

LOS ANGELES, CA, September 16, 2013 **/24-7PressRelease/** -- Microsoft's Office365 is one of the most ubiquitous and essential tools for millions of end users and now leading security-as-a-service firm CloudAccess ensures organizations deploying this SaaS offering can securely manage access with its recently upgraded identity management (IDaaS) adapter from the cloud.

This federated connector (application programming interface also known as API) for Office365 received an upgrade to seamlessly improve integration to various information databases such as Active Directory. According to CloudAccess, it facilitates and protects the essential communication between the SaaS and the identity source database used for account authentication.

"This solution acts as a trusted administrator by supporting tasks as creating accounts, managing permissions, profiles, and resetting passwords," said CloudAccess CEO Kevin Nikkhoo. "The result is the right people get to see the right application in a secure and compliant environment."

The connector is a key part of an identity management deployment which when integrated with access management (single sign on), creates channeled access control. In this configuration, the connector supports the key function of automatic bi-directional user provisioning/deprovisioning.

For example, when a new hire is added through a Human Resources application (like Concur or PeopleSoft), it automatically shares the credentials through Active Directory and creates identity rights and password governance for Office365. The connector simultaneously and securely transfers the information from Active Directory to the application. As most employees need to use a multitude of various applications, these credentials (based on corporate role or need-to-know policies) can be bundled together and validated through a single sign on solution.

"If your employees access Office365 from any computer, smartphone or device, not only do you want to streamline their usage, but you must make certain their credentials are valid and that every log in, and modification is automatically logged and reviewed for regulatory compliance," Nikkhoo added. "Our connector and cloud-based identity and access management simply makes it easier and less expensive to achieve those goals."

Although the connectors are a component of an identity management solution (CloudIDM), the

seamless integration with CloudAccess' Access Management (CloudAM) solution ensures the continuous control of user credential protection across an enterprise regardless of size, hierarchical complexity or operational preferences. It also promotes authentication best practices, centralizes management of an application portfolio and satisfies regulatory compliance.

CloudAccess is the only company that currently provides a multi-tenant cloud security option for both identity and access management as an integrated solution set.

Currently CloudAccess promotes federated access connectors for several dozen popular applications. Additionally, using the company's proprietary identity gateway solution, hundreds of legacy and web applications are additionally enabled for credential administration (identity management) and enterprise access distribution (access management).

Contact CloudAccess at <http://www.cloudaccess.com/contact> to schedule a demo for the integrated identity management and access management solutions or call 877-550-2568 for more information.

CloudAccess provides comprehensive security-as-a-service from the cloud. Our suite of robust and scalable solutions eliminates the challenges of deploying enterprise-class security solutions including costs, risks, resources, time-to-market, and administration. By integrating and centralizing the collective intelligence from our proprietary products like SIEM, Access Management, Identity Management, Log Management, Single Sign On, and Web SSO, Cloud Access offers cost-effective, high-performance solutions controlled and managed from the cloud that meet compliance requirements, diverse business needs and ensure the necessary protection of IT assets.