Wees zeker van je beveiliging. Wees zeker van je mensen. Dankzij Lenovo.

Zo beveilig je medewerkers in een cyberwereld die steeds verandert 〉

Smarter technology for all

Lenovo

De overgang naar hybride werken is blijvend en vormt een uitdagende omgeving voor cyberbeveiliging.

Tegenwoordig moeten de meeste werknemers hybride kunnen werken. Daarom moet de bescherming tegen bedreigingen worden uitgebreid naar meerdere clouds en verschillende platforms.

Zo ontstaat een complexe digitale omgeving waarin onbekende bedreigingen zich makkelijk kunnen verschuilen. Het afdwingen van beveiligingsbeleid op verschillende apparaten en verschillende digitale lagen is een fikse uitdaging. Het is voor de mensen die belast zijn met het leveren van beveiliging een heuse puzzel, die je uit de slaap kan houden.

Veilige hardware en een veilige cloud. Een uniek samenwerkingsverband: Lenovo heeft een speciaal samenwerkingsverband met Microsoft. Onze hardware is voorzien van ThinkShield, wat wordt gebruikt in combinatie met Microsoft Cloud Security-services.

Lenovo ThinkShield is ingebouwde beveiliging

Bij Lenovo begrijpen we dat uitgebreide bescherming hoogstnoodzakelijk is. ThinkShield-beveiliging volgt de beste normen voor beveiliging en beschermt apparaten beter door dit in het ontwerp al in te bouwen.

Dit loopt van de beveiliging van toeleveringsketens tot aan de ontwikkeling van nieuwe Lenovo-producten. Ze zijn dus veilig omdat ze zijn ontwikkeld door de makers van de best vertrouwde zakelijke pc's ter wereld.

Onze unieke ThinkShield-portfolio omvat hardware, services, software en processen. Dit samenspel biedt bescherming op alle niveaus van een onderneming. Door onze samenwerking met toonaangevende beveiligingsproviders kunnen we met isolatie en inperking een complete Zero Trust-defensiestrategie opbouwen. Dit gebeurt samen met Microsoft-beveiligingsoplossingen.

Zero Trust. De toekomst van cyberbeveiliging. Zo ziet de nieuwe benadering eruit.

Zero Trust slaat een andere weg in dan conventionele netwerkbeveiliging. Daarin wordt vooral gekeken naar een ‘corporate perimeter’, apparaten die zijn verbonden via een VPN. Dat is op dit moment de normale gang van zaken.

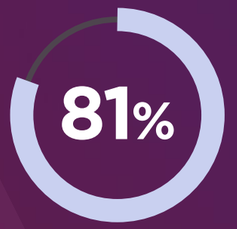
De leidende principes van Zero Trust zijn: ‘Nooit iets vertrouwen. Altijd verifiëren.’

In de hybride werkomgeving van nu mogen we apparaten als regel niet vertrouwen, ook al zijn ze verbonden met een ‘goedgekeurd’ netwerk.

Zero Trust gaat ervan uit dat een aanvaller zich binnen het netwerk kan bevinden. De mate van vertrouwen wordt bepaald binnen de **context**, zoals bijvoorbeeld de **identiteit en locatie van de gebruiker, de beveiligingsstatus van het apparaat** en de gebruikte **app of de service die wordt benaderd**. Bij elke stap wordt het beleid gecontroleerd.

Hierdoor kunnen alleen de juiste **mensen met de juiste middelen en alleen op beveiligde apparaten toegang krijgen tot je gegevens**.

De noodzaak voor Zero Trust is nog nooit zo hoog geweest:



van de ondernemingen is aan de overstap naar hybride werken begonnen[1]

minder risico op een gegevenslek[3]

1070%

toename van ransomware tussen juli 2020 en juni 2021[4]

van de organisaties detecteerde in de afgelopen 18 maanden een phishingaanval[2]

minder oproepen aan IT- en helpdeskanalisten[3]

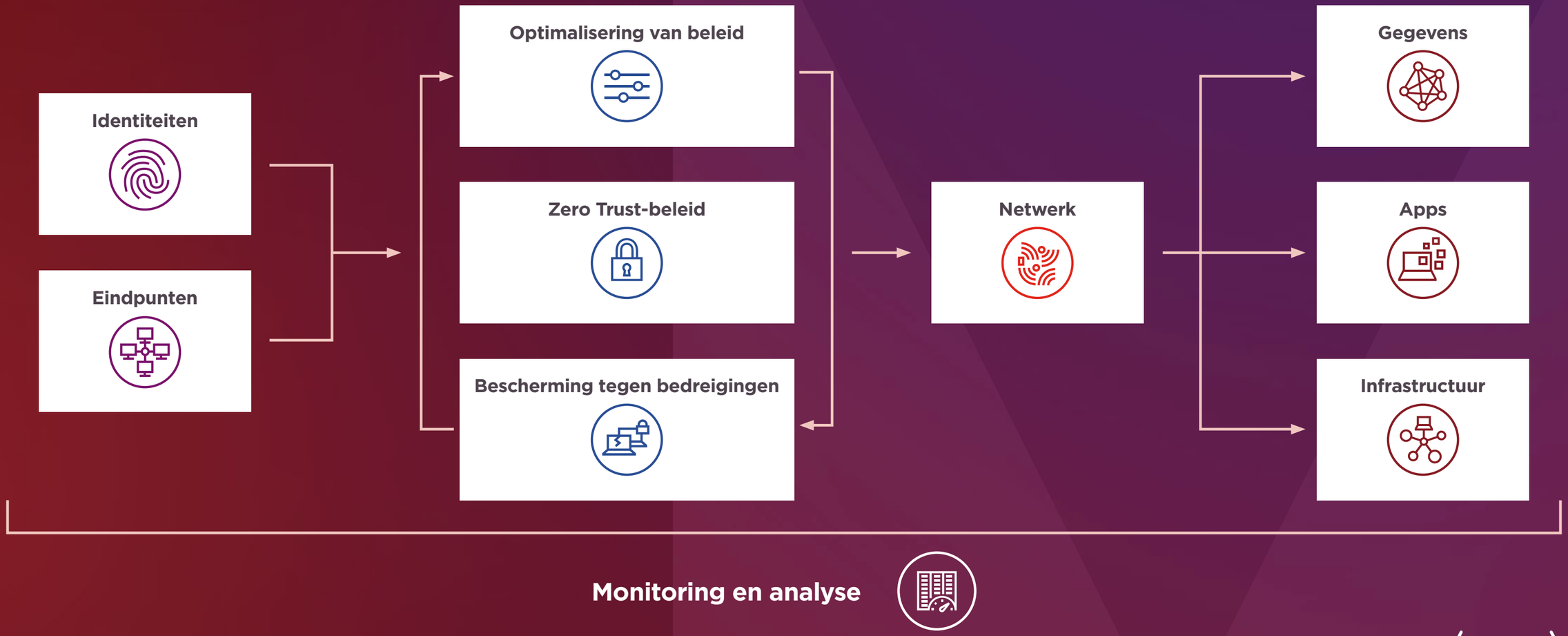
minder tijd besteed aan beheer door betere beveiligingsprocessen[3]

De Lenovo ThinkShield-portfolio en Microsoft-beveiligingsoplossingen zijn speciaal en doelbewust ontworpen voor de implementatie van een **end-to-end Zero Trust-strategie** die je bedrijf op alle niveaus beschermt.

[1] Microsoft Zero Trust Adoption Report, 2021
[2] IBM Cost of a Data Breach Report 2021
[3] The Total Economic Impact™ of Zero Trust solutions from Microsoft, december 2021. Onderzoek uitgevoerd door Forrester Consulting, in opdracht van Microsoft.
[4] 1H Global Threat Landscape Report, door FortiGuard Labs

Zo ziet een Zero Trust-architectuur eruit.

Zero Trust is een concept dat meerdere IT-aspecten omvat. De bescherming begint bij moderne apparaten echter al bij Windows 11, gebruikersidentiteiten en de bewaking van eindpuntapparaten.



Maak hybride werken beter en veiliger voor je werknemers dankzij Lenovo-apparaten met Windows 11 Pro

Windows 11 Pro is de veiligste Windows tot nu toe en **stroomlijnt het beheer** van hybride werkplekken terwijl je **gegevens en toegang altijd en overal zijn beveiligd**.

Het is ontworpen voor moderne **apparaten die zijn geoptimaliseerd voor beveiliging**. Het geeft je de voordelen van de nieuwste bescherming, ingebouwd in de hardware. Die is precies afgestemd op de software. Windows 11 Pro is speciaal ontwikkeld voor **veilig hybride werken**. De **basisbeveiliging is beter dan bij Windows 10**. Er zijn nieuwe vereisten voor de bescherming, die zijn ingebouwd en standaard staan ingeschakeld.

ThinkPad X1 Carbon

Met cloudmanagement kun je de beveiliging van je Lenovo Windows 11 Pro ThinkShield-apparaat verder verbeteren

De beveiliging van identiteiten en eindpuntapparaten is een eerste belangrijke stap op weg naar een Zero Trust-strategie. Identiteiten en apparaten zijn de twee belangrijkste doelwitten voor ID-gegevensdiefstal, phishingmails, ransomware en andere soorten malware en geavanceerde bedreigingen.

Profiteer van Lenovo Windows 11-apparaten en Microsoft Cloud-beveiligingsoplossingen om een Zero Trust-strategie uit te rollen.

Identiteitsbeheer

- Gebruikt meervoudige verificatie (Multifactor Authentication), wat 99,9% van de aanvallen op identiteiten kan stoppen.
- Beschikt over een ‘intelligente’ beleid-engine voor voorwaardelijke toegang. Je kunt hiermee specifieke regels instellen voor de aanmelding van gebruikers. In combinatie met meervoudige verificatie resulteert dit in een krachtige balans tussen beveiliging en gebruikersproductiviteit.

Eindpuntbeheer

- Zorg er met behulp van mobiel toegangsbeheer (Mobile Access Management) voor dat apps voldoen aan de beveiligingsprotocollen van je bedrijf.
- Met het mobiele apparaten-beheer (Mobile Device Management) zorg je ervoor dat apparaten voldoen aan de beveiligingsprotocollen van je bedrijf, zowel op bedrijfsapparaten als op BYOD.

Controleer, bescherm en beheer het gebruik met de voordelen van Security Cloud-oplossingen

Identiteitsbeheer met Azure Active Directory

- Azure Active Directory is een eenvoudige en efficiënte identiteits- en toegangsbeheerservice in de cloud die werkt met meervoudige verificatie en voorwaardelijke toegang.
- Combineert Core Directory-services, applicatietoegangsbeheer en identiteitsbescherming in één oplossing.
- Je werknemers krijgen veilig toegang tot externe bronnen zoals Microsoft 365, de Azure-portal en duizenden andere SaaS-applicaties.
- Interne bronnen worden beveiligd, zoals je intranet en de cloud-apps die door je organisatie zelf zijn gebouwd.

Microsoft Defender voor Eindpunt

Toonaangevende eindpuntbeveiliging die werkt vanuit de cloud:

- Beveiligt tegen ransomware, bestandsloze malware en andere geavanceerde aanvallen op Windows, Mac OS, Linux, Android en iOS.
- Ontdekt verborgen dreigingen door voortdurend in realtime codegedrag en aanvallertechnieken te bewaken en maakt snelle detectie en reactie mogelijk.
- 24/7 geautomatiseerde respons en herstel bij incidenten. Beveiligingsteams kunnen waarschuwingen direct gebruiken voor AI-gestuurd herstel.
- Beheerde service voor het opsporen van bedreigingen met de hulp van onze on-demand Microsoft-experts.

Microsoft Endpoint Manager

Beheer en beveiliging van eindpuntapparaten in één geïntegreerd beheerplatform:

- Beveilig, implementeer en beheer alle gebruikers, apps en eindpuntapparaten zonder de bestaande werkprocessen te verstoren.
- Biedt een moderne werkplek en modern beheer dat in de cloud en op locatie je gegevens veilig houdt.
- Combineert services die je misschien al kent en gebruikt, waaronder Microsoft Intune, Configuration Manager, Desktop Analytics, co-beheer en Windows Autopilot.

Het juiste apparaat op de juiste plek op het goede moment. Dat kan met Lenovo Zero Touch.

Veilige, moderne technologie is de sleutel tot succes voor elk bedrijf. Maar een gewone implementatie met de hand is complex, tijdrovend en foutgevoelig.

Er is nu een eenvoudigere manier om je hybride en externe medewerkers direct aan de slag te laten gaan: **Lenovo Zero-Touch met Autopilot-implementatie**.

Het geeft hybride werken vleugels en verhoogt de productiviteit omdat IT-teams worden ontlast en zich kunnen bezighouden met de innovaties die je bedrijf echt vooruit helpen.

Met **Windows Autopilot** hoeven IT-afdelingen niet langer handmatig nieuwe images te installeren of nieuwe apparaten in te stellen. Het gebeurt allemaal op afstand. Lenovo Windows 11-apparaten worden geleverd met Autopilot vooraf geconfigureerd. IT-beheerders kunnen de gebruikers en configuraties vanaf elke locatie aanpassen.

- **Uitpakken en klaar voor gebruik:** de gebruiker zet het apparaat aan en een paar simpele klikken verder is het klaar voor gebruik.
- **Simpel beheer met profielen:** je kunt tot 350 verschillende profielen maken, beheren en toewijzen. Zo kun je voor iedere gebruiker de instellingen en pc-configuratie bepalen.
- **Moeiteloos verhuizen naar de cloud:** meld apparaten automatisch aan voor Azure Active Directory en het beheer van mobiele apparaten.
- **Probleemloze toewijzingen:** een gepersonaliseerde en gestroomlijnde set-up.
- **Volg de voortgang:** met behulp van Autopilot kunnen gebruikers de voortgang van de apparaatconfiguratie volgen.
- **Productregistratie:** apparaten worden automatisch geregistreerd bij de Autopilot Cloud Deployment-service.

Kies voor ‘Better Together’

Voorgeïnstalleerde beveiliging

- **Beveiliging vanuit de kern** dankzij de beveiliging en gegevens- en identiteitswaarborgen van de TPM 2.0-chip.
- Eenvoudiger en veiliger aanmelden met **wachtwoordloze verificatie** zoals Windows Hello for Business.
- Blokkeer schadelijke software met **de ingebouwde bescherming die standaard aanstaat**.
- Om je **vanaf de start te beschermen, voorkomt** Windows 11 dat malware wordt geladen tijdens het opstarten.
- Gegevens- en netwerkbeveiliging dankzij **hardwarematige ‘root-of-trust’** die de integriteit van het apparaat bewaakt en verifieert.

Beveilig je bedrijf tegen nieuwe bedreigingen

- Bescherm aanmeldgegevens door de **verbeterde phishing-beveiliging** van Microsoft Defender Smartscreen.
- Meld je handsfree aan dankzij **aanwezigheidsdetectie**: deze meldt je aan wanneer je nadert en vergrendelt weer wanneer je weggaat.
- Bescherm je meest gevoelige gegevens met de **Secured-core pc’s van Lenovo**.
- Gebruik de hardwarebescherming voor referenties van **Microsoft Pluton**.
- Profiteer op basis van 43 biljoen beveiligingssignalen die dagelijks worden geanalyseerd van **intelligente dreigingsdetectie en een snelle respons**.
- BitLocker-versleuteling **beschermt je bedrijfsinformatie** zelfs op verloren of gestolen apparaten.
- Betere **bescherming tegen niet-vertrouwde bronnen**: open bestanden en websites in een geïsoleerde container met Microsoft Defender Application Guard.

Modern beveiligingsbeheer

- **Houd beveiligingsfuncties up-to-date** met Windows Update for Business.
- EGebruik de **beveiliging van Zero-Trust-frameworks**.
- **Dwing** met Microsoft Endpoint Manager **beleid af bij medewerkers op locatie en op afstand.**
- Implementeer met Windows Autopilot en Zero-Touch apparaten die al vooraf zijn **geconfigureerd met het beveiligingsbeleid** van het bedrijf.
- Schakel met Azure Active Directory **éénmalige aanmelding** in voor meer beveiliging en zichtbaarheid van al je apps.
- **Cloud-first design maakt uitbreiden eenvoudig** voor Microsoft 365, Microsoft Defender voor Cloud en Microsoft Defender voor Eindpunt.
- Ga met Windows Defender Application Control kwaadaardige scripts tegen en **beveilig tegen malware en andere niet-vertrouwde software**.

Lenovo. Je vertrouwde partner voor de implementatie van Zero Trust-strategieën en hybride werken

Waarom kiezen voor Lenovo?

We hebben de ervaring, expertise, ondernemingskracht en een toegewijd team van experts om je verhuizing naar de cloud, beveiligingsbeleid en je implementaties te ondersteunen. Als geautoriseerde Microsoft CSP-partner levert Lenovo de volledige portfolio Microsoft Cloud-services, met inbegrip van het meest bekende aanbod, zoals Microsoft 365 of Azure.

Microsoft Partner

Microsoft

2022 Partner of the Year Winner
Device Award

Microsoft Gold Partner en Device Partner van het jaar

Lenovo meets Microsoft's strict requirements to be Lenovo voldoet aan de strenge eisen van Microsoft en is erkend als Gold Partner. Dat bevestigt dat Lenovo over de expertise en capaciteiten beschikt die hoogwaardige en veilige oplossingen voor werken op afstand vergen.

Daarnaast heeft Lenovo de prestigieuze Microsoft Device Partner of the Year Award ontvangen. Dit is de erkenning van onze uitmuntendheid in het bouwen, op de markt brengen en verkopen van apparaten en IT-oplossingen voor Microsoft-technologie.

De prijs is het resultaat van Lenovo's staat van dienst en het consistent, flexibel en voorspelbaar leveren van geïntegreerde oplossingen en diensten. Deze voldoen aan de huidige vraag van klanten naar digitale transformatie en kunnen hun bedrijf toekomstbestendig maken.

Onze cloudstrategie: alles van één leverancier

Lenovo wil een echte hybride organisatie zijn die implementatieoplossingen levert voor op locatie en de privé- en publieke cloud. Wij richten ons op de verkoop van opslag-, software- en andere oplossingen die onze klanten nodig hebben. We kunnen deze hardware, services, software, device-as-a-service en ondersteuning aanbieden via één leverancier.

Hier kun je lezen hoe we een Zero Trust Strategy-oplossing leveren voor je bedrijf

Met Lenovo's Managed- en Professional-services wijzen we je de weg naar een soepele, probleemloze upgrade voor Zero Trust-beveiliging.

- Van het ontwerp van de oplossing tot de onboarding en de uiteindelijke migratie, Lenovo biedt alles wat je nodig hebt.
- Als je een Microsoft 365-licentie hebt, werken we Windows 11-apparaten en Microsoft 365 eenvoudig bij en nemen we Azure Active Directory, Microsoft Defender en Endpoint Manager daarin mee.
- Eersteklas ondersteuning: speciale hotline voor gebruikers, 24/7, 365 dagen per jaar.
- Toegewijde experts: lokaal gevestigde experts die precies weten hoe ze je overstap naar veilig hybride werken kunnen ondersteunen.
- Beveiliging op ondernemingsniveau: hoogwaardige verdedigingslinies voor cyberbeveiliging die de groeiende stroom aan malware en gerichte aanvallen kunnen weerstaan.

Smarter technology for all

Lenovo

Neem vandaag nog contact met ons op om te zien hoe Lenovo je bedrijf kan ondersteunen bij het ontwikkelen van een Zero Trust-beveiligingsstrategie.

Een afspraak plannen

Microsoft 365