Evidian

DirX Access
Vertrauensvolle Zusammenarbeit

Identity Federation, Access Management und SSO für die vernetzte Welt

Die Herausforderung

Unternehmen und Organisationen wie öffentliche Verwaltungen oder Anbieter von Finanzdienstleistungen oder von Diensten im Gesundheitswesen nutzen das Internet, um effizienter und kostengünstiger zu arbeiten und um Dienste preiswert anbieten zu können. Sie gehen Online-Partnerschaften ein, nutzen Informationen und Applikationen auf der Basis von Web Services und bieten ihre Dienste auch privaten Nutzern an. Die Nutzung von Cloud- und SaaS-Anwendungen steigt rapide, da sich gezeigt hat, dass dies für viele Unternehmen und Organisationen durch die kostengünstigere und flexible Art, Anwendungen und Dienste zu nutzen, zu großen Einspareffekten führt. Da mehr und mehr sicherheitskritische Daten ihren Weg ins Internet finden, fordern Organisationen eine Web Access Management Lösung, um Daten gegen unbefugte Nutzung zu schützen und den richtigen Benutzern den richtigen Zugriff auf die richtigen Ressourcen zum richtigen Zeitpunkt zu ermöglichen, ohne die Sicherheit zu gefährden. Der Aufbau eines agilen, virtuellen Unternehmens, das interne Anwendungen oder private oder öffentliche Cloud- oder Software-as-a-Service Angebote nutzt, führt zu einigen Heraus-forderungen, um in diesem Umfeld durchgehende Sicherheit zu gewährleisten. Mit dem Aufkommen von Cloud, Mobile und Sozialen Medien ist die Notwendigkeit für eine verstärkte Zugriffskontrolle stark gestiegen, um die Compliance mit den Authentisierungs- und Autorisierungsrichtlinien der Organisation sicherzustellen. Geschäftspartner müssen ihre Identitätsdaten austauschen oder integrieren, aber dieses muss geschehen, ohne Sicherheitslücken zu erzeugen. Um die Benutzerfreundlichkeit zu verbessern, müssen Partner Single Sign-On Verfahren sowohl für interne als auch für externe Cloud-Anwendungen und -Dienste anbieten. Um schnellen Zugriff auf Cloud-Dienste für neue Benutzer bereitzustellen, müssen neue Benutzer schnell im System eingerichtet werden, so dass die aufwendige, manuelle Administration dieser Benutzer in jedem einzelnen Cloud- oder SaaS-Verzeichnis vermieden werden kann. Die Partner müssen zudem Sicherheitsmodelle für Online-Transaktionen der Nutzerdaten berücksichtigen, die die Sammlung und Kontrolle der Identitätsinformationen weg von den Online Service Providern in die Hände ihrer Benutzer verlagern und die Verwaltung dieser Informationen in die Hände von Identity Providern legen. Die Möglichkeit, soziale Identitäten von Google, Facebook oder anderen Identity Providern zur Authentifizierung nutzen zu können, führt zu zusätzlichen Herausforderungen an die Sicherheit beim Zugriff auf Unternehmensanwendungen. Organisationen, die verhindern wollen, dass Hacker unberechtigten Zugriff auf kritische Daten bekommen, haben die zusätzliche Anforderung, die erforderlichen Authentifizierungsmethoden anhand einer Risikobewertung auszuwählen.

Unsere Lösung

DirX Access ist darauf ausgerichtet, die genannten Herausforderungen zu meistern und ermöglicht den Schutz von Web-Applikationen und Web Services. Die aktuellsten Modelle für das Web Access Management und Identity Federation sind bei DirX Access in einem einzigen Produkt implementiert: Authentifizierung mittels mehr Faktor Authentifizierung wie FIDO oder PKI, Autorisierung, Audit und Web Single Sign-On (SSO) zusammen mit Identity Federation basierend auf SAML, OAuth und OpenID Connect, sowie Entitlement Management, die Durchsetzung von Sicherheitsrichtlinien und sichere Web Services sind die wesentlichen Funktionen, um Web Ressourcen sowohl in der Cloud als auch intern im Unternehmen flexibel gegen unberechtigte Nutzung zu schützen.

Atos

Die neuesten Sicherheitsmodelle in einem Produkt

Wesentliche Stärken

Identity Federation
Unterstützt Industrie-Standards für Federation wie SAML, OAuth und OpenID Connect und kann als Identity Provider und als Service Provider eingesetzt werden.

Cloud Unterstützung
Unterstützt standardmäßig Identity Federation mit bekannten Cloud- und SaaS-Providern.

Starke, multi-faktor und adaptive (risikobasierte) Authentifizierung
Bei risikobasierter Authentifizierung wird der Zugriff auf Ressourcen durch eine Risikoanalyse abgesichert. Das Ergebnis legt fest, welche Mindeststärke der Authentifizierung für den Zugriff auf eine Ressource notwendig ist.

Vielfältige Authentifizierung
Vielfältige Authentifizierungsmethoden, wie zum Beispiel Passwörter, X.509 Zertifikate, FIDO basierte Authentifizierung, integrierte Windows-Authentifizierung, Smartcards, HTML Forms, One-Time Password (OTP), Biometrie und Callback oder Authentifizierung.

Step-up Authentifizierung
Fordert eine weitere, stärkere Authentifizierung, wenn auf eine kritische Ressourcen zugegriffen wird.

Zentrale, policy-basierte Autorisierung
Unterstützt die zentrale und konsistente Durchsetzung von Sicherheitsregeln für den Zugriff auf Anwendungen und Web Ressourcen.

User-Managed Access (UMA 2.0)
Der Fokus bei der Autorisierung in einer IoT Umgebung, die in der Regel viele Ressource-Eigentümer hat, wird durch den Standard UMA 2.0 realisiert. Dieser ermöglicht es, die Komplexität des Autorisierungsmanagement an den Ressourceneigentümer zu delegieren.

Standard-basiertes Policy Management
Enthält Funktionen zur Verwaltung von Autorisierungs- und Authentifizierungs-Policies basierend auf dem XACML-Standard.

Authentifizierung mittels Identitäten aus Sozialen Medien
Vereinfacht den Authentifizierungsprozess für die Benutzer beim Zugriff auf weniger kritische Ressourcen durch Nutzung von Identitätsprovidern wie Facebook oder Google und daraus resultierender Vermeidung zusätzlicher Logins.

Web Single Sign-On (SSO)
Ermöglicht den einfachen und sicheren Zugriff auf Ressourcen durch einmalige Authentifizierung.

Zentrale Verwaltung von Sessions
Verwaltet Security Sessions mit den relevanten Benutzerinformationen, die in Autorisierungsentscheidungen genutzt werden können.

Web Services Security für SOA
Ermöglicht die zentrale und konsistente Durchsetzung von Sicherheitsrichtlinien für Web Services in Service-orientierten Architekturen.

Microsoft SharePoint Support
Ermöglicht Identity Federation mit Microsoft SharePoint mittels Claims-basierter Authentifizierung.

Administration und Benutzerverzeichnisse
Nutzt LDAP Directory Server zur Benutzerverwaltung und zum Speichern von Konfigurations- und Policy-Daten; jeder Standard LDAP Directory Server kann als Benutzerdatenhaltung dienen.

Hochverfügbarkeit und Skalierbarkeit
Unterstützt Active-Active-Szenarien, um maximale Verfügbarkeit und Ausfallsicherheit sowie Skalierbarkeit und Lastverteilung zu ermöglichen.

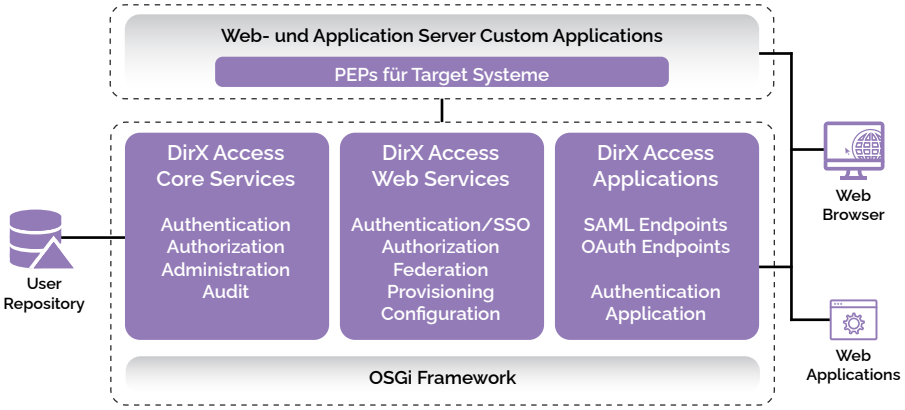
Konfigurationsmöglichkeiten
Integriert sich mit den Applikationen, die geschützt werden sollen, mittels Policy Enforcement Points, die als Plugins in Web Servern oder Application Servern oder anderen Anwendungen eingesetzt werden. Unterstützt auch Reverse-Proxy-Konfigurationen.

Audit
Zeichnet automatisch die Ergebnisse von Authentifizierungs-, Autorisierungs- und anderen sicherheitsrelevanten Ereignissen auf und speichert diese Daten für nachfolgende Analysen.

Ihre Vorteile

- Liefert durchgängige und kostengünstige Sicherheit für unternehmensübergreifende Zusammenarbeit (designt für Hoch-verfügbarkeit und Skalierbarkeit)
- Verbessert in hohem Maße die Benutzerfreundlichkeit und senkt die Kosten für Compliance
- Ermöglicht den nahtlosen, sicheren und komfortablen Zugriff von Kunden und Geschäftspartnern auf Anwendungen und Ressourcen, ohne die Notwendigkeit, deren Identitäten und Passwörter zu verwalten
- Ermöglicht die feingranulare Verwaltung von Berechtigungen für Anwendungen und Services
- Ermöglicht, Identitäten sozialer Medien zu nutzen, um Anmeldevorgänge zu vermeiden, wenn Benutzer bereits bei Identity Providern sozialer Medien registriert sind
- Reduziert das Risiko betrügerischer Aktivitäten durch Stärkung der Authentifizierungsprozesse
- Ermöglicht Unternehmen und Dienstanbietern die Bereitstellung starker Authentifizierungslösungen, die die Abhängigkeit von Kennwörtern verringern
- Unterstützt Millionen von Benutzern in geschäftskritischen Umgebungen
- Nahtlose Integration mit Microsoft Produkten
- Liefert mittels seiner Audit-Services den Nachweis von Aktivitäten, um die Einhaltung von Vorschriften für den Geschäftsverkehr und von Datenschutzbestimmungen nachzuweisen.

DirX Access Architektur



Identity Federation, Access Management und SSO für die vernetzte Welt

For more information: www.evidian.com/dirx

FS-220530-GW-DirX-Access-Factsheet-DE