Microsoft

Hybrid cloud series

Getting a handle on hybrid identity

Organizations work in hybrid environments for a variety of reasons: the need to quickly scale up processing power or storage, the ability to optimize costs, or the need to connect and manage resources operating in two different environments. As companies find themselves working across on-premises and cloud environments, managing identity—how employees access services and how IT governs this access—can become complex.

Hybrid environments without an identity strategy can create challenges

The complexity of managing identity and access across users, apps, and devices is compounded by the enormous growth in the number of endpoints, the accelerating rate of attacks from a variety of vectors, and increasingly complex operations of securing and managing identity access across and beyond the organization. The average employee uses at least 36 cloud services at work,[1] although other estimates put the number much higher.

Simplifying a complex and chaotic identity environment is not only ideal, it's attainable—through these four steps:

1. **Move workers to a single identity to improve productivity**
2. **Reduce management overhead through simpler identity infrastructure**
3. **Monitor anomalous activity for greater security**
4. **Give users the tools to be secure**

Read on to discover how these four steps can deliver tangible benefits for your business.

Microsoft

1. Move workers to a single identity to improve productivity

By reducing the number of logon credentials each worker needs to memorize, a single identity and credential across your hybrid systems results in more productive employees. A single sign-on (SSO) capability reduces password resets, enables employees to maintain their own accounts, and results in faster access to necessary services.

Additionally, with a SSO your company can provide workers with a portal from which to launch pre-integrated applications and provide employees with the desired workflow.

2. Reduce management overhead through simpler identity infrastructure

You can reduce complexity by implementing an identity infrastructure that is synchronized across on-premises servers and cloud services. Identities maintained on Active Directory servers, for example, can be easily extended to the cloud to provide services to workers. In addition, identities can be shared and managed across environments by using modern protocols and cross-platform APIs.

Provisioning and de-provisioning users by accessing a single identity store is much simpler than tracking down every employee account on the multitude of services used by employees. The average worker lost their company $420 in productivity every year due to time wasted managing their passwords.[3] Linking identities in the hybrid cloud allows employees to manage their own information, reset passwords on their own, and significantly reduce overhead.

3. Monitor anomalous activity for greater security

By monitoring users and enforcing single identities, companies can improve the security of the information systems and cloud services. An identity and access management (IAM) system gives your company the ability to analyze the overall activities of users without having to match their various user accounts to the individual. Searching for outliers can focus security efforts on compromised credentials or hacked accounts.

4. Give users the tools to be secure

Once each worker has a single identity, you can focus your efforts on making those identities as secure as possible. Additional factors of authentication—such as a one-time password token or mobile application—can be easily added. Services can be accessed securely from virtually anywhere without the need for a virtual private network, as the data is encrypted through web protocols. Multi-factor authentication allows companies to add extra security to sensitive accounts or for all employees, depending on the use case.

Find solutions for managing identity in a hybrid cloud environment

Azure Active Directory

- Integrates with on-premises Active Directory
- Easily moves on-premises apps to the cloud with Azure Active Directory Domain Services (ADDS)
- Offers identity services using Azure Active Directory Federation Services (ADFS)

Azure Authenticator for multi-factor authentication

- Enhances security in risky use cases with additional authentication

Footnotes

[1]Kohgadai, Ajmal. "12 Must-Know Statistics on Cloud Usage in the Enterprise." Skyhigh Networks. https://www.skyhighnetworks.com/cloud-security-blog/12-must-know-statistics-on-cloud-usage-in-the-enterprise/

[2]Preimesberger, Chris. "How Companies Are Losing Money on Password Time-Wasting." eWEEK. October 21, 2014. http://www.eweek.com/security/how-companies-are-losing-money-on-password-time-wasting