Overzicht van de oplossing

Bescherm uw netwerk met de veiligste printers ter wereld

94%

van de financiële bedrijven noemt copier/printerbeveiliging belangrijk of zeer belangrijk[1]

61%

van de bedrijven meldde minstens één printergerelateerde dataschending in het afgelopen jaar[2]

43%

van de bedrijven ziet printers over het hoofd bij endpointbeveiliging[3]

Slechts 18% van de bedrijven controleert printers op bedreigingen.[3] Hoe zit dat bij u?

Herken de verborgen risico's

IT-afdelingen krijgen de opdracht om vertrouwelijke gegevens te beschermen, van de persoonsgegevens van medewerkers tot klantgegevens, op de meest uiteenlopende apparaten en in allerlei omgevingen. Vaak passen IT-afdelingen de meest rigoureuze beveiligingsmaatregelen toe op de verschillende computers en het bedrijfsnetwerk. Maar de printers en scanners worden vaak over het hoofd gezien. Onbeveiligde apparaten maken het hele netwerk kwetsbaar voor een cyberaanval.

Inzicht in de potentiële kosten

Slechts één gat in de beveiliging kan al voor hoge kosten zorgen. Wanneer persoonlijke informatie openbaar wordt door onbeveiligde printers en scanners, kunnen de gevolgen zeer ernstig zijn: identiteitsfraude, diefstal van concurrentiegevoelige gegevens, reputatieschade of processen. Bovendien kunnen de kosten van niet-naleving van de wet hoog oplopen.

HP kan u helpen

Bescherm uw netwerk met de veiligste printers ter wereld[5], bijvoorbeeld met apparaten die een aanval automatisch detecteren en tegenhouden. HP helpt u bij het automatiseren van uw apparaten, gegevens en documenten met een breed portfolio oplossingen. Onze beveiligingsexperts helpen u bij het uitwerken van een complete beveiligingsstrategie voor uw printers en scanners.

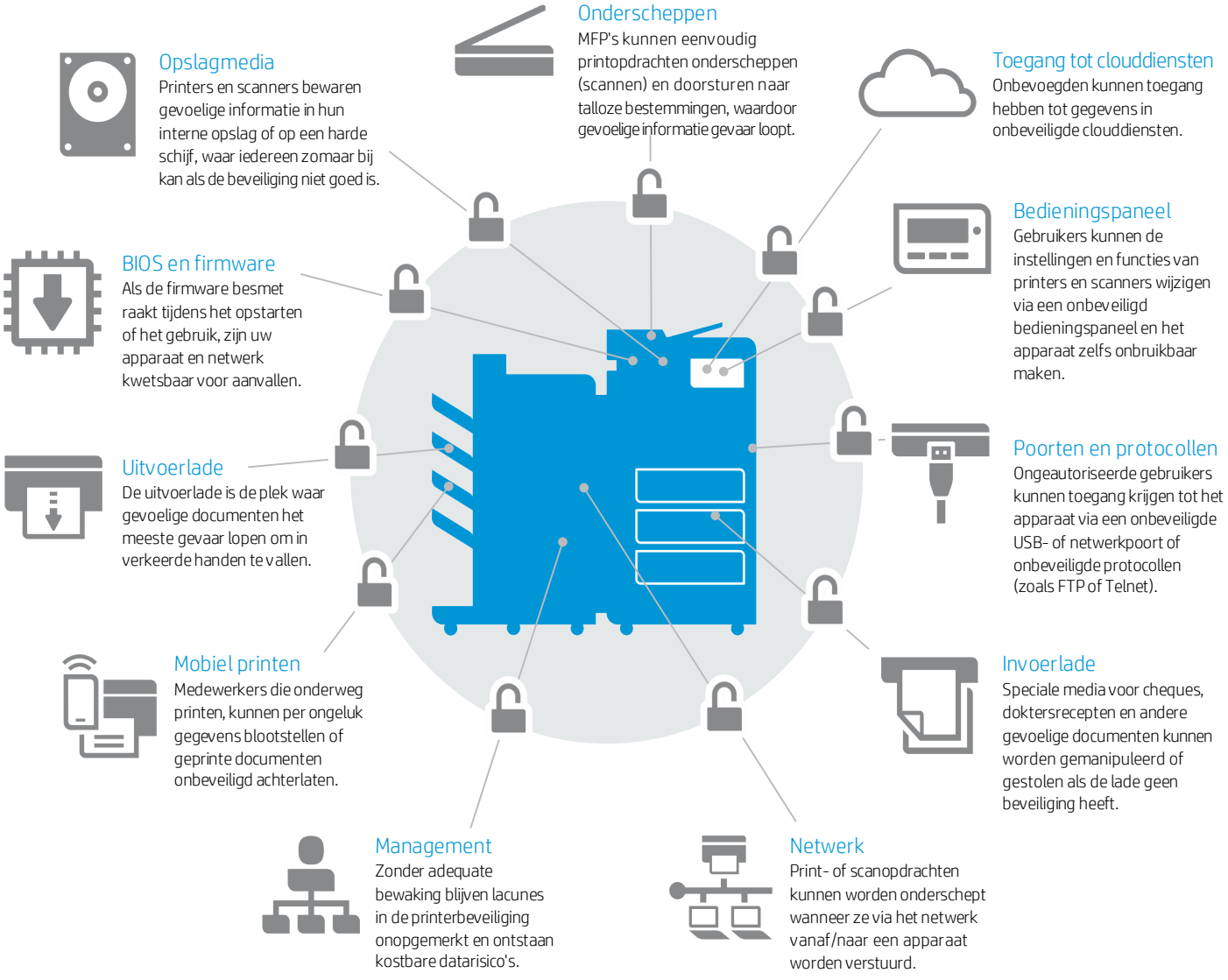
"Dankzij jarenlange investeringen in printerbeveiliging heeft HP het breedste aanbod beveiligingsoplossingen en diensten op de markt."

– Quocirca, januari 2017[4]

Bescherm uw apparaten, gegevens en documenten

Kritische lacunes kunnen op verschillende plaatsen in uw print- en scanomgeving aanwezig zijn. Als u deze kwetsbare punten eenmaal kent, kunt u de risico's gemakkelijker aanpakken.

Zwakke plekken bij het scannen en printen



Opslagmedia
Printers en scanners bewaren gevoelige informatie in hun interne opslag of op een harde schijf, waar iedereen zomaar bij kan als de beveiliging niet goed is.

Onderscheppen
MFP's kunnen eenvoudig printopdrachten onderscheppen (scannen) en doorsturen naar talloze bestemmingen, waardoor gevoelige informatie gevaar loopt.

Toegang tot clouddiensten
Onbevoegden kunnen toegang hebben tot gegevens in onbeveiligde clouddiensten.

BIOS en firmware
Als de firmware besmet raakt tijdens het opstarten of het gebruik, zijn uw apparaat en netwerk kwetsbaar voor aanvallen.

Bedieningspaneel
Gebruikers kunnen de instellingen en functies van printers en scanners wijzigen via een onbeveiligd bedieningspaneel en het apparaat zelfs onbruikbaar maken.

Uitvoerlade
De uitvoerlade is de plek waar gevoelige documenten het meeste gevaar lopen om in verkeerde handen te vallen.

Poorten en protocollen
Ongeautoriseerde gebruikers kunnen toegang krijgen tot het apparaat via een onbeveiligde USB- of netwerkpoort of onbeveiligde protocollen (zoals FTP of Telnet).

Mobiel printen
Medewerkers die onderweg printen, kunnen per ongeluk gegevens blootstellen of geprinte documenten onbeveiligd achterlaten.

Invoerlade
Speciale media voor cheques, doktersrecepten en andere gevoelige documenten kunnen worden gemanipuleerd of gestolen als de lade geen beveiliging heeft.

Management
Zonder adequate bewaking blijven lacunes in de printerbeveiliging onopgemerkt en ontstaan kostbare datarisico's.

Netwerk
Print- of scanopdrachten kunnen worden onderschept wanneer ze via het netwerk vanaf/naar een apparaat worden verstuurd.

Bescherming van het apparaat

HP printers zijn gemaakt om de risico's terug te dringen, de compliance te verbeteren en uw netwerk end-to-end te beschermen samen met monitoring- en beheeroplossingen. (Niet alle kenmerken en oplossingen zijn op ieder HP apparaat beschikbaar.)[6]

Essentiële vormen van beveiliging

Gecodeerde opslag met beveiligd wissen
Gevoelige informatie die op een intern station of harde schijf wordt opgeslagen, kan worden gestolen. HP apparaten werken daarom met ingebouwde codering om de gegevens te beschermen. Op het moment dat de opgeslagen gegevens niet meer nodig zijn, kunt u die gegevens overschrijven met de ingebouwde functie daarvoor en de gevoelige informatie op deze manier veilig verwijderen.

Veilige afvoer
HP Custom Recycling Services zorgen ervoor dat gegevens van de harde schijf worden verwijderd voordat oude producten worden gerecycled.

Veilige printerreparatie
Weet wat voor beveiliging uw onderhoudspartners gebruiken en bescherm uw gevoelige informatie. Kies daarom voor HP Secure Managed Print Services (MPS) of laat u bijstaan door deskundige HP partners.

Uitschakelen van ongebruikte poorten en protocollen
Een correct geconfigureerd apparaat is beter beschermd tegen aanvallen. Schakel daarom fysieke poorten en onveilige protocollen (FTP of Telnet bijvoorbeeld) uit om toegang of gebruik door onbevoegden te voorkomen.

Beheer van de toegang tot apparaten
Met beheerderswachtwoorden zorgt u ervoor dat de apparaatinstellingen alleen te wijzigen zijn door IT-medewerkers of ander bevoegd personeel.

Whitelisting van firmwarecode
Op de volgende pagina leest u hoe whitelisting uw printerpark kan beschermen tegen malware.

Meer informatie

HP Custom Recycling Services
hp.com/go/businessrecycling

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

Meer informatie

Ingebouwde beveiligingsvoorzieningen:
- HP Sure Start (BIOS-integriteit)
- Whitelisting van firmwarecode
- Runtime inbraakdetectie

hp.com/go/PrintersThatProtect

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Geavanceerde beveiliging

Common Criteria Certification

De zakelijke printers van HP voldoen (gecertificeerd) aan internationale beveiligingsnormen, zoals Common Criteria Certification (CCC) en FIPS 140. Dankzij ondertekende firmware-updates weet u zeker dat de firmware authentiek is en dat alle regels zijn nageleefd.

Automatisch detecteren en tegenhouden van aanvallen

De zakelijke printers van HP hebben specifieke beveiligingsvoorzieningen om te voorkomen dat via uw printers uw netwerk wordt aangevallen. Alleen HP printerbeveiliging biedt realtime detectie, automatische bewaking en ingebouwde softwarevalidatie om bedreigingen in de kiem te smoren.[7]

De zakelijke printers van HP, van Pro[8] tot en met Enterprise[7], zijn automatisch in staat om een aanval te detecteren en tegen te houden tijdens alle gebruiksfasen:

- **Tijdens het opstarten.** De opstartcode (voor Pro-apparaten) of het BIOS (voor Enterprise-apparaten) bestaat uit instructies voor het laden van de essentiële hardwarecomponenten en het initiëren van de firmware. De integriteit van de code wordt gecontroleerd bij elke opstartcyclus en dit beschermt uw apparaat tegen aanvallen.
- **Tijdens het laden van de firmware.** Whitelisting wil zeggen dat alleen originele, goed werkende HP firmware (digitaal door HP ondertekend) in het geheugen wordt geladen. Wanneer er een afwijking wordt gedetecteerd, wordt het apparaat opnieuw opgestart in een veilige offline-toestand en blijft het apparaat wachten tot geldige firmware wordt geladen.
- **Tijdens het concrete gebruik.** Geïntegreerde HP functies beschermen het apparaatgeheugen wanneer het apparaat operationeel is en verbinding heeft met het netwerk, dus wanneer de meeste aanvallen plaatsvinden. Is er echt een aanval, dan wordt het apparaat meteen uitgeschakeld.

HP Enterprise-apparaten repareren zichzelf

HP Enterprise-printers kunnen meer dan bedreigingen detecteren en tegenhouden. Ze hebben ook beveiligingsvoorzieningen aan boord om het apparaat automatisch te herstellen. Dit betekent maximale uptime met minimaal werk voor de IT-afdeling.[7] Wanneer er een aanval of afwijking wordt geconstateerd, wordt het apparaat automatisch opnieuw opgestart.

- *HP Sure Start* is het eerste zichzelf reparerende BIOS in de sector.[7] Wanneer het BIOS is gekraakt, start HP Sure Start het apparaat opnieuw op en wordt een geïntegreerde 'gouden kopie' van het BIOS geladen.
- *Runtime inbraakdetectie* bewaakt het geheugen en start het apparaat opnieuw op bij een aanval. Via SIEM-tools (Security Information and Event Management) zoals ArcSight of Splunk kan de systeembeheerder op de hoogte worden gebracht.

Upgrades van de FutureSmart-firmware zijn mogelijk, wat garant staat voor een veilige investering. Het is zelfs mogelijk om een deel van de geïntegreerde functies toe te voegen aan bepaalde bestaande Enterprise-printers.[7]

Afronding van de controlecyclus met HP JetAdvantage Security Manager

Wanneer een apparaat opnieuw wordt opgestart en wanneer een nieuw apparaat aan het netwerk wordt toegevoegd, controleert HP JetAdvantage Security Manager automatisch de beveiligingsinstellingen van het apparaat en worden deze instellingen zo nodig aangepast om naleving van het beleid van het bedrijf te waarborgen.[9] De IT-afdeling hoeft hier niets voor te doen.

Hoe werkt het?

De geïntegreerde beveiligingsvoorzieningen voeren de eerste drie stappen in de cyclus van een HP apparaat uit.

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

HP JetAdvantage Security Manager rondt de controlecyclus af.

Bescherming van gegevens

Of gegevens nu opgeslagen of onderweg zijn, continue bescherming is een absolute vereiste. Hier zijn enkele essentiële stappen voor een veilig transport en gebruik.[6]

Essentiële vormen van beveiliging

802.1x of IPsec (netwerknormen)
Gebruik netwerknormen die met codering werken om gegevens die via het netwerk worden uitgewisseld (tussen het apparaat en beheerprogramma's zoals HP Web Jetadmin of de Embedded Web Server) te beveiligen.

Codering van gegevens tijdens transport
Met bijvoorbeeld Internet Print Protocol over TLS (IPPS) kunt u de printopdrachten die naar het apparaat worden verzonden, coderen en beveiligen. HP Universal Print Driver Secure Encrypted Print biedt symmetrische AES256-codering (en decodering) van printopdrachten, van client tot pagina, met een door de gebruiker gedefinieerd wachtwoord. Daarvoor wordt gebruikgemaakt van FIPS 140-gevalideerde cryptografiebibliotheken van Microsoft.

Bij het scannen staan HP JetAdvantage-workflowoplossingen in voor de bescherming van gevoelige informatie en een verhoging van de efficiëntie. HP Capture and Route bijvoorbeeld integreert naadloos met HP Access Control als extra beveiliging. Gebruikers hoeven zich maar één keer te identificeren en content kan uitstekend worden gemonitord, wat belangrijk kan zijn voor uw 'information governance'.[10]

Codering van opgeslagen gegevens
Met ingebouwde codering beschermt u gevoelige gegevens die op de harde schijf zijn opgeslagen. Een extra beveiligingsniveau is mogelijk in de vorm van de optionele HP Trusted Platform Module (TPM), een accessoire dat in het apparaat kan worden ingebouwd om gecodeerde gebruikersgegevens en data beter te beschermen door de coderingssleutels automatisch te laten verzegelen door de TPM. Deze module genereert de private sleutels voor de bescherming van de identiteit van het apparaat.

Firewall
Voorkom dat malware en virussen in uw netwerk kunnen komen door alleen apparaten binnen het netwerk toegang te geven tot de printer.

Identificatie van gebruikers
Verlaag de kosten en beveiligingsrisico's door gebruikers te verplichten om zich aan te melden met PIN/PIC-, LDAP- of Kerberos-verificatie. Integratie hiervan met Active Directory is ook mogelijk.

Toegangscontrole op basis van functie
HP Access Control Rights Management. Door het gebruik van printerfuncties aan banden te leggen kunt u de kosten en beveiligingsrisico's verder beperken. Toegangscontrole op basis van functie maakt het mogelijk om verschillende gebruikers of afdelingen verschillende mogelijkheden te bieden, afhankelijk van hun behoeften. U beperkt bijvoorbeeld wie mag faxen of wie mag scannen naar e-mail of fax.

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

Meer informatie

HP Access Control
hp.com/go/hpac

HP JetAdvantage Connect
hp.com/go/JetAdvantageConnect

Geavanceerde beveiliging

Geavanceerde verificatie en tracking
Met geavanceerde vormen van verificatie (denk aan wachtwoorden, proximity- of smartcards of biometrie) en tracking zorgt u voor extra beveiliging en controle.

- *HP Access Control Secure Authentication.* Deze robuuste verificatieoplossing zorgt voor extra controle en beveiliging en lagere kosten. Hiermee beschikt u over tal van geavanceerde controlefuncties en opties zoals verificatie door een mobiel apparaat met NFC-ondersteuning tegen de printer te houden.
- *HP Access Control Job Accounting.* Voor het zorgvuldig vastleggen en analyseren van gegevens en het opstellen en verzenden van rapporten. Op basis van de verzamelde gegevens wijst u de printkosten toe, motiveert u medewerkers om slimmer te printen en bezorgt u de IT-afdeling de juiste informatie om prognoses te doen voor het printerpark.

Mobiele apparaten ook in het netwerk
Voor uw printerbeveiliging kunt u probleemloos gebruikmaken van mobiele devices om gebruikers daarmee toegang te bieden tot uw printers. HP biedt servergebaseerde oplossingen voor veilig pull-printen en geavanceerde beheer- en rapportagefunctionaliteit.

- *HP JetAdvantage Connect.* Intuïtief en betrouwbaar mobiel printen voor bedrijven. Bespaar tijd en geld met de naadloze integratie met bestaande IT-netwerktools en regels voor mobiel printen.[11] Gebruikers kunnen veilig printen vanaf de meest uiteenlopende smartphones en tablets, waar en wanneer ze maar willen. Printen is hiermee net zo eenvoudig als printen vanaf een pc.
- *HP Access Control.* Deze oplossing bevat functionaliteit om het mobiele printen goed te kunnen beheren. Hiervoor wordt gebruikgemaakt van uw bestaande e-mailinfrastructuur. Mobiele gebruikers kunnen een printopdracht e-mailen naar hun printerwachtrij en die opdracht vervolgens opvragen op elke printer of MFP die dit ondersteunt. Bescherm uw netwerkprinters met veilige verificatievoorzieningen, zoals Mobile Release.

Digitale certificaten voor printers
Door digitale certificaten te gebruiken voor uw netwerkprinters en MFP's zorgt u voor een verdere verbetering van de beveiliging. Met HP JetAdvantage Security Manager worden uw certificaten automatisch geïnstalleerd en verlengd, wat extra tijdwinst betekent.[9]

Bescherming van het document

Integreer slimme hardware- en softwareoplossingen in uw IT-beveiligingsplan om de gevoelige informatie in uw geprinte documenten te beschermen.[6]

Essentiële vormen van beveiliging

Gecontroleerde toegang tot voorbedrukte formulieren
Voorzie uw printers en MFP's van invoerlades die op slot kunnen. Zo voorkomt u dat speciaal printpapier voor bijvoorbeeld cheques, doktersrecepten of andere gevoelige documenten wordt gestolen.

Optioneel printen met pincode of pull-printen voor gevoelige documenten
Gebruikers kunnen ervoor kiezen om iets te printen na invoer van een pincode of door middel van pull-printen. Zo hebben ze niet altijd hun eigen printer nodig en kan worden voorkomen dat geprinte documenten in verkeerde handen vallen. Deze beveiligingsmaatregelen zorgen er ook voor dat er minder prints voor eeuwig en altijd op de printer blijven liggen, wat kostenbesparend werkt en minder verspilling betekent.

Printen met een pincode houdt in dat gebruikers bij een vertrouwelijke printopdracht een pincode opgeven die vervolgens eerst moet worden ingevoerd op het apparaat voordat de opdracht echt wordt geprint.

Pull-printen houdt in dat printopdrachten worden opgeslagen in de cloud of op de pc van de gebruiker. De gebruiker identificeert zich op de gekozen printlocatie om de opdracht op te vragen (pull) en te printen. HP biedt twee cloudgebaseerde pull-print-oplossingen.

- *HP JetAdvantage Secure Print*. Deze betaalbare oplossing is speciaal ontwikkeld voor het mkb en is heel eenvoudig in te stellen en te gebruiken. Opdrachten kunnen worden opgeslagen in de cloud of op de desktop van de gebruiker en daarna worden vrijgegeven vanaf een mobiel device (apparatuur van verschillende leveranciers ondersteund).[12]
- *HP JetAdvantage Private Print*. De voordelen van pull-print zonder de complexiteit en zonder extra kosten. Eenvoudig in te stellen en geen server, installatie of onderhoud nodig.[13]

Geavanceerde beveiliging

Verplicht pull-printen voor elke printopdracht
HP Access Control Secure Pull Printing. Voor de bescherming van vertrouwelijke informatie, een betere beveiliging van uw apparaten en extra efficiëntie. Deze betrouwbare servergebaseerde oplossing biedt diverse vormen van verificatie, bijvoorbeeld vrijgave via een kaart, en beveiliging en beheer op maat van grote organisaties.

Gebruik van MICR, watermerken en andere functies om kopiëren of wijzigen tegen te gaan
HP en TROY bieden oplossingen om vervalsing te bestrijden, zoals speciale beveiligingstoner die vlekken maakt op het papier bij blootstelling aan chemische stoffen of gebruik van watermerken met variabele data of machinaal uitleesbare codes voor het traceren van documenten. MFP's kunnen geïntegreerde antifraudefuncties hebben, zoals speciale handtekeningen, bedrijfslogo's en speciale lettertypen voor gevoelige documenten, zoals doktersrecepten, geboortebewijzen of afschriften.

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

Veilige documenten met HP en TROY
hp.com/go/HPandTROY

Monitoring en beheer van uw printomgeving

Oplossingen voor de monitoring en het beheer van uw beveiliging helpen u bij het duidelijk krijgen van de zwakke plekken en het uitwerken van één complete strategie voor gegevensbescherming, risicobeheersing en compliance.[6] Werk alle lacunes in de beveiliging weg en voorkom hoge boetes.

HP JetAdvantage Security Manager
Beveilig uw HP printerpark met de oplossing die door Buyers Laboratory (BLI) wordt omschreven als 'trailblazing' (baanbrekend).[9]
hp.com/go/securitymanager

Essentiële vormen van beveiliging

Bijwerken van apparaten met de meest recente firmware/besturingssoftware
Gebruik Web Jetadmin[14] om firmware-updates te pushen naar het hele printerpark. Zo zijn uw apparaten altijd up-to-date met de meest recente beveiligingsfuncties.

Raadplegen van beveiligingslogboeken
HP apparaten sturen printergebeurtenissen/meldingen door naar een syslogserver, zodat de IT-afdeling bepaalde problemen snel kan oppakken.

Evalueren en bijsturen van apparaatinstellingen
HP JetAdvantage Security Manager. Maak de beveiliging van uw printerpark minder duur en arbeidsintensief met de enige policygebaseerde compliancetool voor printerbeveiliging.[9] U bepaalt het beveiligingsbeleid voor het hele printerpark, automatiseert het corrigeren van apparaatinstellingen en installeert en vernieuwt unieke certificaten. En dit alles wordt ondersteund met alle rapporten die u nodig heeft om aan te tonen dat aan alle regels is voldaan.

Geavanceerde beveiliging

SIEM-software voor het detecteren en documenteren van bedreigingen
De gegevens van gebeurtenissen op een HP FutureSmart-apparaat kunnen worden verzonden naar detectietools zoals ArcSight of Splunk voor realtime bewaking. De IT-beveiliging ziet printers in een breder ecosysteem en maakt het eenvoudiger om beveiligingsproblemen te detecteren en aan te pakken.

Automatische configuratie van nieuwe printers in het netwerk
Het onderdeel Instant-on Security van HP JetAdvantage Security Manager zorgt ervoor dat nieuwe apparaten automatisch worden geconfigureerd op het moment dat ze aan het netwerk worden toegevoegd of opnieuw worden opgestart.

Audit van de naleving van de printerbeveiliging
Met HP JetAdvantage Security Manager creëert u rapporten waarmee u kunt aantonen dat het beveiligingsbeleid op uw printers is toegepast en dat klantgegevens veilig zijn.

Hulp van de experts

U hoeft het niet helemaal zelf te doen. Een team van consultants kan u laten zien hoe u de beveiliging van uw gegevens, apparaten en documenten verbetert.

Onze beveiligingsexperts kijken samen met u waar de zwakke plekken zitten en helpen u bij het uitwerken van een compleet beveiligingsbeleid voor uw specifieke behoeften. Vervolgens stellen zij een plan op om de beveiliging binnen uw specifieke omgeving te verbeteren.

Aan de slag

Neem contact op met uw HP salesvertegenwoordiger voor meer informatie over HP beveiligingsfuncties, oplossingen en services die u meer veiligheid bieden.

Ga voor meer informatie naar
hp.com/go/printsecurity

[1] InfoTrends, "Designing Hardware & Solutions", Brendan Morse, oktober 2016.

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

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

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

[5] De claim betreffende de veiligste printers is gebaseerd op een HP review van in 2016 gepubliceerde beveiligingsvoorzieningen van concurrerende printers in dezelfde klasse. Alleen HP biedt een combinatie van beveiligingsvoorzieningen die een aanval kunnen detecteren en tegenhouden en vervolgens de software-integriteit kunnen valideren bij het opnieuw opstarten. Ga voor een lijst met printers naar: hp.com/go/PrintersThatProtect. Voor meer informatie: hp.com/go/printersecurityclaims.

[6] Sommige oplossingen worden niet op alle HP apparaten ondersteund. Mogelijk moet functionaliteit apart worden aangeschaft.

[7] Van toepassing op HP Enterprise-apparaten die vanaf 2015 zijn geïntroduceerd en gebaseerd op een HP review van in 2016 gepubliceerde geïntegreerde beveiligingsvoorzieningen van concurrerende printers in dezelfde klasse. Alleen HP biedt een combinatie van beveiligingsvoorzieningen voor controle van de integriteit tot op BIOS-niveau met automatische reparatiemogelijkheden. Er kan een FutureSmart-servicepackupdate nodig zijn om de beveiligingsvoorzieningen te activeren. Ga voor een lijst met compatibele producten naar hp.com/go/PrintersThatProtect. Ga voor meer informatie naar hp.com/go/printersecurityclaims.

[8] Bepaalde HP LaserJet Pro- en PageWide Pro-apparaten hebben geïntegreerde voorzieningen voor het detecteren en tegenhouden van een aanval. Ga voor meer informatie naar hp.com/go/PrintersThatProtect.

[9] HP JetAdvantage Security Manager moet apart worden aangeschaft. Ga voor meer informatie naar hp.com/go/securitymanager. Claim over concurrentie gebaseerd op intern HP onderzoek naar het aanbod van concurrenten (Device Security Comparison, januari 2015) en het Solutions Report on HP JetAdvantage Security Manager 2.1 van Buyers Laboratory LLC, februari 2015.

[10] Wanneer u informatie stuurt naar een opslagplaats die met een wachtwoord is beveiligd, is een extra wachtwoord nodig.

[11] HP JetAdvantage Connect werkt met de bekende mobiele devices. Er hoeft alleen maar een plug-in te worden geïnstalleerd voor apparaten met Android™, Google Chrome™ of een besturingssysteem van Microsoft. Ga voor meer informatie en een lijst met ondersteunde besturingssystemen naar hp.com/go/JetAdvantageConnect.

[12] HP JetAdvantage Secure Print. Pull-print werkt met elke printer of MFP die met het netwerk is verbonden. On-device verificatie is beschikbaar voor allerlei HP LaserJet-, PageWide- en OfficeJet Pro-apparaten en bepaalde niet-HP apparaten. Voor sommige apparaten kan een firmware-upgrade nodig zijn. Internetverbinding vereist voor opslag in de cloud en het opvragen van printopdrachten. Voor het vrijgeven van printopdrachten vanaf een mobiel device is een netwerkverbinding en QR-code vereist. Ga voor meer informatie en een lijst met ondersteunde printers en MFP's naar hp.com/go/JetAdvantageSecurePrint.

[13] HP JetAdvantage Private Print is alleen beschikbaar in Noord-Amerika en bepaalde landen in Europa. Kaartlezer kan apart worden aangeschaft voor specifieke HP printers en MFP's met touchscreen. Ga voor meer informatie naar hp.com/go/JetAdvantagePrivatePrint.

[14] HP Web Jetadmin is gratis beschikbaar als download op hp.com/go/webjetadmin.

Meld u aan voor updates op
hp.com/go/getupdated

Delen met collega's

4AA3-1295NLE, April 2017, Rev. 8