

Bescherm uw netwerk



Met veilig printen in grootformaat van HP



Firewalls alleen zijn niet bestand tegen cyberaanvallen van hackers. U hebt de uitstekende bescherming van HP nodig om uw apparaten, data, documenten en netwerk te beschermen.

Printerbeveiligingsrisico's	03
Bescherm uw apparaten, data, documenten en netwerk	04
Bescherm uw apparaat	05-06
Bescherm uw data	07
Bescherm uw documenten	08
Bescherm uw netwerk	09
HP Wolf Security	10-11
Hoe werkt zelfherstel?	12
Printers die beveiligen, detecteren en herstellen	13
HP printerportfolio	14
Concurrentievergelijking	15



Herken de verborgen risico's

Hoewel de meeste IT-afdelingen strenge beveiligingsmaatregelen hebben getroffen voor individuele computers, worden printers en scanners vaak over het hoofd gezien en niet beschermd. Als er niet-beveiligde apparaten aanwezig zijn, kan het hele netwerk kwetsbaar zijn voor cyberaanvallen.



Inzicht in de potentiële kosten

Wanneer persoonlijke informatie openbaar wordt als gevolg van onbeveiligde printers en scanners, kan dat uitmonden in identiteitsdiefstal, diefstal van bedrijfsgegevens, reputatieschade aan het merk, rechtszaken en verlies van zakelijke productiviteit en efficiëntie. Wanneer u bovendien niet voldoet aan de wet- en regelgeving, kan dit tot hoge boetes leiden.



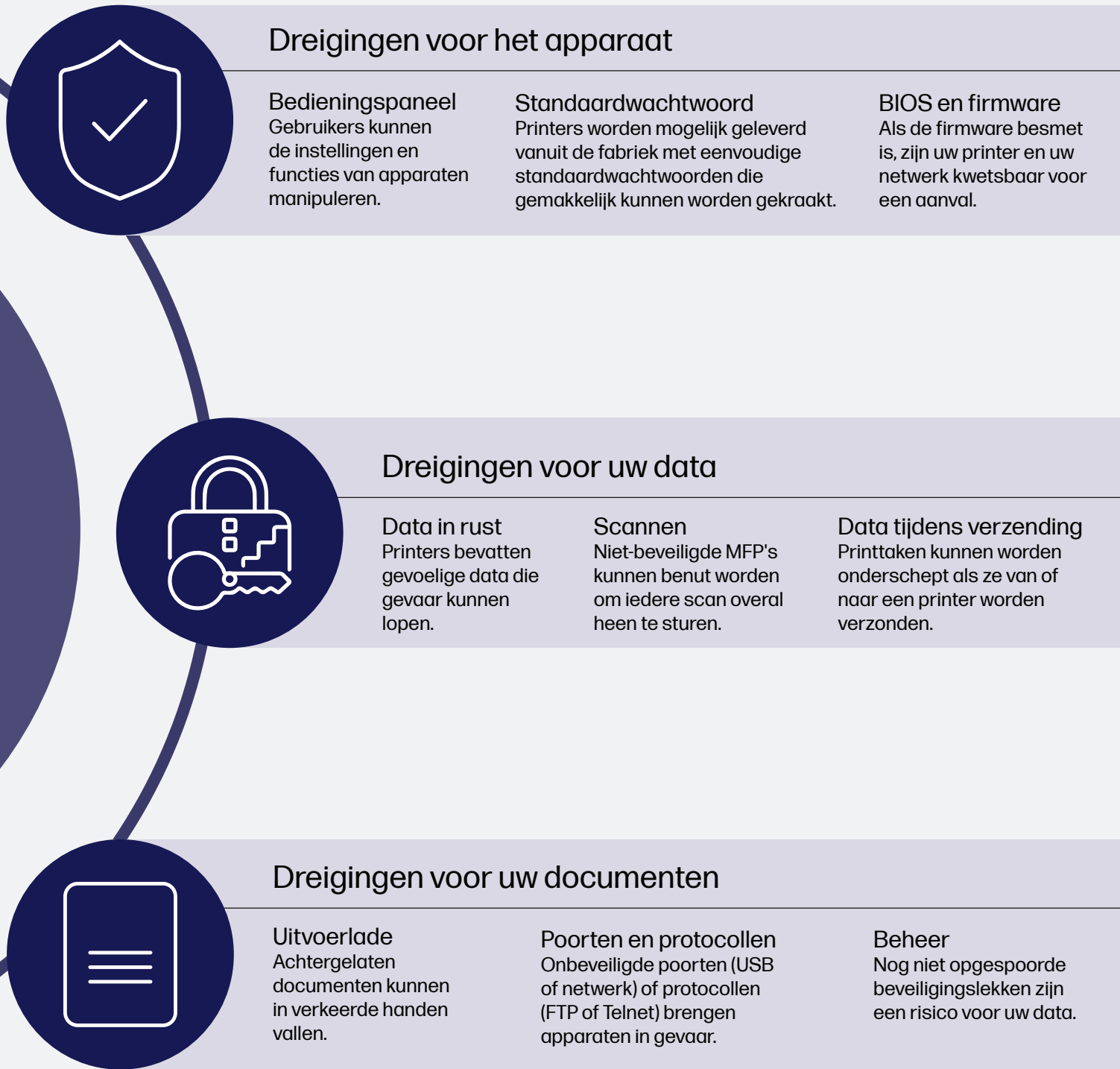
HP helpt

Bescherm uw netwerk met beveiligingsfuncties die in onze grootformaat printers zijn ingebouwd. HP kan u helpen om de beveiliging van uw apparaten, data, documenten en netwerk te automatiseren met een breed assortiment aan oplossingen.

Bescherm uw apparaten, data, documenten en netwerk

Kritische tekortkomingen kunnen op verschillende plaatsen in uw scan- en printomgeving aanwezig zijn. Als u deze kwetsbaarheden eenmaal begrijpt, kunt u de risico's eenvoudiger beperken.

Kwetsbare punten in het print- en scanproces



Bescherm het apparaat



HP Secure Boot

Het BIOS bevat een reeks instructies waarmee tijdens het opstarten essentiële hardwarecomponenten worden geladen en firmware wordt geïnitieerd. Dankzij HP Secure Boot wordt de integriteit van de code telkens gevalideerd wanneer het apparaat opstart, om het apparaat tegen aanvallen te beschermen.

Whitelisting

Whitelisting controleert de firmware tijdens het opstarten automatisch om te bepalen of het authentieke, door HP digitaal ondertekende code betreft. Wanneer er een afwijking wordt gedetecteerd, wordt het apparaat uitgeschakeld en ontvangt het IT-team een melding.

HP Connection Inspector

HP Connection Inspector inspecteert uitgaande netwerkverbindingen die doorgaans worden misbruikt door malware, bepaalt wat normaal is en stopt verdachte activiteiten. Als de printer gevaar loopt, wordt het systeem automatisch opnieuw opgestart.

HP Trusted Platform Module (TPM)

Op de HP Trusted Platform Module (TPM) worden versleutelde logingegevens en data die op uw printer of MFP worden bewaard nog beter beschermd.

Bescherm het apparaat

Uniek beheerderswachtwoord

Alle printers hebben standaard een uniek beheerderswachtwoord, dus is uw printer altijd beveiligd met een wachtwoord, zelfs zonder installatie.

LDAP/Kerberos gebruikersverificatie

Met deze protocollen kunt u de printergebruiker via de bedrijfsdirectory verifiëren om ervoor te zorgen dat de gebruiker alleen toegang heeft tot geautoriseerde opties en informatie.

HP Smartcard-oplossing

Bescherm vertrouwelijke gegevens en controleer de toegang tot het printen door gebruikers te verplichten tweefactorauthenticatie te gebruiken bij de printer.

Rolgebaseerde toegangscontrole

Met rolgebaseerde toegangscontrole kan de beheerder de toegang van gebruikers tot gevoelige gebieden en printerinstellingen beperken door verschillende rollen te configureren en deze aan dergelijke gebruikers toe te wijzen.

Logboek voor beveiligingsincidenten

Biedt volledige zichtbaarheid om kwaadaardige dreigingen snel te detecteren. In het beveiligingslogboek worden de gebeurtenissen weergegeven zoals gedefinieerd door het controlebeleid dat voor elk object is ingesteld.

Runtime-inbraakdetectie

Runtime inbraakdetectie bewaakt voortdurend het kernelgeheugen en detecteert beschadigingen of pogingen tot fraude. Na detectie herstelt het apparaat zichzelf door opnieuw op te starten in een goede staat.

HP Sure Start

HP Sure Start is een geavanceerde, hardwarematige oplossing die uitgebreide beveiliging biedt voor firmware en firmware-instellingen.

Bescherm uw data



In rust



Self-Encrypted harde schijf

Bescherm gevoelige bedrijfsgegevens op de opslagschijf met ingebouwde zelfversleuteling.



Bestanden veilig wissen

Zorgt ervoor dat er geen gegevens achterblijven bij de printer nadat bestanden van de harde schijf zijn verwijderd.



Schijf veilig wissen

Wist alle informatie op de harde schijf van de printer, waardoor het onmogelijk is om gevoelige gegevens te herstellen.

Tijdens het verzenden



Gecodeerde communicatie

Standaardversleutelingsprotocollen 802.1x of IPsec maken gebruik van versleutelde netwerkstandaarden om gegevens te beschermen die via het netwerk worden verzonden als u print vanaf drivers of via aanvragers.

Bescherm uw documenten



Pull-printen



Pull-printen is een functie die end-to-end tracking en rapportage biedt om gevoelige informatie en media te beschermen en het aantal niet-opgehaalde printtaken te verminderen. Dit verhoogt de productiviteit en voorkomt dat achtergelaten documenten in verkeerde handen vallen. HP grootformaat printers zijn ook compatibel met andere pull-printoplossingen van derden.

HP Common Access Card (CAC)¹



Verbeter de beveiliging en de productiviteit met een uniforme printerverificatie in uw hele organisatie.

Versleuteld printen met pincode



Wanneer gebruikers vertrouwelijke printtaken verzenden, kunnen ze een pincode toewijzen aan het document op de printerdriver. Het document wordt dan vastgehouden in de printer tot de gebruiker de pincode op het apparaat invoert. Op deze manier weet de gebruiker zeker dat zijn of haar vertrouwelijke document niet onbeheerd wordt achtergelaten.

Bescherm uw netwerk

Bewakings- en beheeroplossingen helpen u kwetsbaarheden op te sporen en een uniforme, beleidsmatige aanpak te creëren om data te beschermen, de compliance te versterken en risico's terug te dringen. Voorkom tekortkomingen in de bescherming en vermijd hoge boetes.



Bescherm uw apparaten en netwerk



HP Security Manager² helpt u de kosten en middelen te verlagen om een beveiligingsbeleid voor alle apparaten op te stellen, apparaatinstellingen te automatiseren en unieke certificaten te installeren en te vernieuwen. Het onderdeel Instant-on security van HP Security Manager² zorgt ervoor dat nieuwe apparaten automatisch worden geconfigureerd op het moment dat ze aan het netwerk worden toegevoegd of opnieuw worden opgestart.

HP Command Center (HPCC) is een cloudoplossing waarmee IT-beheerders een beveiligingsbeleid kunnen opstellen voor geactiveerde apparaten. Met HPCC kunnen ze de beveiligingsinstellingen van het apparaat evalueren en zo nodig aanpassen aan het vooraf vastgestelde beveiligingsbeleid van het bedrijf.

Compliance-auditrapportage van printerparkbeveiliging



Met HP Security Manager² op locatie en HPCC in de cloud maakt u rapporten waarmee u kunt aantonen dat het beveiligingsbeleid op uw printers is toegepast en dat klantgegevens veilig zijn.

Apparaten die niet compliant zijn, kunnen uw bedrijf schaden



Niet-beveiligde of onvoldoende beveiligde endpoints geven cybercriminelen nog meer gelegenheid om toe te slaan. Om het groeiende aantal dreigingen het hoofd te bieden, implementeren overheidsorganen overal ter wereld strenge beveiligingswetgeving die vereist dat organisaties klantgegevens beter beschermen. Het is noodzakelijk om apparaten en oplossingen zoals HP DesignJet-printers en HP Security Manager² te implementeren, die u helpen aan de nalegingsvereisten te voldoen en uw bedrijfsgegevens te beschermen tegen dreigingen.

Uitstekende bescherming. Veilig en eenvoudig.



HP Wolf Security^{3,4} is nu uitgebreid met HP DesignJet grootformaat printers en -plotters.



Om printbedrijven zoals dat van u te helpen bij het aanpakken van toekomstige kwetsbaarheden en risico's, biedt HP Wolf Security geïntegreerde endpointbeveiliging en veerkracht die begint op hardwareniveau en zich uitstrekt naar software.

Het is een type endpointbeveiliging³, geworteld in zero trust-principes, dat voortdurend in ontwikkeling is zodat u moderne dreigingen voor kunt blijven.

Verbeter uw beveiliging met gemak

HP Wolf Security biedt een uitzonderlijke bescherming, maar stelt systemen ook in staat zichzelf te beschermen en herstellen. Implementeer en beheer systemen zonder afbreuk te doen aan de breedte en diepte van uw beveiligingsdekking.

Bescherm uw bedrijf dat steeds groter wordt

Detecteren

Automatische detectie van problemen of dreigingen voordat u ze zelf kunt ontdekken.

Beschermen

Bescherm uw bedrijf en houd de vaart erin met een optimale beveiliging die ervoor zorgt dat u cyberdreigingen voor blijft.

Herstellen

Automatisch herstel van aanvallen zonder drukke IT-teams te belasten.

3 verschillende beschermingsniveaus

HP DesignJet printers met HP Wolf Security hebben verschillende beschermingsniveaus al ingebouwd. Als u een beveiligde printer met HP Wolf Security koopt, weet u zeker dat u het juiste beveiligingsniveau hebt voor wat u nodig hebt.



HP Wolf Essential Security

Leg een veilige basis met hardwarematige bescherming.

HP Wolf Pro Security

Beveilig uw bedrijf met proactieve bescherming tegen cyberdreigingen.

HP Wolf Enterprise Security

Blijf nieuwe dreigingen voor en ondersteun tegelijkertijd hybride werk.

Hoe werkt zelfherstel?

HP Security Manager voert een beveiligingscontrole in vier stappen uit om uw apparaat veilig te houden.



Besturingscode controleren (BIOS) HP Secure Boot

Voorkomt dat tijdens het opstarten kwaadaardige code wordt uitgevoerd en zorgt dat alleen door HP ondertekende, authentieke code wordt geladen.



Firmware controleren Whitelisting

Zorgt ervoor dat er alleen authentieke firmware wordt geladen die digitaal door HP is ondertekend.



Printerinstelling controleren HP Security Manager²

Inspecteert en herstelt onjuiste beveiligingsinstellingen van het apparaat na het opstarten.



Voortdurende bewaking HP Connection Inspector

Bewaakt voortdurend uitgaande netwerkverbindingen om het binnendringen van malware te voorkomen en kwaadaardige activiteiten automatisch te stoppen.

Printers die beveiligen, detecteren en herstellen

HP grootformaat printers

HP grootformaat printers zijn ontworpen om het risico te verkleinen, de compliance te verbeteren en uw netwerk end-to-end te beschermen. Ze bieden ingebouwde functies en add-on-oplossingen waarmee u beschermd bent tegen aanvallen.



HP DesignJet T850/T950

Printer

De eenvoudigste A4-A0 printervaring ter wereld voor een maximale slagvaardigheid van uw team.⁵

Kijk voor meer informatie op:

HP DesignJet T850/T950 printerserie



HP DesignJet XL 3800

Multifunctionele printer

Bescherm uw netwerk en gegevens met HP's veiligste grootformaat printer, inclusief HP Wolf Enterprise.

Kijk voor meer informatie op:

HP DesignJet XL 3800 MFP



	HP DesignJet T850/T950 printerserie	HP DesignJet XL 3800 multifunctionele printer
Apparaat	HP Secure Boot	✓
	UEFI Secure Boot	✓
	HP Connection Inspector	✓
	Whitelisting	✓
	Uniek beheerderswachtwoord	✓
	TPM	✓
	Runtime-inbraakdetectie	✓
	Sure Start	✓
	LDAP/Kerberos gebruikersverificatie	✓
	Rolgebaseerde toegangscontrole	✓
Data	Bedieningspaneel vergrendelen	✓
	Logboek voor beveiligingsincidenten	✓
	Compatibel met SNMP v3	✓
	Self-Encrypted HDD	✓
	Verwijderbare HDD	✓
	Geen HDD	✓
	Compatibel met IPSec	✓
	TLS/SSL (g)	✓
	Bestanden veilig wissen	✓
	Schijf veilig wissen	✓
Document	802.1x-compatibiliteit	✓
	NTLM v2	✓
	Versleuteld printen met pincode	✓
	Ondersteuning voor IPv4a en IPv6	✓
	CA/JD-certificaten	✓
	Interfaces uitschakelen	✓
	HP CAC¹	✓
	Printen met pincode	✓
	Geïntegreerde Celiveo Enterprise-oplossing	✓
	HP Web JetAdmin	✓
Beheer van de printerbeveiliging	HP Security Manager/HP Command Center	✓
	SIEM-integratie	✓

	RICOH CW 22001 SP/ RICOH IM CW 2200	KIP 600 serie	KIP 7171	Canon CW 3600	Epson T5400	Canon PW 3500 serie	Canon IPF TZ-serie TZ-30000	Canon IPF TM-serie 300/305	Epson SC-T Serie T5700D
Apparaat	Secure Boot ^(a)	✓		✓		✓	✓		✓
	Connection Inspector ^(a)	✓							
	Whitelisting ^(a)	✓		✓		✓		✓ (h)	
	Uniek beheerderswachtwoord ^(a)	✓	✓	✓		✓	✓	✓	✓
	TPM ^(a)	✓		✓		✓		✓	✓
	Runtime-inbraakdetectie			✓		✓			
	Sure Start			✓		✓			
	LDAP/Kerberos gebruikersverificatie	✓		✓		✓			✓
	Rolgebaseerde toegangscontrole ^(a)	✓	✓	✓		✓	✓	(f)	✓ (g)
	Bedieningspaneel vergrendelen ^(a)	✓	✓	✓	✓	✓	✓	✓	✓
Data	Logboek voor beveiligingsincidenten ^(a)	✓		✓		✓			✓
	Netwerkpoothen en protocollen uitschakelen ^(a)	✓		✓	✓	✓	✓	✓	✓
	Compatibel met SNMP v3 ^(a)			✓	✓	✓		✓	✓
	Self-Encrypted HDD ^(a)	✓	✓	✓			✓		✓
	Verwijderbare HDD		✓	✓	✓	✓		✓	✓
	Compatibel met IPSec ^(a)	✓	✓	✓	✓	✓	✓	✓	✓
	TLS/SSL ^(a)	✓	✓	✓	✓	✓	✓	✓	✓
	Bestanden veilig wissen ^(a)	✓	✓	✓ (b)		✓	✓	✓	✓
	Schijf veilig wissen ^(a)	✓		(b)	✓ (b)	✓	✓	✓	✓
	802.1x-compatibiliteit ^(a)	✓		✓		✓	✓	✓	✓
Document	NTLM v2 ^(a)	✓		(c)	✓			✓	
	Versleuteld printen met pincode ^(a)	✓		✓		✓ (e)	✓ (e)		✓
	Geïntegreerde pull-printoplossing ^{(a)(d)}	✓	✓	✓ (e)		✓	✓		✓
	Printen met pincode ^(a)	✓ (e)	✓	✓		✓	✓		✓
	Printerbeheer op basis van beveiligingsbeleid ^(a)								
	SIEM-integratie ^(a)	✓			✓	✓			✓
Printers									

(a) Beveiligingsfuncties van concurrerende printers worden in deze tabel niet weergegeven omdat ze niet worden vermeld in een van hun datasheets/brochures
(b) e-shredding/e-shredding [DoD 5220.22-M]
(c) NTLMv1
(d) Celiveo + API Netgard® MFD
(e) Alleen Netgard
(f) Het is niet mogelijk om verschillende rollen te configureren en deze aan verschillende gebruikers toe te wijzen; alleen beheerderswachtwoord
(g) Toegangsniveau van het menu kan met meerdere pincodes geconfigureerd worden
(h) Serienummer van de printer wordt gebruikt als wachtwoord

Juridische voetnoten en disclaimers

1. Ondersteunt NIPRNet- en SIPRNet-oplossing van de Amerikaanse overheid.
2. HP Security Manager moet apart worden aangeschaft. Kijk voor meer informatie op hp.com/go/securitymanager
3. HP Security is nu HP Wolf Security. Beveiligingsfuncties verschillen per platform; raadpleeg het informatieblad van het product voor meer informatie.
4. Alle HP DesignJet-printers hebben verschillende beveiligingsniveaus, maar alleen bepaalde printers kunnen aanspraak maken op HP Wolf Security. Dit zijn onder andere de HP DesignJet XL 3800 MFP, HP DesignJet T850 printer/T850 MFP en HP DesignJet T950 printer/T950 MFP. HP Wolf Security wordt een standaardfunctie op toekomstige HP DesignJet producten.
5. Op basis van testresultaten met HP Click voor de HP DesignJet T850. Met deze oplossing kunt u in minder stappen printen ten opzichte van grote printoplossingen van concurrenten. Voor het printen van een gecombineerde reeks opdrachten van 5 pagina's met A0 en A4 zijn 3 stappen nodig met HP Click tegenover 12 stappen met concurrent A en 8 stappen met concurrent B. Tests zijn in april 2023 uitgevoerd door Sogeti. Een gedetailleerd testrapport is verkrijgbaar op aanvraag.

© Copyright 2021, 2023 HP Development Company, L.P. De informatie in dit document kan zonder voorafgaande kennisgeving worden gewijzigd. De van toepassing zijnde garanties voor HP producten en diensten zijn vastgelegd in de uitdrukkelijke garantiebepalingen die bij dergelijke producten en diensten op fysieke en/of elektronische wijze worden meegeleverd of gepubliceerd op de website(s) van HP. Niets in dit document mag als een aanvullende garantie worden opgevat. HP is niet aansprakelijk voor technische en/of redactionele fouten c.q. weglatingen in dit document.

4AA8-3169NLE, september 2023

