



OneLogin 2014 State of SaaS Identity Management

February 24, 2014

www.onelogin.com | twitter.com/onelogin

Corporate Headquarters
OneLogin, Inc.
150 Spear Street, Suite 1400
San Francisco, CA 94105
Toll-Free (855) 426-7227
Local (415) 645-6830

EMEA Sales Office
OneLogin Ltd
1210 Parkview
Arlington Business Park
Theale, Reading
RG7 4TY
United Kingdom
+44 (0) 118 391 3540



INTRODUCTION AND METHODOLOGY

OneLogin in collaboration with the Cloud Security Alliance conducted a survey to better understand the maturity of SaaS providers in their implementation of identity management solutions, security standards and assurance certifications.

The goal was to collect data from a broad spectrum of SaaS application vendors to understand the pace at which SaaS companies are adopting standards like SAML, SCIM and SPML, how they integrate their applications with customers' user stores, the status of their security certifications, and market drivers for all of the above.

100 people completed the web-based survey which was open between December 2, 2013 and January 13, 2014. Invitations to take the survey were emailed to Cloud Security Alliance members as well as OneLogin's database of SaaS application vendors. To reduce duplicate SaaS company data, invitations emphasized one respondent per company and responses were deduped based on unique IP addresses.

EXECUTIVE SUMMARY OF RESULTS

SAML is primetime -- 67% of SaaS vendors surveyed leverage it today while 19% plan to implement SAML within the next 12 months. Only 3% had no plans to implement the standard.

SAML across multiple form factors -- The adoption of SAML wasn't just limited to the the web browser as 37% of SaaS vendors support SAML on mobile device resident versions of their app; while 25% support SAML on their desktop versions.

Main reasons for adopting SAML -- 26.4% of respondents cited demand from existing customers; 21.24% cited improved security and compliance; and 21.67% cited quick integration. These top three were followed by 14.83% who cited support for multi-factor authentication while 12.93% cited SAML's ability to lower customer support costs.

SCIM and SPML were less popular among respondents -- Of the two, SCIM is more firmly on SaaS vendors' radar; 15% of SaaS vendors support it today; 17% plan to support it within 12 months; and 13% plan to support it within 24 months. For SPML, the numbers were not as strong; 8% support it today; 15% plan to within the next 12 months; and 11% plan to within the next 24 months.

ISO 27001 certification is popular, but adoption of federal certifications slow going -- In terms of assurance certifications, 31.75% of SaaS vendors had or were working to obtain their ISO 27001; 19.05% on their SOC 1; 14.81% on their SOC 2 certifications; Federal certifications like FedRamp and FISMA were anchored at the other end of the spectrum at 7.41% and 4.76% respectively.

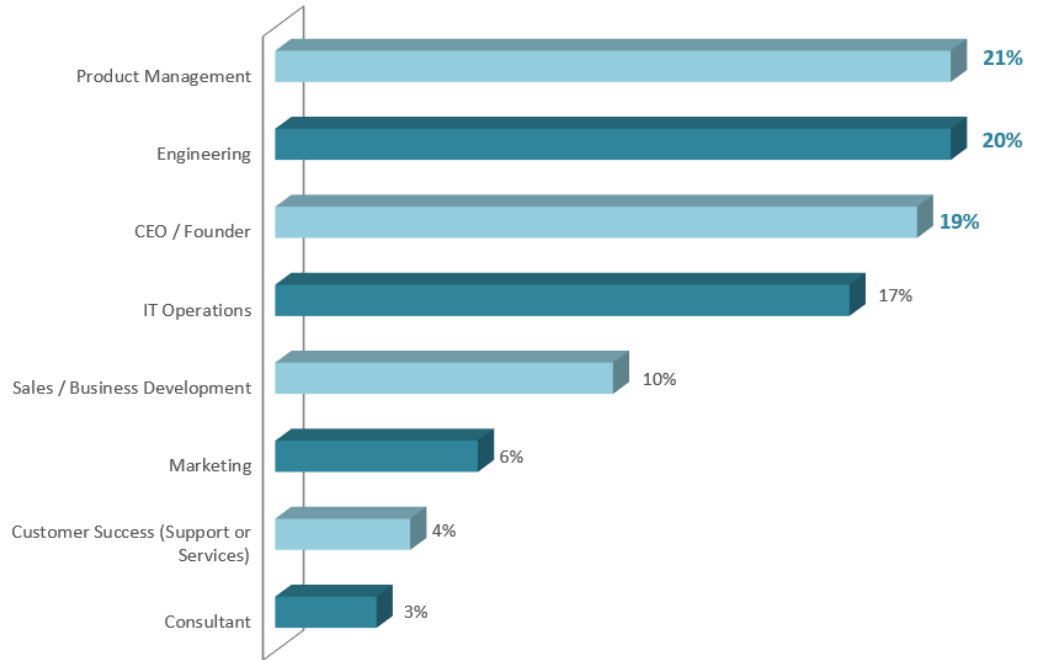
Manual processes still prevalent despite user management APIs -- Despite 68.19% of SaaS vendors having a user management API, vendors admitted that manual processes to add users to their application were still common; 29.14% of SaaS vendors said adding users manually through their app was common; 20.57% admitted that importing users via a delimited file was common.

Giving SOAP a REST -- 51.82% of respondents had a user management API based on REST; 14.64% supported SCIM; Only 2.73% relied on SOAP.

PROFILE OF SURVEY RESPONDENTS

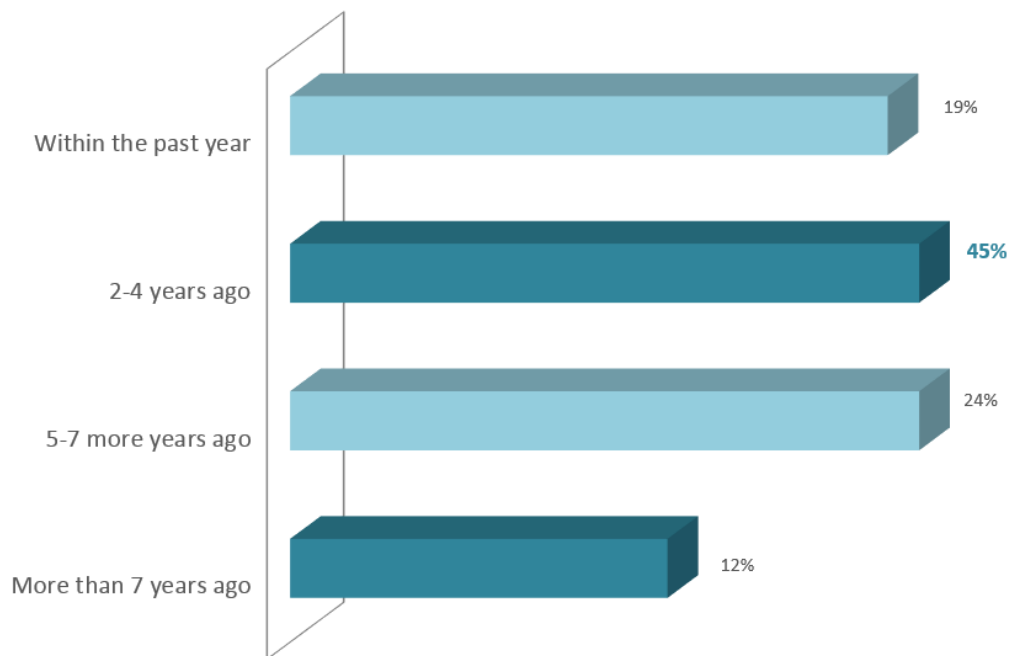
Respondents were primarily in a product management (21%), engineering (20%), CEO/Founder (19%) or IT operations role (17%).

What is your role in the company?



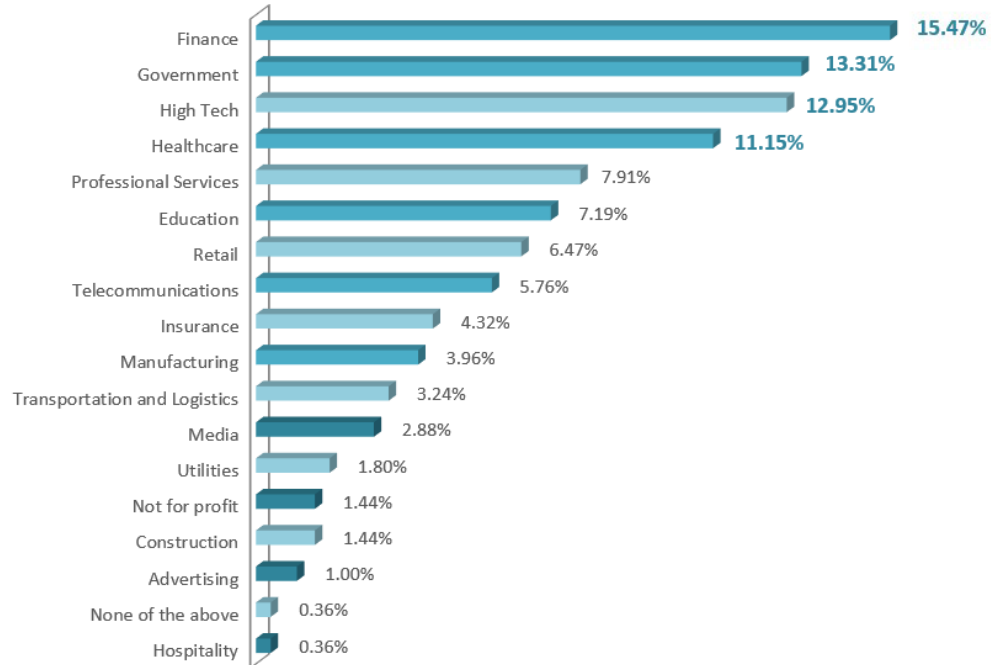
Most SaaS vendors surveyed had first delivered their app within the last 2 - 4 years (45%).

When did your company deliver its first SaaS application?

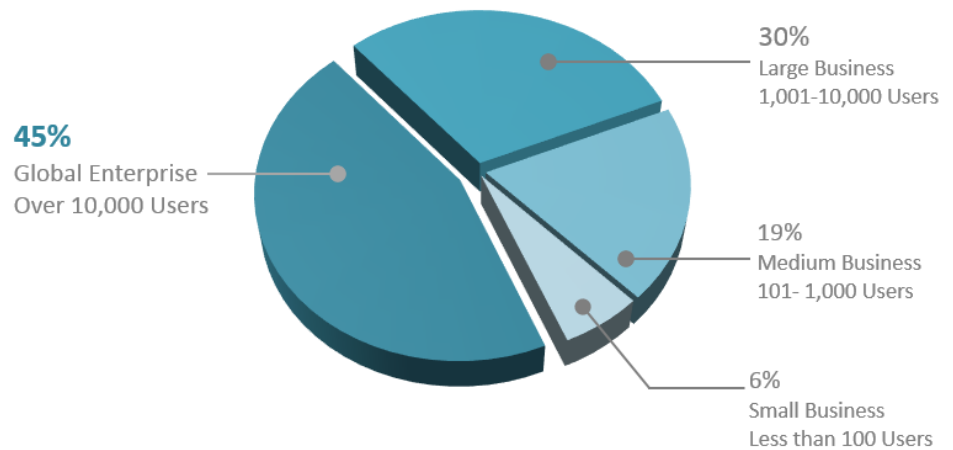


Respondents serve a broad spectrum of industries with Finance (15.47%), Government (13.31%), High Tech (12.95%) and Healthcare (11.15%) leading the way.

What are the top three verticals that you serve?

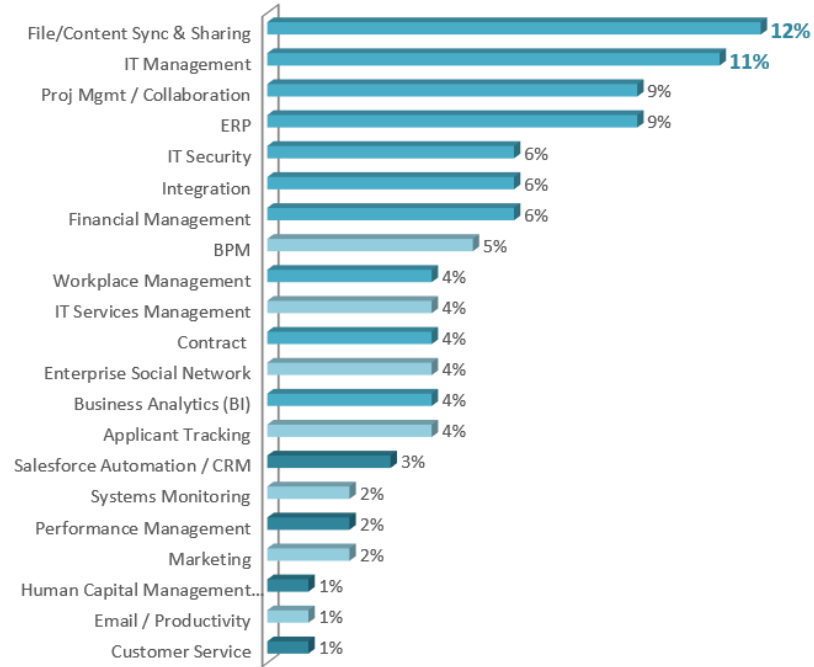


Which size company represents your largest customer segment?

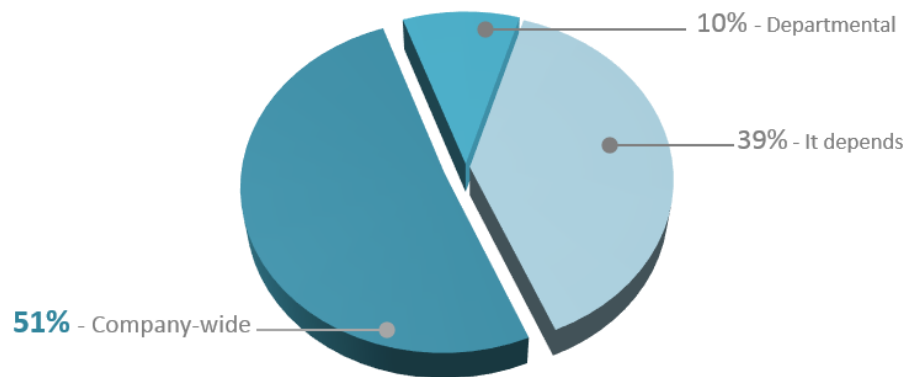


PROFILE OF SAAS OFFERINGS

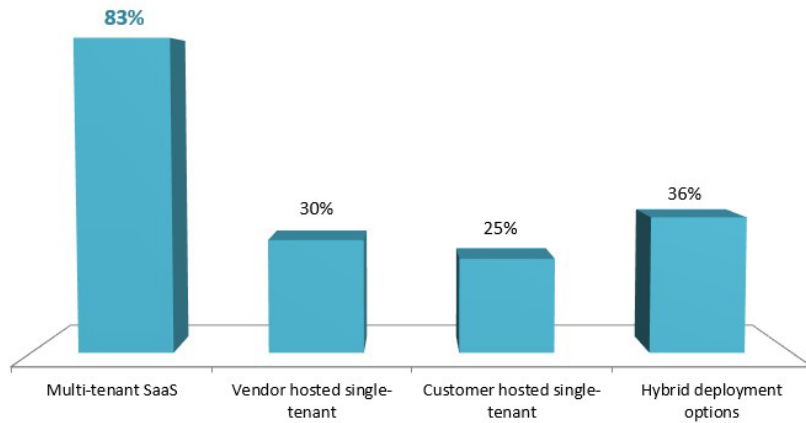
What is the category that best describes your SaaS offering?



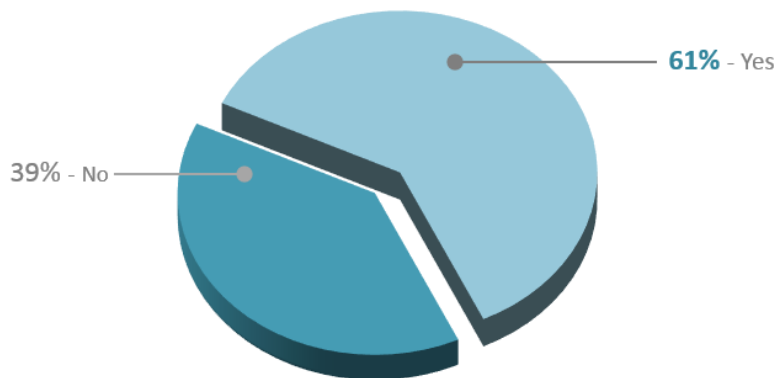
Is your app typically deployed in a department or company-wide?



What deployment options do you provide to your customers?

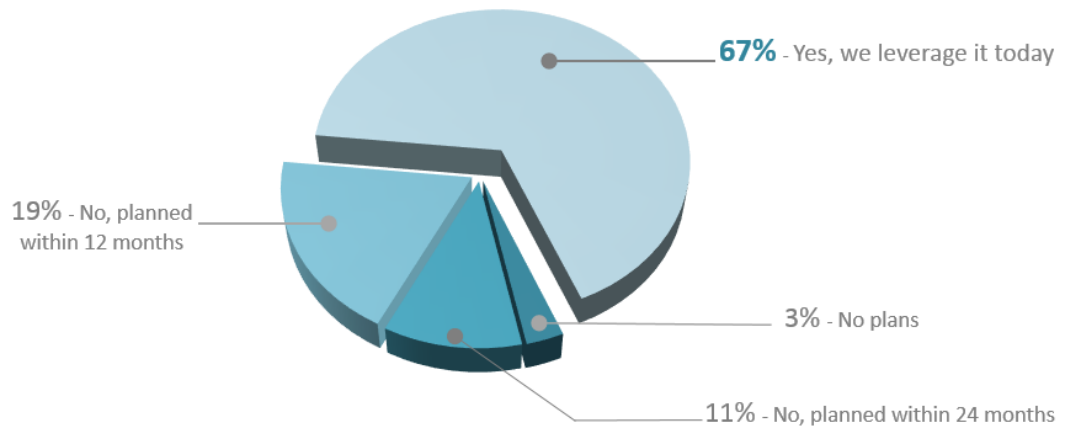


Does your application store information deemed sensitive by regulatory requirements or consensus industry definition?

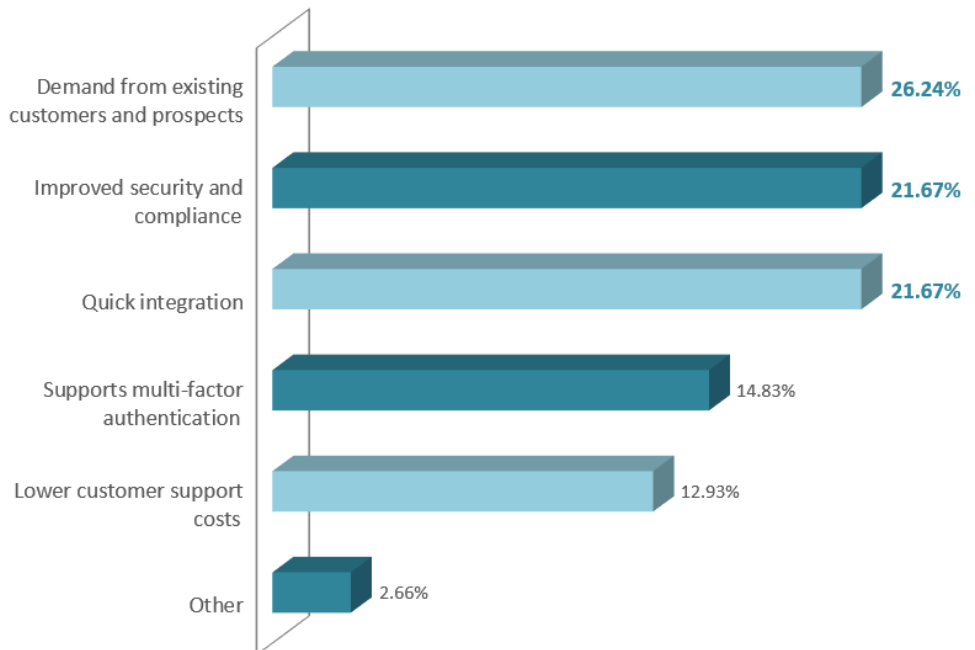


STANDARDS, ASSURANCE CERTIFICATIONS AND USER MANAGEMENT

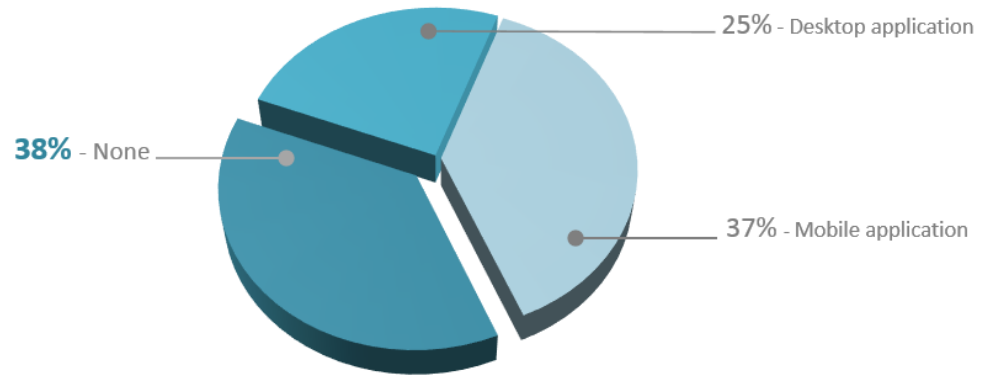
Do you currently leverage or plan to leverage SAML?



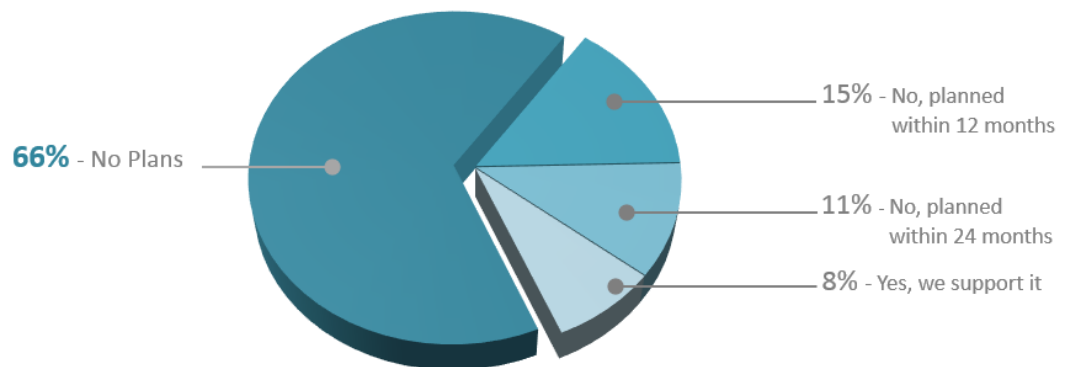
What do you see as the reasons to adopt SAML?



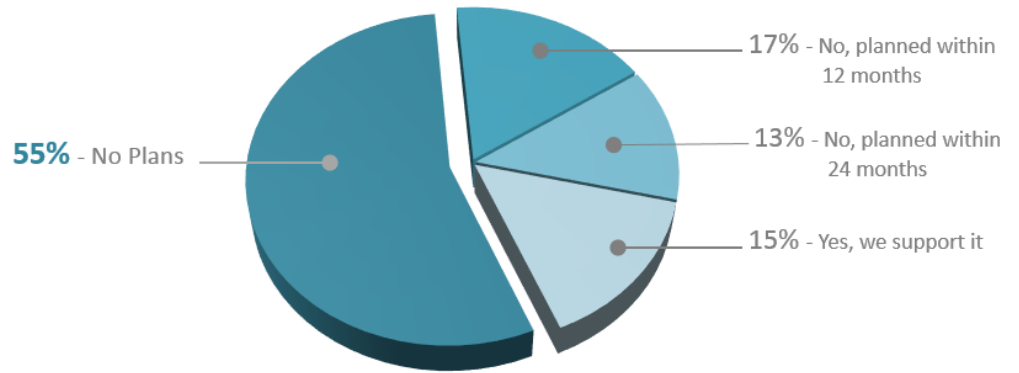
Does your SaaS application also have a mobile or desktop app (not including a web browser) that supports SAML?



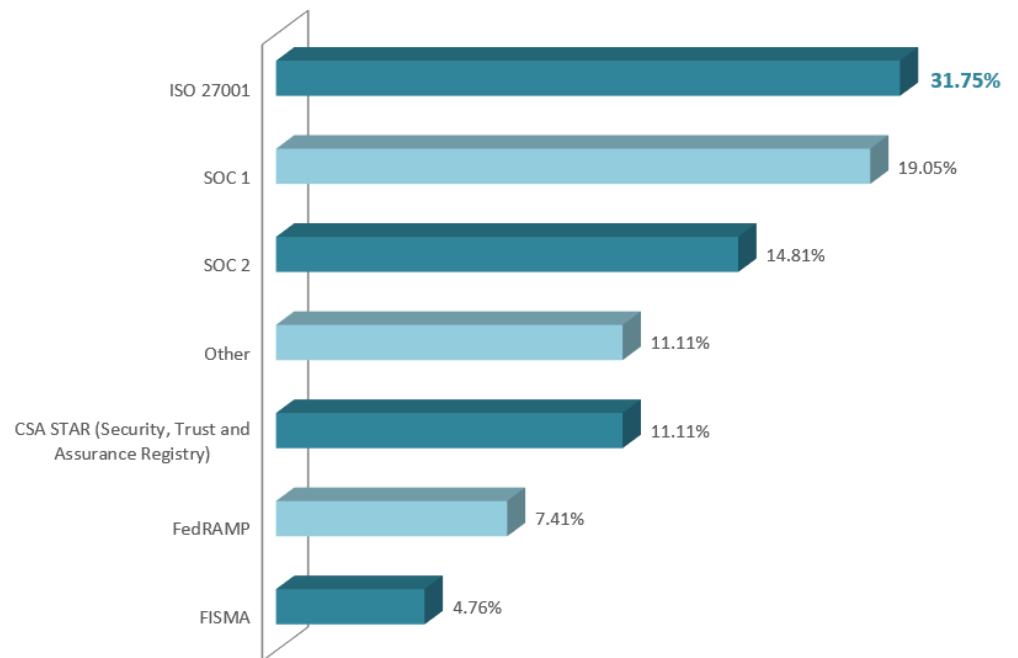
Do you support or are you considering supporting the SPML provisioning standard?



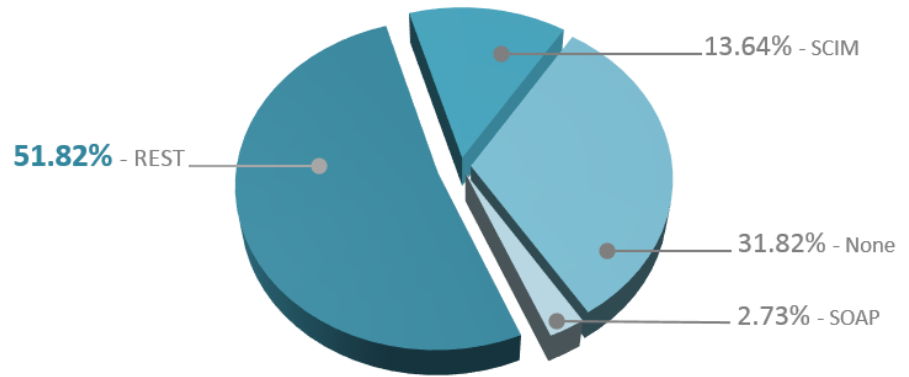
Do you support or are you considering supporting the SCIM provisioning standard?



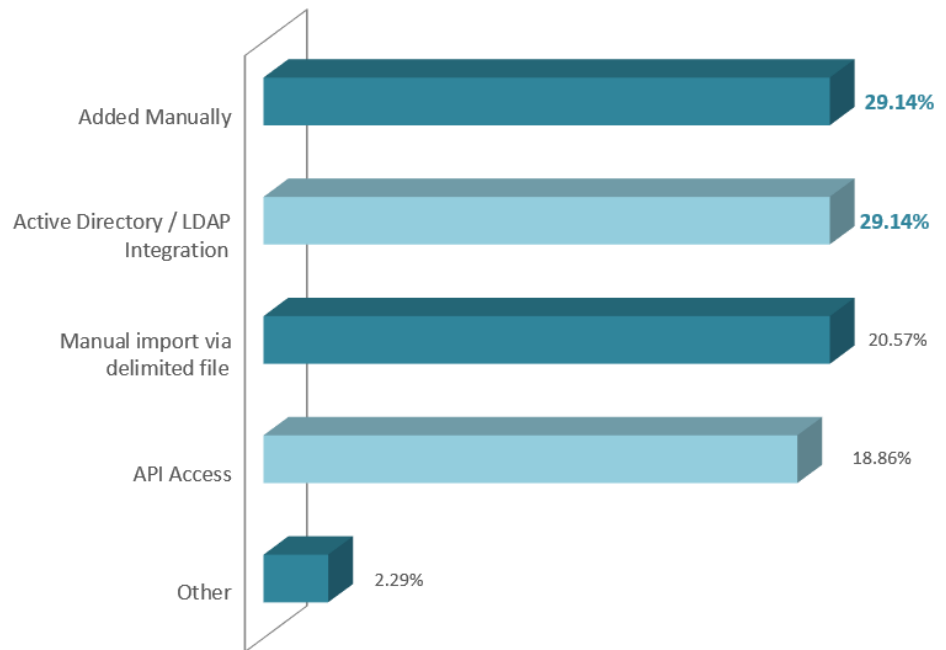
What assurance certifications does your company have or intend to achieve in the next 12 months?



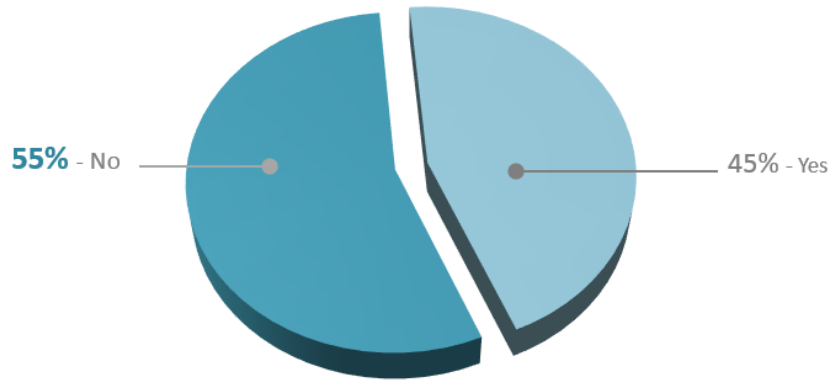
Does your application have a user management API?



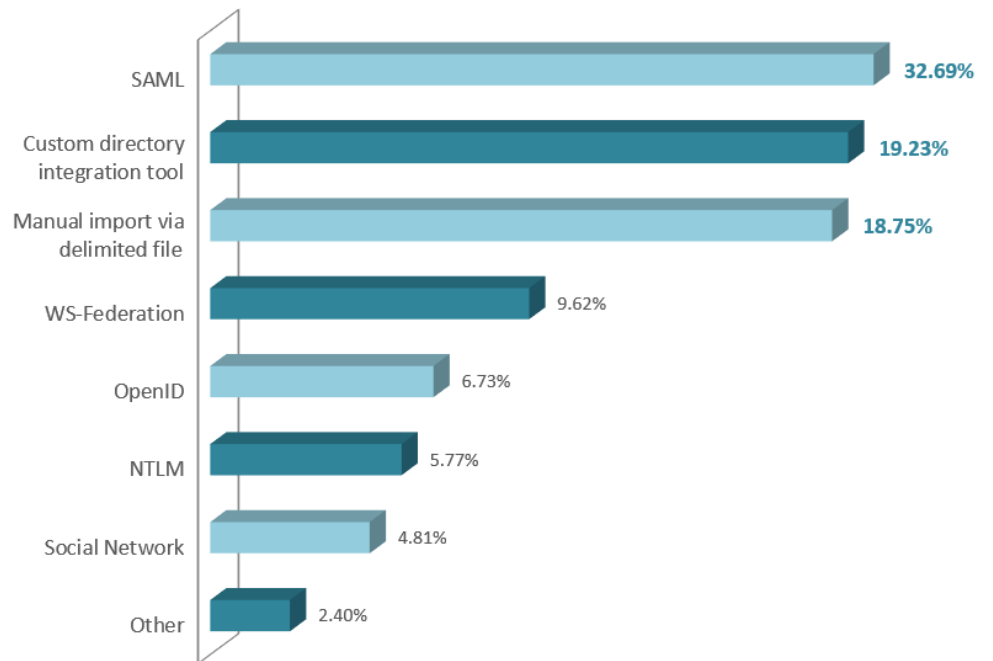
How do your customers most commonly add users to your application?



Have you developed your own directory integration that can sync and authenticate users?



How do your customers integrate your app with their Active Directory or LDAP server?



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 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 regains control over web application access, LOB owners quickly on- and off-board team members, and end-users enjoy easy access to all their apps. OneLogin has over 800 enterprise customers in 44 countries across the globe, including innovators like Netflix, Pinterest, Uber, Yammer and GoPro as well as enterprise stalwarts such as Steelcase, News Corp, Midas, Condé Nast, Herman Miller, The Carlyle Group, and the Victorian Managed Insurance Authority (VMIA). Try our free forever plan with three cloud apps and an unlimited number of users. This plan includes single sign-on for web, mobile and iPad, directory integration, and multi-factor authentication. Signup here <http://www.onelogin.com/signup/>

ABOUT ONELOGIN'S OPEN SOURCE SAML TOOLKITS

The Gold Standard for signing into cloud applications is SAML. Why? It completely eliminates all passwords and instead uses digital signatures to establish trust between the identity provider and the application. Many SaaS vendors already support SAML and you can SAML-enable your internal web apps in as little as two hours using one of OneLogin's open source SAML Toolkits. SAML-enabling your apps using paid vendors can cost tens of thousands a year, but can be free to you as part of the OneLogin community. Over 150 SaaS vendors use OneLogin's SAML Toolkits and free guidance. Get started here <http://www.onelogin.com/partners/get-started/>

ABOUT THE CLOUD SECURITY ALLIANCE

The Cloud Security Alliance is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within cloud computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. For further information, visit us at <https://cloudsecurityalliance.org/>, and follow us on Twitter @cloudsa.