Identity Manager: a személyazonosság-felügyelet alapja

A Micro Focus® Identity Manager komplett, mégis megfizethető megoldás annak szabályozására, hogy ki milyen informatikai rendszerekhez, szolgáltatásokhoz fér hozzá.

Az Identity Managerről röviden:
Az Identity Manager modulárisan, ugyanakkor integrált módon kezeli a teljes személyazonossági életciklust, hogy a vállalat mindig készen álljon az aktuális és jövőbeni igények teljesítésére.

A növekedés komplexitással és biztonsági kihívásokkal jár

A nagyvállalatok fejlődése során folyamatosan kihívást jelent az új alkalmazáskhoz és szolgáltatásokhoz való gyors hozzáférés biztosítása. Figyelembe véve az eszközök számának robbanásszerű növekedését, az IT konzumerizálódása nyomán egyszerűsödő hozzáférést és a bárhol elérhető csatlakozást, a nagyvállalatok nehezen tudják a munkahelyen is biztosítani a dolgozóik által elvárt felhasználói élményt úgy, hogy közben az alkalmazások és az adatok hozzáférését is megfelelően kézben tartják. A nagyvállalatok különböző folyamatokat vezetnek be a kihívás kezelésére, de a sikerhez alapvető fontosságú a személyazonosság stabil és eredményes kezelése. Csak így érhető el a változó üzleti igények követéséhez szükséges rugalmasság.

A folyamatos csatlakozás ma már alapvető elvárás, így bárhol és bármikor lehet dolgozni, és az üzleti felhasználók szívesebben végzik munkájukat mobileszközök felületén. Ilyen kérdések merülnek fel bennük: „Miért nem férhetek hozzá azonnal ahhoz, amire épp most szükségem van?", „Miért nem tölthetek le ehhez egy appot?" vagy „Miért kell már megint egy újabb jelszót megadnom?". Ezek a konzumerizációs, kényelmi trendek határozzák meg a technológiaválasztást.

Hasonló vagy akár nagyobb kihívás a vállalati eszközök és az adatok védelme és a belső és külső szabályozó mechanizmusoknak való megfelelés. A kényes adatok illetéktelen hozzáférésének megelőzése rendkívüli kihívást jelent, amikor az informatikai részleg felügyelete nem terjed ki a felhőalkalmazásokra és a mobileszközökre.

Nem kis feladat megtalálni az egyensúlyt az egyszerű használat és a kontroll megfelelő szintje között. E kihívások legyőzéséhez a szervezetnek olyan átfogó megoldásra van szüksége, amely kezeli a felhasználói személyazonosságokat és a hozzájuk kapcsolódó attribútumokat a különböző alkalmazásokban. Ezek az alkalmazások lehetnek helyben telepítettek, partner által szállítottak vagy szolgáltatás formájában nyújtott szoftverek (software-as-a-service). A stabil személyazonosság-kezelés támogatja a megfelelő hozzáférést, és a biztonsági adatokat kiegészítve segít követni, hogyan és mikor használják a felhasználók a vállalati eszközöket. A Micro Focus személyazonosság-felügyelet (Identity Governance and Administration, IGA) terén követett stratégiai szemlélete bezárja a szervezetet kockázatnak kitevő kiskapukat, ugyanakkor kielégíti a felhasználók sokrétű igényeit – a munkavállalóktól az ügyfelekig.

Az Identity Manager átfogó szemlélettel kezeli a komplex követelményeket

Az Identity Manager a teljes személyazonosság-felügyeleti életciklust kézben tartja, és a személyazonosságok, illetve a kapcsolódó attribútumok kezelésével minimumra szorítja a privilégiumokat. Így a szervezet lefaraghatja a manuális fiókkezelés költségeit, demonstrálhatja a megfelelést, és az illetéktelen hozzáférés kockázatát is csökkentheti. Mindez a szervezet működésében kritikusan érintett valamennyi fél számára előnyös. Többek között alábbiakat teszi lehetővé:

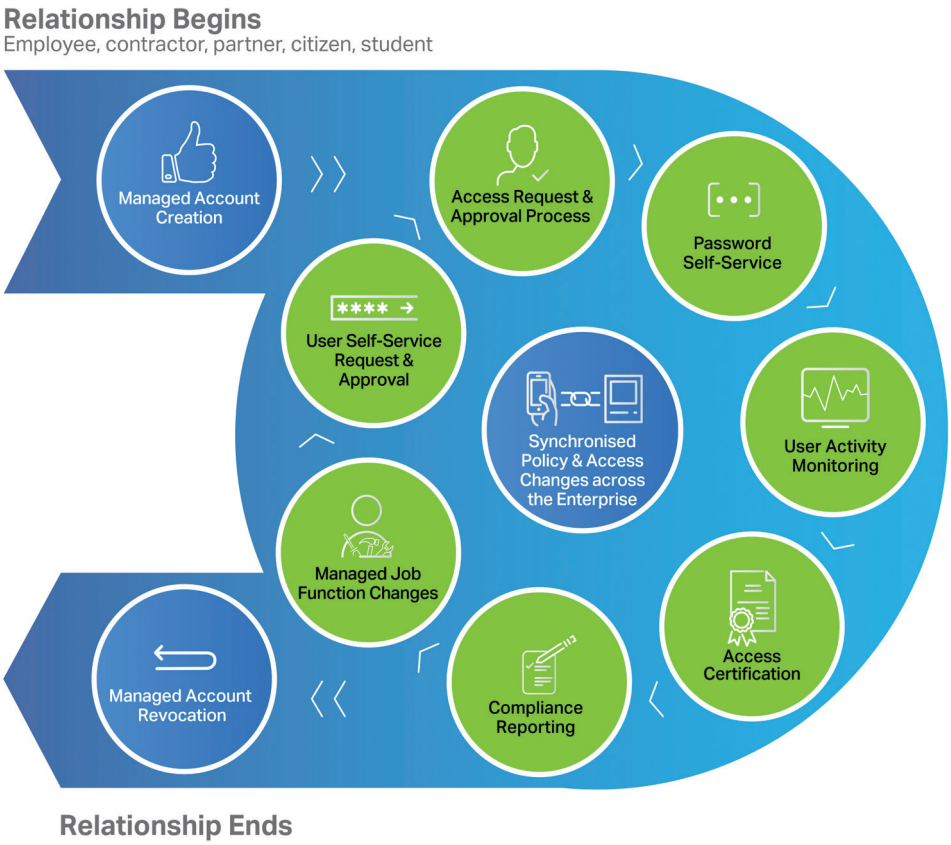
- A CIO mérsékelheti a megfelelés költségét és kényelmesebb hozzáférést biztosíthat a dolgozóknak, így a vállalat új lehetőségeket aknázhat ki
- A CISO a vállalat egészében érvényesítheti a megfelelési és biztonsági szabályokat a hozzáférés terén
- Az üzletágvezetők az erőforrások azonnali, szerepkör-alapú hozzáférésének biztosításával megőrizhetik csapataik produktivitását

- Az IT-vezetők jobban gazdálkodhatnak az erőforrásokkal, és személyazonosság-alapú használati adatokkal láthatják el a főbb érintetteket

Az Identity Manager modulárisan, ugyanakkor integrált módon kezeli a teljes személyazonossági életciklust, hogy a vállalat mindig készen álljon az aktuális és jövőbeni igények teljesítésére. Képességei közé tartoznak az alábbiak:

Menedzselt fióklétrehozás, -visszavonás és munkakörváltoztatások: Az Identity Manager integrált szerepkörök-szabályok-munkafolyamat motorja jelenleg a piacon a leghatékonyabb megoldás. Az erőforráskiosztás a szervezet számára szükséges mértékben automatizálható. A motor az üzleti szabályokat az opcionális szerepkör-alapú erőforráskiosztás hatékonyságával ötvözve leképezi a szervezet üzleti működését, és lehetővé teszi a munkafolyamat-motor számára a standard jóváhagyások és kivételek (pl. a feladatkörök különválasztásából eredő konfliktusok) kezelését.

A személyazonosság és a hozzáférés változásainak menedzselése a vállalat egészében: Az Identity Manager eseményalapú architektúrával rendelkezik, és az összes kapcsolódó rendszerben érvényesíti a személyazonossággal kapcsolatos engedélyeket, gondoskodva arról, hogy csak megfelelő forrásból jöhessenek létre személyazonosságok. Az Identity Manager az attribútumokkal kapcsolatos engedélyeket is érvényesíti, ami azt jelenti, hogy csak a személyazonosság komponenseinek „gazdarendszerei" változtathatják meg azokat, és ha a komponensek engedéllyel nem rendelkező forrásban változnak meg, automatikusan visszaállíthatók az eredeti értékre az engedéllyel rendelkező forrásban. Mindkét képesség kritikus fontosságú, amikor az erőforráskiosztási és a hozzáférési szabályok attribútumokra épülnek. A valós idejű válaszadási képességnek köszönhetően, ha felhasználói életciklus-esemény történik (pl. munkaerőfelvétel, szerepkörváltozás, munkaviszony megszüntetése), az Identity Manager adatkezelési motorja automatikus szabályalapú folyamatokat tud elindítani.



1. ábra: A Micro Focus Identity Managerrel támogatott személyazonosság-kezelési életciklus

Ezen túlmenően, a különböző alkalmazások (pl. a Microsoft SharePoint és az SAP-rendszerek) saját szabályalapú felügyelettel rendelkeznek. Az Identity Manager erőforrás-egyeztető szolgáltatásával egyszerűen konszolidált katalógusba integrálhatók a különböző jogosultságok. Ez a képesség lehetővé teszi az engedélyek automatikus felismerését, és vizuális műveletek alkalmazását az erőforrások megfelelő szerepkörökre vagy Identity Manager-erőforrásokra való leképzéséhez.

A különböző szabályalapú mechanizmusok egy rendszerbe integrálása olyan egységes irányítási mechanizmust hoz létre, amely teljes képet ad a megfelelő személyeknek a felhasználói privilégiumokról, és lehetővé teszi, hogy megalapozott döntéseket hozzanak annak érdekében, hogy a megfelelő emberek férjenek hozzá a megfelelő erőforrásokhoz. Mindez nem csupán az első beállításnál biztosít egyszerű használatot. A jogosultságok folyamatos karbantartása révén lehetővé teszi, hogy a szervezet agilis rendszert alakítson ki az erőforrásgazdálkodáshoz és a jogosultságok kezeléséhez az összes csatlakozó rendszerben – függetlenül attól, hogy hol (helyben vagy a felhőben) található az adott rendszer.

A Designer for Identity Manager segítségével olyan hozzáférés-kérési folyamatok alakíthatók ki, amelyek programozás vagy testre szabás nélkül is jelentősen csökkentik az emberi hiba kockázatát. A rendszergazdák a grafikus felületen a teljes projekt-életciklust kezelhetik, például szkriptírás nélkül megtervezhetik és szimulálhatják a különböző fiókkezelési konfigurációkat.

A Designer egyik funkciója, az Analyzer for Identity Manager hatékonyan megjeleníti és összehasonlítja egymással a személyazonosság-tárból (identity vault) és a kapcsolódó rendszerekből származó adatokat, és minimumra szorítja az alkalmazások személyazonosság-infrastruktúrába történő integrálásának előkészítéséhez szükséges időt. Ezzel mérsékli az új rendszerek csatlakoztatásának idő- és költségigényét.

Önkiszolgáló felhasználói hozzáférés kérése és jóváhagyási folyamata: Egy könnyen kezelhető, felhasználóbarát műszerfal segítségével az üzleti felhasználók hozzáférési kéréseket nyújthatnak be és követhetnek, valamint ugyanarról a helyszínről kezelhetik a jóváhagyási feladatokat. Ez az önkiszolgáló képesség lehetővé teszi, hogy a felhasználók felügyeljék saját személyazonossági információikat, így produktívak maradhatnak, miközben csökkentik az IT-re a kérések teljesítése miatt nehezedő nyomást. Az erőforráskiosztási rendszerrel végrehajtott teljes körű integráció révén a felhasználók szinte azonnal hozzájutnak a szükséges hozzáféréshez, és nem kell a manuális teljesítésre várniuk.

A jóváhagyók jellemzően sokat utazó üzleti vezetők. Ha pedig a felhasználói kérésnek meg kell várnia, amíg a jóváhagyó ismét az irodában lesz, romlik a produktivitás. Napjaink világában a munka már nem helyhez kötött tevékenység. A Mobile Approval Application for Identity Manager egy olyan natív és biztonságos mobilalkalmazás, amely egyszerűn telepíthető bármilyen mobileszközre, és lehetővé teszi, hogy azonnal riasszák a jóváhagyókat, akik így bárhonnan reagálhatnak a kérésekre. Ezen túlmenően, a feladatok delegálhatók, visszaadhatók és újra hozzárendelhetők.

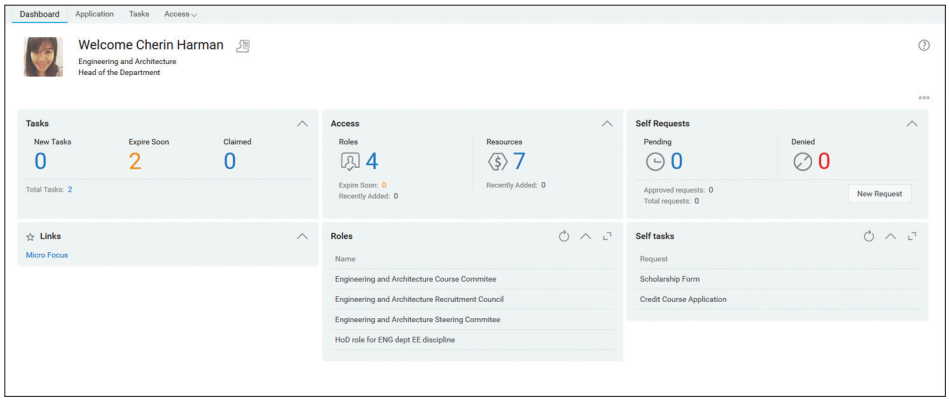
Önkiszolgáló jelszókezelés: A helpdesk számára a felhasználóknak az új jelszó beállításához nyújtott segítség jelenti az egyik legnagyobb költségtételt. Az önkiszolgáló jelszóbeállítás (self-service password reset, SSPR) gyakorlatilag kiiktatja a helpdesk bevonását. Lehetővé teszi, hogy a felhasználók önállóan kezeljék jelszavaikat, és új jelszót állítsanak be, sőt akár újraaktiválják a lezárt fiókokat anélkül, hogy ezzel gyengülne a vállalat biztonsága.

Az önkiszolgáló jelszóbeállításnál a felhasználóknak különböző módszerekkel igazolniuk kell a személyazonosságukat, mielőtt lehetőséget kapnak az új jelszó biztonságos beállítására. Bármilyen módszert is választanak a személyazonosításhoz, az mindig meg fog felelni a szervezet számára szükséges biztonsági szintnek, és az új jelszavak is teljesíteni fogják a követelményeket az „as-you-type" jelszószabály érvényesítésével. Így nem áll fenn a kockázata annak, hogy valaki gyengébb, az előírt követelményeknek meg nem felelő jelszóval vált ki egy erősebbet. Az új jelszavak és a felszabadított fiókok azonnal működnek, így a felhasználók rögtön hozzáférnek rendszereikhez és alkalmazásaikhoz.

Felhasználói tevékenység monitorozása: Azzal, hogy tudjuk, ki fér hozzá mihez, és ezt kézben tartjuk, még nem látjuk a teljes képet. Ugyanilyen fontos – visszamenőleg és valós időben – ismerni azt, mihez kezdenek az emberek a hozzáférésükkel. Ha egy vállalat szándékán kívül megengedi a nem megfelelő, kártékony vagy rendellenes viselkedést, számolnia kell azzal, hogy komoly bírságokat vetnek ki rá, nem fogja tudni teljesíteni az auditok követelményeit, és hogy mindez súlyosan károsítja majd a szervezet adattárait és üzleti hírnevét. A Micro Focus Identity Tracking for Identity Manager az Identity Manager hatékony tájékoztatási és erőforráskiosztási képességeit egy olyan valós idejű korrelációs motorral integrálja, amely teljes képet ad arról, ki fér hozzá mihez, és mire használják az emberek a hozzáférésüket. Ez a felhasználói aktivitást figyelő és korrigáló megoldás az Identity Manager által támogatott összes rendszerben működik, és jelentősen mérsékli a vállalat számára káros, nem megfelelő, rosszindulatú, vagy nem rendeltetésszerű viselkedés előfordulását.

Hozzáféréstanúsítás: A hozzáférés rendszeres ellenőrzése megfelelési követelmény, amelynek teljesítése sok időt vesz igénybe. Az IT számára időpazarlás a hozzáférési jogosultságok összegyűjtése, az üzleti terület számára pedig túl sok munkát jelent ezeknek a jogosultságoknak a tanúsítása. Az Identity Governance megoldás az Identity Managerrel integrálva nagyrészt automatizálja ezt a folyamatot. Lehetővé teszi, hogy a szervezet ellenőrizze és igazolja a felhasználók alkalmazásokhoz és rendszerekhez való hozzáférését a vállalat egészében, ideértve az Identity Manager által kezelt és az azon kívüli elemeket is. Az Identity Governance támogatja a menedzselt és nem menedzselt alkalmazások ellenőrzését, a rendszeres és ad hoc ellenőrzéseket, a supervisori ellenőrzéseket, az alkalmazások és az engedélyek gazdáinak ellenőrzését, ésszerűsíti a kockázatalapú ellenőrzéseket, és automatikusan, illetve manuálisan végrehajtja az ellenőrzés alapján hozott döntéseket.

Megfelelési jelentések készítése: Az Identity Manager rendelkezik a hozzáférések megfelelésének igazolásához szükséges átfogó jelentéskészítési képességekkel. A jelentések nem csak abba nyújtanak betekintést, hogy a felhasználók jelenleg mely rendszereket érik el, de abba is, hogy mely rendszereket érhetnek el



2. ábra. Az Identity Manager testre szabható, üzleti szemléletű irányítópulton jeleníti meg a feladatokkal, a szerepkörökkel és a kérésekkel kapcsolatos információkat

„A központosított személyazonosságkezeléssel tökéletesen tudjuk prezentálni vállalatunkat. Az ügyfeleknek így többé nem kell több azonosítót és jelszót megjegyezniük a tőlünk igénybe vett különféle szolgáltatások eléréséhez."

KANON COZAD
alelnök és alkalmazásfejlesztési igazgató,
UMB Financial Corp.

Kapcsolatfelvétel:
www.microfocus.com

konkrét dátumokon vagy két időpont között. A jelentéskészítési keretrendszer lehetővé teszi, hogy a felhasználók egyéni jelentéseket állítsanak be konkrét igényeiknek megfelelően, és ezeket jövőbeni használatra elmentsék. A szabályalapú adatgyűjtési és -tárolási képességek erőteljesen támogatják a megfelelést, hogy a szervezet mindig készen álljon a következő auditra.

Összegzés

A díjnyertes Identity Manager komplett megoldást kínál annak szabályozására, ki fér hozzá mihez a nagyvállalatnál – a tűzfalon belül éppúgy, mint a felhőben. Lehetővé teszi, hogy Ön biztonságos és kényelmes hozzáférést nyújtson az üzleti felhasználóknak a kritikus információkhoz úgy, hogy közben a megfelelési követelményeket is teljesíti. Az Identity Manager a közös kritériumok (Common Criteria) szerinti EAL3+ szintű biztonsági tanúsítvánnyal rendelkezik. A világszerte ügyfelek ezrei által használt megoldással a Micro Focus a piacon egyedülálló módon jól skálázható alapot biztosít a személyazonosság-kezeléshez, hogy a szervezet kis költségráfordítással őrizhesse meg versenyképességét, agilitását és biztonságát. Integrált szemléletet biztosít a teljes vállalatra kiterjedő megoldások vagy a legégetőbb szükségletekre összpontosító, különálló személyazonosság- és hozzáférés-kezelési termékek bevezetéséhez. Termékeink és megoldásaink segítségével az Ön vállalata is maximális értéket nyerhet ki múltbeli, jelenlegi és jövőbeni IT-beruházásaiból.

További információért, kérjük keressen minket az alábbi elérhetőségek valamelyikén:

1138 Budapest, Váci út 140.
Tel: +36 (1) 489-4600
Fax: +36 (1) 489-4601
iroda@microfocus.com

www.microfocus.com