E-KÖNYV

Miért alkalmazzon Zero Trust stratégiát?

Proaktív biztonság a Zero Trust segítségével

NOVENTIQ
Global expertise, local outcomes

Microsoft
Solutions Partner

NOVENTIQ
Global expertise, local outcomes

Kiknek szól ez a kiadvány?

Informatikai és üzleti vezetőknek, akik a Zero Trust keretrendszer segítségével szeretnének gondoskodni az IT-környezet védelméről. Az útmutató átfogóan ismerteti a Microsoft Zero Trust keretrendszerét, valamint a vállalati biztonsági stratégia két fő pillére, az identitások és a végpontok védelme terén szükséges konkrét lépéseket.

Miért alkalmazzon Zero Trust stratégiát?

Az adatok és az eszközök növekvő mennyisége, a hibrid munka terjedése és az egyre kifinomultabb támadások csökkentik a peremhálózati védelemre épülő IT-biztonság hatékonyságát. Az informatikusoknak rengeteg különböző technológiát kell kezelniük. A cégek általában vegyesen használnak felhőalapú és helyi infrastruktúrát, platformokat és szoftvereket. Több felhőszolgáltatójuk és sokféle felhős rendszerük lehet. A munkatársak saját eszközeiken is dolgozhatnak, és könnyen hozzáférhetnek különböző felhőalkalmazásokhoz és -szolgáltatásokhoz. Az adatok minden eddiginél több helyen érhetők el, ami értékesebbé, de sérülékenyebbé is teszi őket.

A fentiekre válaszul számos vállalat vezet be Zero Trust típusú biztonsági keretrendszert.

A Zero Trust proaktív, integrált biztonsági megközelítés, amely a digitális erőforrások valamennyi rétegére kiterjed. Explicit módon és folyamatosan ellenőrzi az összes tranzakciót a legkisebb jogosultság elvének szem előtt tartásával, és gondoskodik a fenyegetések felderítéséről, fejlett technikákkal való észleléséről és valós idejű elhárításáról.

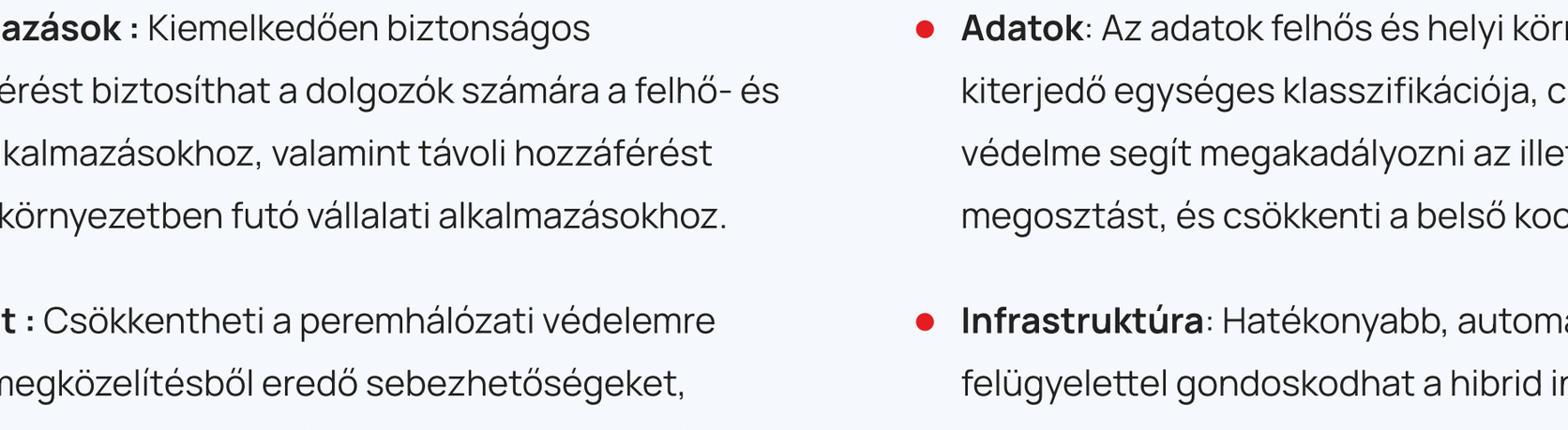
- **Explicit ellenőrzés:** Végezzen hitelesítést a hozzáférés engedélyezése előtt minden alkalommal, az összes rendelkezésre álló adatpont alapján – beleértve a felhasználó személyazonosságát és helyét, az eszköz állapotát, az elérni kívánt szolgáltatást, az adatok besorolását és az anomáliákat.
- **Támadás feltételezése:** Csökkentse minimálisra az incidensek lehetséges kiterjedését a hozzáférés szegmentálásával. Alkalmazzon teljes körű titkosítást és analitikát az átláthatóság, a fenyegetések észlelése és a védelem erősítése érdekében.
- **A legkisebb jogosultság elve**: Korlátozza a felhasználói hozzáférést a szükséges időintervallumra („just-in-time”) és a szükséges mértékre („just-enough-access”) kockázatalapú adaptív szabályok és adatvédelmi megoldások használatával az adatbiztonság és a hatékonyság fenntartása érdekében.

Mindhárom területen kritikus fontosságú a fenyegetésekkel szembeni modern védelem, amely lehetővé teszi a támadások és a rendellenességek észlelését, a kockázatos viselkedések automatikus blokkolását és jelzését, a védelmi intézkedések alkalmazását, valamint a fenyegetésekkel kapcsolatos hatalmas információmennyiség kezelését.

A szervezet egyedi biztonsági kihívásaitól, igényeitől és képességeitől függ, hogy mennyire könnyen tudja alkalmazni ezeket az alapelveket. Más szóval: az Ön cégének is saját útján kell haladnia a Zero Trust modell megvalósítása során.

Annak érdekében, hogy gyorsabban révbe érjen, a Microsoft kidolgozott egy rugalmas Zero Trust keretrendszert, amely irányt mutat a bevezetéshez, és átfogó útmutatást nyújt a Zero Trust tárgykörébe tartozó **hat fő kockázati** területről:

- **Identitások:** Automatizálhatja a kockázatok észlelését és elhárítását, és erős hitelesítéssel gondoskodhat az összes digitális erőforrás biztonságos eléréséről.
- **Alkalmazások :** Kiemelkedően biztonságos hozzáférést biztosíthat a dolgozók számára a felhő- és mobilalkalmazásokhoz, valamint távoli hozzáférést a helyi környezetben futó vállalati alkalmazásokhoz.
- **Hálózat :** Csökkentheti a peremhálózati védelemre épülő megközelítésből eredő sebezhetőségeket, valamint a VPN használatának szükségességét, és fokozhatja a biztonsági megoldások skálázhatóságát a modern környezetekben, ahol az IT-szolgáltatások ma már egyre inkább a felhő köré épülnek.
- **Végpontok**: A rugalmas, integrált felügyeleti megközelítéssel megvédheti azt a nagyobb támadási felületet, amelyet a végpontok növekvő száma és sokfélesége idéz elő.
- **Adatok**: Az adatok felhős és helyi környezetekre is kiterjedő egységes klasszifikációja, címkézése és védelme segít megakadályozni az illetéktelen megosztást, és csökkenti a belső kockázatokat.
- **Infrastruktúra**: Hatékonyabb, automatizált felügyelettel gondoskodhat a hibrid infrastruktúra védelméről, beleértve a helyi és a felhős környezeteket is.



Ha úgy dönt, hogy bevezeti a Zero Trust keretrendszert a fentiek közül valamelyik – vagy az összes – területen, ezzel hatékonyan modernizálhatja cége biztonsági technológiáját és folyamatait, és maximálisra növelheti a védelmet napjaink fenyegetéseivel szemben. Ugyanakkor minden cégnél eltérőek a prioritások a meglévő képességektől és az adott biztonsági terület által jelentett kockázat szintjétől függően. Útmutatónkból általános áttekintést kaphat a Zero Trust modellről, valamint részletes információkat és gyakorlati lépéseket ismerhet meg a keretrendszer két fontos pillére: az identitások és a végpontok kapcsán.

A Microsoft Zero Trust architektúrája

Ebben az e-könyvben a Zero Trust keretrendszer első két elemére összpontosítunk, amelyek megítélésünk szerint a legfontosabbak a kis- és középvállalatok számára.

A Zero Trust alapjai

Identitáskezelés

A felhőalkalmazások és a hibrid munka elterjedése újradefiniálta a biztonsági határvonal fogalmát. A vállalati alkalmazások és adatok egyre inkább átkerülnek a helyi környezetből a hibrid és felhős környezetekbe. Számos cég még a régi identitás- és hozzáférés-kezelési modellre támaszkodik, amely egy olyan világot tükröz, ahol egyértelműen meg lehetett különböztetni egymástól a hálózaton belüli és kívüli dolgokat.

Ezek a rendszerek megnehezítik a dolgozók számára a szükséges alkalmazások és adatok elérését, és túlzott jogosultságokat biztosítanak a megbízhatónak ítélt felhasználóknak, amivel biztonsági réseket idéznek elő. A felhőalapú identitáskezelési megoldásokat, például a teljes környezetben többfaktoros hitelesítést (MFA) és egyszeri bejelentkezést (SSO) alkalmazó Zero Trust keretrendszer jobban igazodik a modern munkahelyek igényeihez.

1 • Többfaktoros hitelesítés

A többfaktoros hitelesítés (MFA) az alkalmazások védelmében segít azzal, hogy a hozzáférés megadása előtt kötelezően előírja a felhasználók számára a személyazonosságuk igazolását egy második hitelesítési módszer, például telefon vagy token használatával.

- A Microsoft Azure Active Directory (Azure AD) és hasonló eszközök ingyenes megoldást kínálnak a többfaktoros hitelesítésre.
- Az Azure Active Directory (Azure AD) Multi-Factor Authentication (MFA) segít az adatokhoz és az alkalmazásokhoz való hozzáférés védelmében, és egy további biztonsági réteget biztosít egy második hitelesítési forma használatával. A szervezetek a többfaktoros hitelesítést feltételes hozzáféréssel is kombinálhatják az egyedi igényeknek megfelelően.

2 • Jelszó nélküli hitelesítés

A jelszómentes hitelesítési módszerek egyszerűbb és biztonságosabb hitelesítési folyamatot tesznek lehetővé a weben és a mobileszközökön. Segítségükkel a felhasználók könnyen és biztonságosan, jelszó nélkül hitelesíthetik magukat.

- Az AAD használata esetén például a Microsoft Authenticator alkalmazás segítségével a felhasználók jelszó nélkül jelentkezhetnek be bármilyen Azure AD-fiókba. A Microsoft Authenticator kulcsalapú hitelesítés útján biztosít egy eszközhöz kötött felhasználói hitelesítő információt, az eszközhöz való hozzáféréshez pedig PIN-kódot vagy biometrikus azonosítót kell megadni. A Windows Hello for Business hasonló technológiát használ.
- Implementálja az egyszeri bejelentkezést (SSO). Így nem kell egyazon személyhez többféle hitelesítő adatot kezelni, és a felhasználói élmény is javul a kevesebb bejelentkezési ablaknak köszönhetően.
- A bevezetést kezdje egy alacsony kockázatú csoport körében, és magyarázza el, milyen előnyökkel jár a jelszavak mellőzése. Konfigurálja a többfaktoros hitelesítést jelszómentes hitelesítési lehetőséggel, amíg az emberek meg nem szokják, majd a háttérben kezdje el kivezetni a jelszavakat és a jelszavaktól való függőséget.
- A Microsoft Azure Active Directory (Azure AD) SSO-megoldást is biztosít a népszerű SaaS-alkalmazások, a helyi alkalmazások és az egyedi fejlesztésű alkalmazások számára, legyen szó bármilyen felhőről, felhasználótípusról és identitásról.

3 • Hozzáférés-szabályozás adaptív, kockázatalapú szabályokkal

Túlléphet az egyszerű „hozzáférés vagy blokkolás” típusú döntéseken, és a kockázattűréstől függő döntéseket hozhat – az engedélyezés és a blokkolás mellett például korlátozhatja is a hozzáférést, illetve további bizonyítékokat kérhet a személazonosság igazolására, például többfaktoros hitelesítés útján.

- Az Azure AD feltételes hozzáférési funkciójával finomhangolt, adaptív hozzáférés-szabályozást valósíthat meg, például többfaktoros hitelesítést írhat elő felhasználói kontextus, eszköz, földrajzi hely vagy a munkamenet kockázati adatai alapján.

- Ehhez a lehetőséghez működő Azure AD-tenant szükséges Azure AD Premium licenccel vagy próbalicenccel. Szükség esetén ingyenesen létrehozhat egyet feltételes hozzáférési rendszergazdai jogosultságokkal.

4 • A régebbi típusú hitelesítés blokkolása

A rosszindulatú szereplők által kihasznált egyik leggyakoribb támadási felület a lopott vagy „visszajátszott” hitelesítő adatok felhasználása a régebbi típusú protokollok – például az SMTP – esetében, amelyek nem képesek modern biztonsági módszerek alkalmazására.

- A régebbi hitelesítési protokollok, például a POP, az SMTP, az IMAP és a MAPI, nem képesek többfaktoros hitelesítés használatára, így kedvelt belépési pontot jelentenek a támadók számára.

- A legegyszerűbb módszer a régi típusú hitelesítés letiltására a teljes szervezetben egy olyan feltételes hozzáférési szabályzat konfigurálása, amely kifejezetten a régi típusú hitelesítést használó kliensekre vonatkozik, és letiltja a hozzáférést.

- A régi típusú hitelesítések letiltásakor fokozatos megközelítést javaslunk – nem célszerű az összes felhasználó számára egyszerre letiltani őket. Mielőtt letiltaná ezeket a hitelesítési protokollokat a címtárban, először fel kell térképeznie, hogy vannak-e olyan alkalmazások, amelyek régi típusú hitelesítést használnak, és hogy mindez milyen hatással van a teljes címtárra.

5 • Automatizált kockázatészlelés és -elhárítás

A valós idejű kockázatfelmérések segíthetnek az identitások védelmében a bejelentkezések és a munkamenetek során.

- Az Azure Identity Protection valós idejű, folyamatos kockázatészlelést, automatikus elhárítást és összekapcsolt felderítést biztosít a kockázatos felhasználók és bejelentkezések kivizsgálása céljából a potenciális sebezhetőségek csökkentése érdekében.

- Kezdésként aktiválja az Identity Protection szolgáltatást. A Microsoft Defender for Cloud Apps szolgáltatásból a felhasználói munkamenetek adatait felhasználhatja az Azure AD-ben a hitelesítést követő, potenciálisan kockázatos felhasználói viselkedések azonosítására.

- Az Identity Protection adatai más eszközökbe is exportálhatók archiválás, illetve további vizsgálat és összefüggések feltárása céljából. A Microsoft Graph-alapú API-k segítségével ezek az adatok további – például SIEM-megoldással történő – feldolgozás céljából is gyűjthetők.

6 • Az identitás- és hozzáférés-kezelő (IAM) megoldás gazdagítása több adattal

Minél több adatot tölt be az IAM-megoldásba, annál jobban növelheti az általános biztonságot az árnyaltabb hozzáférési döntések, valamint a céges erőforrásokhoz hozzáférő felhasználók jobb átláthatósága révén.

- Az Azure Active Directory (Azure AD), a Microsoft Defender for Cloud Apps és a Microsoft Defender for Endpoint egymással együttműködve gazdagabb jelfeldolgozást biztosítanak a jobb döntéshozatal érdekében.

- Konfigurálja a feltételes hozzáférést a Microsoft Defender for Endpoint, a Microsoft Defender for Identity és a Microsoft Defender for Cloud Apps megoldásokban.

7 • Az identitáskezelési biztonság javítása

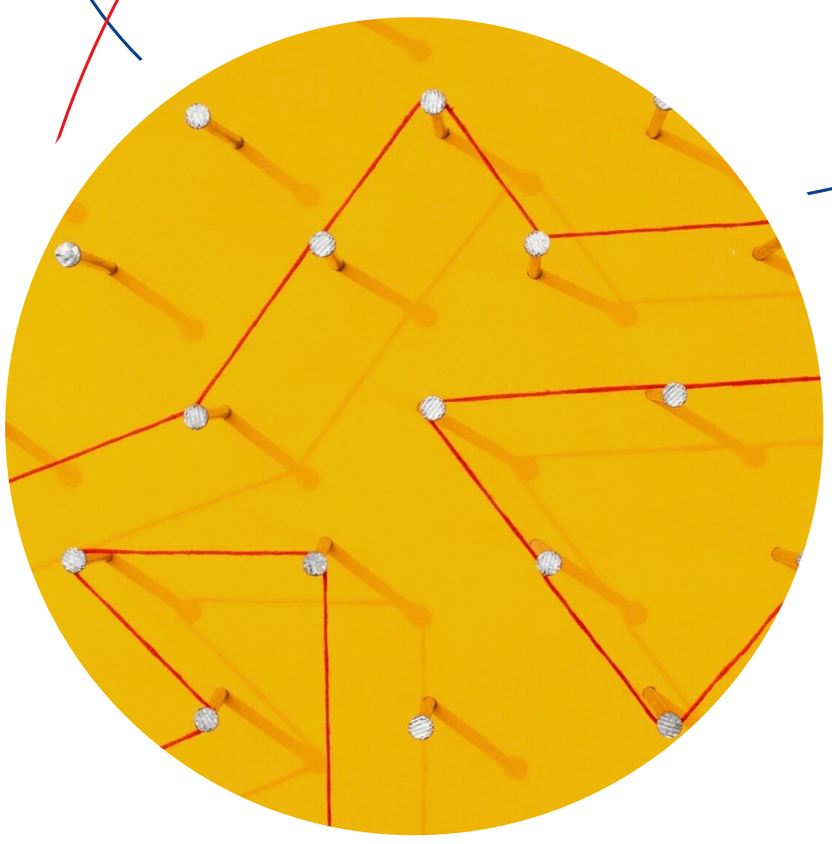
Az Azure AD identitásbiztonsági pontszáma segít az identitáskezelési biztonság felmérésében annak elemzésével, hogy mennyire felel meg a cég környezete a Microsoft ajánlott biztonsági gyakorlatainak.

- Az identitásbiztonsági pontszám az Azure AD valamennyi kiadásában elérhető.

- A korábbi pontszámok megtekintéséhez lépjen a Microsoft 365 Defender portálra, és nézze meg az összesített Microsoft Biztonsági pontszámot. Az összesített pontszám korábbi változásainak áttekintéséhez kattintson az „Előzmények megtekintése” gombra. Egy konkrét dátum kiválasztásával megtekintheti, hogy mely beállítások voltak engedélyezve az adott napon, és hogy ezekért milyen pontszámot kapott.

→ Cége identitásbiztonsági pontszámáról érdeklődjön a Noventiq szakemberétől!

Végpontok



A modern vállalatoknál hihetetlenül sokféle végpont fér hozzá adatokhoz, ezek közül azonban nem mindegyik áll a szervezet felügyelete alatt – vagy akár a birtokában –, így az eszközök konfigurációja és a szoftverjavítások telepítésének állapota eltérő lehet. Ez hatalmas támadási felületet teremt. A mindenre kiterjedő Zero Trust keretrendszer segíthet a végpontbiztonság javításában, így cége megteremtheti a biztonságosabb hibrid munkavégzés feltételeit, és eszközfüggő stratégiákat is alkalmazhat például az IoT- vagy a peremhálózati eszközökhöz.

A végpontvédelem a végpontok monitorozását és védelmét jelenti a kiberfenyegetésekkel szemben. A védett végpontok lehetnek asztali számítógépek, laptopok, okostelefonok, táblagépek és más eszközök. A cégeknek olyan átfogó megoldásra van szükségük, amely az összes végpont mellett a hálózati eszközök, például a routerek felderítését is lehetővé teszi. Szükség van még továbbá a sérülékenységek kezelésére, végpontvédelemre, valamint végponti észlelésre és reagálásra (EDR) szolgáló összetevőre is.

A Zero Trust végpontvédelmi alapelvei

A Zero Trust út, nem pedig cél. Mivel az IT-biztonság valamennyi aspektusára hatással van, a bevezetése elsőre hatalmas feladatnak tűnhet. Az elsőként a jelentős hatású, de kisebb erőfeszítést igénylő területeket célzó, fokozatos megközelítéssel gyors javulások érhetők el, és tisztázható, hogy milyen lépéseket érdemes tenni legközelebb. Az átfogó stratégia kialakítható menet közben is. A lényeg az, hogy belevágjunk.

A Zero Trust sikeres megvalósítása hozzájárulhat a biztonság javításához egy olyan világban, ahol a munkavégzés jelentős része a peremhálózati védelmen kívül eső eszközökön, alkalmazásokban és adatokkal folyik, és segít csökkenteni az adatsértések kockázatát, valamint gondoskodni a folyamatos üzletmenetről.

- **Eszközök regisztrálása az Azure AD-ben:** Ha számos, bárki által használt végponton szeretné felügyelni a biztonságot és a kockázatokat, ehhez szükség van az összes olyan eszköz és hozzáférési pont átláthatóságára, amely hozzáférhet az erőforrásokhoz.
- **A megfelelőség biztosítása a Microsoft Purview segítségével:** Miután azonosította a céges erőforrásokhoz hozzáférő összes végpont identitását, a hozzáférés engedélyezése előtt győződjön meg arról, hogy a végpontok megfelelnek a szervezet által meghatározott biztonsági minimumkövetelményeknek.
- **Adatszivárgás-megelőzési (DLP) szabályzatok alkalmazása az eszközökre** : Miután engedélyezte a hozzáférést az adatokhoz, kritikus fontosságú szabályozni, mit tehet velük a felhasználó. Ha például egy felhasználó céges identitással fér hozzá egy dokumentumhoz, megfelelő módszereket kell alkalmazni annak megakadályozására, hogy a dokumentumot nem védett helyre mentse, vagy megossza egy nem üzleti kommunikációs vagy chatalkalmazás segítségével.
- **Az eszközök valós idejű kockázatértékelésének aktiválása** : Miután regisztrálta az eszközöket az identitásszolgáltatónál, ez az információ felhasználható lesz a hozzáférési döntéseknél, hogy csak a biztonságos és megfelelő eszközök kaphassanak hozzáférést.
- **Eszközök felügyelete a Microsoft Endpoint Managerrel** : Miután engedélyezte a hozzáférést az adatokhoz, a kockázat csökkentése érdekében kritikus fontosságú, hogy szabályozhassa, mit tesz a felhasználó a céges adatokkal.
- **Hozzáférés engedélyezése a nem menedzselt eszközök számára a Microsoft Endpoint Managerrel**: A hatékonyság megőrzése szempontjából kritikus jelentőségű lehet, ha lehetővé teszi munkatársai számára a megfelelő erőforrások elérését a nem menedzselt eszközökről. Az adatok védelme ugyanakkor továbbra is elengedhetetlen.
- **Külső felhasználók eszközeinek regisztrálása az Endpoint Managerben :** A külső felhasználók (például alvállalkozók, beszállítók, partnerek stb.) eszközeinek felügyelet alá vonása az MDM-megoldásban hatékony módszert kínál az adatok védelmére és a munka elvégzéséhez szükséges hozzáférés biztosítására.

Összefoglalás

A Zero Trust keretrendszer bevezetésével hatékonyan modernizálhatja cége biztonsági technológiáját és folyamatait, és maximálisra növelheti a védelmet napjaink fenyegetéseivel szemben. Ugyanakkor minden cégnél eltérőek a prioritások a meglévő képességektől és az adott biztonsági terület által jelentett kockázat szintjétől függően. Útmutatónkban általános áttekintést adtunk a Zero Trust modellről, valamint részletes információkat és gyakorlati lépéseket mutattunk be a keretrendszer két fontos pillére: az identitások és a végpontok kapcsán.

A Microsoft többek között azért javasolja a Zero Trust használatát, mert a keretrendszer a vállalat saját környezetében is növelte a biztonságot és a hatékonyságot. E tapasztalatok alapján a Microsoft a technológiai megoldásaival integrált és azokat kiegészítő Zero Trust-képességeket dolgoz ki – ilyenek például a részletesen konfigurálható hozzáférési kontrollok, az alapértelmezés szerinti hálózati elkülönítés, valamint a gyanús hozzáférési kísérletek AI segítségével történő észlelése. Emellett a Microsoft biztonsági funkciói és szolgáltatásai kialakításukból eredően együttműködnek egymással, és segítenek az IT-csapatoknak a biztonsági technológiák egyszerűbb bevezetésében és folyamatos kezelésében. A Noventiq a Microsoft globális megoldásszállító partnere. Megfelelő erőforrásokkal és kompetenciákkal rendelkezünk a Microsoft-megoldások bevezetéséhez – még a legösszetettebb architektúrák esetében is.

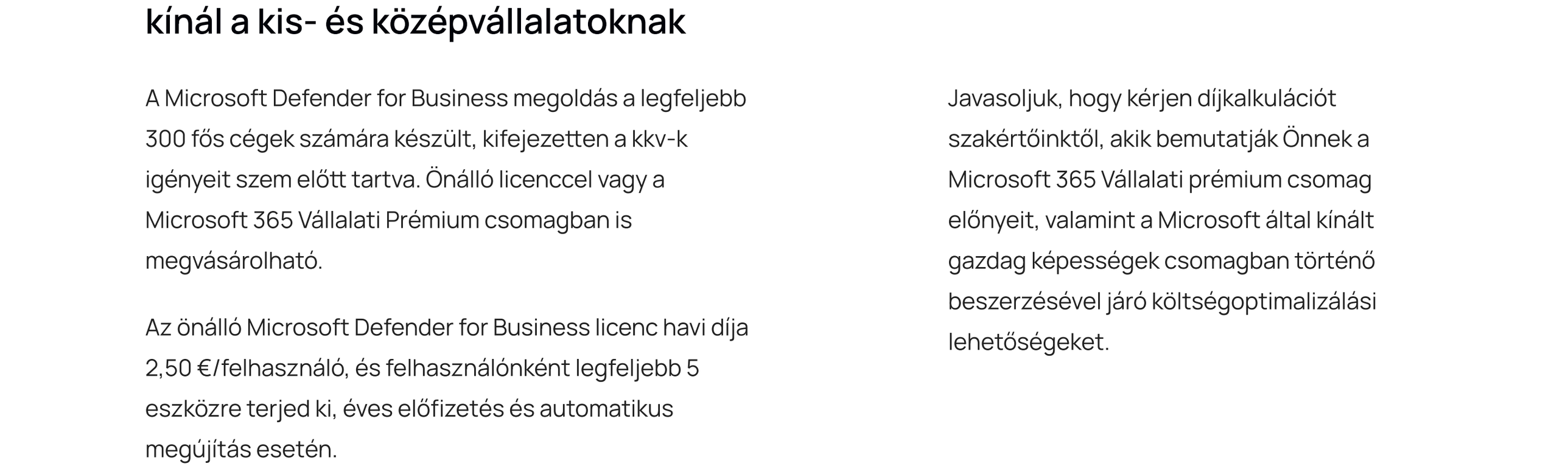
A Microsoft számos olyan megoldást kínál, amely az identitások és az eszközök védelmében segíti a cégeket. A Microsoft Defender for Business és a Defender for Endpoints egyaránt gazdag funkcionalitással támogatja a Zero Trust stratégiával kapcsolatos célok megvalósítását. A Noventiq szakemberei készséggel állnak rendelkezésére mindkét megoldással kapcsolatban, és bemutatják azokat az átfogó csomagokat, amelyek közül kiválaszthatja a cége igényeinek leginkább megfelelőt.

A Microsoft Defender for Business számos nagyvállalati képességet kínál a kis- és középvállalatoknak

A Microsoft Defender for Business megoldás a legfeljebb 300 fős cégek számára készült, kifejezetten a kkv-k igényeit szem előtt tartva. Önálló licenccel vagy a Microsoft 365 Vállalati Prémium csomagban is megvásárolható.

Az önálló Microsoft Defender for Business licenc havi díja 2,50 €/felhasználó, és felhasználónként legfeljebb 5 eszközre terjed ki, éves előfizetés és automatikus megújítás esetén.

Javasoljuk, hogy kérjen díjkalkulációt szakértőinktől, akik bemutatják Önnek a Microsoft 365 Vállalati prémium csomag előnyeit, valamint a Microsoft által kínált gazdag képességek csomagban történő beszerzésével járó költségoptimalizálási lehetőségeket.



Defender for Endpoints 1. és 2. csomag – végpontvédelem többplatformos vállalati környezetben

Defender for Endpoint Plan 2

Defender for Endpoint Plan 1

Block at First Sight	Centralized Management	Cross-Platform Support	Enhanced ASR	Manual Response Actions	Temper Protection	Web Content Filtering

Advanced Hunting	Automated Investigation & Response	Defender for Cloud Apps Integration	Endpoint Detection & Response	Evaluation Lab	Microsoft Threat Exprets	MIP Integration
Threat Analytics	Vulnerability Management (core)	6-Months Searchable Data				

A Nagyvállalati Szerződéssel és a Nagyvállalati Előfizetői Szerződéssel rendelkező vállalatok 2023. június 30-ig 50%-os kedvezményt kaphatnak a Microsoft Defender for Endpoints árából.

(Az ajánlatra további feltételek érvényesek. Teljes körű tájékoztatásért és a jogosultsági feltételek megismeréséért forduljon szakértőinkhez.)

Keresse a Noventiq tanácsadóját, aki segít kiválasztani a cége igényeinek legjobban megfelelő megoldást!

A Noventiq-ről

A londoni központú Noventiq a digitális transzformációs és kiberbiztonsági megoldások és szolgáltatások nemzetközi szinten vezető szállítója. A vállalat támogatja, megkönnyíti és gyorsítja a digitális átalakulás végrehajtását ügyfeleinél, és több mint 75 000, különböző ágazatokban működő cég és szervezet részére kínálja több száz vezető informatikai gyártó, valamint saját szolgáltatásait és megoldásait.

A 2021-es pénzügyi évben a Noventiq 1,1 milliárd dolláros forgalmat könyvelhetett el, és jelenleg egyike az ágazat leggyorsabban növekvő vállalatainak. A Noventiq háromdimenziós növekedési stratégiája a földrajzi terjeszkedésre, valamint a vállalat portfóliójának és értékesítési csatornáinak bővítésére épül. Ezt a stratégiát támogatja a Noventiq aktív felvásárlási politikája is, amely lehetővé teszi a vállalat számára az iparágban zajló folyamatos konszolidáció előnyeinek kihasználását. A 2022-es év kezdete óta a Noventiq 5 vállalat felvásárlását jelentette be Indiában, Törökországban és az Egyesült Arab Emírségekben, amelyek a digitális transzformáció különböző területeivel foglalkoznak. A Noventiq 3900 munkavállalót foglalkoztat közel 60 országban Ázsiában, Latin-Amerikában, Kelet-Európában és Afrikában, jelentős növekedési potenciállal rendelkező piacokon.

Szakterületeink

Digitális transzformáció, kiberbiztonság, információmenedzsment, modern hibrid infrastruktúra, többfelhős megoldások, megoldások a jövő munkahelyéhez, szoftvermérnöki tevékenység, szoftverfejlesztés, IT-szolgáltatás fejlődő piacokon, IT-tanácsadás.

NOVENTIQ
Global expertise, local outcomes

Noventiq – Global expertise, local outcomes

easterneurope@noventiq.com