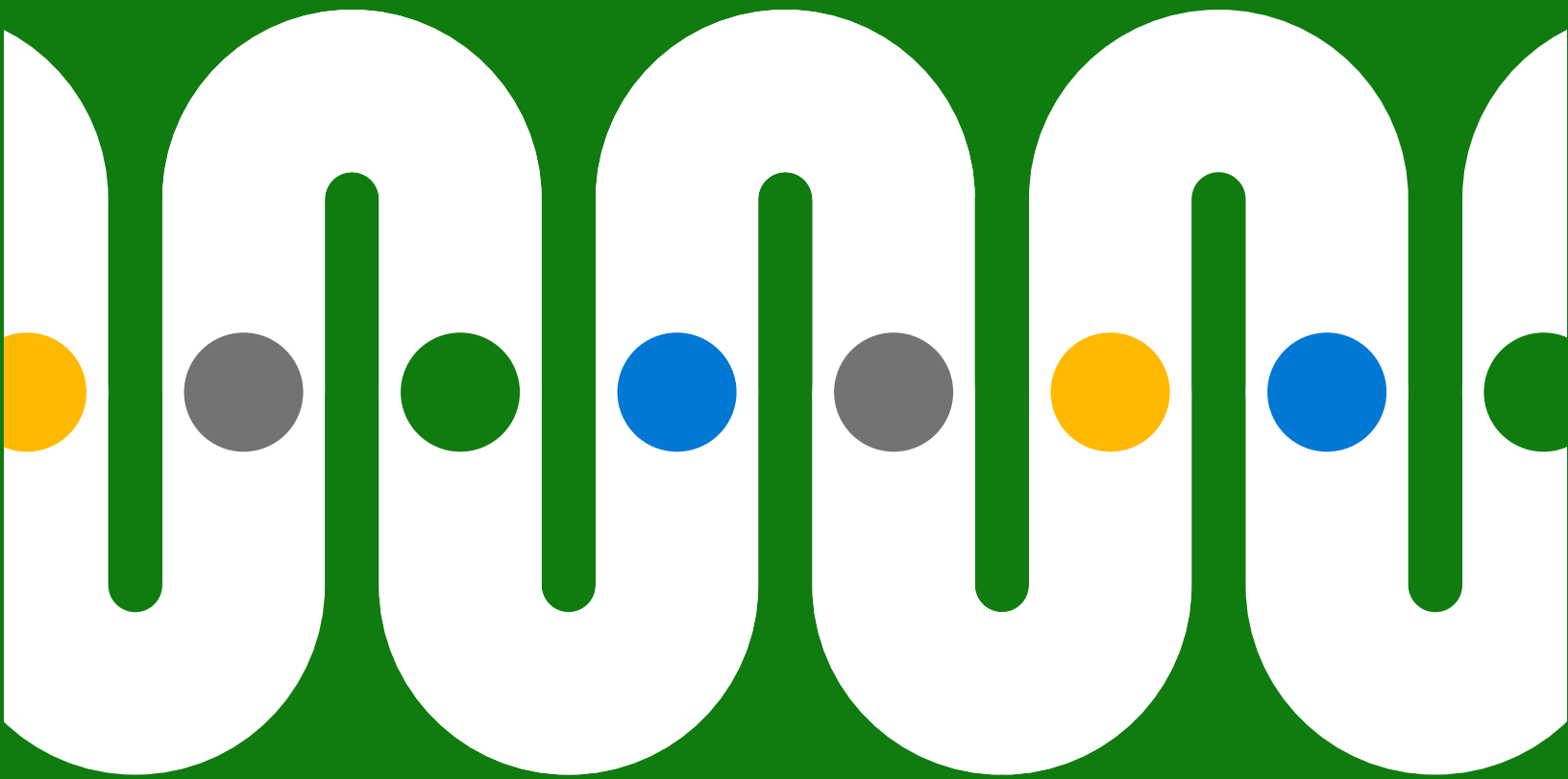
Microsoft Security

Három lépés az átfogó adatvédelem felé



Tartalom

Egy megfelelőségi döntéshozók körében végzett felmérés szerint 95%-uk aggódik az adatvédelmi kihívások miatt.[2]

Bevezetés

A vállalatok digitális lábnyoma jelentősen megnövekedett a hibrid munka következtében, és már messze túlterjed a hagyományos irodákon.

Ez az adatok széttöredezettségéhez és gyakoribb kiszivárgásához vezetett – a helyzetet pedig tovább bonyolítja az alkalmazások, eszközök és helyszínek számának gyors növekedése. Emellett számos dolgozó vált munkakört, mert elégedetlen a jelenlegiben, vagy nagyobb rugalmasságra vágyik, ami csak fokozza a kihívásokat, és új fehér foltokat hoz létre az egyre növekvő adatvagyonokban.[1]

Mindezek a tényezők az információvédelem újragondolására késztetik az informatikai és IT-biztonsági vezetőket. Egy több mint 500 amerikai megfelelőségi döntéshozó körében végzett felmérés szerint majdnem mindegyikük (95%) aggódik az adatvédelmi kihívások miatt.[2]

[1] „How Microsoft can help reduce insider risk during the Great Reshuffle, Alym Rayani", Microsoft Security. 2022. február 28.

[2] „A Vital Findings által a Microsoft megbízásából 2021 szeptemberében 512 amerikai megfelelőségi döntéshozó körében végzett felmérés".

Az IT- és a biztonsági csapatok folyamatosan keresik a hatékonyabb módszereket az adatok teljes életciklusának menedzselésére a többfelhős, a hibrid felhős és a helyi környezetekben. Ez az átfogó megközelítés három kulcsfontosságú lépést tartalmaz:

1. lépés: Az adatok azonosítása

Az adatok tárolási helyének, típusainak, valamint használati és megosztási módjainak azonosítása

2. lépés: Az adatok besorolása

Az adatok besorolása és címkézése annak eldöntése érdekében, hogy mely szabályozások és kockázatcsökkentő intézkedések vonatkoznak rájuk

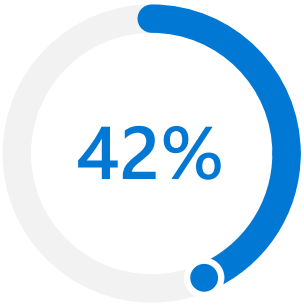
3. lépés: Az adatvesztés megelőzése

Egyensúly megteremtése a kockázatcsökkentés és a munkatársak számára biztosított rugalmasság között, intelligens észlelés és felügyelet segítségével

Mi a megközelítés célja? A hézagok áthidalása és a kockázat minimalizálása a hatékonyság feláldozása nélkül.

1. lépés

Az adatok azonosítása



Arra a kérdésre, hogy mennyi adatuk „sötét”, a vállalatok 42%-a válaszolta, hogy legalább a fele.[3]

Ezek a „rejtett” adatok számos formát ölthetnek – az e-mail-mellékletektől kezdve az ügyféllátogatások jegyzetein át a gépi naplókig és a videofelvételekig.

Ha nem tudja azonosítani az adatokat – azt, hogy hol találhatók, milyen típusúak, illetve hogyan használják és kivel osztják meg őket –, akkor a megfelelő szabályozások és védelem alkalmazása lehetetlenné válik.

A modern vállalatok folyamatosan, hatalmas mennyiségben állítanak elő adatokat. Nem csupán dokumentumokról, e-mailekről és üzenetekről van szó, hanem biztonsági felvételekről, földrajzi helyadatokról és sok minden másról – mindezt fokozza az alkalmazások, az eszközök és a tárolási helyek számának folyamatos növekedése a helyi környezetben és a felhőben egyaránt.

Az összes ilyen adat azonosítása nehézkes lehet, és a vállalatok 42 százaléka szerint az adataik legalább fele „sötét”[3] – azaz összegyűjtött, de ismeretlen vagy üzleti célokra nem használt információkból áll. Előfordul, hogy az adatok akkor válnak „sötétté”, amikor az őket létrehozó dolgozó projektet vagy munkakört vált; gyakran egyszerűen nincsenek olyan rendszerek, amelyek az adatokat a létrehozásuk vagy módosításuk pillanatában azonosítanák.

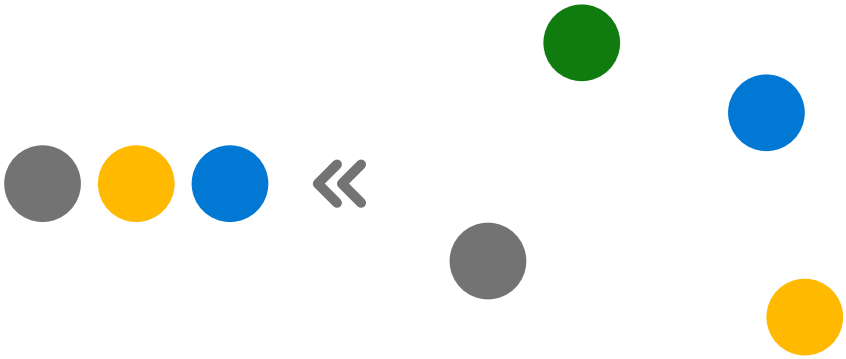
[3] „2022 State of Data Governance and Empowerment Report”, Enterprise Strategy Group. 2022. július.

Szeretne teljes körű felderítési munka-folyamatot kialakítani egy egységes platformon?

Tudjon meg többet a Microsoft Purview adatfelderítési képességeiről a **Microsoft.com** oldalon!

A jövőben ez a kihívás csak egyre súlyosabb lesz. A létrehozott, rögzített, replikált és fogyasztott új adatok mennyisége 2026-ra várhatóan több mint kétszeresére nő, a nagyvállalati adatok pedig több mint kétszer olyan gyorsan gyarapodnak, mint a fogyasztói adatok.[4]

A mesterséges intelligencia (AI) és a gépi tanulás (ML) segíthet a bizalmas adatok – például e-mail-címek, egészségügyi adatok, hitelkártyaszámok vagy szellemi tulajdon – felismerése és automatikus besorolása révén. Az AI és az ML továbbá javíthatja a besorolás pontosságát, illetve visszamenőlegesen is felülvizsgálhatja az adatokat. Az azonosítási folyamatok a cég teljes adatvagyonára kiterjedhetnek, és bárhol, bármilyen felhőben tárolt tartalmak megőrzésére, összegyűjtésére, elemzésére, ellenőrzésére és exportálására alkalmasak.



[4] „Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth", John Rydning, IDC. 2022. május.

2. lépés

Az adatok besorolása

A besorolásoknak és a szabályozásoknak egyaránt követniük kell az adatok mozgását.

Ha például egy munkatárs hitelkártyaszámokat másol át egy Microsoft Word-dokumentumból egy Excel-táblázatba, akkor a releváns besorolásnak és szabályoknak automatikusan érvényesnek kell lenniük mindkét dokumentumra.

Szeretné jobban kezelni és védeni a környezetében lévő bizalmas adatokat?

Tudjon meg többet a Microsoft Purview adatklasszifikációs és -védelmi képességeiről a **Microsoft.com** oldalon!

A pontos adatklasszifikáció segít a megfelelő szabályozások és kockázatcsökkentő intézkedések meghatározásában a különböző típusú adatokkal való véletlen vagy szándékos visszaélés, illetve az illetéktelen hozzáférés megakadályozása érdekében. A titkosítás és a vízjelek további védelmet nyújtanak az adatoknak – a tárolás, a továbbítás és a használat során egyaránt.

Azonban a klasszifikációnak és a szabályozásoknak követniük kell az adatok vállalaton belüli mozgását. A címkézési és védelmi szabályok nem korlátozódhatnak adott dokumentumokra, hanem minden digitális erőforrásra ki kell terjedniük – legyen szó helyi vagy felhőalapú tárhelyekről, szoftverszolgáltatásokról (SaaS) vagy az operációs rendszer saját alkalmazásairól.

A hagyományos adatklasszifikációs módszerek jelentős manuális munkát igényelnek, aminek során nagy a kockázata a hibáknak vagy a kritikus adatok véletlen figyelmen kívül hagyásának. A beépített és betanítható osztályozók segíthetnek a folyamat automatizálásában, egy integrált megoldás pedig lehetővé teszi, hogy a rendszergazdák központilag kezeljék a szabályzatokat az összes rendszerben.

3. lépés

Az adatvesztés megelőzése

A DLP-házirendekkel megelőzhető az előírásoknak meg nem felelő műveletek végrehajtása.

Ha például egy munkatárs megpróbál letölteni egy hitelkártyaszámokat tartalmazó táblázatot egy pendrive-ra vagy feltölteni egy felhőtárhelyre, a DLP-házirend „nem megfelelőként” azonosíthatja és megakadályozhatja ezt a tevékenységet.

Bizalmas információk intelligens észlelésére és felügyeletére lenne szüksége?

Tudjon meg többet az adatvesztés megelőzéséről a Microsoft Purview segítségével a **Microsoft.com** oldalon!

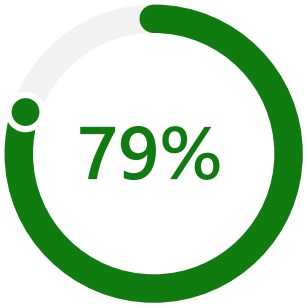
Az adatok azonosítása és besorolása után az adatveszteség-megelőzés (DLP) megoldásokkal átfogó védelmi szabályzatok alkalmazhatók, amelyek enyhítik a „sötét” adatokhoz vagy az adatszivárgáshoz hasonló veszélyeket azzal, hogy a jelenlegi és a korábbi munkatársak nem oszthatnak meg, nem tehetnek közzé és nem továbbíthatnak engedély nélkül bizalmas adatokat – sem szándékosan, sem véletlenül.

Az intelligens DLP-megoldások a kontextust figyelembe véve igyekeznek megtalálni az arany középutat a rugalmas használat és a kockázatos tevékenységek blokkolása között. Például az érintettek folytathatják, amit csinálnak, de emlékeztetőt kapnak a lehetséges kockázatokat és a vonatkozó szabályozásokat illetően. Ez segíthet a bizalmas adatok védelmében, miközben felkészíti a felhasználókat a kockázatok jobb megértésére.

A DLP-megoldások elősegítik a szellemi tulajdon és más kritikus fontosságú üzleti adatok védelmét, továbbá az olyan előírások betartását, mint az Európai Unió általános adatvédelmi rendelete (GDPR), az USA egészségügyi információk hordozhatóságáról és elszámoltathatóságról szóló törvénye (HIPAA), valamint a kaliforniai fogyasztóvédelmi törvény (CCPA).

A DLP átfogó alkalmazása következetesen, a vállalat minden szintjén gondoskodik a szabályozások betartatásáról, így az adatok teljes életciklusa alatt védelmet nyújt a „leggyengébb láncszemekkel” történő visszaélések ellen.

Ne utólag gondoskodjon az adatvédelemről. Használjon beépített megoldást!



Egy megfelelőségi döntéshozók körében végzett felmérés szerint 79%-uk több megfelelőségi és adatvédelmi terméket is vásárolt.

A többség legalább hármat vásárolt.[5]

Számos vállalat próbálkozik utólag gondoskodni az információvédelemről, különféle megoldások használatával az adatok életciklusának egyes szakaszaiban. Ez azonban arra kényszeríti a biztonsági, adatkezelési, megfelelőségi és jogi csapatokat, hogy egy gyakran nem elég hatékony, erőforrás-pazarló vegyes rendszert tartsanak fenn.

A „beépített" megközelítés képes megszüntetni a hiányosságokat és egységesen kezelni az adatok azonosítását, az adatklasszifikációt és a DLP-t. Integrált megoldással könnyebb a szabályozások központi kezelése és érvényesítése. Egy ilyen megoldás csökkenti a felhasználók képzési idejét is, akik a szabályokkal kapcsolatos értesítéseket a megszokott módon, az éppen használt alkalmazásokon belül kapják meg.

[5] „200 USA-beli megfelelőségi döntéshozó körében (n=100: 599–999 fős cégek, n=100: legalább 1000 fős cégek) a Microsoft megbízásából, az MDC Research együttműködésével 2022 februárjában végzett felmérés."

Beépített, integrált megoldás: Microsoft Purview

A Microsoft Purview segít abban, hogy cége megfelelhessen a mai decentralizált, adatgazdag munkahelyek kihívásainak, és olyan átfogó megoldáscsomagot kínál, amellyel teljes adatvagyonát kézben tarthatja, megvédheti és menedzselheti.

Lépjen túl az irányításon!

[További információ a Microsoft Purview adatvédelmi megoldásairól >]

Az adatvédelem egy adott területe érdekli? További információ arról, hogyan segíthet a Microsoft Purview a következőkben:

Adatfelderítés >

Adatklasszifikáció és adatvédelem >

Adatveszteség megelőzése >

Microsoft Security