Deloitte.

Zero Trust Threat Modenhedsmodel (Baseret på "Microsoft Zero trust Maturity Model . Se note")

Modenhedsscore (72%)	72%

Expend to see the original English text...

Forklaringer på stadier af Zero Trust implentering >>			Traditionel	Avanceret	Optimeret
			Det er her, de fleste organisationer generelt er i dag, hvis de ikke har startet deres Zero Trust -rejse: > Lokal identitet med statiske regler og noget SSO. > Begrænset synlighed er tilgængelig for enhedsoverensstemmelse, cloudmiljøer og logins. > Flad netværksinfrastruktur resulterer i en bred risikoeksponering.	I denne fase har organisationer påbegyndt deres Zero Trust-rejse og gør fremskridt på et par centrale områder: > Hybrid identitet og finjusterede adgangspolitikker er adgang til data, apps og netværk. > Enheder er registreret og overholder IT -sikkerhedspolitikker. > Netværk segmenteres, og cloud -trusselbeskyttelse er på plads. > Analytics begynder at blive brugt til at vurdere brugeradfærd og proaktivt identificere trusler.	Organisationer i den optimale fase har foretaget store forbedringer af sikkerheden: > Cloud-identitet med realtidsanalyse dynamisk gate-adgang til applikationer, arbejdsbyrder, netværk og data. > Beslutninger om dataadgang styres af cloud -sikkerhedspolitiske motorer, og deling er sikret med kryptering og sporing. > Tillid er helt fjernet fra netværket -mikroskyperimetre, mikrosegmentering og kryptering er på plads. > Automatisk trusselregistrering og reaktion er implementeret.
Score (0-100%)	Emne (9)	Start herunder i C9. Vælg estimeret modenhedsniveau for hvert emne. (Udfyldt af 6/6)			
33%	#1: Identiteter	1. Traditionel	> Lokal identitetsudbyder er i brug (Fx AD) > Der er ingen SSO mellem cloud- og onpremises -apps > Synligheden i identitetsrisiko er meget begrænset	> Cloud-identitet føder fra lokalt system (on-premAD) > Betingede adgangspolitikker giver adgang til og giver afhjælpning > Analyse forbedrer synligheden	>Passwordfri godkendelse er aktiveret > Bruger, enhed, placering og adfærd analyseres i realtid for at bestemme risiko og levere løbende beskyttelse
67%	#2: Devices	2. Avanceret	> Enheder tilsluttes domæne og administreres med løsninger som Group Policy Object eller Config Manager > Enheder skal være på netværket for at få adgang til data	> Enheder er registreret hos cloud-identitetsudbyder > Der gives kun adgang til skystyrede og kompatible enheder > DLP -politikker håndhæves for Bring Your Own Devices og virksomhedsenheder	> Endpoint-trusselregistrering bruges til at overvåge enhedsrisiko > Adgangskontrol er forbundet med enhedsrisiko for både virksomheds- og BYOD -enheder
100%	#3: Applikationer	3. Optimeret	> Lokale apps tilgås via fysiske netværk eller VPN > Nogle kritiske cloud -apps er tilgængelige for brugere	> On-premises-apps vender mod internettet, og cloud-apps er konfigureret med SSO > Cloud Shadow IT -risiko vurderes; kritiske apps overvåges og kontrolleres	> Alle apps er tilgængelige med mindst privilegieret adgang med kontinuerlig verifikation > Dynamisk kontrol er på plads for alle apps med overvågning og respons i sessionen
67%	#4: Infrastruktur	2. Avanceret	> Tilladelser administreres manuelt på tværs af miljøer > Konfigurationsstyring af VM'er og servere, hvor arbejdsbelastninger kører	> Arbejdsbelastninger overvåges og advares om unormal adfærd > Hver arbejdsbyrde tildeles appidentitet > Menneskelig adgang til ressourcer kræver Just-In-Time	> Uautoriserede implementeringer blokeres, og advarsel udløses > Granulær synlighed og adgangskontrol er tilgængelig på tværs af alle arbejdsbyrder > Bruger- og ressourceadgang er segmenteret for hver arbejdsbyrde
100%	#5: Netværk	3. Optimeret	> Få netværkssikkerhedsperimetre og fladt åbent netværk > Minimal trusselsbeskyttelse og statisk trafikfiltrering > Intern trafik er ikke krypteret	> Mange ind-/udgående sky-mikroperimetre med en vis mikrosegmentering > Cloud native filtrering og beskyttelse mod kendte trusler Bruger til app intern trafik er krypteret	> Fuldt fordelt indgang/udgang cloud-mikroperimetre og dybere mikrosegmentering > ML-baseret trusselsbeskyttelse og filtrering med kontekstbaserede signaler > AI trafik er krypteret
67%	#6: Data	2. Avanceret	> Adgang styres af perimeterkontrol, ikke datafølsomhed > Følsomhedsmærkater påføres manuelt med inkonsekvent dataklassificering	> Data klassificeres og mærkes via regex/søgeordsmetoder > Adgangsbeslutninger styres af kryptering	> Klassificeringen forstærkes af smart machine learning -modeller > Adgangsbeslutninger styres af en cloud -sikkerhedspolitisk motor > DLP -politikker sikrer deling med kryptering og sporing
72%	Gennemsnitlig score				