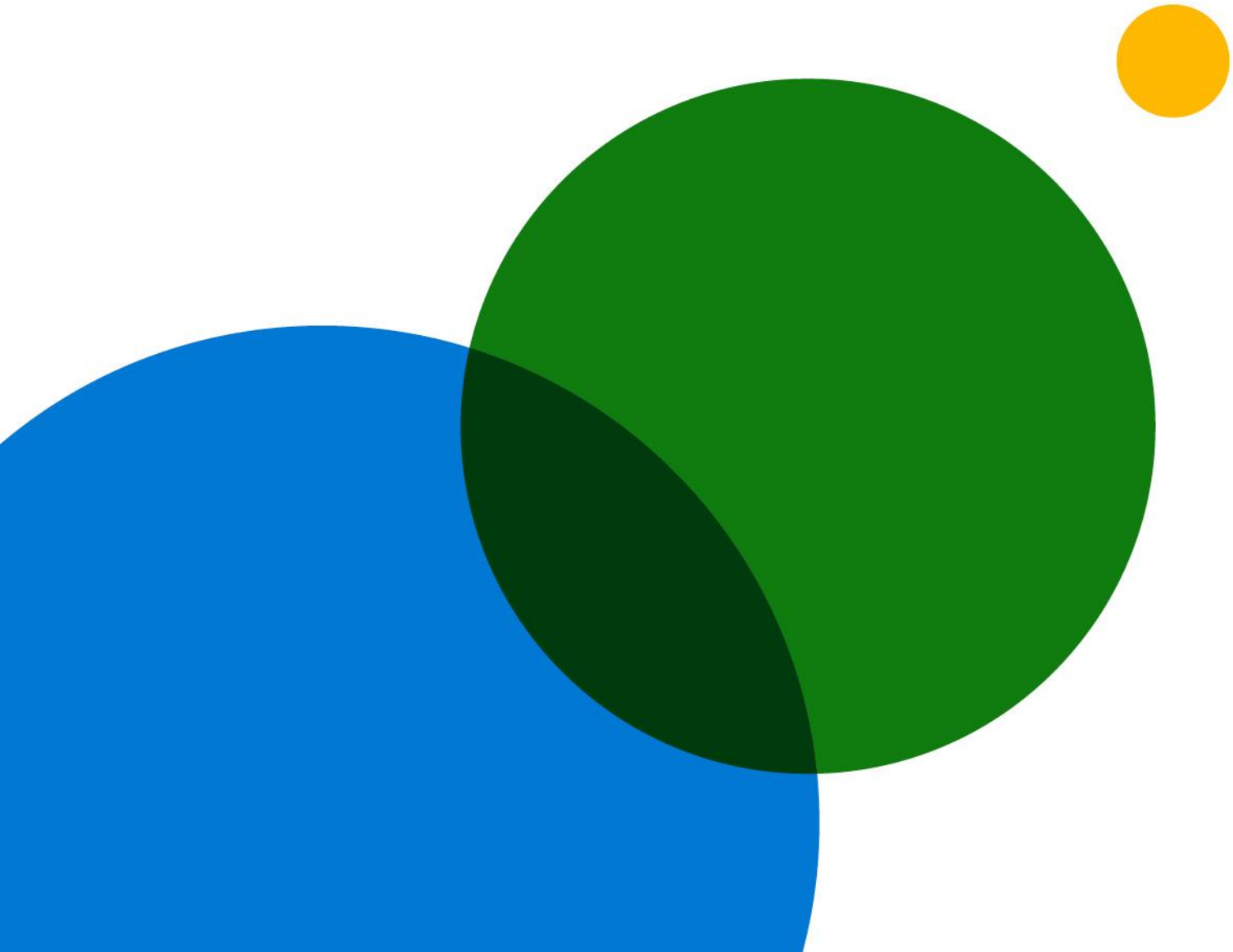
Microsoft Security

hypothesis

Rapport om implementering av nulltillit



Innhold

Innledning

Vasu Jakkal / viseadministrerende direktør for sikkerhet, samsvar og identitet

Det siste året har vært bemerkelsesverdig på grunn av utviklingen innen cybersikkerhet og fremveksten av nulltillit som ledende strategi for vår bransje og organisasjoner over hele verden.

I starten av pandemien ble arbeidsplasser nesten tømt over natten, og ansatte flyttet inn på hjemmekontor. Omleggingen tvang mange organisasjoner til å tilpasse seg raskt for å støtte ansatte som jobbet der de kunne – ved hjelp av personlige enheter, samarbeid via skytjenester og deling av data utenfor bedriftsnettverket. Etter hvert som organisasjoner tilpasset seg transformasjonen, stod de også overfor stadig mer avanserte kriminelle på nettet som hele tiden utvikler seg med hensyn til målretting, taktikk og ressurser.

I dag er hybrid arbeid den nye virkeligheten. På bakgrunn av dette og i møte med hurtige endringer fortalte organisasjonene vi spurte, at de er avhengige av nulltillit for økt sikkerhet og samsvar, raskere oppdagelse og utbedring av trusler og enklere og mer tilgjengelig sikkerhetsanalyse.

Basert på prinsippene om å verifisere eksplisitt, å bruke prinsippet om minste privilegium for tilgang og å regne med sikkerhetsbrudd, bidrar en nulltillitsarkitektur med sikkerhetstiltak på tvers av identitet, endepunkter, apper, infrastruktur, nettverk og data i kombinasjon med økt synlighet, automatisering og orkestrering. Ikke bare anbefaler vi denne tilnærmingen til kunder og partnere. Vi bruker den selv i vår globale sikkerhets- og programvareutvikling her i Microsoft.

Denne rapporten belyser veien til nulltillitssikkerhet – uavhengig av marked og bransje. Vi håper at forskningen vår kan bidra til å akselerere din egen implementering av nulltillit, kaste lys over hvordan andre i bransjen din ligger an, og gi innsikt i den fremtidige tilstanden til dette feltet.

Metode

Microsoft bestilte denne rapporten og forskningen som ligger til grunn for den, fra Hypotese Group, et innsikts-, design- og strategibyrå. Forskningen inkluderte to faser i USA for å fremheve trender og momentum i implementeringen av nulltillit. Flere markeder ble lagt til i den andre fasen for å undersøke globale trender.

Første del av forskningen fant sted i august 2020, med en 15-minutters nettundersøkelse som ble utført i USA blant 300 sikkerhetsbeslutningstakere (SDM-er) som har befatning med nulltillitsstrategier i selskaper innen en rekke bransjer. I tillegg til nettundersøkelsen ble fem dyptgående intervjuer gjennomført på nettet i september 2020 blant SDM-er fra USA innen en rekke bransjer.

I april 2021 ble den globale forskningen utført i USA, Tyskland, Japan og Australia/New Zealand blant av en lignende gruppe beslutningstakere innen sikkerhet. Over 900 deltakere tok en 15-minutters undersøkelse på nettet med spørsmål rundt nulltillitstrategi, både implementering, praksiser, fordeler, utfordringer og hvordan de tenker å investere i fremtiden.

Ting du bør vite om innføring av nulltillit

01 / Organisasjoner er klare til å innføre nulltillitsstrategi, og skiftet fremskyndes av overgangen til hybrid arbeid og Covid-19

Sikkerhetsbeslutningstakere (SDM-er) sier at utvikling av en nulltillitsstrategi er øverste sikkerhetsprioritering, og 96 % sier at det er avgjørende for organisasjonens suksess. De viktigste motivasjonsfaktorene for å innføre nulltillitssikkerhet er å forbedre den generelle sikkerheten og sluttbrukeropplevelsen. Overgangen til hybrid arbeid, fremskyndet av COVID-19, fremmer også den bredere innføringen av nulltillitsstrategier: 81 % av organisasjoner har begynt å gå i retning av en hybrid arbeidsplass, og 31 % er allerede på plass. 94 % har imidlertid bekymringer om overgangen, og disse gjelder i hovedsak at ansatte skal misbruke situasjonen, at IT-avdelingen skal overbelastes, og at organisasjonen skal rammes av cyberangrep. Viktige tiltak er derfor økt opplæring av ansatte og innføring av flerfaktorautentisering (MFA) for å sikre en problemfri brukeropplevelse og overgang.

02 / Nulltillitsstrategi gir fleksibilitet med hensyn til hvor organisasjoner kan begynne implementeringen slik at tilnærmingen kan skreddersys etter behov

Færre enn 15 % av organisasjonene begynte å implementere nulltillitsstrategien på samme risikoområde. Dette er i stor grad fordi implementeringen er en prosess som dekker hele sikkerhetsarkitekturen og ikke en rekke ulike, individuelle teknologier. Tilsvarende er rekkefølgen av implementering av individuelle komponenter innenfor et risikoområde svært varierende, og sikkerhetspersonell begynner slett ikke alltid med de samme komponentene.

03 / Selv om nulltillitsstrategien er vanlig og styrker organisasjoners evne til å håndtere trusler, er det fortsatt mye arbeid som gjenstår

76 % av organisasjonene har i det minste begynt å implementere en nulltillitsstrategi, og 35 % hevder å være ferdig. Men de som hevder at implementeringen er gjort, sier samtidig at de ikke er ferdige med å implementere nulltillitsstrategien på tvers av alle risikoområder og komponenter. Nulltillitsstrategien er overbevisende fordi den gir økt smidighet, raskere oppdagelse av trusler og bedre evne til å håndtere sikkerheten for Internet of Things (IoT) og driftsteknologi. Bruken øker i USA (fra 70 % i august 2020 til 79 % i april 2021). USA ligger også foran på implementering av nulltillit i forhold til andre land som begynte innføringen senere, og organisasjoner i USA hevder å være mindre begrenset av budsjetter. Men mens 57 % av organisasjonene hevder å være i forkant av andre når det gjelder innføring, har rundt halvparten fortsatt mer arbeid å gjøre siden de ikke har implementert nulltillit fullstendig på tvers av alle risikoområder og komponenter.

04 / Fremover vil nulltillitsstrategien forbli en fremskutt prioritering og kreve gjennomtenkte beslutninger når det gjelder ansatte og leverandører

Nulltillitsstrategien forventes å forbli på topp i to år fra nå, og organisasjoner forventer å øke investeringen. Å overvinne utfordringer som gjelder ansatte (f.eks. bemanning av sikkerhetsteam og oppslutning fra ledelsen), vil være avgjørende for investeringen i nulltillit. Når det gjelder leverandørstrategi, har sikkerhetsbeslutningstakere en preferanse for helhetlige eller konsoliderte leverandører, siden valg av leverandør ofte avhenger av tilgjengeligheten av intern ekspertise. Fordelene med å velge det beste fra samme leverandør er økt ekspertise, flere ressurser og enkelhet, selv om det kan ta lengre tid å implementere, være vanskeligere å integrere i den eksisterende sikkerhetsarkitekturen og øke potensielle sårbarheter.

Hvem vi har snakket med

Globalt

* 1000 eller flere ansatte i USA, over 500 eller flere ansatte i Tyskland, Japan, Australia/New Zealand

Samlede forsknings-resultater

Organisasjoner er klare til å innføre en nulltillitsstrategi

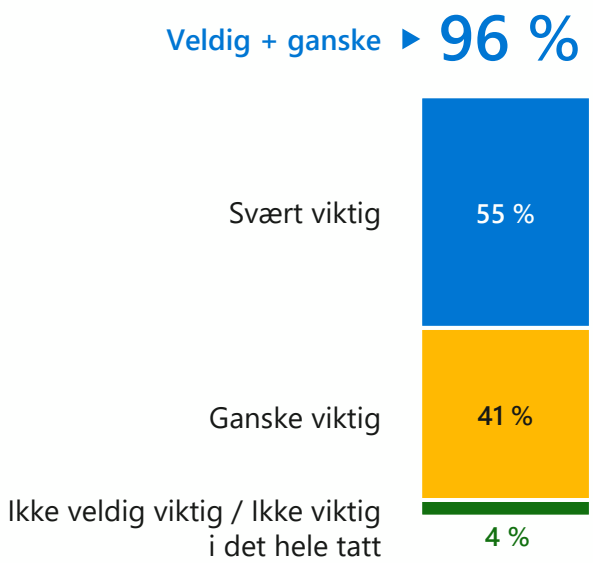
En nulltillitsstrategi står fremst på sikkerhetsagendaen på tvers av markeder og bransjer, og en rekke organisasjoner har vedtatt en nulltillitsstrategi de siste årene. Selv om nulltillit prioriteres høyt av alle (53 %), prioriteres det spesielt høy av organisasjoner i USA (56 %) og Tyskland (53 %).

Nesten alt sikkerhetspersonell (96 %) mener at en nulltillitsstrategi er avgjørende for organisasjonens suksess. (Se eksempel 1) I tillegg til å styrke den generelle sikkerheten og forbedre sluttbrukeropplevelsen håper sikkerhetsarbeidere at nulltillit skal forenkle sikkerhetsprosedyrene for ansatte. (Se eksempel 2)

En amerikansk sikkerhetsbeslutningstaker i servicenæringen forklarer: *«Målet er å styrke sikkerheten samlet sett, men det handler om å redusere friksjon i sluttbrukeropplevelsen og gjøre livet enklere for sluttbrukerne.»*

Videre oppfatter 31 % av sikkerhetspersonell at nulltillitsstrategien er et viktig verktøy i det nært forestående skiftet til hybrid arbeid etter pandemien. Denne faktoren er spesielt viktig i Australia/New Zealand (44 %).

Eksempel 1. Nulltillit er viktig



Eksempel 2. Motivatorer for nulltillit

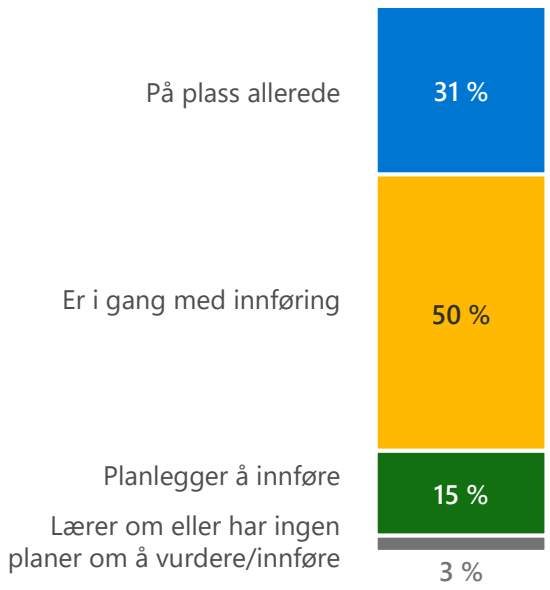
Fremste motivatorer	
Forbedre den samlede sikkerhetsposisjonen	47 %
Forbedre opplevelsen og produktiviteten til sluttbrukere	44 %
Transformer måten sikkerhetsteam samarbeider på	38 %
Forenkle sikkerhetsstakken	35 %
Redusere sikkerhetskostnader	35 %

Overgangen til hybrid arbeid fremmer bredere bruk av nulltillitsstrategier

81 % av store organisasjoner har begynt på overgangen mot en hybrid arbeidsplass, og 31 % har allerede fullført skiftet. Men når det gjelder «ferdig implementert», er variasjonene store fra marked til marked: Australia og New Zealand leder an med 37 %, er Tyskland langt bak, der bare 20 % av organisasjonene har gått over til en hybrid modell. (Se eksempel 3)

Men selv om globale markeder innfører hybride modeller i ulikt tempo, forventer de fleste (91 %) organisasjonene som ikke er i mål, at de kommer i mål i løpet av de neste fem årene. Viktig er det at 94 % er bekymret for overgangen, og det de bekymrer seg for er at ansatte skal misbruke situasjonen, at IT-avdelingen skal overbelastes, og at risikoen for cyberangrep skal øke. (Se eksempel 4)

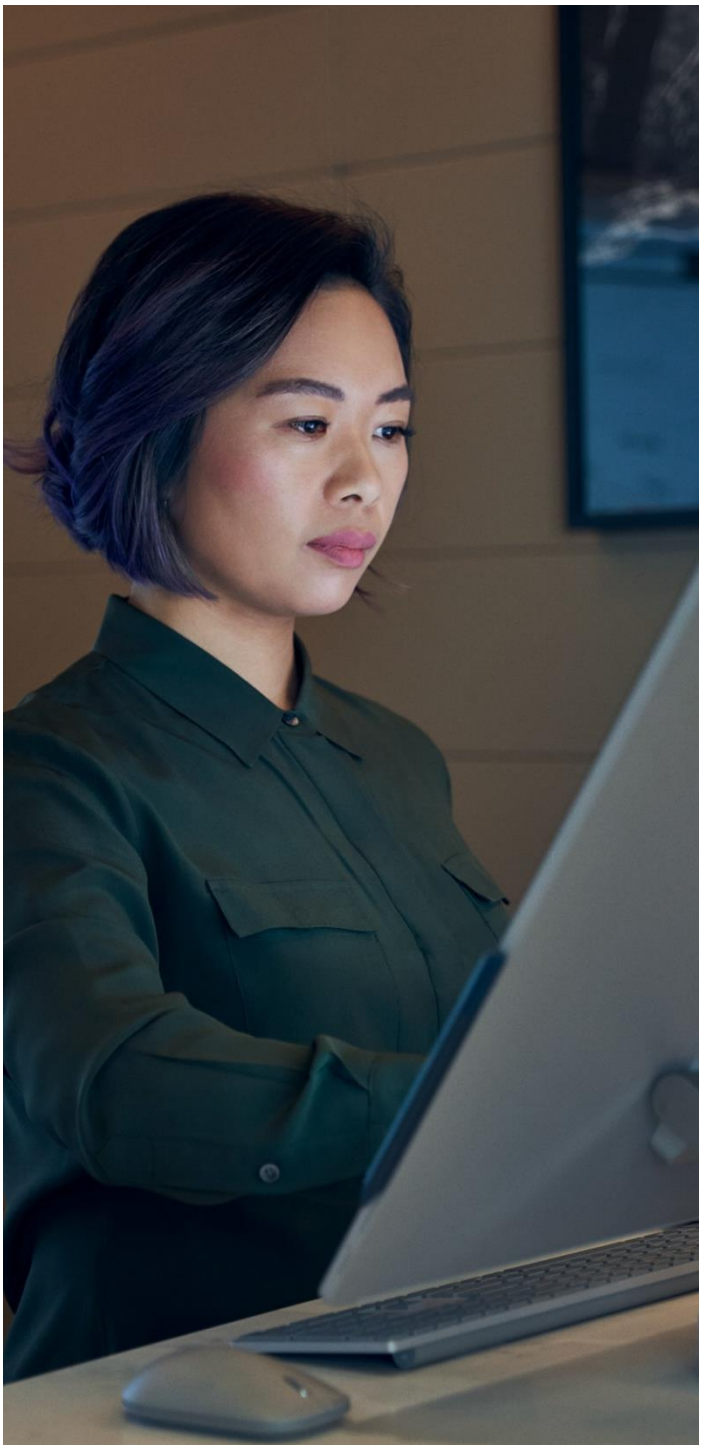
Eksempel 3. Innføring av hybrid arbeid



Eksempel 4. Bekymringer for hybrid arbeid

Ansatte som laster ned usikre apper	37 %
En økning i IT-arbeidsbelastning	37 %
Angrep med løsepengevirus	36 %
Phishingangrep	35 %
Feilaktig bruk av personlige enheter	34 %
Uautorisert datatilgang	31 %
Manglende evne til å administrere alle enheter	30 %
Bruk av personlige e-postkontoer	30 %
Manglende overholdelse av dataforskrifter	24 %

Covid-19 har ført til et raskere skifte til nulltillitsstrategier



For å redusere forekomsten av problemer fremhever interessenter viktigheten av økt opplæring av ansatte (54 %) (spesielt i Japan (61 %) og Tyskland (58 %)) og flerfaktorautentisering (MFA) (50 %) (spesielt i USA (52 %) og Tyskland (56 %)) for å sikre en problemfri brukeropplevelse og overgang.

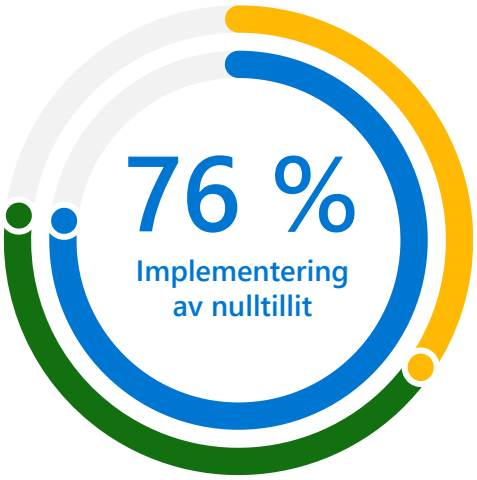
Sikker bruk av hjemmekontor og hybrid arbeid kan hjelpes av en nulltillitsstrategi, og COVID-19 har fremskyndet implementering av en nulltillitsstrategi for 72 % av organisasjoner – selv om det er variasjoner mellom markedene. Pandemien bidro til innføring i rundt syv av ti organisasjoner i USA (76 %), Japan (71 %) og Australia/New Zealand (69 %), men implementeringen har vært betydelig lavere i Tyskland (62 %). Kanskje skyldes dette langsommere overgang til hybrid arbeid.

Nulltillit er bredt implementert rundt om i verden og på offensiven i USA

Nulltillit er ikke bare et moteord, det er en realitet. 76 % av organisasjoner har i det minste begynt å implementere denne strategien, og 35 % mener de er ferdige med implementeringen. Men dataene maler et altfor optimistisk bilde. Mange organisasjoner som anser seg som ferdig implementert, er etter det de sier selv, ikke klargjort på alle risikoområder. I dag er USA i forkant med hensyn til nulltillit i forhold til andre land, og de fortsetter å vokse raskt: Sammenlignet med august 2020 økte implementeringen av nulltillit i USA fra 70 % til 79 % – et betydelig hopp i løpet av bare åtte måneder.
(Se eksempel 5)

Nulltillitsstrategier dominerer for øyeblikket på sikkerhetsområdet, men utbredelsen er relativt ny. 82 % av selskapene implementerte nulltillitsstrategier i løpet av de siste tre årene, og 21 % gjorde det i løpet av de siste 12 månedene. Når det er sagt, begynte 26 % av amerikanske organisasjoner implementering for tre år siden eller mer, i forhold til 19 % av japanske organisasjoner, 6 % av organisasjonene i Australia/New Zealand og 3 % av organisasjonene i Tyskland. Denne tidlige implementeringen i USA – som samsvarer med færre budsjettbegrensninger – kan bidra til å forklare hvorfor organisasjoner i USA ligger i forkant med nulltillit i forhold til organisasjoner i andre markeder. Tilsvarende kan den begynnende innføringen av nulltillit i Tyskland bidra til å kontekstualisere lavere innføring: 97 % av tyske organisasjoner begynte å implementere for bare tre år siden.

Eksempel 5. Implementering av nulltillit



	USA (2020)	USA	DE	JP	AUS/NZ
Implementering av nulltillit	70 %	79 %	75 %	76 %	71 %
• Ferdig implementert	27 %	44 %	19 %	32 %	28 %
• Implementering pågår	43 %	35 %	56 %	44 %	43 %

35 % Ferdig implementert

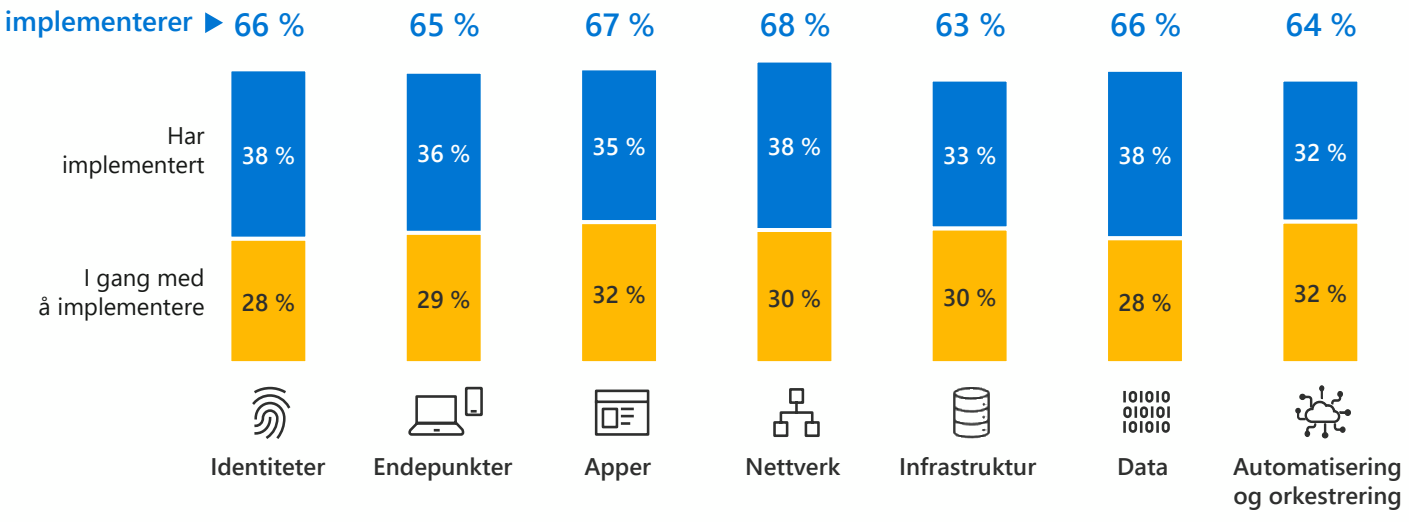
42 % Implementering pågår

Det finnes ikke én tilnærming til nulltillit, så det er mulig å starte innføringen hvor som helst

Det finnes ikke ett risikoområde (identiteter, endepunkter, apper, nettverk, infrastruktur, data, automatisering og orkestrering) som peker seg ut som et åpenbart startpunkt for en nulltillitsstrategi. Færre enn 15 % starter med det samme risikoområdet. Organisasjoner starter på forskjellig sted, alt etter behov og tilgjengelige interne ressurser. Men målet er uansett å innføre nulltillit innen alle risikoområder for å få enda bedre beskyttelse mot trusler. Nulltillit ses derfor på som en komplett strategi som innføres over tid. (Se eksempel 6)

I tillegg til å identifisere sikkerhetsrisikoene må organisasjoner også prioritere individuelle komponenter i hvert sikkerhetsrisikoområde. For endepunkter, apper, nettverk, data og automatisering/orkestrering er det ikke noe klart utgangspunkt. Det er store variasjoner i hvilke komponenter sikkerhetseksperter blinker ut som høyeste prioritet. Sterk godkjenning implementeres imidlertid vanligvis først for identiteter, og verktøy for trusseloppdagelse er en åpenbar prioritering innen infrastruktur. (Se eksempel 7)

Eksempel 6. Nåværende implementering av nulltillit – områder for sikkerhetsrisiko



Eksempel 7. Implementering av komponenter for nulltillitssikkerhet (topp 3) – rangert etter hva som er implementert først

Identiteter	
Sterk godkjenning (dvs. flerfaktorautentisering, passordfri godkjenning)	32 %
Automatisert risikooppdagelse og utbedring	27 %
Adaptive tilgangsretningslinjer for å regulere tilgang til ressurser	22 %

Apper	
Kontinuerlig oppdagelse og risikovurdering av skygge-IT	23 %
Detaljert tilgangskontroll for apper (f.eks. begrenset synlighet eller skrivebeskyttelse)	22 %
Tilgangskontroll for apper basert på retningslinjer	20 %

Infrastruktur	
Sikkerhetsteam har tilgang til verktøy for trusseloppdagelse	25 %
Beskyttelse av skyarbeidsbelastninger både ved bruk av hybrid sky og flere skyer	19 %
Detaljert innsyn og tilgangskontroll for alle arbeidsbelastninger (virtuelle maskiner, servere osv.)	17 %

Automatisering og orkestrering	
Ende-til-ende-synlighet opprettes med en sentralisert plattform for undersøkelse og respons	29 %
Trusseldata samles inn og analyseres fra alle risikoområder (identiteter, endepunkter, apper, nettverk, infrastruktur)	28 %
Automatisert undersøkelse og respons er aktivert	22 %

Endepunkter	
Retningslinjer/kontroller for hindring av datatap for alle uadministrerte og administrerte enheter	27 %
Risikoevaluering av enheter i sanntid / oppdagelse av endepunkttrusler	26 %
Enheter registreres hos ID-leverandøren	24 %

Nettverk	
Sikre tilgangskontroller for å beskytte nettverk	25 %
Trusselbeskyttelse og -filtrering med kontekstbaserte signaler	24 %
All trafikk er kryptert	20 %

Data	
Tilgangsbeslutninger styres av en egen motor for sikkerhetsretningslinjer	21 %
Data klassifiseres og merkes	21 %
De mest sensitive filene beskyttes alltid med kryptering	20 %

Vi så ikke på dette som en rekke separate teknologier, men som en samlet strategi og tilnærming for å behandle hver brukerressurs – både i og utenfor nettverket vårt – som uklarert før de kunne verifiseres.»

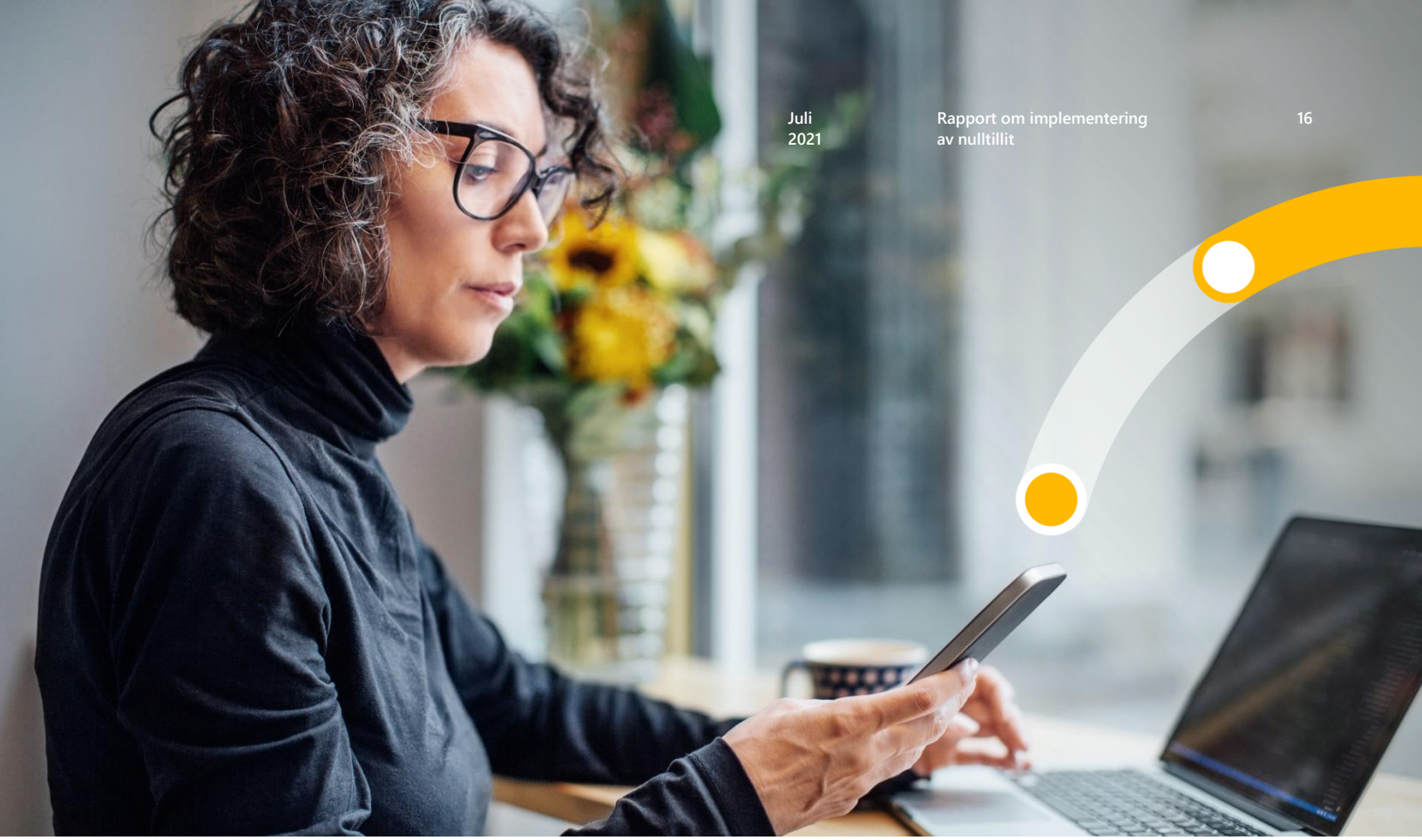
Amerikansk sikkerhetsbeslutningstaker
Servicenæring

Når organisasjoner begynner å implementere en nulltillitsstrategi, er økt smidighet, hastighet og beskyttelse noen av de vanligste fordelene. Ressursfordeler er mindre vanlige

Når nulltillitsstrategien er implementert, drar organisasjoner nytte av økt smidighet (37 %), hastighet (35 %) og bedre beskyttelse av kundedata (35 %). (Se eksempel 8) Direkte fordeler for ansatte, for eksempel frigjøring av tid for sikkerhetsteam (27 %) og redusert behov for ressurser til å administrere infrastruktur (22 %), er imidlertid mindre vanlige.

Det er viktig å merke seg at organisasjoner har tro på at nulltillitsstrategien vil hjelpe dem med å håndtere de fleste trusler og endringer i miljøet, spesielt når det gjelder IoT- og driftsteknologi (47 %).

Eksempel 8. Fordeler med nulltillitssikkerhet



Organisasjoner har tro på at de skal klare å få fullt utbytte av nulltillitsstrategien sin

79 % har tro på evnen sin egen generelle evne til å håndtere sikkerhetstrusler, selv om troen reduseres noe når trusselen innebærer en fabrikasjon av sannhet: Sikkerhetsbeslutningstakere stoler minst på evnen til å håndtere trusler som innebærer syntetiske identiteter (20 %) og syntetiske medier (10 %).

I lys av fordelene man oppnår, oppfattes nulltillit generelt som positivt. I de fire markedene oppfatter sikkerhetsbeslutningstakere deres organisasjoners tilnærming som både praktisk og ambisiøs, og de beskriver den som trygg (37 %) og effektiv (31 %) samt motiverende (25 %), inspirerende (25 %) og spennende (25 %). Særlig i Japan beskriver sikkerhetspersonell nulltillit som både krevende (27 %) og transformerende (25 %), noe som tyder på at fordelene er omfattende når de først er på plass – selv om strategien ikke nødvendigvis er enkel å implementere.

Mange mener de ligger i forkant med implementeringen av nulltillitssikkerhet, men de er fortsatt ikke i mål

Bare 35 % av organisasjonene har implementert en fullstendig nulltillitsstrategien. 52 % rapporterer at de ligger i foran skjema, og 57 % mener de ligger foran andre organisasjoner. Det er spesielt i Japan (66 %) og Australia/New Zealand (63 %) at organisasjoner opplever at de ligger foran andre organisasjoner. Selv om selvtilliten preger alle markeder, preges de også av et gap mellom subjektiv oppfatning og faktisk realitet. Blant respondentene som mener at de ligger i forkant av andre organisasjoner, sier bare 42 % at de har implementert en fullstendig nulltillitsstrategi. (Se eksempel 9)

Selv om mange organisasjoner har tillit til nulltillitsstrategien sin og føler seg klare til å håndtere fremtidige sikkerhetstrusler, gjenstår det fortsatt mye arbeid før implementeringen er fullført på alle risikoområder. Blant organisasjoner som mener at de har fullført implementeringen av en nulltillitsstrategi, har nesten halvparten per i dag ikke implementert strategien innen alle sikkerhetsrisikoområder. Infrastruktur og identiteter er med størst sannsynlighet ikke implementert.

Eksempel 9. Sammenligning av implementering av nulltillitsstrategi

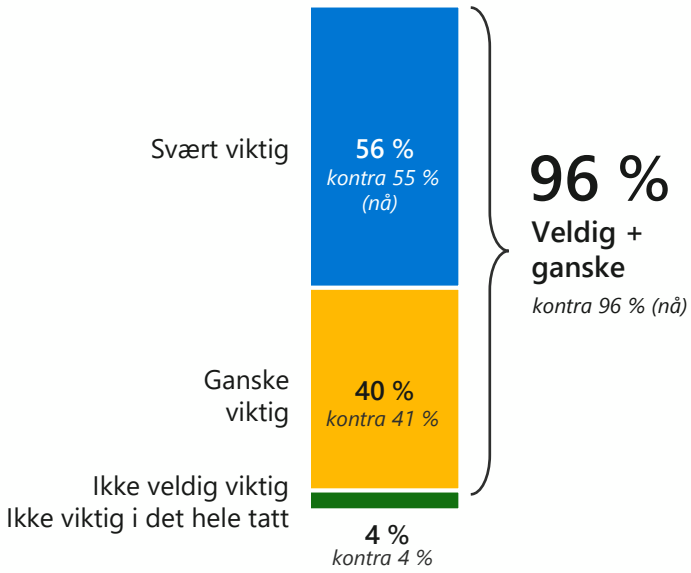
	USA	DE	JP	AUS/NZ
Foran	59 %	46 %	66 %	63 %
På linje	40 %	52 %	34 %	32 %
Bak	2 %	2 %	0 %	6 %

Ser vi to år frem i tid, vil nulltillitsstrategien fortsatt ligge på topp som sikkerhetsprioritering

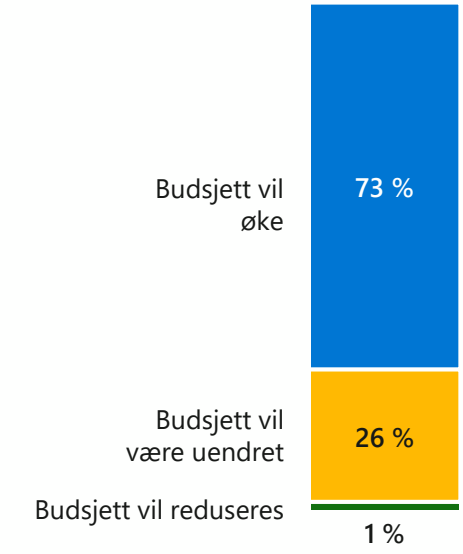
Organisasjoner er helt med på nulltillitsstrategien, og beslutningstakere sier at strategien vil fortsette å ha høyeste prioritet de neste to årene. Den relative viktigheten av nulltillitsstrategien som sikkerhetsinitiativ forventes å øke (fra 53 % til 58 %) innen 2023. Dette henger sammen med at sikkerhetsbeslutningstakere ser for seg at strategien vil forbli avgjørende for den generelle suksessen (96 %). (Se eksempel 10)

Forventet viktighet rager spesielt høy blant japanske organisasjoner. 70 % av dem sier at nulltillitsstrategien vil være helt avgjørende de neste to årene i forhold til gjennomsnittet på 56 %. Budsjetter for nulltillitsstrategier forventes også å vokse. 73 % av organisasjonene forventer å øke sine budsjetter. Dette tallet er litt lavere i Tyskland (67 %), der 31 % forventer at budsjettene vil holde seg på dagens nivå. (Se eksempel 11)

Eksempel 10. Forventet viktighet av nulltillit de neste to årene

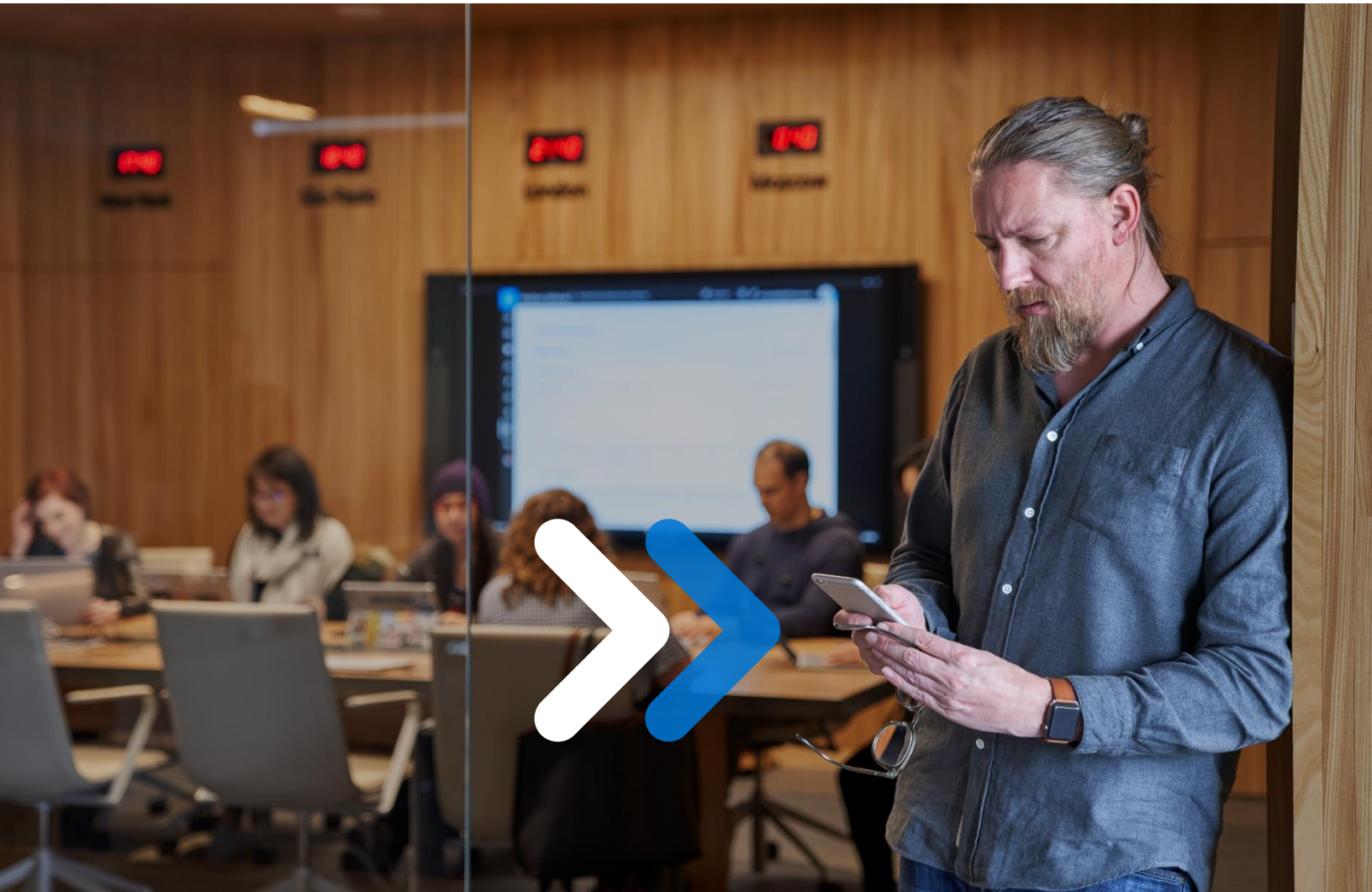


Eksempel 11. Forventet nulltillitsbudsjett de neste to årene



Å bevise at nulltillitssikkerhet virkelig fungerer, kan fremme mer investering

Organisasjoner som helhjertet går inn for en nulltillitsstrategi, forventer å doble investeringen i strategien de neste to årene, og de som ennå ikke har innført nulltillit, risikerer å ligge stadig lenger etter. Disse organisasjonene ligger ikke bare bak konkurrentene når det gjelder prioritering av nulltillit i sikkerhetsplanleggingen (42 % kontra 66 %) og med hensyn til budsjettøkning (66 % kontra 72 %), de føler seg også betydelig mindre trygge på sikkerhetsadministrasjonen av IoT- og driftsteknologi i fremtiden (40 % kontra 53 %).



Å overvinne motstand fra ansatte er nøkkelen til å satse ekstra sterkt på nulltillitssikkerhet

Til tross for raske fremskritt i implementeringen av nulltillitsstrategier, må organisasjoner takle en rekke utfordringer for å komme seg videre med implementeringen. (Se eksempel 12) Ressurs- og ledelsesutfordringer er mest utbredt i disse kategoriene. Tiden det tok å implementere nulltillitsstrategier og mangel på støtte fra toppledelsen topper listen over hindringer, og sistnevnte utfordring er spesielt fremtredende i Australia/New Zealand (65 %).

Videre spiller budsjettbegrensninger – som 45 % av organisasjonene peker på som en hindring – sannsynligvis også en rolle i utfordringer knyttet til ressurser og ledelse.

21 % av sikkerhetsbeslutningstakere nevner vanskeligheter med å bevise avkastning av investering i nulltillit som en hindring for implementering, og denne bevisutfordringen kan gjøre toppledelsen lunken. Det er mer sannsynlig at markeder utenfor USA opplever budsjettbegrensninger (60 % av organisasjonene i Japan, 57 % av organisasjonene i Tyskland, 57 % av organisasjonene i Australia/New Zealand). Dette kan ha en ringvirkning og medføre til redusert og langsommere implementering av nulltillitsstrategier i Japan, Tyskland og Australia/New Zealand sammenlignet med USA.

Eksempel 12. Hindringer for nulltillitssikkerhet

Ressursutfordringer 60 %	Lederskap 53 %	Teknologisk 46 %	Leverandør 46 %	Budsjettbegrensninger 45 %
20 % Tar for lang tid å implementere	**20** % Mangel på støtte fra flertallet i toppledelsen	**21** % Vanskeligheter med å integrere sikkerhetsløsninger	**21** % Trenger implementeringsstøtte fra leverandører	**21** % Kostnader til implementering av en nulltillitsstrategi
19 % Mangel på intern endringsledelse	**19** % Mangel på støtte fra interessenter	**19** % Manglende kompatibilitet med eldre systemer	**21** % Vanskeligheter med å identifisere de riktige leverandørene	**21** % Vanskeligheter med å bevise avkastning
18 % Trenger mer opplæringsmateriell	**19** % Trenger hjelp til å lage en overbevisende prosjektbegrunnelse	**19** % Vanskeligheter med å skalere i hele organisasjonen	**17** % Kan ikke finne innovative partnere	**14** % Har ikke stort nok budsjett
17 % Ikke nødvendig for en organisasjon av vår størrelse	**18** % Mangel på støtte fra organisasjonen			
16 % Har ikke kvalifisert mannskap til å implementere				

«Den første runden med argumentering var utfordrende, men da alle interessenter først ble enige om å investere i dette prosjektet, var det full enighet.»

Amerikansk sikkerhetsbeslutningstaker
FinTech

Sikkerhetsbeslutningstakere har en viss hang til å foretrekke helhetlige eller konsoliderte leverandører

Når det gjelder leverandørstrategi for nulltillitssikkerhet, står organisasjoner overfor valget mellom en helhetlig («best-in-suite») eller individuell («best-in-breed») tilnærming. Den første strategien innebærer å kjøpe én produktpakke for hele nulltillitsarkitekturen fra én helhetlig eller konsolidert leverandør. Dette er en løsning som sikkerhetsbeslutningstakere mener gir mer kompetanse, flere ressurser og en enklere hverdag for organisasjoner som har knepent med ressurser internt. De negative sidene ved denne tilnærmingen er økt sårbarhet og mangel på fleksibilitet. (Se eksempel 13)

Den sistnevnte strategien, med ulike teknologikomponenter som er de beste i sin klasse, innebærer å gå til innkjøp av individuelle komponenter for nulltillitssikkerhet fra spesialiserte leverandører. I motsetning til å velge den beste kombinasjon-sløsningen fra én leverandør benytter strategien med individuelle kvalitetskomponenter seg av forskjellige leverandører som spesialiserer seg på ulike områder, og derfor gir strategien mer fleksibilitet med bedre tilpassing etter organisasjonens strategi. Men, som sikkerhetseksperter sier, er fører individuelle komponenter til en dyrere og mer ressurskrevende løsning som og hemmer synlighet. Og dette er ulemper som skaper leverandør- og budsjettutfordringer. (Se eksempel 14)

Organisasjoner har delte meninger, men et lite flertall av sikkerhetsbeslutningstakere (55 %) foretrekker å arbeide med leverandører som leverer helhetlige pakkeløsninger. (I Australia/New Zealand peker tallene derimot i motsatt retning: 52 % foretrekker løsninger satt sammen av individuelle komponenter.)

Eksempel 13. Fordeler og bakdeler med én helhetlig pakke

⊕ Fordeler med én helhetlig pakke	
Leverandøren har bransjespesifikk ekspertise på alle løsningene	24 %
Flere ressurser tilgjengelige for å planlegge nulltillitsstrategien	23 %
Forenklet sikkerhetsstakk	22 %

⊖ Bakdeler med én helhetlig pakke	
Avhengigheten av én enkelt leverandør øker sårbarheten	34 %
Krever mer kompleks integrasjon med eldre arkitektur	33 %
Mindre fleksibilitet for spesialisert funksjoner	29 %

Eksempel 14. Fordeler og bakdeler med individuelle komponenter

⊕ Fordeler med individuelle komponenter	
Fleksibilitet til å velge de beste løsningene for hver komponent i nulltillitsstrategien	33 %
Kan tilpasse løsningen bedre etter organisasjonens arkitektur eller strategi	30 %
Bedre innovasjonsmuligheter med ulike leverandører	26 %

⊖ Bakdeler med individuelle komponenter	
Høyere kostnader	29 %
Ingen mulighet til å dele data mellom ulike løsninger	26 %
Mange løsninger for ansatte å ta i bruk og administrere	26 %

Noen siste tanker

Sikkerhetsrisikoer blir ikke bare hyppigere, men også mer sjofle. Organisasjoner i alle markeder og bransjer velger derfor en nulltillitsstrategi som sier: «Aldri stol på noe eller noen, alltid verifiser». Nulltillitsstrategi ligger øverst på prioriteringslisten til organisasjoner som ønsker å forbedre den generelle sikkerheten, sluttbrukeropplevelsen og produktiviteten, samt å forenkle sikkerhetsprosedyrer for ansatte og redusere kostnadene. Men selv om fordelene med nulltillitsstrategier er velkjente og godt dokumentert, er ressursbegrensninger og skepsis blant lederne en hindring for universell implementering.

Implementering av nulltillitsstrategier har skutt fart de siste tre årene, delvis på grunn av COVID-19 pandemien. Overgangen til hjemmekontor og hybrid arbeid fører samtidig til en bredere innføring av nulltillitssikkerhet, fordi denne typen sikkerhet beskytter systemer og data også når ansatte logger seg på eksternt, ofte fra personlige enheter. Fremskyndet innføring som følge av COVID-19 gir en god pekepinn på den samlede nulltillitsberedskapen. Organisasjoner som har innført strategien i løpet av pandemien, har implementert nulltillit på flere sikkerhetsrisikoområder enn sine kolleger.

Men når det er sagt, er ikke selv de mest avanserte nulltillitsbrukerne helt i mål. Organisasjoners misoppfatninger av egen nulltillitsmodenhet kan gjøre at de sliter med sårbarheter de ikke engang vet om.

Et flertall av organisasjoner, uavhengig av markeder, mener at nulltillitsstrategier bare vil bli viktigere med tiden, og de forventer at budsjettene øker i takt med dette. Dette forventede prioriteringsskiftet er spesielt avgjørende for ikke-amerikanske markeder, der budsjettbekymringer er en vesentlig hindring for innføring av nulltillitssikkerhet. Fullstendig implementering kan være økonomisk og logistisk svært krevende, men man kan ikke lukke øynene for de åpenbare fordelene med nulltillitssikkerhet, og Microsoft vil fungere som veileder og støtte for organisasjoner som begir seg ut på denne sikkerhetsreisen.

Hvis du vil lære mer om nulltillitssikkerhet og utføre en vurdering av hvor moden organisasjonen din er, kan du gå til

aka.ms/zerotrust

Detaljerte forskningsmål og målgrupperekruttering

Målene for forskningen:

Forstå den nåværende tilstanden for nulltillitstilnærminger

Få kjennskap til tankesett, gode fremgangsmåter, fordeler og utfordringer ved å ta i bruk nulltillitstilnærminger

Utforske fremtiden for nulltillitstilnærminger

Kontekstualisere innovasjoner og trender innen nulltillit

Deltakende sikkerhetsbeslutningstakere oppfylte følgende kriterier:

Ansvarlig for sikkerheten i organisasjonen sin, inkludert cybersikkerhet, sikkerhetsoperasjoner, trusselbeskyttelse, identitetsadministrasjon, risikostyring, appsikkerhet, digital juss og hendelsesrespons

Jobbet heltid i et selskap på organisasjonsnivå (1000 eller flere ansatte i USA, 500 eller flere ansatte i DE/JP/AU/NZ)

I alderen 25–75

kjenner til nulltillit

Involvert i beslutningstaking for utvikling/implementering av nulltillitsstrategier

Av de 911 beslutningstakere som ble intervjuet under forskningsdelen utført i april 2021:

I USA ble 477 sikkerhetsbeslutningstakere intervjuet

I Tyskland ble 201 sikkerhetsbeslutningstakere intervjuet

I Australia/New Zealand ble 126 sikkerhetsbeslutningstakere intervjuet

I Japan ble 107 sikkerhetsbeslutningstakere intervjuet

Obs! Forskningen ble utført under den globale COVID-19 pandemien, med varierende stadier av eskalering/kontroll i de ulike landene

Microsoft Security hypothesis