

Slutpunktssäkerhet är ett kärnelement i din resa mot nollförtroende

Tre rekommendationer för att förbereda för nollförtroende



Sammanfattning

Nollförtroende innebär en långsiktig resa. Det är inte en produkt eller lösning som organisationer implementerar: det är en strategisk ram för säkerhetshantering som byggs upp över tid. I denna eBook finns praktisk vägledning för IT-beslutsfattare som navigerar genom en övergång till nollförtroende, med särskilt fokus på den roll slutpunktssäkerhet har i skapandet av en modern, verkligt säker grund för distansarbetets värld.

Innehållsförteckning

Läget i cybervärlden	3
Konsekvenserna av distansarbetets värld	4
Säkerhetsstrategier behöver förändras	5
Att förstå grunderna inom nollförtroende	6
Att aktivera nollförtroende-principer	7
Tre rekommendationer för att förbereda för nollförtroende	8
Viktiga lärdomar	11
Ta nästa steg	11

Läget i cybervärlden

Säkerhetshot är på uppgång tack vare en arbetsvärld där distans/hybridarbete och molnet blir allt mer utbrett.

Komplexiteten i att skydda en organisations datatillgångar har vuxit enormt de senaste åren. Molnet har varit banbrytande för företagens produktivitet eftersom användning inom distans- och hybridarbete växer men det kommer med en kostnad. Övergången från att hantera endast lokal infrastruktur till att omfatta molnet har skapat en större attackyta för motståndare med växande konsekvenser. Om en angripare lyckas kan den t.ex. påverka alla kunder i en viss molntjänst, inte bara enskilda kunder och deras kunder längs med hela leverantörskedjan. Fördelen för hotaktörer – både nationer och vanliga brottslingar – kan bli enorm och till följd kan de fortsätta hitta nya sårbarheter att utnyttja.



Kostnaden för globala skador till följd av cyberbrott förväntas stiga till **10,5 biljoner USD** år 2025ⁱ

Verizon rapporterade **5 200 bekräftade dataläckor** i en studie från 2022 – **upp 1,3 gånger fler jämfört med det föregående året**ⁱⁱ



Konsekvenserna av distansarbetets värld

Organisationer behöver hitta sätt att ligga steget före det nya hotlandskapet.

Vad är då konsekvenserna med en arbetsvärld där distansarbete blir allt mer utbrett? Två saker:

Alla organisationer är sårbara ...

"[O]m en fokuserad entitet verkligen vill komma in i ditt system har den en hög chans att lyckas."

– Amiral Michael Rogers, f.d. direktör på National Security Agency och f.d. befälhavare i U.S. Cyber Commandⁱⁱⁱ

... och kostnaden om man gör fel kan bli stor.

"Den genomsnittliga kostnaden för en dataläcka nådde rekordsumman 4,88 miljoner dollar under 2024".^{iv}

Attackvektorer blir fler, attackytorna blir större och inget företag är någonsin helt skyddat. Organisationer måste utgå från det värsta och stärka sina försvar inför den oundvikliga attacken.

69 % av organisationer har upplevt någon typ av cyberattack på grund av en dåligt hanterad tillgång som är ansluten till internet.^v



Säkerhetsstrategier måste utvecklas

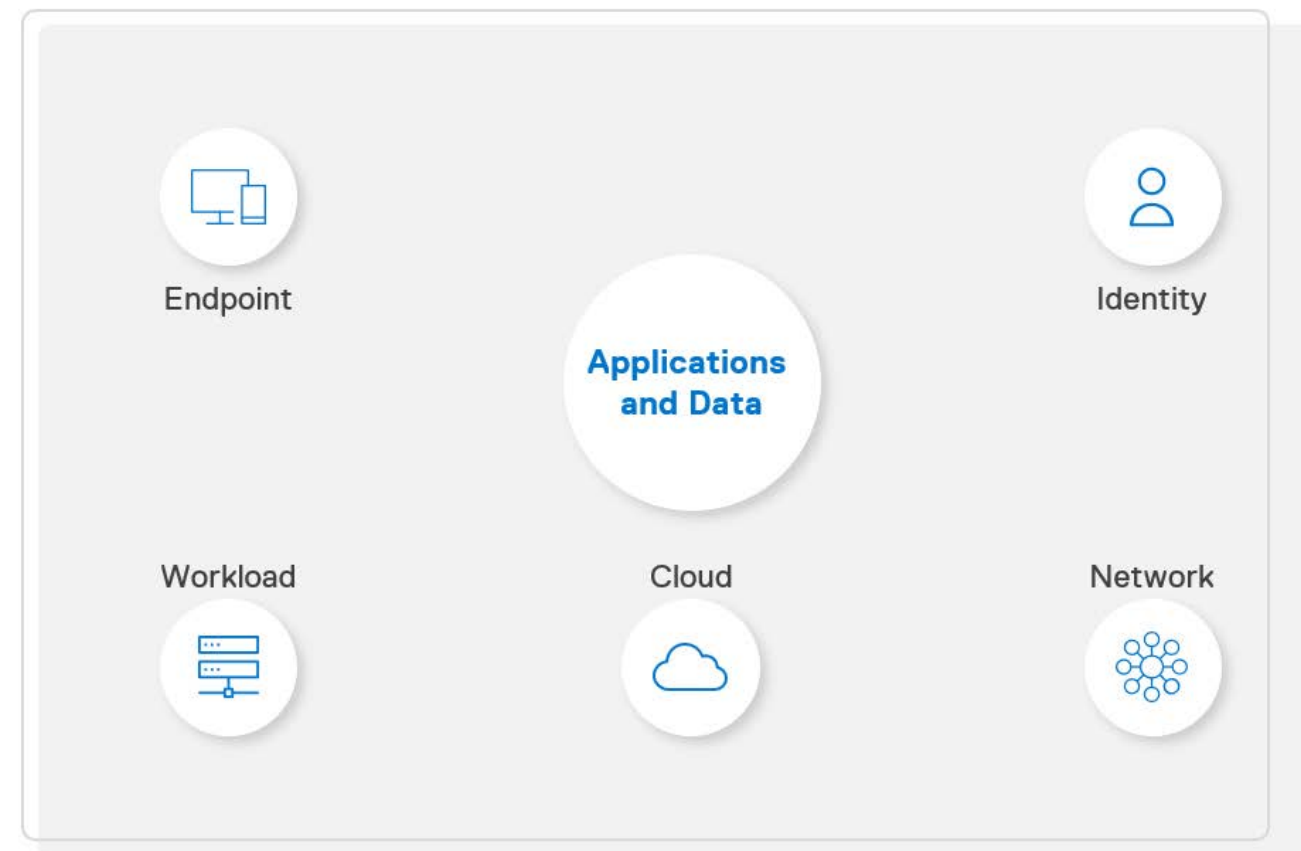
Vi måste omfamna den molnbaserade miljön. Det är där nollförtroende kommer in i bilden.

Traditionella säkerhetsmodeller fungerar inte längre.
Detta är anledningen:

För att en organisation ska ha en effektiv säkerhetsställning måste den täcka fem kontrollpunkter: Slutpunkt, arbetsbelastning, identitet, nätverk och moln. Målet är att skydda program och data.

Organisationer som använder silobaserade traditionella metoder är mer känsliga för angrepp.

Nästa ...

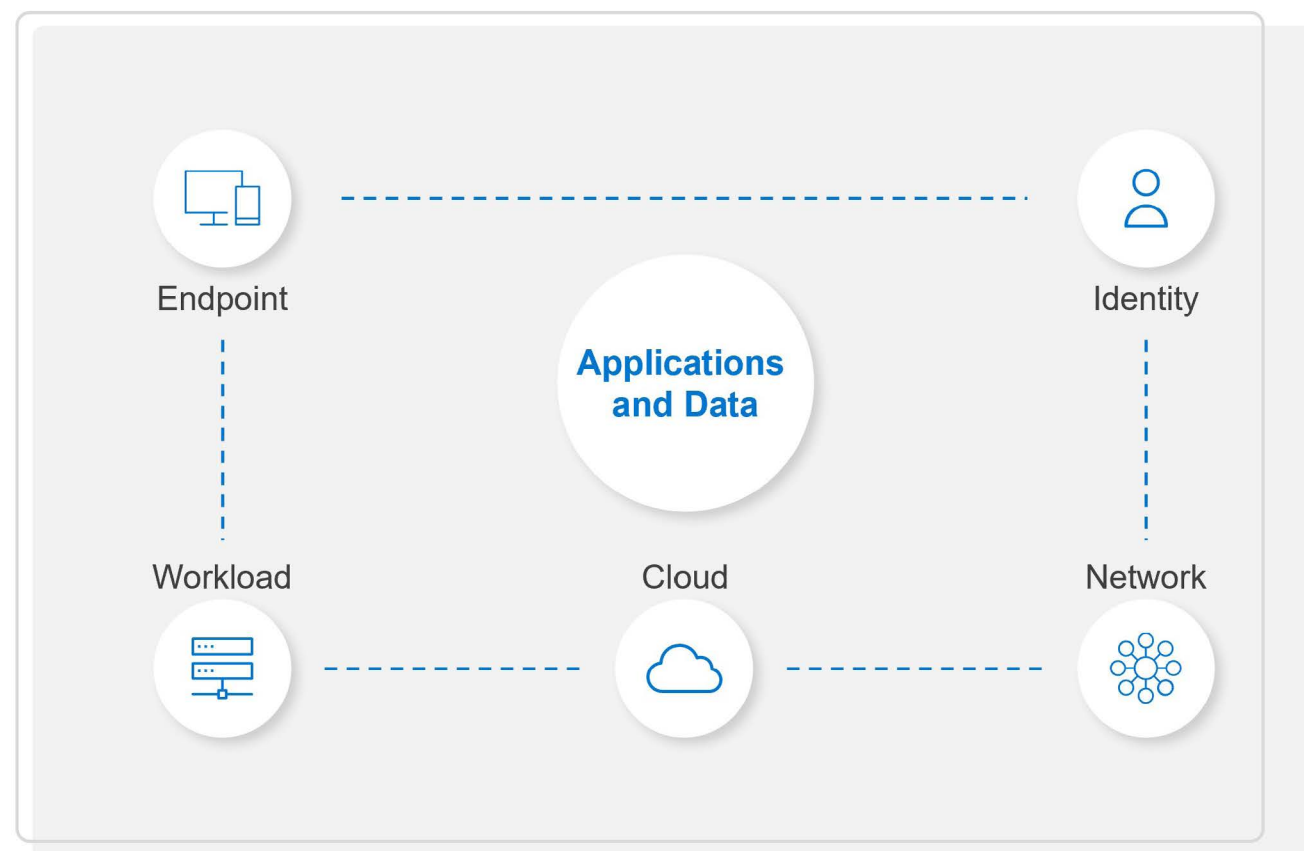


Säkerhets- strategier måste utvecklas

Vi måste omfamna
den molnbaserade
miljön. Det är där
nollförtroende
kommer in i bilden.

Moderna metoder har gått i riktningen mot större kontroll med bättre kommunikation mellan kontrollpunkterna. Men i takt med att vi anammar en miljö som allt mer präglas av distans/hybridarbete måste vi stärka gränsen ännu mer.

Nästa ...



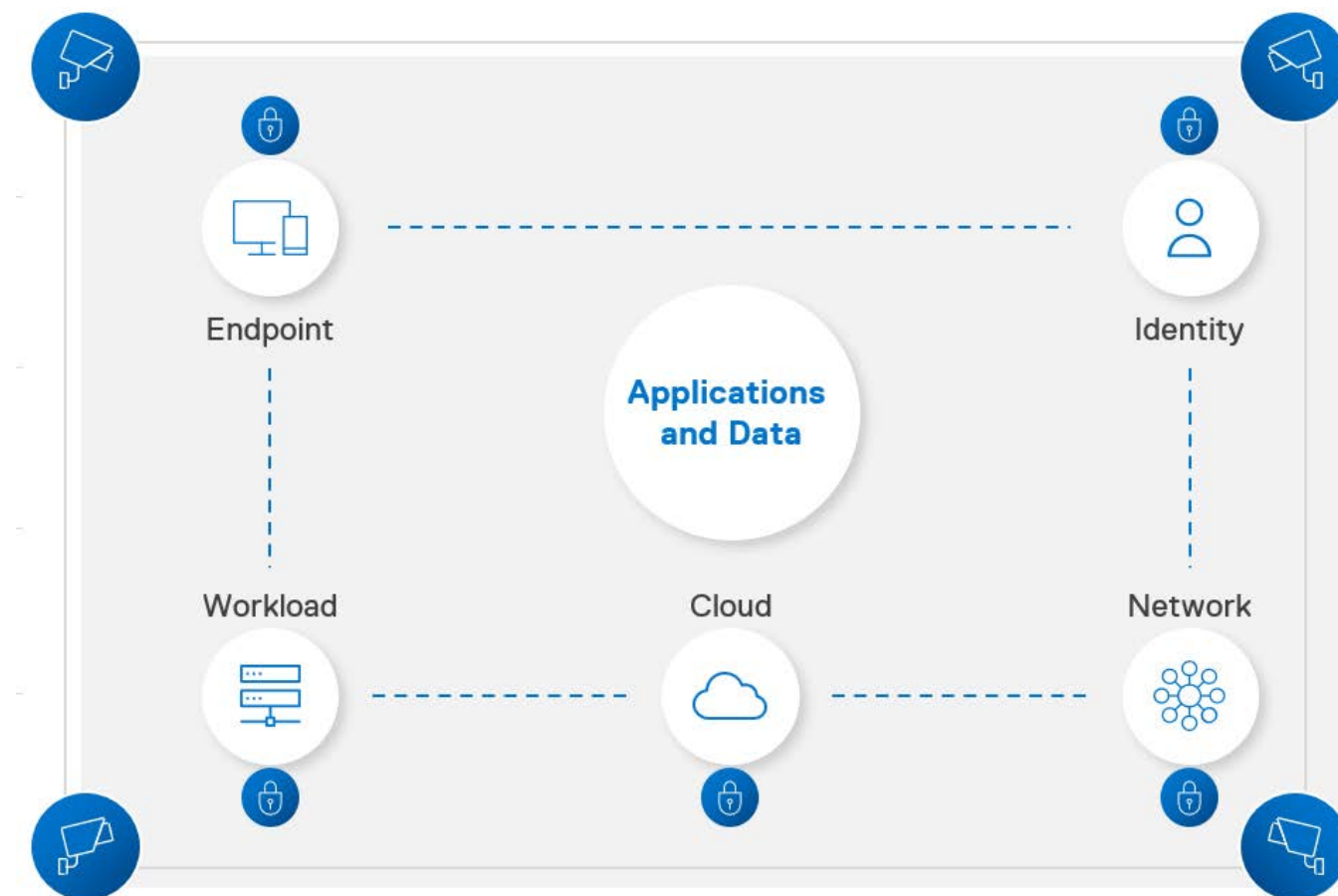
Säkerhetsstrategier måste utvecklas

Vi måste omfamna den molnbaserade miljön. Det är där nollförtroende kommer in i bilden.

Idag arbetar anställda från alla möjliga platser – hemma, på kaféer, på hotell – ofta genom att använda oskyddat Wi-Fi med begränsad eller ingen anslutning tillbaka till brandväggsskyddade kontor och datacenter. Standarden kan vara en direktanslutning från sina enheter till internet där de ansluter till molnbaserade

filserverar och SaaS-program (software-as-a-service) – och arbetar med företagsdata.

I takt med att attackerna blir mer sofistikerade och antalet attackvektorer växer fungerar traditionella säkerhetsstrategier som byggs på underförstått förtroende inte längre. Det är där nollförtroende kommer in i bilden.

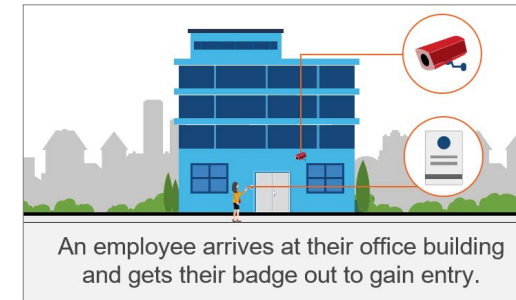


Att förstå grunderna inom nollförtroende

Nollförtroende är ett nytt sätt att se på säkerhet. Det ersätter *underförstått* förtroende – dvs. när användarna väl är autentiserade kan de röra sig fritt i nätverket. Nollförtroende vänder på paradigmet och ger organisationerna full kontroll över IT-miljön.

Vi kan illustrera nollförtroende med ett välbekant koncept: byggandet av säkerhetsprotokoll.

Du arbetar på ett företag. När du blev anställd fick du ett ID-kort och lärde dig säkerhetsprotokollen. Varje dag går du in i byggnaden. Det finns kameror överallt. Du stämplar in på flera ställen. När du sätter dig vid ditt skrivbord låser du upp din dator med ett lösenord.



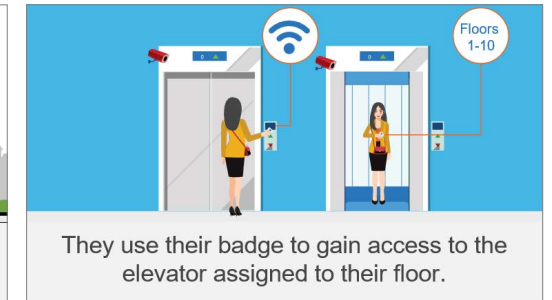
Nästa ...

Att förstå grunderna inom nollförtroende

Nollförtroende är ett nytt sätt att se på säkerhet. Det ersätter *underförstått* förtroende – dvs. när användarna väl är autentiserade kan de röra sig fritt i nätverket. Nollförtroende vänder på paradigmet och ger organisationerna full kontroll över IT-miljön.

Vi kan illustrera nollförtroende med ett välbekant koncept: byggandet av säkerhetsprotokoll.

Du arbetar på ett företag. När du blev anställd fick du ett ID-kort och lärde dig säkerhetsprotokollen. Varje dag går du in i byggnaden. Det finns kameror överallt. Du stämplar in på flera ställen. När du sätter dig vid ditt skrivbord låser du upp din dator med ett lösenord.



Nästa ...

Att förstå grunderna inom nollförtroende

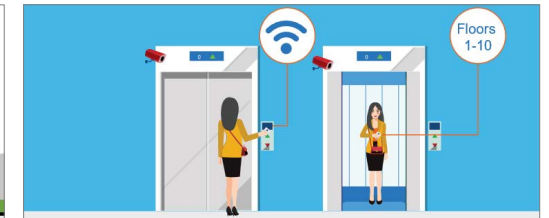
Nollförtroende är ett nytt sätt att se på säkerhet. Det ersätter *underförstått* förtroende – dvs. när användarna väl är autentiserade kan de röra sig fritt i nätverket. Nollförtroende vänder på paradigmet och ger organisationerna full kontroll över IT-miljön.

Vi kan illustrera nollförtroende med ett välbekant koncept: byggandet av säkerhetsprotokoll.

Du arbetar på ett företag. När du blev anställd fick du ett ID-kort och lärde dig säkerhetsprotokollen. Varje dag går du in i byggnaden. Det finns kameror överallt. Du stämplar in på flera ställen. När du sätter dig vid ditt skrivbord låser du upp din dator med ett lösenord.



An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.



The employee uses their badge again to activate their floor selection in the elevator.

Nästa ...

Att förstå grunderna inom nollförtroende

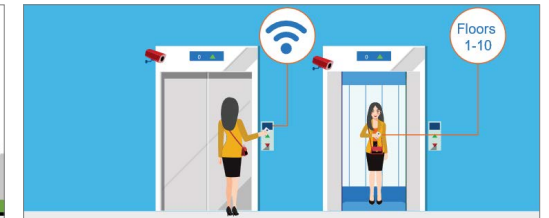
Nollförtroende är ett nytt sätt att se på säkerhet. Det ersätter *underförstått* förtroende – dvs. när användarna väl är autentiserade kan de röra sig fritt i nätverket. Nollförtroende vänder på paradigmet och ger organisationerna full kontroll över IT-miljön.

Vi kan illustrera nollförtroende med ett välbekant koncept: byggandet av säkerhetsprotokoll.

Du arbetar på ett företag. När du blev anställd fick du ett ID-kort och lärde dig säkerhetsprotokollen. Varje dag går du in i byggnaden. Det finns kameror överallt. Du stämplar in på flera ställen. När du sätter dig vid ditt skrivbord låser du upp din dator med ett lösenord.



An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.



The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

Nästa ...

Att förstå grunderna inom nollförtroende

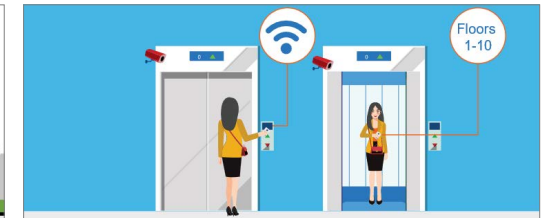
Nollförtroende är ett nytt sätt att se på säkerhet. Det ersätter *underförstått* förtroende – dvs. när användarna väl är autentiserade kan de röra sig fritt i nätverket. Nollförtroende vänder på paradigmet och ger organisationerna full kontroll över IT-miljön.

Vi kan illustrera nollförtroende med ett välbekant koncept: byggandet av säkerhetsprotokoll.

Du arbetar på ett företag. När du blev anställd fick du ett ID-kort och lärde dig säkerhetsprotokollen. Varje dag går du in i byggnaden. Det finns kameror överallt. Du stämplar in på flera ställen. När du sätter dig vid ditt skrivbord låser du upp din dator med ett lösenord.



An employee arrives at their office building and gets their badge out to gain entry.



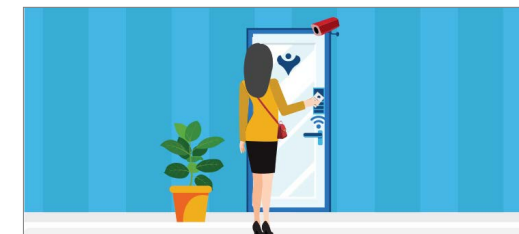
They use their badge to gain access to the elevator assigned to their floor.



The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.



They swipe their ID card to gain entry to their suite.

Nästa ...

Att förstå grunderna inom nollförtroende

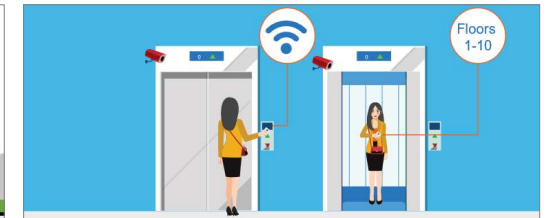
Nollförtroende är ett nytt sätt att se på säkerhet. Det ersätter *underförstått* förtroende – dvs. när användarna väl är autentiserade kan de röra sig fritt i nätverket. Nollförtroende vänder på paradigmet och ger organisationerna full kontroll över IT-miljön.

Vi kan illustrera nollförtroende med ett välbekant koncept: byggandet av säkerhetsprotokoll.

Du arbetar på ett företag. När du blev anställd fick du ett ID-kort och lärde dig säkerhetsprotokollen. Varje dag går du in i byggnaden. Det finns kameror överallt. Du stämplar in på flera ställen. När du sätter dig vid ditt skrivbord låser du upp din dator med ett lösenord.



An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.



The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.



They swipe their ID card to gain entry to their suite.



The employee arrives at their desk and unlocks their computer using a password.

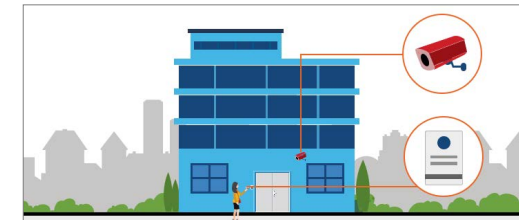
Nästa ...

Att förstå grunderna inom nollförtroende

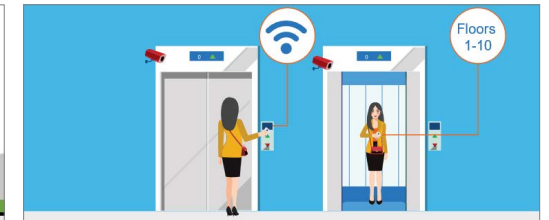
Så här fungerar nollförtroende.

Din arbetsgivare identifierade dig på dag ett. All åtkomst du har begärt sedan dess har verifierats för att skydda organisationens tillgångar (användare, data osv.). Säkerhetsvakter övervakar alla rörelser inuti byggnaden på bildskärmar för ökad trygghet. Alla avvikande beteenden – t.ex. att försöka komma in i en lokal utan tillbörlig anledning – undersöks.

Idag befinner sig användare, enheter, program och data utanför sina företagsnätverk i större utsträckning än någonsin tidigare. Som följd har användaridentitet blivit en blind fläck och komprometterade identiteter är nyckelelementet i de flesta läckorna. Kursen inom nollförtroende åtgärdar detta.



An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.



The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.



They swipe their ID card to gain entry to their suite.



The employee arrives at their desk and unlocks their computer using a password.

Att aktivera nollförtroende- principer

Slutpunktssäkerhet
är en kritisk del av
en övergång till
nollförtroende.

För en effektiv nollförtroende-strategi måste du säkra slutpunkterna.

Enligt MITRE ATT&CK®-ramen finns det idag nio "första åtkomstmetoder" som motståndare använder för att få åtkomst till nätverk (*se illustration*).^{vi} Som forskningen visar kan traditionella försvar inte hålla slutpunkterna säkra i den molnbaserade världen. En angripare behöver bara en enda ingångspunkt. Med hjälp av slutpunkter kan hotaktörer utnyttja massor av sårbarheter genom en enhets hela livscykel.

I takt med att antalet enheter på ett nätverk växer blir slutpunkter en allt större attackvektor.

Säkerhetspolicyer i en nollförtroende-modell definierar det "säkra" i uttrycklig detalj – allt annat blockeras. Hothanderingen håller sedan utkik efter allt som avviker från det säkra, flaggar ovanligt beteende och utlöser den lämpliga åtgärden för att ta itu med det potentiella hotet.

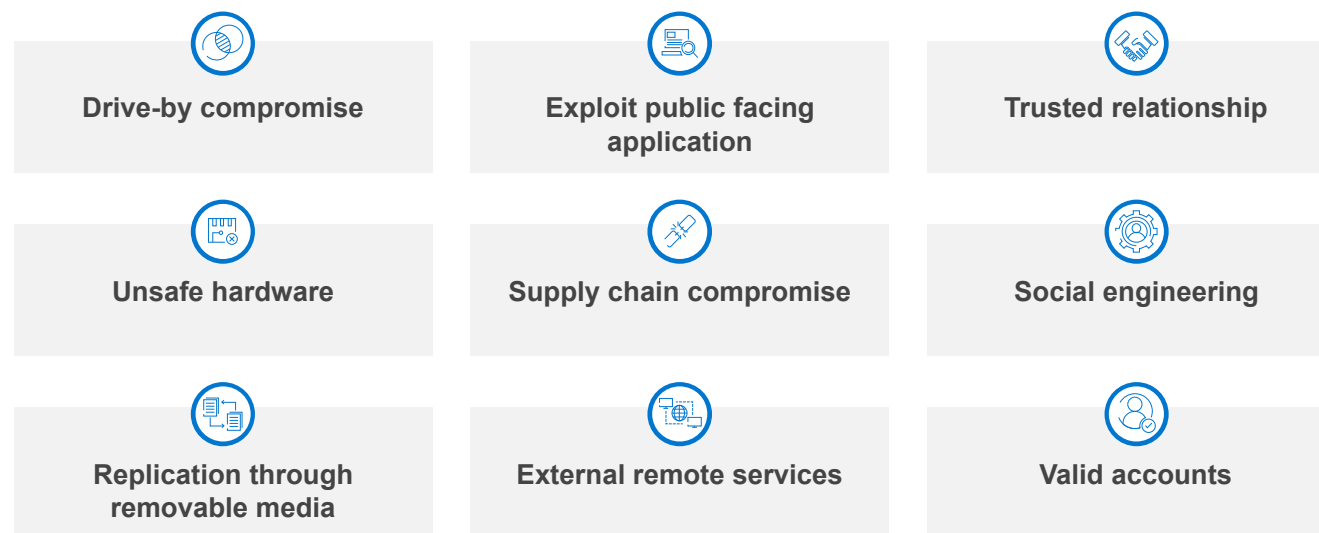


Illustration 1/3

Att aktivera nollförtroende- principer

Slutpunktssäkerhet
är en kritisk del av
en övergång till
nollförtroende.

För en effektiv nollförtroende-strategi måste du säkra slutpunkterna.

Enligt MITRE ATT&CK®-ramen finns det idag nio "första åtkomstmetoder" som motståndare använder för att få åtkomst till nätverk (*se illustration*).^{vi} Som forskningen visar kan traditionella försvar inte hålla slutpunkterna säkra i den molnbaserade världen. En angripare behöver bara en enda ingångspunkt. Med hjälp av slutpunkter kan hotaktörer utnyttja massor av sårbarheter genom en enhets hela livscykel.

I takt med att antalet enheter på ett nätverk växer blir slutpunkter en allt större attackvektor.

Säkerhetspolicyer i en nollförtroende-modell definierar det "säkra" i uttrycklig detalj – allt annat blockeras. Hothanderingen håller sedan utkik efter allt som avviker från det säkra, flaggar ovanligt beteende och utlöser den lämpliga åtgärden för att ta itu med det potentiella hotet.

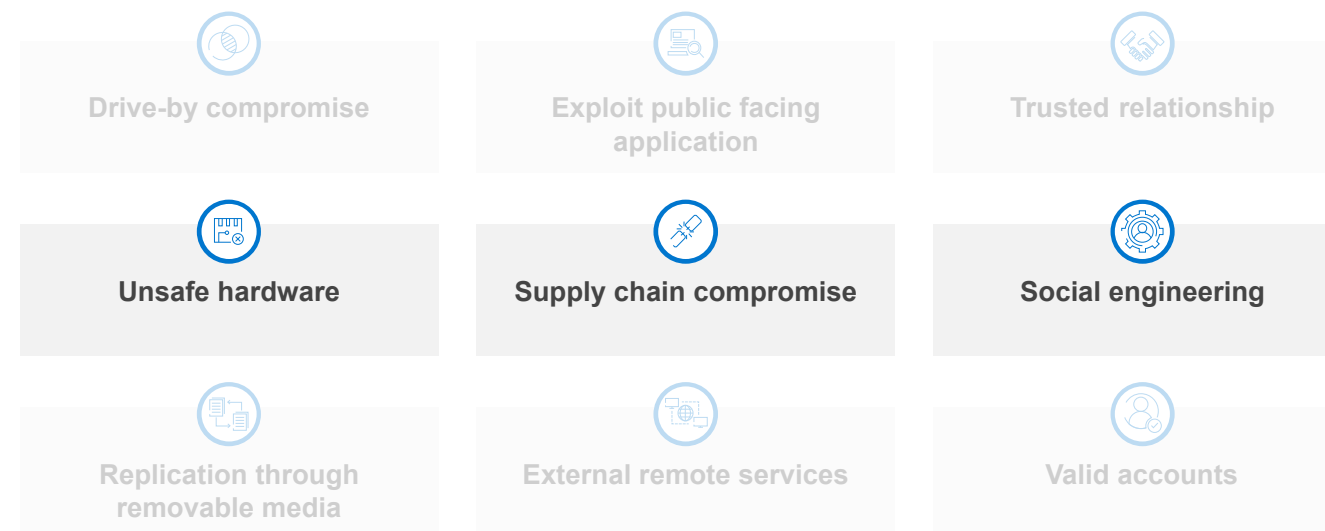


Illustration 2/3

Att aktivera nollförtroende- principer

Slutpunktssäkerhet
är en kritisk del av
en övergång till
nollförtroende.

För en effektiv nollförtroende-strategi måste du säkra slutpunkterna.

Enligt MITRE ATT&CK®-ramen finns det idag nio "första åtkomstmetoder" som motståndare använder för att få åtkomst till nätverk (se *illustration*).^{vi} Som forskningen visar kan traditionella försvar inte hålla slutpunkterna säkra i den molnbaserade världen. En angripare behöver bara en enda ingångspunkt. Med hjälp av slutpunkter kan hotaktörer utnyttja massor av sårbarheter genom en enhets hela livscykel.

I takt med att antalet enheter på ett nätverk växer blir slutpunkter en allt större attackvektor.

Säkerhetspolicyer i en nollförtroende-modell definierar det "säkra" i uttrycklig detalj – allt annat blockeras. Hothantering håller sedan utkik efter allt som avviker från det säkra, flaggar ovanligt beteende och utlöser den lämpliga åtgärden för att ta itu med det potentiella hotet.

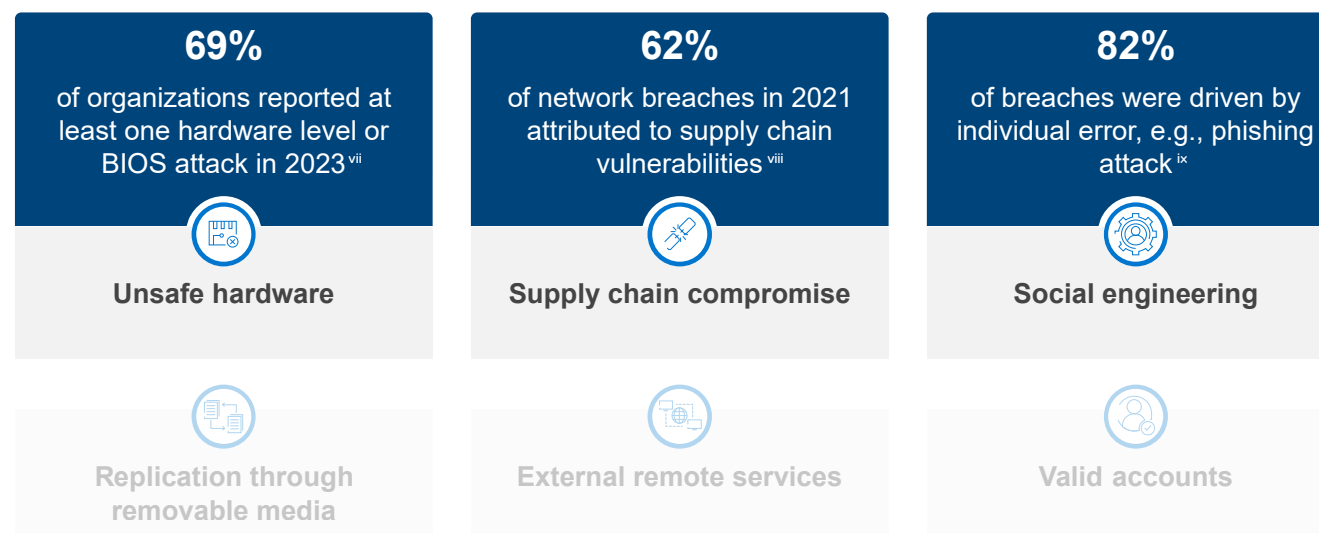


Illustration 3/3

Tre rekommendationer för att förbereda för nollförtroende

Positionera ditt företag för en lyckad övergång till nollförtroende.

1

Etablera rätt policyer och kontroller som stöder ditt företags prioriteringar.

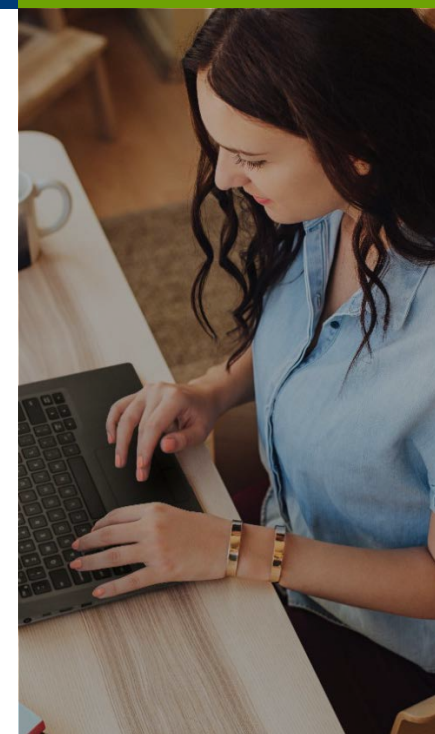
Policymotorer och policyhantering är kritiska för effektiva implementeringar av nollförtroende. Ingen organisation har en obegränsad säkerhetsbudget så du måste avgöra vad som är viktigast för din verksamhet. Vilka är de viktigaste tillgångarna och de immateriella rättigheter du vill skydda? Väg den attackytan mot ditt företags tillåtna risk.

Granska sedan de i nuläget aktiva policyerna och kontrollerna. Dagens risker kommer från den molnbaserade värld vi lever i. Tar din policymotor med det i beräkningarna?

Med aktiva policyer som styr åtkomst till dina viktigaste tillgångar kan du sedan utöka omfattningen.

MER INFORMATION

För mer information kan du [titta på den här videon](#) där cyberexperter från Dell pratar om viktiga säkerhetsrisker som företag står inför idag.



Då fler användare, enheter, program och data befinner sig utanför sina företagsnätverk i större utsträckning än någonsin tidigare uppger 82 % av IT-beslutsfattare att de har behövt omvärdera sina säkerhetspolicyer.*

Tre rekommendationer för att förbereda för nollförtroende

Positionera ditt företag för en lyckad övergång till nollförtroende.

2

Börja med säkra enheter.

Planera nollförtroende på en säker grund. Stärk dina försvar med enheter som har utformats och utvecklats med säkerhet i åtanke. Detta omfattar:

A. Skydd baserat på hårdvara och fast mjukvara som säkrar slutpunktsstacken och tillåter synlighet (t.ex. upptäcka om ett BIOS har komprometterats och varna IT-avdelningen). Utrusta din organisation med teknik som verifierar identitet vid varje ny åtkomstbegäran med en så liten inverkan på medarbetarnas produktivitet som möjligt.

B. Skydd och integritetskontroller för leverantörskedjan som säkrar varje steg i datorns livscykel. Som vi har sett de senaste åren kan attacker mot leverantörskedjor vara förödande. I en arkitektur med verkligt nollförtroende börjar autentisering, verifiering och övervakning i leverantörskedjan. Samarbeta med leverantörer som 1) använder säker praxis och 2) låter dig validera dina enheters integritet, från inköp till tillverkning till leverans.

MER INFORMATION

För mer information om bästa praxis inom enhetssäkerhet kan du läsa Dell and Intels informationsdokument, [*Achieving Pervasive Security Above and Below the OS*](#).



År 2021 spred ett IT-hanteringsföretag en ransomware-attack till minst 1 500 kunder.^{xi}

Tre rekommendationer för att förbereda för nollförtroende

Positionera ditt företag för en lyckad övergång till nollförtroende.

3

Sträva efter smidig integrering och interoperabilitet i hela ditt ekosystem.

Tre saker är avgörande för att uppnå en effektiv säkerhetsställning på hög nivå:

- A. Integrering av alla försvar i IT-ekosystemet
- B. Synlighet i realtid samt
- C. Förmåga att vidta åtgärder när det behövs.

I vår molnbaserade värld, där till och med den minsta okontrollerade sårbarheten kan bli till en mardröm, är det viktigt att alla system känner igen potentiella hot och är inställda på att vidta nödvändiga åtgärder.

Är dina system integrerade eller är de silobaserade? Kan din policymotor utlösa ett specifikt arbetsflöde när en IT-administratör blir varnad om ett korrupt

BIOS i nätverket? I en integrerad miljö borde automatiseringar omedelbart sätta BIOS i fråga i karantän, begränsa all ytterligare åtkomst och släppa korrigeringar.

Har du synlighet in i alla dina slutpunkter? Du ska helst ha en stor mängd telemetri som flödar in från alla lager, från leverantörskedja (t.ex. lastkajen) till den fasta mjukvaran (t.ex. sabotagevarningar på BIOS-nivå).

Men den telemetrin är bara så bra som dina integreringar. Kan du omsätta dina data i åtgärder? Det är viktigt att du har rätt resurser – t.ex. skicklig cybersäkerhetspersonal – för att förstå de data- och programarbetsflöden som hanterar problem.



41 % av organisationer driftsätter nollförtroende^{xii}

Viktiga lärdomar

Säkerhetens framtid stavas nollförtroende.

- När vi omfamnade arbetets framtid blev attackvektorerna så många fler.
- En läcka är bara en tidsfråga. Minimera attackytan med försvar som förbereder för det värsta.
- Nollförtroende är ett nytt förhållningssätt gentemot säkerhet som ger organisationer explicit kontroll över IT-miljön.
- Slutpunktsskydd med aktivering av nollförtroende-principer är nyckeln till att bibehålla en säker, modern grund.
- Identifiera dina viktigaste tillgångar för att prioritera konstruktionen och implementeringen av din nollförtroende-arkitektur.
- Köp in enheter från leverantörer som erbjuder inbyggt skydd och som investerar i sina kontroller av leverantörskedjan.
- Utvärdera interoperabiliteten mellan säkerhet och IT. Fortsätt att bädda in arbetsflöden för att stärka din säkerhetsställning.

Ta nästa steg

Säkerhet är ett överväldigande ämne för organisationer av alla storlekar. Samarbeta med en erfaren säkerhets- och teknikpartner för att få hjälp med att effektivisera din övergång till nollförtroende.

Dell Trusted Workspace hjälper till med att säkra slutpunkter för en modern, nollförtroende-redo IT-miljö. Minska attackytan med en heltäckande portfölj av hårdvaru- och mjukvaruskydd – bara hos Dell. Vår mycket koordinerade och försvarsbaserade strategi avvärjer hot genom att kombinera inbyggda skydd med kontinuerlig vaksamhet. Slutanvändare håller produktiviteten uppe och IT-avdelningen känner sig trygg med säkerhetslösningar som är byggda för dagens molnbaserade värld.

Kontakta oss: global.security.sales@dell.com

Besök oss: Dell.com/Endpoint-Security

Följ oss: [LinkedIn @DellTechnologies](#) | [Twitter @DellTech](#)

ⁱ Cybersecurity Almanac 2nd Edition. Cybersecurity Ventures, 2022 <https://cybersecurityventures.com/cybersecurity-almanac-2022/>

ⁱⁱ Ponemon Institute and IBM, Cost of a Data Breach Report, 2024 <https://www.ibm.com/security/data-breach>

ⁱⁱⁱ American College of Cardiology, You Will Be Hacked. Planera nu: Cybersecurity in Health Care, 2021 <https://www.acc.org/Latest-in-Cardiology/Articles/2021/11/01/01/42/Feature-You-Will-Be-Hacked-Plan-Now-Cybersecurity-in-Health-Care>

^{iv} Ponemon Institute and IBM, Cost of a Data Breach Report, 2024 <https://www.ibm.com/security/data-breach>

^v ESG Complete Survey Results, Security Hygiene and Posture Management, 2022 <https://www.esg-global.com/research/esg-complete-survey-results-security-hygiene-and-posture-management>

^{vi} MITRE ATT&CK <https://attack.mitre.org/tactics/TA0001/>

^{vii} Futurum Group, Endpoint Security Trends, 2023. <https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/industry-market/futurum-group-endpoint-security-trends-research-report.pdf>

^{viii} Verizon Data Breach Investigations Report, 2022 <https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/>

^{ix} Verizon Data Breach Investigations Report, 2022 <https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/>

^x Absolute Endpoint Risk Report, 2021 <https://www.absolute.com/go/reports/endpoint-risk-report/>

^{xi} TechTarget, 2021 <https://www.techtarget.com/searchsecurity/news/252503605/Kaseya-1500-organizations-affected-by-REvil-attacks>

^{xii} Ponemon Institute and IBM, Cost of a Data Breach Report, 2022 <https://www.ibm.com/security/data-breach>

Upphovsrätt © 2024 Dell Inc. eller dess dotterbolag. Med ensamrätt. Dell Technologies, Dell och andra varumärken är varumärken som tillhör Dell Inc. eller dess dotterbolag. Andra varumärken kan vara varumärken som tillhör sina respektive ägare.