

# **Starling Cloud Platform from One Identity (OI)**

## **Enterprise access management for the cloud**

The use of both on-premise software solutions and cloud-based applications is a reality in companies today. What does this mean for secure access management in terms of Identity Governance & Administration (IGA)? There is no universal solution, because each company's cloud journey is highly individual. The Starling platform from One Identity provides the technical and administrative basis for a company-specific solution that ensures that current IT security requirements are met even in a hybrid environment.

## **Secure integration of cloud-based services**

Today's organizations must be flexible to constantly changing and evolving requirements. A cloud-based IT infrastructure usually includes storage space, computing power or even application software and enables companies to react to changing conditions in a demand-oriented and resource-saving manner. IT security is a major concern because numerous users may have access to the cloud resources. The encryption of stored data plus access and rights control are therefore crucial. One Identity Starling Connect provides the necessary connectors to integrate the various systems and offers many services to significantly increase security, e. g. through two-factor authentication and the automated management of access requests or certifications.

## **Connectivity is the key**

Companies have many different systems and applications within their environment and the cloud. To ensure employee productivity even during the implementation of a new professional identity and access management system, it is important that all applications can be integrated as quickly and easily as possible. One Identity provides a large number of connectors covering various interfaces and standards. Thus, authorization requirements or access certifications can be managed centrally and across the entire system landscape.

## **Strong access protection thanks to two-factor authentication**

Compromised passwords represent a high security risk for companies. To protect organizations against data security breaches, they can establish the strongest possible authentication for accessing corporate systems with two-factor authentication. The SaaS-based solution of One Identity offers different authentication methods. For example, users can use the mobile app for iOS, Android and Chrome to generate initial passwords or have one-time passwords sent to them via SMS or phone calls. Alternatively, authentication via keypress can also be selected. Once the username and password have been entered into

an application, an SMS verification is sent to the mobile app. Here the user can then approve or reject the login attempt.

## **Product characteristics & features**

- Synchronization of data and settings based on a standardized SCIM v.2.0. schema
- Standardization of provisioning processes
- Two-factor authentication via keystroke, SMS or call
- ADFS adapter
- Federation protocol support including SAML 2.0 for support logins to cloud applications (e.g. Google Apps, Salesforce)
- RADIUS agent for authentication via RADIUS protocol
- HTTP agent for IIS web sites
- Comprehensive audit trails for regulatory compliance

## **Your benefits at a glance**

- Automated assignment of user roles, provisioning, and enforcement of IAM policies
- Reduced risk of security breaches due to compromised authentication data
- Improved management of a wide variety of systems across the enterprise
- Consolidation of access control for hybrid system environments
- Simplification of complex user authorizations and processes
- Realization of compliance and real IGA
- Ensure a company-wide secure user access policy

„Hybrid and cloud-based system environments present IT security with special challenges. Against the background of legal requirements, compliance demands and individual security regulations companies are required to implement a policy-driven identity and access management system that ensures the highest possible level of security, transparency and compliance with regulations across the entire infrastructure. With Starling Cloud Platform and its optional services companies can provide the administrative foundation for this.”

Gerald Appel (Team Lead One Identity)