CLOUD ADOPTION & RISK IN HEALTHCARE REPORT

Q2 2015 Published Q3 2015

skyhigh

TABLE OF CONTENTS

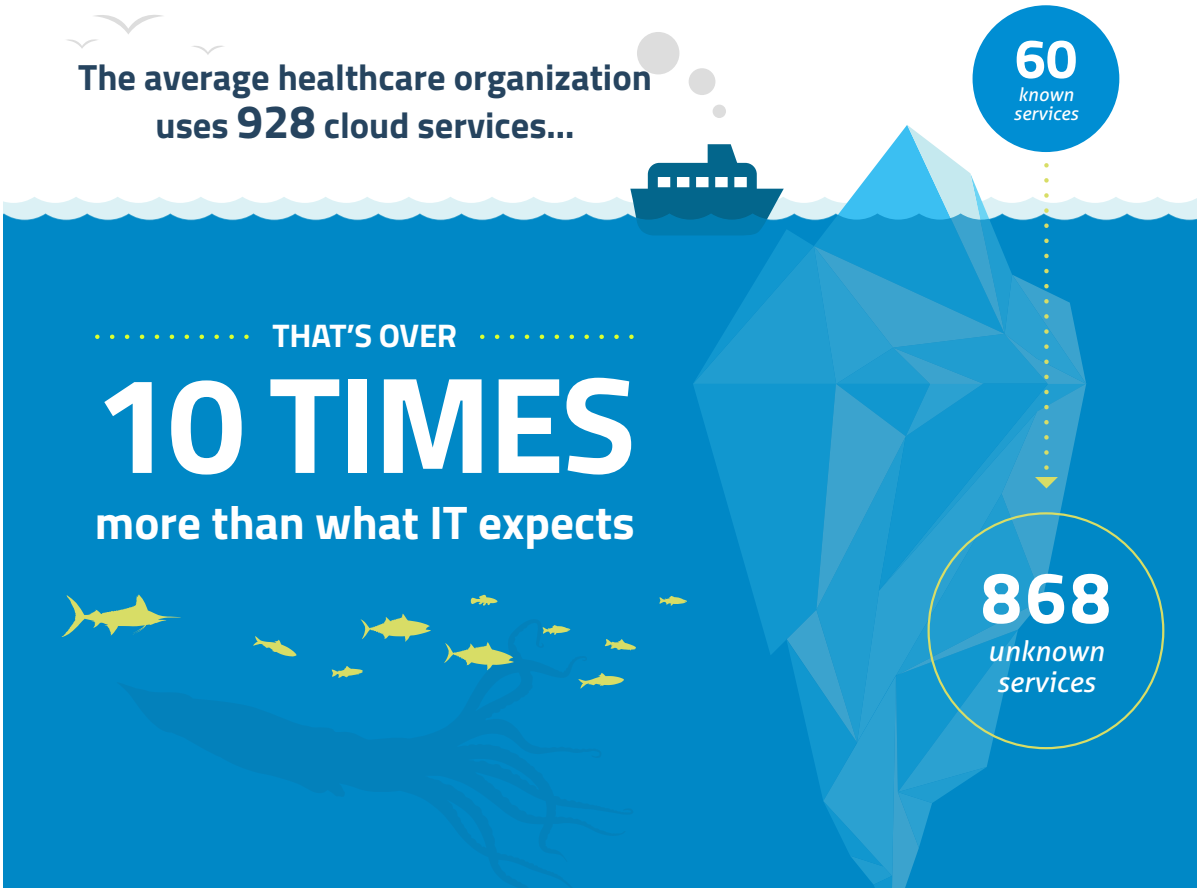
INTRODUCTION

Healthcare providers and payers are embracing cloud services to reduce IT cost, increase employee productivity and improve patient outcomes. While technology is changing the way healthcare is delivered, the sensitivity of patient data has not changed. HIPAA and HITECH require that protected health information (PHI) be secured even as it migrates to the cloud. Healthcare organizations take special care in assessing the compliance controls of cloud services, but employees can also introduce cloud services into the workplace, creating "shadow IT", which are services not known by the IT department. To better understand these trends and the risks in cloud adoption in the healthcare industry, Skyhigh publishes a Cloud Adoption & Risk in Healthcare report.

What makes this report unique is that it's based on actual usage data for over 1.6 million employees at healthcare providers and payers, rather than surveys that ask people to self-report their behavior. In this quarter's report, we explore the incidence of insider threats within these organizations and expose a worldwide black market in stolen login credentials that cyber criminals use to gain access to sensitive information in cloud services. We also detail the top 20 enterprise and consumer cloud services in healthcare, the top cloud services used to connect with business partners, and how prolific one employee can be in terms of cloud usage and high-risk behavior.

OVERVIEW OF CLOUD ADOPTION

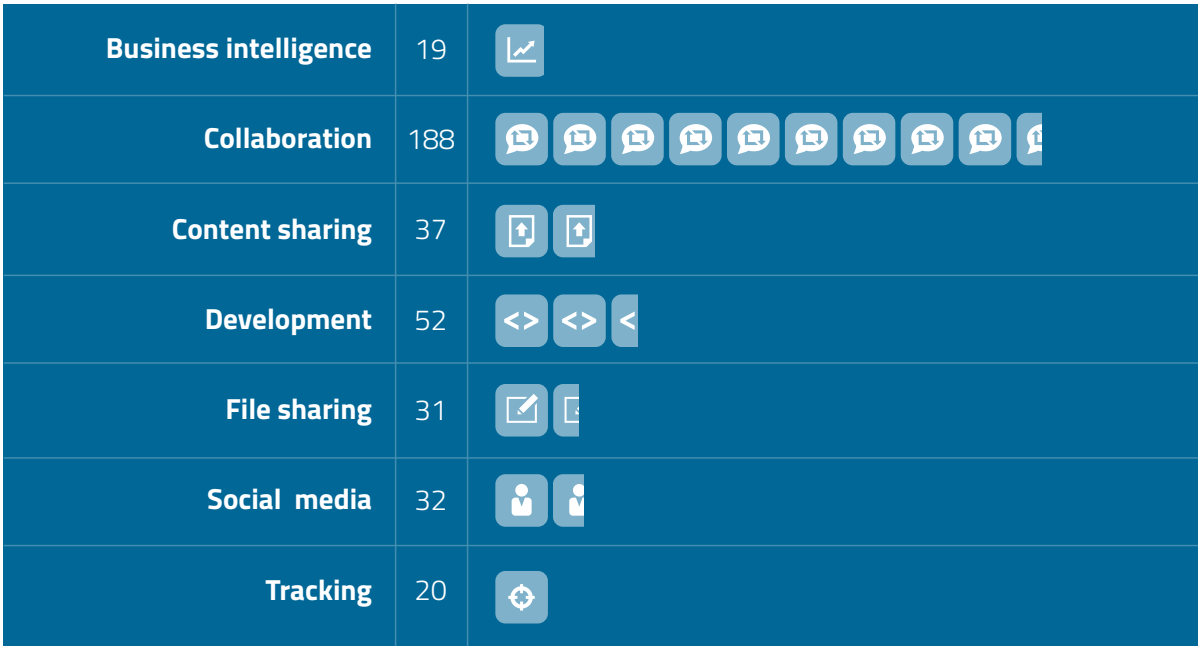
The average healthcare organization uses 928 cloud services, which comes as a surprise to many IT departments. When employees bring cloud services to the work environment for increased productivity and efficiency without the knowledge or approval of IT, they may not realize the risk they're introducing to the organization. Just 7.0% of cloud services meet enterprise security and compliance requirements, as rated by Skyhigh's CloudTrust Program. Only 15.4% support multi-factor authentication, 2.8% have ISO 27001 certification, and 9.4% encrypt data stored at rest. The average healthcare organization uploads 6.8 TB to the cloud each month and without proper controls this data could be at risk.



By far, the most popular cloud category in healthcare are collaboration tools. The average healthcare organization uses a dizzying 188 collaboration services, including Microsoft Office 365, Gmail, and Evernote. Of course, using this many collaboration services can actually create silos and impede collaboration. Collaboration services are followed by development with 52 services per organization (e.g. SourceForge, GitHub, etc.), content sharing with 37 services (e.g. YouTube, LiveLeak, etc.), social media with 33 services (Facebook, Twitter, etc.), and file sharing with 31 services (Dropbox, Google Drive, etc.).

The average healthcare organization uses

many cloud services in each category



The average healthcare employee uses 26 distinct cloud services including 8 collaboration services, 4 file-sharing services, 4 social media services, and 4 content sharing services. What's troubling is that each employee is tracked on average by 4 marketing analytics and advertising services. These services are used to deliver targeted ads to users across the Internet but they are also increasingly used by cyber criminals to determine the sites healthcare employees frequent most. Armed with this information, criminals attempt to compromise these sites in order to ultimately compromise a target healthcare organization in what's known as a "watering hole attack."

INSIDER THREATS IN THE CLOUD

A cloud service may be secure, but employees can still use it in risky ways. While Edward Snowden is the most well-known example of an insider threat, most insider threat incidents are quiet and may not even be uncovered in a timely manner, if at all. Healthcare records containing Social Security numbers and addresses are worth approximately 20 times a credit card number on the black market because cyber criminals can open multiple fraudulent accounts. Records for terminally ill patients are worth even more because it's less likely the patient or family will detect the fraud. Consider the example of a hospital employee who sells these records. In many cases, a healthcare organization has no way to detect risky user behavior, whether intentional or unintentional. Since most organizations are concerned about a high-profile whistleblower, they underestimate insider threats.

Just 33%

of healthcare companies surveyed reported an insider threat incident in the last year

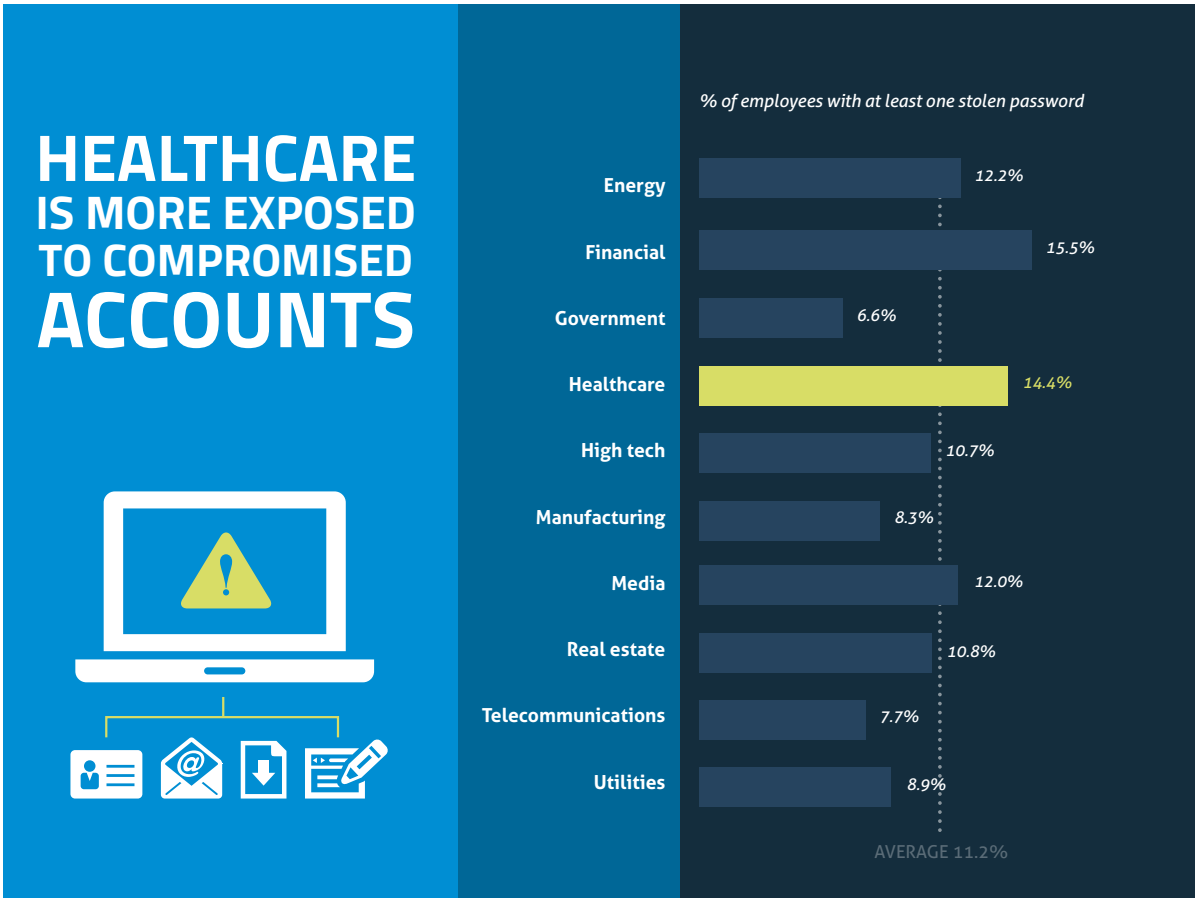
But 79%

of healthcare companies had behavior indicative of an insider threat in the last quarter alone

We surveyed healthcare organizations in partnership with the Cloud Security Alliance and found that just 33% of organizations knew of an insider threat incident in the last year. However, examining actual anomaly detection data collected across healthcare users, we found that 79% of organizations had behavior indicative of an insider threat in the last quarter alone. While not all of these events turn out to be malicious activity, the incidence of potentially destructive behavior by employees is much higher than most healthcare organizations realize.

COMPROMISED CREDENTIALS

There were more software vulnerabilities discovered and more data breaches in 2014 than any year on record. Following one of the largest breaches of the year, eBay prompted 145 million users to change their passwords after cyber criminals compromised their account credentials. With healthcare organizations uploading significant volumes of data to the cloud, the theft of a username and password can have a far-reaching impact. Research by Joseph Bonneau at the University of Cambridge shows that 31% of passwords are re-used in multiple places. With the average healthcare employee using 26 different cloud services, one compromised password could give criminals access to a significant amount of data.



We found that 89.2% of healthcare organizations have exposure to compromised credentials. While this number is lower than the overall average of 91.7% across all industries, 14.4% of healthcare employees have at least one compromised credential, compared with just 11.2% across all industries. Anecdotally, we identified one health insurance company with 9,932 compromised credentials. Considering that just 15.4% of cloud providers offer multi-factor authentication that can make it more difficult for attackers to exploit stolen credentials, we recommend healthcare organizations use strong, unique passwords for each cloud service and change them regularly to limit exposure to compromised credentials.

THE TOP CLOUD SERVICES

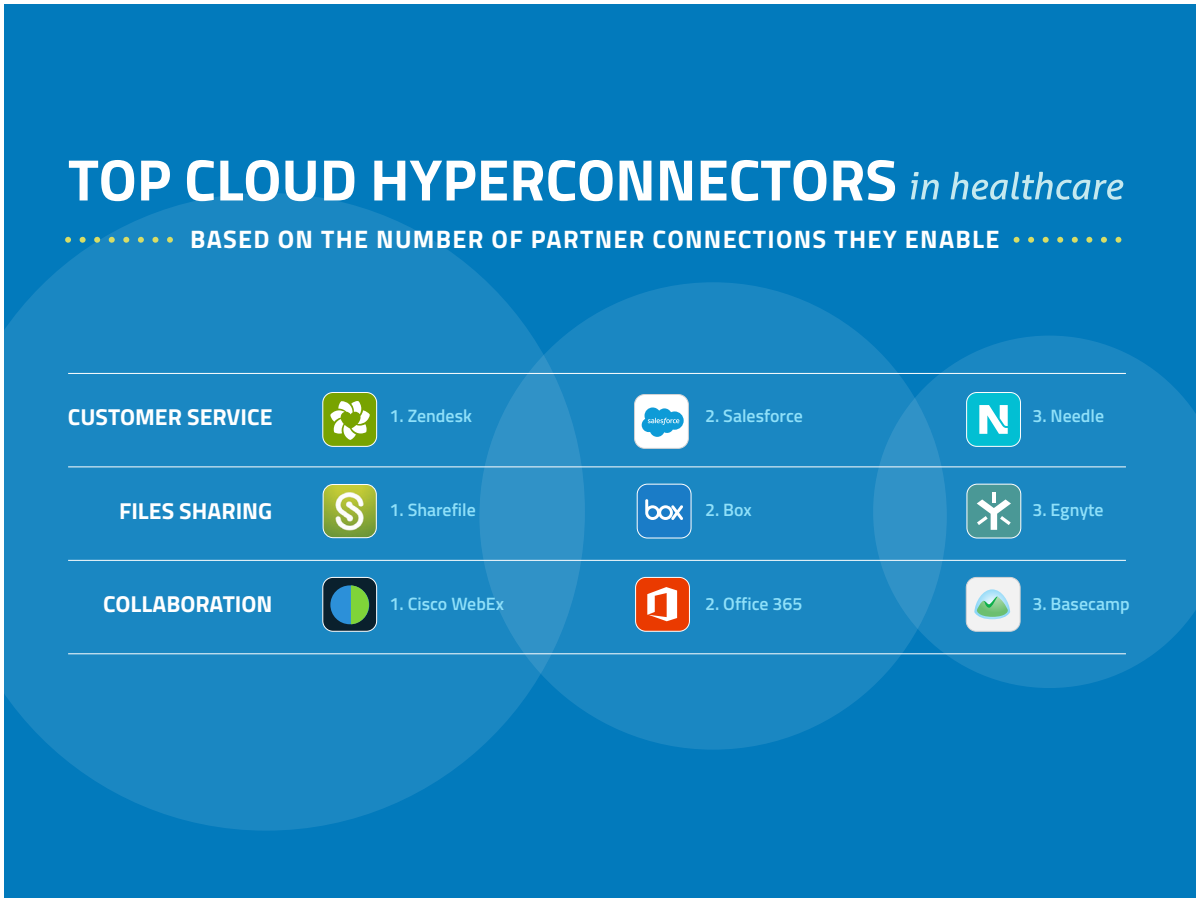
From the perspective of a software company, developing a cloud service is very different from software installed by the customer. The cloud has freed developers to reimagine enterprise software with delightful user experiences, innovative new features, and access from mobile devices. With faster release cycles and updates that occur immediately across all customers, cloud applications are not only more cost effective to manage, they're often first to market with innovative features. That's why an increasing number of healthcare organizations are deploying the top enterprise cloud services – not because they're the best cloud version available but because they are the best software available, period. That's also why we wanted to look at the top services based on user count.

1. Cisco WebEx
2. ADP
3. Microsoft Office 365
4. Concur
5. Zendesk
6. Salesforce
7. Caremark
8. Oracle RightNow
9. ServiceNow
10. GoToMeeting
11. Box
12. MINDBODY
13. Oracle Taleo
14. Citrix ShareFile
15. SAS OnDemand
16. Fieldglass
17. Adobe EchoSign
18. NetSuite
19. join.me
20. Hightail

Consumer-grade cloud services today are so good that they can easily rival enterprise software. It's no wonder, then, that employees bring these cloud services to work in order to do their jobs better. However, these services can also increase organizational risk. Healthcare organizations are increasingly attractive targets as the value of a healthcare record can be as much as 20 times more than a stolen credit card on the darknet. In order to exfiltrate this sensitive data undetected, cyber criminals deploy an array of sophisticated kill chains that leverage consumer cloud services. Skyhigh has detected attacks using Twitter to exfiltrate data 140 characters at a time and another that encoded stolen data into videos that were uploaded to YouTube.

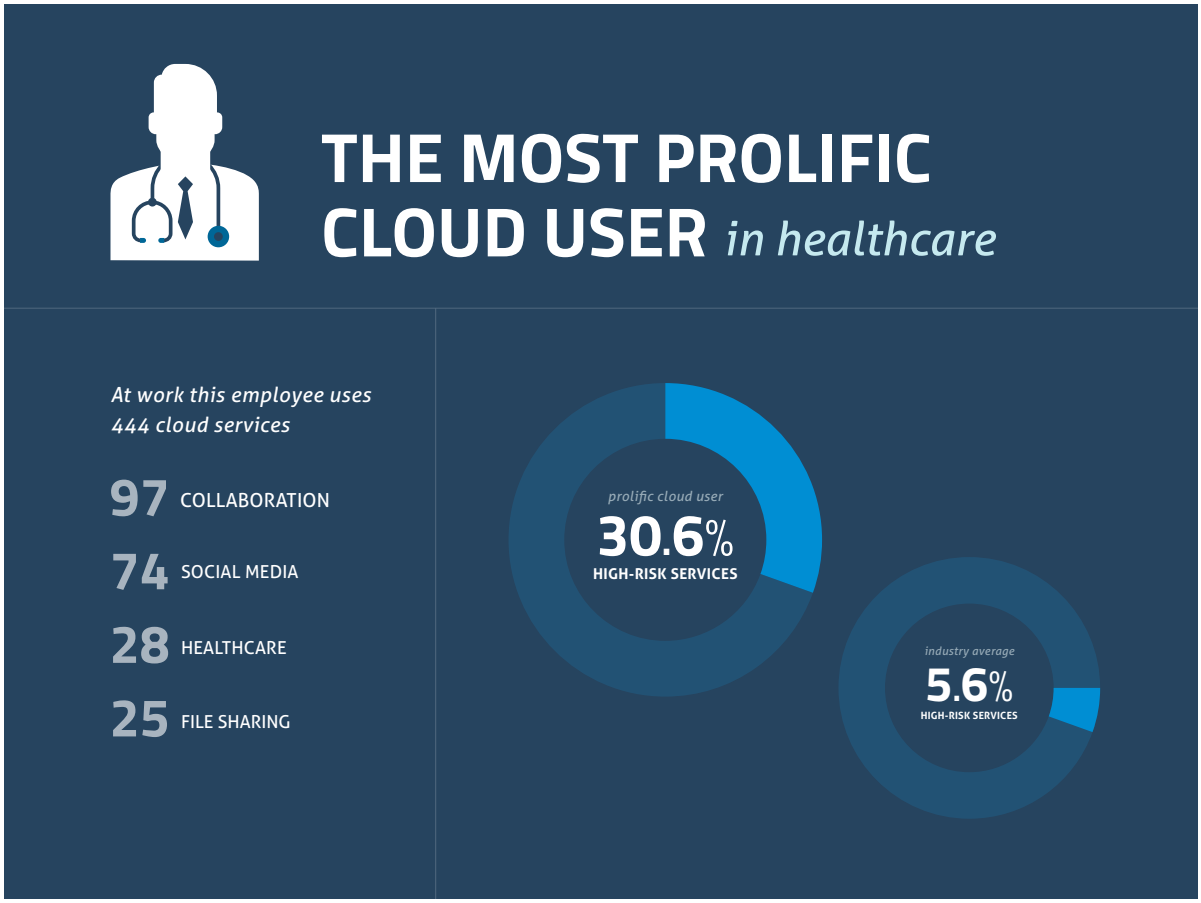
1. Facebook
2. Twitter
3. Pinterest
4. YouTube
5. Linkedin
6. StumbleUpon
7. Tumblr
8. Flickr
9. Yahoo! Mail
10. Vimeo
11. Gmail
12. Instagram
13. Dropbox
14. Spotify
15. Google Drive
16. SlideShare
17. Apple iCloud
18. GitHub
19. Shutterfly
20. Skype

Healthcare organizations also increasingly use the cloud to collaborate with business partners. The average healthcare organization connects with 1,004 partners via cloud services. Not all cloud services are created equal and a handful drive an outsized number of these partner connections. These cloud service "hyperconnectors" are helping healthcare organizations deliver better patient outcomes and control costs. The top cloud service categories used by healthcare organizations to connect with business partners include collaboration, file sharing, and customer service. The top partner categories that healthcare companies connect to are business services, high tech, financial services, and other healthcare companies.



A HEAD IN THE CLOUDS

The average employee uses 26 cloud services, which comes as a surprising to many in IT. The average person may not even be able to name this many apps, since they fade into the background of everyday usage. However, there are employees whose cloud usage is even more prolific. The most prolific healthcare user across all employees in our study uses an impressive 444 cloud services including 97 collaboration services, 74 social media services, 28 healthcare services, and 25 file-sharing services. While their behavior may be done with good intensions, unchecked cloud usage can also expose healthcare organizations to risk.



Chances are, most of the services in use by this individual are not known to the IT department. Out of 444 services, 136 services they use are high-risk, or 30.6 percent. Across all cloud services in use globally, just 5.6% are high-risk, often because they lack proper security controls, have onerous terms and conditions that claim ownership of uploaded data, or they are hosted in high-risk countries without strong data protections. Among the high-risk services in use by this user are Convert OnlineFree, a service that converts Word documents to PDF, Mega, the notorious file sharing service run by Kim Dotcom, and Online OCR, a service that converts images to text.

ABOUT SKYHIGH NETWORKS

Skyhigh Networks, the cloud security and enablement company, helps enterprises safely adopt cloud services while meeting their security, compliance, and governance requirements. Over 400 enterprises including Aetna, Cisco, DIRECTV, HP, and Western Union use Skyhigh to gain visibility into all cloud services in use and their associated risk; analyze cloud usage to identify security breaches, compromised accounts, and insider threats; and seamlessly enforce security policies with encryption, data loss prevention, contextual access control, and activity monitoring. Headquartered in Campbell, Calif., Skyhigh Networks is backed by Greylock Partners, Sequoia Capital, and Salesforce.com. For more information, visit us at **www.skyhighnetworks.com** or follow us on Twitter **@skyhighnetworks**.

UNCOVER SHADOW IT

If you'd like to learn the scope of Shadow IT at your company, including detailed statistics profiled in this report, sign up for a complimentary cloud audit

REQUEST COMPLIMENTARY CLOUD AUDIT

bit.ly/ComplimentaryCloudAudit

"With Skyhigh we discovered a wide range of services, allowing us to understand their associated risks and put in place policies to protect corporate data."

CISCO

Steve Martino
VP Information Security