CipherCloud®
Trust in the Cloud™

CLOUD ADOPTION & RISK REPORT FOR NORTH AMERICA & EUROPE

2014 Trends

333 W. San Carlos Street
San Jose, CA 95110

EXECUTIVE SUMMARY

Few advances come close to the power of cloud computing to re-chart the path of enterprise IT. With faster time to market, massive economy of scale, and unparalleled agility, the cloud is being adopted by enterprises at an unprecedented rate.

At the same time, however, few organizations have a strategic and coherent approach to managing cloud security and risk. Limited visibility, uncertain responsibility boundaries, and the lack of effective governance frameworks have all contributed to the current state of the art. As one Fortune 500 company CISO puts it: "Go to the cloud and hope for the best."

This report, with insights drawn from CipherCloud's customers and our extensive cloud risk knowledge base, helps to shed light on enterprise cloud usage, risks observed, and geo-specific trends. This report includes anonymized data of cloud user activity collected for the full 2014 calendar year, spanning thousands of cloud applications and millions of enterprise cloud users.

> "Organizations vastly underestimate the level of Shadow IT."

Our findings suggest that organizations vastly underestimate the level of Shadow IT when it comes to cloud adoption. As a result, hundreds of high-risk cloud applications are in common use across North America and European enterprises.

To achieve governance, it is imperative that organizations build the necessary legal and technological infrastructure to address cloud risks. This report discusses key points of focus for enterprise IT in order to address the competing tensions between business efficiency and security control and visibility.

Key Findings

- **The average global enterprise utilizes over 1,100 cloud applications**
  Our study found widespread cloud adoption across North America and Europe. In our 2014 data, a typical North America enterprise used over 1,245 cloud applications while those in Europe used 981 applications on average.

- **86% of cloud applications used by enterprises are unsanctioned "Shadow IT"**
  Our study found that enterprises vastly underestimate the extent of Shadow IT cloud applications used by their organizations. Various media sources claim 10% to 50% of cloud applications are not visible to IT. Our statistics show that on average 86% of cloud applications are unsanctioned. For example, a major US enterprise estimated 10–15 file sharing applications were in use, but discovered almost 70.

- **Publishing, Social, and Career clouds are 2014's most risky cloud categories**
  Our research rated 52% of applications in Publishing as high risk. Similarly, 42% in Social and 40% in Career clouds are rated as high risk. These three represent the highest risk across all cloud applications.

- **Europe is narrowing the gap of cloud adoption to North America**
  Contrary to widespread beliefs that Europe lags North America significantly in cloud adoption, our research found that European enterprises leverage the cloud just as extensively as North America—an average European organization used 80% as many cloud applications in 2014, distributed across similar application categories.

- **70% of US cloud applications used by European organizations are not "Safe Harbor" approved**
  In our data set, we found that only 9% of the clouds used by European enterprises were either Europe-based or in European-approved data transfer regions; 21% were US clouds and Safe Harbor approved. The rest, a whopping 70%, were US clouds without Safe Harbor certification.

The CipherCloud Risk Model

CipherCloud is committed to providing enterprises with accurate risk ratings based on open standards, a transparent process, and the most current risk factors. The CipherCloud Risk Intelligence Lab™ uses the principles of transparency, community, and alignment with standards to provide extensive research, automated testing, and expert analysis of cloud application risks.

SECURITY	PRIVACY	ENVIRONMENT	COMPLIANCE
• Multi-factor Authentication • Single Sign-On • Encryption of data-at-rest • SSL/TLS • Landing domain • Login domain • HTTP headers	• Privacy policy • Cookie policy • Data retention Data ownership • Third-party access • Business Transactions • Privacy Compliance • Data Residency	• Location • Service Level Agreement • Disaster recovery • Multi-tenancy • Type of usage • Control of environment • Data breaches	• Safe Harbor • Comodo • ISO 27001 • PCI AoC • HIPAA • FedRAMP • CSA CCM • SAS 70 • SSAE16 • SOC 1, 2, 3

Figure 1: CipherCloud risk model components.

The CipherCloud Risk Intelligence Lab™ analyzes tens of thousands of cloud applications globally in the compiling its CloudSource™ knowledge base. CipherCloud utilizes a standards-based model for cloud risk scoring, with over 100 attributes across four risk categories: Security, Privacy, Environment and Compliance. The cloud risk model includes security controls defined by the Cloud Security Alliance Cloud Control Matrix, Privacy best practices detailed by TRUSTe, and industry and regulatory standards such as HIPAA and PCI DSS. Figure 1 provides a more detailed view of the attributes used in our cloud risk model.

CipherCloud examines factors such as whether the cloud application uses multi-factor authentication, whether data stored in the cloud is encrypted, the location of cloud data centers, third-party data access, and compliance certifications. All risk attributes are independently verified by our staff of expert researchers. Risk scores range from 1 (lowest risk) to 10 (highest risk).

Cloud Computing Is Transforming the Global Enterprise Right Under Our Eyes

CipherCloud research found that enterprises in both North America and Europe are leveraging cloud applications extensively. An average global enterprise uses over 1,000 distinct cloud applications (see Figure 2). The number of applications used in North America (1,245) is slightly higher than that in Europe (981).

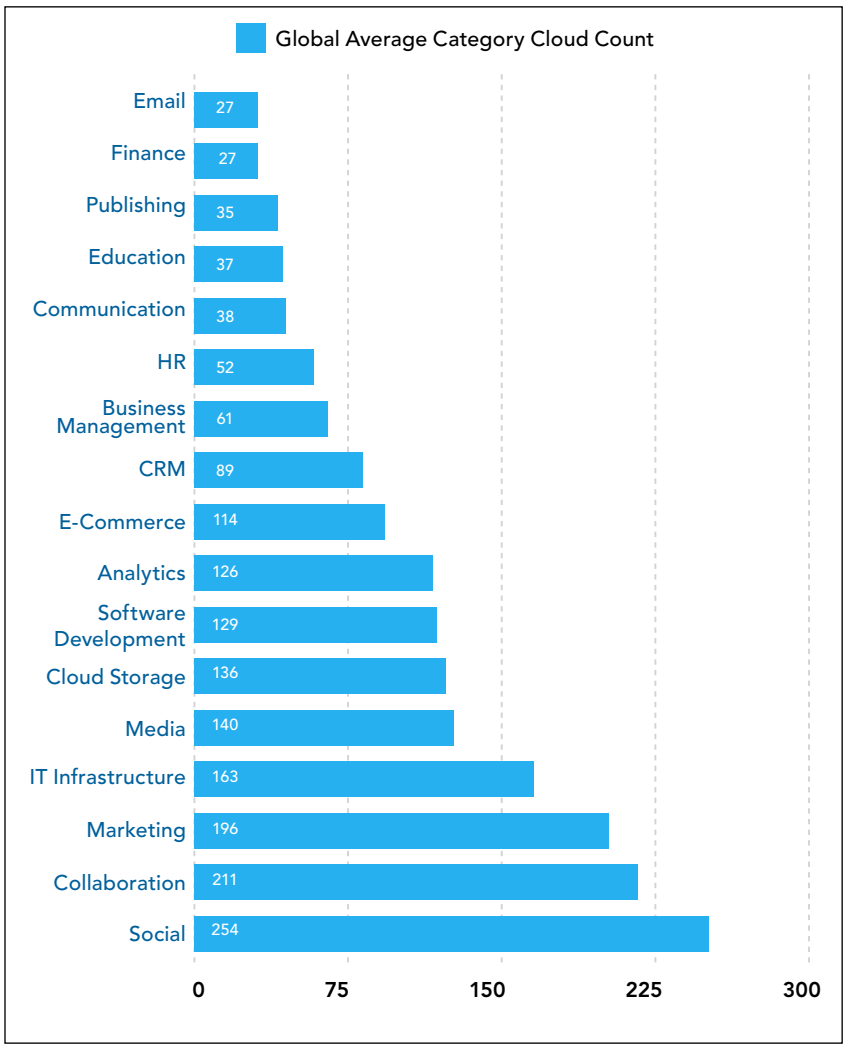


Figure 2: Average number of cloud applications accessed globally by enterprises by category.

Figure 2 shows the global average ranking of cloud applications by popularity. Social, Collaboration, Marketing, and IT infrastructure are the most popular cloud categories—an average enterprise uses approximately 100 different applications in each of these categories.

Enterprises Underestimate the Extent of Shadow IT

We all know that the use of Shadow IT within businesses is exploding, but few enterprises have been able to accurately assess the extent of the problem. Self-reported surveys of the percent of enterprises using cloud services range from as low as 19%[1] to 50%—clearly ignoring Shadow IT. Other surveys have shown as many as 80%[1] of end-users admitting to using unsanctioned applications, but without any measurements of actual usage.

CipherCloud worked closely in 2014 with large enterprises globally to discover all cloud applications in use, and compare them with internal metrics of what is approved. The chart below compares IT approved applications with Shadow IT across North American and European enterprises.

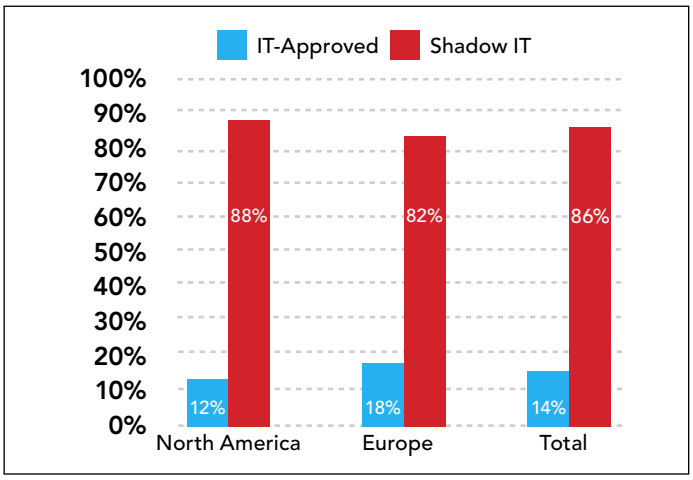


Figure 3: IT-approved applications vs. Shadow IT globally in 2014.

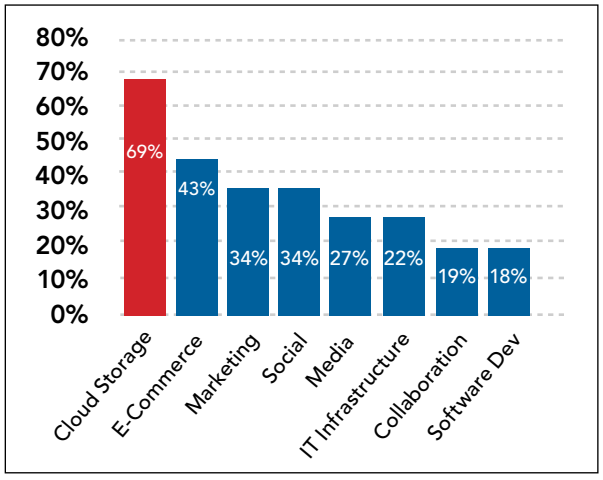


Figure 4: Cloud applications discovered by a major enterprise by category.

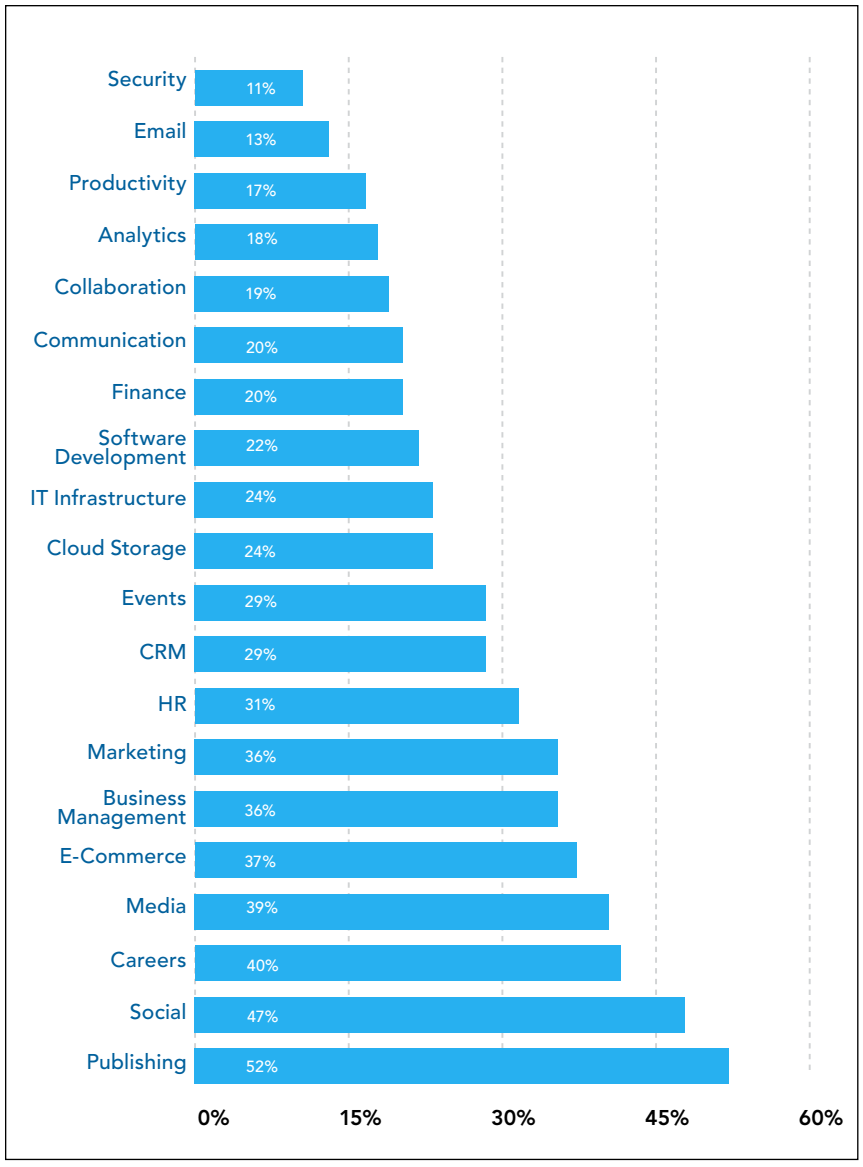
Specific anecdotes also help to illustrate the problem. A major US enterprise used CipherCloud to discover all their cloud applications in use. They expected to find 8–10 applications being used for file sharing, and were very surprised to find 69 separate applications in use for file sharing, with a large number of high-risk clouds.

[1] Eurostat survey of enterprise cloud adoption for 2014 (http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises)
[2] Frost & Sullivan—The Hidden Truth Behind Shadow IT: http://www.mcafee.com/us/resources/reports/rp-six-trends-security.pdf

Publishing, Social and Career Clouds Are 2014's Top Three Most Risky Cloud Categories

Information workers frequently use publishing, social, and career cloud applications to do their jobs, often with great effect. However, our research showed that in 2014 these three categories comprise the top three most risky clouds: Our intelligence lab rated 52% of Publishing cloud applications as high risk. Similarly, 42% in Social and 40% in Career clouds are deemed high risk.

Software Development, Cloud Storage, IT Infrastructure, CRM, HR and Business Management categories also had significant percentages of applications with an overall risk score of 8 or higher (22%–36%).



Examples of the types of applications in the top categories:

- **Publishing:** Wordpress, Adobe Creative Cloud
- **Social:** LinkedIn, Twitter
- **Careers:** Indeed, Resumonk

Figure 5: Top 20 cloud application categories by percentage of high risk cloud providers.

Europe Narrows the Gap in Cloud Adoption

Contrary to conventional wisdom that Europe lags North America in cloud adoption, CipherCloud research found that European enterprises have largely caught up to US in cloud usage. More specifically, we found that top cloud applications used by European enterprises are in largely the same categories as those used in North America, albeit European companies use 80% as many applications on average (see Figure 6). For example, North America organizations used an average of 94 IT Infrastructure applications, compared with 69 in Europe. Similarly, North America companies used on average 68 analytics clouds and Europe used 58.

This may have to do with the fact that Europe's cloud application market is projected to grow faster than North America through 2018. One analyst firm estimates that Europe will grow at a 19.1% CAGR while North America will grow at a 15.9% CAGR[3].

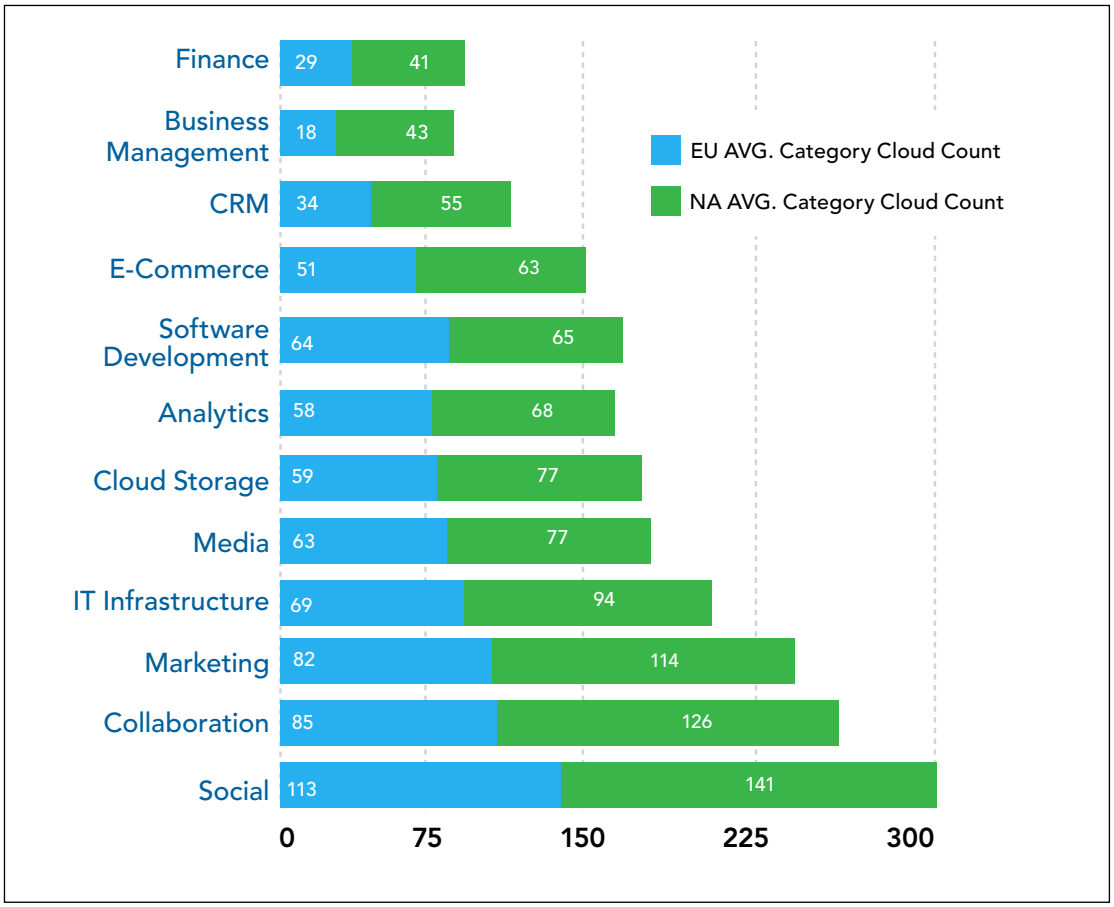


Figure 6: Average number of cloud applications accessed by North American and European enterprises by category.

[3]Apps Run the Cloud: https://www.appsrunthecloud.com/opinions/index/150

European Enterprises Are as Cloud-Risky as Those in North America

CipherCloud found that an average North American enterprise uses 1,245 cloud applications while 981 applications were found in use by an average European firm. With that many cloud applications, an average of 56 high-risk clouds per organization were found in North America and 42 high-risk ones per organization were found in Europe. Perhaps more alarmingly, in both North America and Europe, over 300 users per organization were found using high-risk clouds in 2014 (see Figure 7).

Figure 7 also depicts a break down between high-, medium-, and low-risk clouds in use by both geos. A similar pattern was observed throughout, with the exception that a higher percentage of medium-risk clouds were used in Europe vs. North America.

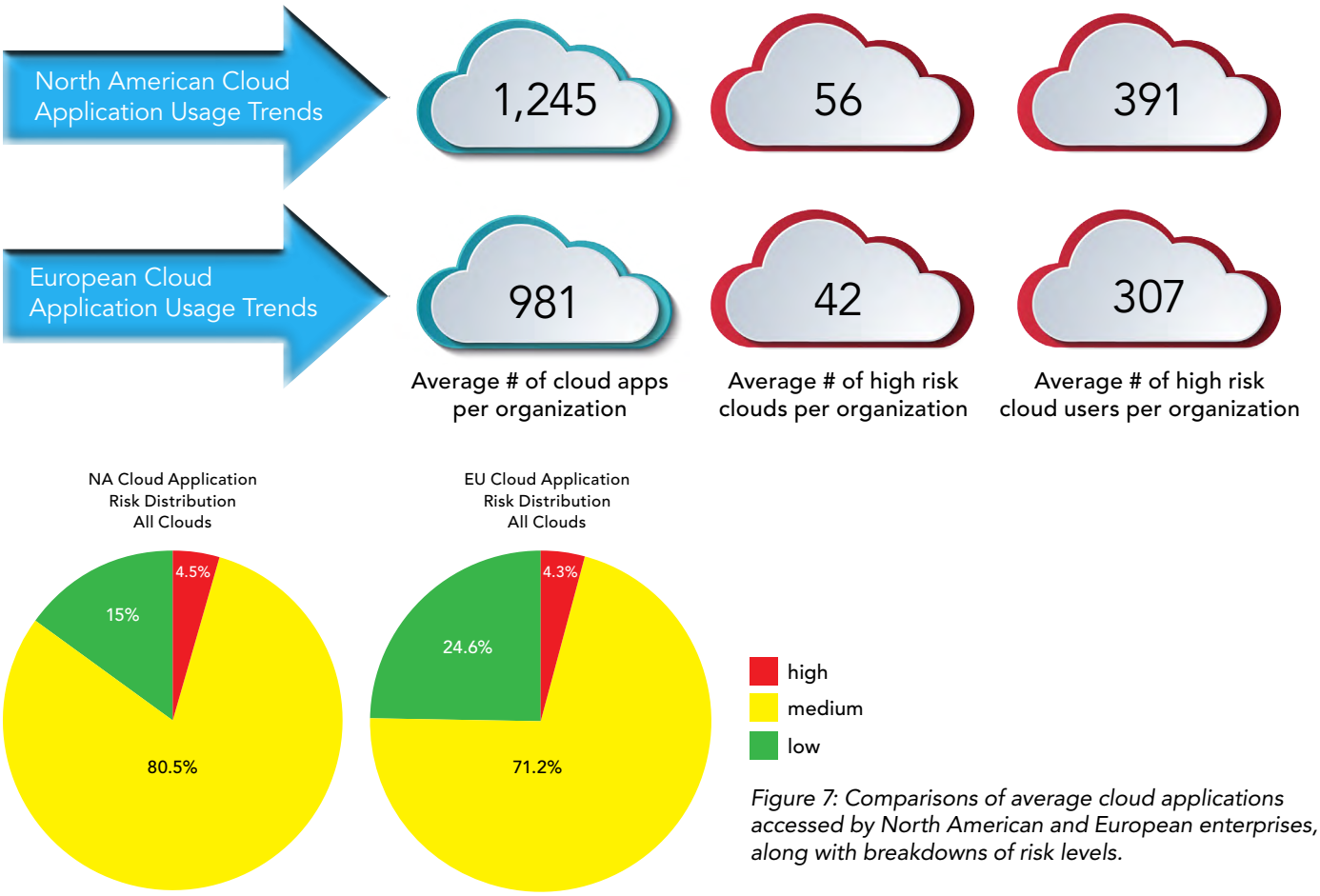
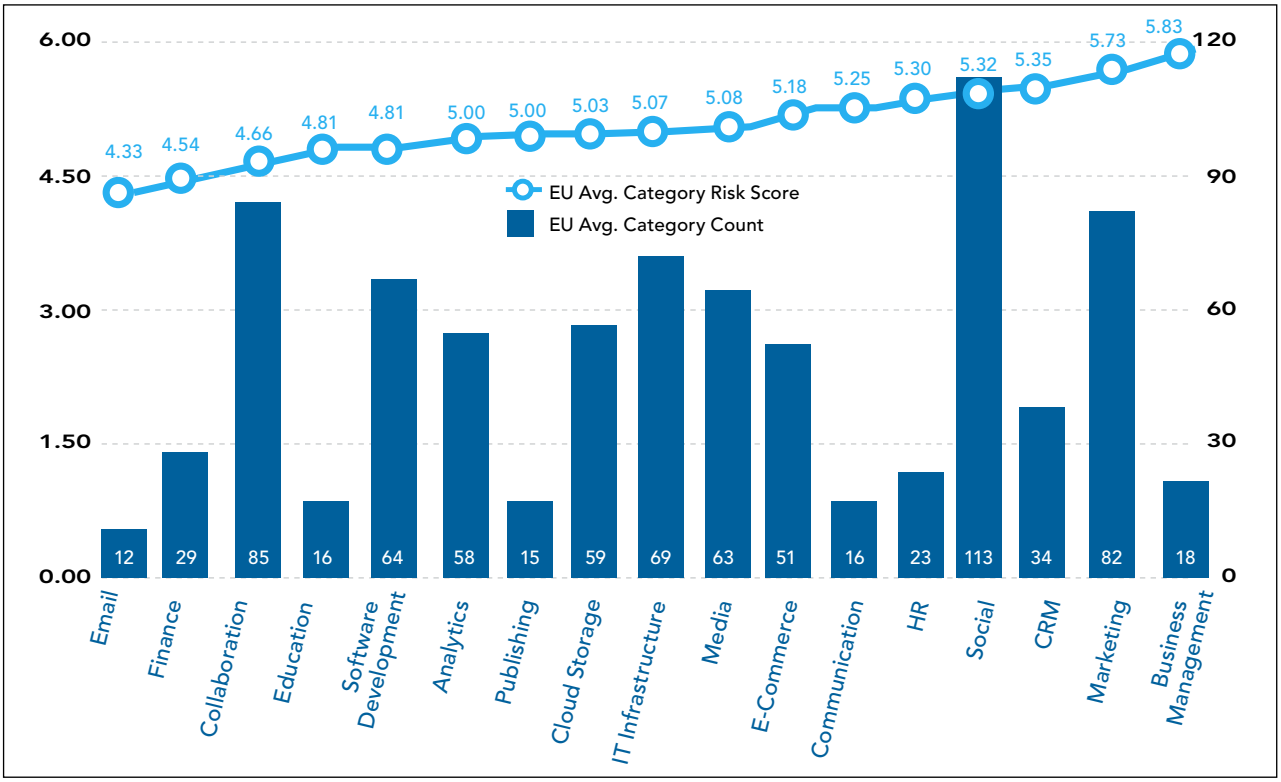


Figure 7: Comparisons of average cloud applications accessed by North American and European enterprises, along with breakdowns of risk levels.

Figure 7 shows a deeper look at each cloud application category used in North America and Europe, as well as the associated risk scores. Overall, the categories in use and the risk scores are fairly comparable between the two regions, with a few exceptions. For example, the average risk score for software development clouds used by North America (5.15) is noticeably higher than those used in Europe (4.81), even though both regions used a similar number of cloud applications for software development. In contrast, communication clouds used by European companies carry a higher average risk score (5.25) than those used by North America (4.86).



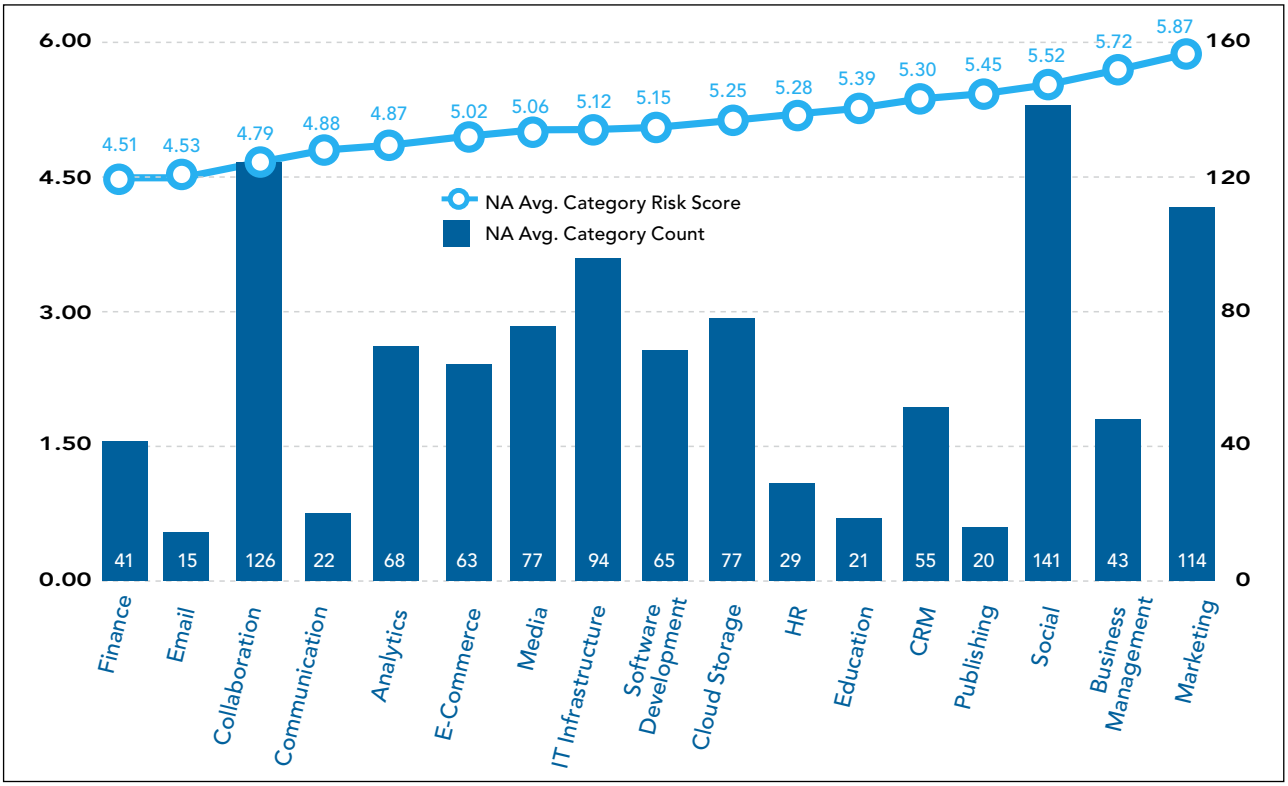


Figure 8: Comparison of commonly used cloud application categories in Europe (top) and North America (bottom), as sorted by the average risk score per category.

European Companies Are Not Enforcing "Safe Harbor" Principles with Cloud Applications

European Union data privacy laws require that transfers of personal information be restricted to European Union member states, or countries approved by the European Union for international data transfer. The US does not have country-wide approval, but US businesses can become Safe Harbor compliant by following seven fundamental data protection principles, and hence become eligible to handle transfers of personal data from European territories.

By Law, European organizations can only transfer personal data to US businesses that are "Safe Harbor" certified. In practice, however, this seems to have little impact on actual cloud usage by enterprise users. CipherCloud research found that 70% of cloud applications used by European organizations are based in the US and not Safe Harbor approved. Only 9% of applications accessed were based in Europe and approved data transfer regions while 21% were US "Safe Harbor" compliant clouds.

This trend likely corresponds with Shadow IT. Enterprise-sanctioned cloud applications used in Europe are more likely to be Safe Harbor certified, while those accessed directly by end-users appear to be largely non-compliant.

A 2013 study by the European Union Commission found that the US-EU Safe Harbor principles are not well enforced; over 30% of Safe Harbor certified providers violate at least one of the Safe Harbor principle requirements.

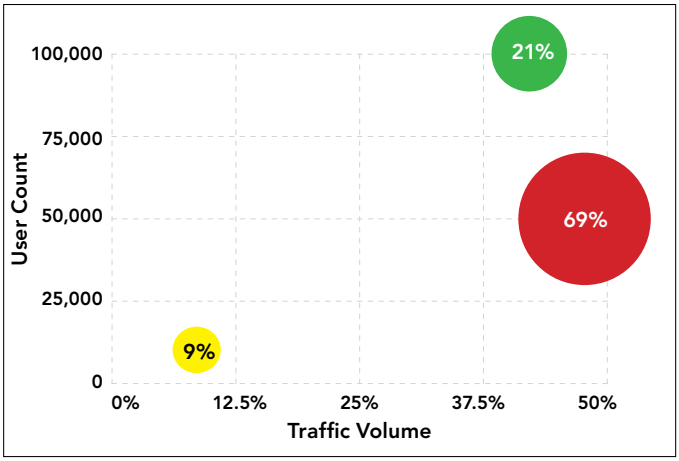


Figure 9: Distribution of EU-based, Safe Harbor-certified, and non-Safe Harbor cloud applications.

EU Safe Harbor Compliance (45 days of user activity)

EU Safe Harbor Certified	Cloud App Count (%)	Total Traffic Volume (%)	Total Users*
EU-based	9%	8%	10204
YES*	21%	42.4%	98716
NO*	69%	49.6%	46307

*US-EU Safe Harbor is a streamlined process for US companies to comply with the European Union Directive 95/46/EC on the protection of personal data. The Safe Harbor Privacy Principles allow US companies to register their certification if they meet the European Union requirements via the US Department of Commerce.

Call to Action

Cloud computing offers organizations a rare chance to challenge the status quo in technology delivery methods and has already had a global impact on the traditional IT stack. To unlock the power of the cloud and at the same time effectively manage the tension between business efficiency and enterprise controls, CipherCloud recommends these strategic areas of focus:

1. Designate cloud security as a strategic area of IT security
2. Enhance cloud situational awareness and improve your cloud governance posture
3. Establish a systematic, integrated technological approach to support your governance needs

To support these goals, firms should undertake the following immediate actions:

- **Develop a multi-faceted cloud governance and control framework:** Combine commercial best practices, regulatory obligations, and line-of-business requirements to form a sustainable cloud governance strategy. As part of this governance strategy, take a deep dive into your cloud user activities by department and business function, and understand the business needs for each cloud application. Balance these needs with your regulatory requirements to develop a practical and meaningful control framework.

- **Establish integrated technologies to discover, protect, and monitor cloud usage:** Discover who is doing what with which cloud applications is only the first step. You need to make sure that you have ongoing means to manage cloud access and exert continuous controls. In addition, your controls need to be granular enough to meaningfully limit your data exposure to the cloud without hindering cloud functionality. Most importantly, discovering, protecting, and consistently monitoring should be integrated functions rather than discrete capabilities that you have to manage separately.

- **Be proactive in your cloud management strategies:** Do you have a way to enhance cloud literacy across your organization both in terms of risk education as well as best practices? Can you utilize your user access pattern to guide and optimize your cloud adoption? Do you have a way to consolidate redundant applications and can you effectively migrate users from risky apps to approved ones?

> "Never again should it be possible to say 'We didn't know' or 'we were surprised,."
>
> "No data movement to and from the cloud and everywhere in between should be invisible and uncontrolled."

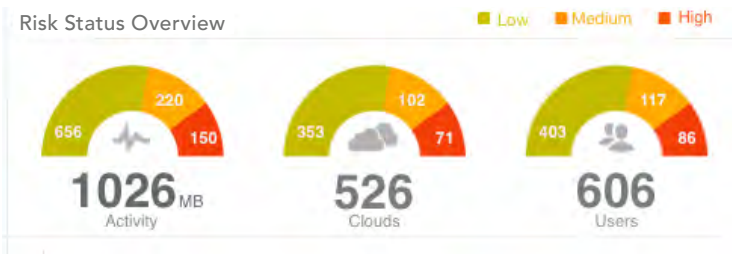
These are the statements from practitioners living in the world of cloud transformation and this is the reality that CipherCloud is here to enable.

About CipherCloud for Cloud Discovery

CipherCloud for Cloud Discovery makes it simple and cost effective to continuously discover and categorize all the cloud applications users are accessing, identify the risks for each application, and analyze the impact on the company's network resources and compliance posture. Intuitive drill-down dashboards provide detailed information on the top cloud applications being accessed by number of events, data volume, and risk level.

Our rich knowledge base, CloudSource™, supports a growing list of thousands of applications. CloudSource tracks more than a 100 granular risk metrics across security, privacy, compliance, environment and legal categories for each application.

Also, CipherCloud for Cloud Discovery is unique because it does not require you to share sensitive log data outside the organization. The solution is built on a popular and highly extensible platform, enabling detailed analysis of logs from proxy servers and firewalls.



CipherCloud
Trust in the Cloud

CipherCloud, the leader in cloud visibility and data protection, delivers cloud adoption while ensuring security, compliance and control. CipherCloud's open platform provides comprehensive cloud application discovery and risk assessment, data protection—searchable strong encryption, tokenization, data loss prevention, key management and malware detection—and extensive user activity and anomaly monitoring services.

CipherCloud is experiencing exceptional growth and success with over 3 million business users across 11 different industries.

The CipherCloud product portfolio protects popular cloud applications out-of-the-box such as Salesforce, Box, Microsoft Office 365, and ServiceNow.

Named SC Magazine's 2013 Best Product of the Year, CipherCloud's technology is FIPS 140-2 validated and the company is backed by premier venture capital firms Transamerica Ventures, Andreessen Horowitz, Delta Partners, and T-Venture, the venture capital arm of Deutsche Telekom. For more information, visit www.ciphercloud.com and follow us on Twitter @ciphercloud.

WP-CC-RN-20150202

Headquarters:
CipherCloud
333 West San Carlos Street
San Jose, CA 95110
www.ciphercloud.com

sales@ciphercloud.com
1-855-5CIPHER (1-855-524-7437)