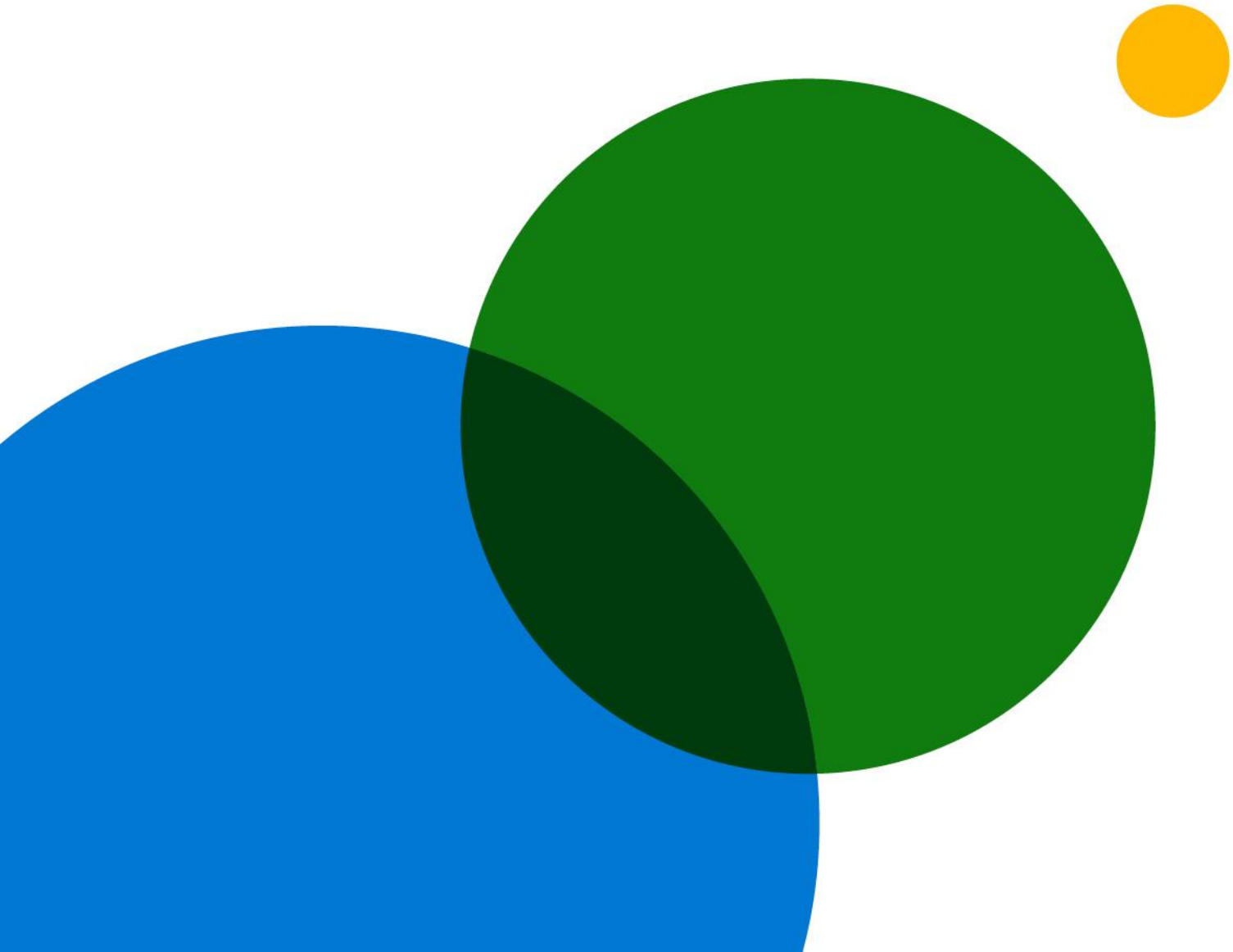
Microsoft Security

hypothesis

Zero Trust-rapport: så har strategin införts



Innehåll

Inledning

Vasu Jakkal / Corporate Vice President, Security, Compliance and Identity

Under det senaste året har det skett en anmärkningsvärd utveckling inom cybersäkerhet. Under denna tid Zero Trust också blivit en vägledande strategi för vår bransch och organisationer runt om i världen.

När pandemin bröt ut tömdes arbetsplatserna nästan omedelbart på folk. Denna omställning tvingade många organisationer att snabbt anpassa sig, så att medarbetarna kunde arbeta på det sätt de kunde – med sina egna enheter, samarbeta via molntjänster och dela data utanför företagets nätverk. Under denna omställning var de också tvungna att hantera sofistikerade cyberbrottslingar som ständigt kom med nya sätt för att hitta sina mål, utveckla sin taktik och skaffa nya resurser.

I dag har hybridarbete blivit en självklarhet. Mot denna bakgrund, och ställda inför snabba förändringar, har de organisationer som ingått i undersökningen berättat hur de förlitar sig på Zero Trust för att öka säkerheten och uppnå en smidigare regelefterlevnad. De använder också strategin för att snabbare kunna identifiera och avhjälpa hot, samt oftare och enklare utföra mer omfattande säkerhetsanalyser.

Den omfattande Zero Trust-arkitekturen baseras på principerna om uttrycklig verifiering, minsta privilegierad åtkomst och att förutsätta intrång. På så sätt kan man skapa ett skydd inom och mellan identiteter, slutpunkter, appar, infrastruktur, nätverk och data, tillsammans med ökad synlighet, automatisering och orkestrering. Vi rekommenderar inte bara detta tillvägagångssätt för våra kunder och partner, vi använder också själva denna strategi för global säkerhet och programvaruutveckling här på Microsoft.

I den här rapporten belyser vi hur Zero Trust kommit att användas på olika marknader och i olika branscher. Vår förhoppning är att lärdomarna och slutsatserna från denna undersökning kan bidra till att du snabbare kan börja tillämpa din egen Zero Trust-strategi. Vi vill också uppmärksamma de framsteg som gjorts hos andra i branschen och ge insikter om vad som händer i framtiden inom detta område som ständigt förändras.

Metodik

Microsoft gav Hypothesis Group – en insikts-, design- och strategibyrå – i uppdrag att genomföra en undersökning som skulle ligga till grund för denna rapport om hur organisationer infört en Zero Trust-strategi. Undersökningen omfattade två faser i USA som skulle belysa trender och drivkrafterna för att införa Zero Trust-strategin. I en andra fas, där globala trender skulle lyftas fram, tillkom ytterligare marknader.

Den första undersökningen genomfördes under augusti 2020, då en 15-minuters onlineenkät genomfördes i USA med 300 beslutsfattare inom säkerhet. Kravet på respondenterna vara att de skulle ha arbetat med att ta fram beslut om Zero Trust-strategier på företag från en rad olika branscher. Utöver onlineenkäten genomfördes fem djupintervjuer online under september månad 2020 bland amerikanska beslutsfattare inom säkerhet från ett flertal branscher.

I april 2021 genomfördes en global undersökning i USA, Tyskland, Japan och Australien/Nya Zeeland i en liknande grupp beslutsfattare inom säkerhet. Över 900 deltagare gick igenom 15-minutersenkäten med frågor kring hur de hade infört en Zero Trust-strategi, bästa praxis, fördelar, utmaningar och hur de planerade investera i framtiden.

Bra att veta om att införa en Zero Trust-strategi

01 / Organisationer är beredda att kapitalisera på sin Zero Trust-strategi, vilken påskyndats av omställningen till en hybridarbetsplats och Covid-19

Beslutsfattare inom säkerhet menar att deras viktigaste säkerhetsåtgärd är att utveckla en Zero Trust-strategi, och 96 procent säger att det är en fråga som är avgörande för organisationens framgång. De främsta drivkrafterna för att införa en Zero Trust-strategi är att förbättra det övergripande säkerhetsläget och slutanvändarnas upplevelse. Omställningen till en hybridarbetsplats, vilket påskyndats av COVID-19, driver också på införandet av en Zero Trust-strategi: 81 procent av företagen har börjat ställa om mot en hybridarbetsplats, och 31 procent är helt klara. Däremot är dock 94 procent oroade över omställningen, främst beroende på farhågor om att den kan missbrukas av de anställda, större arbetsbelastning för IT-funktionen och risken för cyberangrepp. Med tanke på detta finns det flera viktiga åtgärder som behöver vidtas innan en sådan strategi införs. Medarbetarna behöver utbildning och det krävs multifaktorautentisering (MFA) för att säkerställa en smidig användarupplevelse och omställning.

02 / Med en Zero Trust-strategi får organisationer en flexibilitet att först påbörja implementeringen och sedan skräddarsy den efter behov

Färre än 15 procent av organisationerna började sin implementering av Zero Trust-strategin inom samma säkerhetsriskområde. Detta beror till stor del på att implementeringen utförs som en komplett process mellan pelare och funktioner i säkerhetsarkitekturen, och inte som en serie skilda och individuella tekniker. Det varierar också ganska mycket i vilken ordning som enskilda komponenter i Zero Trust implementeras inom ett säkerhetsriskområde. Det kan skilja sig betydligt mellan olika säkerhetsexperter vilka komponenter de väljer att implementera först.

03 / Trots att många redan har börjat införa en Zero Trust-strategi, och att den förbättrar organisationernas förmåga att hantera hot, finns det fortfarande mycket kvar att göra

76 procent av organisationerna har åtminstone börjat implementera en Zero Trust-strategi, medan 35 procent hävdar att den är helt implementerad. De som påstår sig ha genomfört en fullständig implementering medger dock att de inte har slutfört implementeringen av Zero Trust-strategin inom alla säkerhetsriskområden och komponenter. Zero Trust-strategin är tilltalande eftersom den ger ökad agilitet, det går snabbare att identifiera hot och organisationen får en bättre förmåga att hantera säkerheten för Sakernas Internet (IoT) och driftteknik (OT). Antalet organisationer som inför strategin ökar i USA (70 procent i augusti 2020 till 79 procent i april 2021). USA ligger också långt fram när det gäller Zero Trust-implementering i förhållande till andra länder som börjat införa strategin senare. Organisationer i USA hävdar också att de är mindre begränsade i sina budgetar. Samtidigt som 57 procent av organisationerna hävdar att de ligger före andra när det gäller införande, har ungefär hälften av dem fortfarande mer arbete kvar att göra eftersom de inte har implementerat Zero Trust fullt ut inom alla säkerhetsriskområden och säkerhetskomponenter.

04 / Om man tittar framåt kommer Zero Trust-strategin fortfarande ha högsta prioritet och kräva noggranna beslut gällande medarbetare och leverantörer

Zero Trust-strategin förväntas har fortsatt högsta säkerhetsprioritet två år framåt, och organisationerna räknar med att öka sina investeringar. För att kunna övervinna de utmaningar medarbetarna utgör (inklusive förstärkning av säkerhetsteamen och ledningens engagemang) måste investeringarna i Zero Trust fördubblas. När det gäller leverantörsstrategier föredrog beslutsfattarna i viss mån att arbeta med heltäckande eller konsoliderade leverantörer, eftersom valet av leverantör ofta är beroende av tillgången på intern expertis. Fördelarna med att välja en komplett lösning är bland andra tillgången till expertkunskaper och resurser samt enkelheten, även om implementeringen kan ta längre tid. Lösningen kan dock vara svårare att integrera i den befintliga säkerhetsarkitekturen och öka den potentiella sårbarheten.

Dessa pratade vi med

Globalt

*Över 1 000 anställda i USA, över 500 anställda i Tyskland, Japan, Australien/Nya Zeeland

Övergripande slutsatser

Organisationer är beredda att kapitalisera på sin Zero Trust-strategi

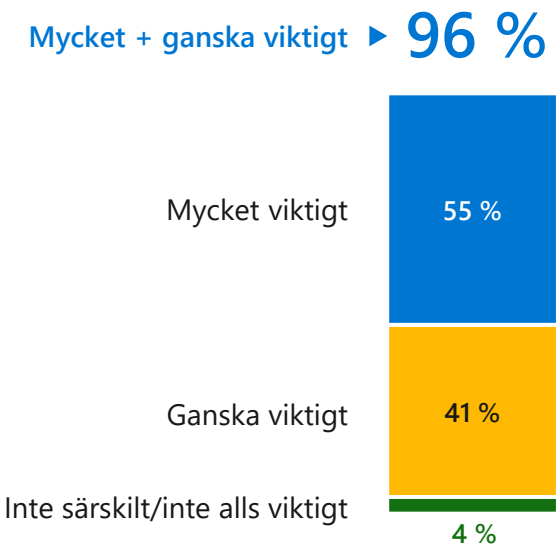
Zero Trust-strategin har högsta säkerhetsprioritet på i princip alla marknader och inom alla branscher, där ett antal organisationer infört en Zero Trust-strategi de senaste åren. Även om Zero Trust är en fråga högt på dagordningen för de flesta (53 procent), är den särskilt högt prioriterad för organisationer i USA (56 procent) och Tyskland (53 procent).

Nästan alla säkerhetsexperter (96 procent) anser att en Zero Trust-strategi är avgörande för organisationens framgång. (Se bevis 1) Förutom att förstärka det övergripande säkerhetsläget och förbättra slutanvändarnas upplevelse, vill säkerhetsexperterna använda Zero Trust-strategin för att förenkla säkerhetsrutinerna för medarbetarna. (Se bevis 2)

Som en amerikansk beslutsfattare som arbetar med säkerhet inom besöksnäringen uttrycker det: *"Målet är att förbättra det totala säkerhetsläget, men det handlar minst lika mycket om att göra det smidigare och enklare för slutanvändarna."*

Dessutom menade 31 procent av säkerhetsexperterna att en Zero Trust-strategi var ett viktigt verktyg i den förestående omställningen till en hybridarbetsplats efter pandemin. Denna drivkraft är särskilt framträdande i Australien/Nya Zeeland (44 procent).

Bevis 1. Betydelsen av Zero Trust



Bevis 2. Drivkrafter bakom Zero Trust

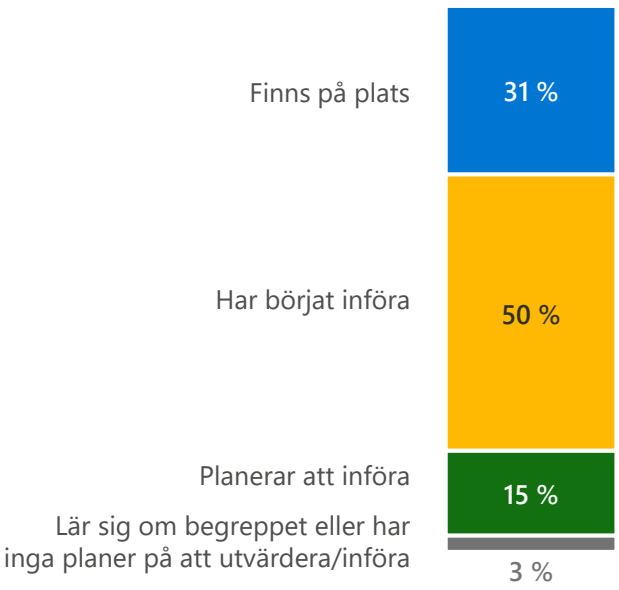
De främsta drivkrafterna	
Förbättra det sammantagna säkerhetsläget	47 %
Förbättra slutanvändarnas upplevelse och produktivitet	44 %
Förändra hur säkerhetsteam arbetar tillsammans	38 %
Förenkla säkerhetsstacken	35 %
Minska säkerhetskostnaderna	35 %

Omställningen till en hybridarbetsplats driver införandet av Zero Trust-strategi

81 procent av alla organisationer har börjat ställa om till en hybridarbetsplats, där 31 procent redan har gjort det helt och hållet. Det skiljer sig dock åt en hel del mellan olika marknader: Australien och Nya Zeeland har kommit längst med 37 procent, Tyskland ligger långt efter där bara 20 procent av organisationerna har ställt om till en hybridmodell. (Se bevis 3)

De olika marknaderna ställer om till en hybridarbetsplats i olika takt, men den stora majoriteten (91 procent) av organisationerna som inte har genomfört omställningen förväntar att de gjort så inom de kommande fem åren. Men vad som är anmärkningsvärt är att 94 procent oroar sig inför omställningen. De främsta farhågorna gäller eventuellt missbruk från de anställdas sida, en ökad arbetsbelastning på IT-funktionen och större risk för cyberangrepp. (Se bevis 4)

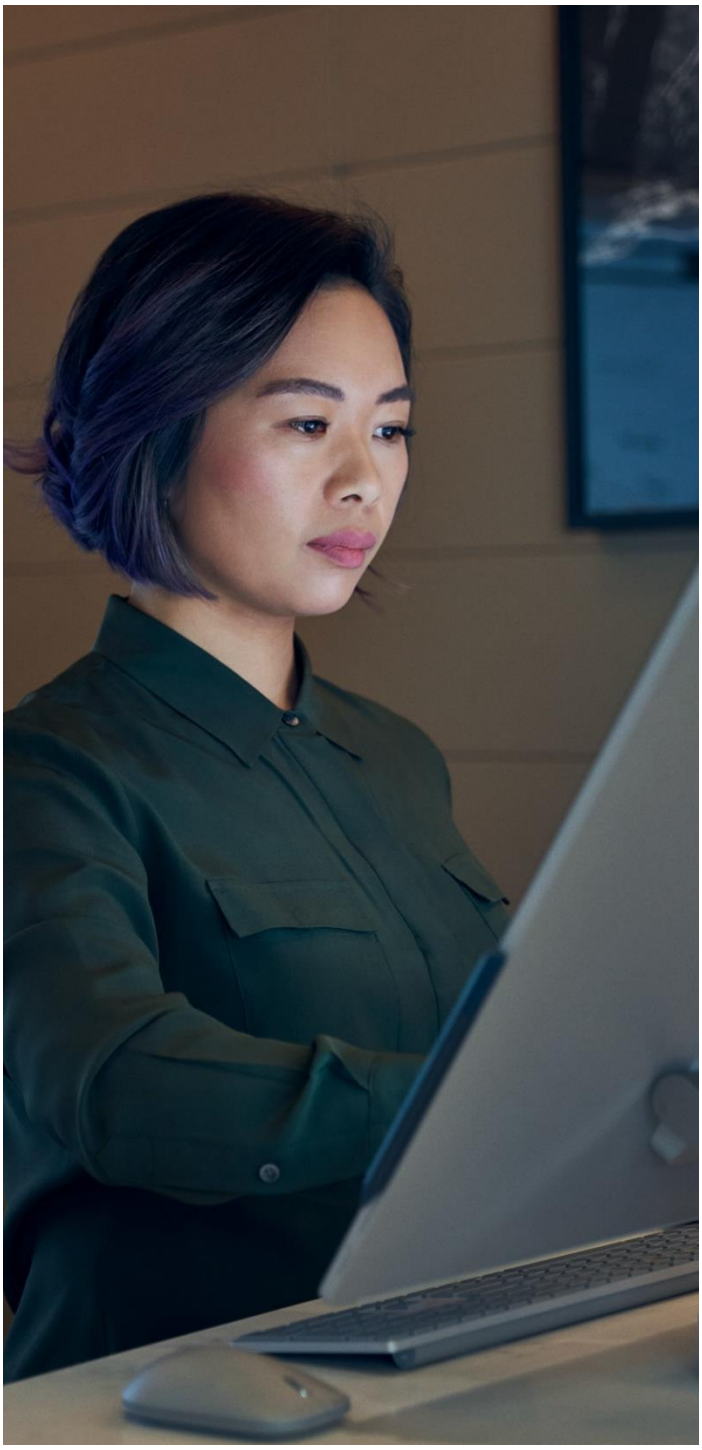
Bevis 3. Omställning till en hybridarbetsplats



Bevis 4. Farhågor inför en hybridarbetsplats

Anställda laddar ned osäkra appar	37 %
Större belastning på IT-funktionen	37 %
Angrepp av utpressningsprogram	36 %
Nätfiskeattacker	35 %
Felaktig användning av personliga enheter	34 %
Ej auktoriserad dataåtkomst	31 %
Oförmåga att hantera alla enheter	30 %
Användning av personliga e-postkonton	30 %
Bristande efterlevnad av dataförordningar	24 %

Covid-19 har påskyndat planerna på att ställa om till en Zero Trust-strategi



För att minimera eventuella problem lyfter intressenterna fram betydelsen av mer utbildning för medarbetare (54 procent) (särskilt i Japan (61 procent) och Tyskland (58 procent)) och multifaktorautentisering (MFA) (50 procent) (särskilt i USA (52 procent) och Tyskland (56 procent)) för att säkerställa en smidig användarupplevelse och övergång.

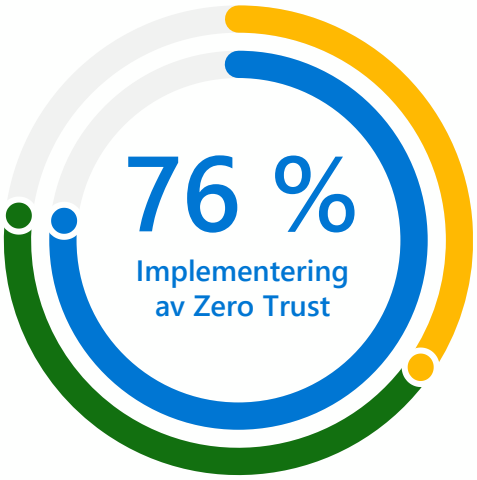
Eftersom distans- och hybridarbete kan utföras säkrare med en Zero Trust-strategi på plats, har COVID-19 påskyndat införandet av en sådan strategi för 72 procent av organisationerna, även om det ser olika ut på olika marknader. Pandemin satte verkligen fart på införandet av en Zero Trust-strategi för cirka 7 av 10 organisationer i USA (76 procent), Japan (71 procent) och Australien/Nya Zeeland (69 procent), men implementeringen har varit betydligt lägre i Tyskland (62 procent). Detta kan eventuellt bero på en långsammare omställning till en hybridarbetsplats.

Zero Trust har implementerats på många håll i världen och intresset växer i USA

Zero Trust är inte bara ett modeord – det är på riktigt. 76 procent av organisationerna har åtminstone börjat implementera denna strategi och 35 procent anser att de genomfört den fullt ut. Dessa siffror ger dock en alltför optimistisk bild, eftersom många organisationer som anser sig vara fullt implementerade inte är färdiga inom alla säkerhetsriskområden. I dag ligger USA steget före gällande införandet av en Zero Trust-strategin i förhållande till andra marknader, och det växer fortfarande snabbt. I augusti 2020 hade 70 procent av organisationerna i USA infört en Zero Trust-strategi, vilket på bara åtta månader ökade till 79 procent. (Se bevis 5)

Frågan om Zero Trust-strategi dominerar numera säkerhetsområdet, vilket är en stor förändring. 82 procent av företagen har implementerat Zero Trust-strategier under de senaste tre åren, och 21 procent har gjort det under de senaste 12 månaderna. Med detta sagt började 26 procent av organisationerna i USA med implementeringen för mer än 3 år sedan, jämfört med 19 procent av de japanska organisationerna, 6 procent av organisationerna i Australien/Nya Zeeland och 3 procent av organisationerna i Tyskland. Att implementeringen började tidigare i USA – parallellt med färre budgetbegränsningar – kan vara en bidragande orsak till varför organisationer i USA ligger före i Zero Trust-införandet jämfört med organisationer på andra marknader. Att införandet av Zero Trust är så pass lågt i Tyskland kan bero på att 97 procent av de tyska organisationerna inte började med sin implementeringen förrän för tre år sedan.

Bevis 5. Implementering av Zero Trust



	USA (2020)	USA	DE	JP	AUS/NZ
Implementering av Zero Trust	70 %	79 %	75 %	76 %	71 %
• Helt genomförd	27 %	44 %	19 %	32 %	28 %
• Pågår	43 %	35 %	56 %	44 %	43 %

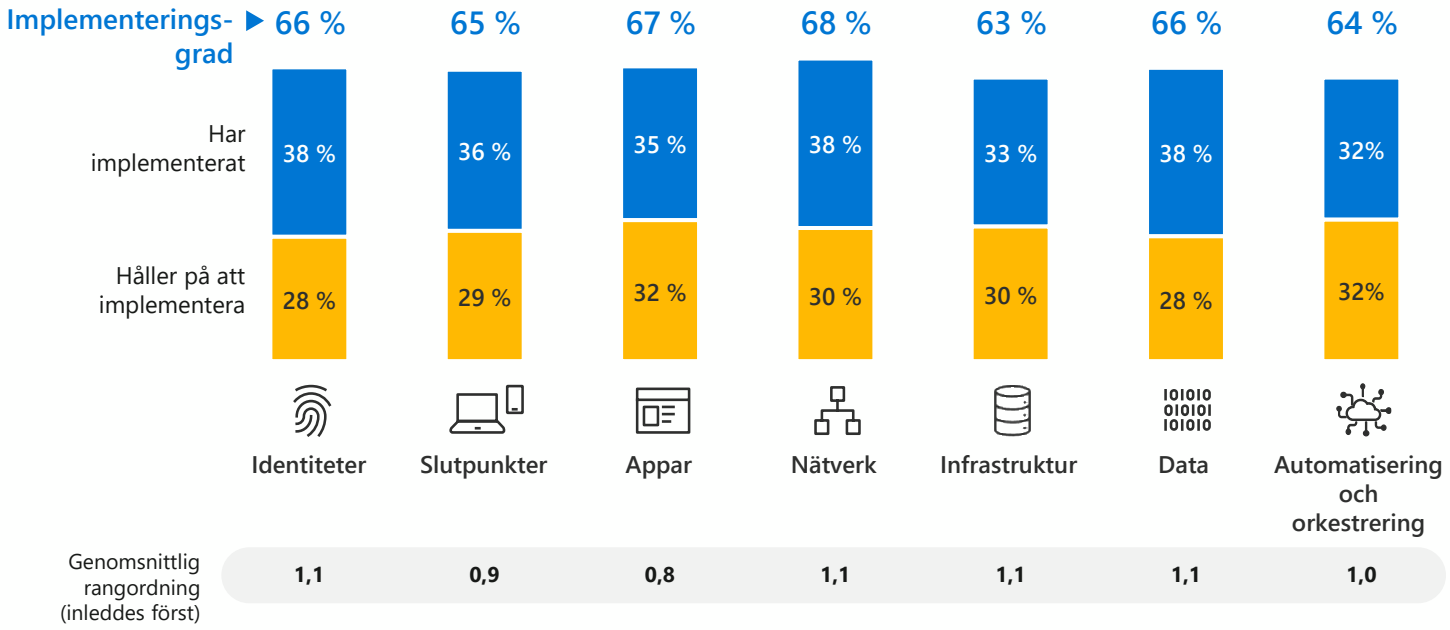
- 35 procent helt genomförd
- 42 procent har en pågående implementering

Det finns ingen metod för Zero Trust-implementering som passar alla, vilket innebär att man kan börja var som helst

Inget enskilt säkerhetsriskområde (identiteter, slutpunkter, appar, nätverk, infrastruktur, data, automatisering och orkestrering) sticker ut som en primär startpunkt för en Zero Trust-strategi. Färre än 15 procent av de tillfrågade har inlett sin implementering inom samma säkerhetsriskområde. Organisationerna börjar inom olika områden, eftersom de troligen gör det utifrån sina olika behov och tillgängliga interna resurser. De inför sedan sin Zero Trust-strategi allt eftersom inom alla säkerhetsriskområden för att uppnå bättre skydd mot olika hot. Zero Trust uppfattas därför som en komplett strategi som kan införas över tiden. (Se bevis 6)

Utöver säkerhetsriskområdena i en Zero Trust-strategi, måste organisationerna också identifiera vilka enskilda komponenter inom respektive säkerhetsriskområde som bör prioriteras. För slutpunkter, appar, nätverk, data och automatisering/orkestrering finns det ingen tydlig startpunkt. Vilka komponenter som säkerhetspersonal prioriterar högst varierar avsevärt. Stark autentisering implementeras dock vanligtvis före identiteter, och verktyg för hotidentifiering har ofta hög prioritet inom området Infrastruktur. (Se bevis 7)

Bevis 6. Aktuell implementering av Zero Trust – säkerhetsriskområden



Bevis 7. Komponent vid Zero Trust-implementering (topp 3) – prioriteras högst (implementeras först)

Identiteter	
Stark autentisering (det vill säga multifaktorautentisering, autentisering utan lösenord)	32 %
Automatisk riskidentifiering och motåtgärder	27 %
Adaptiva åtkomstprinciper för att förhindra åtkomst till resurser	22 %

Slutpunkter	
Policyer/kontroller för skydd mot dataförlust för alla ohanterade och hanterade enheter	27 %
Riskutvärdering av enheter i realtid/ skydd mot hot mot slutpunkter	26 %
Registrering av enheter med identitetsprovider	24 %

Appar	
Löpande identifiering av skugg-IT och riskbedömning	23 %
Detaljerad åtkomstkontroll till dina appar (till exempel begränsad synlighet eller skrivskydd)	22 %
Policybaserad åtkomstkontroll för appar	20 %

Nätverk	
Kontroller för säker åtkomst för att skydda nätverk	25 %
Hotskydd och filtrering med sammanhangsbaserade signaler	24 %
All trafik krypteras	20 %

Infrastruktur	
Åtkomst för säkerhetsteam till verktyg för hotidentifiering	25 %
Skydd för laster i molnet för både hybridmiljöer och modeller med flera moln	19 %
Detaljerade kontroller för synlighet och åtkomst för alla laster (virtuella maskiner, servrar och så vidare)	17 %

Data	
Åtkomstbeslut regleras genom en säkerhetspolicymotor	21 %
Data klassificeras och märks	21 %
De känsligaste filerna skyddas kontinuerligt med kryptering	20 %

Automatisering och orkestrering	
Komplett synlighet etableras med en centraliserad plattform för utredning och åtgärd	29 %
Hotdata samlas in och analyseras från alla domäner (identiteter, slutpunkter, appar, nätverk, infrastruktur)	28 %
Automatiserad utredning och åtgärder har aktiverats	22 %

Vi betraktade det inte som bara en serie tekniker, utan som en strategi och metod för att behandla alla användarresurser, oavsett om de fanns i eller utanför nätverket, som opålitliga tills de kunde verifieras.”

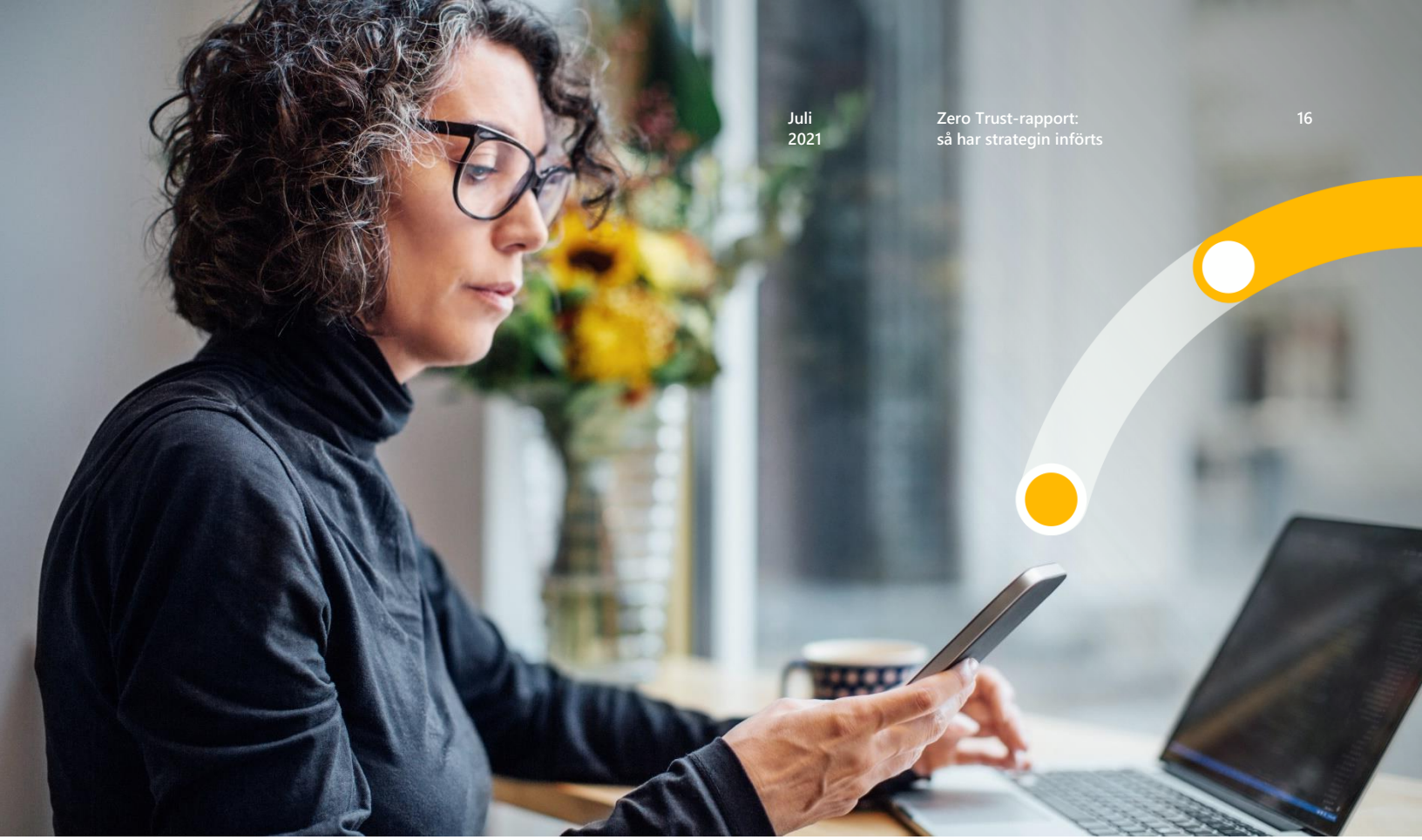
Beslutsfattare i USA inom säkerhet inom besöksnäringen

När organisationer väl började implementera en Zero Trust-strategi ansågs de främsta fördelarna vara ökad agilitet, snabbhet och skydd. Resursfördelar var mindre vanliga.

När Zero Trust-strategin väl implementerats kunde organisationerna dra nytta av ökad agilitet (37 procent), snabbhet (35 procent) och skydd av kunddata (35 procent). (Se bevis 8) Omedelbara fördelar för personalen, inklusive att frigöra tid för säkerhetsteamen (27 procent) och att färre resurser behövdes för att hantera infrastrukturen (22 procent), var mindre vanligt förekommande.

Men det är också viktigt att framhålla att organisationerna var övertygade om att deras Zero Trust-strategi kunde hjälpa dem hantera de flesta hot mot och förändringar i miljön, särskilt när det gällde IoT- och OT-säkerhet (47 procent).

Bevis 8. Fördelar med Zero Trust



Organisationer menar att de får ut mesta möjliga av sin Zero Trust-strategi

79 procent känner sig på det stora hela trygga i sin förmåga att hantera säkerhetshot, även om övertygelsen minskar när hotet innebär en ”påhittad sanning”. Beslutsfattare inom säkerhet känner sig minst säkra på att hantera hot som omfattar syntetiska identiteter (20 procent) och deepfakes – som fejkade videor (10 procent).

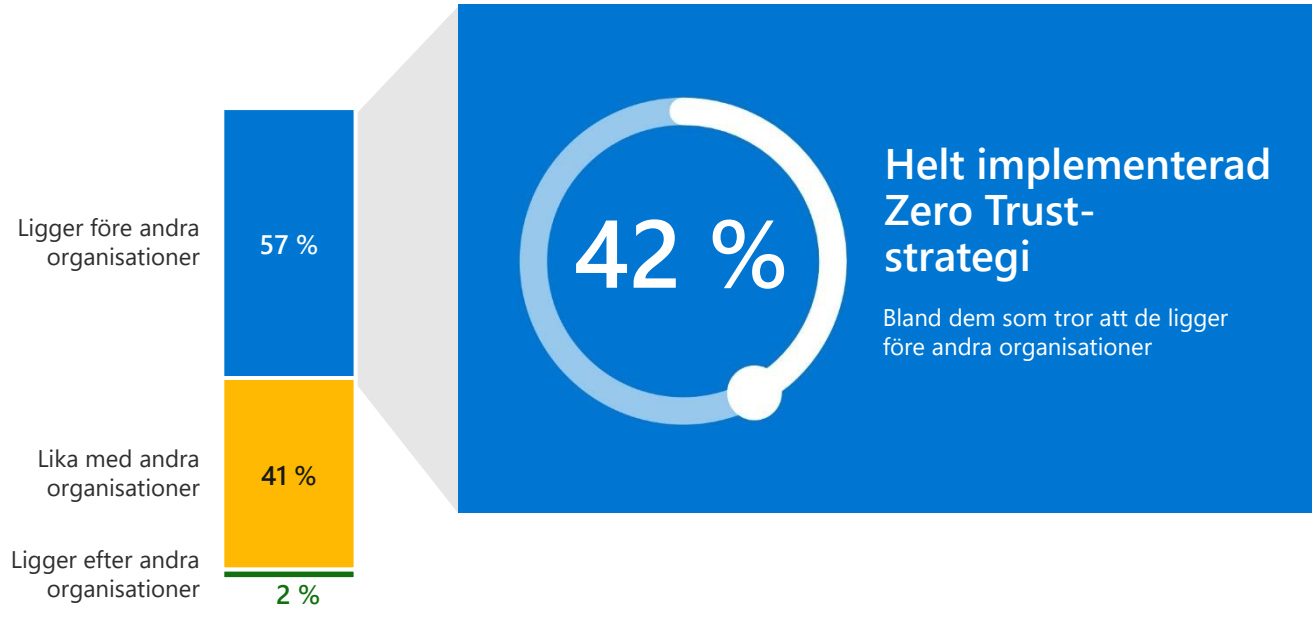
Men med tanke på fördelar som finns med Zero Trust är dock uppfattningen i allmänhet positiv. På de fyra undersökta marknaderna ser beslutsfattarna sina organisationers strategi både som praktisk och ambitiös. De beskriver den som trygg (37 procent) och effektiv (31 procent) samt motiverande (25 procent), inspirerande (25 procent) och spännande (25 procent). Särskilt i Japan beskriver säkerhetsexperterna Zero Trust som både krävande (27 procent) och omvandlande (25 procent), vilket tyder på att fördelarna med strategin är långtgående när den väl har införts – även om den inte varit alldeles lätt att implementera.

Många tror att de ligger steget före med sin Zero Trust-implementering, men de har fortfarande mycket kvar att göra

Det är bara 35 procent av organisationerna som har infört sin Zero Trust-strategi fullt ut. Trots detta menar 52 procent att de har hunnit längre än vad de planerat och 57 procent tror att de hunnit längre än andra organisationer. Särskilt i Japan (66 procent) och Australien/Nya Zeeland (63 procent) tror sig organisationerna ha hunnit längre än andra. Uppfattningen skiftar mellan olika marknader, men det verkar finnas ett gap mellan tro och verklighet: bland dem som menar att de ligger för andra organisationer hävdar bara 42 procent att de har genomfört sin Zero Trust-strategi fullt ut. (Se bevis 9)

Trots att många organisationer känner sig trygga i sin Zero Trust-strategi och beredda på att hantera framtida säkerhetshot, finns det fortfarande mycket kvar att göra innan implementeringen är helt klar inom alla riskområden. Bland de organisationer som anser att deras Zero Trust-strategi har genomförts fullt ut, har till exempel nästan hälften inte implementerat den inom alla säkerhetsriskområden. Infrastruktur och identiteter är de områden där implementeringen har fått vänta.

Bevis 9. Jämförelse av Zero Trust-implementering



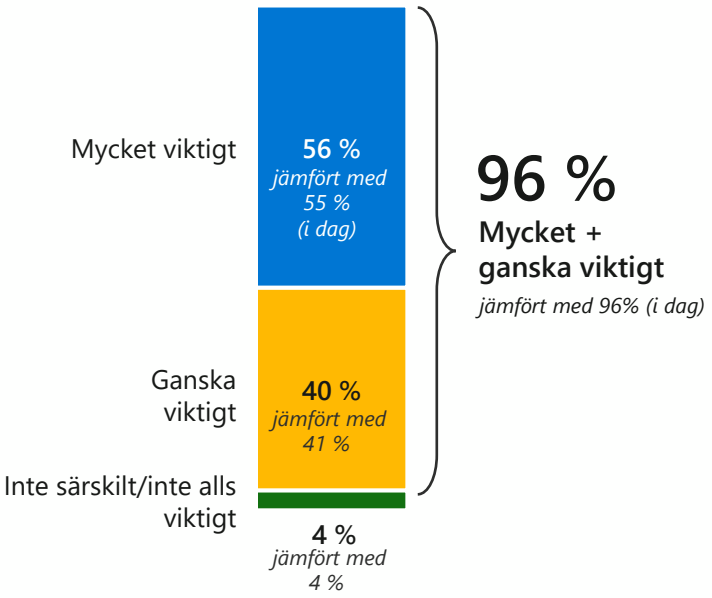
	USA	DE	JP	AUS/NZ
Före	59 %	46 %	66 %	63 %
Lika	40 %	52 %	34 %	32 %
Efter	2 %	2 %	0 %	6 %

Om vi blickar framåt mot de kommande två åren kommer en Zero Trust-strategi fortsatt vara en högt prioriterad säkerhetsåtgärd

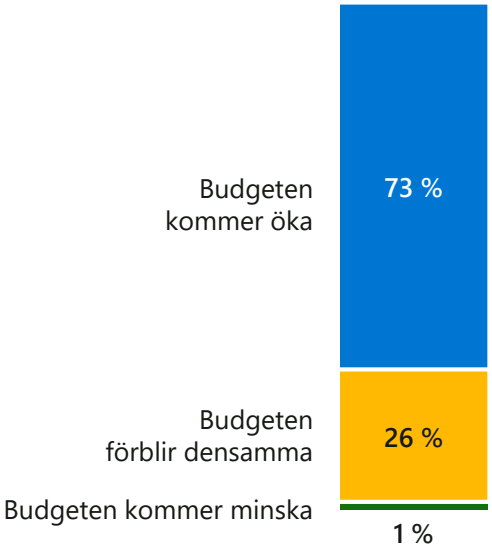
Organisationer är helt införstådda med vikten av en Zero Trust-strategi, och beslutsfattarna menar denna säkerhetsåtgärd kommer fortsätta ha högsta prioritet under de kommande två åren. Den relativa betydelsen av Zero Trust-strategin som säkerhetsåtgärd beräknas öka (53 procent till 58 procent) till 2023, eftersom beslutsfattarna räknar med att strategin kommer förbli avgörande för organisationens framgång på det stora hela (96 procent). (Se bevis 10)

Den förväntade betydelsen är särskilt hög hos japanska organisationer, där 70 procent säger att Zero Trust-strategin kommer vara mycket viktig under de kommande två åren jämfört med det totala genomsnittet på 56 procent. Budgetarna för en Zero Trust-strategi förväntas också öka, 73 procent av alla organisationer förväntar sig att budgetarna ska öka. Denna siffra är dock något längre i Tyskland (67 procent), där 31 procent förväntar att deras budgetar kommer vara oförändrade. (Se bevis 11)

Bevis 10. Förväntad betydelse av Zero Trust de kommande två åren

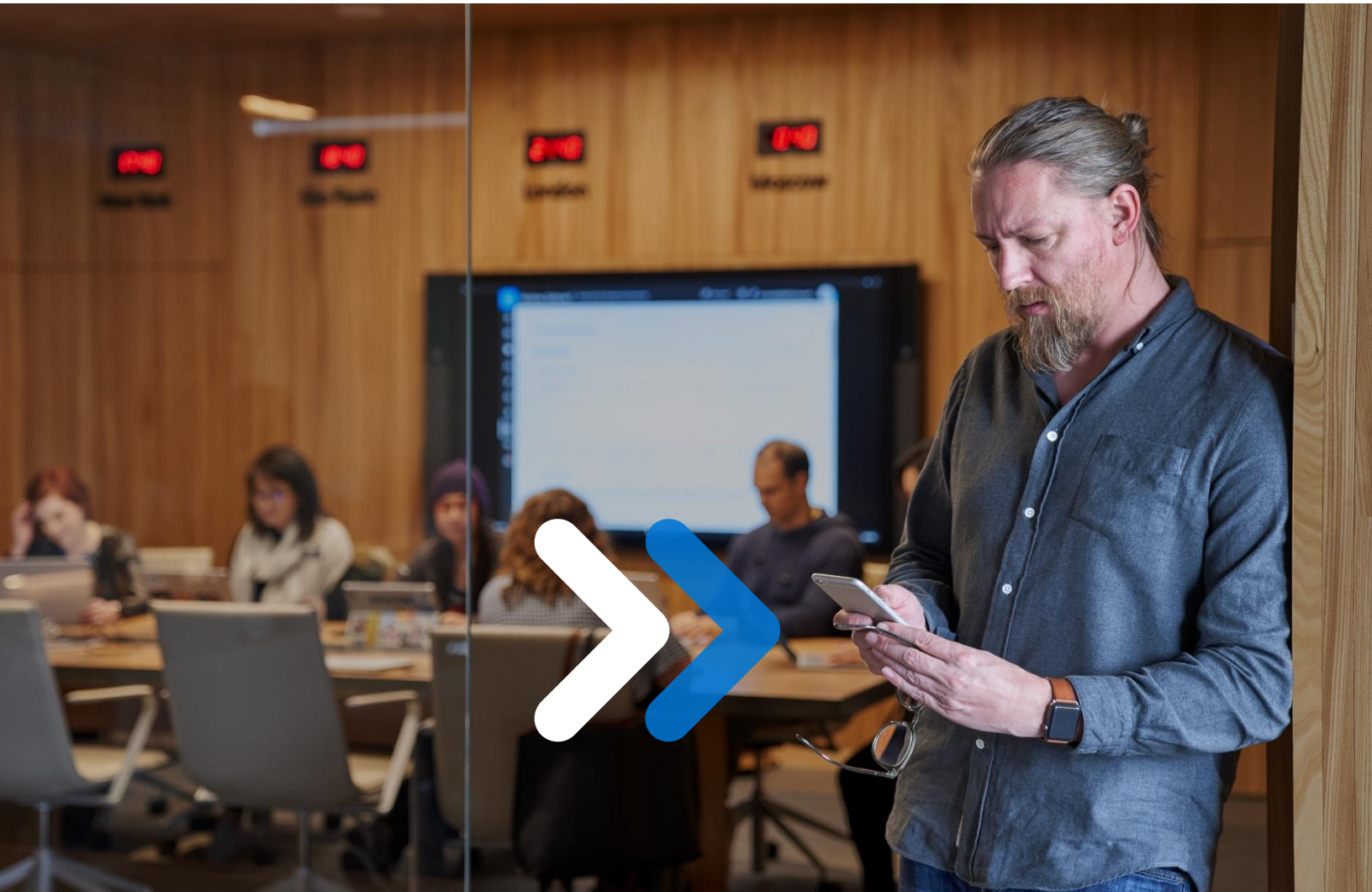


Bevis 11. Förväntad Zero Trust-budget under kommande två år



Om Zero Trust-strategin visar sig vara framgångsrik kan investeringarna öka ytterligare

Organisationer som tagit till sig Zero Trust-strategin till fullo förväntar sig att investeringarna kommer fördubblas under de kommande två åren, och de som ännu inte har börjat implementera strategin riskerar att halka efter. Dessa organisationer hamnar inte bara på efterkälken jämfört med helt implementerade organisationer när det handlar om att prioritera Zero Trust i sina säkerhetsplaner (42 procent jämfört med 66 procent) och förutse budgetökningar (66 procent jämfört med 72 procent). De känner sig också betydligt mindre säkra på hur de ska hantera IoT- och OT-säkerhet i framtiden (40 procent jämfört med 53 procent).



Att övervinna personalrelaterade utmaningar är nyckeln för en lyckad Zero Trust-investering

Trots att många organisationer uppnått snabba framgångar i att införa en Zero Trust-strategi, måste de övervinna en mängd utmaningar för att kunna gå vidare med implementeringen. (Se bevis 12) Utmaningar med resurser och ledarskap är de vanligaste inom dessa kategorier. Den tid som krävs för att genomföra Zero Trust-strategier och bristen på stöd från ledningen är de främsta hindren. Det senare är särskilt framträdande i Australien/Nya Zeeland (65 procent).

Dessutom spelar budgetbegränsningar – som 45 procent av organisationerna identifierar som ett hinder – sannolikt också en roll för utmaningar med resurser och ledarskap.

Till exempel nämner 21 procent av beslutsfattarna inom säkerhet att svårigheten att påvisa lönsamheten med Zero Trust varit ett hinder för implementeringen. En utmaning som kan göra det svårt att få ledningens stöd. Eftersom marknader utanför USA i större utsträckning uppgett budgetbegränsningar som ett problem (60 procent organisationerna i Japan, 57 procent av organisationerna i Tyskland och 57 procent av organisationerna i Australien/Nya Zeeland) kan detta i sin tur leda till en mer begränsad och långsammare implementering av Zero Trust-strategier i Japan, Tyskland och Australien/Nya Zeeland jämfört med USA.

Bevis 12. Hinder för Zero Trust

Resursutmaningar 60 %	Ledarskap 53 %	Teknik 46 %	Leverantör 46 %	Budget-begränsningar 45 %
20 % Tar för lång tid att implementera	**20 %** Brist på stöd från ledningen	**21 %** Svårt att integrera säkerhetslösningar	**21 %** Behöver implementeringsstöd från leverantörer	**21 %** Kostnaden för att implementera en Zero Trust-strategi
19 % Brist på intern förändringshantering	**19 %** Brist på stöd från intressenter	**19 %** Inkompatibilitet med äldre system	**21 %** Svårigheter att hitta rätt leverantörer	**21 %** Svårt att bevisa avkastningen på investeringen
18 % Behöver mer utbildningsmaterial	**19 %** Behöver hjälp med att visa på tydlig affärsnytta	**19 %** Svårigheter att skala ut i hela organisationen	**17 %** Oförmåga att hitta innovativa partner	**14 %** Har inte tillräckligt stor budget
17 % Behövs inte för en organisation av vår storlek	**18 %** Brist på acceptans i organisationen			
16 % Har inte rätt kompetens för att implementera				

"Det var svårt att få acceptans till en början, men när alla intressenter var överens om att vi skulle investera i det här projektet var alla med på tåget."

Beslutsfattare i USA inom säkerhet inom fintech

Beslutsfattare inom säkerhet har en viss förkärlek för heltäckande eller konsoliderade leverantörer

När det gäller leverantörsstrategin för Zero Trust ställs organisationer inför två val: ”bäst i klassen” eller ”bäst i kategorin”. Den tidigare strategin handlar om att köpa en serie produkter för hela Zero Trust-arkitekturen från en heltäckande eller konsoliderad leverantör, en lösning som beslutsfattarna menar ger mer expertkunskaper och resurser, och blir enklare att hantera för organisationer med bristande resurser. Med den här metoden kan dock sårbarheten öka och flexibilitet bli mindre. (Se bevis 13)

Den senare strategin, ”bäst i kategorin”, handlar om att skaffa enskilda teknikkomponenter inom en speciell kategori för Zero Trust från specialiserade leverantörer. Till skillnad från ”bäst i klassen” förlitar sig denna strategi på leverantörer som är specialiserade på olika områden och därmed erbjuder större flexibilitet och kan anpassa sig bättre till organisationens strategi. Säkerhetsexperter anser att ”bäst i kategorin” är dyrare, kräver mer resurser och hämmar synligheten – nackdelar som i slutändan kan leda till leverantörs- och budgetutmaningar. (Se bevis 14)

Organisationerna är ganska splittrade, men en liten majoritet av beslutsfattarna (55 procent) föredrar att arbeta med heltäckande leverantörer (”bäst i klassen”). (Organisationer i Australien/Nya Zeeland lutar sig dock åt motsatt håll, där 52 procent föredrar ”bäst i kategorin”.)

Bevis 13. Fördelar och hinder med ”bäst i klassen” – rankade som de två främsta

⊕ Fördelar med ”bäst i klassen”	
Leverantören har branschspecifika expertkunskaper om olika lösningar	24 %
Fler resurser tillgängliga för att planera Zero Trust-strategin	23 %
Förenklad säkerhetsstack	22 %

⊖ Nackdelar med ”bäst i klassen”	
Beroendet av en enda leverantör ökar sårbarheten	34 %
Kräver mer komplex integration med äldre arkitektur	33 %
Mindre flexibilitet för specialiserade funktioner	29 %

Bevis 14. Fördelar och hinder med ”bäst i kategorin” – rankade som de två främsta

⊕ Fördelar med ”bäst i kategorin”	
Flexibilitet för att hitta de bästa lösningarna för var och en av komponenterna i Zero Trust-strategin	33 %
Kan bättre anpassa lösningen till organisationens arkitektur eller strategi	30 %
Större möjligheter till innovation med olika leverantörer	26 %

⊖ Nackdelar med ”bäst i kategorin”	
Ökade kostnader	29 %
Oförmåga att dela data mellan olika lösningar	26 %
Fler lösningar att införa och hantera för de interna teamen	26 %

Efterord

Eftersom säkerhetsriskerna inte bara ökar utan också blir mer skadliga, väljer organisationer på olika marknader och branscher en Zero Trust-strategi som hjälper dem att ”aldrig lita på något och alltid verifiera”. Zero Trust-strategin är den högst prioriterade säkerhetsåtgärden för organisationer som vill förbättra sitt totala säkerhetsläge, slutanvändarnas upplevelse och produktivitet, förenkla säkerhetsrutinerna för medarbetarna och minska kostnaderna. Men även om fördelarna med en Zero Trust-strategi är uppenbara, kan begränsade resurser och ledningens tvekan stå i vägen för en bredare implementering.

Antalet organisationer som infört en Zero Trust-strategi har ökat i snabb takt under de tre senaste åren, delvis på grund av COVID-19-pandemin. Omställningen till distansarbete och en hybridarbetsplats har varit viktiga faktorer som driver på införandet av Zero Trust-strategierna, då dessa skyddar data och system även om medarbetarna ansluter till dem utifrån – och i bland från sina egna enheter. Pandemin har också medfört att antalet organisationer som infört strategin ökat i snabbare takt, och Zero Trust-beredskapen ökat totalt sätt. De organisationer som började tillämpa strategin under pandemin har också implementerat den inom fler säkerhetsriskområden än andra.

Men även de organisationer som kommit en bra bit på väg med sin Zero Trust-strategi har mycket kvar att göra. Då en hel del också har en felaktig bild av hur långt de kommit, innebär det en sårbarhet de inte är medvetna om.

En majoritet av alla organisationer på olika marknader tror att en Zero Trust-strategi kommer bli viktigare med tiden, och förväntar sig att deras budgetar i sin tur kommer att öka. Denna förväntade prioriteringsförändring är särskilt avgörande för marknader utanför USA, där budgetbegränsningar kan innebära ett stort problem. En fullständig implementering kan te sig både ekonomiskt och logistiskt överväldigande, men fördelarna med en Zero Trust-strategi obestridliga. Microsoft kan då finnas på plats för att vägleda och stötta organisationer när de inleder denna resa.

Om du vill veta mer om Zero Trust och göra en bedömning av hur långt organisationen kommit med sin Zero Trust-strategi kan du besöka

aka.ms/zerotrust

Mer om undersökningens målsättningar och målgruppsrekrytering

Undersökningen hade bland annat följande målsättningar:

Förstå det aktuella läget för Zero Trust-strategier

Identifiera tänkesätt, bästa praxis, fördelar och utmaningar med att använda Zero Trust-strategier

Utforska framtiden för Zero Trust-strategier

Kontextualisera innovationer och trender inom Zero Trust-strategier

De beslutsfattare inom säkerhet som deltog i undersökningen uppfyllde följande kriterier:

Ansvarade för säkerheten i organisationen, bland annat cybersäkerhet, säkerhetsåtgärder, hotskydd, identitetshantering, riskhantering, säkerhet för appar, digital kriminalteknik och incidenthantering

Var heltidsanställda på ett större företag (över 1 000 anställda i USA, över 500 anställda i DE/JP/AU/NZ)

25–75 år

känner till Zero Trust

Deltog i beslutsfattandet för utveckling/implementering av Zero Trust-strategin

Fördelning av de 911 beslutsfattare inom säkerhet som intervjuades under undersökningsfasen i april 2021:

I USA intervjuades 477 beslutsfattare

I Tyskland intervjuades 201 beslutsfattare

I Australien/Nya Zeeland intervjuades 126 beslutsfattare

I Japan intervjuades 107 beslutsfattare

Obs: Undersökningen genomfördes under den globala COVID-19-pandemin, som befann sig i olika skeden i spridningen

Microsoft Security hypothesis