempts to hack into user cloud accounts

1.3% of employees across all customer organizations were responsible for all data exfiltration, data destruction, and account takeover incidents.

Anomalous frequent downloads account for 40% of these, followed by anomalous frequent sharing at 23%—both of which indicate data exfiltration attempts. Combined, they constitute 63% of the most destructive incidents. Too many suspicious logins at 14% and anomalous frequent logins at 23% constitute the bulk of the rest of the destructive activities, and indicate account takeover attempts.

1.3% of employees across all customer organizations were responsible for all data exfiltration, data destruction, and account takeover incidents.
In 3% of companies, the vast majority of users—70% or more—are indulging in high risk behavior when using cloud apps.
The good and bad news is that high risk users are concentrated in 12% of companies. 88% of companies with no high risk users, means the risk to those businesses is reduced, but not eliminated. However, for the 12% of companies that do have high risk users, there is a 55% chance that 10% or more of users demonstrate high risk activity. Please note that the population of data examined in this report comes from organizations that have already demonstrated a higher commitment than average to secure themselves against cloud risks. These risk statistics could easily be higher for enterprises who haven’t adopted cloud security that identifies suspicious user behavior.

Over half of all organizations with employees who exhibit high risk behavior have 10% or more of their users categorized as high risk.

Identifying Threats — Is there malicious activity going on?

Elastica Cloud Threat Labs takes a multilayered data science approach to identifying malicious cloud related activity, leveraging machine learning and computational analysis to detect suspicious user behavior. Blue Coat 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 endpoints and accounts. Automated policy controls can be set to trigger when a user passes certain thresholds for very fast response.
Threats from the Leakage of Sensitive and Compliance Related Data

23% of all files stored in the cloud are broadly shared

Oversharing is particularly risky when files contain sensitive data. 12% of broadly shared documents contain compliance related data or confidential data such as source code and legal information—up slightly from 10% in the last report. This indicates that employees are storing a growing percentage of sensitive documents in file sharing apps. The increase is small but, considering leakage of these documents can be very expensive, this is a concerning trend for businesses.
Accounting shares 1 file containing PCI & PII in tabbed spreadsheet with three individuals.

Operations shares file with outside vendor for an estimate.

Sales does not see tab with compliance related data and shares with global sales group.

Marketing creates a public link instead of selecting share recipients.
What is considered sensitive data?

Not all documents stored in file sharing apps are sensitive. The majority are innocuous business files, i.e., meeting notes. For the purposes of this report, we consider compliance related data such as Personally Identifiable Information (PII), Payment Card Information (PCI), and Protected Health Information (PHI) as well as source code (Python, Javascript, etc.) to be the most sensitive data.

If we look across all industries, we find that the 12% of broadly shared files that do contain sensitive data are distributed as shown here.

Source code continues to dominate, though it is down from 48% in the last report. What has grown is the proportion of PII, up from 33%, and PCI, up from 5%.

Broken down by industry, a few expected deviations are apparent.

% of sensitive data broadly shared in the cloud
How is data identified in cloud apps?
Elastica 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 shown here.
Cost of a Typical Data Breach

Healthcare and Education face the highest financial risk from leakage of sensitive cloud data.

Elastica calculated that the potential financial impact on the average organization from the leakage of sensitive cloud data was just over $2M, up from $1.9M in the last Shadow Data Report.
Conclusion

Know your organization
Develop a comprehensive cloud governance strategy. What are your guidelines for approving/blocking cloud vendors? Guidelines on acceptable cloud application use by department and role? What is your data loss prevention policy that defines the types of sensitive data you have as a company and their relative risk if exposed? What is your process for responding to Incidents when they occur?

Know your cloud apps
Determine which cloud apps your employees are adopting and using. Then identify which are business ready and satisfy your specific security requirements, and which have insufficient security controls and must be blocked or replaced with more secure alternatives.

Know your cloud users
Understand how your employees are sharing and collaborating using cloud apps. Are they disciplined about limiting sharing to relevant contacts, or are they sharing indiscriminately? Have they committed a risky exploit such as data exfiltration and, if so, could their account or devices be compromised? How much risk do they pose to your organization going forward?

Know your cloud data
Understand what data your employees are storing and sharing in the cloud. Does a document contain PHI? PII? Source Code? Classifying your data and setting corporate usage policies around it is critical to avoid data leakage.

Knowledge is power
As shown in this report, threats to an organization’s digital security abound in the cloud. Whether it is risky apps, risky users, or insufficient data governance policies, it’s highly probable that an organization is exposed to possible compliance violations or remediation costs. To keep secure, Blue Coat recommends the following best practices.
About Blue Coat & Elastica Cloud Security

Blue Coat, Inc. is a leading provider of advanced web security solutions for global enterprises and governments, protecting 15,000 organizations including over 70 percent of the Fortune Global 500. Through the Blue Coat Security Platform, Blue Coat unites network, security and cloud, protecting enterprises and their users from cyber threats—whether they are on the network, on the web, in the cloud or mobile. Blue Coat was acquired by Bain Capital in May 2015. On June 12, 2016, Symantec and Blue Coat, Inc. announced they have entered into a definitive agreement under which Symantec will acquire Blue Coat for approximately $4.65 billion in cash. The transaction has been approved by the Boards of Directors of both companies and is expected to close in the third calendar quarter of 2016.

Elastica, acquired by Blue Coat in November, 2015, is the leader in Data Science Powered™ Cloud Access Security. Its CloudSOC™ platform empowers companies to confidently leverage cloud applications and services while staying safe, secure and compliant. A range of Elastica Security Apps deployed on the extensible 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 intrusions and compliance violations, and investigation of historical account activity for post-incident analysis.

Request a Free Shadow IT and Shadow Data Risk Assessment to Get Started
elastica.net/risk-assessment

ELASTICA CLOUD THREAT LABS

provides in-depth information and security insights of advanced threats to SaaS apps, including cloud storage services such as Google Drive, Box, Office 365, and Dropbox.

Check out the latest cloud threat discoveries.
elastica.net/CTL