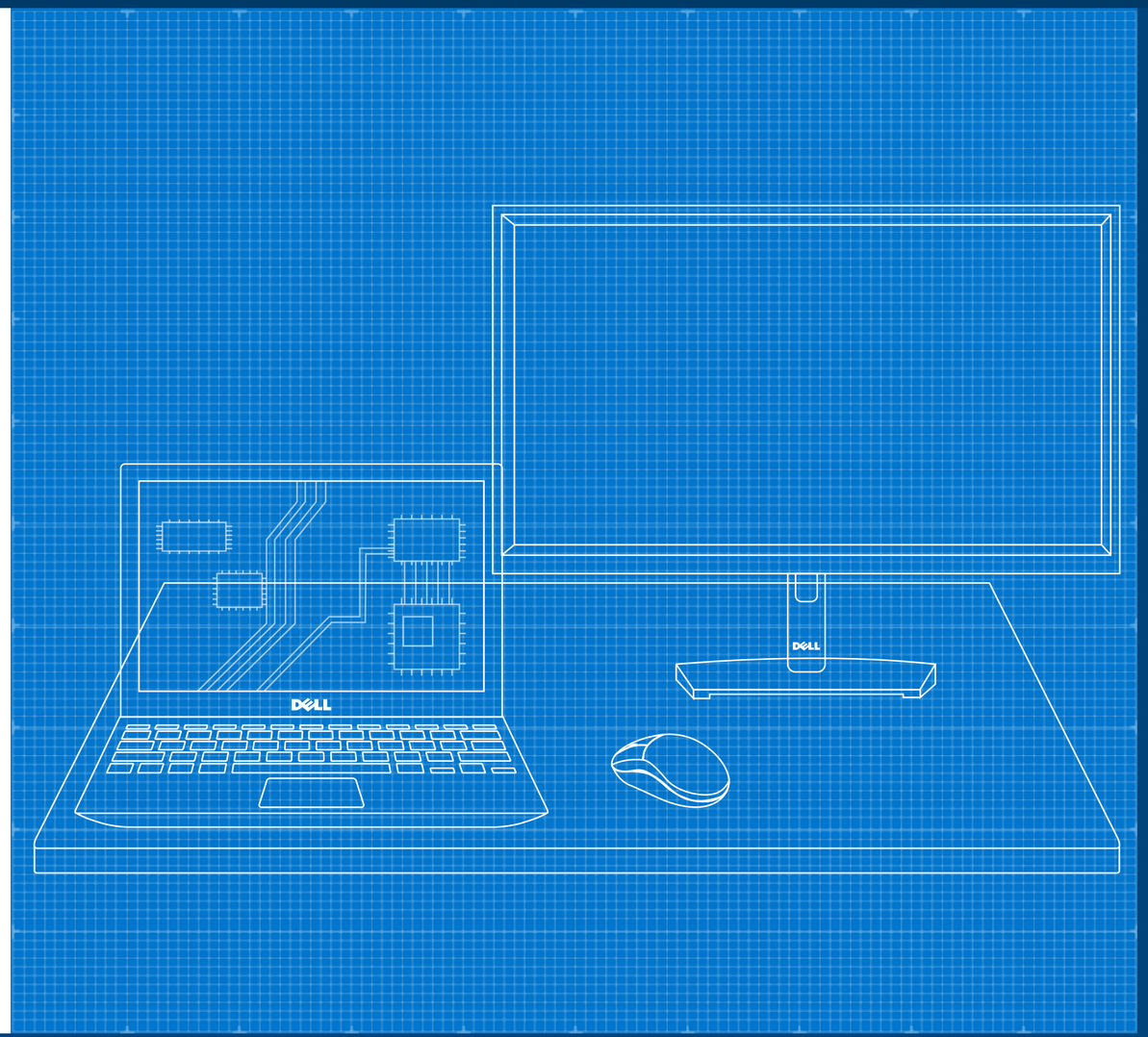
DELL Technologies

Strukturen hos en betrodd arbetsyta

Förbättra säkerheten i datorparken med hjälp av flera lager av försvar



Sammanfattning

Cyberattacker är inte bara oundvikliga. De blir också allt fler och allt mer sofistikerade. Slutpunktsenheter, nätverk och molnmiljöer har blivit viktiga måltavlor.

I denna eBook får IT- och säkerhetsbeslutsfattare vägledning i de element som krävs för att skapa ett effektivt slutpunktsförsvar i detta föränderliga hotlandskap.

Innehållsförteckning

Hotbilden

Övergången till hybridarbete medförde en ny nivå av komplexitet och attackvektorer – och **och slutpunkter, nätverk och moln utgör stora attackytor.**

Dessutom använder angripare numera sofistikerade tekniker som riktar sig mot olika lager av datorstacken, vilket innebär att de smälter in med giltiga systemprocesser. Vissa metoder tillåter till och med att angripare får privilegierad åtkomst och kan inaktivera mjukvaruskydd *helt oupptäckta*.

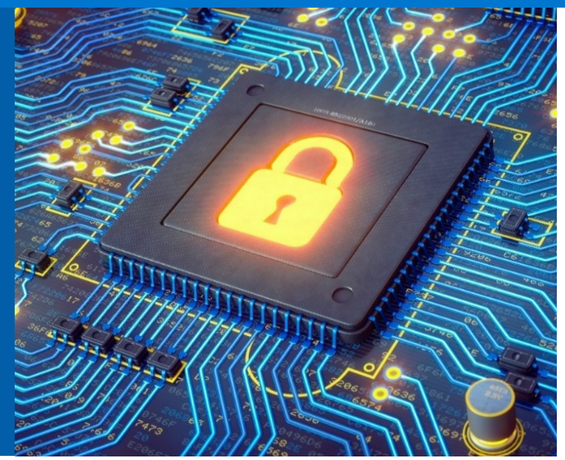
För att bekämpa dessa hot har många organisationer påbörjat en resa mot nollförtroende. Men för att kunna tillämpa nollförtroendeprinciperna måste du kunna upprätthålla enhetens förtroende.

Hur upprätthåller du enhetsförtroende när attacker blir allt vanligare och avancerad teknik skapar nya attackvektorer?

[1] CrowdStrike Global Threat Report, 2024.
[2]Dell Innovation Index, 2023.

Visste du att …

75 % av attackerna under 2023 var inte baserade på skadligt program[1]



Endast 41 % av de tillfrågade organisationerna kan med tillförsikt säga att säkerheten är inbäddad i deras teknik och program[2]

Utforska nollförtroende för att påskynda cyberelasticiteten. Se vår eBook: *Slutpunktssäkerhet är ett kärnelement i din resa mot nollförtroende*.

Utmaningar

För effektiv slutpunktssäkerhet är det viktigt att förstå hur dina motståndare arbetar.

Givet den potentiella belöningen av ett lyckat intrång **gör angripare ofta flera försök mot samma organisation, samt utnyttjar olika metoder och ingångspunkter för att förbättra sina odds.** Till exempel kan angripare försöka dra fördel av sårbarheter via dussintals vektorer under en enda enhets livscykel.

Befintligt försvar gör inte tillräckligt för att hålla slutpunkter säkra. När organisationer stärker försvaret vid en attackyta, förflyttar sig hotaktörerna bara till en annan. När världen blev hybrid kunde hotaktörer identifiera nya slutpunktsattackvektorer, vilket har lett till förödande konsekvenser.

Se attackexempel till höger

Attack mot leverantörskedjan: Riktar in sig på leverantörer för att få tillgång till deras – och, i förlängningen, deras kunders – system, data och/eller nätverk. **EXEMPEL: En attack mot en hårdvaruleverantörskedja initierad av komponentmanipulering:**

Angripare hejdar en datorleverans och byter hårddiskar.

IT-avdelningen installerar de komprometterade enheterna över hela företaget.

Angripare installerar skadliga program för att kunna extrahera inloggningsuppgifter när användare loggar in.

Attack som inbegriper social manipulation Lurar slutanvändare att tillhandahålla känslig information som kan användas för att få åtkomst till enheter och nätverk. **EXEMPEL: En spoofingattack, initierad av ett nätfiskemeddelande:**

Slutanvändare faller för ett nätfiskemeddelande och matar in sina inloggningsuppgifter på en falsk webbsida.

Angriparen använder giltiga inloggningsuppgifter för att komma åt nätverket på distans.

Angriparen exfiltrerar data över en webbtjänst, krypterar stulna data och begär en lösensumma.

Säkra den moderna arbetsytan

När det gäller slutpunktsskydd behöver du förebyggande, detektering och svar, samt återställning och åtgärder i olika faser under enhetens hela livscykel – från inköp och tillverkning av datorer, till frakt och installation, under användning och vid avyttring. Tänk dig storleken på den sammanlagda attackytan!

Den effektivaste cybersäkerhetsstrategin är den som utgår från det värsta scenariot. En sådan strategi förutsätter att ett intrång är möjligt och bäddar in flera lager av skydd för att störa attacken så snabbt och så ofta som möjligt. Den inbegriper också åtgärder avsedda att minimera risken för att en återkommande händelse inträffar.

[3]Dell Innovation Index, 2023.

FÖREBYGGANDE ÅTGÄRDER	DETEKTERING OCH SVAR	ÅTERSTÄLLNING OCH ÅTGÄRDER
Gör dig själv till en mindre måltavla med hjälp av försvar utformat för att blockera attacker.	*Var alltid beredd på intrång och var vaksam.*	*Dämpa effekten av en attack och återgå till arbetet.*

Strukturen hos en betrodd arbetsyta

Modern slutpunktssäkerhet kräver tre saker:

1. **Mjukvarusäkerhet:** Idag, mer än någonsin tidigare, hittar vi användare, enheter och data utanför företagets nätverk. Mjukvarusäkerhet skyddar inte bara enheter, utan utökar också skyddet till nätverks- och molnmiljöer där skadlig aktivitet ofta har sitt ursprung.

2. **Hårdvarusäkerhet:** Enheter måste ha inbyggda säkerhetsfunktioner. Detta gäller säkerhet för hårdvara och fast programvara som skyddar enheten som används. För att försvara arbetsytan måste du ha inbyggda funktioner som ger dig synlighet och kontroll över enheten.

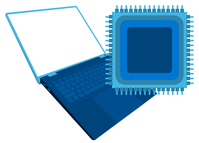
3. **Säkerhet i leverantörskedjan:** Enheter måste byggas på ett säkert sätt. Det här innebär att arbeta med leverantörer som a) förstår hotbilden och b) kan använda den kunskapen i takt med att landskapet utvecklas. Säker datordesign, utveckling och testning minimerar risken för produktsårbarheter, medan kontroll av leverantörskedjan minskar risken för produktmanipulation.

Packa upp flera lager av säkerhet

(Representativa exempel på de säkerhetsåtgärder som listas)

Mjukvarusäkerhet

- Nästa generations antivirus (NGAV)
- Slutpunktsdetektering och svar (EDR)
- Managed Detection And Response (XDR)
- Molnbaserat dataskydd
- Nätverksskydd
- Automatiserad självläkning



Säkerhet för hårdvara och fast programvara

- Verifiering vid uppstart
- Verifiering vid körning
- Användarautentisering
- Säkerhetsmeddelanden och varningar/telemetri

Säkerhet i leverantörskedjan

- Rutiner för säker utveckling
- Rutiner för säkra leverantörskedjor
- Komponentverifiering
- Manipuleringssäker förpackning

Vår strategi: Dell Trusted Workspace

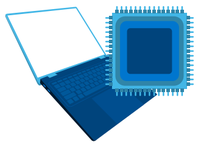
Dell är en säkerhets- och IT-partner för organisationer över hela världen. Till skillnad från punktlösningar fokuserar Dell på övergripande säkerhetsresultat och erbjuder en uppsättning lösningar som stör attackfaserna och gör dig mer motståndskraftig mot cyberattacker. **Dell Trusted Workspace omfattar:**

- Unikt **skydd för hårdvara och fast mjukvara** som gör Dell-datorerna till världens säkraste kommersiella datorer.[4] *(Medbyggd och inbyggd säkerhet)*
- Ett ekosystem av **branschledande mjukvarupartner** erbjuder skydd mot avancerat hot, för enheten, nätverket och molnet. *(Påbyggd säkerhet)*

[4] Enligt Dells interna analys i oktober 2024. Gäller datorer med Intel-processorer. Alla funktioner är inte tillgängliga för alla datorer. För vissa funktioner krävs ytterligare köp. Validerad av Principled Technologies. En jämförelse av säkerhetsfunktioner, april 2024.

Påbyggd mjukvarusäkerhet från partners ekosystem

- **Dell SafeGuard and Response: CrowdStrike** och **Secureworks** möjliggör hotupptäckt, svar och åtgärder.
- **Dell SafeData: Netskope** erbjuder synlighet, övervakning och förebyggande av dataförlust för molnbaserade program. **Absolute** möjliggör självläkning för program och nätverk.



Inbyggd säkerhet för hårdvara och fast mjukvara via världens säkraste kommersiella datorer[4]

Exempel på funktioner som skyddar enheten under användning:

- **Dell SafeBIOS** med säkerhetsfunktionerna för extern BIOS-verifiering*, Indicators of Attack* samt CVE-detektering* hjälper till att fånga upp skadlig aktivitet innan datorn komprometteras.
- **SafeID:** skyddar användaruppgifter på ett dedikerat säkerhetschip.*
- **Verifiering av fast programvara utanför värddatorn** skyddar integriteten hos privilegierad fast programvara.*
- Med **Dell Trusted Device-appen** integrerar Dell enhetstelemetri med branschledande mjukvara så att säkerheten i hela datorflottor kan förbättras.*

Medbyggd säkerhet i leverantörskedjan hjälper till att säkerställa att datorerna är säkra från första uppstart

- **Dell SafeSupply Chain** – tillägg som Dell Secured Component Verification* (SCV) ger extra garantier för produktintegriteten.

** Unikt för Dell*

Få allt att falla på plats

Med både hård-och mjukvarubaserade motåtgärder på plats kan du minska attackytan med försvar som hjälper till att förhindra vanliga attacker.

Detekterings- och svarsfunktioner hanterar smygande attacker som skulle kunna slinka igenom.

I fallet med en attack som inbegriper social manipulation, som diskuteras på sidan 4, när du arbetar med Dell, kan förebyggande åtgärder som **rutiner för säkra leverantörskedjor** störa en attack tidigt i attackfaserna. Om en attack slinker igenom finns också ytterligare motåtgärder – t.ex. **SCV** – på plats.

I fallet med en attack som inbegriper social manipulation, och även om en angripare lyckas lura en användare att lämna över giltiga inloggningsuppgifter, kan **hårdvarubaserad användarverifiering såsom SafeID** sätta stopp för angriparens framfart och neka ytterligare åtkomst. Säkerhetsmjukvara såsom **Next-Gen Secure Web Gateway** kan erbjuda ett ytterligare lager av övervakningsskydd.

Motverka en attack mot en hårdvaruleverantörskedja initierad av komponentmanipulering.

Angripare hejdar en datorleverans och byter hårddiskar.

- **Rutiner för säkra leverantörskedjor**
- Manipuleringssäker förpackning
- Dörrlås

IT-avdelningen installerar de komprometterade enheterna över hela företaget.

- Säker komponentverifiering (SCV)
- Verifiering vid körning

Angripare installerar skadliga program för att kunna extrahera inloggningsuppgifter när användare loggar in.

- Säkerhetförmedling för molnåtkomst (CASB)
- Next-Gen Secure Web Gateway

Motverka en attack som inbegriper social manipulation initierad av ett nätfiskemeddelande.

Slutanvändare faller för ett nätfiskemeddelande och matar in sina inloggningsuppgifter på en falsk webbsida.

- NGAV
- EDR
- XDR

Angriparen använder giltiga inloggningsuppgifter för att komma åt nätverket på distans.

- Flerfaktorsautentisering med SafeID
- Zero Trust Network Access

Angriparen exfiltrerar data över en webbtjänst, krypterar stulna data och begär en lösensumma.

- Next-Gen Secure Web Gateway + User Entity Behavior Analytics

Viktiga lärdomar

Intrång är oundvikligt. Effektiv slutpunktssäkerhet förutsätter alltid det sämsta tänkbara scenariot och fokuserar på att störa attackfaserna oavsett var de inträffar, från enhet till nätverk till moln.

Det finns ingen lösning som blockerar 100 % av attackerna. Kombinera hård- och mjukvarubaserade motåtgärder för bästa försvar.

För att du ska vara säker måste även dina leverantörer vara säkra. Kräv av dina leverantörer att de beskriver sina säkerhetsåtgärder.

Latitude bärbara datorer och 2-i-1-datorer

För mer information:

Kontakta oss: Global.Security.Sales@Dell.com

Besök oss: Dell.com/Endpoint-Security

Följ oss: LinkedIn @DellTechnologies | X @DellTech

Ta nästa steg

Säkerhet är ett överväldigande ämne för organisationer av alla storlekar. **Samarbeta med en erfaren säkerhets- och teknikpartner för att modernisera slutpunktssäkerheten.**

Dell Trusted Workspace hjälper till med att säkra slutpunkter för en modern, nollförtroende-redo IT-miljö. Minska attackytan med en heltäckande portfölj av hård- 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.