onelogin

flyingpenguin
the poetry of information security

2013 State of Cloud Application Access Survey Results

January 31, 2013

www.onelogin.com | twitter.com/onelogin

OneLogin, Inc. | 50 Osgood Place, Suite 100, San Francisco, CA 94133

855.426.7227

INTRODUCTION AND METHODOLOGY

OneLogin in collaboration with the flyingpenguin conducted a survey regarding the adoption, use, and security of cloud applications within organizations of all sizes and industries.

The goal was to collect the views of IT and business people alike regarding the pace of cloud application adoption and usage within their organizations.

200 people completed the web-based survey which was open between December 7th, 2012 and January 7th, 2013. An invitation to take the survey was mailed out to approximately 26,000 people and was also promoted on LinkedIn and Twitter. Listed below are the key findings.

EXECUTIVE SUMMARY

Adoption of cloud applications is growing rapidly in all sizes of organizations; 78% of respondents plan to increase the number of cloud applications in 2013 and 35% will add at least four new apps. The vast majority of access to cloud applications involves mobile and BYOD; 80% use smart phones, 71% use tablets and 80% are from non-company systems. Most organizations cited major concerns in areas of identity management, governance and complexity. The following are some of the key areas cited:

Shadow IT - 71% of respondents admit to using cloud applications that have not yet been sanctioned by their IT department (like Dropbox and Gmail) to get work done.

Unsafe password management - 43% of respondents admit that employees manage passwords in spreadsheets or on sticky notes and 34% share passwords with their co-workers for applications like FedEx, Twitter, Staples and LinkedIn. 20% experienced an employee still able to login after leaving the company.

Single sign-on challenges - 48% of respondents are still not able to sign in to cloud applications with a single set of credentials.

Need to provision external users - 72% of respondents have the need to provide external users (for example consultants) with temporary access to their cloud applications.

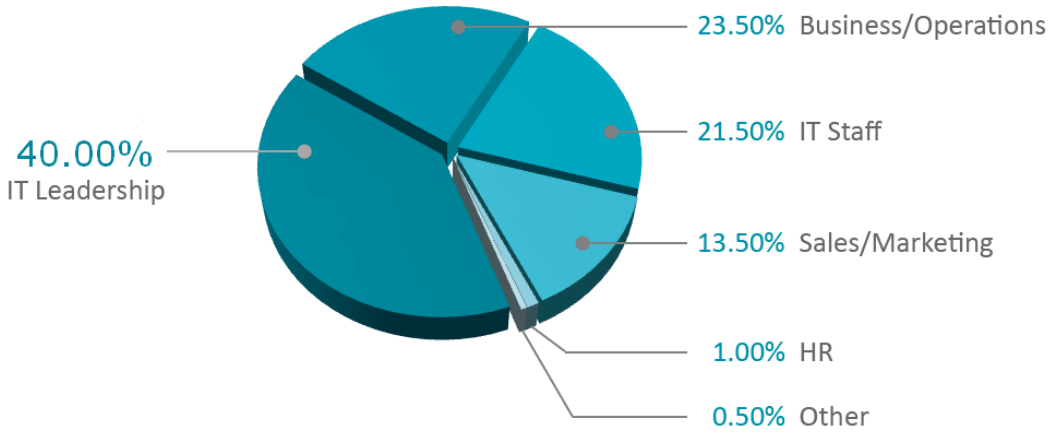
Complex directory infrastructures - 59% of respondents had multiple on-premise directories with Active Directory being cited as the most used directory (40%), followed by LDAP (17%) for managing user identities and application access.

Different security model for cloud application access - 34% of respondents claimed that their security model for cloud applications was different than for on-premise applications vs. 45% claiming it's the same.

PROFILE OF SURVEY RESPONDENTS

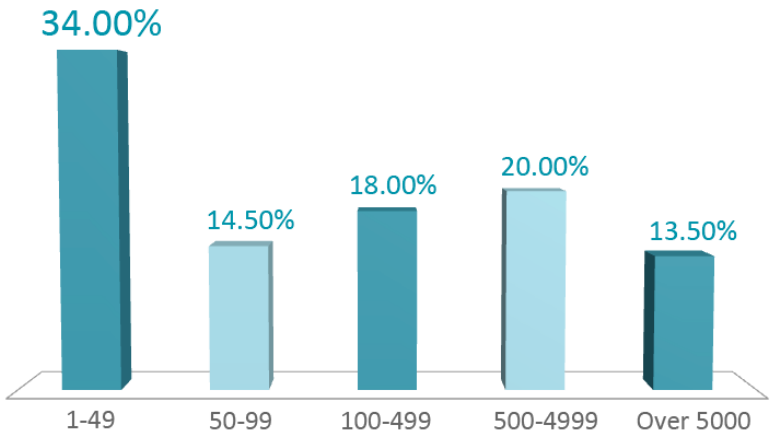
Respondents were primarily in an IT Leadership (40%) role, Business/Operations (23%) or IT Staff (21.50%).

What's your role?



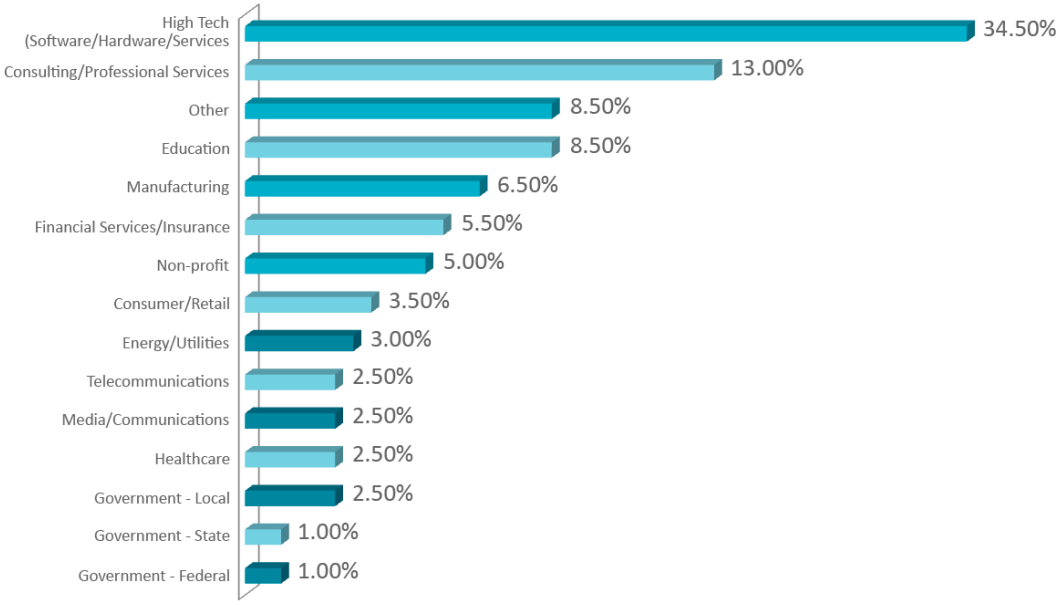
The smallest organizations, those with less than 50 employees accounted for the largest number of respondents (34%) with a smaller yet more evenly distributed number of respondents from organizations with 50-99 (14.5%), 100-499 (18%), 500-4999 (20%) and 5,000 or more (13.5%) employees.

How many employees?

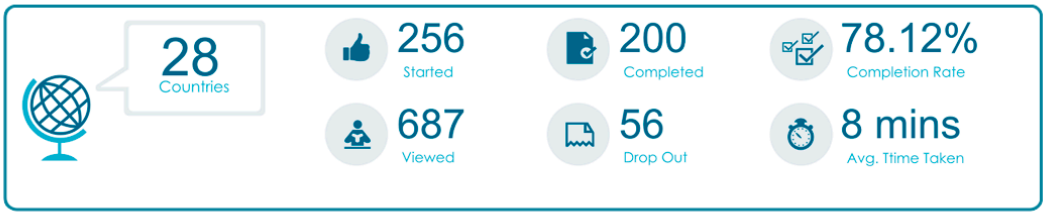


Respondents came from a broad spectrum of industries, but with a heavy weighting towards High Tech (34.5%).

What's your industry?



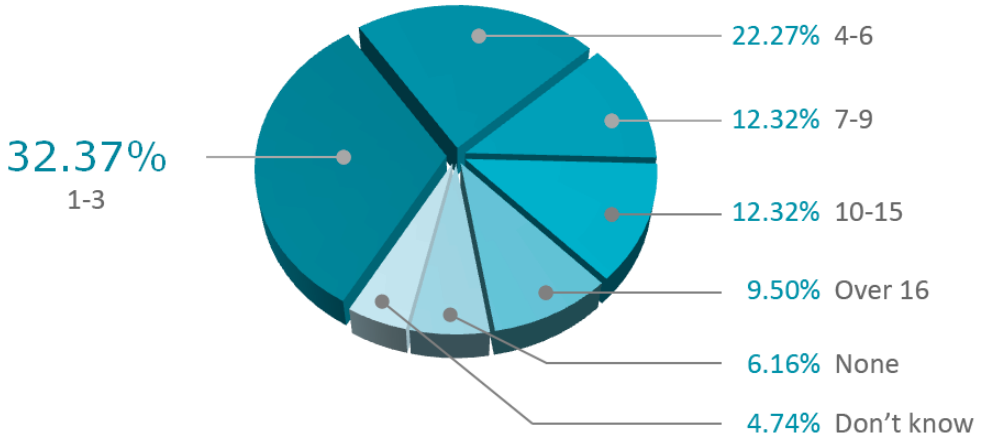
Survey Visitor Statistics



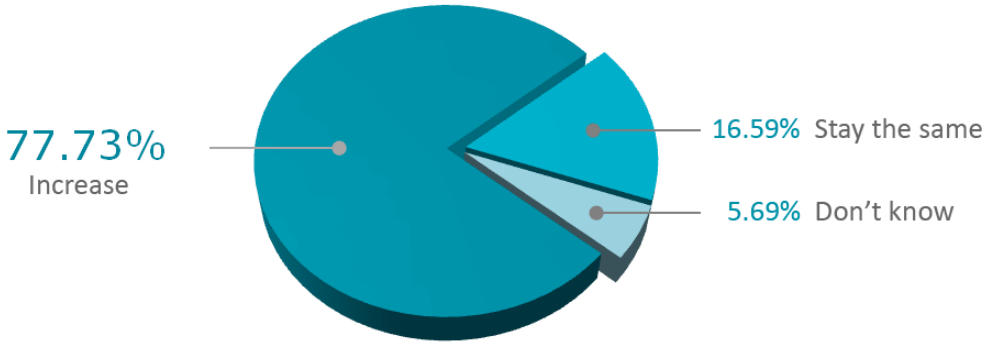
Countries Surveyed

SURVEY RESULTS

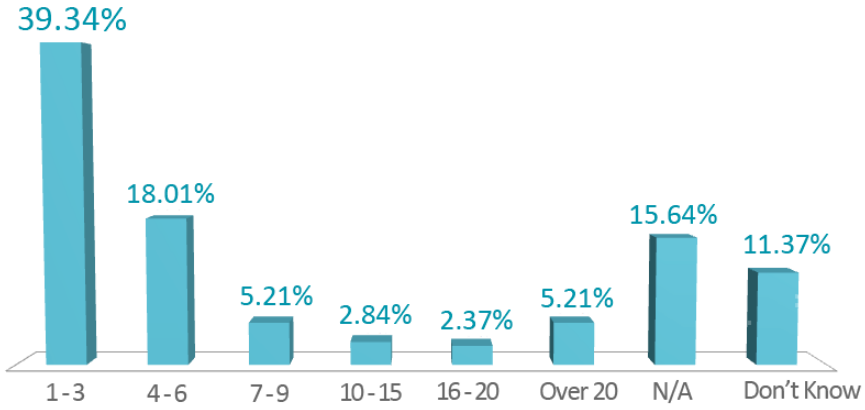
How many cloud applications (SaaS) do you currently have running within your organization?



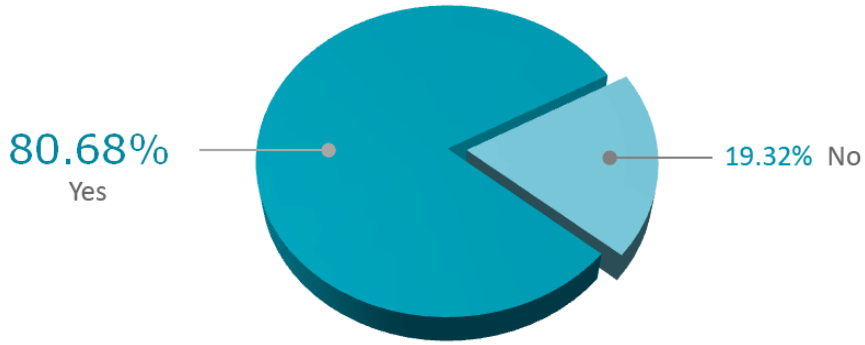
Do you expect to increase or decrease your total number of cloud applications in 2013?



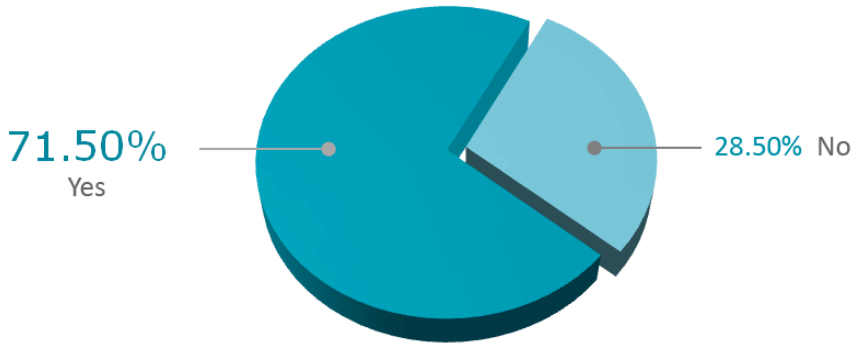
If an increase, by approximately how many more cloud applications will you add in 2013?



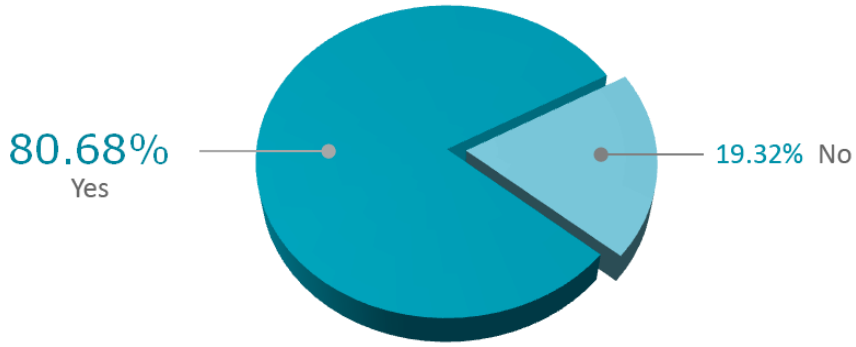
Do you use/access work-related cloud apps from a smartphone?



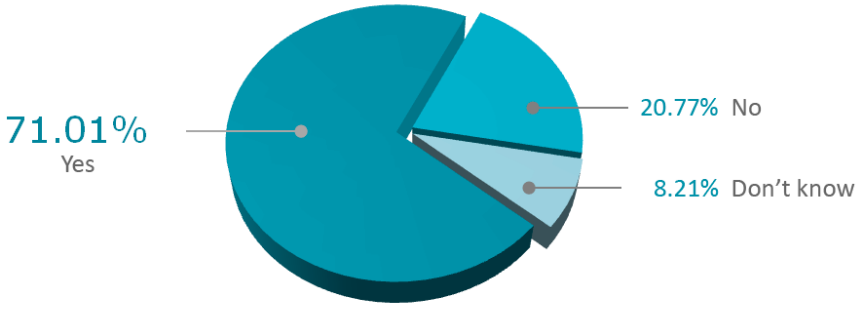
Do you use/access work-related cloud apps from a tablet?



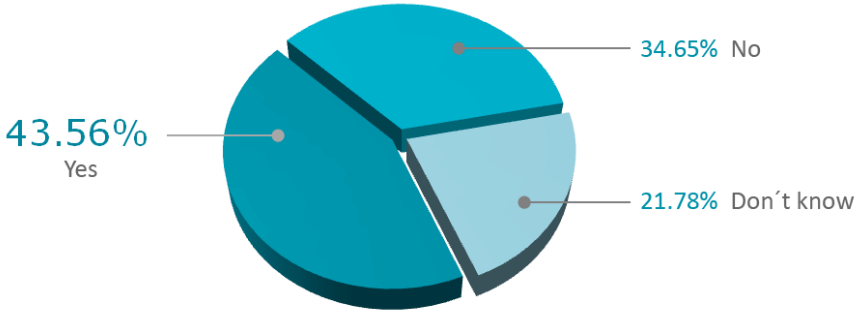
Do you use/access work-related cloud apps from non-company computers?



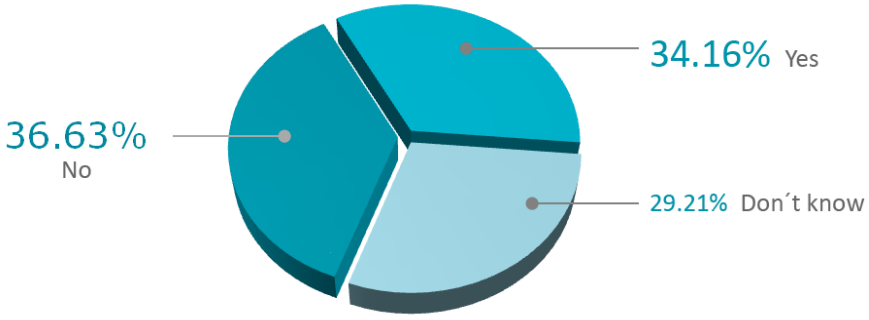
Do you or employees ever use cloud applications (e.g. Dropbox, Gmail, etc.) to get work done even though they have not yet been sanctioned by IT?



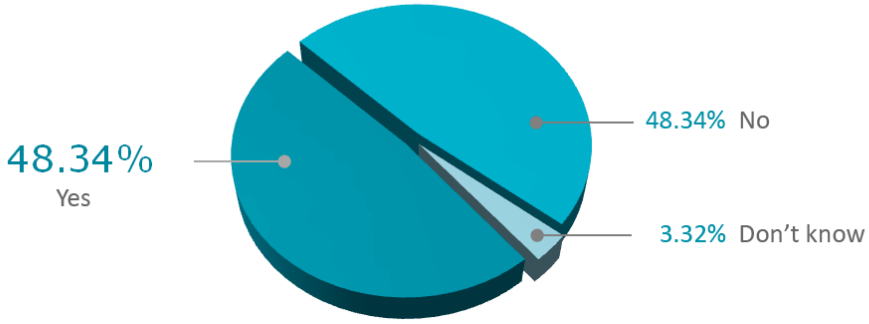
Do employees ever manage passwords in spreadsheets or on sticky notes?



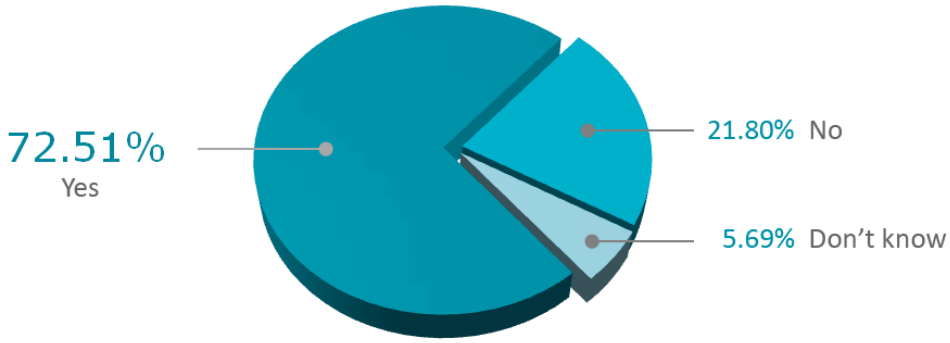
Do employees ever share passwords for public web applications like FedEx, Twitter, Staples, or LinkedIn?



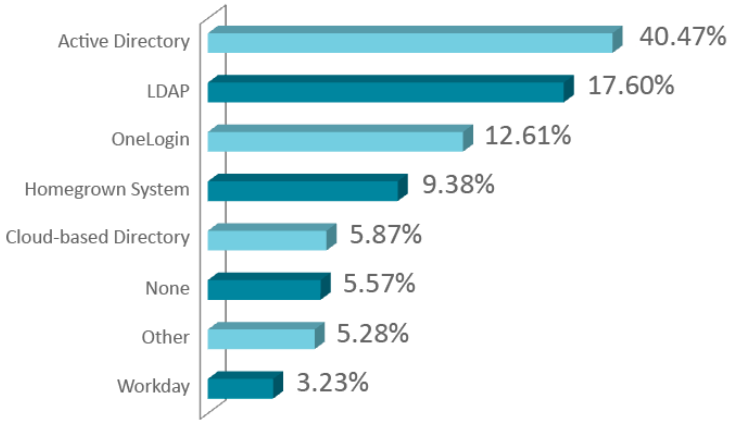
Are you able to sign-on with a single set of credentials (single sign-on) to your cloud applications?



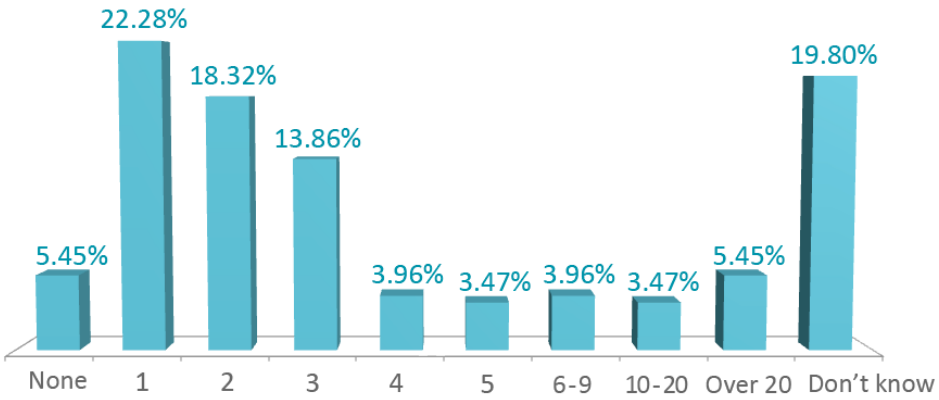
Does your company ever have the need to provide internal or external users (for example, consultants) with temporary access to your cloud applications?



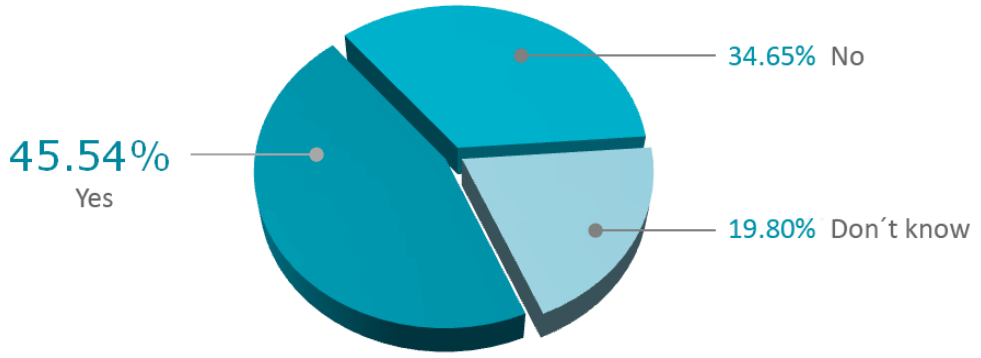
What directories do you currently use to manage user identities and application access (Select all that apply)?



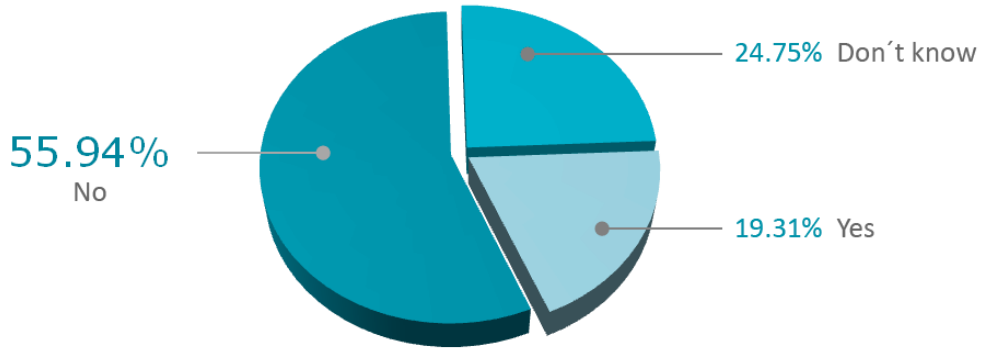
Approximately how many directories do you currently have within your global environment?



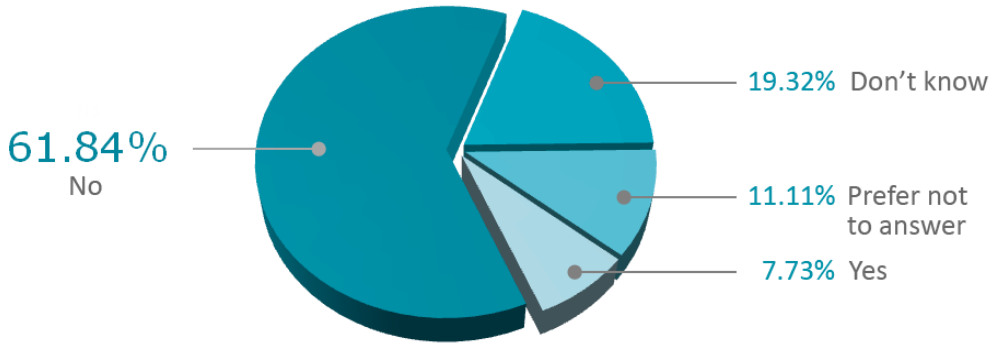
Is your security model for on-premises applications the same as for your cloud applications?



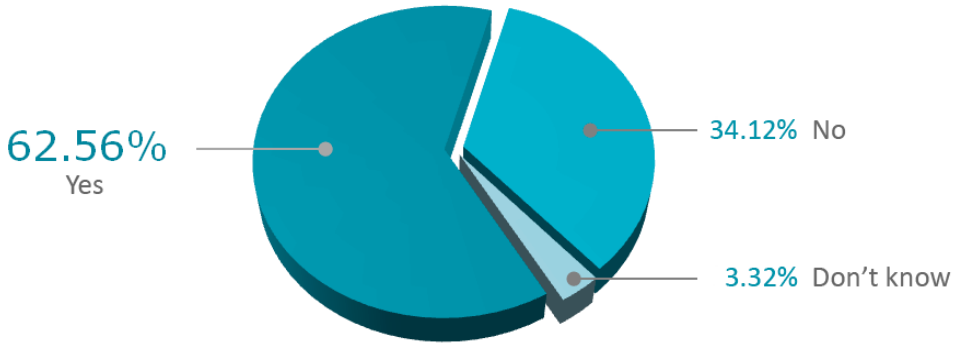
Within the last year, was there ever a case when an employee was able to access a web/cloud application after they no longer worked for the company?



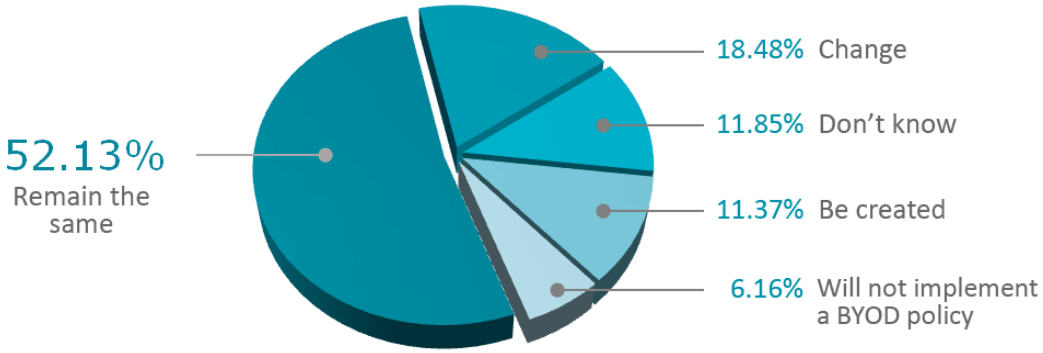
Has sensitive data ever been compromised by unauthorized access?



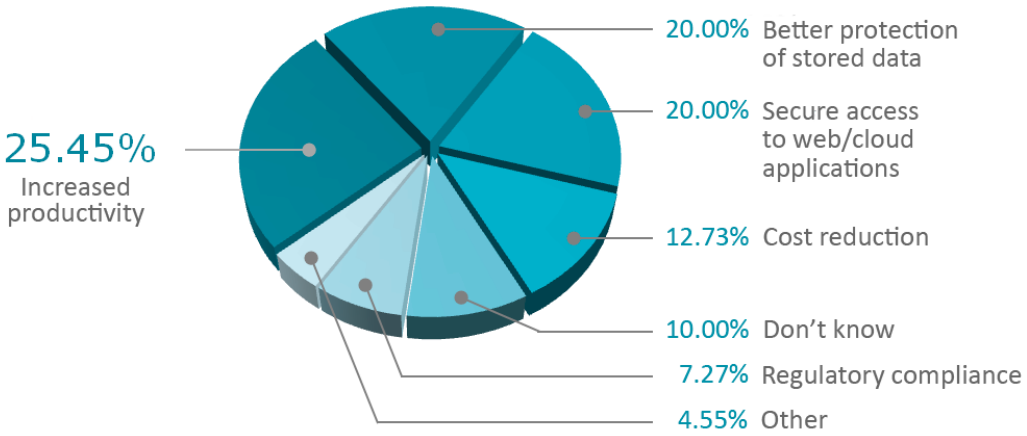
Do you have a policy to allow users bring their own devices for corporate use (BYOD)?



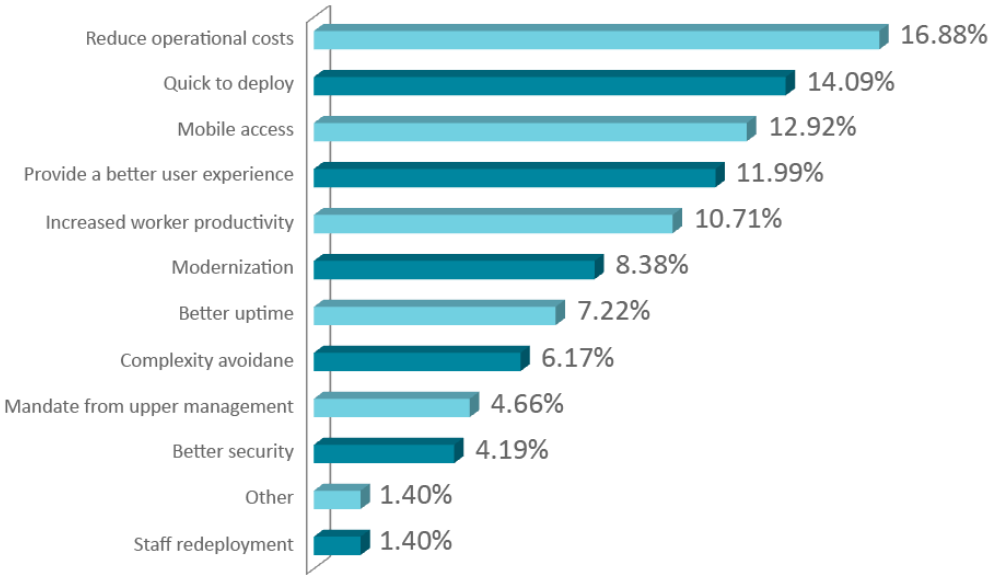
In 2013, will your BYOD policy?



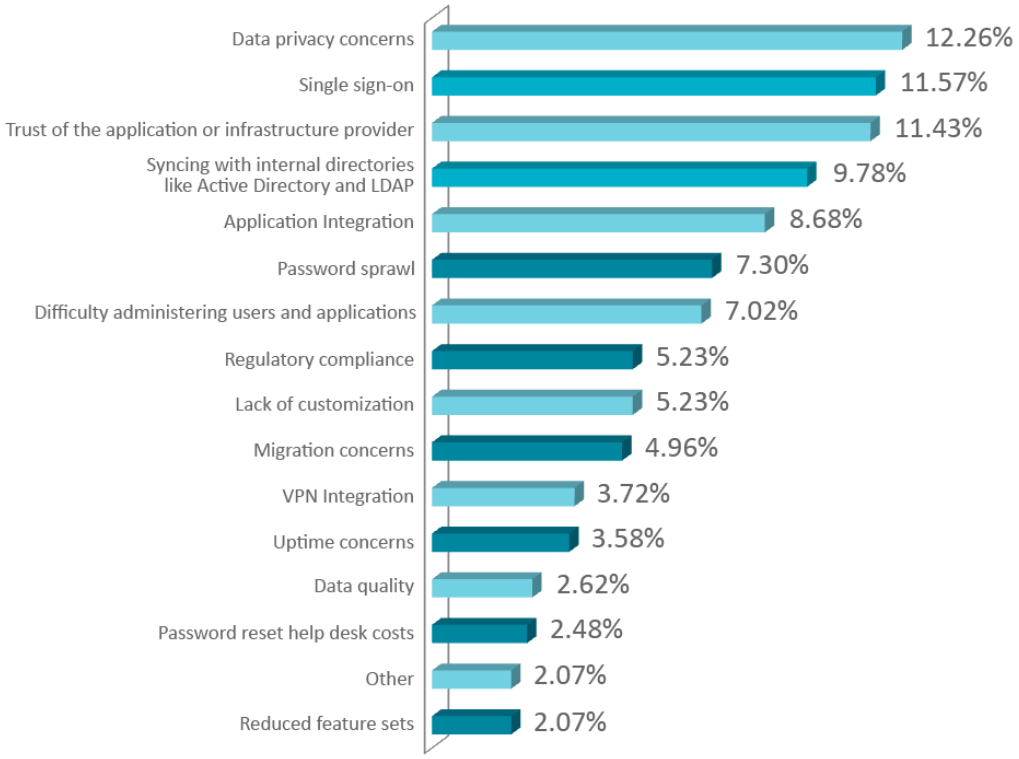
If creating or changing your BYOD policy, then what are the drivers?



What were/are some of the key drivers for adopting public cloud applications at your organization (Select all that apply)?



What are some of the impediments to adopting public cloud applications at your organization (Select all that apply)?



ABOUT ONELOGIN

OneLogin is the innovator in enterprise identity management and provides the industry's most comprehensive solution for managing user identities in the cloud and behind the firewall. Unique capabilities like Federated Cloud Search and OneLogin for iPad extend the genius of single sign-on (SSO), break down SaaS data silos, and increase productivity. OneLogin comes pre-integrated with more applications, authentication methods, directories, VPNs and SAML tools, so you can get up and running in minutes with no professional services required. IT gains control over web application access, LOB owners quickly on- and off-board team members, and end-users enjoy easy access to all their apps.

ABOUT FLYINGPENGUIN

flyingpenguin, a security consultancy, designs and assesses risk mitigation and response solutions as well as delivers strategic and competitive knowledge to security software and hardware vendors. Innovation, transparency and quality are hallmarks of flyingpenguin services, aimed to help reduce costs and improve efficiencies of managing risk.