IDC

June 2022

**Författare:**
Martin Sundblad

# Digitalt förtroende och säkerhet

Ett IDC InfoBrief i samarbete med

Hewlett Packard Enterprise | intel

# Sammanfattning

Säkerhet och försvar mot angrepp behöver knappast betonas, eller lyftas högre än det redan lyfts i svenska företag.

Säkerhet och försvar för en CISO håller dock på att bli något betydligt större. Program för IT-säkerhet kommer att bli en del av företagens program för förtroende och riskhantering. Säkerhet och förtroende blir en del av affärsverksamheten där IT ingår.

Samhällets och företagens digitalisering gör att varumärke till allt större del handlar om digitalt förtroende. Om affären blir digital, skapas också förtroendet via digitala media – mekanismer som har samma ingredienser som traditionella relationsförtroenden, men som också har nya ingredienser.

I denna Infobrief ser vi på vägen från IT-säkerhet till program för digitalt förtroende, något som de flesta företag behöver förhålla sig till. Vägen kommer att gå via en arkitektur med Zero Trust, men slutar inte där.

## I detta Infobrief avhandlar vi

| | |
|---|---|
| **Digitalt förtroende** | Företagen i Sverige har redan insett att ett program för varumärke och förtroende är större än enbart IT-säkerhet. Digitalt förtroende omfattar såväl den egna organisationen, kunder, partners, lagstiftare och anställda. |
| **Zero Trust** | En arkitektur för Zero Trust är en nödvändig utgångspunkt, men byggs successivt eftersom den ser olika ut för olika företag. 19% av företagen anser fortfarande att IT-säkerhet kan läggas till i efterhand i produkter och processer. |
| **Det digitala samhället** | Offentlig sektor är en av de största investorerna i IT-säkerhet och skydd. Förutom skyddet av offentlig data har offentlig s ektor en avgörande roll i att stärka det digitala förtroendet hos medborgarna. |

# Hoten ökar – säkerhet och skydd har blivit en av de högst prioriterade frågorna

**16%** av Europeiska företag har betalat mer än $50.000 de senaste 12 månaderna i Ransomware-attacker.

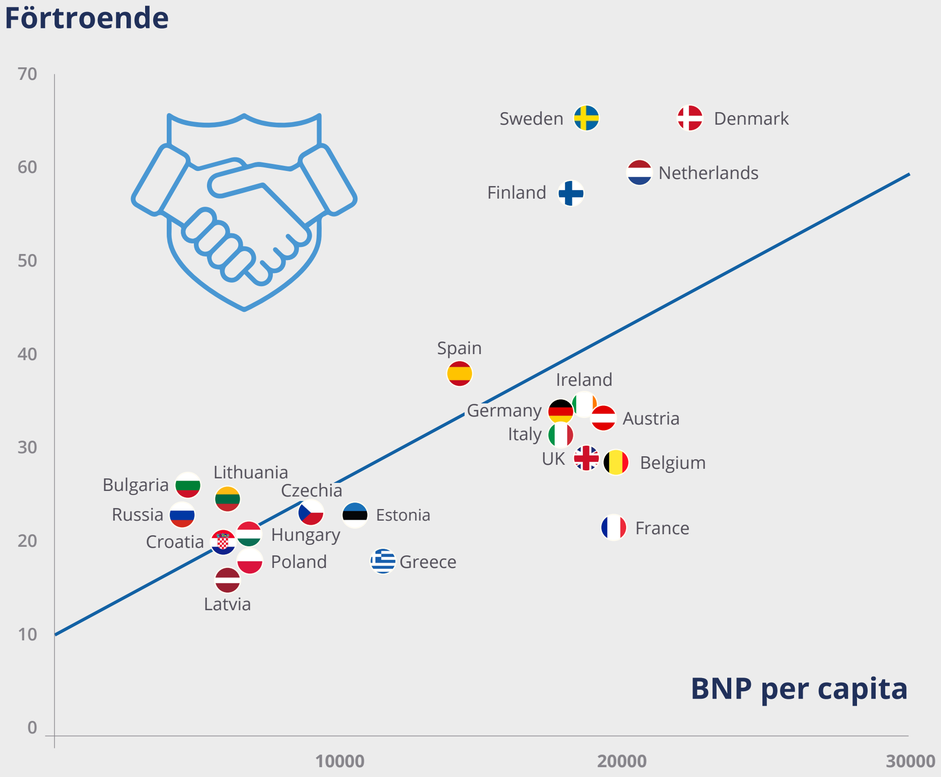
**34%** av dem som haft Ransomware-attacker hade allvarliga störningar i verksamheten i mer än en vecka.

**Attackerna använder genvägar**

30% genom phishing,
15 genom stulna identiteter,
14% genom underleverantörer och
7% genom medvetet fientliga insiders.

# Sambandet är starkt mellan förtroende och framgång

Förtroende är en grundläggande tillgång i ett samhälle, och sambandet är starkt mellan förtroende i ett land och BNP per capita, mellan förtroende och upplevd livskvalitet, och mellan förtroende och förväntad livslängd.




*Källa: Cambridge Journal of Economics*

**Sverige är ett av de länder som har de högsta förtroendekapital för samhälle, rättsväsende och polis i Europa.**

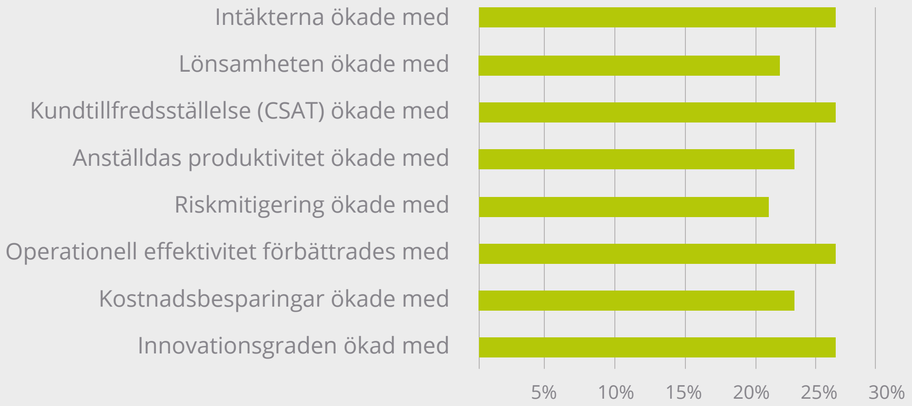
På samma sätt som det finns en koppling melllan förtroende och BNP per capita finns det ett samband mellan förtroende och upplevd livskvalitet och mellan förtroende och förväntat livslängd. Enligt OECD (Yann, Algan m fl) bygger ett samhälles välstånd (ytterst BNP per capita) på förtroende för institutioner, såväl för rättsväsende som för myndigheter.

*Man nämner räkneexemplet att Afrika i medeltal skulle haft 546% högre BNP per capita år 2000 om man haft samma förtroendenivå som Sverige, eller, för att ta ett närmare exempel, 17% högre i Italien.*

# Digitaliseringen innebär att sättet att bygga varumärke och förtroende flyttas

Digital transformation har, oavsett om det berör kundsidan eller interna processer, en stark och pålitlig påverkan på nyckeltalen. Digitaliseringen förändrar affärstransaktioner och i grunden kommunikation mellan företag och kund, och mellan samhälle och medborgare. Vi har en hybridmodell i sättet att skapa förtroende, men går alltmer mot att förtroende skapas och upprätthålls digitalt.

**Organisationer som varit effektiva i sin digitala transformation hade, i genomsnitt, förrbättrade nyckeltal**




**Lönsamheten i digitaliseringen är väl känd:**

**16%** årligen förväntas investeringarna i digital transformation växa.

**Investeringarna i IT-säkerhet växer i motsvarande grad:**

**10%** förväntas säkerhetstjänster och Managed Security växa i Sverige fram till 2025.

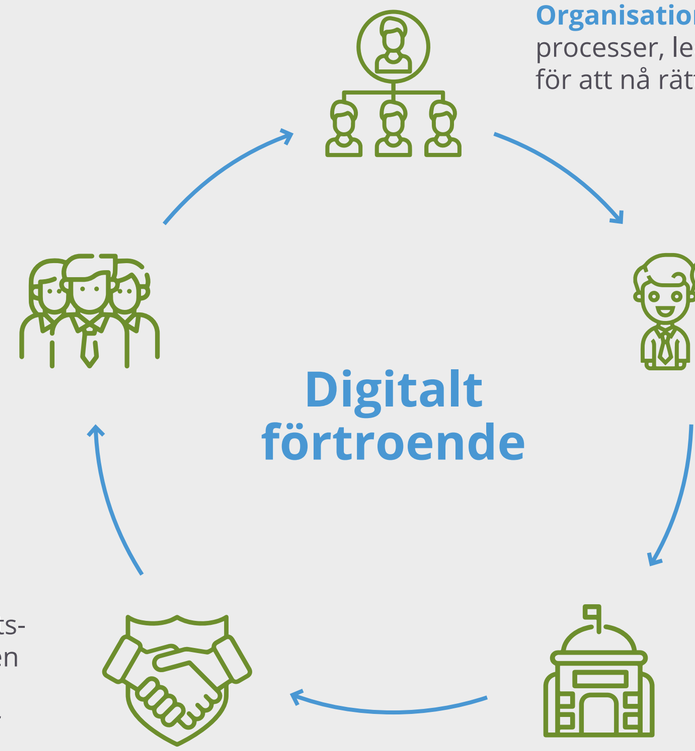
**Mognadsgrad och medvetandet har växt mycket under de senaste åren, men fortfarande anser:**

**19%** av företagen att IT-säkerhet är något som man lägger till i slutänden av ett projekt, eller något som överhuvud taget inte är en del av projekten.

# Ett heltäckande program för digitalt förtroende går bortom den rena IT-säkerheten

**82%** av företag och organisationer anser att digitalt förtroende är fundamental för att kunna göra affärer...

...men bara **38%** har ett program som går bortom ren IT-säkerhet




**Organisationen** ska ha ramverken i processer, ledarskap och infrastruktur för att nå rätt säkerhetsnivå.

**Kunderna** ska ges rätt transparens för säkerhetsnivåer och –åtgärder. Data ska hanteras med rätt integritet och transparens.

**Regulatoriska myndigheter** ska ges rätt förutsättningar och rätt input för att kunna fatta beslut. Företagen behöver ha kontinuerlig kommunikation för att vara väl informerade om krav, uppfyllnad och deras påverkan på förtroendet hos övriga intressenter.

**Partners** och leverantörer måste ges rätt nivå i säkerhets-arbete och dataintegritet, men även kunna ge transparens tillbaka. Samtliga kontaktytor (APIer, informationsutbyte) behöver vara en del.

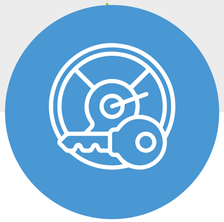
**Anställda** ska ges transparens kring data-integritet, övervakning och säkerhet. Frågan om övervakning måste i varje enskilt fall balanseras mot behovet av förtroende.

# Att bygga digitalt förtroende griper in i hela verksamheten



## Verksamhetsnytta

***Nyttan för verksamheten*** – i kundförtroende, partnerhantering, varumärke, organisatorisk effektivitet, och säkerhet i verksamhetens produkter och tjänster – bygger på en medvetenhet om alla led, och på en kontinuerlig bevakning.



## Resultat och KPIer

En förändring av en verksamhets kultur mot att fokusera på förtroende kräver ***nya mätvärden och KPIe****r*; mätvärden som kontinuerligt byggs upp och förändras allt eftersom kulturen förändras.

## Processelement

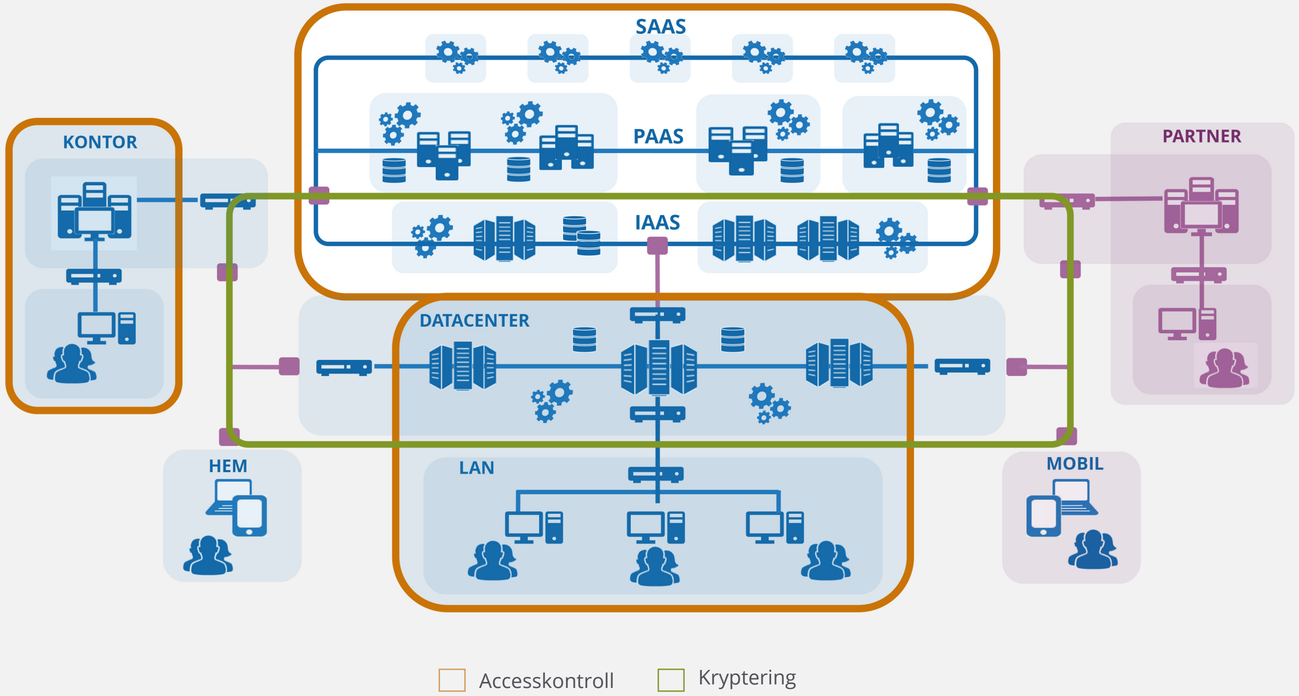
Även om mer än 64% av organisationer i Europa har ett program för digitalt förtroende, ***ligger mätvärden, KPIer och kultur kvar på ett fokus kring IT***, snarare än process, resultat och verksamhetsnytta.

## Teknisk bas

Den tekniska basen utgör just det – den bas i IT-säkerhet som processer, produkter och tjänster ut mot kund och medborgare bygger på, men ett program för digitalt förtroende ska omfatta samtliga fyra delar.

# En arkitektur för Zero Trust är grundläggande

Zero Trust bygger på en modell med olika säkerhetsnivåer, och undvikande av begreppen “innanför” och “utanför”. Istället för att anta att användare inom ett systemskal är fria att röra sig, finns granulära system av kryptering och separation av olika lager av tech-stacken, och separation av nätverken.




Zero Trust innefattar samtliga komponenter i organisationen – servrar, molnmiljöer, datacenters, nätverk, kontor, hemma-kontor, mobila enheter, samt partners och kunder.

En traditionell modell bygger på att allt som är inom ett skal går att lita på. Skalet runt varje system är barriären och skyddet för attacker. Nackdelen är dels att om väl attacken nått innanför skalet så kan den sprida sig, dels att antalet nya enheter och kontaktytor för varje system ökar, och ibland (som i fallet med pandemin) okontrollerat.

# Ingredienserna och stegen i Zero Trust beror på utgångspunkt och verksamhet

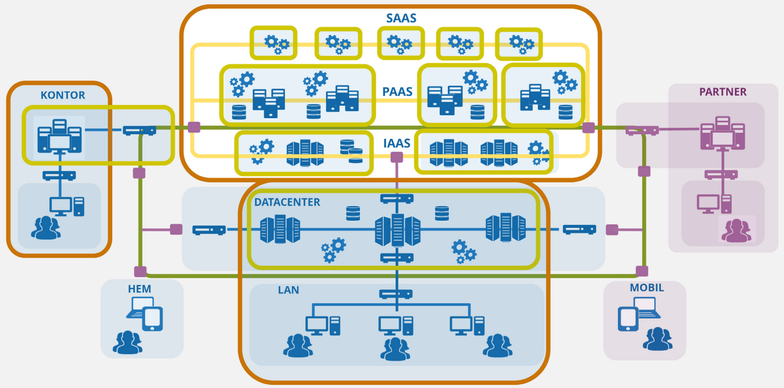
Autenticering / Accesskontroll

Kryptering

1

En del är att etablera flera gränser där kommunikation mellan molntjänster och datacenters krypteras, och autenticering upprättas mellan kluster av system.

Målet är en kombination av granulär accesskontroll, kryptering och identitetskontroll.

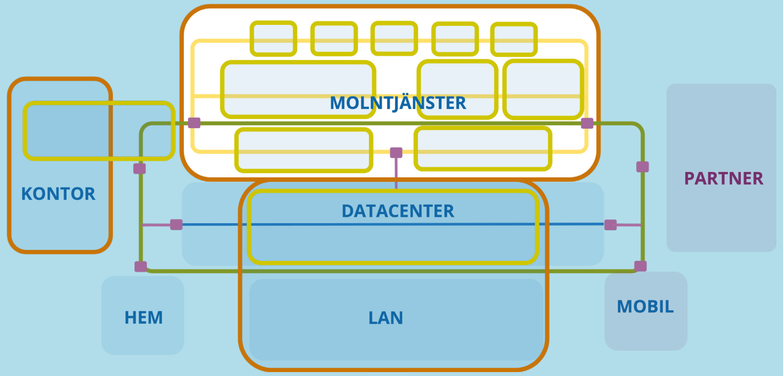



2

Nästa steg är att införa mikrosegmentering inom de kluster du identifierat, där dynamiska accesskontrollregler införs för servrar och containrar också på nätnivå.

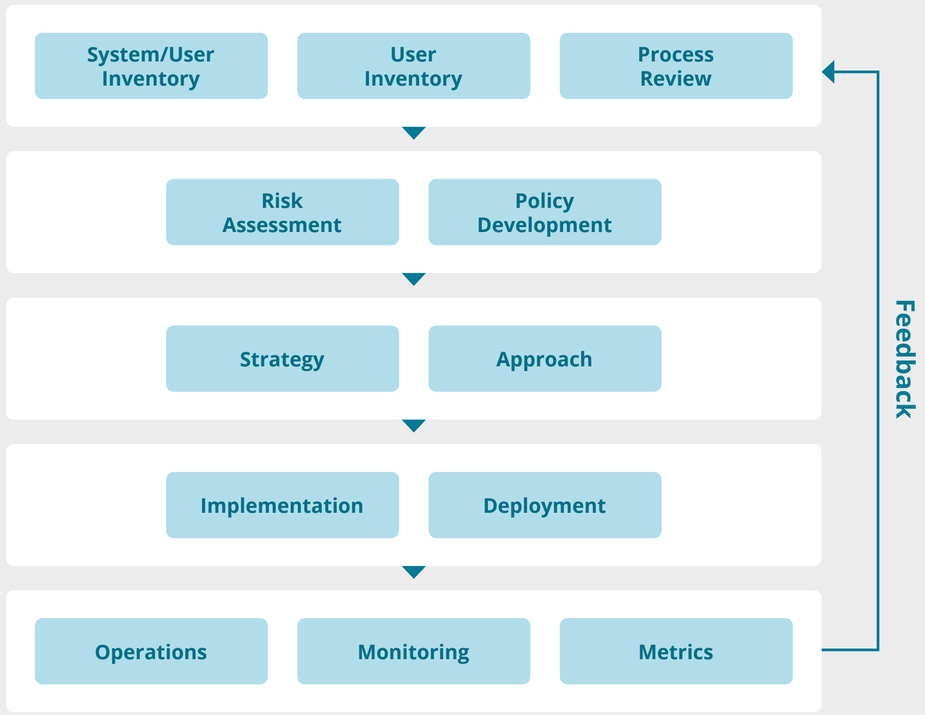
De användare som arbetar mobilt, eller från olika typer av kontor ska sedan anslutas med kryptering och flerfaktorsautenticering.

*Identity Aware Proxies* (IAPs) hanterar regelbaserad åtkomst från enheter och användare. *Software-Defined Perimeter* (SDPs) hanterar autenticeringen för krypterad kommunikation för applikationer innanför och utanför företagsgränsen.



# Vägen till Zero Trust är iterativ, och är olika beroende på förutsättningar

## NIST Zero Trust Architecture




*Källa: NIST, https://csrc.nist.gov/publications/detail/sp/800-207/final*

Eftersom planen för införande är beroende på verksamhet, system och utgångspunkt, behöver vägen till en Zero Trust-arkitektur gå via proof-of-concept över pilotprojekt och utvärdering. Målbilden kan göras klar, men vägen dit bör vara iterativ. När du väl valt angreppssätt behöver du utvärdera din organisations förmågor och kunskaper för att se vilken kapacitet som finns internt, och vilken som behöver köpas in, t ex för MFA – multi-factor autotenticering.

Se till att kostnaden för säkerhet och infogande i din Zero Trust-arkitektur är en del av upphandlingsunderlaget för nya system, snarare än att infoga dem i ett senare skede.

Planering följer en enkel modell för iterativ utveckling – Utvärdera dina förutsättningar, Jämför med målarkitektur, Välj ut pilotprojekt baserat på ekonomiskt utfall och begränsningar, Utvärdera på nytt.

# Zero Trust-arkitektur – Rekommendationer

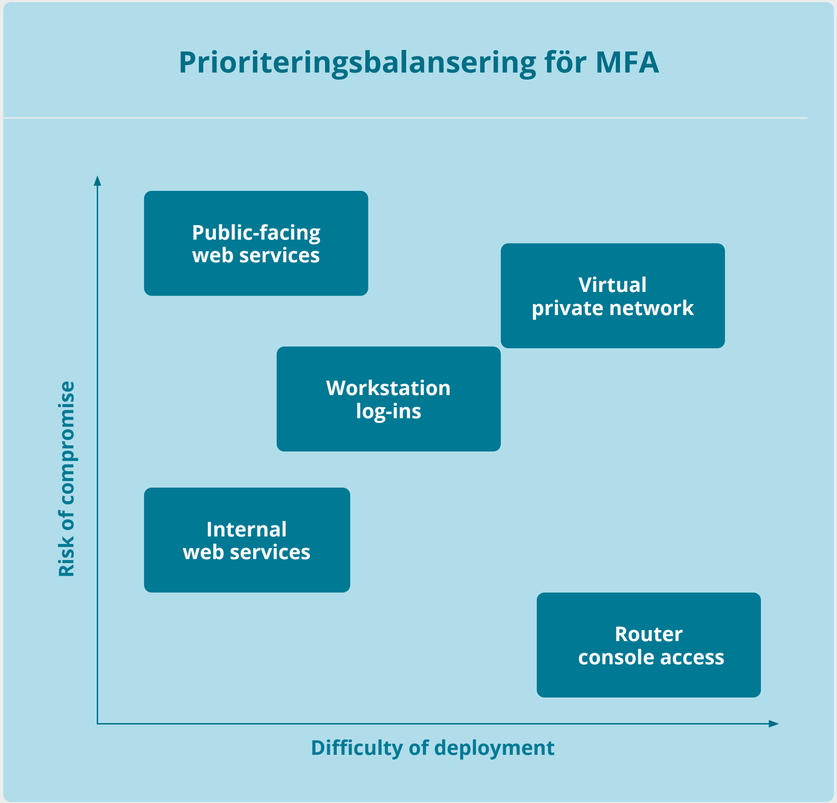
1. **Utvärdera och bygg målbilden för din Zero Trust-arkitektur.** Alla företag har olika förutsättningar och systempark. Kontroll över förutsättningarna, såväl systemmässigt som kompetensmässigt, är grunden.

2. **Hitta nästa steg.** Företag med stora resurser on-premise, bör börja med mikrosegmentering server-to-server. Företag dominerade av molntjänster bör börja med Identity-Aware Proxies (IAP) eller Software Defined Perimeter (SDP).

3. **Se över skalbarheten i infrastrukturen.** Nätverket kan inte ses som en enhetlig Trusted Zone. De enheter som finns på nätverket kan vara ägda och konfigurerade av tredje part. Ingen resurs ska betraktas som säker.

4. **Utvärdera, mät och prioritiera** utifrån kostnad och måluppfyllelse för din Zero Trust-arkitektur. När du implementerar multi-faktor-autenticering (MFA) bör du till exempel väga komplexitet mot risk.

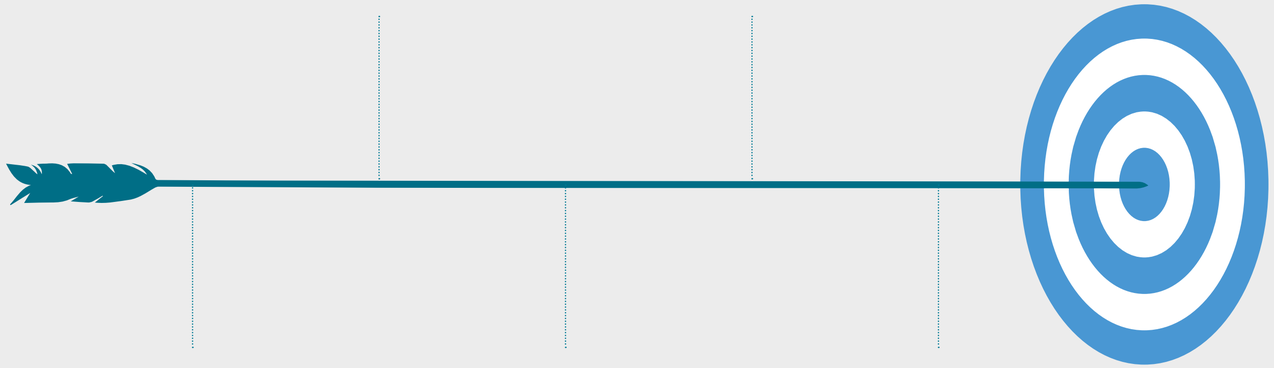
5. **Bygg trovärdiga mätvärden.** En Zero Trust-arkikektur kostar – nyttan måste kunna mätas, inte minst för att kunna utvärdera och prioritera dina pilotprojekt och proof-of-concepts.



# Bortom Zero Trust – Detect, Respond, Recover

**Protect**
Att implementera första linjens försvar mot attacker, baserad på Zero Trust.

**Respond**
Att utveckla processer för när skadan är skedd.



**Identify**
Att identifiera kritiska enheter och processer. Att sköta riskhantering och beredskap.

**Detect**
Att implementera Security Analytics och automatisk detektion.

**Recover**
Att kunna koordinera samtliga aktiviteter inom Recovery.

**Ett ramverk för en uthållig IT-säkerhet inkluderar även processerna runtom arkitekturen.**

5 komponenter ingår – *Identify, Protect, Detect, Respond, Recover.*

Ransomware har blivit en framgångsrik affär – 1/3-del av företagen har haft en attack som gett nertider på mer än en vecka. Processerna för "när det händer" är lika viktiga som skyddet.

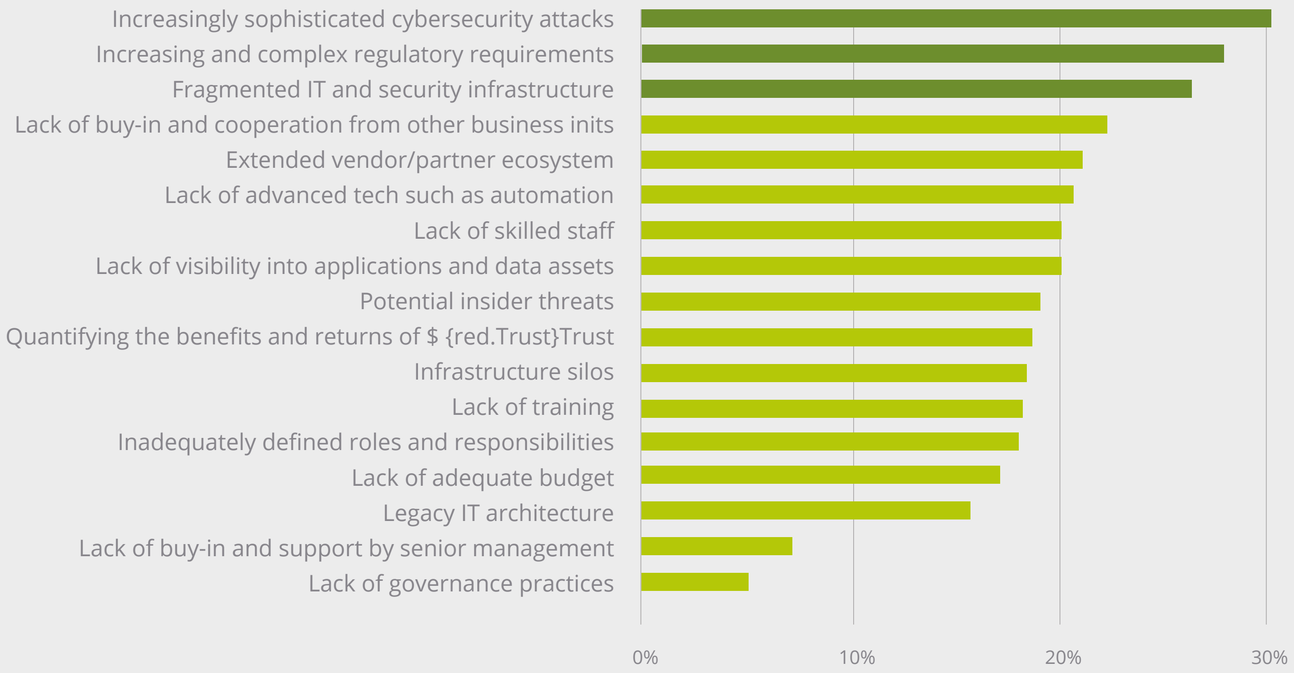
XDR och MDR har blivit accepterade – 70% av företagen använder eller planerar implementation inom de närmaste 12 månaderna. Se till likheterna mellan XDR och MDR, valet bör falla på det som passar kunskapsnivån och förmågan i den egna organisationen.

**Recovery går bortom ren "IT Recovery" och omfattar såväl**

- Identifiering av (för verksamheten) kritiska applikationer
- Isolering av enheter – logiskt och fysiskt
- Säkrad, fysiskt isolerad backup (Immutability)
- Säkrad, separerad recovery-enhet

# Utmaningarna inom digitalt förtroende är fortfarande fokuserade kring IT

**IDC Security Survey:**
Vilka prioriteringar har din organisation i sitt program för Digital Trust?



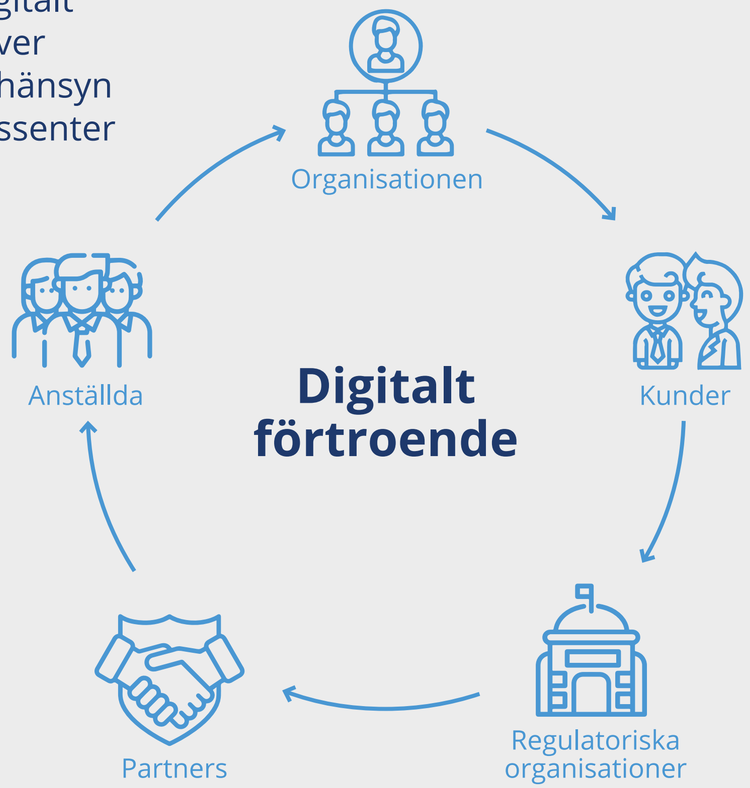

*Källa: IDC, 2021*

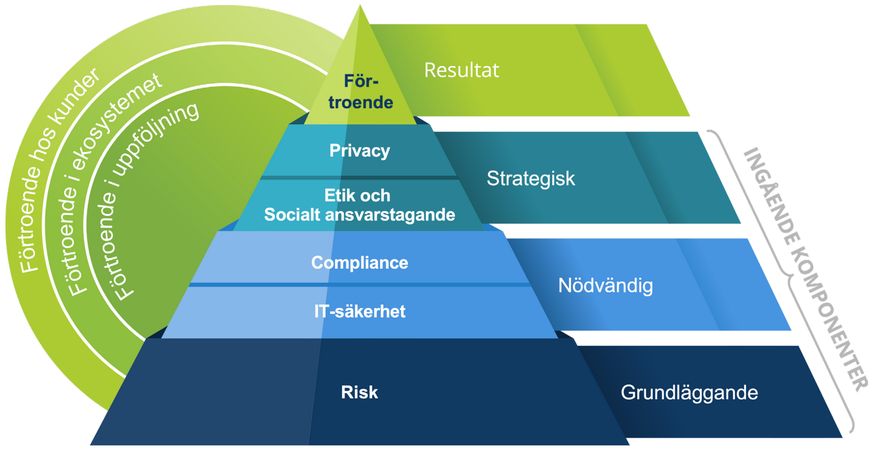
Kunskapen om ett utökat ansvar för säkerhet och förtroende är stor i företag och organisationer, **men i utvärderingar dominerar IT-säkerhet:**

- Allt fler, större och mer sofistikierade cyberattacker
- Alltmer komplicerat och mångfacetterat regelverk
- Fragmentering i IT och Säkerhetsarkitektur

# Steget från ren IT-säkerhet till ett program för digitalt förtroende omfattar hela organisationen

En strategi för digitalt förtroende behöver engagera och ta hänsyn till samtliga intressenter




**Ett program för digitalt förtroende har som grund Riskhantering, Compliance och en Zero Trust-arkitektur.** Därutöver kommer Dataintegritet, Etik och Ansvarstagande att behöva vägas, såväl i den egna organisationen som hos kunder och ekosystem. Förtroende är något som byggs långsamt, men som snabbt kan erodera, och måste därför byggas långsiktigt och hållbart.

# Digitalt förtroende bygger också på digital kompetens

**13%** av invånarna i Sverige åldern 15-75 har ingen eller begränsad digital förmåga. Därutöver har 18% en lägre kunskapsnivå, vilket totalt utgör 31% med någon form av begränsningar i hur de kan ta till sig av digital konsumtion. De konsumenter som ska agera i ett digital relation till företag har därmed till stora delar begränsningar i förutsättningar att bygga digitalt förtroende och i digital konsumtion.

**63%** av företagen säger sig ha svårt att rekrytera personal med tillräcklig digital kompetens. Det påverkar också tillväxt, innovation och lönsamhet redan idag.

**IDC Resilience Survey:**

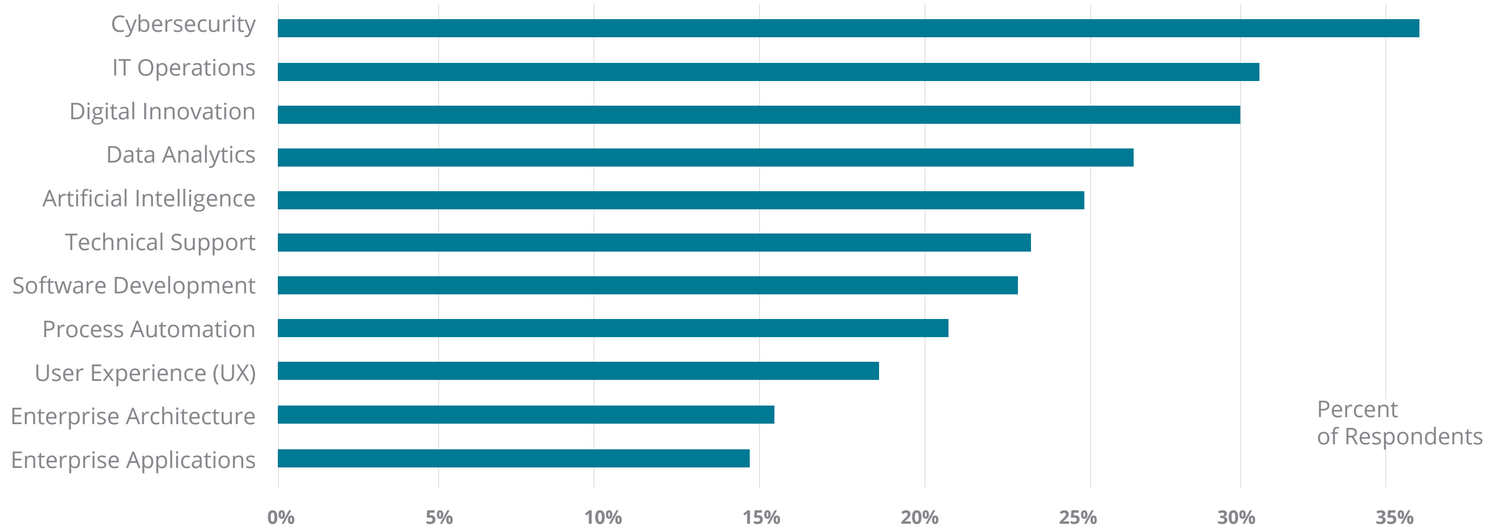
## På vilket sätt har en brist på kunskap eller kompetenser i ditt företag påverkat:


*Källa: IDC, 2021*

# Säkerhet är den kunskap som efterfrågas mest

**IDC Global Skills Survey:**

Vilka IT-kunskaper/förmågor har du störst behov av under nästa 12 månader?



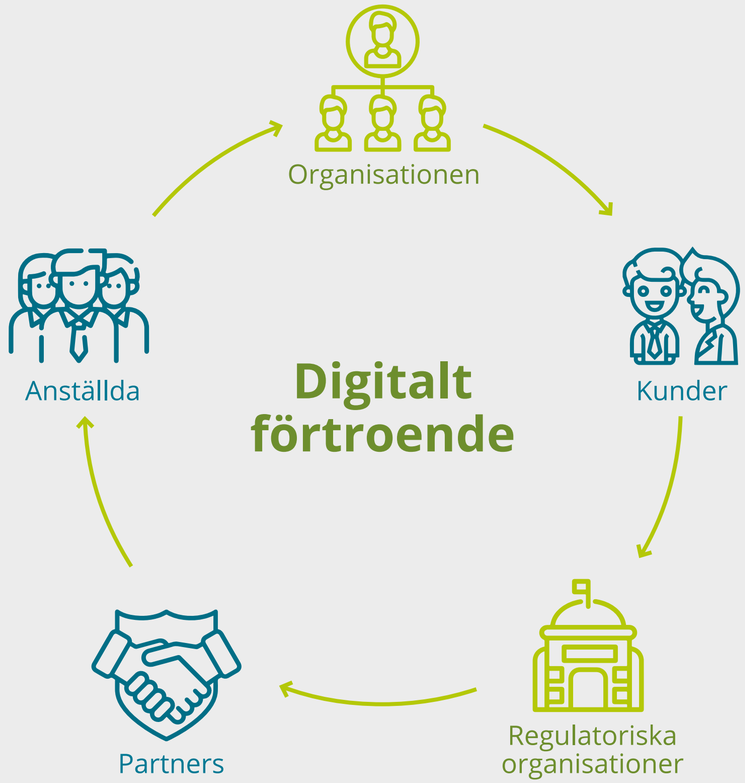

*Källa: IDC, 2021*

När det gäller att skapa förtroende och uthållighet är efterfrågan på kunskap inom säkerhet och skydd den mest efterfrågade och där företagen har störst behov av intern utbildning. IT-säkerhet är också det kunskapsområde som snabbast håller på att "demokratiseras" – kunskapen behövs inte bara av IT-professionella, utan överallt i verksamheten.

*Organisationer i Sverige står därför inte bara inför en teknisk utmaning, utan också inför en utmaning i att bygga kunskap.*

# Digital kunskap behöver byggas i alla led

Bristen på digital kompetens hotar alla led i värdekedjan,
och hotar också den tilltron till digitaliseringen i företag och samhälle.




Flera led i kedjan är utsatta

**Anställda**

I de flesta företag finns det eftersatta grupper med lägre digital kompetens. I många företag är de "kontorslösa" (deskless workers) grupper som kommit sent in i den digitala transformationen.

**Partners**

I ekosystemet ställs krav på IT-säkerhet och IT-infrastruktur, mer sällan på IT-kompetens.

**Kunder**

Ditt digitala förtroende bygger på dina kunders mottagande och kunnande, såväl företag som konsumenter.

# Rekommendationer

1. **Bygg förtroendet i alla led** – kunder, partners, anställda, processer, organisation.

2. **Ta fram en arkitektur för Zero Trust.**
Definiera målbilden, men bygg arkitekturen stegvis.

3. **Utveckla mätvärden / KPIer.**

Med SDP och IAP kommer nya möjligheter att mäta. KPIer kan innehålla
- *Riskreduktion per enhetskostnad* – för att beskriva ROI för varje säkerhetsrelaterat project
- *Projekteffektivitet* – för att mäta kompetensen och utfallet i projektutförandet.
- *Flexibilitet och hållbarhet* – kvalitet och antal kontroller per anslutning/session för att mäta hur stabil och flexibel arkitekturen är.

4. **Se över den digitala kompetensen**,
såväl hos din kundbas som i ditt ekosystem.

5. **Bygg ut kompetensen internt** – se över hur kunskap om IT-säkerhet och förtroende kan byggas in i organisation och processer.

## *Partnerskap med fokus på säkerhet*

*Förtroendet för teknik som motverkar cyberattacker och dataintrång är enligt undersökningar högt, speciellt hos verksamhetschefer och ledning – men hur skyddad är egentligen verksamheten? När organiserad cyberbrottslighet kommit att bli en etablerad mångmiljardindustri behöver åtgärder implementeras för att aldrig lita på något innan det kan bevisas vara säkert. Inte heller går det att lita på någon som försöker få tillgång till data och applikationer innan access kan garanteras vara korrekt och verifierad. Cyberattackerna växer i antal och blir mer avancerade varför det krävs säkerhetsrutiner och avancerade system som klarar av att detektera och motverka hoten. Det krävs också att företag och organisationer kontinuerligt gör riskanalyser och anpassar sig efter de nya säkerhetshot som uppstår då de ständigt antar ny form och lurar bakom varje hörn.*

*Då säkerheten genomsyrar alla andra stora tekniktrender behöver den också alltid tas i beaktning oavsett projekt, uppdrag eller investering en organisation står inför. Intel och HPE arbetar tillsammans för att förebygga hoten genom att ständigt verka för att tekniken som leder cybersäkerhetsutvecklingen ska finnas tillgänglig. Vi jobbar innovativt för att leverera en teknik med en integrerad säkerhetskedja (chain of trust) genom hela processen från design, tillverkning och logistik till implementation och användning. Med en avancerad infrastruktur baserad på Zero Trust där säkerheten finns inbyggd ända nedifrån hårdvarans iLO-chip, kan vi påskynda utvecklingen och leverera en plattform som möjliggör upptäckt och förhindrande av nya säkerhetshot. HPE:s Project Aurora etablerar säkerhetsmätningar av varje entitet där en chain of trust skapas genom att varje underliggande lager verifierar nästa lager nedifrån hardware root of trust och upp genom hela plattformen. Vårt mål är att driva hårdvaru- och mjukvaruinnovationer framåt och utgöra en vital del av ekosystemet. Med vår gemensamma teknologi kan vi leverera säkra digitaliseringsplattformar som skyddar data och bidrar till ökad trygghet för företag och organisationer.*

**I samarbete med:**

Hewlett Packard Enterprise | intel