



Beskyt dit netværk med verdens sikreste printere¹

94 %

af virksomhederne i den finansielle sektor siger, at sikkerheden for kopimaskiner/printere er vigtig eller meget vigtig²



61 %

af organisationerne rapporterede mindst ét brud på datasikkerheden for printere inden for det sidste år³



43 %

af firmaerne overser printere i deres sikkerhedspraksis for slutpunkter⁴





Kun 18 % af virksomhederne overvåger printere for mulige trusler.⁴ Gør din?

Opdag de skjulte trusler

Beskyttelse af personlige oplysninger, herunder de ansattes og kunders data på tværs af enheder og platforme, er en vigtig del af it-sikkerheden i dag. De fleste it-afdelinger fokuserer på beskyttelse af computere og netværk, men glemmer tit sikkerheden omkring scannere og printere. Ubeskyttede enheder udgør en sikkerhedsrisiko for hele netværket.

Forstå de potentielle omkostninger

Selv et enkelt sikkerhedshul kan vise sig at være dyrt. Hvis personlige data bringes i fare på grund af en ubeskyttet scanner eller printer, kan det ende i identitetstyveri, tyveri af forretningshemmeligheder, ødelæggelse af brandets omdømme og dyre retssager. Manglende overholdelse af lovmæssige krav for beskyttelse af personlige oplysninger kan også medføre store bøder.

HP kan hjælpe

Beskyt dit netværk med verdens sikreste printere.¹ HP-printere er altid på vagt. De er i stand til at opdage og stoppe både kendte og nye trusler. HPs store udvalg af produkter og løsninger kan hjælpe dig med at automatisere sikkerheden omkring enheder samt håndteringen af data og dokumenter. Vores sikkerhedsekspert er parat til at hjælpe dig med at skabe og implementere en sikkerhedsstrategi for håndteringen af scanning og udskrivning.

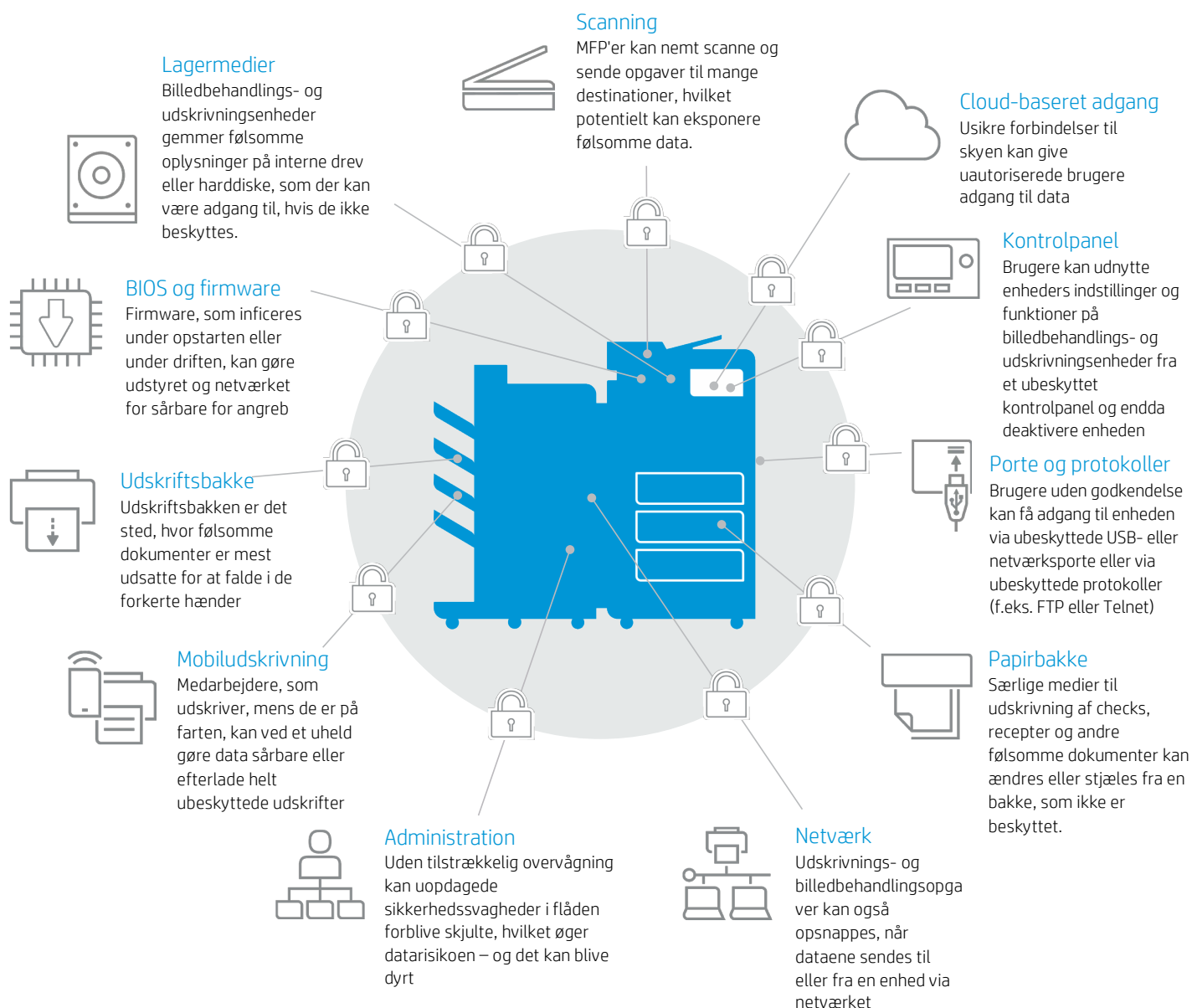
"HP har det største udvalg af uovertrufne sikkerhedsløsninger og tjenester på markedet, og det vidner om deres langsigtede investering i printersikkerhed."

– Quocirca, januar 2017⁵

Beskyt dit udstyr, dine data og dine dokumenter

Der kan opstå farlige sikkerhedshuller i miljøet til scanning, udskrivning og kopiering. Erkendelse af disse svage punkter er det første skridt i begrænsningen af risici.

Sårbare punkter i scannere, printere og kopimaskiner





Beskyt udstyret



Flere oplysninger

HP Custom Recycling-tjenester
hp.com/go/businessrecycling

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

HP-printere er designet til at fungere med løsninger til overvågning og styring af sikkerhed og er med til at forbedre sikkerheden på netværket, så du nemmere kan leve op til sikkerhedskravene (nogle funktioner og løsninger fås ikke med alle HP-enheder⁶).

Grundlæggende sikkerhedsfunktioner

Krypteret lager med funktion til sikker sletning

Vigtige data, der opbevares på et internt drev eller en intern harddisk, udgør en potentiel sikkerhedsrisiko, fordi de kan stjæles. Mange HP-enheder leveres derfor med indbygget kryptering, så dataene beskyttes. Når dataene ikke længere skal gemmes, kan du bruge den indbyggede funktion til sikker overskrivning, så de vigtige data slettes permanent.

Sikker bortskaffelse

HP Custom Recycling-tjenesterne omfatter sletning af data fra harddiske, inden de udtjente produkter sendes til forsvarlig genbrug.

Sikker printerreparation

Du kan altid være sikker på, at dine vigtige data er i gode hænder hos vores serviceteknikere. Med *HP Secure Managed Print Services (MPS)* og HP-partnere får du hjælp af de bedste eksperter.

Deaktiver ubrugte porte og protokoller

Reducer risikoen for angreb ved at konfigurere udstyret korrekt. Ved at deaktivere fysiske porte og netværksprotokoller som FTP og Telnet forhindrer du uautoriseret adgang til og brug af udstyret.

Administratoradgang til enheden

Angiv administratoradgangskoder, så kun it-personale og andre autoriserede brugere kan administrere og konfigurere enhedsindstillingerne.

Godkendelseslister over firmwarekode

Læs på næste side, hvordan godkendelseslister kan være med til at beskytte din flåde mod malware.

Avancerede sikkerhedsfunktioner

Common Criteria Certification

HP-printere til erhvervsbrug er certificeret for overholdelse af internationale sikkerhedsstandarder som Common Criteria Certification (CCC) og FIPS 140, som sikrer, at firmwareopdateringerne er signeret og lever op til kravene om kodeintegritet og ægthed.



Flere oplysninger

Integrerede printersikkerhedsfunktioner:

- HP Sure Start (BIOS-integritet)
- Godkendelseslister over firmwarekode
- Registrering af indtrængen under drift
- HP Connection Inspector

hp.com/go/PrintersThatProtect

HP JetAdvantage Security Manager:

hp.com/go/securitymanager

Printersikkerhedsfunktionerne opdager og stopper angreb automatisk

HP-printere til erhvervsbrug har indbyggede sikkerhedsfunktioner, som forhindrer printerens i at blive brugt som en bagdør til angreb på netværket. Det er kun HP's printersikkerhed, der giver beskyttelse i realtid, automatiseret overvågning og indbygget softwaregodkendelse, så truslerne elimineres i samme øjeblik, de opstår.⁷

HP-printere til erhvervsbrug fra Pro⁸ til Enterprise⁷ er konstant på vagt og kan stoppe trusler i alle driftsfasen:

- **Under opstart.** Startkoden i Pro-modellerne og BIOS i Enterprise-modellerne er et instruktionssæt, der bruges til indlæsning af vigtige hardwarekomponenter og initialisering af firmware. Kodeintegriteten kontrolleres under hver opstart, hvilket er med til at sikre enheden mod angreb.
- **Under indlæsning af firmware.** Godkendelseslistefunktionen kontrollerer firmwaren under startfasen for at sikre, at koden er original og digitalt signeret af HP. Hvis der opdages noget unormalt, genstarter enheden til en sikker offlinetilstand, og der sendes besked til it-afdelingen.
- **Under drift.** HP-printere har indbyggede funktioner til beskyttelse af enhedens hukommelse, når maskinen er tændt og er på netværket – dvs. når den er mest udsat for angreb. Når et angreb opdages, slukker maskinen automatisk.

HP Enterprise-enheder kan reparere sig selv

HP Enterprise-printere opdager og stopper ikke alene angreb. De har også selv-reparerende evner til at komme sig hurtigt efter et angreb, så it-afdelingen slet ikke behøver at gribe ind.⁷ Funktioner omfatter automatisk genstart, når et angreb finder sted, eller når der opstår andre unormale situationer. Administratorer får direkte besked via SIEM-værktøjer (Security Information and Event Management) som ArcSight, Splunk og SIEMONSTER.

- *HP Sure Start* er den eneste selvreparerende BIOS på markedet.⁷ Hvis BIOS'en kompromitteres, genstarter HP Sure Start maskinen og indlæser en "sikker" BIOS-version.
- *Funktionen til registrering af indtrængen under drift* overvåger komplekse firmware- og hukommelsesfunktioner og forhindrer forsøg på indtrængen ved at genstarte maskinen, når der registreres et angreb.
- *HP Connection Inspector* evaluerer løbende netværksforbindelser for at fastslå, hvad der er normalt, stoppe mistænkelige anmodninger og automatisk udløse en genstart, når der opdages et malwareangreb.

HP FutureSmart-firmware er en god investering, fordi den kan opgraderes, så mange eksisterende HP Enterprise-printere kan opgraderes med funktioner som godkendelseslister, registrering af indtrængen under drift og HP Connection Inspector.⁷

HP JetAdvantage Security Manager fuldender kontrollen

Efter hver genstart, eller når en ny enhed føjes til netværket, foretager *HP JetAdvantage Security Manager* en automatisk kontrol af enhedens sikkerhedsindstillinger og ændrer dem om nødvendigt, så virksomhedens sikkerhedspolitik altid overholdes.⁹ Der er ikke behov for, at it-afdelingen griber ind.

Hvordan fungerer det?

De indbyggede sikkerhedsfunktioner har fokus på fire primære trin i en HP-enheds cyklus.

Når der registreres et angreb, kan HP Enterprise-enheder genstarte sig selv og udføre selv-reparation.

HP JetAdvantage Security Manager fuldender kontrollen.

Fire. Kontinuerlig overvågning

Driftsbeskyttelse og afvisning af angreb, når enheden kører.

Undersøgelse af udgående netværksforbindelser for at stoppe mistænkelige anmodninger (kun Enterprise-modeller).

Tre. Indstillingerne kontrolleres

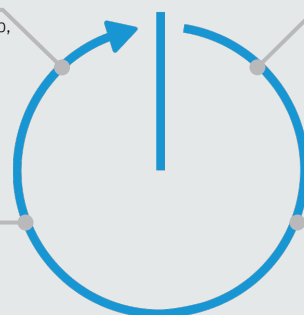
Efter genstart kontrollerer HP JetAdvantage Security Manager sikkerhedsindstillingerne på enheden og retter dem om nødvendigt.

En. Kontrol af BIOS/startkode

Forhindring af kørsel af skadelig kode under opstart ved kun at tillade indlæsning af original kode, der er signeret af HP.

To. Firmwaren kontrolleres

Kun original, godkendt firmware, der er digitalt signeret af HP, kan indlæses.





Beskyt dine data



Flere oplysninger

HP Web Jetadmin
hp.com/go/wja

HP Universal-printerdriver med sikker, krypteret udskrivning
hp.com/go/upd

HP JetAdvantage-løsninger til arbejdsgange
hp.com/go/documentmanagement

HP Access Control
hp.com/go/hpac

Dine data kræver beskyttelse, uanset om de opbevares på en statisk placering, eller du tager dem med dig. Her er nogle vigtige trin til sikker brug af dine data.⁶

Grundlæggende sikkerhedsfunktioner

802.1x- eller IPsec-netværksstandard

Brug netværksskryptering til beskyttelse af data, der sendes via netværket mellem enheden og styringsværktøjer som *HP Web Jetadmin* og *HP Embedded Web Server*.

Krypter data, når de sendes

Beskyt udskriftsopgaver, når de sendes til en printer, med kryptering som f.eks. IPPS (Internet Print Protocol over TLS). Du kan også bruge *HP Universal Print Driver Secure Encrypted Print*, som byder på ægte, symmetrisk AES256-kryptering og dekryptering af udskriftsopgaver, der understøtter brugerdefinerede adgangskoder via FIPS 140-validerede kryptografiske biblioteker fra Microsoft®.

Når du scanner, hjælper *HP JetAdvantage-løsningerne til arbejdsgange* med at beskytte de følsomme data og forbedre effektiviteten. HP Capture and Route fungerer f.eks. gnidningsfrit med HP Access Control og giver bedre sikkerhed og større brugervenlighed med understøttelsen af ét adgangskodelag og muligheden for overvågning af indhold for at kontrollere, at de sendte oplysninger opfylder de opstillede krav og regler.¹⁰

Krypter statiske data

Harddisken med indbygget kryptering hjælper med at beskytte dine vigtige forretningsdata. Du kan også vælge at montere et TPM-modul (HP Trusted Platform Module) i maskinen for at få endnu bedre beskyttelse af de krypterede logonoplysninger vha. forsegling af krypteringsnøglerne til maskinen i TPM-modulet. Modulet giver en sikker identitetsstyring ved at generere og beskytte private certifikatnøgler.

Firewallbeskyttelse

Du kan begrænse adgangen fra printerne til computerne på netværket og dermed forhindre malware og virus i at få adgang til netværket.

Indbygget brugergodkendelse

Du kan vælge, at brugerne skal logge på med PIN/PIC-, LDAP- eller Kerberos-godkendelse, så du får bedre sikkerhed uden ekstra omkostninger. Du kan også integrere brugeradgangskrav med Active Directory.

Rollebaserede adgangsrettigheder

HP Access Control Rights Management gør det muligt at øge sikkerheden og reducere omkostningerne ved at bruge printerens indbyggede funktioner til styring af adgangsrettigheder. Du kan bruge rollebaseret adgangskontrol til at give de enkelte brugere – eller endda hele afdelinger – forskellige rettigheder, afhængigt af deres behov. Du kan for eksempel bestemme, hvem der skal have tilladelse til at faxe, scanne dokumenter til e-mail eller scanne dokumenter til fax.

Avancerede sikkerhedsfunktioner

Avanceret godkendelse og sporing

De avancerede godkendelsesfunktioner (f.eks. adgangskoder, adgangschips, chipkort, biometribaseret adgang) og sporingsfunktioner giver endnu bedre styring af sikkerheden.

- *HP Access Control Secure Authentication* giver dig fuld kontrol, forbedrer sikkerheden og er med til at reducere omkostningerne. Du kan vælge mellem en bred vifte af løsninger og muligheder, herunder berøringsfri godkendelse ved hjælp af mobile enheder med nærfeltkommunikation.
- *HP Access Control Job Accounting* gør det muligt at spore og indsamle data samt at analysere og indrapportere resultaterne. Brug data-mining til at analysere udskrivningsomkostninger, motivere medarbejderne til at udskrive smartere og give it-afdelingen de nødvendige oplysninger til at lægge en mere effektiv strategi for printerflåden.



Flere oplysninger

HP Access Control
hp.com/go/hpac

HP JetAdvantage Connect
hp.com/go/JetAdvantageConnect

HP Capture and Route
hp.com/go/hpcr

Mobilenheder er inkluderet i netværksadgang

Du kan inkludere mobilenhederne i den samle sikkerhedspolitik for adgang til udskrivningsfaciliteter. HP tilbyder serverbaserede løsninger til sikker pull-udskrivning samt avancerede styrings- og rapporteringsmuligheder.

- *HP JetAdvantage Connect* tilbyder intuitiv, driftssikker mobiludskrivning beregnet til virksomheder. Spar tid og penge ved at genbruge de eksisterende it-netværkssværktøjer og -politikker til styring af mobiludskrivning.¹¹ Brugere kan udskrive i sikkerhed fra en lang række smartphones og tablets – når de vil, og hvornår de vil – ligeså nemt som på en pc.
- *HP Access Control* giver mulighed for styring af mobiludskrivning. Systemet bruger den eksisterende e-mailinfrastruktur, så mobilbrugere kan sende udskriftsjob med e-mail direkte til udskriftskøen og derefter hente udskriften på en hvilken som helst printer eller MFP-enhed, der understøtter denne funktion. Beskyt dine netværksprintere med funktioner til sikker godkendelse, herunder Mobile Release.

Stop dataudslip, inden de opstår

HP-løsninger hjælper med at beskytte mod tab af data. Med *HP Capture and Route Data Loss* kan du forhindre, at følsomme oplysninger scannes eller faxes. Med *HP Access Control Print Data Loss Prevention* kan du forhindre, at følsomme dokumenter udskrives. Der kan sættes sporing på de vigtigste data, så eventuelle dataudslip forhindres uden at fjerne ressourcer fra andre vigtige områder i virksomheden. Få smarte sikkerhedsadvarsler baseret på betingelser, som du selv vælger.

Forsyn printerne med digitale certifikater

Sikkerheden i printermiljøet forbedres væsentligt, når netværksprintere og MFP'erne forsynes med digitale certifikater. Spar tid ved at bruge HP JetAdvantage Security Manager til automatisk at installere og forny certifikater.⁹



Beskyt dine dokumenter

Brug smarte hardware- og softwareløsninger sammen med din it-sikkerhedspolitik for at opnå den bedste beskyttelse af de følsomme oplysninger i de udskrevne dokumenter.⁶

Grundlæggende sikkerhedsfunktioner

Styring af adgang til fortrykte formularer

Du kan udstyre dine printere og MFP'er med aflåste papirbakker for at forhindre evt. tyveri af særlige medier til udskrivning af checks, recepter og andre følsomme dokumenter.

Brug en valgfri pinkode eller pull-udskrivning for at beskytte følsomme dokumenter

Brugerne kan vælge at forsyne deres udskriftsjob med en pinkode eller bruge pull-udskrivning og dermed mindske behovet for brug af personlige printere og eliminere risikoen for, at udskrifterne falder i de forkerte hænder. Disse sikkerhedsforanstaltninger mindsker også problemet med uafhængte udskrifter, hvilket kan reducere omkostningerne og mængden af affald.

Pinkodeudskrivning fungerer ved, at brugerne kan forsyne fortrolige udskriftsjob med en pinkode, som skal angives på printeren, før dokumenterne udskrives.

Ved pull-udskrivning opbevares udskriftsjob i skyen eller på brugerens pc. Brugerne skal angive deres brugernavn og adgangskode på den enhed, de vil udskrive på. HP tilbyder to cloud-baserede løsninger til pull-udskrivning:

- *HP JetAdvantage Secure Print* er en prismæssigt overkommelig løsning designet til små og mellemstore virksomheder. Ved denne løsning opbevares udskriftsjobbet i skyen eller på brugerens computer. Løsningen er nem at konfigurere og bruge, gør det muligt at starte udskriftsjob fra mobilenheder og kan bruges med printere fra flere producenter.¹²
- *HP JetAdvantage Private Print* er HP's gratis, cloud-baserede løsning, der tilbyder alle fordelene ved pull-udskrivning på en nem og overskuelig måde. Det er nemt at konfigurere og kræver hverken servere, installation eller vedligeholdelse.¹³

Avancerede sikkerhedsfunktioner

Brug pull-udskrivning på alle udskriftsjob

HP Access Control Secure Pull Printing hjælper med at beskytte fortrolige oplysninger og forbedrer printerens sikkerhed og effektivitet. Denne robuste, serverbaserede løsning tilbyder flere typer godkendelse, herunder godkendelse vha. id-kort samt avancerede sikkerheds- og styringsfunktioner designet til større organisationer.

Brug MICR, vandmærker og andre funktioner, der forhindrer kopiering og uønskede ændringer

HP's og TROY's løsninger til forhindring af forfalskninger omfatter særlig printertoner, der pletter papiret, hvis det udsættes for kemisk manipulation. De giver også mulighed for brug af forskellige datavandmærker på udskrifterne samt brug af maskinelt aflæselige koder, der kan bruges til sporing og kontrol af de enkelte dokumenter. Nogle MFP-enheder har indbyggede funktioner til bekæmpelse af forfalskninger, herunder brugerdefinerede underskrifter, firmalogoer og sikre skrifttyper til brug på følsomme dokumenter som recepter, fødselsattester og udskrifter af retsbøger.



Flere oplysninger

HP JetAdvantage Secure Print
hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Private Print
hp.com/go/JetAdvantagePrivatePrint

HP Access Control
hp.com/go/hpac

HP- og TROY-dokumentbeskyttelse
hp.com/go/HPandTROY



Overvågning og styring af printermiljøet



Flere oplysninger

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Løsninger til sikkerhedsovervågning og -styring kan hjælpe med at udpege svagheder og etablere en solid, politikbaseret sikkerhedsstrategi for beskyttelse af data, reduktion af sikkerhedsrisici og sikring af overholdelse af gældende krav og regler.⁶ Luk sikkerhedshullerne, og undgå de dyre bøder.

Grundlæggende sikkerhedsfunktioner

Opdater enhederne med nyeste firmware og operativsystem

Brug HP Web Jetadmin¹⁴ til at overføre firmwareopdateringer til flåden og sikre, at alle enheder er opdateret og beskyttet med de seneste sikkerhedsfunktioner.

Hold øje med printerens logfiler

HP-enheder sender meddelelser om hændelser på printerens til en syslog-server, så it-personale kan gribe ind og løse evt. problemer, så snart de opstår.

Gennemgå og optimer enhedsindstillinger

Du kan administrere de grundlæggende sikkerhedsindstillinger for printerne i hele flåden ved hjælp af *HP Print Manageability Integration Kit* (MIK), som er et plugin til Microsoft® System Center Configuration Manager (SCCM). Microsoft SCCM er en populær løsning til fjernadministration, planlægning, implementering, konfiguration og overvågning af endpoint-klienter. HP Print MIK kan hjælpe med at opdage, undersøge og optimere de femten vigtigste sikkerhedsindstillinger og vise resultaterne i en overskuelig rapport.

Hvis du er på udkig efter avanceret sikkerhedsstyring af printerflåden, anbefaler vi *HP JetAdvantage Security Manager*.⁹ Denne omkostningseffektive løsning er designet til at etablere en sikkerhedspolitik på flådeniveau, automatisere optimeringen af enhedsindstillingerne samt til at installere og forny entydige certifikater og producere rapporter til brug for dokumentation af efterlevelse.



Flere oplysninger

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Avancerede sikkerhedsfunktioner

Brug SIEM-software til at opdage og dokumentere trusler

Hændelsesdata, der rapporteres af HP FutureSmart-enheder, kan sendes til hændelsesrapporteringssystemer som ArcSight, Splunk og SIEMonster, hvor hændelser kan overvåges i realtid. Det gør det nemt for it-personale at se printerne som en del af det overordnede it-miljø samt opdage og reagere på evt. sikkerhedsadvarsler, der opstår i printerne, med det samme.

Automatisk konfiguration af nye printere, der sluttes til netværket

Funktionen Instant-on Security, der findes i HP JetAdvantage Security Manager, konfigurerer automatisk nye enheder, så snart de føjes til netværket, eller når de genstarter.

Rapportering til brug for dokumentation af printerflådens sikkerhed

Brug HP JetAdvantage Security Manager til at fremskaffe faste beviser for efterlevelse af krav og regler for printermiljøet og beskyttelse af kunders data.

Det kan skade forretningen, hvis krav og regler ikke efterleves

Manglende eller mangelfuld beskyttelse af endpoint-klienter skaber god grobund for cyberkriminalitet. I kampen mod den voksende trussel er myndigheder overalt i verden ved at indføre strikse sikkerhedsregler, som kræver, at virksomheder og organisationer skal beskytte kunders data bedre.

Virksomheder og organisationer, der ikke overholder disse regler, risikerer store omkostninger pga. bøder, tab af

fortjeneste, dårligt omdømme og retssager.

Derfor er det yderst vigtigt at vælge udstyr og løsninger som HP Enterprise-printere og HP JetAdvantage Security Manager, der kan hjælpe med at imødekomme de lovbestemte krav og samtidig beskytte virksomheden mod sikkerhedstrusler.



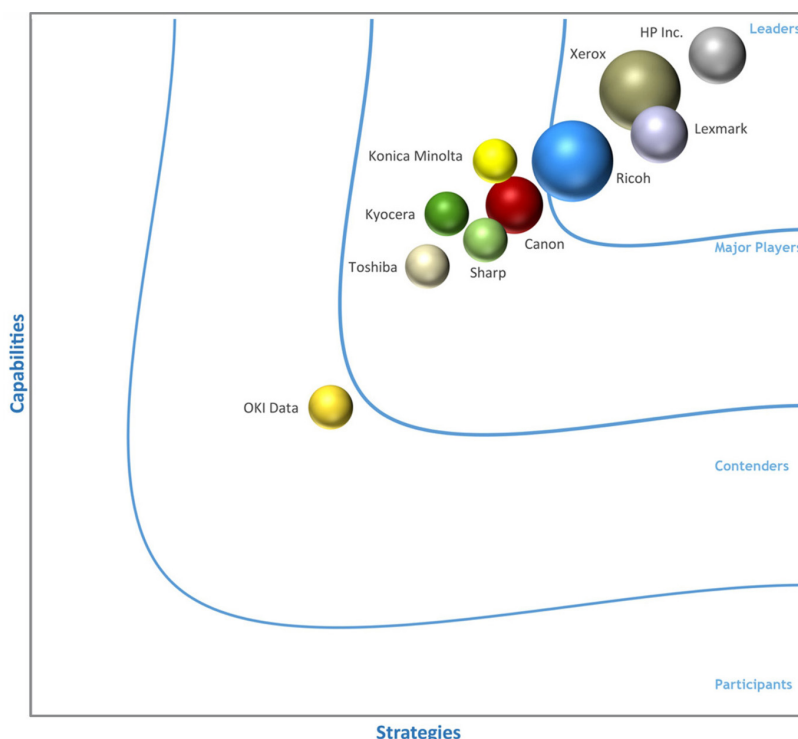
Du får den nødvendige hjælp

Du behøver ikke selv at stå for hele beskyttelsen. Et konsulentteam står parat til at vise dig, hvordan du forbedrer sikkerheden for dine data, udstyr og dokumenter.

Sammen med vores printersikkerhedseksperter kan du hurtigt finde eventuelle fejl og mangler i printersikkerheden. Vi kan hjælpe med at skabe en omfattende printersikkerhedspolitik, som passer til dine forretningsbehov, og som er baseret på den sikkerhedspraksis, der gælder i branchen, og vi kan sammen lave en plan for, hvordan du bedst forbedrer sikkerheden i netop dit it-miljø.

Anerkendt som førende inden for branchen

HP anerkendes som førende i den første IDC MarketScape-rapport med titlen: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment. (Rapporten finder du [her](#)). Rapporten siger bl.a. "HP Inc.'s tilgang til sikkerhed tager højde for hele infrastrukturen med udskrivning og dokumenter, idet de starter med at låse enheden og udvider det til alle aspekter af enhedsbrug og beskyttelse af indhold." Den viste graf er fra IDC 2017 Vendor Assessment.¹⁵



IDC MarketScapes leverandøranalysemodel er beregnet til at give et overblik over de konkurrencemæssige forhold blandt ICT-leverandører på et givet marked. Researchmetodikken benytter en streng scoremetodik baseret på både kvalitative og kvantitative kriterier, der resulterer i en enkelt grafisk illustration af hver enkelt leverandørs placering på et givet marked. Mulighedsscoren måler leverandørens produkt, markeds lancering og forretningsførelse på kort sigt. Strategiscoren vurderer forholdet mellem leverandørstrategier og kundekrav set over 3-5 år. Leverandørens markedsandel er repræsenteret ved størrelsen af ikonerne.¹⁵

Kom godt i gang

Henvend dig til en salgsrepræsentant for at få flere oplysninger om HP's sikkerhedsfunktioner, -løsninger og -tjenester, som kan hjælpe dig med at opnå bedre beskyttelse, så du får færre bekymringer.

Få flere oplysninger
hp.com/go/printsecurity

¹ Udsagnet om "verdens sikreste printere" er baseret på HPs undersøgelse af sikkerhedsfunktioner i konkurrerende printere i samme klasse i 2017. Kun HP tilbyder en kombination af sikkerhedsfunktioner, der kontrollerer for at registrere og automatisk stoppe et angreb, og derefter autovalidere softwareintegriteten ved genstart. Her finder du en liste over printere: hp.com/go/PrintersThatProtect. Flere oplysninger: 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 Spiceworks-undersøgelse blandt 309 it-beslutningstagere i Nordamerika, EMEA og APAC på vegne af HP, november 2016

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

⁶ Løsningerne fås muligvis ikke i alle HP-enheder; Løsningerne kræver muligvis ekstra køb.

⁷ HP's mest avancerede integrerede sikkerhedsfunktioner fås på enheder i HP Enterprise-klassen med FutureSmart-firmware 4.5 eller nyere og er baseret på HP's undersøgelse fra 2017 af integrerede sikkerhedsfunktioner i konkurrerende printere i samme klasse. Det er kun HP, der tilbyder en kombination af sikkerhedsfunktioner til integritetskontrol helt ned til BIOS-niveau med selvreparerende egenskaber. Du kan finde en liste over kompatible produkter på hp.com/go/PrintersThatProtect. Du kan finde flere oplysninger på hp.com/go/printersecurityclaims.

⁸ Udvalgte HP LaserJet Pro- og PageWide Pro-modeller har indbyggede funktioner, som kan opdage og stoppe et angreb. Du kan få flere oplysninger på hp.com/go/PrintersThatProtect.

⁹ HP JetAdvantage Security Manager skal købes separat. Du kan få flere oplysninger på hp.com/go/securitymanager.

¹⁰ Der skal opgives en ekstra adgangskode, når dataene sendes til et adgangskodebeskyttet datalager.

¹¹ HP JetAdvantage Connect fungerer med førende mobilenheder. Der skal installeres et plugin på mobilenheder med Android™-, Google Chrome™- og Microsoft®-operativsystemer. Du finder flere oplysninger og en liste over understøttede operativsystemer på hp.com/go/JetAdvantageConnect.

¹² HP JetAdvantage Secure Print: Pull-udskrivning fungerer med alle netværksforbundne printere eller MFP'er. Der fås godkendelse på enheden til mange HP LaserJet-, PageWide- og OfficeJet Pro-enheder og til udvalgte ikke-HP-enheder. Nogle enheder kræver måske en firmwareopgradering. Der kræves internetforbindelse til cloud-lagring og hentning af udskrivningsjob. Afsendelse af udskrivningsjob fra en mobilenhed kræver netværkstilslutning og QR-kode. Der findes flere oplysninger samt en liste over understøttede printere og MFP'er på hp.com/go/JetAdvantageSecurePrint.

¹³ HP JetAdvantage Private Print kan anvendes gratis og kræver, at printeren er tilsluttet internettet, og at webtjenester er aktiveret. Fås ikke i alle lande. Du kan få flere oplysninger på hp.com/go/JetAdvantagePrivatePrint.

¹⁴ HP Web Jetadmin er gratis og kan downloades på hp.com/go/webjetadmin.

¹⁵ Baseret på IDC-gennemgang af kopileverandører og opfattelsen af HP's ledelse: "HP har en fordel med sine stærke it-tjenester og sine kompetencer ... der sikrer en omfattende og integreret sikkerhedsstrategi på tværs af hele it-infrastrukturen." KILDE: [IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment](#), af Allison Correia og Robert Palmer, oktober 2017, IDC Doc #US41988517.

Tilmeld dig for at få opdateringer

hp.com/go/getupdated



Del med kolleger

© Copyright 2014-2018 HP Development Company, L.P. Oplysningerne i dette dokument kan ændres uden varsel. De eneste garantier for HP's produkter og tjenesteydelser findes i de udtrykkelige garantierklæringer, der følger med de pågældende produkter og tjenester. Ingen af oplysningerne heri må tolkes som en yderligere garanti. HP er ikke ansvarlig for tekniske eller redaktionelle fejl eller udeladelser heri.

Android og Google Chrome er varemærker tilhørende Google Inc. Microsoft er et amerikansk registreret varemærke tilhørende Microsoft-koncernen.

4AA3-1295DAE, januar 2018, rev. 11

