Evidian

IDaaS Identity as-a-Service

Align your IAM with your cloud strategy

The attack-surface landscape is expanding across all industries due to the rapid adoption of web-based Cloud technology, mobility and the explosion of connected devices. More and more accounts are needed to access resources and services, resulting in an increasing amount of account information to be remembered and a higher risk of security breaches.

Businesses must increase security and reduce the exposure of their entire network and software environment by implementing security controls and policies to manage access to applications and protect data. Evidian's Identity-as-a-Service (IDaaS) solution helps businesses secure access to legacy and new web-based applications and resources in the Cloud or on-premise through a central point of control, ensuring maximum efficiency, productivity and traceability.

Evidian IDaaS is a fully-featured access management-as-a-service solution that integrates bleeding edge multi-factor authentication (MFA), identity federation and Single-Sign-On (SSO) solutions for an outstanding user experience with an added level of security. The solution delivers fast time-to-value through quick onboarding, scalability and flexibility.

Facilitate access management of hybrid infrastructures

Businesses are aware of the multiple benefits of the Cloud, but migrate at their own pace to mitigate risk, ensure compliance and meet business objectives. Some businesses may even decide to keep dedicated and sensitive applications on-premise. Evidian IDaaS facilitates access control management for all applications and assists businesses at every step of their migration journey.

Evidian IDaaS provides all user profiles with a secure and single point of access to applications, thus replacing multiple existing access pages that use less secure dedicated authentication solutions. It also supports fine-grained synchronization capabilities for provisioning identities available on-premise or in Cloud-based directories.

Strengthen authentication

Reinforce security thanks to strong authentication based on multi-factor authentication. Evidian IDaaS supports a comprehensive list of authentication mechanisms including Evidian Push Authentication, the latest FIDO 2 framework, and third-party authentication delegation (via RADIUS and SAML).

• Evidian Push Authentication provides fast, convenient and frictionless one-touch authentication from mobile devices

• Evidian IDaaS supports new passwordless Fast IDentity Online (FIDO) 2.0 authentication

Support Identity Federation

With Evidian IDaaS, it's possible to control who accesses IT resources while delegating partner identity authentication to an external identity provider (IdP). The solution supports SAML (Security Assertion Markup Language) 2.0 and OpenID Connect as well as OAuth 2.0 for Single Sign On (SSO), identity federation and authorization control. Users can also be provisioned between trusted domains in more complex business environments involving partners and affiliates.

Fully-featured access management as-a-service

Personalize the access portal

Evidian IDaaS adapts to the needs all organizations, regardless of size, to provide a highly customizable standalone access portal or the capacity to integrate into preexisting corporate portals thanks to the Evidian Connect SDK. The navigation menu is dynamically generated to display the right Web resources associated with a specific profile and to let users access self-service facilities such as password reset, profile management, and authentication means enrollment.

Increase productivity

Because enterprise mobility has been shown to positively impact productivity, allowing users to connect from anywhere while enjoying a user-friendly experience has become a must.

Providing a unique point of authentication and access for all users, whatever their location and device, is key to improving productivity, avoiding password fatigue and maximizing IT resources.
Evidian universal Single Sign-on (SSO) combined with strong authentication means users have only one authentication method to access resources, leading to a better user experience and reduced attack surface.

Protect REST API

REST APIs are becoming increasingly popular among developers and data scientists. They are commonly used to create custom applications or to open one's IT system to the internet. With Evidian IDaaS, it's possible to protect your APIs by managing API authorization (OAuth 2.0), securing publishing with access protection and ensuring that only the right resources are accessed by the right users using the right applications.

Enforce security

Evidian IDaaS was built with security in mind to guarantee data confidentiality, prevent session or identity usurpation, and ensure trust in protecting information streams. Thanks to its self-service functionality, users can manage their passwords and enroll authenticators, thus avoiding exchanging sensitive information with third parties and reducing helpdesk calls.

Evidian IDaaS doesn't require the use of plug-ins for Web browsers or modifications of applications reducing potential risks in working environments.

IDaaS can also complement CASB, Cloud Security and Network Security aaS to provide a comprehensive protection for all businesses.

Zero Trust

A significant number of businesses and CISOs are looking to move towards a Zero Trust Security framework, which includes continually assessing access to corporate services regardless of whether they are on-premise, internet-facing, or Cloud-hosted. Authentication and access right governance are key topics that need to be tackled to conform to "Zero Trust" where every access role must be designed following the least privilege principle – for everyone, always, everywhere. Evidian IDaaS helps build the secure foundation necessary for "Zero Trust" by providing a fully-featured authentication and access management-as-a-service solution.

For more information: **www.evidian.com**

CT-200429-RD-FS-IDAAS