The Top 7 Ways

to Protect Your Data in the New World of Shadow IT and Shadow Data

Brought to you by Elastica and Centrify

Introduction

According to research conducted by Elastica, most companies use over 500 cloud applications. Although the applications themselves can be considered secure, employees are increasingly using them without proper IT oversight and in ways that often violate corporate regulations. This paper explores the challenges of securing enterprise cloud apps and the emergence of *"Shadow IT"* and *"Shadow Data,"* and presents the top seven ways an organization can protect their sensitive data in these environments.

Trends and Challenges in IT Security

Today's CIOs find themselves in a "Catch 22." On one hand, the organization's business units demand access to certain cloud applications and services. On the other, using those applications can pose a variety of security risks. If they deny access to these applications, they may be seen as impeding business productivity. Conversely, if an organization allows cloud applications to be used indiscriminately without putting any security controls in place, the organization may suffer a security breach that could cost CIOs their jobs.

Security practices have changed considerably in the last few years. Five to seven years ago, security was defined by protecting assets within a well-defined enterprise perimeter. Enterprises relied on technologies like Intrusion detection or prevention, firewalls, data loss prevention, network vulnerability scanning capabilities, and network forensic tools. The IT team was able to do a reasonable job of protecting data within the perimeter.

The proliferation of laptops, mobile devices, and remote workers, and the prevalence of cloud applications demonstrate that traditional perimeter defense techniques are no longer sufficient. With the cloud, business units can get up and running without the oversight, blessing, or even knowledge of anyone in the IT organization—resulting in what we call *"Shadow IT."*

Leveraging cloud-based services undoubtedly provides numerous benefits: zero infrastructure costs, the ability to be up and running quickly, and immediate access to the latest and greatest software. This approach carries with it a security benefit as well. In particular, through economies of scale, many cloud service providers have more resources allocated to security than most internal IT departments can provide. However, the security capabilities that existed in the context of traditional enterprise applications are no

longer applicable in the context of cloud applications. In particular, traditional enterprise security technologies have little to no visibility into cloud application usage, even though these applications handle a wealth of sensitive information.

The next few sections will focus on the seven things your organizations can do to mitigate some of the risks of Shadow IT.

#1
Discover what's on your network

Security has to begin with some level of visibility. Every major framework for determining enterprise security strategy starts with understanding how information moves and is accessed across the enterprise to establish a baseline of activity. If enterprises don't know where they are today, it's hard to determine if subsequent security efforts are a step in the right direction.

There are essentially two kinds of organizations: those that openly use cloud, and those that use cloud but don't know they are using it. In the case of the latter, once an audit is conducted, it becomes clear that there is considerable activity outside the purview of the IT department.

This situation stems from the plethora of cloud applications that are readily available to end-users. Elastica actively tracks over 5,000 cloud applications, several hundred of which are entirely centered on file sharing. Why are file sharing applications so rampant? It is largely to get around some of the controls that IT teams have put into place.

For example, some IT organizations might block applications like Dropbox, but that doesn't stop employees from finding alternatives, like Bitcasa, to share corporate data without IT oversight.

Discovery can start simply—for example, by looking at firewall log data to see which cloud services are being accessed. To understand how these services are being used, and by whom, requires more advanced work.

#2
Assess security implications

Once an organization has discovered what's in use, they need to assess the security implications of those services and apps, especially from the perspective of an organization's governance, risk, and compliance posture. Having to perform this assessment alone is painstaking, and not all cloud apps are created equal.

For example, only some cloud apps provide two-factor authentication capabilities or password strength checks. At Elastica, we have more than 60 criteria that we use to determine whether or not an app is enterprise-ready. Some high level dimensions that are typically considered are access, service, data, and compliance.

The other critical thing to understand is how apps are being used within the environment—and it's often in unexpected ways. For example, most organizations often don't know what data is being shared via the file sharing apps the employees are using. This uncontrolled data is what is known as *"Shadow Data."*

The following diagram, based on information collection by Elastica, highlights how file-sharing applications are being used in the enterprise:

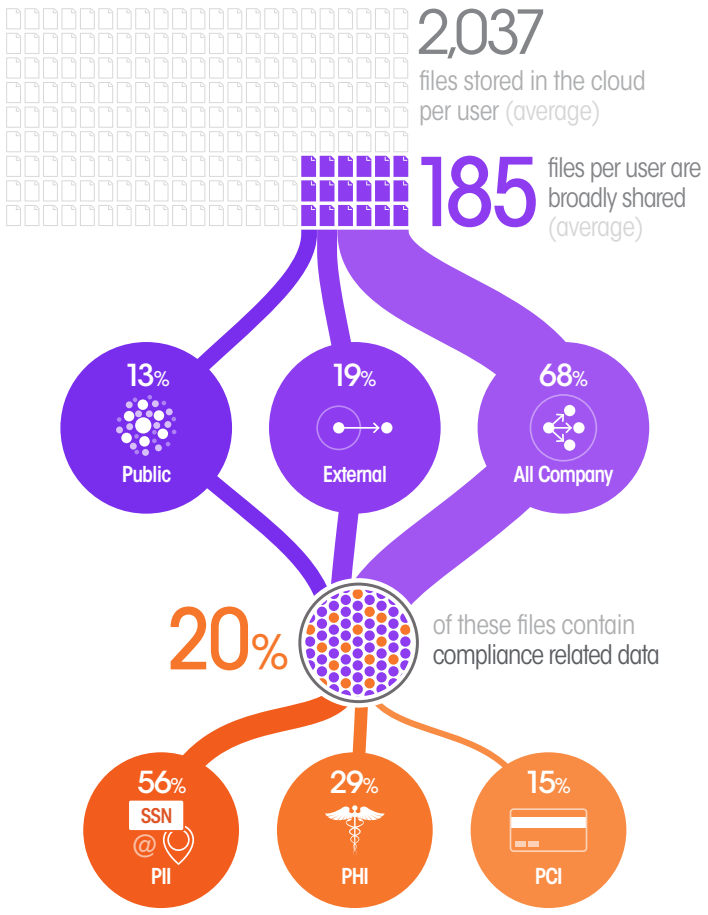


Figure 1. How file-sharing apps are being used across the enterprise

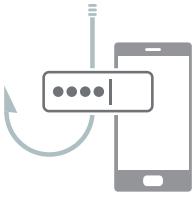
On average, there are more than 2,000 files stored per user in a cloud-based file-sharing app like Box or Google Drive. Out of these, 185 files are "broadly shared," meaning files that are either shared publicly or shared externally where they can be accessed by someone outside the organization. Alternatively, files may be shared internally but on a wide scale. Elastica found that 13% of organizations' files were shared publicly, 19% were shared externally, and 68% were shared with the entire company.

What's intriguing is that 20% of broadly shared files contain some sort of compliance-related data. That is a frightening prospect, since this content could comprise Personally Identifiable Information (PII) including Social Security numbers, Payment Card Information (PCI) including credit card information, or Protected Health Information (PHI). This type of exposure is an issue for any organization that is concerned with compliance.

How employees access cloud applications internally also matters. IT should be able to create policies for how, when and where users can access applications—and from which devices. As an example, an employee who is working at headquarters between 8am and 5pm can access Salesforce from her laptop, tablet or smartphone, but will be prompted for additional authentication when she is away from the office or working after hours.

Centrify offers the capability of protecting any cloud application with per-app and per-device policies, including multi-factor authentication. Even if a particular cloud service does not inherently provide two-factor authentication, a third-party service like Centrify can add that layer of authentication, because it provides the authentication mechanism for each app, manages the user identity within each app, and secures the devices used for app access.

When assessing security implications, organizations shouldn't just think about what the cloud service provides in isolation, but should also think about what the cloud service provides in conjunction with a third-party service, whether it be Centrify or Elastica.



#3
Act to compensate for risk

After completing risk assessment, organizations must then act on that assessment data to compensate for the corresponding risk.

The preventative actions taken in the traditional security world have been very black and white: an application or service was either allowed or disallowed. This simple binary classification stems from the very coarse blocking techniques provided by legacy perimeter security tools such as firewalls.

For cloud apps, however, a more granular control approach is needed. One example of such an approach would be to understand what is going on within the application beyond the simple fact that it is being accessed. Traditional firewalls can be used to determine, for example, that a particular user accessed a file sharing service like Box or Google Drive. What is really required for security, however, is a more detailed insight into the transaction. For example, user 'Bob' went to Dropbox or Google Drive and he shared the file named confidential.docx, which contained proprietary information, with a risky user named 'Alice' from a particular IP address.

With the deeper level of visibility, we can then put granular protection into place, such as creating specific policies around app usage, or implementing a solution that detects anomalous user behavior. An example of such aberrant behavior might include phishing attacks, insider threats, and malware. In these situations, an attacker may have gained access to a username and password, and then used it to gain complete network access.

Alternatively, there may be a situation where someone inside the organization has gone rogue and they have suddenly decided to do something to compromise the company. Since this behavior is anomalous, it can be identified and acted upon. For example, if the VP of Sales is suddenly accessing customer records that he doesn't typically touch, that could be cause for investigation. Perhaps he or she is getting ready to leave the company. The ability to understand and profile user behavior, and then look for deviations from that profile is incredibly valuable.

This type of anomaly detection approach has been implemented in the past in different contexts. Credit card companies are very good at knowing what typical transactions are, and flagging anomalous or atypical transactions. If a customer normally purchases products that are worth a few hundred dollars from New York State, but then suddenly starts logging in from Russia and starts making $10,000 worth of transactions, it is truly a behavioral anomaly of some sort, and can be blocked. The same techniques can be applied to protecting cloud services. While anomaly detection approaches are not entirely new in a security context, what makes them different for cloud services is the rich degree of content one can leverage. Having deeper visibility and deeper granularity, coupled with broader context around a transaction, allows one to make far more accurate decisions.

There are three different types of attacks that most cloud services have to be concerned with: front door attacks, back door attacks, and device theft. A back door attack involves an attacker compromising the data center from the backend, and attempting to pilfer data en masse.

A front door attack, on the other hand, would involve something as simple as a single stolen user password. It could be an insider engaged in nefarious behavior. Or perhaps a users machine was infected with a security exploit, which harvested the data in the cloud services that machine had access to. There was a recent case where a specific piece of malware targeted Salesforce. Once on a system, the exploit would piggyback between systems and connect to Salesforce through a third-party conduit. It would redirect traffic from the end-user to Salesforce, but through a third-party malicious server that would steal the user's credentials, and then would use those credentials for subsequent attacks.

Attacks like phishing, insider threats, malware, and device theft also represent front door attacks. A front door attack is one where attacker gets in without violating any of the backend mechanics, or defenses, of the cloud app. This distinction between front door and back door attacks is important, because most cloud services focus very heavily on dealing with the back door. They make sure that their back end infrastructure is protected as much as possible, but they often leave the front door unprotected, leaving it to us, the users, to deal with this vulnerability.

A third element is device theft. Devices today are very small, mobile, and can be stolen easily. If a device is physically stolen and compromised, it can provide a conduit into the enterprise data via the cloud application installed on the device.

#4

Control identity

The fourth step in the process is controlling identity. In the past, IT managed the identities for all of the resources that employees used. Even if the identity wasn't well managed, it was still relatively safe because resources were all within the corporate firewall, and attackers from outside couldn't get through. Today, people have moved their resources out of the datacenter. Either IT has deployed a cloud service themselves, or employees are moving files to an unmanaged file sharing service.

Identities now reside not only outside the firewall, but also on disparate systems. When users access cloud apps outside the firewall, their identity is not related to their central corporate identity—typically their domain account. This means that IT has no control over the access to those outside apps, and users have to remember credentials across multiple apps, sites, and services.

These issues can be solved with a centrally managed identity. IT must centralize user identity and deploy apps that support centralized identity. By implementing a cloud single sign-on solution like Centrify, employees can utilize their corporate identity, rather than manage different external usernames and passwords per app. Centralized identity is convenient for the employee, and also benefits the IT organization.

#5

Manage shared accounts

Today, employees don't often treat their credentials with the care IT would prefer, often utilizing sticky notes and spreadsheets for storing sensitive account information. End users don't fully appreciate the threats that bad password hygiene can have for their data, and the security of a business—but they are well aware of the difficulties of remembering multiple usernames and passwords for all the sites and apps they use. If IT can provide a solution that delivers app single sign-on, employees only need to remember one username and password, and the sticky notes and spreadsheets become a thing of the past. Users get easy access to apps, and IT boosts app security, and eliminates the risks of poor password management.

The next step in the process is to manage shared accounts. For example, the enterprise may only have one account with a particular supplier. The enterprise would need the ability to track the usage, so that

when someone actually uses a shared account, the system knows that it was “Joe in accounting at 10 PM from his mobile phone.” With centralized identities, a simple rule can be defined to say that specific people can use a shared identity but no one else can gain access. By using a product that enables control of shared accounts, the risk associated can be reined in.

#6

Manage provisioning and deprovisioning

Critical for controlling app security is the ability to automatically provision and deprovision accounts. As employees are hired, change job titles, move between groups, and eventually leave the company—their app entitlement and accounts should automatically change. When apps were all within the corporate perimeter, IT could easily control users’ roles and application access. Now with external systems, it’s a challenge to automatically change what rights people have as they move around the organization.

Cloud identity and access management solutions should enable provisioning and deprovisioning of users based on their roles as defined in a centralized directory service.

#7

Secure mobile devices

Once IT has better management and visibility into the security of their apps, they must finally look at the mobile devices used by employees. Bring your own device (BYOD) doesn’t have to be insecure. Not all BYOD usage is bad—people want to use their iPads to access work resources. What needs to be determined is the security posture of these devices.

Mobile device management (MDM) can enforce some policies on these personal devices. At the very least, a passcode should be set on the device. Many employees connect to their corporate accounts using personal mobile devices that don’t have even a simple passcode to prevent access in the case that the device is lost or stolen.

With the right mobile solution, however, IT can also track the types of app installed on the devices and possibly provide blacklisting and whitelisting of apps. Containers can be utilized, which are special subspaces in a mobile environment that allow apps to be run in a more secure place. For example, Samsung’s container technology called Knox, Apple iOS 8, and other vendors provide solutions to create a much safer environment for running apps.

Any mobile device solution should also integrate with the central identity and access management solution. This allows matching new devices to existing users from the central user databases. The provisioning and management of the devices can be linked to the provisioning cycle of employees.

The most advanced cloud identity services allow IT to include device posture as part of app access policy. In this case, IT can allow access to a specific app only from managed devices, with secure passcodes, and even then only on specific networks. All of these capabilities combine to make the mobile platform that is much more secure and helps mitigate against the weak security postures of most unmanaged mobile devices.

Conclusion

The rapid growth in the use of cloud applications and mobile and personal devices by employees presents unique security challenges for corporate IT departments. Though cloud applications are generally considered secure, the responsibility of ensuring proper access control, security, and compliance remains with the company. This requires organizations to develop risk mitigation best practices for adopting cloud applications. The process starts with uncovering “Shadow IT” where organizations discover and assess the risk posed by the cloud applications used by employees. The access to sanctioned cloud applications should then be controlled and managed through the use of a full featured IDaaS. The security implications of data residing and being shared on the cloud application must be assessed for compliance and exposure risks. Finally, the use of cloud applications by employees must be continuously monitored to uncover risky or anomalous behavior to proactively identify and protect against internal or external threats.

By implementing risk mitigation best practices for cloud applications, corporations can remediate the risks presented by “Shadow IT” and “Shadow Data” and securely enable cloud applications for employees while protecting their sensitive data in these environments.

About Elastica

Elastica is the leader in Data Science Powered™ Cloud App Security. Its CloudSOC™ platform empowers companies to confidently leverage cloud apps 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 app 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. Learn more about Elastica at http://www.elastica.net. Follow us on Twitter @ElasticaInc

About Centrify

Centrify provides unified identity management across cloud, mobile and data center environments that delivers single sign-on (SSO) for users and a simplified identity infrastructure for IT. Centrify's unified identity management software and cloud-based Identity-as-a-Service (IDaaS) solutions leverage an organization's existing identity infrastructure to enable single sign-on, multi-factor authentication, privileged identity management, auditing for compliance and enterprise mobility management. Centrify customers can typically reduce their total cost of identity management and compliance by more than 50 percent, while improving business agility and overall security. Centrify is used by more than 5,000 customers worldwide, including nearly half of the Fortune 50 and more than 60 Federal agencies. For more information, please visit http://www.centrify.com/. Follow us on Twitter at @Centrify.

Try Centrify Identity Service for free at www.centrify.com/express/identity-service/