Cloud Cybersecurity Report
The Extended Perimeter

DATA

APPS

ACCOUNTS

Q1 2015 REPORT
Executive Summary

The adoption of public cloud applications continues to accelerate for both organizations and individuals at an exponential rate, evidenced across the massive growth in the volume of accounts, files, collaboration, and connected third-party cloud applications.

The rapid surge of accounts, files, and applications presents increased risk in the form of an extended data perimeter. The adoption of cloud applications has significantly increased the threat surface for cyber attacks. Faced with this massive growth and the elevated risk, security professionals are looking to enable their organizations to embrace and leverage the benefits of cloud technologies while remaining secure and compliant.

“Sensitive data is moving to the cloud, beyond the protection of your perimeter controls. ... As this occurs, the amount of data, and, most importantly, the amount of sensitive or ‘toxic’ data the enterprise stores in these software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS) platforms is increasing by the day - and regardless of its locations, S&R pros still need to protect it effectively.”

Forrester Research (2015, March)
Market Overview: Cloud Data Protection Solutions

Key Findings

The Attack Surface: Exponential Growth in Corporate Cloud Adoption Per Organization

- ↑4x External collaboration via public cloud applications
- ↑4x Number of unique third-party cloud applications connected to corporate systems
- ↑10x Files stored in public cloud applications from last year
Increased Security Risk

100,000 files per organization that represent risk

Number of files per organization stored in public cloud applications that violate corporate data security policy, amplifying the danger of exposing sensitive information.

4,000 exposed files per organization contain username & password information

Number of exposed files per organization stored in public cloud applications containing credentials to corporate systems, inviting cybercriminals to hijack corporate SaaS environments.

1 in 4 employees violating security policies

Number of employees that violate corporate data security policy in public cloud applications, opening organizations to risk of data breach and compliance concerns.

45,000 third-party apps installs conducted by privileged users

Third-party cloud applications with access to privileged users accounts significantly elevates organizational risk.
One in Four Users Violate Security Policies in the Cloud

There’s no question that the hypergrowth of public cloud applications raises data governance and cybersecurity concerns. On average, 12% of files within an organization’s SaaS portfolio contains sensitive data, while nearly one in four users (25%) own data that violates corporate security policy.

The average organization has 100,000 files that contain sensitive information stored within public cloud applications. Considering users’ heightened ability to access and distribute information in cloud apps, such a high volume of sensitive files raises data protection concerns.

On average, each organization found a staggering 4,000 instances of exposed credentials. These usernames and passwords were excessively accessible across the entire company, externally, or, in the most severe cases, publicly - a cybersecurity attack waiting to be realized.

Forrester explains “Many breaches are the result of insider activity,” sharing that 46% of breaches are due to user behavior.

Forrester Research (2015, March)
Market Overview: Cloud Data Protection Solutions
65% of Security Teams Care About What Type of Sensitive Data is Exposed, 35% About How/Where it is Exposed

Organizations are taking two main approaches to protect their most sensitive corporate assets in the cloud through security policies. 65% of organizations worry primarily about what type of sensitive data is exposed while 35% worry about where information is exposed as a starting point for their cloud cyber security strategy.

Focus on What Data is Exposed

Information that organizations worry about most includes intellectual property and confidential information (59%), PCI data - credit card data (19%), PII data - social security numbers (13%), objectionable content for CIPA compliance - e.g. curse words, harassment (5%) and PHI/healthcare related data such as medical conditions, prescription drug terminology, patient identification numbers, or medicare identification numbers (4%).
Focus on Where Data is Exposed

An organization on average collaborates with 865 other organizations. Between 2014 and 2015, external collaboration via public cloud platforms increased four times. 35% of organizations exclusively worry about how information is exposed as a starting point for their cloud cyber security strategy. These files are then further broken down by accessibility, for instance: organization-wide (anybody within the company), externally accessible (specific external collaborators such as a partner), and publicly accessible. As many public cloud applications allow files to be indexable by search engines, the risk implication of 24,000 publicly-accessible files per organization is immense.

By focusing on exposed information, organizations are capable of assessing the risk of this data and then choosing from several options. Security teams can notify end users to raise awareness, asking end users if they are aware of what they are sharing and if they are confident it is appropriate to share, they can revoke sharing and quarantine the information, or they can narrow in on excessively risky sharing, such as sharing with competitors, or files that contain sensitive information.

Data Exposure per Organization

An organization on average collaborates with 865 Other Organizations

In the last year alone, external collaboration via public cloud applications increased four times.

<table>
<thead>
<tr>
<th>Accessible Publicly</th>
<th>Accessible by External Collaborators</th>
<th>Accessible Organization-Wide</th>
</tr>
</thead>
<tbody>
<tr>
<td>2%</td>
<td>10%</td>
<td>12%</td>
</tr>
</tbody>
</table>

24,000 Files
Publicly accessible per organization
70% of Corporate Cloud-Based External Collaboration Occurs With Non-Corporate Entities

Public cloud applications are often used for their ability to share files and collaborate. While users have the potential to exercise a high degree of control over the accessibility of their files, the volume of excessively exposed content may be surprising, with 12% available organization-wide, 10% exposed externally, and 2% accessible publicly, as mentioned above.

The overwhelming amount of collaboration with personal, non-corporate email addresses (such as Gmail, Yahoo, Hotmail, and so on) suggests potentially inappropriate sharing, such as stockpiling of company assets for personal use. This diversion of corporate assets means organizations are no longer in control of the accessibility of potentially sensitive information - a compromise to the integrity of the security program given the increased susceptibility of individuals to cyberthreats.

Anatomy of a Cyberattack

In examining enterprise collaboration via public cloud applications, CloudLock discovered a fascinating phenomenon: 6% of collaboration is occurring inbound-only, suggesting the potential malicious use of collaboration as a mechanism to execute phishing attacks. For instance, consider a cybercriminal flooding an organization with files resembling typical business documents. Within the documents resides a disguised phishing attack to lure employees. Should the employee then unintentionally click on links within the document, they initiate an attack leading to a data breach.
77,000 Third-Party Cloud Apps Discovered That Touch Corporate Systems

Third-party cloud application usage is increasing exponentially year over year. CloudLock focuses on the riskiest of third-party cloud applications - the cloud apps users enable with their corporate credentials to connect to core business systems via OAuth, introducing cybersecurity implications.

CloudLock sees a 4x increase in the number of third-party applications enabled per organization, from 130 to 475. The total number of unique third-party cloud apps ballooned to 77,000, amounting to 2.5 million installs. Meanwhile, third-party SaaS application installations performed by privileged users (administrators and super admins) has grown to represent 2% of all third-party app instances.
Top Third-Party Apps
Gaming / Entertainment / Non-Productivity Apps

Unique Apps by Category

Color shows sum of total installs
Third-Party Cloud Apps Expose New Cyberthreats

Third-party cloud applications are user-enabled Software-as-a-Service apps that communicate with core, corporate SaaS platforms via an OAuth connection. In order to offer users beneficial functionalities and automate activities, third-party cloud applications typically request permission to act on behalf of the user.

Many apps request not only the ability to view basic profile information and files, but go as far as to modify, manage, and potentially delete corporate data the user has access to. As 12% of information within an organization’s SaaS portfolio is sensitive in nature, such extensive access scopes raise cybersecurity and data protection concerns.

Given their elevated access and privilege levels, the risk implication grows considerably in the instances of administrators enabling such apps - a highly discouraged practice that comprises 45,000 (2%) of application installs. Consider the example of a super administrator enabling a third-party cloud application with an extensive access scope. In the event the application vendor was compromised and the app hijacked in a cyber attack, the malicious party would be capable of impersonating the super administrator to take full advantage of their elevated privileges, including the ability to delete accounts, externalize or transfer data, provision and deprovision users, change all users’ passwords, modify administrator’s settings, perform email log searches, and perform audit large searches.
Over Half of Third-Party Apps Banned due to Security Concerns

While enterprise SaaS vendors typically offer a marketplace of third-party applications that have been vetted and undergone security review, users have no shortage of additional means of enabling third-party apps, raising issues around trustworthiness and security. Over half of third-party apps assessed in 2015 are banned due to security-related concerns, with security professionals citing excessive access scopes in 24% of bans and subpar vendor trustworthiness (applications of questionable origin or intent) 30% of bans.

The Weaponization of Third-Party Apps

Security professionals are not the only ones aware that many third-party apps demand extensive permission sets. Third-party SaaS application vendors represent a valuable payload to cybercriminals. Should a vendor be compromised, the malicious individual would be able to leverage the permissions your employees granted to the application to access, exfiltrate, and externalize sensitive information and otherwise wreak havoc within the cloud environment of all organizations with at least one instance of the application.
Turning Insight into Action

Modern enterprises are building their digital backbone in the cloud. Adopting cloud applications affords organizations a wide range of benefits, including dramatic reductions in total cost of ownership, increased flexibility and scalability, a transition from capital expenditure to operational expenditure, and a substantial boost to employee productivity.

Cloud application providers are taking great strides in securing access at the infrastructure layer and have never been more secure. So risk does not stem from the fact that cloud applications are used. Rather, risk is a product of neglecting the extension of the perimeter introduced by cloud applications. At the center of the expanded perimeter is the user, intersecting data, user profiles and applications.

Security professionals can not only keep up with the increased security demand of the cloud but can actually align security with the business strategy of their organizations. A few best practices CloudLock recommends:

1. Continuously monitor your cloud environments at the application, platform, and infrastructure layer.

2. Gain deep insight into what information is shared and how it is shared.

3. Analyze user behavior and look for anomalies that could indicate a potential cyber attack or malicious insider behavior.

4. Understand what applications your users are using with a strong focus on those apps that actually connect into your corporate environment.

5. Treat your users as part of the solution, not part of the problem. Users can be a great asset in your cloud cybersecurity strategy and can actually serve as an accelerator to new cloud adoption. Focus on training, raising awareness and giving them access to new productivity tools they are uncovering rather than blocking or changing application behavior. If you don’t, users will find workarounds, anyway.

6. Take risk-appropriate controls. Not all files in your cloud apps are going to be equally important. Focus encryption on those assets that matter most.

7. Trust the insight of the security community, tapping into crowdsourced insight will be much more reliable than vendor-based security ratings.
Methodology

CloudLock bases findings on anonymized usage data over 2014 and 2015

- 77,500+ Apps
- 750 Million Files
- 6 Million Users
CloudLock offers the cloud security fabric enabling enterprises to protect their data in the cloud, reduce risk, achieve compliance, manage threats and increase productivity.

By analyzing **15 billion+ objects** for more than **6 million** end users daily, CloudLock delivers the only complete, risk-appropriate and people-centric approach to cloud security.

🌐 www.cloudlock.com  📧 info@cloudlock.com  ☎️ (781) 996-4332