Lita på din säkerhet. Lita på din personal. Med Lenovo.

Så här håller du personalen säker i en föränderlig cybersäkerhetsmiljö 〉

Smarter technology for all

Lenovo

Den ofrånkomliga övergången till hybridarbetet har orsakat en cybersäkerhetsmiljö som är full av utmaningar.

Nuförtiden behöver de flesta medarbetarna ha utrustning som fungerar till hybridarbete. Ett resultat av det är att skyddet mot hot måste utökas så att det täcker flera olika moln och flera olika plattformar.

Det leder till en komplex digital miljö som kan bli en dold fristad för okända hot. Att upprätthålla säkerhetspolicyerna på många olika typer av enheter och i flera olika digitala lager är en riktigt svår uppgift. Det är sådant som man kan ligga vaken om nätterna för, om man är ansvarig för att upprätthålla det skyddet.

Kombinationen av säker maskinvara och molnet – ett unikt partnerskap: Lenovo har ett unikt partnerskap med Microsoft, där maskinvara som drivs av ThinkShield kombineras med Microsoft Cloud Security-tjänsterna.

Security by Design med Lenovo ThinkShield

Vi på Lenovo förstår att det är bråttom med ett omfattande, heltäckande skydd. Vi bygger vår ThinkShield-säkerhetsstrategi på bästa praxis, för att öka säkerheten för vår enhetsportfölj redan på designstadiet.

Det gäller allt från att se till att leveranskedjorna är säkra till att ta fram nya Lenovo-produkter, som är säkra och konstruerade av tillverkarna av världens mest betrodda företagsdatorer.

Vår unika ThinkShield-portfölj med maskinvara, tjänster, programvara och processer ger ett skydd som når alla nivåer i företaget. Våra partnerskap med branschledande säkerhetsleverantörer möjliggör ett omfattande, heltäckande försvar som fångar in och isolerar hoten i en Zero Trust-strategi, som drivs med Microsofts säkerhetslösningar.

Zero Trust. Framtidens cyberskydd. Den nya riktningen.

Zero Trust skiljer sig mycket från vanlig nätverkssäkerhet där det finns ett ”företagsområde” som ska skyddas, eller där enheterna ansluts via ett VPN, vilket i hög grad är normen i dag.

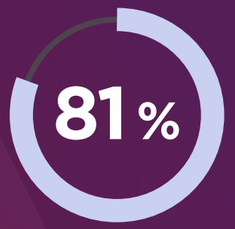
De vägledande principerna för Zero Trust är: ”Lita aldrig på någonting. Kontrollera alltid allting.”

I dagens värld med hybridarbete är det bäst att enheterna inte är betrodda som standard, även när de är anslutna till ett nätverk med behörigheter.

Zero Trust utgår från att det finns en angripare inne i nätverket. Förtroendet byggs upp baserat på **sammanhanget**, vilket kan vara **användarens identitet och plats, enhetens säkerhetsstatus** och vad det är för **app eller tjänst som efterfrågas**. Det sker policykontroller vid varje steg.

Det säkerställer att det bara är **rätt personer med rätt resurser på säkra enheter som kan komma åt dina data**.

Behovet av Zero Trust har aldrig varit mer brådskande:

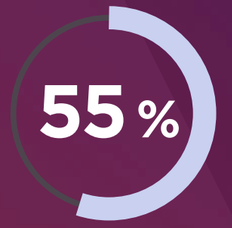


av företagen har påbörjat övergången till hybridarbete[1]

lägre risk för dataintrång[3]

1 070 %

fler ransomware-angrepp mellan juli 2020 och juni 2021[4]



av organisationerna uppger att de har identifierat ett angrepp med nätfiske under de senaste 18 månaderna[2]

färre samtal till IT-avdelning och helpdesk-analytiker[3]

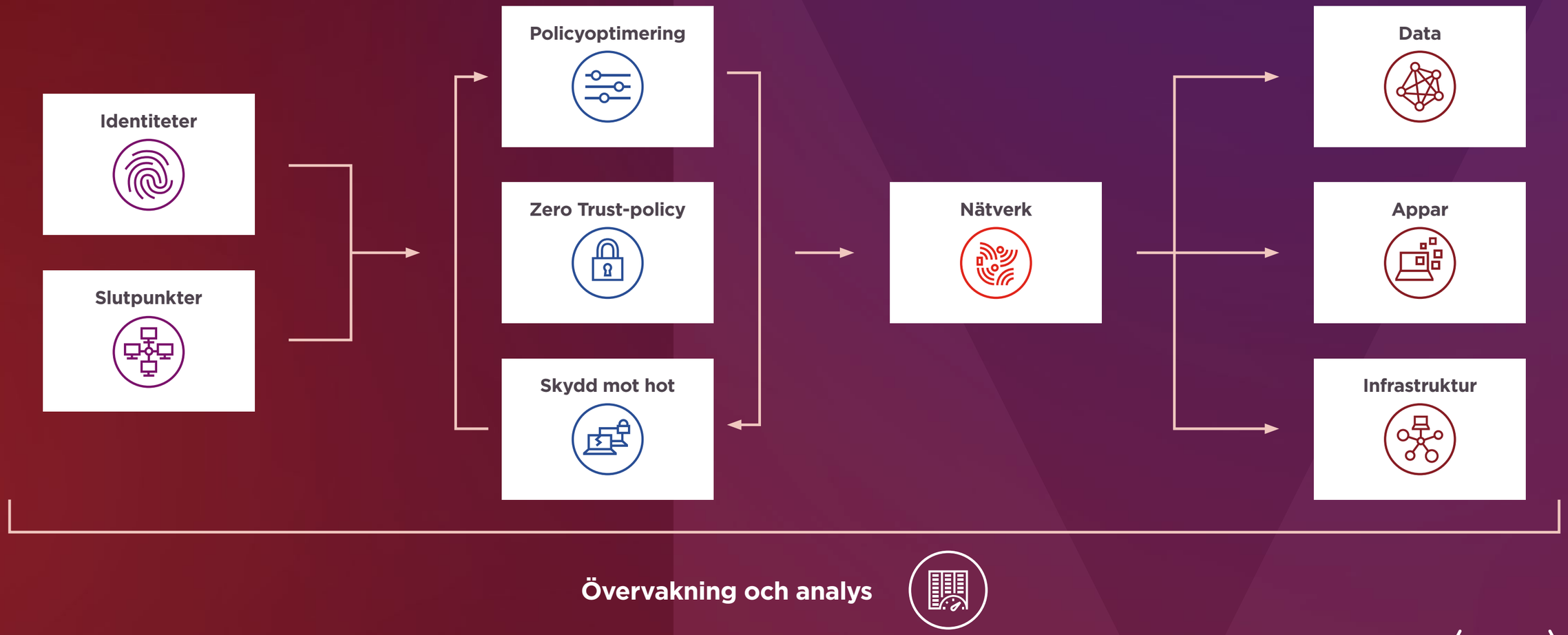
kortare hanteringstiden till följd av förbättrade säkerhetsprocesser[3]

Lenovos ThinkShield-portfölj och Microsofts säkerhetslösningar har utformats specifikt och målmedvetet för att du lättare ska kunna implementera en **heltäckande Zero Trust-strategi** och skydda verksamheten på alla nivåer.

[1] Microsofts rapport Zero Trust Adoption, 2021
[2] IBM:s rapport Cost of a Data Breach, 2021
[3] The Total Economic Impact™ of Zero Trust solutions from Microsoft, december 2021. Studie av Forrester Consulting på uppdrag av Microsoft.
[4] Rapporten 1H Global Threat Landscape från FortiGuard Labs

Så här ser en Zero Trust-arkitektur ut.

Zero Trust-konceptet återfinns i många olika delar av IT-miljön, men skyddet börjar med moderna Windows 11-enheter, användaridentiteter och enhetsövervakning av slutpunkterna.



Förbättra och säkra hybridarbetet för dina medarbetare med hjälp av Lenovos enheter med Windows 11 Pro

Windows 11 Pro – det säkraste Windows-operativsystemet hittills – hjälper dig att **effektivisera hanteringen** av din hybridarbetsplats samtidigt som du **både skyddar dina data och ser till att de går att komma** åt överallt.

Det är ett operativsystem som utformats för moderna enheter som är optimerade för säkerhet, och det ger dig de senaste fördelarna med ett **maskinvarubaserat skydd** som är tätt integrerat med programvaran. Windows 11 Pro har konstruerats särskilt för **säkert hybridarbete** med en **högre grundläggande säkerhetsnivå än Windows 10**. Det innebär att det ställs helt nya krav på skyddet, som ska vara inbyggt och aktiverat som standard.

ThinkPad X1 Carbon

Förbättra säkerheten för din ThinkShield-enhet från Lenovo med Windows 11 Pro med hjälp av molnhantering

Att skydda identiteter och slutpunktsenheter är det första viktiga steget när det gäller att skapa en Zero Trust-strategi. Identiteter och enheter är de två huvudområden som ID-tjuvar, nätfiske, ransomware och andra typer av skadlig programvara och avancerade hot riktas mot.

Kombinera Lenovos Windows 11-enheter med Microsofts molnsäkerhetslösningar och inför en Zero Trust-strategi.

Identitetshantering

- Inför flerfaktorautentisering (MFA), som kan stoppa 99,9 % av identitetsangreppen.
- Tillhandahåller en ”smart” policymotor för villkorsbaserad åtkomst, där du kan ställa in specifika regler för användarens inloggning. När det kombineras med MFA går det att upprätta en kraftfull balans mellan säkerheten och användarnas produktivitet.

Slutpunktshantering

- Se till att apparna följer företagets säkerhetsprotokoll med hjälp av Mobile Access Management (MAM).
- Se till att enheterna uppfyller företagets säkerhetsprotokoll med Mobile Device Management (MDM), vare sig det handlar om företagets enheter eller användarnas egna.

Kontroll, skydd och hantering med fördelarna i Security Cloud-lösningar

Identitetshantering med Azure Active Directory

- Azure Active Directory är en enkel och effektiv molnbaserad tjänst för identitets- och åtkomsthantering med flerfaktorautentisering och villkorsbaserad åtkomst.
- I en och samma lösning kombineras centrala katalogtjänster, hantering av programåtkomst och identitetsskydd.
- Den gör det enklare för dina anställda att på ett säkert sätt komma åt externa resurser, till exempel Microsoft 365, Azure-portalen och tusentals andra SaaS-applikationer.
- Gör interna resurser säkra, till exempel intranätet eller molnappar som utvecklats inom organisationen.

Microsoft Defender for Endpoint

Denna branschledande, molndrivna säkerhetslösning för slutpunkter:

- Gör det enklare att skydda systemet mot ransomware, skadlig kod utanför filer och andra typer av sofistikerade angrepp på Windows, Mac OS, Linux, Android och iOS.
- Upptäcker dolda hot genom att kontinuerligt övervaka kodbeteende och angriparteknikер i realtid, och på så sätt möjliggöra snabb identifiering och åtgärd.
- Automatiserad incidentrespons och åtgärd dygnet runt – hjälper säkerhetsteamen att omedelbart gå från varningar till AI-styrda åtgärder.
- Hotsökning på begäran hanterad av Microsoft-experter.

Microsoft Endpoint Manager

Få slutpunktsenhetshantering och säkerhet på en och samma hanteringsplattform:

- Säkrar, distribuerar och hanterar alla användare, appar och slutpunktsenheter utan att störa befintliga arbetsprocesser.
- Gör det enklare att skapa en modern arbetsplats och upprätta en modern hantering för att hålla data säkra, både i molnet och lokalt.
- Kombinerar tjänster som du kanske redan känner till och använder, som Microsoft Intune, Configuration Manager, Desktop Analytics, samhantering och Windows Autopilot.

Rätt enhet, på rätt plats, i rätt tid med Lenovos Zero Touch-implementeringslösning

Säker, modern teknik är grunden till ett framgångsrikt företag. Men det vanliga, manuella sättet att distribuera tekniken är komplext, tidskrävande och leder lätt till fel.

Nu finns det ett enklare sätt att se till att din hybridarbetande och distansarbetande personal kommer i gång – **Lenovo Zero-Touch-distribution med autopilot**.

Det sätter fart på hybridarbetet, ökar produktiviteten och frigör dina IT-team så att de kan fokusera på innovation som ger tillväxt.

Med **Windows Autopilot** behöver IT-avdelningen inte längre göra nya avbildningar eller konfigurera nya enheter manuellt. Allt görs på distans. På Lenovos Windows 11-enheter har Autopilot konfigurerats i förväg. IT-chefer kan anpassa användarna och tillämpa konfigurationer från vilken plats som helst.

- **Startklart redan när förpackningen öppnas** – det är bara för användaren att slå på enheten så är den klar att använda med några enkla klick.
- **Enkel profilhantering** – skapa, hantera och tilldela upp till 350 olika profiler för att bedöma en användares inställningar och datorupplevelse.
- **Enkel övergång till molnet** – anslut enheter automatiskt till Azure Active Directory och registrera dem med hanteringen av mobila enheter.
- **Problemfri etablering** – personlig och effektiv installation.
- **Spåra framsteg** – med hjälp av Autopilot kan användarna spåra förloppet för enhetskonfigurationen.
- **Produktregistrering** – enheterna registreras automatiskt i tjänsten Autopilot Cloud Deployment.

Anta strategin ”Bättre tillsammans”

Säkerhet direkt ur förpackningen

- **Skydd ända inifrån kärnan** med den kretskortsbaserade säkerheten i TPM 2.0 samt skydd för data och identiteter.
- Enklare och säkrare inloggning med **lösenordslösa autentiseringsmetoder** som Windows Hello for Business.
- Gör det enklare att blockera skadlig kod med ett **inbyggt skydd som redan är aktiverat från början**.
- För att **hålla dig säker redan från början** förhindrar Windows 11 att skadlig kod laddas när du startar datorn.
- Data och nätverk skyddas med en **maskinvarubaserad root-of-trust** som gör det enklare att upprätthålla och verifiera enhetens integritet.

Skydd mot föränderliga hot

- Skydda autentiseringsuppgifter med det **förbättrade skyddet mot nätfiske** i Microsoft Defender Smartscreen.
- Logga in utan händerna med **närvaroidentifiering** – som loggar in dig när du närmar dig datorn och som låser den när du går bort från den.
- Skydda dina mest känsliga data med **Secured-core-datorer från Lenovo**.
- Få ett maskinvarubaserat autentiseringsskydd med **Microsoft Pluton**.
- Dra fördel av **smart hotidentifiering och snabba åtgärder** som baseras på 43 biljoner säkerhetssignaler som analyseras dagligen.
- BitLocker-krypteringen gör det enklare att **skydda företagets information**, även när den finns på borttappade eller stulna enheter.
- Få ett bättre **skydd mot opålitliga källor** – med Microsoft Defender Application Guard kan du öppna filer och webbplatser i en isolerad behållare.

Modern säkerhetshantering

- **Håll säkerhetsfunktionerna uppdaterade** med Windows Update for Business.
- Gör det möjligt att införa **Zero-Trust-säkerhetsramverk**.
- **Se till att policyerna efterlevs för de anställda både på kontoret och på distans** med Microsoft Endpoint Manager.
- Distribuera enheter som redan i förväg har **konfigurerats med företagets säkerhetspolicyer** med hjälp av Windows Autopilot och Zero-Touch-distribution.
- Uppnå säkerhet och synlighet med **säker enkel inloggning** till alla dina appar med Azure Active Directory.
- **En konstruktion som sätter molnet främst gör systemet enkelt att bygga ut** med Microsoft 365, Microsoft Defender for Cloud och Microsoft Defender for Endpoints.
- Gör det **enklare att förhindra skadlig kod** och skydda mot skadlig kod och annan opålitlig programvara med Windows Defender Application Control.

Lenovo – din betrodda partner för att implementera Zero Trust-strategier och hybridarbete

Varför välja Lenovo?

Erfarenhet, expertis, kapacitet i storföretagsklassen och ett team med specialexperter som gör det lättare för dig att införa molnet samt att definiera och implementera säkerhetspolicyerna. Som auktoriserad Microsoft Cloud Solutions Provider-partner (CSP) kan Lenovo erbjuda hela Microsoft Cloud-tjänsteutbudet, inklusive Microsoft 365 och Azure-tjänsterna.

Microsoft Partner

Microsoft

2022 Partner of the Year Winner
Device Award

Microsoft Gold Partner and Device Partner of the Year

Lenovo uppfyller Microsofts strikta krav för att bli erkänd som guldpartner, något som bekräftar att Lenovo har den expertis och den kapacitet som krävs för att tillhandahålla avancerade och säkra lösningar för distansarbete.

Utöver det har Lenovo tilldelats det prestigefyllda priset Microsoft Device Partner of the Year. Det är ett erkännande av ett utmärkt arbete med att bygga, marknadsföra eller sälja enheter och IT-lösningar som främjar Microsoft-baserad teknik.

Priset tillföll Lenovo på grund av deras meritlista när det gäller att leverera integrerade lösningar och tjänster på ett konsekvent, flexibelt och förutsägbart sätt, för att kunna möta kundernas efterfrågan på digitalisering och framtidssäkring av deras verksamheter.

Vår molnstrategi: allt från en och samma leverantör

Lenovos mål är att bli en äkta hybridorganisation som kan distribuera lokala, privata och offentliga moln med fokus på att uppfylla kundernas behov av lagring, program och lösningar. Förutsättningen för detta är vår kapacitet att leverera maskinvara, tjänster, programvara, device-as-a-service och support – allt från en och samma leverantör.

Så här får vi din Zero Trust-strategilösning att fungera för ditt företag

Med Lenovos hanterade och professionella tjänster kommer du på rätta vägen mot en smidig, problemfri uppgradering till ett Zero Trust-försvar.

- Lenovo kan möta alla dina behov, från lösningsdesign till personalintroduktion och slutlig migrering.
- Om du har en Microsoft 365-licens uppdaterar vi helt enkelt Windows 11-enheterna och Microsoft 365 och inkluderar Azure Active Directory, Microsoft Defender och Endpoint Manager.
- Premier Support – specialtelefon för användarna, dygnet runt, 365 dagar om året.
- Specialexperter – lokalt baserade experter som är redo att hjälpa dig med att uppnå ett säkrare hybridarbete.
- Säkerhet i storföretagsklassen – de bästa cyberförsvaren, som stoppar den växande mängden skadlig kod och riktade angrepp.

Smarter technology for all

Lenovo

Kontakta oss i dag så får du veta hur Lenovo kan hjälpa dig att bygga upp företagets Zero Trust-säkerhetsstrategi.

Boka in ett möte

Microsoft 365