



Üzleti terv a teljes felügyelet bevezetéséhez

Gyakorlati útmutató a cég teljes felügyeleti
keretrendszerének megvalósításához



Tartalom

- 03 [Bevezetés](#)
- 04 [A biztonságos digitális átalakuláshoz teljes felügyeletre van szükség](#)
- 05 [A teljes felügyelet gyakorlati megközelítése](#)
- 06 [A teljes felügyelet bevezetésének három szakasza](#)
- 07 [A teljes felügyelet bevezetésének megtervezése](#)
- 10 [A teljes felügyelet megvalósítása a cégnél](#)
- 11 [A haladás mérése](#)
- 15 [A teljes felügyelet mint a túlélés záloga](#)
- 16 [Következő lépések](#)

A digitális átalakulás az új környezetet is formálja

A különböző cégek azért vállalják a digitális átalakulást, hogy kezelni tudják az üzleti környezet folyamatos változásait:

- A változó üzleti modelleket és partneri kapcsolatokat
- A technológiai trendeket
- A jogszabályi, a geopolitikai és a kulturális tényezőket

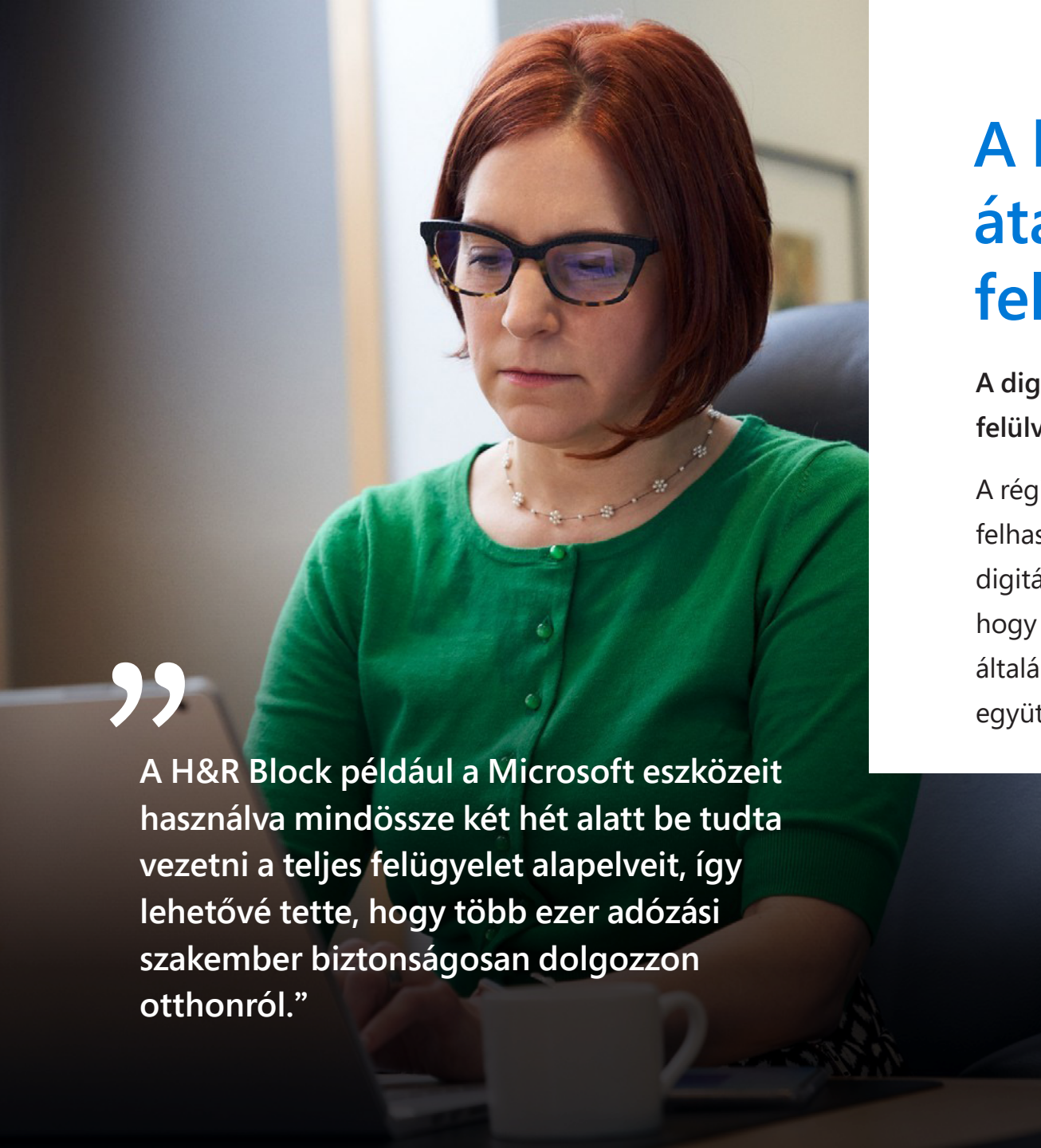
A COVID-19 következtében elterjedt távmunka felgyorsította az átalakulást, és a biztonságot a költségközpontúság helyett inkább a fejlődés stratégiai elemévé tette.

”

A COVID világossá tette mindannyiunk számára, hogy a jövőben is lesznek problémák, és hogy nagyon gyorsan kell reagálnunk az új helyzetekre.

A teljes felügyeleti modell megvalósításakor egyre kevésbé számít, hogy egy garázsból, a felhőből vagy egy adatközpontból végezzük-e a munkát.”

Identitás- és hozzáférés-kezelési megoldások vezetője, pénzügyi szolgáltató cég



A biztonságos digitális átalakuláshoz teljes felügyeletre van szükség

A digitális átalakuláshoz szükség van a hagyományos biztonsági modellek felülvizsgálatára.

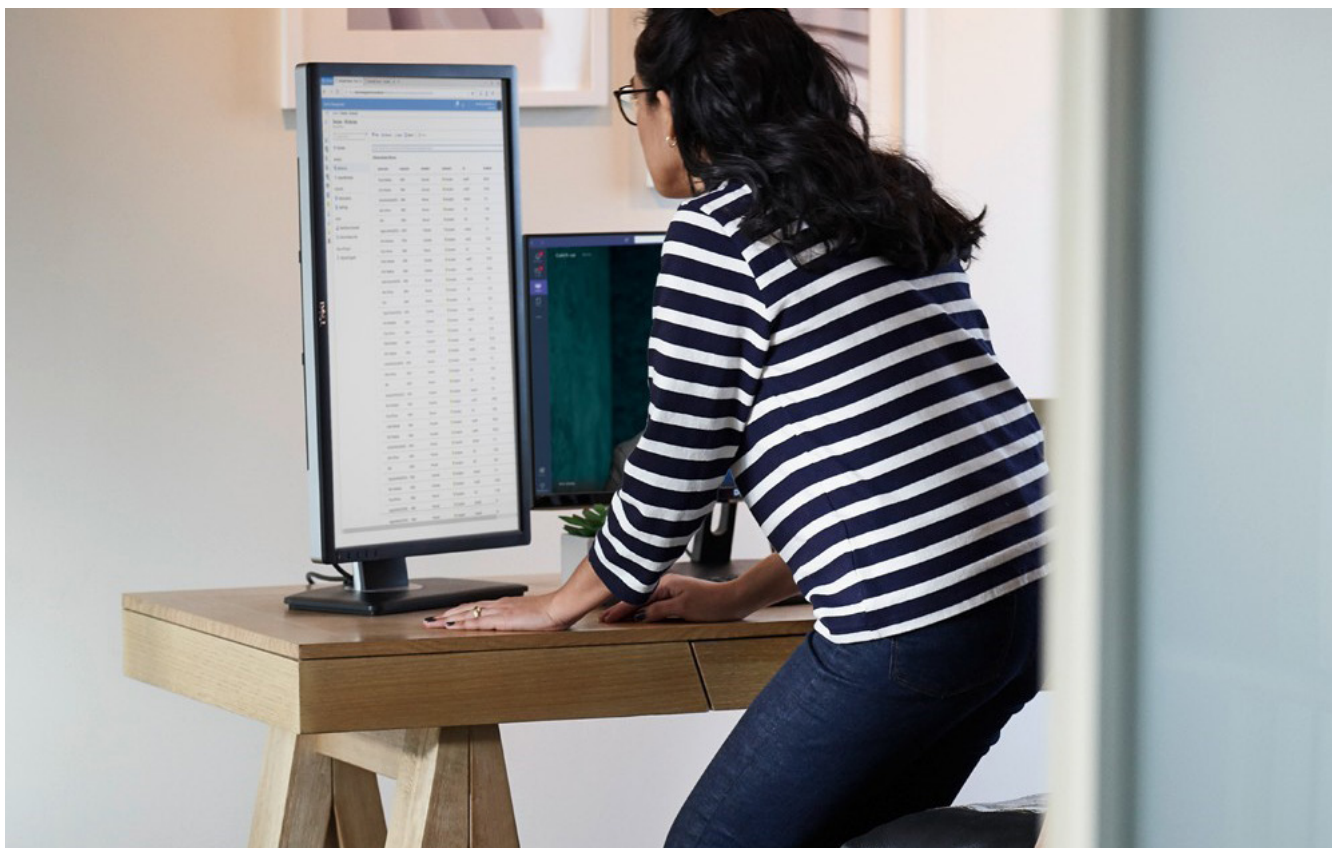
A régi biztonsági módszerek nem biztosítják azt a rugalmasságot, felhasználói élményt és védelmet, amelyre szükség van a gyorsan változó digitális ökoszisztémához. Sok cég azért vezeti be a teljes felügyeletet, hogy ezeket a problémákat kezelni tudja, és megfeleljen annak a ma már általános elvárásnak, hogy a munkatársak bárhol, bármikor és bárkivel együttműködve dolgozhassanak.

”

A H&R Block például a Microsoft eszközeit használva mindössze két hét alatt be tudta vezetni a teljes felügyelet alapelveit, így lehetővé tette, hogy több ezer adózási szakember biztonságosan dolgozzon otthonról.”

Ez a tudás és a bevett gyakorlatok egyrészt az ügyfelekkel folytatott beszélgetésekből származnak, másrészt azokra a saját tapasztalatainkra épülnek, melyeket a teljes felügyelet bevezetése során szereztünk a Microsoftnál.

A teljes felügyelet bevezetésének gyakorlati megközelítése: nagy tervek, kis lépések, gyors fejlődés



Dolgozzon ki egy többéves üzleti tervet:

A gyors eredmények rangsorolásához
és fokozatos fejlődéshez minden
kezdeményezés esetében.

**A meglévő technológiák
felhasználásához,**
melyek már üzemelnek vagy
licenccel rendelkeznek.

**Koherens kezdeményezések
strukturálásához**
egyértelmű eredményekkel,
előnyökkel és tulajdonjoggal.

A teljes felügyelet bevezetése

Létrehoztunk egy gyakorlatban használható ajánlott eljárási keretrendszert, amely végigvezeti Önt a teljes felügyelet bevezetésének egész folyamatán. Minden fázishoz útmutatást, ajánlott eljárásokat, forrásokat és eszközöket kap, amelyek segítenek a megvalósításban.



01 Tervezés

Dolgozzon ki egy üzleti esetet olyan eredményekre fókuszálva, amelyek pontosan megfelelnek a cég kockázati és stratégiai céljainak.

02 Megvalósítás

Alakítson ki hosszú távú stratégiát a teljes felügyelet bevezetéséhez, a kezdeti intézkedéseket pedig az üzleti igények szerint rangsorolja.

03 Mérés

Kövesse nyomon a teljes felügyelet bevezetésének sikerességét, hogy megbizonyosodhasson arról, hogy a teljes felügyelet mérhető fejlődést eredményez.

A teljes felügyelet megtervezése: a jó kialakítás

Javasolt rangsorolás:

→ **Hosszú távú célok meghatározása** – A teljes felügyelet sokrétű, és több évre tervezhető. A célok, az eredmények és az architektúrák **egyértelmű** meghatározásával a cégek nagyobb sikert érhetnek el, mintha csupán reaktív megközelítést használnának.

Megjegyzés: Az előnyök és a megvalósítás módja gyakran nagy mértékben különbözik attól függően, hogy milyen szerepkörökről vagy feladatokról van szó.

→ **A vezetőség támogatásának megnyerése** – A teljes felügyelet sikeres megvalósításakor az üzleti eredmények vannak a középpontban, így a vezetők is támogatják az ambiciózus célokat, a költségvetés megoszlását és a belső átalakításokat.

→ **A végfelhasználók támogatása** – A teljes felügyelet lehetővé teszi a technológiai csapatoknak, hogy közvetlenül tartsanak kapcsolatot a végfelhasználókkal, és hogy a biztonsággal is elősegíthessék a felhasználói élményt és a hatékonyságot.



Hosszú távú célok meghatározása és a vezetőség megnyerése

A vezetőség támogatásának megszerzéséhez első lépéseként meg kell határozni és követni kell az üzleti prioritásokat, majd ki kell tűzni egy olyan célt, amelyben kiemelt szerepe van az üzleti eredményeknek.

Noha ezeket a célkitűzéseket mindig az üzleti prioritásokhoz és a kulturális környezethez kell igazítani, mégis felvázolható több olyan szempont, amely a legtöbb cégnél megjelenik:

- **Üzleti rugalmasság**, hogy gyorsan ki lehessen aknázni az új lehetőségeket a kockázatkezelés, a távmunka lehetővé tétele és a felhőbe való migrálás során.
- **Összetettség kezelése**, ami az üzleti partnerségek, a verseny és a dinamikus technikai környezet folyamatos változásaiból ered.
- **Mérhetőség**, mellyel biztosítható a számonkérhetőség az üzleti eredmények és a kockázatok terén.

”

A teljes felügyelet kialakításánál nálunk az egyik legfontosabb szempont a felülről lefelé irányuló támogatás. A vezérigazgatónk tisztában van vele, milyen veszélyekkel jár a teljes felügyelet hiánya, és megköveteli tőlünk ennek kialakítását.”

Identitás- és hozzáférés-kezelési megoldások vezetője, pénzügyi szolgáltatások



Stabil üzleti eset kidolgozása a teljes felügyelethez

A stabil üzleti eset segít abban, hogy elnyerjük a felső vezetés támogatását, és hogy elősegítsük az összes üzleti tevékenység összehangolását. Noha a teljes felügyeleti modellnek számos előnye van, a cégek általában az alábbi négy üzleti esetet tekintik olyannak, amely a sikereket növeli:

- Annak támogatása, hogy a munka bárhol és bármikor elvégezhető legyen.
- A felhőbe való biztonságos és gyors migrálás lehetővé tétele.
- Költségmegtakarítás a biztonsági ökoszisztéma egyszerűsítésével.



Koncentráljon a megjelenő üzleti eredményekre:

- **A kockázatok proaktív elkerülése** és kezelése.
- **Kockázatkezelés olyan partnereknél**, akik gyenge biztonsági programokkal rendelkeznek.
- **Rugalmasság a biztonság és a megfelelés terén** a szerepkörökben és a cégekben megjelenő gyors változások kezelése érdekében.

A teljes felügyelet megvalósítása: a jó kialakítás

A programot könnyen átlátható és egységes kezdeményezésekre kell bontani. A Microsoft tapasztalata szerint a műszaki stratégiák és architektúrák természetes módon rendezhetők az alábbi biztonsági kezdeményezések köré:

- A munkavégzés biztonsága
- Modern biztonsági műveletek
- Az üzemeltetési technológia (OT) és az eszközök internetes hálózata (IoT), *ha vonatkozik a szervezetre*
- Adatközpont, szolgáltatások és API

Ezek a Microsoft saját tapasztalatain és az ügyfelek által végzett sikeres megvalósításokon alapulnak.



A kezdeményezések rangsorolása és megtervezése:

- **Minden kezdeményezést az üzleti célokhoz kell igazítani,** és értékelni kell az üzletre gyakorolt pozitív hatást, a nehézségeket és a kihívásokat.
- **Rövid távú terv kialakítása.** Induljon gyorsan mérhető eredményekkel, és nyerje el a felső vezetés támogatását.
- **Hosszú távú ütemterv kidolgozása.**



A haladás mérése – a jó kialakítás

Azonosítsa a szervezetnél a fontosabb mérföldköveket és a teljesítménycélokat, mérje fel őket, és készítsen jelentést a sikerekről és a tanulságokról.

- **Az üzlet támogatása** – mérje fel a felhasználói élmény problémáit, és hogy mennyi ideig tart jóváhagyást szerezni a belső biztonsági kezdeményezésekhez.
- **A biztonság hatékonysága** – határozza meg, hogy mennyivel csökkent a biztonsági incidensek száma vagy hatása azt követően, hogy a szervezet bevezette a teljes felügyeleti stratégiát.
- **A biztonság egyszerűsége** – csökkentse az integrálandó beszállítók számát, és csökkentse a manuális feladatok (például a jelszóváltoztatás miatti ügyfélszolgálati kérések) költségét.



Az üzleti támogatás javulásának mérése

A teljes felügyeletnek az is célja, hogy egyszerűbbé tegye a felhasználói és a fejlesztői élményeket:

- A felhasználói munkafolyamatot megszakító biztonsági műveletek száma (például a többletellenőrző hitelesítésre vonatkozó felszólítások száma naponta).
- Az üzembe helyezési mérföldkövek (például azoknak az alkalmazottaknak a százalékos aránya, akik egyszeri bejelentkezéssel férnek hozzá az alkalmazásokhoz).
- Láthatósági mérföldkövek (például az alkalmazáshasználat csökkenése a nem megfelelő bejelentkezési folyamat miatt).
- A felügyelt eszközök átlagos rendszerindítási ideje másodpercben.
- Az alkalmazások biztonsági értékelésének átlagos napi száma.

Fontos figyelni a végfelhasználókra, felmérni a felhasználói hozzáférések egyszerűségét, a jelszómódosítási folyamatot stb.

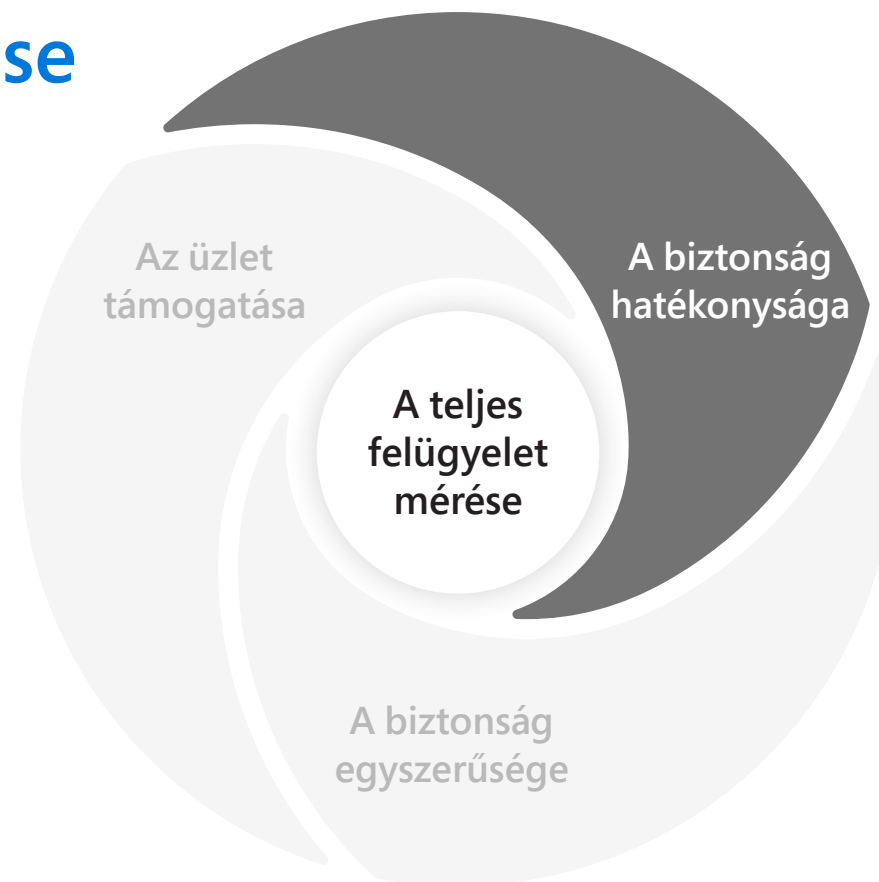


A biztonság hatékonyságának mérése

Mérje fel a biztonsági állapotot és a biztonsági incidensek hatását:

- Biztonsági incidensek száma (súlyosság szerint).
- Az üzembe helyezési mérföldkövek (például azoknak az alkalmazottaknak a százalékos aránya, akik aktívan használják az MFA-t).
- Láthatósági mérföldkövek (például a felügyelt eszközök és alkalmazások százalékos aránya).
- Biztonsági állapot – kövesse nyomon a fejlődést a [Microsoft Biztonsági pontszámával](#).

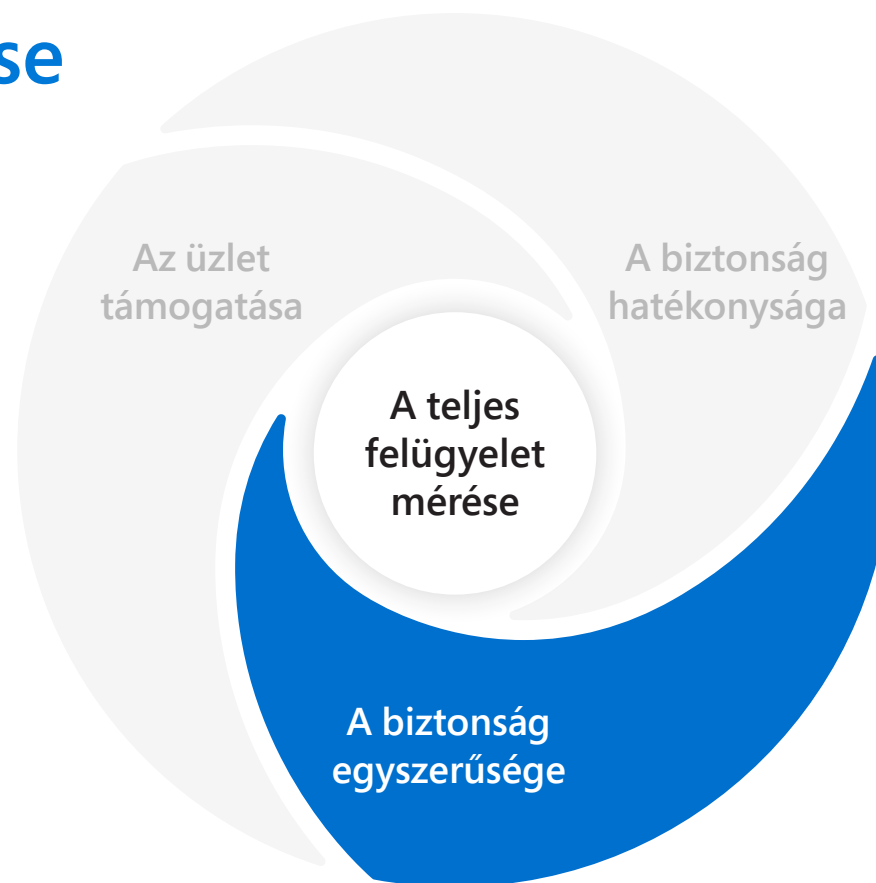
Teljes rálátás: Amint a teljes felügyeletnek köszönhetően egyre jobb láthatóságot ér el, olyan incidenseket is feltárhat, amelyek korábban nem kerültek felszínre.



A biztonság egyszerűségének mérése

A teljes felügyelet gyakran segít abban, hogy egyszerűsítsük a biztonság eléréséhez szükséges követelményeket.

- A hasonló vagy azonos funkciókat teljesítő, de különböző biztonsági eszközök száma.
- Az egyéni integrációt kívánó biztonsági eszközök száma.
- Annak az időnek a százalékos aránya, amelyet az IT-ügyfélszolgálat a kevésbé értékes tevékenységekkel, például a jelszómódosításokkal töltött.
- Az ismétlődő munkafolyamatok manuális lépéseinek száma (például gyakori riasztások vagy incidensek kivizsgálása, a felhasználók manuális kiépítése, a megfelelőségi jelentések készítése).
- A biztonsági csapatok vizsgálatainál a vakriasztások százalékos aránya.
- Az eszközkarbantartással töltött idő aránya a tényleges incidensekre adott válaszok függvényében.



A teljes felügyelet kulcsfontosságú tényező a digitális átalakulásban

Az induláshoz nem szükséges felforgatni és kicserélni a technológiát.

A teljes felügyeletbe fektetett erőforrásokat először a jelenlegi üzleti igényekhez kell igazítani, és a gyors eredményekre kell összpontosítani. Minden kisebb eredmény hozzájárul a kockázatok csökkentéséhez és a digitális ökoszisztéma biztonsági állapotának javításához.

Soha nem késő elkezdni, és bármilyen léptékben elindítható.



”

Mióta a Microsoft 365 technológiáival bevezettük a teljes felügyeletet, az alkalmazottaink bárhol a világon végezhetik a munkájukat az alapvető biztonsági igények szoros ellenőrzésének fenntartása mellett.”

□ Igor Tsyganskiy, technológiai igazgató,
Bridgewater Associates

Következő lépések

Köszönjük, hogy elolvasta a teljes felügyelethez ajánlott eljárásokat bemutató útmutatónkat. Ha még nem tette meg, olvassa el a [Microsoft teljes felügyeleti modelljéről írt tanulmányt](#) (ide kattintva le is töltheti), amelyben részletesen bemutatjuk a teljes felügyelet főbb elveit és azt a kész modellünket, amely az általános követelményeket hat alapvető összetevőre bontva ismerteti.

A [Microsoft Teljes felügyelet](#) megoldásának külső webhelyén további hasznos információkat, technikai útmutatókat és egyéb forrásokat is talál.

