DirX Access Trusted Collaboration

Identity Federation, Access Management, and SSO for the Connected World

The Challenge

Enterprises and other organizations such as government agencies, financial or healthcare service providers use the Internet to work more efficiently and cost-effectively and offer services at low cost. They enter into online partnerships, use information and applications based on Service-Oriented Architectures with web services and also offer their services to private consumers. Cloud and SaaS (software as a service) application adoption has soared as it has proved to offer great economies of scale for many organizations by providing a lower-cost, flexible way to use applications and services. As more and more security-critical data finds its way into the web, organizations demand a web access management solution to protect data against unauthorized use and to enable the right users to have the right access to right resources at the right time without comprising security. Building a business-agile virtual enterprise using on premise applications and private and public cloud or SaaS offerings involves numerous security challenges to provide end- to-end security. The emergence of cloud, mobile and social computing has heightened the need for strengthened access controls to ensure compliance with the organization's authentication and authorization policies. Partners must share or integrate their identity data, but they must do it without creating security holes. To improve the user experience, partners must offer single sign-on (SSO) capabilities to applications and services hosted internally or in the cloud. They must also provide rapid onboarding of new users to cloud services to avoid the daunting task of manually and individually provisioning and managing users in each Cloud or SaaS directory.

Partners also need to consider security models that move collection and control of identity information away from online service providers and into the hands of their users and assign the management of this data to online identity providers.

The demand to leverage social identities to support user authentication using identities provided by Google, Facebook, LinkedIn or other third-party identity providers leads to an extra challenge in terms of security when accessing an enterprise's application.

For organizations that want to avoid that hackers gain unauthorized access to critical data there is an additional need to protect their web sites and portals by additional contextual authentication mechanisms that require users to authenticate with an appropriate authentication method which is selected based on risk indicators associated with the user's login activities.

Our Solution

DirX Access, part of Atos' DirX family for IAM solutions, is tailored to meet these challenges and enables the protection of web applications and services. The latest security models for web access management have been implemented and integrated in a single product: authentication, authorization, audit, and web single sign-on (SSO), in conjunction with identity federation based on SAML, OAuth 2.0 and OpenID Connect, just-in-time provisioning, entitlement management, policy enforcement and secure web services, supply the main functions for protecting web resources flexibly against unauthorized use, either in the cloud or on premise. DirX Access enables the consistent enforcement of security policies in an enterprise or in the cloud leveraging central, policy- based authentication and authorization services. It supports compliance with official and internal regulations based on audit functions.

The latest Security Models in a single Product

Key Strengths

- **Identity Federation**

  Supports industry federation standards such as SAML, OAuth 2.0 and OpenID Connect and can be deployed both as identity provider and service provider.

- **Cloud support**

  Supports out-of-the-box identity federation with Cloud and SaaS service providers.

- **Strong, multi-factor, and adaptive (risk-based)**

  With risk-based authentication (also called adaptive authentication), access to resources is secured by means of risk analysis. Risk analysis is based on the evaluation of predefined conditions and takes into account historical and contextual data. The result of the risk analysis determines the minimum strength of the authentication method to be used for accessing the resource.

- **Versatile authentication**

  Enables secure and convenient access to web applications and resources thanks to once- only authentication and provides a broad range of authentication methods including multi-factor authentication and support of FIDO-based authentication methods.

- **Step-up authentication**

  Requests re-authentication using a stronger authentication mechanism when accessing a more critical resource.

- **Central, policy-based authorization**

  Supports central, consistent enforcement of security policies for accessing web applications and resources.

- **User-managed access (UMA 2.0)**

  Allows users to manage access to their resources and data in an un-precedently fine-grained and configurable way. The implementation of the UMA 2.0 standard represents a bridge to the authorization within an IoT (internet of things) world.

- **Standards-based policy management**

  Comprises functions to manage authorization and authentication policies based on the XACML standard.

- **Authentication with social media identities**

  Seamless access through social identity providers such as Facebook or Google eases the authentication process for users when accessing low-risk resources by avoiding additional logins.

- **Web single sign-on**

  Enables secure and convenient access to web applications and resources thanks to once-only authentication.

- **Centralized session management**

  Manages security sessions by maintaining user information (claims) that can be used in authorization decisions.

- **Web services security for SOA**

  Enables central, consistent enforcement of security policies for web services in service-oriented architectures.

- **Microsoft SharePoint Support**

  Provides identity federation with Microsoft SharePoint by supporting the WS Federation Passive Requestor Profile for authentication in SharePoint.

- **Administration and user repository**

  Leverages LDAP directory servers for storage of configuration and policy data; any standard LDAP directory can serve as a user repository.

- **Reliability, High Availability and Scalability**

  Supports active-active deployments to achieve maximum availability and failover security as well as scalability and load balancing.

- **Various deployment models**

  Integrates with the applications it protects through policy enforcement points deployed as plug-ins to web and web application servers or other applications and also supports reverse-proxy configurations.

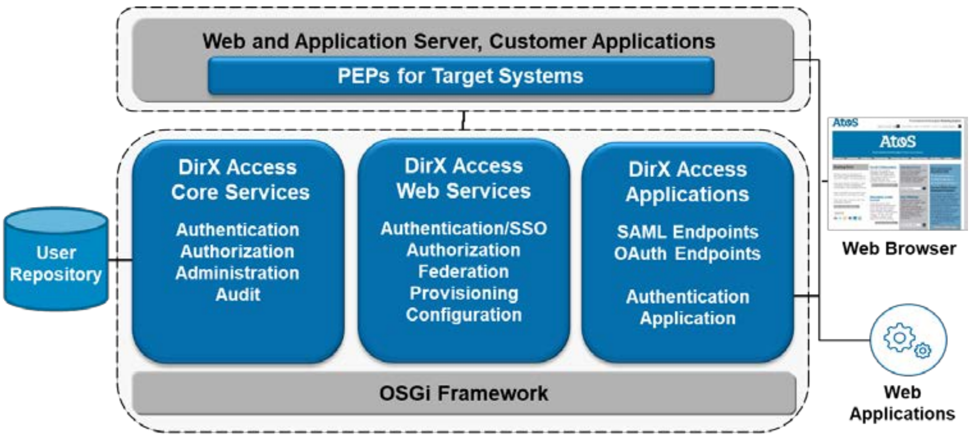
- **Audit**

  Automatically records results of authentication, authorization and other security-related events and stores these records securely for later analysis.

Your Benefits

- Provides cost-efficient end-to-end security for the extended enterprise (designed to support both highly available and highly scalable deployments)
- Highly improves the user experience and lowers costs of compliance
- Enables seamless, secure and convenient access to web applications and resources by customers and business partners without the need to manage their identities and credentials or to synchronize their user repositories
- Allows fine-grained entitlement management across multiple applications and services
- Allows to leverage social media identities to eliminate the need to follow registration processes if users are already signed up at a social media identity provider
- Reduces risk of fraudulent activities by strengthening authentication processes
- Enables enterprises and service providers to deploy strong authentication solutions that reduce reliance on passwords.
- Support millions of users in large-scale and mission-critical infrastructures
- Seamless integration with Microsoft products
- Provides proof of activity via audit services that help to prove compliance with business and privacy regulations

DirX Access Architecture



Identity Federation, Access Management, and SSO for the Connected World

For more information: www.evidian.com/dirx

Factsheet-Evidian-DirX-Access-V9-en