<table>
<thead>
<tr>
<th>No.</th>
<th>Section Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>INTRODUCTION TO THE CLOUD ADOPTION AND RISK REPORT</td>
</tr>
<tr>
<td>02</td>
<td>THE BASICS: STATISTICS ON CLOUD ADOPTION AND RISK</td>
</tr>
<tr>
<td>03</td>
<td>THE COVETED TOP 20 ENTERPRISE CLOUD SERVICES LIST</td>
</tr>
<tr>
<td>04</td>
<td>TOP 20 CONSUMER APPS IN THE ENTERPRISE</td>
</tr>
<tr>
<td>05</td>
<td>TOP 10 FILE SHARING, COLLABORATION, AND SOCIAL MEDIA CLOUD SERVICES</td>
</tr>
<tr>
<td>06</td>
<td>JUST ANOTHER DATA BREACH?</td>
</tr>
<tr>
<td>07</td>
<td>MALWARE INCIDENTS AND DATA EXFILTRATION BY INDUSTRY</td>
</tr>
<tr>
<td>08</td>
<td>MALWARE DOESN’T SLEEP AT NIGHT</td>
</tr>
<tr>
<td>09</td>
<td>SKELETONS IN THE CLOSET: DATA SENT TO HIGH-RISK CLOUD SERVICES</td>
</tr>
</tbody>
</table>
In our professional lives, we all seek to make more data-driven decisions. We know that logical decisions made with complete information yield better results than those based on conjecture or suspicion. To that end, Skyhigh Networks produces a quarterly “Cloud Adoption and Risk (CAR) Report” that provides key data metrics pertaining to the use of cloud in the enterprise. This data is valuable and has proven interesting to those enabling (IT), securing (Security), using (Employees), analyzing (Analysts), and covering (Journalists) cloud in the enterprise. What makes this report unique is that it's based on hard, empirical data. Rather than relying on surveys alone that show only what people think is happening, we base our findings on actual usage data collected from customers throughout the world. You'll notice we have adopted a new format for easier consumption in this, our 5th quarterly Cloud Adoption and Risk Report. Share your thoughts with us and enjoy the data!
With every CAR Report, we include the data from more and more companies, making the statistics and findings richer every quarter. This quarter’s findings are based on anonymized data collected from over 10.5 million enterprise employees across all major verticals - Education, Financial Services, Food & Beverage, Healthcare, High-Tech, Media, Oil & Gas, Manufacturing, Retail, and Utilities.

The companies included in the report range in size, from 506 to 200,000+ employees with an average size of 38,990 employees. The number of cloud services used by each enterprise varies just as much, ranging from 327 to 3,201, with a total of 3,816 unique cloud services identified in use overall. The first surprising finding in this report is that the average number of cloud services used in the enterprise, which had increased in every prior quarter, actually decreased slightly from 759 to 738. We are in the early innings of the movement to the cloud, so it is unlikely that this flattening is due to decreased supply or demand of cloud services. Instead, this flattening is likely the result of IT’s efforts to educate employees on the perils of high-risk cloud services, the consolidation of services in a particular category to lower cost and risk, and greater awareness among employees on the care required when dealing with corporate data.

Consolidation to low-risk, enterprise-ready services is a good thing, as the data shows that the majority of the 3,861 services in use lack basic security features, putting organizations at risk. Only 9% of services used were Skyhigh Enterprise-Ready™, meaning that they fully satisfied the most stringent requirements for data protection, identity verification, service security, business practices, and legal protection. Only 11% encrypt data at risk, only 16% provide multi-factor authentication, and only 4% are ISO 27001 certified.
In quarters past, the most popular (i.e. most tweeted) data has been the coveted Top 20 Cloud Services in the Enterprise list, based on number of users. This quarter, we’re changing things up and splitting consumer and enterprise services so we can provide Top 20 lists for both.

The Top 20 Enterprise Cloud Services list offers insight into the cloud apps and services businesses are standardizing on and provides CIOs with a short-list of services that have reached mass-adoption across enterprises. The data shows that 4 vendors have successfully transitioned their legacy on-premise software to the cloud (i.e. Microsoft Office 365, SAS On Demand, Informatica Cloud, and Ariba - an SAP company). Three companies on the list have successfully accomplished multi-billion dollar disruptions (i.e. Salesforce, ServiceNow, and SuccessFactors – an SAP company). And one company on the list has created a new category, Web-Conferencing, replacing the legacy office rituals of in-person meetings. Several services, including Splunk Storm, SurveyMonkey, Qualtrics, Get Satisfaction, and GitHub showed remarkable growth rates but have not yet cracked the Enterprise Top 20. The top four categories represented are Collaboration (4 services), Business Intelligence (2), Development (2), and Marketing (2).
While this report aims to expose trends in enterprise cloud usage, it is important to be mindful of consumer apps used in the enterprise. There are legitimate reasons employees are using consumer apps in the enterprise at work – for example, a social media manager posting on the company’s Facebook page to engage with users, or a UX designer using Pinterest to create a design “look and feel book” for an upcoming project. However, consumer apps can present real risks to enterprises. Data loss in consumer apps can occur due to malware or insider threat. Skyhigh routinely sees and alerts its customers to incidents where sites such as Twitter, YouTube, and Pinterest are used to exfiltrate data. Data loss can also occur due to the acceptance of terms and conditions related to IP ownership. For example, users of Prezi, the cloud-based presentation and collaboration service, grant the company “irrevocable and royalty-free rights to use, distribute, and otherwise exploit” the content that the users upload.

Additionally, apps in categories such as Content Sharing and Media Services can have significant implications on bandwidth. Google, Yahoo, and Facebook dominate the list, and the top three categories represented are Content Sharing (7 Services), Social Media (7), and Collaboration (4).
### TOP SERVICES by category

#### FILE SHARING
1. Dropbox
2. Google Drive
3. Box
4. OneDrive
5. eFolder
6. Yandex.disk
7. Goodsync
8. Solidfiles
9. Sharefile
10. 4Shared

#### COLLABORATION
1. Office 365
2. Gmail
3. Cisco Webex
4. Google Docs
5. Prezi
6. Yahoo Mail
7. Yammer
8. Evernote
9. Intralinks
10. ClearSlide

#### SOCIAL MEDIA
1. Facebook
2. Twitter
3. LinkedIn
4. Sina Weibo
5. Tumblr
6. Myspace
7. VK
8. LiveJournal
9. Renren
10. Foursquare

### FILE SHARING
Dropbox and Google Drive are firmly entrenched in the top two spots, driven by consumer use. OneDrive and Box are duking it out as the top business-sponsored cloud service. The bottom half of the list remains in constant flux, with Sharefile as the one new ranking service, replacing Filefactory.

### COLLABORATION
The collaboration space, which boasts the most cloud services of any category, has seen a bit of a shake-up with three new players making the Top 10 list for the first time: Intralinks, Evernote, and ClearSlide. Most interesting, however, is the fact that Office 365 has overtaken Gmail as the top collaboration service.

### SOCIAL MEDIA
In social media, the top three players (ie Facebook, Twitter, and LinkedIn) are constant. This quarter extends two recent trends: 1) significant movement at the bottom, and 2) internationalization of social media with four of the top ten sites (Sina Weibo, VK, LiveJournal, and Renren) hailing from outside of the United States.
The last quarter saw several notable cloud service security breaches, including eBay, TweetDeck and AOL. Our data shows that the breadth of the eBay breach significantly overshadows that of TweetDeck and AOL, as the average enterprise has more eBay users than the other two services combined.

Many believed that the eBay breach did not have implications on the enterprise because most eBay users visit the service exclusively for personal reasons and do not store sensitive corporate data within the service. However, employees often use the same password across cloud services. According to a recent study by Joseph Bonneau from the University of Cambridge, 31% of passwords are re-used. This is critical because it means that hackers can use compromised consumer credentials to guess the login/password information of corporate cloud services. Applying the 31/100 ratio from the study across the average 15,800 eBay users per company shows that approximately 4,900 employees per company have passwords to other cloud services that could be guessed using compromised eBay credentials.
Examining the average number of malware incidents and data exfiltration events over the last quarter for companies in each industry, it is clear that High-Tech companies are exposed to the most high-risk behavior in the cloud, with an average of 193 data exfiltration events and 41 malware incidents per quarter. And, this is not surprising since High-Tech companies tend to have permissive policies regarding the use cloud services.

Equally interesting is the relative risk exposure of Financial Services and Healthcare. Given their regulatory compliance requirements and focus on security, one would expect to see fewer high-risk activities in those industries compared to non-regulated industries. However, the number of high-risk activities are actually marginally higher than the other industries with an average of 58 and 63 data exfiltration events per quarter for Financial Services and Healthcare and an average of 23 and 29 malware incidents per quarter, respectively.
In any movie where robots rise up against their human makers, fear and panic sets in. This happens in films such as The Terminator (1984), Screamers (1995), and I, Robot (2004). Why? Because robots are mindless and are not constrained by human limitations: the need for food, water, or sleep. This is what makes malware so effective, and so frightening. In our recent findings, we discovered that malware incidents occurred consistently regardless of time of day, and was actually 118% more active at night while employees are sleeping. The data, which was normalized across time zones, shows that for the quarter, the number of malware incidents that occurred during working hours (8am – 8pm) was 987, as compared to the 2,157 malware incidents that occurred during non-working hours (8pm – 8am).

This underlies the need for security teams to be able to continuously monitor behavior. The benefit of monitoring behavior extends to human-led activities as well. As recent findings confirmed, hackers in China had mobilized as part of the People’s Liberation Army Unit 61398 and were actively targeting U.S.-based companies. The members of this highly specialized operations unit stood out because, based on Dynamic DNS data captured, they were highly consistent. They worked approximately from 8am to 5pm. 98% of the connections occurred Monday through Friday. Though they were not mindless drones working around the clock, these hackers acted as a highly-efficient force; the team consisted of specialized workers who had assigned roles to play (from the coders working on intrusion, to the sniffers collecting data once the target is breached)*. This case study illustrates the importance of real-time alerts and close monitoring.

* Source: [http://www.fireeye.com/blog/technical/2014/05/the-pla-and-the-800am-500pm-work-day-fireeye-confirms-doj-findings-on-apt1-intrusion-activity.html](http://www.fireeye.com/blog/technical/2014/05/the-pla-and-the-800am-500pm-work-day-fireeye-confirms-doj-findings-on-apt1-intrusion-activity.html)
Cloud services may be considered high-risk for many reasons. They may have a discouraging known-compromise history, they may permit risky behaviors, such as anonymous use, they may lack basic security features such as encryption in transit and admin activity logging, and they may have sneaky terms and conditions that put your data at risk. For example, users of some popular collaboration services grant the company irrevocable and royalty-free rights to use, distribute, and otherwise exploit the content that the users upload.

These risky cloud services are a concern because they can serve as a vector for data loss, whether it is intentional or not. Last quarter, the average company uploaded 86.5 gigabytes of data to high-risk cloud services. If you look at the types of high-risk services that corporate data was going to, the top five categories were: slide sharing (6.1%), file sharing (4.0%), photo sharing (7.85%), video sharing (40.1%), and web conferencing (4.81%)

In addition, nearly two thirds of that data was sent to services that were miscategorized by URL categorization services rendering them ungoverned by existing firewalls and proxies. This can result in the loss of corporate data and IP as well as violation of internal security policies and external regulatory requirements.