

# Confidently Adopting Cloud Services in Your Enterprise

If you are considering adopting cloud services into your enterprise, managing who has access to what and securely protecting identity information are major concerns. Consulting and our partners can help you implement the necessary strategies both inside and outside your firewall to resolve security and access concerns to cloud-based services.

## Cloud Security at a Glance:

### ■ Identity Manager:

You can enforce enterprise compliant processes with internal applications on physical hardware as well as virtually hosted and remote SaaS applications.

### ■ CloudAccess:

This solution gives cloud service vendors the power to manage user access, secure data storage, and ensure regulatory and corporate compliance—all without storing sensitive identity information on their end.

**Micro Focus can help you craft an identity-driven cloud security strategy that will allow you to confidently adopt cloud computing into your enterprise.**

## Adopt Cloud Services Confidently

The promise of reducing costs by paying for computing resources, software and services as needed may be enticing. However, you may also be reluctant to utilize such cloud services because of security concerns. Consulting and our partners can help you address these concerns so you can confidently enjoy the benefits of cloud computing while maintaining a secure enterprise.

## Cloud Security Begins Inside Your Firewall

The heart of any enterprise cloud security strategy starts with your identity management solution. Without an identity management solution specifically designed to include the cloud, you may be at risk. Identity Manager, the next-generation identity management solution from Micro Focus, can help.

With the NetIQ® Identity Manager family of products, you can enforce enterprise compliant processes with internal applications on physical hardware as well as virtually hosted and remote SaaS applications. Imagine being able to control who has access to what applications—no matter where those applications are running.

Identity Manager provides incredibly scalable and highly available user provisioning and de-provisioning, not only for physical and virtual resources inside your firewall, but also for cloud-deployed resources outside your

firewall. Identity Manager can report user information for any accessed resource, even if that resource is in the cloud.

## Effective Cloud Security Involves Your Service Providers

Enjoying a cloud-ready identity management solution is only half of any cloud security strategy. Cloud service providers should also have your security in mind. Luckily, Micro Focus has a solution that is easily implemented by cloud service providers. It allows you to control your own identity information inside your firewall while still guaranteeing secure access to providers' cloud services.

Micro Focus® CloudAccess gives cloud service vendors the power to manage user access, secure data storage, and ensure regulatory and corporate compliance—all without storing sensitive identity information on their end. With a few simple plug-ins to your existing identity management infrastructure, you can enjoy simple, secure cloud interactions with any cloud service provider using CloudAccess.

## CloudAccess Strategy—A Consulting Overview

Consulting and its partners are experts in identity management and cloud security solutions. Let them start with a cloud security strategy engagement, a two-week engagement that assesses the current readiness of your identity management solution to provide secure, identity-driven access to cloud services.

**To truly capitalize on all the benefits of cloud computing and ensure compliance across your enterprise, you must have a solid cloud security strategy. Consulting and its partners can help.**

Contact us at:  
[www.microfocus.com](http://www.microfocus.com)

Like what you read? Share it.



The cloud security strategy engagement features interconnected business and technology tracks that converge into a final, integrated cloud security roadmap that is tailored to your organization. The cloud security strategy methodology includes three distinct phases: assessment, analysis and planning.

#### **Assessment Phase**

During the assessment phase, the following tasks will be accomplished:

- Confirm drivers and goals
- Assess the current state of the identity management infrastructure and architecture
- Assess current identity-related and cloud security processes

#### **Analysis Phase**

Using the results of the assessment phase, the analysis phase will:

- Determine key technology and process gaps

- Identify needed cloud security capabilities and integration points
- Identify and prioritize potential cloud security initiatives

#### **Planning Phase**

Using the results of the assessment phase, the analysis phase will:

- Define high-level, future-state cloud security architecture
- Develop a phased implementation roadmap
- Document and present final recommendations

With a CloudAccess cloud security strategy engagement from Consulting or one of its partners, you can confidently start to adopt cloud services into your enterprise. To learn more about how Consulting and our partners can help you with your cloud computing initiatives, [visit here](#).