BALASYS

One Identity
Identity Manager

Szüntesse meg a vállalati identitás és hozzáférés kezelés kockázatait

ELŐNYÖK

Szabályozza felhasználói- és adat-hozzáféréseit on-premise, cloud, vagy hibrid erőforrásain az igényléstől a teljesítésig.

Csökkentse kockázatait azzal, hogy a felhasználói csak a szükséges hozzáférésekkel rendelkeznek.

Teljesítse az audit és compliance kötelezettségeket a hitelesítési és tanúsítási szabályokkal.

Helyezze a hozzáférési kérések jóváhagyását a megfelelő döntéshozók kezébe.

Csökkentse a kockázatot.

Szabályozza a hozzáféréseit.

Szabályozza felhasználóit.

Biztosítsa az adatok védelmét.

Alapozza üzleti igényeire a hozzáférés és jogosultság menedzsment (IAM) rendszerét.

ÁTTEKINTÉS

A hagyományos jogosultság és hozzáférés menedzsment (IAM) rendszerek kiépítése költséges, megvalósításuk és fenntartásuk pedig időigényes.

A jogosultsági életciklus menedzsmentjével kapcsolatos valamennyi feladatot az informatikai részleg végzi, ami a legtöbb szervezetet megterheli.

Az informatikai szervezetek gyakran több elkülönített, szűk területre összpontosító eszközt és biztonsági szabályzatot alkalmaznak az IAM projektek megvalósítása során, és manuális érvényesítési folyamatokat működtetnek, annak érdekében, hogy a különböző részlegek egyedi hozzáférés menedzsment igényeit ki tudják elégíteni. Ez sebezhetővé teszi az IT környezetet, növeli a kockázatot, és megnehezíti az SLA-k teljesítését.

Ezzel szemben a termelékenység növelhető, ha azokhoz az adatokhoz és alkalmazásokhoz ad csak hozzáférést a felhasználóknak a szervezet, amelyekre valóban szükségük van a feladatuk elvégzéséhez.

Mindemellett pedig csökkentheti a kockázatot, biztosíthatja az adatok védelmét, teljesítheti az üzemidőre vonatkozó követelményeket, és a megfelelőségi elvárásokat, ha csupán a legszükségesebb jogosultságok állnak a felhasználók rendelkezésére. A megfelelő jogosultság és hozzáférés menedzsment eszközök kiválasztása lehetővé teszi, hogy ne az IT képességek, hanem az üzleti igények határozzák meg az IAM folyamatok működését. Az Identity Manager rendszerrel egyesítheti a különböző biztonsági szabályokat és teljesítheti a jogosultság szabályozási igényeket.

A moduláris és skálázható IAM megoldással növelheti az üzleti agilitását.

1. Ábra: A Governance Heatmap a szabályzatsértések gyors részletezéseit teszi lehetővé

FUNKCIÓK

Kockázatcsökkentő

Megalapozottabb biztonsági döntéseket hozhat az egyesített, több forrásból származó biztonsági információkkal és szabályzatokkal.

Self-service hozzáférés portál

Lehetővé teheti a vállalat számára, hogy időt takarítson meg. Csökkentheti IT részlegének terheltségét, a vállalati igényekre szabható online self-service portál segítségével. A teljes jogosultságkezelési életciklus előre definiált munkafolyamataival a felhasználóknak lehetősége van hozzáféréseket igényelni például fizikai eszközökhöz, levelezési listákhoz, és csoportokhoz is.

Csatlakozás a felhőhöz

Az on-premise alkalmazásokon túl a hibrid és a SaaS alkalmazásokra is kiterjesztheti a hozzáférés menedzsment folyamatait a One Identity Manager (7.1-es vagy újabb verziója) segítségével.

Governance 360

Részletes, valós idejű szabályozási jelentéseket biztosíthat az auditorok számára arról, hogy milyen erőforrások vannak a környezetében, azokhoz ki férhet hozzá, illetve mikor és miért kapták vagy utasították el a hozzáférést.

Privileged Access Governance

Egységes szabályozási megközelítés minden alkalmazottra nézve, a szerepkörüktől és a hozzáférési szintjüktől függetlenül. A felhasználók egységes felületen kérelmezhetik, oszthatják ki és igazolhatják a privilegizált és az általános felhasználói hozzáféréseket.

Kétfaktoros hitelesítés

Az Identity Managerrel lehetővé teheti a kétfaktoros hitelesítést a vállalati alkalmazások integrált üzembe helyezésével és a One Identity Starling Two-Factor Authentication (2FA) szolgáltatással integrálva.

Access Review dashboard

Igény szerinti vagy rutinszerű hitelesítést írhat elő, és egy átlátható, tömör irányítópult-nézetben jelenítheti meg a csoport vagy a terjesztési lista állapotát; ez azt is lehetővé teszi, hogy részletes jelentéseket készítsen feltárás céljából, illetve hogy biztosítsa a megfelelőséget.

Adatgazdálkodás

Szabályozhatja, és könnyen átláthatóvá teheti adatait.

Jelszó visszaállítás

Visszaállíthatja a felhasználói fiókok jelszavait, és olyan felhasználói szabálybeállításokat adhat meg, melyek tükrözik a szervezet jelszavakra vonatkozó szabályait és követelményeit. Több jelszószabályzatot is engedélyezhet a felhasználói szerepköröktől függően.

Hozzáférés megfelelően

Növelheti a biztonságot, ha csak azt a hozzáférést biztosítja az alkalmazottak, az alvállalkozók, a partnerek, és az ügyfelek számára, amelyre mindenképpen szükségük van – se többet, se kevesebbet.

Hozzáférés megfelelően

Növelheti a biztonságot, ha csak azt a hozzáférést biztosítja az alkalmazottak, az alvállalkozók, a partnerek, és az ügyfelek számára, amelyre mindenképpen szükségük van – se többet, se kevesebbet.

Megfelelő jogosultság kiosztás

Kiküszöbölheti a manuális hibákat, azáltal, hogy automatizálja az alkalmazás jogosultság kiosztását bármely rendszer esetében, on-premise vagy cloud. A jogosultság kiosztást olyan vállalati alkalmazásokra is kiterjesztheti, mint például az Exchange Online, a SharePoint és az Oracle E-Business Suite.

Megfelelőség, most

Külső előírások? Nem probléma. Belső szabályzatok? Nem probléma. Elérheti azt a teljes átláthatóságot, amely lehetővé teszi az összes előírásnak való megfelelést.

Vertikális és horizontális skálázás

A korábbi beruházásokat és infrastruktúrát felhasználva fejlesztheti tovább IAM rendszereit. Migrálja a meglévő legacy platformokat egy moduláris és integrált megoldás beépítésével a „hagyományos" IAM keretrendszerbe. Lehetővé téve ezzel a konzisztens IAM stratégia megvalósítását.

ONE IDENTITY™

A One Identity-ről

A One Identity a Quest Software egyik üzletága, amely segíti a vállalatok jogosultság és hozzáférés kezelését (Identity and Access Management, IAM). Jogosultság szabályozást (Identity Governance), hozzáférés kezelést, privilegizált felhasználó kezelést és jogosultságot, mint szolgáltatást (Identity as a Service) tartalmazó egyedi termékportfóliója támogatja a szervezeteket üzleti lehetőségeik kihasználásában, mindezt biztonsági béklyók nélkül, mégis védelmet nyújtva a fenyegetések ellen.