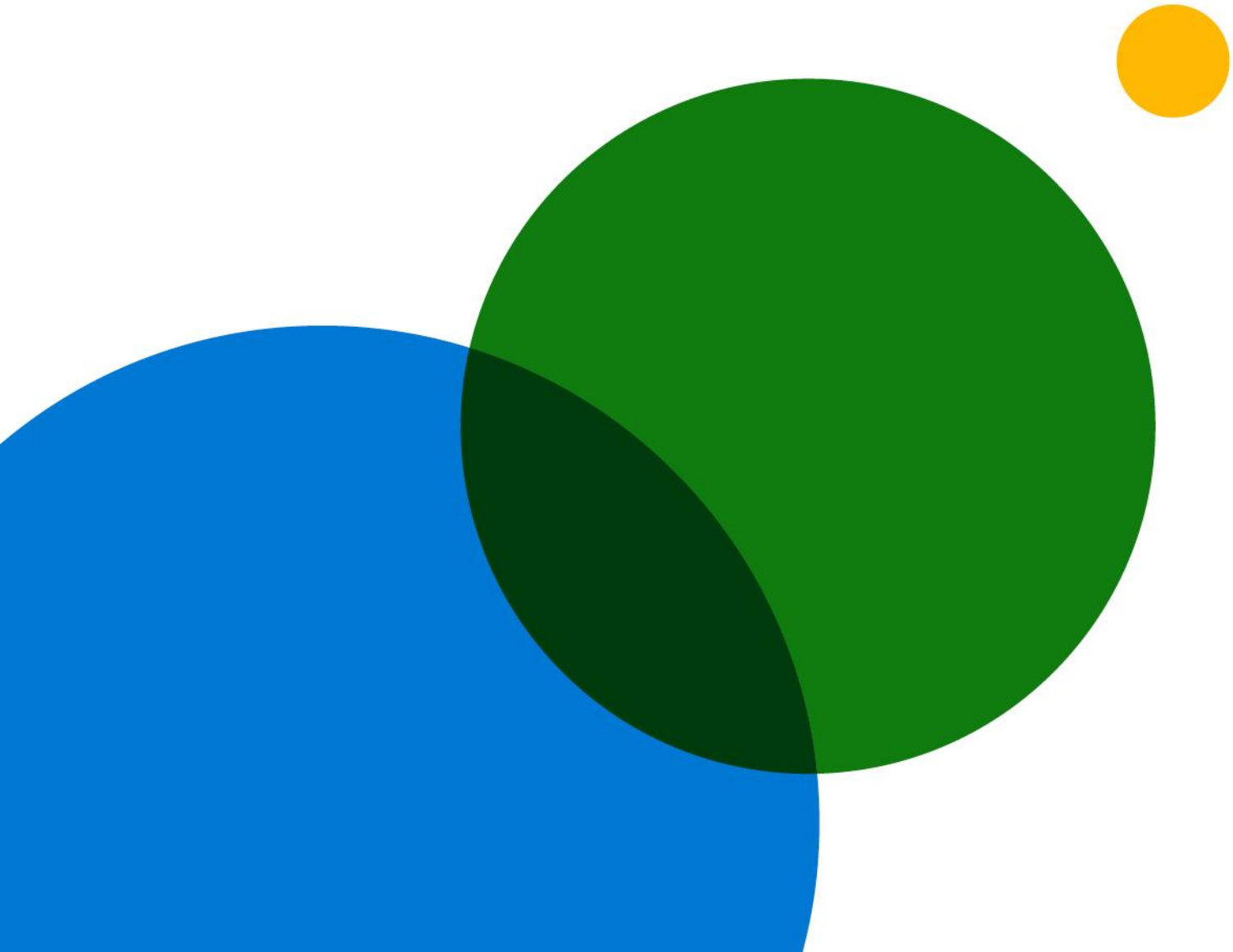
Microsoft Security

hypothesis

Jelentés a Zero Trust modell bevezetéséről



Tartalom

03
Bevezetés

04
Módszertan

05
Tudnivalók a Zero Trust modell bevezetéséről

06
Kikkel beszéltünk?

07
A kutatás általános tanulságai

24
Részletes kutatási célkitűzések és célközönség toborzása

Bevezetés

Vasu Jakkal / biztonságért, megfelelőségért és identitásért felelős vállalati alelnök

Az elmúlt év figyelemre méltó volt a kiberbiztonság fejlődése és a Zero Trust modelljének iparágunk és a világszerte működő szervezetek számára irányadó stratégiaként történő elterjedése szempontjából.

A világjárvány kezdetén a munkahelyek egyik napról a másikra szinte teljes mértékben távoli munkahelyekké alakultak. Ez a váltás számos céget gyors alkalmazkodásra kényszerített – támogatniuk kellett a dolgozóikat, akik úgy végezték a munkájukat, ahogyan tudták: személyes eszközeikkel, felhőszolgáltatásokon keresztül együttműködve dolgoztak, és a vállalati hálózat határain kívül osztottak meg egymással adatokat. Az átalakuláshoz fokozatosan alkalmazkodó cégek egyre kifinomultabb kiberbűnözőkkel kerültek szembe, akik célpontjaik kiválasztása, taktikájuk és erőforrásaik terén is egyre fejlettebb módszerekkel dolgoznak.

Napjainkban a hibrid munkavégzés az új valóság. Ennek és a gyors változásoknak a fényében az általunk készített felmérésben részt vevő cégek úgy nyilatkoztak, hogy a biztonság és a megfelelőség terén szükséges nagyobb agilitás, a fenyegetések gyorsabb észlelése és ezek elhárításának nagyobb gyorsasága, valamint a nagyobb egyszerűség és a biztonsági analitika fokozott rendelkezésre állása érdekében támaszkodnak a Zero Trust modellre.

A „Zero Trust" Architecture elvein alapuló megoldások az explicit ellenőrzés, a legkisebb jogosultsággal járó hozzáférések használata és a biztonsági incidens megtörténtének feltételezésén alapulva személyazonosságon, végpontokon, alkalmazásokon, az infrastruktúrán, a hálózaton és az adatokon belül és azokon keresztül hoz létre biztosítékokat, amelyeket fokozott láthatóság, automatizálás és orkesztráció egészít ki. Nemcsak az ügyfeleinknek és partnereinknek ajánljuk ezt a szemléletet, hanem a globális biztonság és a szoftverfejlesztés terén a Microsoftnál is ezt a megközelítést alkalmazzuk.

Ez a jelentés a Zero Trust bevezetésének útját vázolja fel különböző piacokon és iparágakban. Reméljük, hogy a kutatás révén szerzett tapasztalatok segíthetnek felgyorsítani saját Zero Trust Strategy elfogadását, megvilágítják, milyen fejlődési utat jár be a többi cég, és betekintést nyújtanak ennek a gyorsan fejlődő területnek a jövőben várható állapotába.

Módszertan

A Microsoft a Hypothesis Groupot, egy elemzésekkel, tervezéssel és stratégiával foglalkozó szervezetet bízott meg a Zero Trust modell bevezetéséről szóló jelentés és kutatás elkészítésével. A kutatás két fázisban zajlott az Egyesült Államokban, melynek során a Zero Trust bevezetésének trendjei és menete képezték a vizsgálat tárgyát; a második fázisban pedig további piacok kerültek be a vizsgálatba a globális trendek feltárása érdekében.

A kezdeti kutatásra 2020 augusztusában került sor, amikor egy 15 perces online felmérés készült az Egyesült Államokban 300 olyan biztonsági döntéshozó (SDM) részvételével, akik különböző iparágakban tevékenykedő cégeknél vesznek részt a Zero Trust Strategyel kapcsolatos döntések meghozatalában. Az online felmérés mellett 2020 szeptemberében öt online mélyinterjú is készült különböző egyesült államokbeli iparágak biztonsági döntéshozóival.

2021 áprilisában a biztonsági döntéshozók hasonló csoportjában globális kutatásra került sor az Egyesült Államokban, Németországban, Japánban és Ausztráliában/Új-Zélandon. Több mint 900 résztvevő vett részt egy 15 perces online felmérésben, amely a Zero Trust Strategy bevezetésére, a legjobb gyakorlatokra, az előnyökre, a kihívásokra és az érintett cégek jövőbeni beruházási terveire vonatkozó kérdéseket tartalmazott.



Tudnivalók a Zero Trust modell bevezetéséről

01 / A cégek készen állnak a Zero Trust Strategy előnyeinek kihasználására, aminek a hibrid munkahelyekre való áttérés és a Covid-19 is új lendületet adott.

A biztonsági döntéshozók (SDM-ek) szerint a Zero Trust Strategy kidolgozása biztonsági prioritásaik között az első helyen van; 96% szerint a kérdés kulcsfontosságú szerepet játszik cégük sikerében. A Zero Trust Strategy bevezetésének elsődleges motivációja az általános biztonsági helyzet és a végfelhasználói élmény javítása. A hibrid munkavégzésre való áttérés, amit a COVID-19 is felgyorsított, a Zero Trust Strategy szélesebb körű elfogadását is elősegíti: a nagyvállalati szervezetek 81%-a már megkezdte a hibrid munkavégzésre való áttérést, 31%-uk pedig már teljesen átállt rá. A 94%-uknak azonban aggályaik vannak az áttérést illetően, főleg a dolgozói visszaélések, a megnövekedett informatikai munkaigény és a kibertámadások miatt. Ezt figyelembe véve a stratégia legfontosabb szempontjai közé tartozik a dolgozók fokozott képzése és a többfaktoros azonosítás (MFA) a zökkenőmentes felhasználói élmény és átállás biztosítása érdekében.

02 / A Zero Trust Strategy a cégek rugalmasan dönthetik el, hol kezdjenek hozzá a bevezetés folyamatához; a megközelítés tehát az igényeikhez igazítható.

A szervezetek kevesebb, mint 15%-a kezdte el a Zero Trust Strategy bevezetését ugyanazon a biztonsági kockázati területen. Ez nagyrészt azért van így, mert a bevezetésre nem különálló, egyedi technológiák soraként, hanem a biztonsági architektúra pilléreit és képességeit átfogó, végponttól végpontig tartó folyamatként tekintenek. Hasonlóképpen a Zero Trust egyes összetevőinek bevezetési sorrendje egy-egy biztonsági kockázati területen belül is nagyon változó lehet, és a biztonsági szakemberek között is jelentős különbségek vannak abban, hogy melyik összetevő bevezetését veszik előre.

03 / Bár a Zero Trust Strategy széles körben elfogadottá vált, és javítja a szervezetek képességét a fenyegetések kezelésére, még mindig van tennivaló.

A szervezetek 76%-a már legalábbis belekezdett a Zero Trust Strategy bevezetésébe, 35%-uk pedig azt állítja, hogy már teljes mértékben bevezette. Azok azonban, akik azt állítják, hogy teljes mértékben bevezették a modellt, elismerik, hogy a Zero Trust Strategy bevezetését még nem fejezték be az összes biztonsági kockázati területen és összetevőt illetően. A Zero Trust Strategy azért vonzó lehetőség, mert nagyobb agilitást biztosít, lehetővé teszi a fenyegetések gyorsabb észlelését, és jobb képességet biztosít a tárgyak internetének (IoT) és az operatív technológiák (OT) biztonságának kezelésére.
Az USA-ban a bevezetés egyre szélesebb körű (2020 augusztusában 70%, 2021 áprilisában 79%); az USA más országokhoz képest is előrébb jár a Zero Trust modell bevezetésében, máshol ugyanis később kezdték el bevezetni, és emellett az amerikai cégeknek – állításaik szerint – kevésbé kell pénzügyi korlátokkal számolniuk. Azonban míg a szervezetek 57%-a azt állítja, hogy mások előtt áll a bevezetés terén, mintegy felüknél még számos tennivaló van, mivel a Zero Trust bevezetése még nem történt meg minden biztonsági kockázati területen és összetevőnél.

04 / A jövőre nézve a Zero Trust Strategy továbbra is kiemelt prioritás marad, és körültekintő döntéshozatalt igényel a munkatársakkal és a beszállítókkal kapcsolatban.

A Zero Trust Strategy várhatóan két év múlva is az első számú biztonsági prioritás marad, a cégek pedig a várakozásaik szerint növelni fogják a beruházásaikat. A személyzeti kihívások leküzdése (beleértve a biztonsági csapatok személyi összetételének biztosítását és a vezetőség elkötelezettségét) kulcsfontosságú szerepet fog játszani a Zero Trust terén végzett beruházások megduplázásában. A szállítói stratégiát illetően a biztonsági döntéshozók némileg előnyben részesítik az átfogó szolgáltatásokat nyújtó, illetve több szakterületet egyesítő szolgáltatókkal való együttműködést, mivel a szállító kiválasztása gyakran a belső szakértelem rendelkezésre állásától függ. Az egy gyártótól történő beszerzés előnyei közé tartozik a nagyobb szakértelem, az erőforrások jobb rendelkezésre állása és az egyszerűség, bár a megvalósítás hosszabb időt vehet igénybe, integrálhatósága a meglévő biztonsági architektúrába nehezebb lehet, illetve a potenciális sebezhetőség is nőhet.

Kikkel beszéltünk?

Globális



*1000+ alkalmazott az USA-ban; 500+ alkalmazott Németországban, Japánban, Ausztráliában/Új-Zélandon

A kutatás általános tanulságai

A szervezetek készen állnak a Zero Trust Strategy kiaknázására

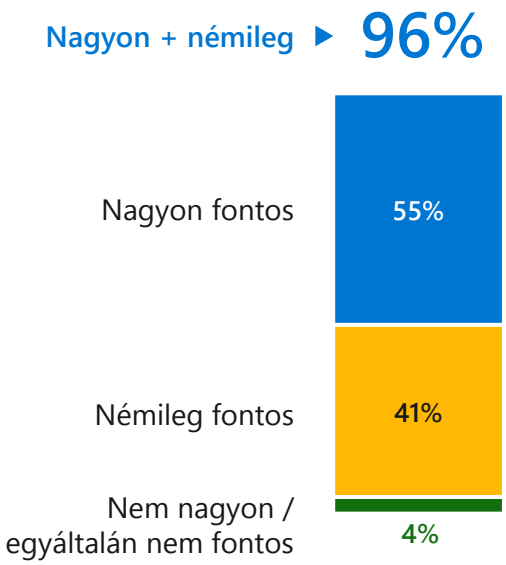
A Zero Trust Strategy napjaink 1. számú biztonsági prioritása a legkülönbözőbb piacokon és iparágakban; a „Zero Trust" modellt az elmúlt években számos szervezet vezette be. Bár a Zero Trust mindenki számára kiemelt fontosságú (53%), az egyesült államokbeli (56%) és németországi (53%) vállalkozások számára különösen fontos.

Szinte minden biztonsági szakember (96%) úgy véli, hogy a Zero Trust Strategy kritikus fontosságú a cégük sikere szempontjából. (Lásd: 1. melléklet) Általános biztonsági helyzetük megerősítése és a végfelhasználói élmény javítása mellett a biztonsági szakemberek a Zero Trust Strategytől azt várják, hogy egyszerűsítse a biztonsági eljárásokat a munkatársak számára. (Lásd: 2. melléklet)

Ahogy egy a vendéglátóiparban dolgozó amerikai biztonsági döntéshozó kifejtette: *„A cél az, hogy összességében javítsuk a biztonsági helyzetünket, de az egész végső soron arról szól, hogy csökkentsük a végfelhasználói élményben jelentkező nehézségeket, és megkönnyítsük a felhasználók életét."*

Ezen túlmenően a biztonsági szakemberek 31%-a a Zero Trust Strategyt a hibrid munkavégzésre való, a járvány végével mind közelibbé váló átállásban is fontos eszköznek tekinti; ez a motiváció különösen hangsúlyos Ausztráliában/Új-Zélandon (44%).

1. melléklet. A Zero Trust kritikus fontosságú



2. melléklet. A Zero Trust motivációs tényezői

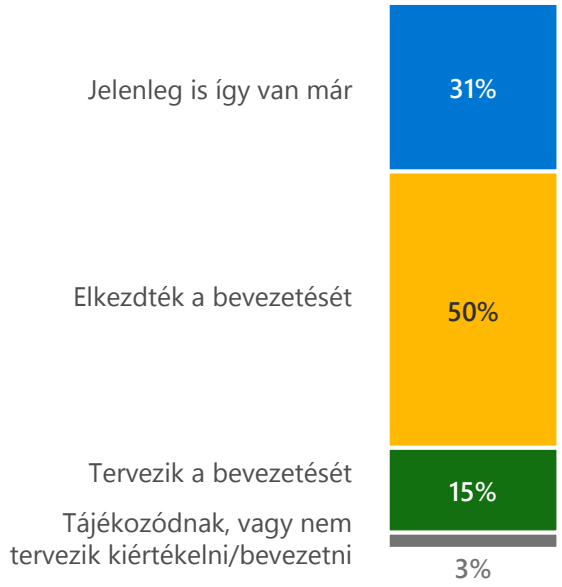
Fő motivációs tényezők	
Javítja az általános biztonsági helyzetet	47%
Javítja a végfelhasználói élményt és hatékonyságot	44%
Átalakítja a biztonsági csapatok együttműködésének módját	38%
Egyszerűsíti a biztonsági feladatokat	35%
Csökkenti a biztonsági költségeket	35%

A hibrid munkahelyekre való áttérés elősegíti a Zero Trust Strategy szélesebb körű bevezetését.

A nagyvállalati szervezeteknek már 81%-a kezdte meg a hibrid munkahelyre való átállást, 31%-uk pedig már teljesen átállt a hibrid munkavégzésre. Ezzel együtt a teljes körű átállás aránya nem egységes az egyes piacokon: míg Ausztrália és Új-Zéland 37%-kal vezet, addig Németország messze le van maradva, mindössze a szervezetek 20%-a állt már át a hibrid modellre. (Lásd: 3. melléklet)

Bár a globális piacok eltérő ütemben haladnak a hibrid munkavégzés felé, a szervezetek túlnyomó többsége (91%-a), amelyek még nem fejezték be az átállást, azt tervezi, hogy a következő öt évben megteszi ezt. Kulcsfontosságú, hogy 94%-uk aggódik az átállás miatt: az aggodalmak listájának élén a munkatársak által elkövetett visszaélések, a megnövekedett informatikai munkaterhelés, valamint a kibertámadások megnövekedett kockázatai állnak. (Lásd: 4. melléklet)

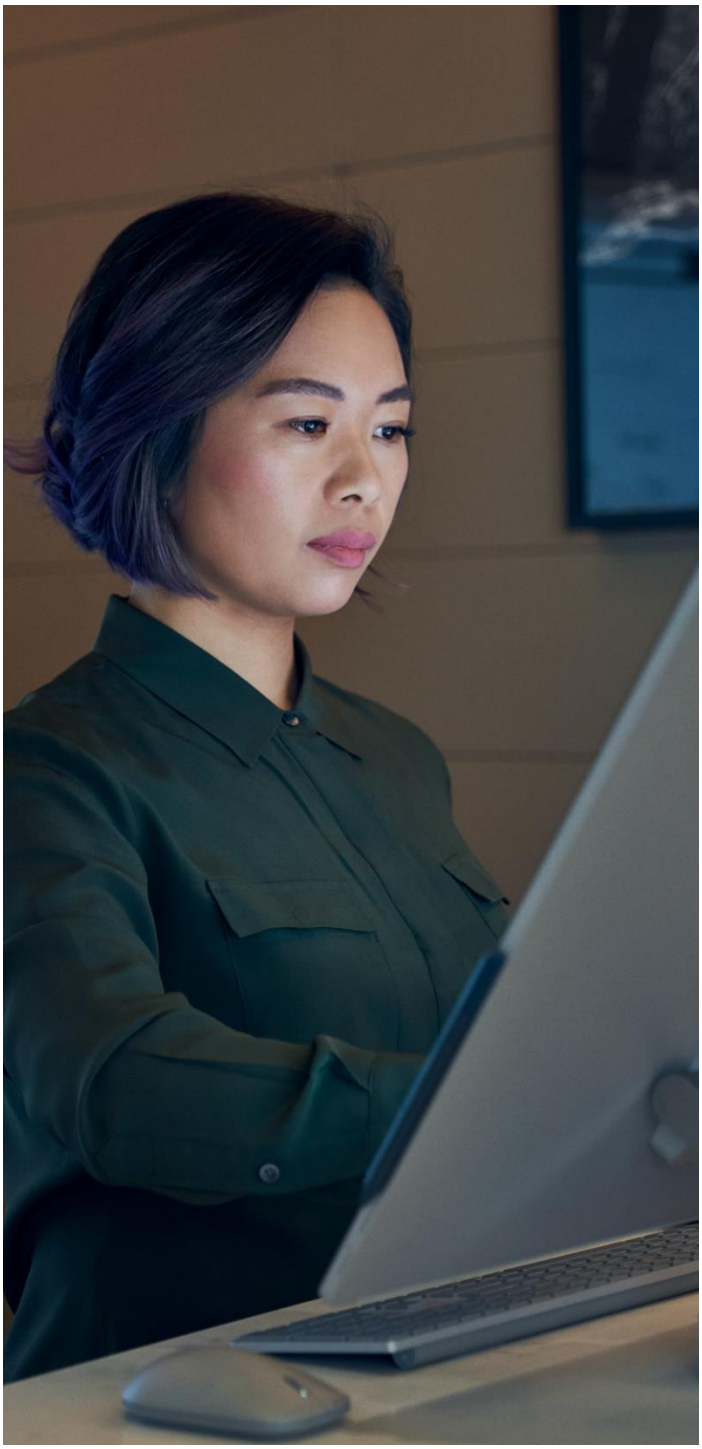
3. melléklet. Hibrid munkavégzésre irányuló szándékok



4. melléklet. Hibrid munkavégzéssel kapcsolatos aggodalmak

A munkatársak nem biztonságos alkalmazásokat töltenek le	37%
Megnövekedett IT-munkaterhelés	37%
Támadások zsarolóprogramokkal	36%
Adathalász támadások	35%
Személyes eszközök helytelen használata	34%
Jogosulatlan hozzáférés adatokhoz	31%
Az összes eszköz kezelésének képtelensége	30%
Személyes e-mail-fiókok használata	30%
Adatvédelmi előírások be nem tartása	24%

A covid-19 új szempontokat hozott, amelyek felgyorsítják a Zero Trust Strategy való áttérést



A potenciális problémák minimalizálása, valamint a felhasználói élmény és átmenet zökkenőmentes biztosítása érdekében az érdekeltek hangsúlyozzák a dolgozók fokozott képzésének fontosságát (54%) (különösen Japánban [61%] és Németországban [58%]) és a többfaktoros azonosítás (MFA) szerepét (50%) (különösen az Egyesült Államokban [52%] és Németországban [56%]).

Mivel a biztonságos távoli és hibrid munkavégzést a Zero Trust Strategy segítheti, a COVID-19 a szervezetek 72%-ánál felgyorsította a Zero Trust Strategy bevezetését, bár a piacok között aszimmetriák mutatkoznak. Míg a világjárvány az Egyesült Államokban (76%), Japánban (71%) és Ausztráliában/Új-Zélandon (69%) tízből hét szervezetnél katalizálta a bevezetés folyamatát, addig Németországban (62%), talán a hibrid munkavégzésre való lassabb átállás miatt, a bevezetési arány jelentősen alacsonyabb maradt.

A Zero Trust modellt széles körben vezetik be világszerte, szerepe az Egyesült Államokban egyre nő

A Zero Trust nem csak egy hívószó; a Zero Trust valóság. A szervezetek 76%-a legalábbi megkezdte e stratégia bevezetését, 35%-uk pedig arról számol be, hogy teljes mértékben bevezette azt. Ez az adat azonban túlzottan optimista képet fest, mivel sok cég, amely úgy véli, hogy a modellt már teljes mértékben alkalmazza, egyúttal saját bevallása szerint még nem fejezte be a stratégia bevezetését az összes biztonsági kockázati területen. Napjainkban az USA a többi piachoz képest élen jár a Zero Trust Strategy bevezetésének terén, és továbbra is gyors ütemben bővül: 2020 augusztusához képest a Zero Trust Strategy bevezetése az Egyesült Államokban 70%-ról 79%-ra nőtt, ami jelentős ugrást jelent mindössze nyolc hónap alatt. (Lásd: 5. melléklet)

Bár a Zero Trust Strategy jelenleg kulcsszerepet játszik a biztonság területén, elterjedtsége viszonylag új keletű. Az elmúlt három évben a vállalatok 82%-a vezetett be Zero Trust Strategy, 21%-uknál ez az elmúlt 12 hónapban történt meg. Ezzel együtt az amerikai cégek 26%-a kezdte meg a bevezetést már több mint 3 évvel ezelőtt; a japán cégeknél 19%, az ausztrál/új-zélandi cégeknél 6%, a németországi cégeknél pedig 3% ez az arány. Ez a korábbi amerikai bevezetés – a kisebb költségvetési korlátokkal együtt – magyarázatot adhat arra, hogy az amerikai vállalkozások miért járnak élen a Zero Trust bevezetésében más piacok vállalkozásaihoz képest. Hasonlóképpen a Zero Trust viszonylagos németországi fejletlensége segít az alacsonyabb bevezetési arányok kontextusba helyezésében: a német szervezetek 97%-a mindössze az elmúlt három évben kezdte meg a modell bevezetését.

5. melléklet. A Zero Trust bevezetése



	USA (2020)	USA	DE	JP	AUS/NZ
A Zero Trust bevezetése	70%	79%	75%	76%	71%
• Teljes körűen bevezetve	27%	44%	19%	32%	28%
• Folyamatban	43%	35%	56%	44%	43%

35% teljes körűen bevezette

42%-nál a bevezetés folyamatban van

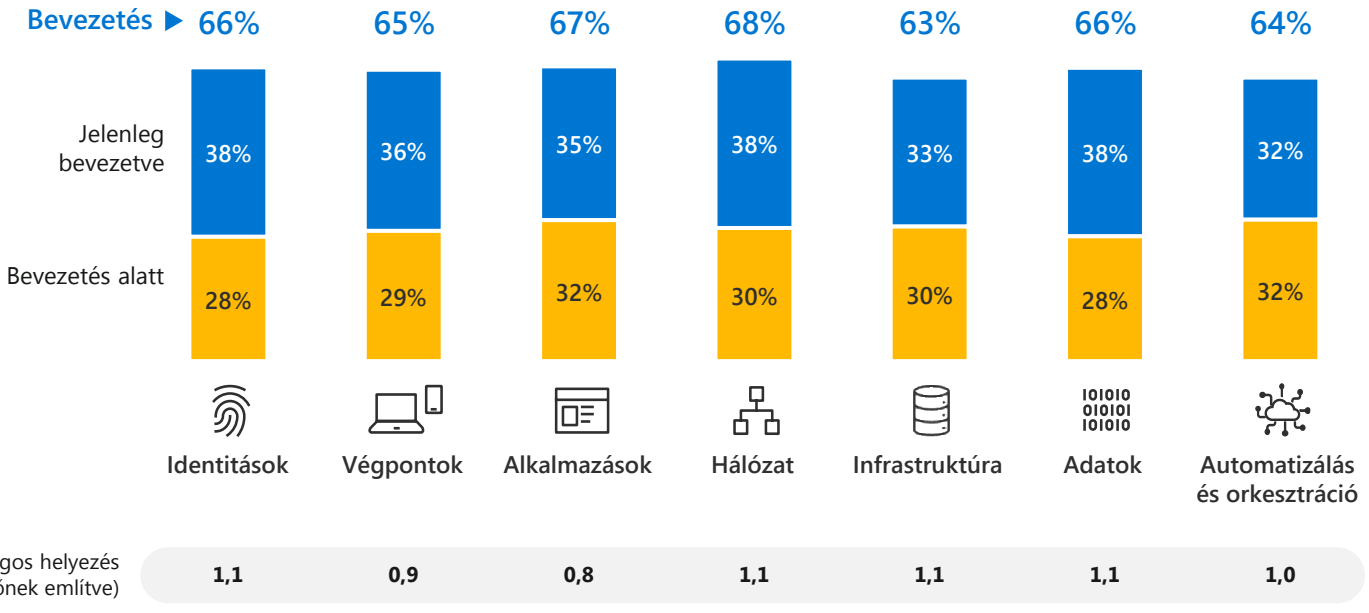
A Zero Trust bevezetéséhez nem létezik mindenki számára megfelelő megközelítés, így bárhol elkezdhetjük

Egyetlen biztonsági kockázati terület (identitások, végpontok, alkalmazások, hálózat, infrastruktúra, adatok, automatizálás és orkesztráció) sem emelkedik ki a Zero Trust Strategy elsődleges kiindulópontjaként – a szervezetek kevesebb, mint 15%-a vág bele ugyanazzal a biztonsági kockázati területtel. A szervezetek, valószínűleg az igényeik és a rendelkezésre álló belső erőforrások függvényében, különböző helyekről indulnak. Végső soron a fenyegetésekkel szembeni még nagyobb védelem érdekében arra törekszenek, hogy a Zero Trust Strategyt az összes biztonsági kockázati területen bevezessék; a Zero Trust ezért teljes körű stratégiának számít, amelynek alkalmazása időbe kerül. (Lásd: 6. melléklet)

A Zero Trust Strategy biztonsági kockázati területein túl a cégeknek azonosítaniuk kell az egyes biztonsági kockázati területek azon összetevőit, amelyeket prioritásként kell kezelniük. A végpontok, alkalmazások, hálózat, adatok és automatizálás/orkesztráció esetén nincs egyértelmű kiindulópont; a biztonsági szakemberek között jelentős a nézetkülönbség abban, hogy mely komponenseket tartják a legfontosabbnak. Az identitások területen azonban jellemzően az erős hitelesítést alkalmazzák először, az infrastruktúrán belül pedig egyértelmű prioritást élveznek a fenyegetések észlelésére szolgáló eszközök. (Lásd: 7. melléklet)

---

6. melléklet. Zero Trust jelenlegi bevezetettsége – biztonsági kockázati területek



7. melléklet. Zero Trust összetevő bevezetése (első 3) – 1.-nek rangsorolva (elsőként bevezetve)

Identitások	
Erős hitelesítés (pl. többfaktoros azonosítás, jelszó nélküli hitelesítés)	32%
Automatizált kockázatészlelés és -elhárítás	27%
Adaptív hozzáférési házirendek az erőforrásokhoz való hozzáféréshez	22%

Végpontok	
Adatveszteség-megelőzési házirendek/ kontrollok a nem felügyelt és felügyelt eszközökre	27%
Eszközök valós idejű kockázatértékelése / végponti fenyegetések észlelése	26%
Az eszközök regisztrálva vannak identitásszolgáltatónál	24%

Alkalmazások	
Árnyékinformatikai rendszerek folyamatos felfedése és kockázatértékelése	23%
Alkalmazások részletes hozzáférés-szabályozása (például korlátozottan látható vagy csak olvasható)	22%
Házirendalapú hozzáférés-szabályozás az alkalmazásokhoz	20%

Hálózat	
Biztonságos hozzáférés-szabályozás a hálózatok védelme érdekében	25%
Veszélyforrások elleni védelem és szűrés kontextusalapú jelek alapján	24%
Minden forgalom titkosítva van	20%

Infrastruktúra	
Biztonsági műveleti csapat hozzáfér fenyegetésészlelési eszközökhöz	25%
Felhő munkaterhelés elleni védelme hibrid és többfelhős környezetben	19%
Részletes láthatósági és hozzáférés-szabályozás minden munkaterhelésnél (virtuális gépek, szerverek stb.)	17%

Adatok	
A hozzáférési döntéseket biztonsági házirendi motor szabályozza	21%
Az adatok osztályozva és címkézve vannak	21%
A legérzékenyebb fájlokat folyamatosan titkosítás védi	20%

Automatizálás és orkesztráció	
A teljes körű áttekinthetőséget a kivizsgálás és reagálás érdekében központosított platform biztosítja	29%
A fenyegetési adatok gyűjtése és elemzése területeken átívelően történik (identitások, végpontok, alkalmazások, hálózat, infrastruktúra)	28%
Az automatikus vizsgálat és reagálás támogatottak	22%



Nem pusztán technológiák soraként tekintettünk rá, hanem olyan stratégiai és megközelítési módszerként, amely mindaddig, amíg nem tudjuk ellenőrizni, minden felhasználói erőforrást – akár a hálózatunkon belül, akár azon kívül található – megbízhatatlanként kezel.”

USA-beli biztonsági döntéshozó
Vendéglátás

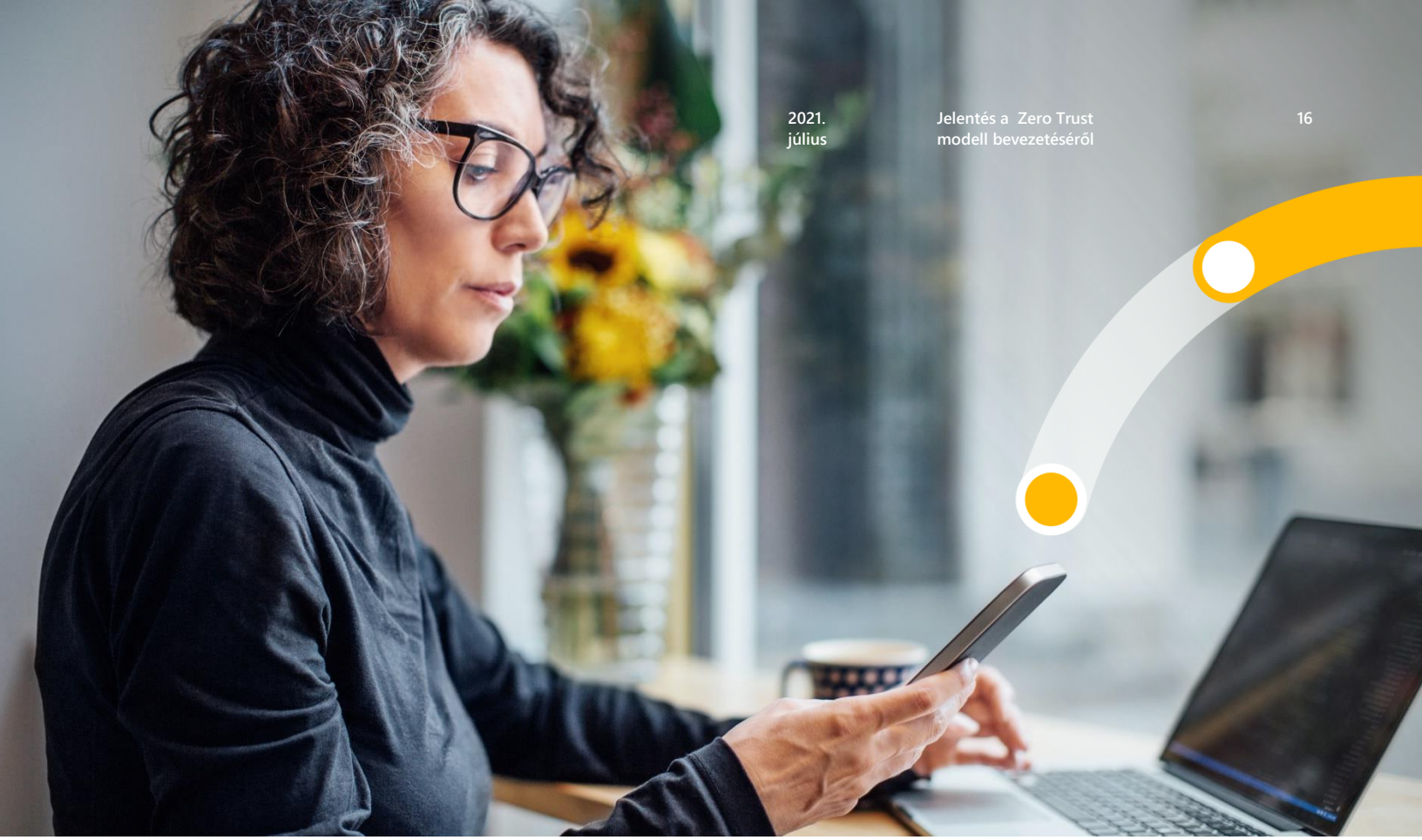
Amint a szervezetek elkezdik a Zero Trust Strategy bevezetését, a legfőbb előnyök közé tartozik a megnövekedett agilitás, gyorsaság és védelem; az erőforrások terén kevésbé gyakran jelentkeznek előnyök.

A Zero Trust Strategy bevezetése után az előnyök között a megnövekedett agilitás (37%), sebesség (35%) és az ügyféladatok védelme (35%) említhető. (Lásd: 8. melléklet) A dolgozók számára jelentkező közvetlen előnyök, például a biztonsági csapat terhelésének (27%) és az infrastruktúra kezeléséhez szükséges erőforrásoknak (22%) a csökkenése azonban ritkábban realizálódnak.

Fontos, hogy a szervezetek úgy vélik, hogy a Zero Trust Strategy segíteni fogja őket a legtöbb fenyegetés és környezeti változás kezelésében, különös tekintettel az IoT és az üzemeltetés biztonságára (47%).

8. melléklet. A Zero Trust előnyei





A cégek biztosak abban, hogy a legtöbbet hozzák ki Zero Trust Strategy

79% bízik abban, hogy általánosságban képes kezelni a biztonsági fenyegetéseket, bár ez a bizalom csökken, ha a fenyegetés meghamisított igazsággal kapcsolatos: a biztonsági döntéshozók a legkevésbé a szintetikus azonosságokkal (20%) és a mélyhamisítványokkal (10%) operáló fenyegetések kezelésében bíznak.

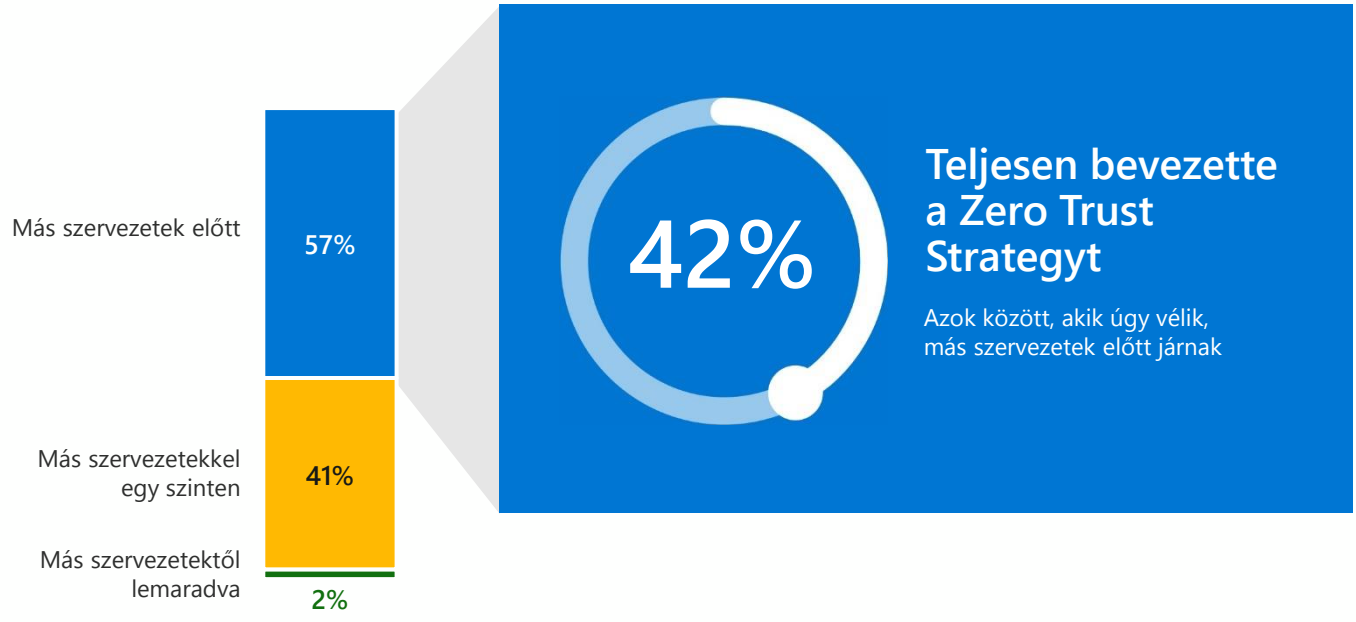
Az elért előnyök fényében a Zero Trust általában pozitív asszociációkat vált ki. A négy piacon az biztonsági döntéshozók egyszerre tartják gyakorlatiasnak és ambiciózusnak a cégük megközelítését, amelyet magabiztosként (37%) és hatékonyként (31%), valamint motiválóként (25%), inspirálóként (25%) és izgalmasként (25%) írnak le. Japánban a biztonsági szakemberek a Zero Trust modellt egyszerre nevezik nagy igényeket támasztónak (27%) és átalakításokkal járónak (25%), ami arra utal, hogy – bár nem könnyű bevezetni – a bevezetés után a stratégia nagy horderejű előnyökkel jár.

Sokan úgy vélik, hogy élen járnak a Zero Trust bevezetésében, de még mindig van mit tenniük

Bár a vállalkozásoknak csak 35%-a vezette be teljes mértékben a Zero Trust Strategy 52%-uk azt állítja, hogy előrébb tart, mint ahogyan tervezte, és 57%-uk véli úgy, hogy előrébb tart más cégeknél. A cégek különösen Japánban (66%) és Ausztráliában/Új-Zélandon (63%) vélik úgy, hogy előrébb járnak, mint mások. Miközben a piacokon mindenütt nagy a bizalom, úgy tűnik, szakadék tátong az észlelés és a valóság között: azok közül, akik úgy érzik, hogy más cégek előtt járnak, csak 42% állítja, hogy teljes mértékben bevezette a Zero Trust Strategyt. (Lásd: 9. melléklet)

Bár sok cég bízik Zero Trust Strategyban és érzi úgy, hogy készen áll a jövőbeli biztonsági fenyegetések kezelésére, a kockázati területek teljes lefedéséhez még mindig rengeteg a tennivaló. Például azon cégeknek, amelyek úgy vélik, teljes mértékben bevezették a Zero Trust Strategyt, közel a fele még nem végezte al a bevezetést az összes biztonsági kockázati területen; a bevezetés a legtöbbször az infrastruktúra és az identitások területén hiányzik.

9. melléklet. A Zero Trust bevezetésének összehasonlítása



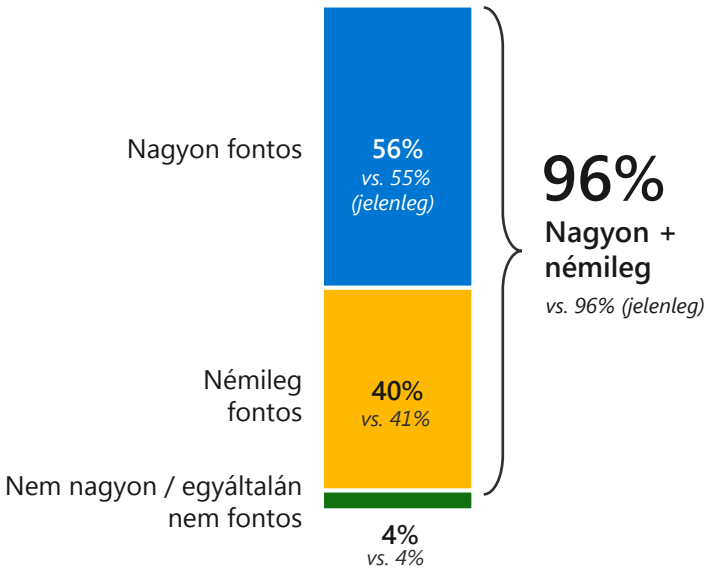
	USA	DE	JP	AUS/NZ
Elöl	59%	46%	66%	63%
Egy szinten	40%	52%	34%	32%
Lemaradva	2%	2%	0%	6%

Ami a következő két évet illeti, a Zero Trust Strategy kiemelt biztonsági prioritás marad

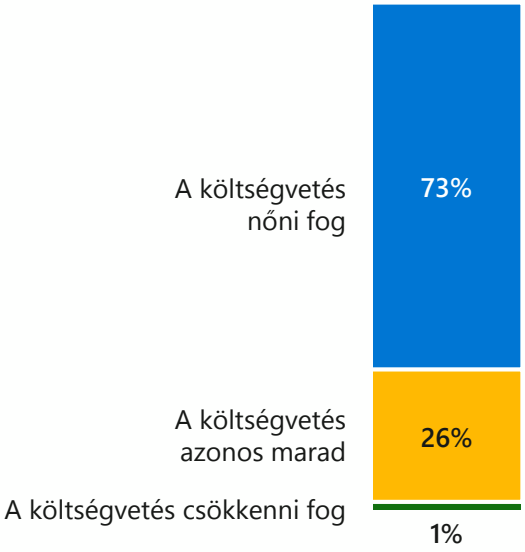
A szervezetek teljesen elkötelezték magukat a Zero Trust Strategy mellett, és a döntéshozók szerint a következő két évben is ez lesz a legfontosabb biztonsági prioritás. A Zero Trust Strategy mint biztonsági kezdeményezés relatív fontossága az előrejelzések szerint 2023-ra növekedni fog (53%-ról 58%-ra), mivel a biztonsági döntéshozók szerint a stratégia az átfogó siker szempontjából (96%) továbbra is kritikus fontosságú marad. (Lásd: 10. melléklet)

A várt fontosság különösen magas a japán cégek körében: az 56%-os általános átlaggal szemben a Zero Trust Strategy 70%-uk szerint lesz nagyon fontos a következő két évben. A költségvetésük növekedésére számító szervezetek 73%-ánál a Zero Trust Strategy fordított pénzek várhatóan növekedni fognak. Igaz, ez a szám valamivel alacsonyabb Németországban (67%), ahol 31% arra számít, hogy a költségvetésük változatlan marad. (Lásd: 11. melléklet)

10. melléklet. A Zero Trust a következő két évben várható fontossága

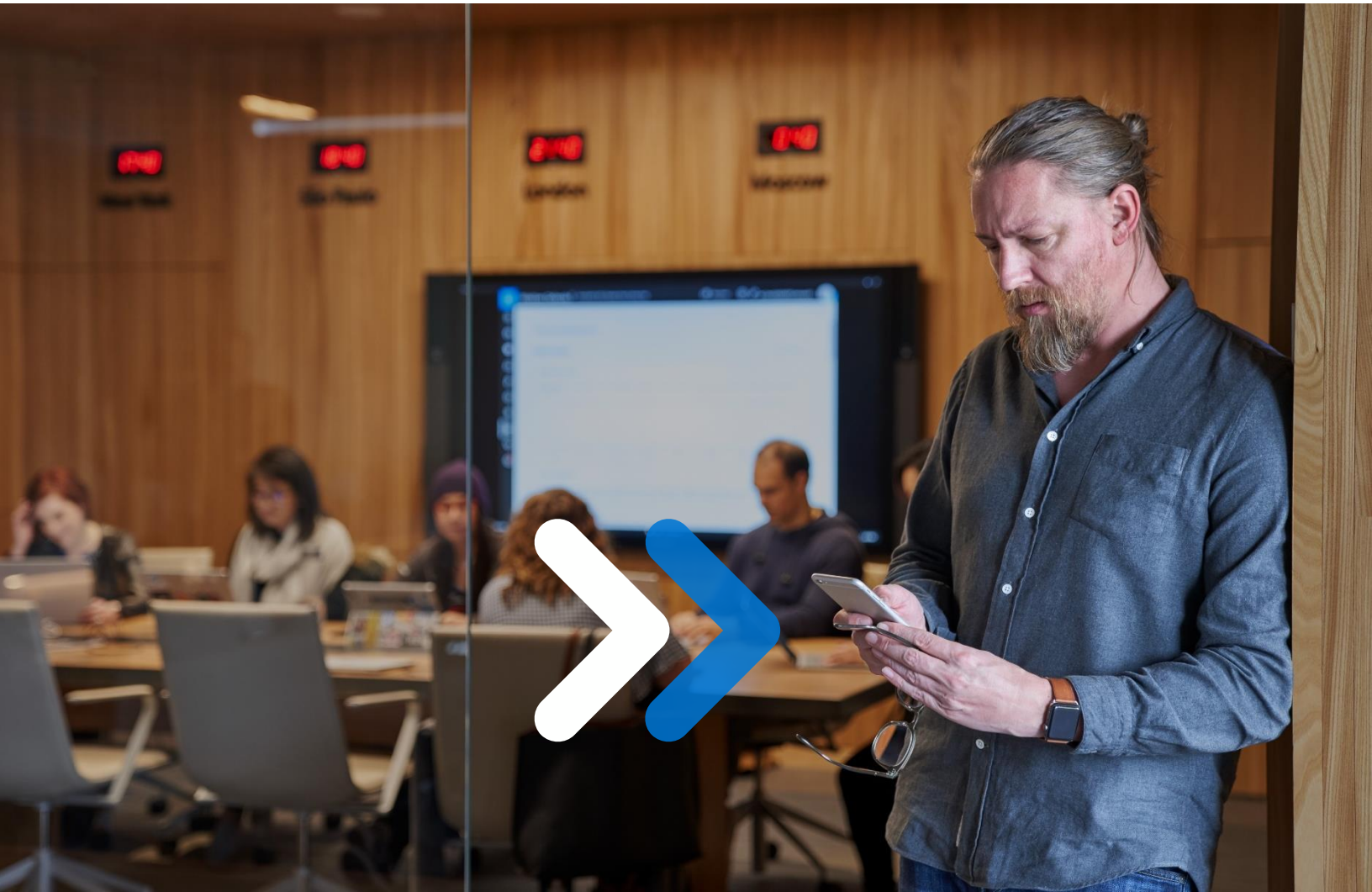


11. melléklet. A következő két évben várható Zero Trust költségvetés



A Zero Trust Strategy sikereinek bizonyítása további beruházásokhoz vezethet

Azok a szervezetek, amelyek teljes mértékben elkötelezték magukat a Zero Trust mellett, arra számítanak, hogy a következő két évben meg fogják duplázni a befektetéseiket; azok pedig, amelyek még nem kezdték el az átállást, azt kockáztatják, hogy még jobban lemaradnak. Ezek a szervezetek nem csak abban maradnak le az új modellt már teljes körűen bevezetett társaik mögött, hogy biztonsági terveikben a Zero Trust Strategy prioritást biztosítanak-e (42% vs. 66%), és hogy a költségvetésük növekedésére számítanak-e (66% vs. 72%), hanem abban is, hogy jelentősen kevésbé bíznak abban, hogy a jövőben kézben fogják tudni tartani az IoT és az üzemeltetés biztonságát (40% vs. 53%).



A dolgozókkal kapcsolatos kihívások leküzdése kulcsfontosságú lesz a Zero Trusttal kapcsolatos beruházások megduplázásában

A Zero Trust Strategy bevezetésében tapasztalható gyors előrelépés dacára a szervezeteknek még számtalan kihívást kell legyőzniük, ha tovább szeretnének haladni az átállás terén. (Lásd: 12. melléklet) Ezekben a kategóriákban az erőforrásokkal és a vezetéssel kapcsolatos kihívások a legelterjedtebbek. A Zero Trust Strategy bevezetéséhez szükséges idő és a felső vezetés támogatásának hiánya áll az akadályok listájának élén; ez utóbbi különösen hangsúlyos Ausztráliában/Új-Zélandon (65%).

Ezenkívül a költségvetési korlátok – amelyeket a cégek 45%-a említ akadályként – valószínűleg szintén szerepet játszanak az erőforrásokkal és vezetéssel kapcsolatos kihívásokban.

A biztonsági döntéshozók 21%-a például a Zero Trustba történő befektetés megtérülésének bizonyításával kapcsolatos nehézségeket említi a bevezetés gátjaként, ez ugyanis a vezetőség elkötelezettségének akadálya lehet. Mivel a nem amerikai piacokon nagyobb a valószínűsége a költségvetési korlátoknak (Japánban ez a szervezetek 60%-ánál, Németországban a szervezetek 57%-ánál, Ausztráliában/Új-Zélandon a szervezetek 57%-ánál jellemző), ennek tovagyűrűző hatása lehet, aminek következtében elképzelhető, hogy a Zero Trust Strategy bevezetésére kisebb mértékben és lassabban kerül sor Japánban, Németországban és Ausztráliában/Új-Zélandon, mint az Egyesült Államokban.

12. melléklet. A Zero Trust akadályai

Kihívások az erőforrások terén 60%	Vezetés 53%	Technológia 46%	Szállítók 46%	Költségvetési korlátok 45%
20% A bevezetése túl sokáig tart	**20%** A szélesebb felső vezetés támogatásának hiánya	**21%** Nehézség a biztonsági megoldások integrálásánál	**21%** A szállítóktól támogatás szükséges a bevezetéshez	**21%** A Zero Trust Strategy bevezetésének költségei
19% A belső változásmenedzsment hiánya	**19%** Az érintettek támogatásának hiánya	**19%** Nem kompatibilis a régebbi rendszerekkel	**21%-os** Nehézséget jelent a megfelelő szállítók azonosítása	**21%** A megtérülés bizonyításának nehézsége
18% Több oktatási anyagra lenne szükség	**19%** Segítségre van szükség a meggyőző üzleti indokoláshoz	**19%** Nehézségek a szervezeti szintű skálázásban	**17%** Képtelenség innovatív partnereket találni	**14%** Nincs elég nagy költségvetés
17% Nem szükséges egy olyan méretű szervezetnél, mint a miénk	**18%** A szervezet nem elkötelezett			
16% A megfelelő bevezetéséhez hiányzik a megkívánt szakértelem				

„A kezdeti elkötelezettség kihívást jelentett, de miután érintettként egyetértésre jutottunk arról, hogy beruházunk ebbe a projektbe, mindenki biztosította a szükséges támogatást.”

USA-beli biztonsági döntéshozó
FinTech



A biztonsági döntéshozók kis mértékben inkább a teljes körű megoldást biztosító, azaz több szakterületet egyesítő szolgáltatók felé hajlanak

A szállítói Zero Trust Strategy megválasztásakor a szervezetek az egy vagy több gyártótól történő beszerzés között választhatnak. Az előbbi stratégia esetén a cég a teljes Zero Trust Architecture termékcsomagját egyetlen teljes körű megoldást biztosító, azaz több szakterületet egyesítő (konszolidált) szolgáltatótól szerzi be, ami a biztonsági döntéshozók szerint több szakértelmet, erőforrást és egyszerűséget kínál azok számára, akiknek a belső erőforrásai szűkösek. Az ezzel a megközelítéssel kapcsolatos aggályok között megemlíthető viszont a nagyobb sebezhetőség és a rugalmasság hiánya. (Lásd: 13. melléklet)

Az utóbbi stratégia, a több gyártótól történő beszerzés esetén a Zero Trust technológia összetevőinek beszerzése különböző, specializált szállítóktól történik. Az egy gyártótól történő beszerzéssel ellentétben ez a stratégia különböző területekre szakosodott gyártókra támaszkodik, és így nagyobb rugalmasságot biztosít, szorosabb összhangba hozható a szervezet stratégiájával. Ezzel együtt a biztonsági szakemberek úgy látják, hogy a több gyártótól történő beszerzés költségesebb, több erőforrást igényel, és gátolja az átláthatóságot, ami végső soron kihívásokhoz vezet szállítói és költségvetési téren. (Lásd: 14. melléklet)

Bár a szervezetek nagyrészt megosztottak a kérdésben, a biztonsági döntéshozók enyhe többsége (55%) a teljes körű (egy gyártótól beszerzett) megoldásokat részesíti előnyben. (Az ausztráliai/új-zélandi szervezetek azonban az ellenkező irányba hajlanak, 52%-uk a több gyártótól történő beszerzés mellett teszi le a voksát.)

13. melléklet. Egyetlen gyártótól történő beszerzés előnyei és hátrányai – legfontosabb 2 között említettek

⊕ Egyetlen gyártótól történő beszerzés előnyei	
A szállító több megoldást átölelő, ágazatspecifikus szakértelemmel rendelkezik	24%
Több erőforrás áll rendelkezésre a Zero Trust Strategy megtervezéséhez	23%
Egyszerűsített biztonsági feladatok	22%

⊖ Egyetlen gyártótól történő beszerzés hátrányai	
Az egyetlen szállítóra való hagyatkozás növeli a sérülékenységet	34%
Összetettebb integrációt igényel a régebbi architektúrákkal	33%
Kisebb rugalmasság a speciális funkcióknál	29%

14. melléklet. Több gyártótól történő beszerzés előnyei és hátrányai – legfontosabb 2 között említettek

⊕ Több gyártótól történő beszerzés előnyei	
Rugalmasság a Zero Trust Strategy összetevőihez illő legjobb megoldások keresésében	33%
A megoldás szorosabban összehangolható a szervezet architektúrájával vagy stratégiájával	30%
Különböző gyártókkal több lehetőség az innovációra	26%

⊖ Több gyártótól történő beszerzés hátrányai	
Nagyobb költségek	29%
Az adatok nem oszthatók meg különböző megoldások között	26%
A belső csapatoknak számos megoldást kell bevezetniük és kezelniük	26%

Záró gondolatok

Mivel a biztonsági kockázatok nemcsak egyre gyakoribbak, hanem jellegükben egyre aljasabbá is válnak, a vállalkozások a különböző piacokon és iparágakban a Zero Trust Strategyt választják, amely a „soha ne bízz, mindig ellenőrizz” alapelvre épül. A Zero Trust Strategy a legfőbb biztonsági prioritás azon szervezetek számára, amelyek célja az általános biztonsági helyzetük, a végfelhasználói élmény és a hatékonyság javítása, a biztonsági eljárások egyszerűsítése a dolgozók számára, valamint a költségek csökkentése. Bár a Zero Trust Strategy előnyei jól ismertek, a korlátozott erőforrások és a vezetők szkepticizmusa a modell egyetemes bevezetésének útjában állnak.

A Zero Trust Strategy bevezetése az elmúlt három évben, részben a COVID-19 világjárvány miatt, felgyorsult. Lényeges szerepet játszik, hogy a távoli és hibrid munkavégzésre történő átállás ösztönzi a Zero Trust megközelítések szélesebb körű bevezetését, ezek ugyanis a rendszerek és adatok védelmét ígérik még arra az esetre is, ha a dolgozók az irodán kívül, esetenként saját személyes eszközeik használatával férnek hozzájuk. A COVID miatt felgyorsult bevezetés jó előrejelzője, hogy a Zero Trust modellre való általános felkészültség milyen szinten áll, mivel a stratégiát a világjárvány idején bevezető szervezetek több biztonsági kockázati területen vezették be a modellt, mint a társaik.

Ezzel együtt azoknak is van még tennivalójuk, akik élen járnak a Zero Trust Strategy bevezetésében, a vállalatok a Zero Trustra való saját felkészültségükkel kapcsolatos téves elképzelései pedig olyan sebezhetőségeket hagyhatnak maguk után, amelyekről ezek a cégek nem is tudnak.

A cégek többsége a különböző piacokon úgy véli, hogy a Zero Trust Strategy fontossága idővel csak növekedni fog, és ennek megfelelően a költségvetésük bővülésére számítanak. A prioritásokban várhatóan bekövetkező váltás különösen fontos a nem amerikai piacok számára, ahol a költségvetési korlátok jelentős akadályai a bevezetésnek. A teljes körű bevezetésre való törekvés pénzügyi és logisztikai szempontból is megterhelő lehet; ennek ellenére a Zero Trust megközelítés előnyei tagadhatatlanok, és a Microsoft ott lesz, hogy segítse és támogassa a cégeket, amelyek belevágnak ennek a szép jövő előtt álló határterületnek a meghódításába.

Ha többet szeretne megtudni a Zero Trust modellről, és felmérné vállalkozása felkészültségét a Zero Trusttal kapcsolatban, látogasson el a következő oldalra:

aka.ms/zerotrust

Részletes kutatási célkitűzések és célközönség toborzása

A kutatás célkitűzései a következők voltak:

A Zero Trust megközelítések jelenlegi állapotának megértése

A Zero Trust megközelítések bevezetésével kapcsolatos gondolkodásmódok, bevált módszerek, előnyök és kihívások feltárása

A Zero Trust megközelítések jövőjének vizsgálata

A Zero Trust megközelítés újításainak és trendjeinek kontextusba helyezése

Az átvilágítási kritériumok alapján a biztonsági döntéshozóknak a következőknek kell megfelelniük:

Felelősség a szervezet biztonságáért, ideértve a kiberbiztonságot, a biztonsági műveleteket, a fenyegetésekkel szembeni védelmet, az identitáskezelést, a kockázatkezelést, az alkalmazásbiztonságot, a digitális kriminalisztikát és az incidensekre való reagálást

Teljes munkaidős alkalmazott egy nagyvállalati szintű cégnél (1000+ alkalmazott az USA-ban, 500+ alkalmazott DE/JP/AU/NZ cég esetén)

25–75 közötti korosztály

Ismeri a Zero Trustot

Részvétel a Zero Trust Strategy fejlesztésével és bevezetésével kapcsolatos döntésekben

A 2021. áprilisi kutatási szakaszban megkérdezett 911 biztonsági döntéshozó közül:

Az USA-ban 477 biztonsági döntéshozót kérdeztünk meg

Németországban 201 biztonsági döntéshozót kérdeztünk meg

Ausztráliában/Új-Zélandon 126 biztonsági döntéshozót kérdeztünk meg

Japánban 107 biztonsági döntéshozót kérdeztünk meg

Megjegyzés: A kutatás a COVID-19 világjárvány idején történt, amely a terjedés/visszaszorulás különböző fázisaiban tartott.

© Hypothesis Csoport 2021. © Microsoft 2021.
Minden jog fenntartva. 21.07.

Microsoft Security hypothesis