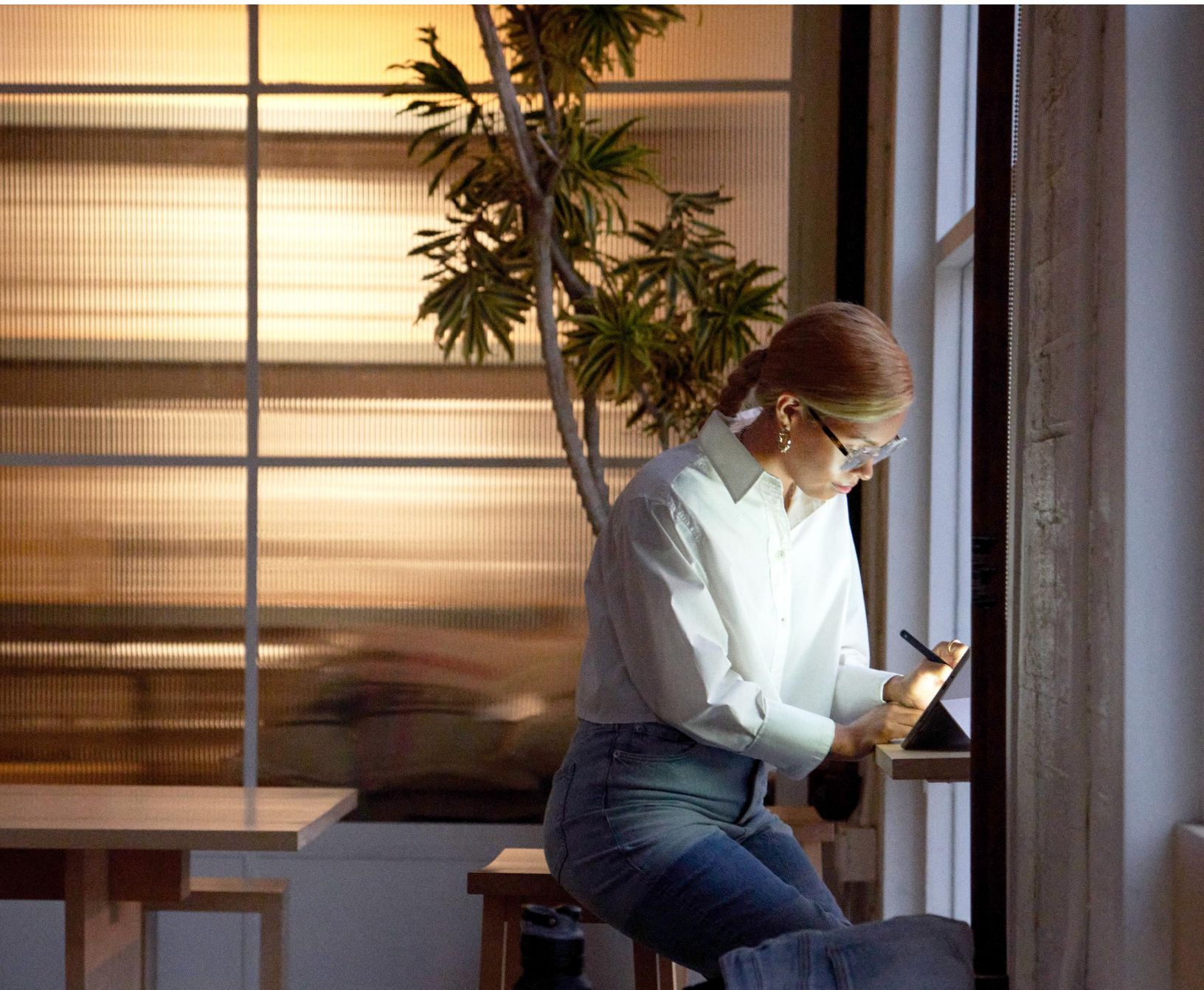
Microsoft Surface

De juiste keuze: hoe je apparaatkeuze het plan voor cyberveerkracht kan maken of breken



Wat houdt cyberveerkracht in?

Tegenwoordig zijn bijna alle organisaties, van koffietentjes tot wereldwijde ondernemingen, afhankelijk van data, analytics, automatisering en digitale technologieën. Deze afhankelijkheid heeft, samen met de opkomst van thuiswerken, het risico en de kosten van cyberaanvallen op lokale én wereldwijde schaal verhoogd.

Omdat deze scenario's steeds frequenter en geavanceerder worden, moeten beveiligingsleiders verder gaan kijken dan preventie. Cyberveerkracht is het vermogen van een organisatie om snel te reageren op een negatieve gebeurtenis en daarvan te herstellen, waardoor beveiligingskwetsbaarheden minder kostbaar zijn. Veerkracht kan het verschil betekenen tussen terrein verliezen of met het herstel een sprong vooruit maken.

---

5 x toename van cyberaanvallen op extern beheerde apparaten tussen mei 2021 en mei 2022.[1]

$ 4,24 mln. gemiddelde wereldwijde kosten van een datalek in 2022.[1]

[1]Microsoft, Microsoft Digital Defense-rapport 2022. Microsoft, 2022.

(vervolg) Wat houdt cyberveerkracht in?

Hoe is dit mogelijk? Er zijn belangrijke principes die alle bedrijven, van grote tot hele kleine, kunnen inzetten om tijdens een crisis veerkracht te tonen. Dat vereist een pragmatische kijk op cyberbeveiliging, waarbij wordt aangenomen dat lekken onvermijdelijk zijn. Met andere woorden: 'uitgaan van een lek'.

Uitgaan van een lek betekent een flinke breuk met de traditionele beveiligings-mentaliteit. Vroeger dachten IT'ers dat ze een veilig netwerk met een versterkte beschermingsmuur konden opbouwen waarin alle bedrijfsactiviteiten plaatsvonden, terwijl apparaten van eindgebruikers sterk werden beperkt.

Maar bij de traditionele benadering wordt voorbijgegaan aan de eisen van moderne werkomgevingen, veranderende bedrijfs-modellen, nieuwe technologieën en veranderende bedreigingen. Het stimuleren van veerkracht vereist Zero Trust, een samenwerking tussen zakelijke stakeholders, IT-leiders en beveiligers, en het gebruik van geavanceerde technologie die is ontworpen om de bescherming te verbeteren.

Tegen 2026 bevat

50%

van de arbeidscontracten van directeuren prestatie-eisen op het gebied van risico's.[1]

Tegen 2025 zal

60%

van de organisatie cyberbeveiliging-srisico's gebruiken als belangrijkste bepalende factor voor transacties en zakelijke relaties met derden.[1]

---

[1]Gartner-persbericht, "Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23", 21 juni 2022. https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio

In twee stappen op weg naar cyberveerkracht

1 Implementeer basismaatregelen

Het merendeel van de cyberaanvallen kan op een paar eenvoudige manieren worden gestopt, zoals het afdanken van verouderde applicaties, apparaten en infrastructuur. Ook het automatiseren van handmatige processen, het gebruik van meervoudige verificatie (MFA), het invoeren van Zero Trust-principes en moderne antimalware worden aanbevolen.

Door regelmatig firm- en software-updates te installeren, worden kwetsbaarheden voortdurend opgelost. Firmware-aanvallen vormen voor organisaties een van de belangrijkste risico's: via firmware van apparaten zoals laptops, printers en routers kunnen kwaadwillenden onbeperkt en ongezien toegang tot je netwerk krijgen.

Een belangrijke eerste stap is het controleren van gebruikersendpoints om te bepalen welke er makkelijk toegankelijke firmware hebben.

98% van de aanvallen kan met elementaire hygiënemaatregelen worden gestopt.[1]

45% van de beveiligingsdeskundigen ziet e-mail- en samenwerkingstools als het meest kwetsbare aspect van hun organisatie.[2]

[1]Microsoft, Microsoft Digital Defense-rapport 2022. Microsoft, 2022.
[2]Microsoft, Cyberveerkracht, 2022.

Belangrijke onderdelen van cyberveerkracht

Beschermen en verdedigen

Alle goede veerkrachtstrategieën beginnen met het beschermen van systemen, applicaties en data. Verleen alleen toegang voor geautoriseerde gebruikers die klant-, werknemers- en bedrijfsdata nodig hebben. Analyseer ook applicaties en endpointapparaten op kwetsbaarheden die overal kunnen bestaan, van de chip tot de cloud.

Detecteren en inspecteren

Omdat cyberaanvallen steeds frequenter en geavanceerder worden, wordt het steeds belangrijker om apparaten en software te diagnosticeren en voortdurend op afwijkingen te controleren. Hier kan automatisering nuttig zijn, door systeemreacties op bepaalde dreigingen te activeren en prioriteit te geven aan dreigingen waar een teamlid naar moet kijken.

Herstellen

Aanvallen zijn onvermijdelijk. De acceptatie van dit feit opent de deur naar planning om de verstoring te beperken en efficiënt te herstellen met apparaten die voor veerkracht zijn ontworpen.

2 Investeer in technologie die bestand is tegen verstoringen

Beveiligingsbeslissers investeren veel in softwarebeveiliging. Firewalls en dataversleuteling, inbraakdetectie en aanvalspreventie staan bovenaan de lijst. Maar als je niet begrijpt hoe kwetsbaar hardware is, kan dat alle inspanningen ondermijnen.

Een typische beveiligingsinfrastructuur bestaat uit meerdere lagen die samenwerken om de middelen, data en bedrijfsvoering van een organisatie te beschermen.

Een lek op hardwareniveau, zoals in een laptop, tablet, telefoon of IoT-apparaat, breidt zich uit naar hogere lagen, tot de data en netwerken die deze apparaten zouden moeten beschermen.

Samenwerken met technologiebeslissers om het juiste apparaat te kiezen is de basis van je plan voor cyberveerkracht. Factoren zoals de prestaties, afgestemd op het gebruik, de schaalbaarheid, compatibiliteit, betrouwbaarheid en beveiliging van het apparaat zelf, spelen allemaal een rol.

Belangrijkste onderdelen van een veerkrachtige infrastructuur

- Stel een firmwarebeschermingsplan op en blijf bij met firmware- UEFI-, en besturingssysteemupdates die extra bescherming tegen nieuwe bedreigingen kunnen bieden.
- Versnel het automatiseren van handmatige taken, zoals updates en apparaatactivering op afstand, zodat je IT'ers meer tijd voor arbeidsint-ensieve taken hebben.
- Stel een schema voor het bijwerken van UEFI-, firmware- en beveiligingsupdates in.
- Schakel MFA voor alle eindgebruikers in en implementeer voorwaardelijke toegang.
- Implementeer biometrie, zoals Windows Hello voor Bedrijven, om minder afhankelijk van codes, kaarten en wachtwoorden te worden.
- Schaf apparaten met een Beveiligde kern aan of configureer je apparaten om aan vergelijkbare eisen te voldoen.
- Verminder het aantal kwetsbaarheden in endpointapparaten door ongebruikte functies, zoals bluetooth of videocamera's, uit te schakelen.

Kies voor cyber-veerkrachtige apparaten

- Zoek uit wat de best practices en standaarden voor apparaatbeveiliging in je sector zijn.
- Evalueer je huidige apparaten en bepaal welke gaten of risico's ze op het gebied van functies, leeftijd, versie of beveiliging hebben.
- Vergelijk verschillende apparaatopties op basis van functies, voor- en nadelen, recensies en beoordelingen.
- Neem contact op met experts of leveranciers die je advies of aanbevelingen over apparaten kunnen geven.
- Test en evalueer de prestaties en beveiliging van je gekozen apparaten voordat je ze in je organisatie implementeert.
- Monitor en onderhoud je apparaten regelmatig om te zorgen dat ze correct en veilig functioneren.

Houd apparaten actueel

Je IT-team kan apparaten natuurlijk testen en isoleren, maar je kunt het risico verlagen door de firmware actueel te houden, zodat het IT-team zich kan richten op veerkracht en groei in plaats van verdediging en reparaties.

Naast firmware nemen ook aanvallen op extern beheerde apparaten toe. Dit kunnen laptops, camera's en technologie voor slimme vergaderruimten zijn, die bijvoorbeeld via open poorten kwetsbaar zijn en door hackers kunnen worden misbruikt. Uit een recent onderzoek bleek dat 46% van de aanvallen op IoT/OT bestond uit extern beheerde apparaten.[1]

[1]Microsoft Security Insider, Niet gepatcht en onbeschermd, het unieke beveiligingsrisico van IoT-/OT-apparaten, 2022.

Kies een partner om te helpen bij het ontwikkelen van een strategie voor cyberveerkracht

In een wereld van complexe IT-uitdagingen kan de juiste IT-partner bedrijven beschermen en op herstel voorbereiden. Een goede IT-partner raadt de meest geschikte hardware, software en beveiligingsoplossingen voor het bedrijf aan, en zorgt dat je met minder leveranciers en oplossingen te maken hebt. Een waardevolle IT-partner heeft de kennis en ervaring om een uitgebreid, en met het bedrijf meegroeiend cyberveerkrachtplan te ontwerpen en implementeren. Uiteindelijk moet een IT-partner het belang van de klant voor ogen hebben en de klant helpen zijn zakelijke doelen te behalen.

Microsoft heeft samen met zijn partners Surface-apparaten ontwikkeld om bedreigingen tegen firmware, het besturingssysteem en cloudapplicaties te beperken. De apparaten zijn helemaal voor Zero Trust ontworpen, zodat beveiligings- en IT-beslissers met vertrouwen kunnen investeren in strategieën en technologieën die toekomstige aanvallen zullen voorkomen, in plaats van alleen bescherming te bieden tegen de vele aanvallen waar ze vandaag onder lijden.

Zoek een Microsoft-partner: geautoriseerde Microsoft-resellers, Surface voor Bedrijven

Hoe Microsoft Surface cyberveerkracht opbouwt

Microsoft Surface-apparaten zijn zo ontworpen dat elementaire beveiligings-hygiëne wordt gestimuleerd. Elke laag wordt door Microsoft onderhouden, van de firmware en het besturingssysteem tot de cloud. Surface-apparaten, Windows 11 en Microsoft 365[1] helpen je organisatie veerkrachtiger te worden met een Zero Trust-benadering van beveiliging en risicobeheersing die innovatie en productiviteit niet in de weg zit.

Bij het ontwerpen van Surface hebben we nagedacht over alle manieren waarop cyberaanvallen apparaten en gebruikers kunnen treffen. Beveiliging is het effectiefst als het in het ontwerp is ingebouwd, zodat het de meest kwetsbare aspecten kan beschermen, dus zo hebben we dat ook aangepakt. Daardoor biedt Surface van chip tot cloud bescherming. We hebben Surface ontworpen om je gerust te stellen met de wetenschap dat een door Microsoft onderhouden geïntegreerde oplossing je bedrijf beschermt. Laten we eens nader bekijken hoe Microsoft Surface cyberveerkracht opbouwt.

Bedrijven met Surface-apparaten kunnen tot 34% minder beveiligingsincidenten ondervinden, waardoor ze minder hier minder tijd aan kwijt zijn.[2]

*Uniek voor Microsoft Surface.
**CRU's (door klanten vervangbare eenheden) zijn onderdelen die je bij je Surface Commercial Authorized Device Reseller kunt kopen. Een deskundige monteur kan de onderdelen aan de hand van de Onderhoudshandleiding van Microsoft ter plekke verwisselen. Het openen en/of repareren van je apparaat kan onder andere elektrische schokken, brand en persoonlijk letsel veroorzaken. Wees voorzichtig als je zelf reparaties uitvoert. Apparaatschade die tijdens de reparatie wordt veroorzaakt, valt niet onder Microsofts hardwaregarantie of beschermingsabonnementen. Onderdelen zullen kort na de lancering beschikbaar worden. Het precieze moment is afhankelijk van het onderdeel en de markt.
[1]Voor sommige functies zijn softwarelicenties benodigd. Apart verkrijgbaar.
[2]Een whitepaper over bedrijfswaarde, in opdracht van Microsoft, september 2022 | Doc. #US49453722 IDC-onderzoek, uitgevoerd op basis van enquêtes en interviews tussen december 2021 en februari 2022. Alle respondenten waren IT-beslissers bij grote organisaties (250 tot > 5000 werknemers) die organisaties vertegenwoordigen uit de Verenigde Staten, Australië, India, Spanje, Frankrijk, het Verenigd Koninkrijk, Nieuw-Zeeland en Duitsland. De kosten- en besparingsresultaten zijn gebaseerd op schattingen van gemiddelde kosten en tijd die rechtstreeks door respondenten zijn verstrekt. De werkelijke kosten en besparingen kunnen variëren, afhankelijk van de apparaten en implementatie. Klik hier voor het gedetailleerde rapport.

Word cyberveerk-rachtig, van hardware tot samenwerking en de cloud

“Microsoft biedt alle diensten en beschermingen die we voor onszelf en onze klanten nodig hebben, op hetzelfde platform.”

– NIP Group

Microsoft Surface kan de beveiligingskloof helpen dichten door beveiligingsteams, bedrijfsleiders en werknemers meer mogelijkheden te bieden. De combinatie van voor veiligheid ontworpen Surface-apparaten, Windows 11 en Microsoft 365* zorgt voor een geïntegreerde oplossing met ingebouwde beschermingslagen en apparaatbeheer op afstand die zich uitstrekt van de hard- en firmware tot de cloud.

Windows 11 bevat standaard diep geïntegreerde hardware- en software-beveiligingsfuncties, die proactieve bescherming en veerkracht tegen veranderende bedreigingen bieden.

---

*Voor sommige functies zijn softwarelicenties benodigd.
**Apart verkrijgbaar.

“De beveiligde pc is een poging om de ‘beste omgeving ter wereld’ te creëren. Ik denk dat we deze omgeving met succes hebben gecreëerd door de nieuwste technologieën, waaronder Microsoft 365, met onze eigen technologieën te combineren.”

– NTT Communications Corporation

Gemaakt voor beveiliging

Onze beveiligingsaanpak begint met hardware. Surface beschermt data door versleuteling tijdens het opstarten. Een **Trusted Platform Module 2.0** (TPM 2.0) fungeert als veilige kluis voor wachtwoorden, pincodes en certificaten, beschermt hardware tegen manipulatie en beperkt toegang tot alleen gemachtigde personen. In elke fase van de opstartcyclus wordt de firmwarecode gecontroleerd op echtheid, zodat het systeem geen kwaadaardige code kan uitvoeren.

Het aanmelden gebeurt veilig en zonder wachtwoord met **Windows Hello voor Bedrijven**, dat dankzij een infraroodcamera voor betere gezichtsherkenning de best mogelijke biometrische beveiliging biedt. Biometrisch aanmelden is het moeilijkst te foppen, zodat alleen gemachtigde gebruikers toegang tot het apparaat hebben.

We ontwerpen veel Surface-apparaten met verwijderbare SSD's[1], zodat gevoelige data op het apparaat extra kunnen worden beschermd.

Microsoft werd in het Gartner® Magic Quadrant™ for Unified Endpoint Management Tools 2022 uitgeroepen tot koploper.[2]

IT-medewerkers van bedrijven die Surface gebruiken, waren 40% minder tijd kwijt aan lopend onderhoud.[3]

Ontworpen voor vertrouwen

Microsoft Intune* bevat **Surface Management Portal**, een speciale, gecentraliseerde oplossing voor endpointmanagement in de cloud. Surface Management Portal is ontworpen om gebruikers, apps en apparaten op grote schaal te beheren en configureren, terwijl Microsoft Intune* het beheren van mobiele applicaties (MAM) en mobiele apparaten (MDM) afhandelt.

*Voor sommige functies zijn softwarelicenties benodigd. Apart verkrijgbaar.

[1]CRU's (door klanten vervangbare eenheden) zijn onderdelen die je bij je Surface Commercial Authorized Device Reseller kunt kopen. Een deskundige monteur kan de onderdelen aan de hand van de Onderhoudshandleiding van Microsoft ter plekke verwisselen. Het openen en/of repareren van je apparaat kan onder andere elektrische schokken, brand en persoonlijk letsel veroorzaken. Wees voorzichtig als je zelf reparaties uitvoert. Apparaatschade die tijdens de reparatie wordt veroorzaakt, valt niet onder Microsofts hardwaregarantie of beschermingsabonnementen. Onderdelen zullen kort na de lancering beschikbaar worden. Het precieze moment is afhankelijk van het onderdeel en de markt.

[2]Gartner, Magic Quadrant for Unified Endpoint Management Tools, Tom Cipolla, Dan Wilson, et al., 1 augustus 2022. GARTNER is een gedeponeerd handels- en servicemerk van Gartner, Inc.en/of haar gelieerde bedrijven in de VS en daarbuiten, en MAGIC QUADRANT is een gedeponeerd handelsmerk van Gartner, Inc. en/of haar gelieerde bedrijven in de VS en daarbuiten, en deze handelsmerken worden hierin met toestemming gebruikt. Alle rechten voorbehouden. Gartner doet geen aanbevelingen met betrekking tot leveranciers, producten of services die in haar publicaties worden vermeld en adviseert technologiegebruikers niet alleen die leveranciers te selecteren die de hoogste beoordelingen krijgen. De onderzoekspublicaties van Gartner bestaan uit de meningen van de onderzoeksorganisatie van Gartner en mogen niet worden beschouwd als feiten. Gartner wijst alle garanties, expliciet dan wel impliciet, met betrekking tot dit onderzoek af, met inbegrip van garanties betreffende verkoopbaarheid of geschiktheid voor een bepaald doel.

[3]Een whitepaper over bedrijfswaarde, in opdracht van Microsoft, september 2022 | Doc. #US49453722 IDC-onderzoek, uitgevoerd op basis van enquêtes en interviews tussen december 2021 en februari 2022. Alle respondenten waren IT-beslissers bij grote organisaties (250 tot > 5000 werknemers) die organisaties vertegenwoordigen uit de Verenigde Staten, Australië, India, Spanje, Frankrijk, het Verenigd Koninkrijk, Nieuw-Zeeland en Duitsland. De kosten- en besparingsresultaten zijn gebaseerd op schattingen van gemiddelde kosten en tijd die rechtstreeks door respondenten zijn verstrekt. De werkelijke kosten en besparingen kunnen variëren, afhankelijk van je specifieke apparaatmix en implementatie. Klik hier voor het gedetailleerde rapport.

Windows Update regelt het implementeren en bijwerken van firmware, software en stuurprogramma's. Eind-tot-eindbeveiliging zorgt dat alleen goedgekeurde programmatuur wordt geïnstalleerd.

Het op afstand beheren van apparaat-beveiliging kan je IT-team enorm veel tijd besparen, zodat firmware- en gijzelsoftware-aanvallen worden beperkt en problemen worden opgelost voor ze uit de hand lopen.

Windows Autopilot, dat samenwerkt met Microsoft Intune*, stroomlijnt het veilig op afstand implementeren van nieuwe apparaten door vooraf de benodigde beveiligingsinstellingen en -beleid in te stellen, wat leidt tot nog meer tijdbesparing.

"De geavanceerdheid van de biometrische verificatie via de gezichtsherkenning van Windows Hello die we zien bij Surface is absoluut toonaangevend."

– Mashreq

Vergrendelde firmware

Surface-apparaten blokkeren bedreigingen proactief door belangrijke externe toegangspunten tot firmware via de Unified Extensible Firmware Interface (UEFI) te verwijderen. Windows Update heeft toegang tot de door Microsoft gemaakte UEFI, zodat het risico op externe toegang tot de firmware kleiner is.

Samen met de **Device Firmware Configuration Interface (DFCI)** maakt de UEFI van Microsoft een fijnmaziger beheer van firmware via Microsoft Intune* mogelijk.

DFCI verkleint het aanvalsoppervlak door onnodige hardwareonderdelen uit te schakelen en de afhankelijkheid van het lokale UEFI-wachtwoord (BIOS-wachtwoord) te verwijderen. Met DFCI kunnen opstartopties worden vergrendeld, zodat gebruikers geen ander besturingssysteem kunnen starten, en omdat beveiligings-updates op de achtergrond worden toegepast, blijft het apparaat voortdurend beschermd tegen de nieuwste bedreigingen.

34% minder beveiligingsincidenten met Surface-apparaten.[2]

30% minder tijd van IT-medewerkers kwijt aan beveiligingsincidenten bij het gebruik van Surface-apparaten.[2]

---

*Voor sommige functies zijn softwarelicenties benodigd. Apart verkrijgbaar.
[1]Surface Go en Surface Go 2 maken gebruik van een UEFI van derden en ondersteunen geen DFCI. Ga voor informatie over de Microsoft-bescherming voor Surface Go en Go 2 naar https://www.microsoft.com/en-us/surface/business/surface-go-2.
[2]Een whitepaper over bedrijfswaarde, in opdracht van Microsoft, september 2022 | Doc. #US49453722 IDC-onderzoek, uitgevoerd op basis van enquêtes en interviews tussen december 2021 en februari 2022. Alle respondenten waren IT-beslissers bij grote organisaties (250 tot > 5000 werknemers) die organisaties vertegenwoordigen uit de Verenigde Staten, Australië, India, Spanje, Frankrijk, het Verenigd Koninkrijk, Nieuw-Zeeland en Duitsland. De kosten- en besparings-resultaten zijn gebaseerd op schattingen van gemiddelde kosten en tijd die rechtstreeks door respondenten zijn verstrekt. De werkelijke kosten en besparingen kunnen variëren, afhankelijk van je specifieke apparaatmix en implementatie. Klik hier voor het gedetailleerde rapport.

Standaard actieve, krachtige Windows 11-beveiliging

Surface-apparaten met Windows 11 beschikken standaard over nieuwe hardwarebeveiligingsfuncties. **Beveiliging op basis van virtualisatie (VBS)** en **door hypervisor afgedwongen code-integriteit (HVCI)**, ook bekend als **geheugenintegriteit**, zijn ontworpen als nog sterkere basis die meer weerstand tegen aanvallen biedt. VBS en HVCI werken samen om betere bescherming tegen veelvoorkomende en geavanceerde malware te bieden door gevoelige beveiligingshandelingen in een geïsoleerde omgeving uit te voeren. Door het uitvoeren van code vooraf te controleren, voorkomen VBS en HVCI dat malware zijn weg naar het systeemgeheugen vindt. Als een bedreiging toch toegang tot systeem-bronnen krijgt, kan HVCI de effecten beperken en indammen.

We leveren Surface-apparaten met Windows 11 en de **beveiligingsfuncties ingeschakeld**. Zo kunnen beveiligings- en bedrijfsleiders beveiligingsgedrag in de organisatie normaliseren, wat de verantwoording binnen teams verbetert.

Zelfs voor het aanmelden met een van de biometrische opties die wachtwoorden en pincodes overbodig maken, zorgt **Secure Boot** dat de firmware net zo authentiek is als toen het apparaat de fabriek verliet. Secure Boot en Trusted Boot voorkomen samen dat malware en beschadigde onderdelen tijdens het opstarten worden geladen.

Na het opstarten zorgt de versleuteling van **BitLocker** dat data zelfs op kwijtgeraakte, gestolen of verkeerd afgedankte apparaten ontoegankelijk is.

Voor robuuste cyberbeveiliging moet je je ontwikkelen van het simpelweg handhaven van de bescherming tot veerkracht tegen huidige en nieuwe bedreigingen. Cyberveerkracht is een organisatiebrede inspanning waarvoor iedereen verantwoordelijk is. Organisaties hebben een geïntegreerde benadering nodig, met beveiliging in elke laag van de chip tot de cloud, zodat mensen en data overal worden beschermd.

Wil je meer weten over de geïntegreerde, cyberveerkrachtige oplossingen die door Microsoft zijn ontworpen en in Surface, Windows 11 en Microsoft 365 zijn ingebouwd? Neem dan nu contact met je vertegenwoordiger op.

Microsoft Surface

Afvinklijst voor yberveerkracht

Waar je bij het evalueren van de invloed van je apparaten op cyberveerkracht rekening mee moet houden

Met deze vragen en onderwerpen kun je beter inschatten hoe je apparaat-portfolio ervoor staat als onderdeel van je beveiligingsplanning:

- ☐ Hoeveel prioriteit geeft de leiding aan beveiliging wat kwetsbaarheden in apparaten voor eindgebruikers betreft?
- ☐ Hoeveel budget wil de leiding vrijmaken voor nieuwe apparaten om de beveiliging op niveau te houden?
- ☐ Wat zou een beveiligingslek kunnen kosten?
- ☐ Hebben we een volledig beeld van de endpoints en waar die kwetsbaarheden kunnen veroorzaken? Zowel kwantiteit als kwaliteit.
- ☐ Staat ons bedrijf werknemers toe om eigen apparaten te gebruiken en met het netwerk te verbinden?
- ☐ Van hoeveel oplossingen zijn we in ons huidige beveiligingsecosysteem afhankelijk?
- ☐ Gebruiken we verschillende soorten apparaten en besturingssystemen? Kunnen we dat consolideren?

Met leiders over beveiliging praten

Gebruik deze gespreksaanzetten om de discussie over beveiliging op gang te brengen en uiteindelijk beslissingen over cyberveerkracht te nemen:

- Hoeveel prioriteit geven we aan de beveiliging van ons intellectueel eigendom, data en mensen?
- Wat is belangrijker: beveiliging of werknemerservaring, en in welke mate?
- Blijven we loyaal aan onze leveranciers of kunnen we consolideren?
- Het omarmen van een Zero Trust-model zal onze cyberveerkracht versterken. Hoeveel steun is er voor deze andere beveiligingsmentaliteit?

Cyberveerkracht is een teaminspanning

Als organisaties veerkrachtig willen zijn, moeten technologiebeslissers zakelijke beslissers in alle gebieden van de organisatie betrekken bij het plannen voor veerkracht.

Functie	Belang voor apparaatkeuze	Ter overweging
Chief Financial Officer	Rendement op apparaatinvestering	De zakelijke onderbouwing en totale eigendomskosten evalueren
Chief Sustainability Officer	Afstemming met MVO-doelen	Uitstootschatter voor Microsoft Surface
Chief Security Officer	Integratie in beveiligingsecosysteem, bescherming van data en intellectueel eigendom	Endpointbeveiliging voor Microsoft Surface
Chief Human Resources Officer	Support voor productiviteit, veelzijdigheid, apparaten en werknemerservaring	Understanding the role of Modernized PCs in Hybrid Work Environment Optimization

Aanvullende informatie

Microsoft Security Insider

Microsoft Secure

Meer informatie over Zero Trust

In vijf stappen naar cyberveerkracht

Zakelijke veerkracht: Cloud Adoption Framework | Microsoft Learn

De workshop voor Chief Information Security Officers (CISO's): beveiligings-documentatie | Microsoft Leren

Ben je mkb'er? Ontdek hoe je met Surface en beveiliging je potentieel kunt waarmaken.