



Bescherm uw netwerk met de best beveiligde printers ter wereld.

94%

van de financiële bedrijven noemt copier/printerbeveiliging belangrijk of zeer belangrijk²



61%

van de bedrijven meldde minstens één printergerelateerde dataschending in het afgelopen jaar³



43%

van de bedrijven ziet printers over het hoofd bij endpointbeveiliging⁴





Slechts 18% van de bedrijven controleert printers op bedreigingen.⁴ Hoe is dat bij u?

Herken de verborgen risico's

IT moet doorlopend vertrouwelijke informatie, zoals gegevens van werknemers en klanten, op verschillende apparaten en in uiteenlopende omgevingen beschermen. Hoewel de meeste IT-afdelingen strenge beveiligingsmaatregelen hebben getroffen voor individuele computers en het netwerk, worden printers en scanners vaak over het hoofd gezien en niet beschermd. Als er niet-beveiligde apparaten zijn aangesloten, kan het hele netwerk kwetsbaar zijn voor cyberaanvallen.

Inzicht in de potentiële kosten

Eén inbreuk op de beveiliging kan een bedrijf al op hoge kosten jagen. Wanneer persoonlijke informatie openbaar wordt door onbeveiligde printers en scanners, kan dat uitmonden in diefstal van identiteit, diefstal van concurrentiegevoelige informatie, reputatieschade aan het merk en rechtszaken. Bovendien kan niet voldoen aan de wet- en regelgeving tot hoge boetes leiden.

HP helpt

Bescherm uw netwerk met de veiligste printers ter wereld.¹ HP printers zijn altijd waakzaam om elke aanval te detecteren en te stoppen en passen zich intussen aan nieuwe bedreigingen aan. HP kan u helpen de beveiliging van uw printers, data en documenten te automatiseren met een breed portfolio oplossingen. Onze printbeveiligingsexperts kunnen een end-to-end beveiligingsstrategie voor uw printers en scanners ontwikkelen.

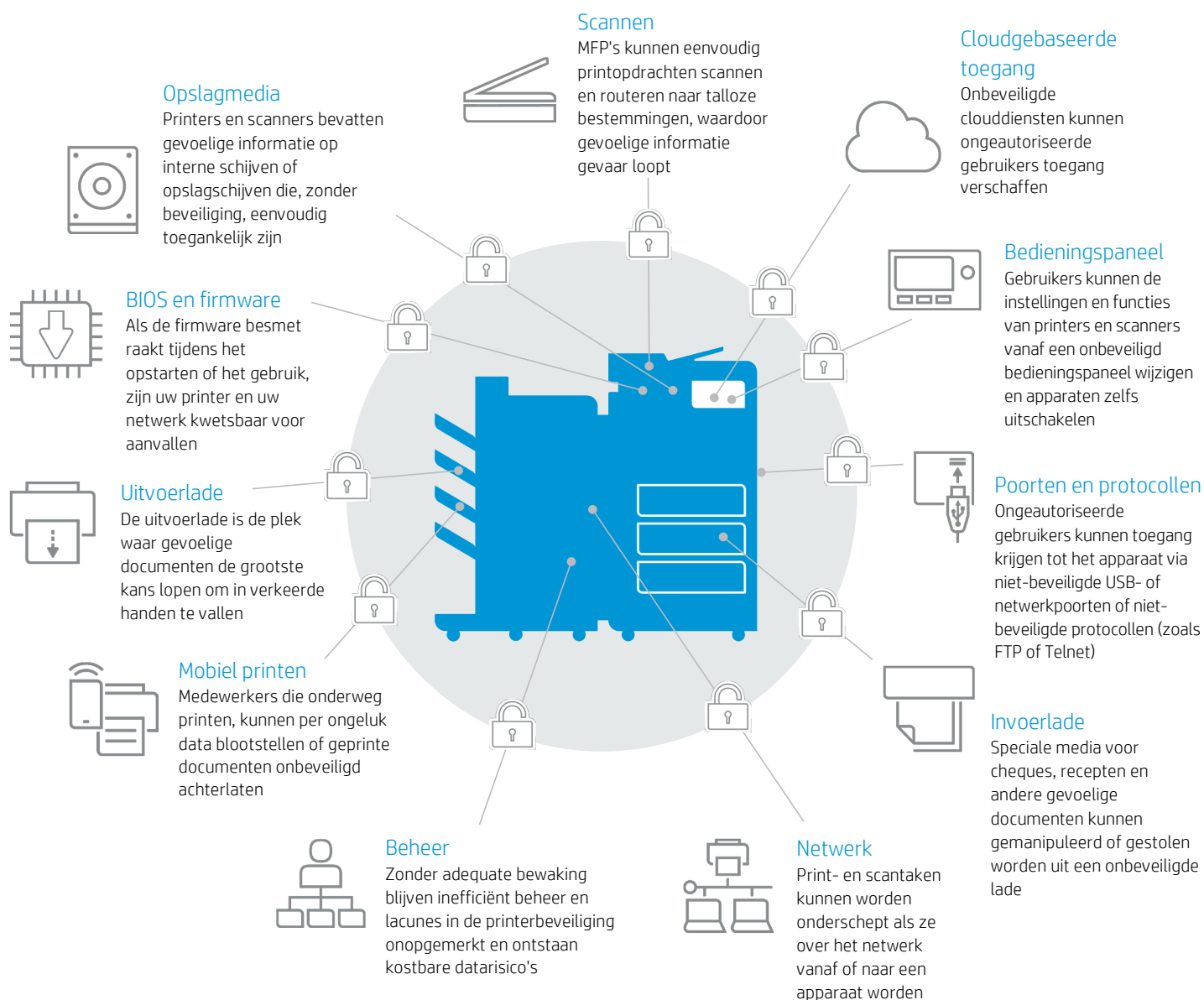
"Dankzij jarenlange investeringen in printerbeveiliging heeft HP het breedste aanbod beveiligingsoplossingen en diensten op de markt."

– Quocirca, januari 2017⁵

Bescherm uw apparatuur, uw data en uw documenten

Uw print- en scanomgeving kan op verschillende plaatsen kritische lacunes bevatten. Als u deze kwetsbare punten eenmaal kent, kunt u de risico's gemakkelijker beperken.

Op welke plaatsen is uw print- en scanproces kwetsbaar?





Bescherm het apparaat



Meer informatie

HP Custom Recycling Services
hp.com/go/businessrecycling

HP Secure Managed Print Services
hp.com/go/securemps

HP printers zijn ontworpen om met behulp van bewakings- en beheeroplossingen de risico's terug te dringen, de naleving te verbeteren en uw netwerk compleet te beschermen. (Niet alle kenmerken en oplossingen zijn op ieder HP apparaat beschikbaar⁶).

Fundamentele beveiligingsmaatregelen

Versleutelde opslag met beveiligd wissen

Gevoelige gegevens op de interne drive of vaste schijf lopen het risico gestolen te worden. Veel HP apparaten beschikken over ingebouwde encryptie om gegevens te beveiligen. Als opgeslagen gegevens niet langer nodig zijn, kunt u de ingebouwde functies van het apparaat gebruiken om deze te overschrijven en kritische informatie veilig te verwijderen.

Veilige afstoting

HP Custom Recycling Services kan ervoor zorgen dat alle data van de opslagschijven zijn gewist alvorens de oude producten verantwoord te recyclen.

Veilige toegang voor reparatiedoeleinden

Kennis van de beveiligingspraktijk van de leveranciers van printeronderhoud helpt om gevoelige data te beschermen. Kies *HP Secure Managed Print Services (MPS)* of vraag uw HP partner om assistentie.

Uitschakelen van niet-gebruikte poorten en protocollen

Geef aanvallers geen kans door uw apparaten zorgvuldig te configureren. Schakel fysieke poorten en niet-veilige protocollen (zoals FTP of Telnet) uit om ongeautoriseerde toegang en onbedoeld gebruik te voorkomen.

De beheerder regelt de toegang tot apparaten

Stel beheerderswachtwoorden in zodat alleen het IT-team of ander geautoriseerd personeel apparaten kan installeren en configureren.

Whitelisting van firmwarecode

Lees op de volgende pagina hoe whitelisting uw printerpark kan beschermen tegen malware.

Geavanceerde beveiligingsmaatregelen

Common Criteria-certificering

Zakelijke HP printers zijn gecertificeerd als compatibel met internationaal erkende beveiligingsstandaarden, zoals Common Criteria Certification (CCC) en FIPS 140. Controleer of de code van apparaatupdates gesigndeerd is om zeker te zijn van de authenticiteit en integriteit van de code en om compliance te waarborgen.



Meer informatie

Ingebouwde printerbeveiligingsfuncties:

- HP Sure Start (BIOS-integriteit)
- Whitelisting van firmwarecode
- Runtime inbraakdetectie
- HP Connection Inspector

hp.com/go/PrintersThatProtect

HP JetAdvantage Security Manager:

hp.com/go/securitymanager

Printerbeveiligingsfuncties detecteren en stoppen automatisch een aanval

Zakelijke printers van HP bevatten beveiligingsfunctionaliteit die de apparaten beschermt en uw netwerk minder kwetsbaar maakt voor aanvallen. Alleen HP printbeveiliging biedt real-time detectie, automatische bewaking en ingebouwde softwarevalidatie om bedreigingen onschadelijk te maken zodra ze optreden.⁷

De HP zakelijke printers, van Pro-⁸ tot Enterprise-modellen,⁷ zijn altijd waakzaam om in elke fase van het gebruik aanvallen te detecteren en af te slaan:

- **Tijdens het opstarten.** De opstartcode (voor Pro-apparaten) of het BIOS (voor Enterprise-apparaten) is een reeks instructies die wordt gebruikt om essentiële hardwarecomponenten te laden en firmware te starten. De integriteit van de code wordt telkens als het apparaat opstart gevalideerd, om het apparaat te beschermen tegen aanvallen.
- **Tijdens het laden van de firmware.** *Whitelisting* controleert de firmware tijdens het opstarten om te bepalen of het authentieke, door HP digitaal ondertekende code betreft. Wanneer een afwijking wordt gevonden, start het apparaat op in een veilige offlinemodus en ontvangt het IT-team een melding.
- **Tijdens het gebruik.** Ingebouwde HP functionaliteit beschermt het apparaatgeheugen als het apparaat wordt ingeschakeld en verbonden is met het netwerk, omdat dan de kans op aanvallen het grootst is. Bij een aanval schakelt het apparaat zichzelf automatisch uit.

HP Enterprise-apparaten kunnen zich herstellen

HP Enterprise printers zijn niet alleen in staat aanvallen te detecteren en te stoppen, ze herstellen zich ook automatisch na een aanval zonder dat het IT-team hoeft in te grijpen.⁷ Deze functies starten de printer automatisch opnieuw op als een aanval of afwijking wordt opgemerkt. Beheerders kunnen worden gewaarschuwd via Security Information and Event Management (SIEM)-tools, zoals ArcSight, Splunk en SIEMonster.

- *HP Sure Start* is het enige zelfherstellende BIOS in de industrie.⁷ Als het BIOS beschadigd is, start HP Sure Start het apparaat opnieuw op met een veilige 'gouden kopie' van het BIOS.
- *Run-time inbraakdetectie* valideert complexe firmware- en geheugenbewerkingen, stopt de inbreuk automatisch en start het apparaat opnieuw op bij een eventuele aanval.
- HP Connection Inspector controleert uitgaande netwerkverbindingen om te bepalen wat normaal is, stopt verdachte verzoeken en start het apparaat automatisch opnieuw op voor zelfherstel.

Dankzij de investeringsbescherming van de upgradeable HP FutureSmart-firmware kunt u whitelisting, runtime-inbraakdetectie en HP Connection Inspector toevoegen op veel bestaande HP Enterprise printers.⁷

HP JetAdvantage Security Manager voltooit de controlecyclus

Na het opstarten, of wanneer een nieuw apparaat aan het netwerk wordt toegevoegd, voert *HP JetAdvantage Security Manager* automatisch een evaluatie uit en herstelt zo nodig de beveiligingsinstellingen van het apparaat conform het configuratiebeleid.⁹ Het IT-team hoeft niet in actie te komen.

Hoe werkt het?

De ingebouwde beveiligingskenmerken voeren de eerste vier stappen in de cyclus van een HP apparaat uit.

Na een aanval kunnen HP Enterprise-apparaten opnieuw opstarten en zichzelf herstellen.

HP JetAdvantage Security Manager voltooit de controlecyclus.

Vier. Continue bewaking

Bescherm uw bedrijf en stopt aanvallen tijdens het gebruik. Controleert uitgaande netwerkverbindingen om verdachte verzoeken te stoppen (alleen Enterprise).

Drie. Instellingen controleren

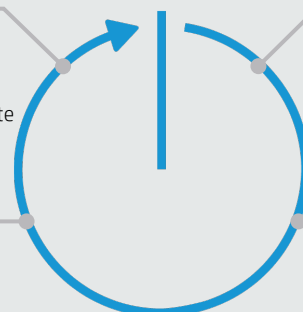
Na het opstarten controleert HP JetAdvantage Security Manager de beveiligingsinstellingen van het apparaat, waarbij foute instellingen worden hersteld.

Eén. BIOS/opstartcode controleren

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

Twee. Firmware controleren

Waarborgt dat alleen authentieke, goede firmware, die digitaal ondertekend is door HP, wordt geladen.





Bescherm uw data



Meer informatie

HP Web Jetadmin
hp.com/go/wja

HP Universal Print Driver met Secure Encrypted Print
hp.com/go/upd

HP JetAdvantage workflowoplossingen
hp.com/go/documentmanagement

HP Access Control
hp.com/go/hpac

Of gegevens nu opgeslagen of onderweg zijn, ze moeten continu beschermd worden. Hier zijn enkele essentiële stappen om een veilig transport en gebruik te waarborgen.⁶

Fundamentele beveiligingsmaatregelen

802.1x- of IPsec-netwerkbeveiliging

Gebruik versleutelde netwerkstandaarden ter bescherming van data die verstuurd worden via het netwerk, tussen het apparaat en beheertools zoals *HP Web Jetadmin* of de *HP Embedded Web Server*.

Versleutel data tijdens verzending

Bescherm printtaken op weg naar de printer via versleuteling, bijvoorbeeld met Internet Print Protocol over TLS (IPPS). Of gebruik *HP Universal Print Driver Secure Encrypted Print*, dat echte symmetrische AES256-encryptie en -decryptie van printtaken biedt, van de client tot de pagina, met een door de gebruiker ingesteld wachtwoord en de FIPS 140-gevalideerde cryptografiebibliotheken van Microsoft®.

Tijdens het scannen helpen *HP JetAdvantage workflowoplossingen* gevoelige informatie te beschermen en de efficiëntie te verhogen. Zo integreert HP Capture and Route bijvoorbeeld naadloos met HP Access Control voor extra beveiliging met gemakkelijke eenmalige authenticatie en de mogelijkheid inhoud te bewaken voor informatiebeheer.¹⁰

Versleutel opgeslagen gegevens

Bescherm gevoelige bedrijfsgegevens op de opslagschijf met ingebouwde versleuteling. Als aanvullende beveiliging kan de optionele HP Trusted Platform Module (TPM) worden geïnstalleerd om versleutelde inloggegevens en data beter te beschermen door de encryptiecodes van het apparaat automatisch te verzegelen in de TPM. Het beveiligt de apparaatidentiteit door private sleutels te genereren en te beschermen.

Firewallbescherming

Zorg dat malware en virussen uw netwerk niet kunnen binnendringen door de printertoegang te beperken tot apparaten in het netwerk.

Standaard gebruikersauthenticatie

Verlaag de kosten en verklein de risico's door te eisen dat gebruikers zich aanmelden met pin- of pic-code, LDAP of Kerberos-authenticatie. U kunt deze methoden ook integreren met Active Directory.

Rolgebaseerde toegangscontrole

HP Access Control Rights Management helpt u om de kosten te reduceren en de risico's te verkleinen door beperking van de printerfunctionaliteit. Rolgebaseerde toegangscontrole maakt het mogelijk verschillende soorten gebruikers, of zelfs hele afdelingen, verschillende rechten te geven, afhankelijk van hun behoeften. U kunt bijvoorbeeld bepalen wie mag faxen, scannen naar e-mail of scannen naar fax.

Geavanceerde beveiligingsmaatregelen



Meer informatie

HP Access Control
hp.com/go/hpac

HP JetAdvantage Connect
hp.com/go/JetAdvantageConnect

HP Capture and Route
hp.com/go/hpcr

Geavanceerde authenticatie en tracking

Gebruik geavanceerde authenticatie (zoals wachtwoorden, proximitykaarten, smartcards of biometrie) en trackingoplossingen voor extra veiligheid en controle.

- *HP Access Control Secure Authentication* herstelt de controle, versterkt de beveiliging en reduceert de kosten. U krijgt de beschikking over geavanceerde controleopties zoals touch-to-authenticate met mobiele apparaten die NFC ondersteunen.
- *HP Access Control Job Accounting* maakt het gemakkelijk om data accuraat te volgen en te verzamelen, deze te analyseren en rapporten te genereren en te verzenden. Gebruik de verzamelde data om de printkosten door te belasten, werknemers te motiveren om slimmer te printen en IT de noodzakelijke informatie te verschaffen om prognoses te maken over de toekomst van het printerpark.

Netwerktogang geldt ook voor mobiele apparaten

Maak mobiele apparaten onderdeel van uw totale printbeveiligingsstrategie om de toegang tot printers te controleren. HP biedt servergebaseerde pull-printoplossingen en geavanceerde beheer- en rapportagemogelijkheden.

- *HP JetAdvantage Connect* biedt intuïtief en betrouwbaar mobiel printen speciaal voor bedrijven. Het bespaart tijd en geld doordat voor het beheer van mobiel printen naadloos gebruik wordt gemaakt van bestaande IT-netwerkt tools en -policy's.¹¹ Gebruikers kunnen waar en wanneer dat nodig is veilig printen vanaf een groot aantal smartphones en tablets, met hetzelfde gemak als waarmee ze printen vanaf een pc.
- *HP Access Control* bevat functionaliteit voor het beheren van mobiel printen. Het maakt gebruik van de bestaande e-mailinfrastructuur en stelt mobiele gebruikers in staat naar hun printwachtrij te e-mailen en te printen op elke printer of MFP die de oplossing ondersteunt. Bescherm netwerkprinters met veilige authenticatiefuncties zoals Mobile Release.

Dicht datalekken voordat ze schade aanrichten

HP oplossingen bieden functionaliteit die beschermt tegen dataverlies. Met *HP Capture and Route Data Loss Prevention* kunt u verhinderen dat gevoelige informatie wordt gescand of gefaxt. Met *HP Access Control Print Data Loss Prevention* kunt u voorkomen dat vertrouwelijke documenten worden geprint. Traceer uw belangrijke data om diefstal te ontmoedigen en schendingen te voorkomen zonder uw workflows te vertragen. Ontvang intelligente beveiligingswaarschuwingen op basis van kenmerken die u kiest.

Digitale certificaten voor printertogang

Vergroot de veiligheid van uw printomgeving door digitale certificaten in te stellen voor netwerkprinters en MFP's. Bespaar tijd door met HP JetAdvantage Security Manager automatisch certificaten te installeren en te vernieuwen.⁹



Bescherm het document



Meer informatie

HP JetAdvantage Secure Print
hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Private Print
hp.com/go/JetAdvantagePrivatePrint

HP Access Control
hp.com/go/hpac

Documentbescherming van HP en TROY
hp.com/go/HPandTROY

Integreer slimme hardware- en softwareoplossingen in uw IT-beveiligingsplan om vertrouwelijke informatie in geprinte documenten te beveiligen.⁶

Fundamentele beveiligingsmaatregelen

Beperk de toegang tot voorbedrukte formulieren

Installeer afsluitbare invoerladen in uw printers en MFP's om diefstal van speciaal papier voor cheques, recepten of andere gevoelige documenten te voorkomen.

Bescherm vertrouwelijke documenten door veilig te printen met pincode of pull-printing

Gebruikers kunnen kiezen voor pin- of pull-printing, zodat minder personal printers nodig zijn en printtaken minder snel in verkeerde handen vallen. Deze beveiligingsmaatregelen beperken ook het aantal niet-opgehaalde prints, wat kosten en verspilling reduceert.

Bij printen met pin moeten gebruikers die een vertrouwelijke printtaak versturen een pincode instellen, die zij op de printer dienen in te voeren om de taak vrij te geven.

Bij pull-printen worden de printtaken in de cloud of op uw pc opgeslagen. Gebruikers authenticeren zich op de printlocatie van hun keuze om hun documenten vrij te geven en te printen. HP biedt twee cloudgebaseerde pull-printoplossingen:

- *HP JetAdvantage Secure Print* is een betaalbare oplossing voor MKB-bedrijven waarbij printtaken worden opgeslagen in de cloud of op de desktop-pc van de gebruiker. Het is gemakkelijk te installeren en te gebruiken, het stelt gebruikers in staat printtaken vrij te geven vanaf een mobiel apparaat en het ondersteunt apparaten van meerdere merken.¹²
- *HP JetAdvantage Private Print*, de cloudgebaseerde pull-printoplossing van HP, geeft u de voordelen van pull-printen zonder de complexiteit. De oplossing is eenvoudig zonder server, installatie of onderhoud te implementeren.¹³

Geavanceerde beveiligingsmaatregelen

Stel pull-printen verplicht voor elke printtaak

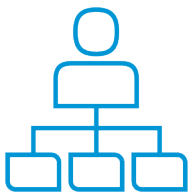
HP Access Control Secure Pull Printing beschermt vertrouwelijke informatie, beveiligt apparaten beter en verhoogt de efficiëntie. Deze krachtige servergebaseerde oplossing biedt diverse vormen van authenticatie, inclusief vrijgave via een badge en beveiliging en beheer op enterpriseniveau.

Gebruik MICR, watermerken of andere kenmerken om kopiëren of wijzigen te voorkomen

Tot de antivervalsingsoplossingen van HP en TROY behoren beveiligingstoner die vlekken op het papier maakt als er met chemicaliën is geknoeid, het gebruik van variabele watermerken op geprinte pagina's en het genereren van machinaal leesbare codering om individuele documenten te volgen en te controleren. MFP's kunnen antifraudekenmerken, zoals speciale handtekeningen, bedrijfslogo's en beveiligingsfonts, aanbrengen op gevoelige documenten zoals recepten, geboortebewijzen of afschriften.



Monitor en beheer uw printeromgeving



Meer informatie

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Bewakings- en beheeroplossingen helpen u kwetsbaarheden op te sporen en een uniforme policygebaseerde aanpak te creëren voor het beschermen van gegevens, het terugdringen van risico's en het versterken van de compliance.⁶ Voorkom lacunes in de beveiliging en vermijd hoge boetes.

Fundamentele beveiligingsmaatregelen

Werk apparaten bij met de nieuwste firmware-/OS-versies

Gebruik HP Web Jetadmin¹⁴ om firmware-updates naar alle printers te sturen, zodat deze altijd voorzien zijn van de nieuwste apparatuurbeschermings- en beveiligingskenmerken.

Controleer de printerbeveiliging met incidentenlogboeken

HP apparaten sturen printervoorvallen en meldingen naar een syslogserver, zodat het IT-team eventuele problemen kan oplossen.

Evalueer en herstel de beveiligingsinstellingen van apparaten

Gebruik de *HP Print Manageability Integration Kit* (MIK), een plug-in voor Microsoft® System Center Configuration Manager (SCCM), om de essentiële printerbeveiligingsinstellingen voor het hele printerpark te beheren. Microsoft SCCM is een veelgebruikte beheeroplossing om netwerkeindpoints op afstand te plannen, te implementeren, te configureren en te bewaken. De HP Print MIK kan de 15 belangrijkste beveiligingsinstellingen detecteren, evalueren, herstellen en het resultaat rapporteren.

Kies *HP JetAdvantage Security Manager*⁹ als u voor uw hele printerpark uitgebreid beveiligingsbeheer wilt implementeren. Met deze oplossing verlaagt u de kosten en het aantal resources om een beveiligingspolicy voor al uw printers in te stellen, apparaatinstellingen automatisch te herstellen en unieke certificaten te installeren en te vernieuwen. Daarnaast kunt u ook rapporten over uw compliance genereren.



Meer informatie

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Geavanceerde beveiligingsmaatregelen

Gebruik SIEM-software om bedreigingen te detecteren en te documenteren

Stuur uit HP FutureSmart-apparaten afkomstige voorvalgegevens naar incidentdetectietools zoals ArcSight, Splunk en SIEMonster voor real-time bewaking. IT-beveiliging ziet de printer-endpoints als onderdeel van het totale IT-ecosysteem en kan printerbeveiligingsproblemen signaleren en oplossen.

Nieuwe printers worden automatisch geconfigureerd als ze in het netwerk worden aangesloten

De functie Instant-on Security uit HP JetAdvantage Security Manager configureert nieuwe apparaten automatisch als deze op het netwerk worden aangesloten of na opnieuw opstarten.

Compliance-auditrapportage van printerparkbeveiliging

Gebruik HP JetAdvantage Security Manager om proof-of-compliance-rapporten te genereren waarmee u kunt aantonen dat beveiligingsbeleid wordt toegepast om printers en klantgegevens te beveiligen.

Niet-naleving kan nadelige gevolgen hebben voor uw bedrijf

Niet-beveiligde of onvoldoende beveiligde endpoints geven cybercriminelen nog meer gelegenheid om toe te slaan. Om de groeiende bedreigingen het hoofd te bieden, implementeren overheidsorganen overal ter wereld strenge beveiligingswetgeving die vereist dat organisaties klantgegevens beter beschermen.

Het niet naleven van de wet- en regelgeving kan bedrijven veel geld kosten en leiden tot boetes,

verlies van klanten, reputatieschade en groepsgedingen.

Het is noodzakelijk om apparaten en oplossingen zoals HP Enterprise printers en HP JetAdvantage Security Manager te implementeren, die u helpen aan de nalevingsvereisten te voldoen en uw bedrijfsgegevens te beschermen tegen bedreigingen.



Alle hulp die u nodig heeft

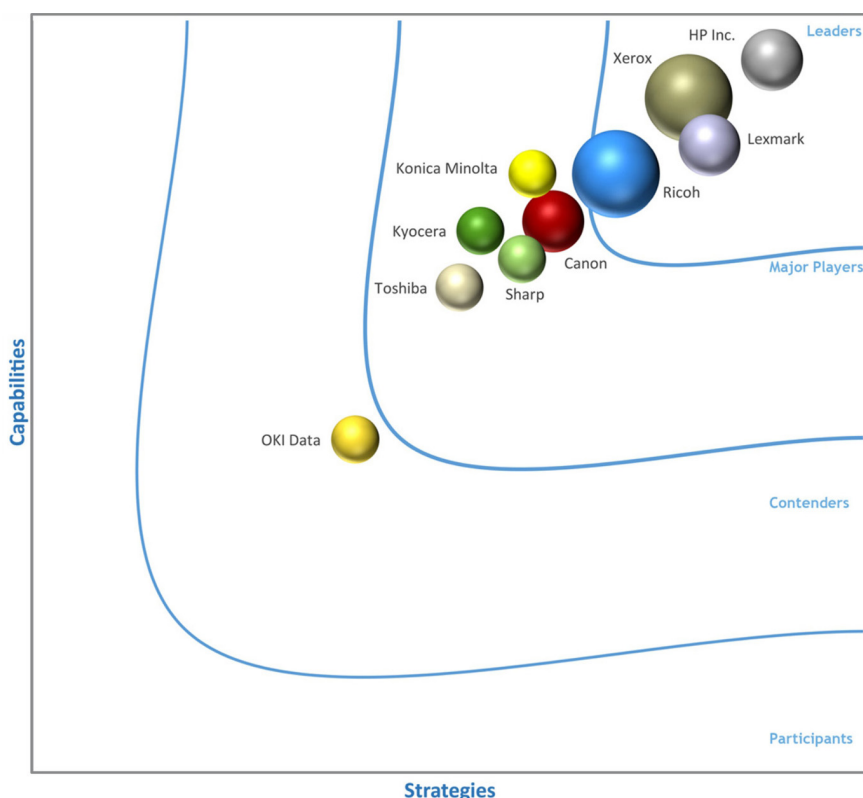
U hoeft de bescherming en beveiliging niet alleen aan te pakken. Een supportteam van adviseurs kan u vertellen hoe u de beveiliging van uw data, apparaten en documenten kunt verbeteren.

Evalueer samen met printbeveiligingsexperts de zwakke plekken in uw printerbeveiliging. Wij helpen u de kwetsbaarheden in uw printerbeveiliging te evalueren, een uitgebreide printerbeveiligingspolicy op te stellen op basis van de bedrijfsbehoeften en best practices en een plan te creëren om uw unieke omgeving beter te beveiligen.

Erkend als industrieleider

HP wordt genoemd als leider in het eerste IDC MarketScape-rapport "Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment". (U vindt het rapport [hier](#).) In het rapport staat: "HP Inc. beveiligt de gehele print- en documentinfrastructuur, variërend van de vergrendeling van apparaten tot alle aspecten van apparatuurgebruik en bescherming van content". De getoonde grafiek is afkomstig uit de IDC 2017 Vendor Assessment.¹⁵

Het IDC MarketScape vendoranalysemodel is ontworpen om een overzicht te bieden van het concurrentievermogen van IT-leveranciers in een gegeven markt. De onderzoeksmethode omvat een rigoureuze scoringsmethode op basis van kwalitatieve en kwantitatieve criteria die resulteert in één grafische illustratie van de positie van elke vendor in een gegeven markt. De capaciteitscore meet het vendorproduct, go-to-market en bedrijfsvoering op korte termijn. De strategiescore meet de afstemming van de strategie van de vendor op de behoeften van klanten over een periode van drie tot vijf jaar. De grootte van de pictogrammen geeft het marktaandeel van de vendor aan.¹⁵



Begin hier

Neem contact op met uw verkoopvertegenwoordiger voor meer informatie over HP beveiligingskenmerken, oplossingen en services die u extra bescherming en zekerheid bieden.

Meer informatie

hp.com/go/printsecurity

¹ Claim over 'De veiligste printers' is gebaseerd op een evaluatie door HP van in 2017 gepubliceerde beveiligingskenmerken in concurrerende printers uit dezelfde klasse. Alleen HP biedt een combinatie van beveiligingskenmerken die kan bewaken om aanvallen te detecteren, deze automatisch te stoppen en daarna bij het opnieuw opstarten de software-integriteit te valideren. Kijk voor een lijst van printers op: hp.com/go/PrintersThatProtect. Kijk voor meer informatie op: hp.com/go/printersecurityclaims.

² InfoTrends, "Designing Hardware & Solutions," Brendan Morse, oktober 2016.

³ Quocirca, "Managed Print Services Landscape, 2016," quocirca.com/content/managed-print-services-landscape-2016, juli 2016.

⁴ Enquête van Spiceworks onder 309 IT-professionals in Noord-Amerika, EMEA, Azië en Oceanië, die uitgevoerd werd namens HP, november 2016.

⁵ Quocirca, "Print security: An imperative in the IoT era", quocirca.com/content/print-security-imperative-iot-era, januari 2017.

⁶ Bepaalde oplossingen worden niet op alle HP apparaten ondersteund; mogelijk moet functionaliteit apart worden aangeschaft.

⁷ De meest geavanceerde ingebouwde HP beveiligingsfuncties zijn beschikbaar op HP Enterprise-klasse apparaten met FutureSmart firmware 4.5 of hoger; de claim is gebaseerd op een evaluatie door HP van in 2017 gepubliceerde ingebouwde beveiligingskenmerken van concurrerende printers uit dezelfde klasse. Alleen HP biedt een combinatie van beveiligingsfuncties, van integriteitscontrole tot zelfherstellend BIOS. Kijk voor een overzicht van compatibele producten op hp.com/go/PrintersThatProtect. Kijk voor meer informatie op hp.com/go/printersecurityclaims.

⁸ Bepaalde HP LaserJet Pro- en PageWide Pro-apparaten bevatten ingebouwde beveiliging die een aanval kan detecteren en afweren. Kijk voor meer informatie op hp.com/go/PrintersThatProtect.

⁹ HP JetAdvantage Security Manager moet apart worden aangeschaft. Kijk voor meer informatie op hp.com/go/securitymanager.

¹⁰ U heeft een extra wachtwoord nodig als u informatie naar een met een wachtwoord beveiligde repository stuurt.

¹¹ HP JetAdvantage Connect werkt met de meeste gangbare mobiele apparaten. Voor apparaten met Android™-, Google Chrome™- en Microsoft®-besturingssystemen moet eenmalig een plug-in worden geïnstalleerd. Kijk voor een lijst met ondersteunde besturingssystemen op hp.com/go/JetAdvantageConnect.

¹² HP JetAdvantage Secure Print: Pull-printing werkt met iedere op het netwerk aangesloten printer of MFP. Authenticatie op het apparaat is beschikbaar voor een groot aantal HP LaserJet, PageWide en OfficeJet Pro apparaten en bepaalde niet-HP apparaten. Voor sommige apparaten is een firmware-upgrade vereist. Voor opslag in de cloud en het ophalen van printtaken is een internetverbinding nodig. Voor het vrijgeven van printtaken vanaf een mobiel apparaat zijn een netwerkverbinding en een QR-code nodig. Kijk voor meer informatie en een lijst van ondersteunde printers en MFP's op hp.com/go/JetAdvantageSecurePrint.

¹³ HP JetAdvantage Private Print is gratis beschikbaar, de printer moet verbinding hebben met internet en webservices moeten ingeschakeld zijn. Niet in alle landen beschikbaar. Kijk voor meer informatie op hp.com/go/JetAdvantagePrivatePrint.

¹⁴ HP Web Jetadmin kan gratis worden gedownload van hp.com/go/webjetadmin.

¹⁵ Op grond van een evaluatie van hardcopyleveranciers door IDC en inzicht in het leiderschap van HP wordt gezegd: "De pluspunten van HP Inc. zijn krachtige IT-services en capaciteiten...die een uitgebreide, geïntegreerde beveiligingsstrategie in de hele IT-infrastructuur mogelijk maken." BRON: IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment, door Allison Correia en Robert Palmer, oktober 2017, IDC Doc #US41988517.

Meld u aan voor updates op

hp.com/go/getupdated



Delen met collega's

© Copyright 2014-2018 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 garantievoorwaarden die bij dergelijke producten en diensten op fysieke en/of elektronische wijze worden meegeleverd of gepubliceerd op 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.

Android en Google Chrome zijn geregistreerde handelsmerken van Google Inc. Microsoft is een in de V.S. geregistreerd handelsmerk van de Microsoft-groep.

