



Forsvar nettverket ditt med verdens sikreste skriveresystem¹

94 %

av finansbedrifter sier at kopimaskin-/skriveresikkerhet er viktig eller veldig viktig²



61 %

av organisasjoner rapporterte minst ett utskriftsrelatert brudd i løpet av det siste året³



43 %

av selskapene overser skrivere i sine praksiser for endepunktsikkerhet⁴





Bare 18 % av selskaper overvåker skrivere mot trusler.⁴ Hva med ditt?

Gjenkjenn skjult risiko

IT-avdelingen får stadig i oppgave å beskytte konfidensiell informasjon, inkludert medarbeideridentiteter og kundedata, på flere enheter og i flere miljøer. Selv om mange IT-avdelinger tar i bruk strenge sikkerhetstiltak på individuelle datamaskiner og i nettverket, blir ofte utskrifts- og bildeenheter oversett og eksponert. Når det finnes usikrede enheter, kan hele nettverket utsettes for et nettsikkerhetsangrep.

Forstå potensielle kostnader

Bare ett sikkerhetsbrudd alene kan potensielt bli svært kostbart. Hvis privat informasjon settes i fare på grunn av usikker utskrift og bildebehandling, kan følgene omfatte identitetstyveri, stjålet konkurranseinformasjon, et svekket merkevareimage og -rykte og rettsvister. Dessuten kan manglende regulatorisk og juridisk samsvar føre til kraftige bøter.

HP kan hjelpe

Forsvar nettverket ditt med verdens sikreste utskrift.¹ HP-skrivere er alltid på vakt, og oppdager og stanser kontinuerlig trusler samtidig som de tilpasser seg nye. HP kan hjelpe deg med å automatisere enhets-, data- og dokumentbeskyttelse med en bred portefølje av løsninger. Utskriftssikkerhetseksperter våre kan hjelpe deg med å utvikle og anvende en komplett sikkerhetsstrategi for bildebehandling og utskrift.

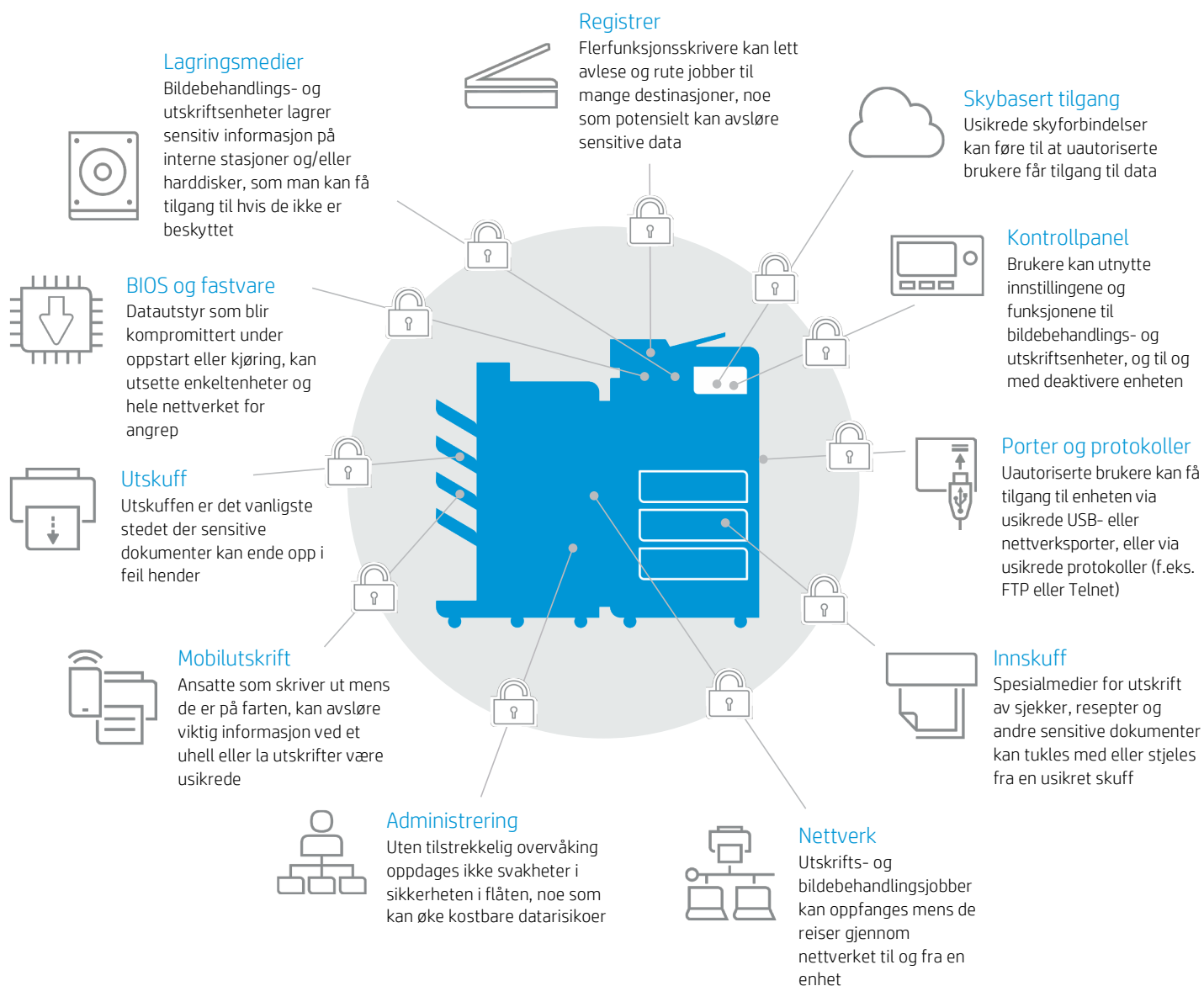
«Som et resultat av deres langsiktige investering i skriftersikkerhet, har HP det bredeste og dypeste utvalget av sikkerhetsløsninger og -tjenester på markedet.»

– Quocirca, januar 2017⁵

Forsvar enheter, data og dokumenter

Kritiske hull i sikkerheten kan forekomme på flere steder i bildebehandlings- og utskriftsmiljøet ditt. Så snart du forstår disse sårbarhetene, kan du enkelt redusere risikoen.

Sårbarheter ved bildebehandling og utskrift





Beskytt enheten



Finn ut mer

HP Custom gjenvinningstjenester
hp.com/go/businessrecycling

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

HP-skrivere er laget for å jobbe sammen med sikkerhetsovervåkings- og administrasjonsløsninger for å bidra til å forminske risiko, forbedre samsvar og beskytte nettverket ditt fra ende til ende. (Ikke alle funksjoner og løsninger er tilgjengelig på alle HP-enheter.⁶⁾)

Grunnleggende sikkerhetspraksiser

Kryptert lagring med sikker sletting

All sensitiv informasjon lagret på den interne stasjonen eller harddisken, er potensielt sårbar for tyveri. Mange HP-enheter kommer med innebygd kryptering for å beskytte data. Når lagrede data ikke lenger behøves, kan du bruke innebygde enhetsmuligheter til sikker overskriving og trygg fjerning av sensitiv informasjon.

Sikker avhending

HP Custom gjenvinningstjenester kan sørge for at data elimineres fra harddisker før gamle produkter gjenvinnes på en ansvarlig måte.

Sikker tilgang til skriverreparasjon

Å kjenne til skrivevedlikeholdsleverandørers sikkerhetspraksiser vil bidra til å beskytte sensitive data. Velg *HP Secure Managed Print Services (MPS)* eller HP-partnere for eksperthjelp.

Deaktiver ubrukte porter og protokoller

Reduser angrepsflaten gjennom passende enhetskonfigurasjon. Deaktiver fysiske porter og usikre protokoller (som FTP eller Telnet) for å hindre uautorisert tilgang eller bruk.

Administratortilgangskontroll for enhet

Angi administratorpassord slik at kun IT-personale eller annet autorisert personell kan sette opp og konfigurere innstillinger.

Hvitelisting av fastvarekode

Se neste side for informasjon om hvordan whitelisting kan beskytte flåten din mot skadelig programvare.

Avanserte sikkerhetspraksiser

Common Criteria Certification

HP-bedriftsskrivere er sertifiserte som samsvarende med internasjonalt anerkjente sikkerhetsstandarter, som Common Criteria Certification (CCC) og FIPS 140. Sørg for at enhetens fastwareoppdateringer kodesigner for å bekrefte ektheten av og integriteten til koden og for å opprettholde samsvar.



Finn ut mer

Innebygde skriftersikkerhetsfunksjoner:

- HP Sure Start (BIOS-integritet)
- Hvitelisting av fastvarekode
- Run-time intrusion detection
- HP Connection Inspector

hp.com/go/PrintersThatProtect

HP JetAdvantage Security Manager:

hp.com/go/securitymanager

Utskriftssikkerhetsfunksjoner oppdager og stopper automatisk angrep

HP-bedriftsskrivere inkluderer sikkerhetsfunksjoner som bidrar til å beskytte dem mot å bli et inngangspunkt for angrep i nettverket ditt. Kun HP-utskriftssikkerhet kan tilby sanntidsoppdagelse, automatisert overvåking og innebygd programvarevalidering for å stoppe trusler når de starter.⁷

HP-bedriftsskrivere, fra Pro⁸ til Enterprise,⁷ er alltid på vakt, og oppdager og stopper kontinuerlig trusler under alle faser av driften:

- **Under oppstart.** Oppstartskoden (for Pro-enheter) eller BIOS (for Enterprise-enheter) er et sett av instruksjoner som brukes for å laste kritiske maskinvarekomponenter og initiere fastvare. Integriteten til koden valideres ved hver oppstartssyklus og bidrar til å beskytte enheten din mot angrep.
- **Ved lasting av fastvare.** Hvitelisting sjekker automatisk fastvare under oppstart for å fastslå om den er ekte, god kode som er digitalt signert av HP. Hvis uregelmessigheter oppdages, startes enheten på nytt i en trygg, frakoblet tilstand og varsler IT-avdelingen.
- **Under kjøretid.** HP-innebygde funksjoner bidrar til å beskytte enhetsminne mens enheter er på og koblet til nettverket, akkurat når de fleste angrep skjer. Enheten slår seg av i tilfelle et angrep.

HP Enterprise-enheter kan reparere seg selv

I tillegg til å kunne oppdage og stoppe trusler, reparerer HP Enterprise-skrivere seg selv automatisk etter angrep, slik at IT-avdelingen ikke behøver å blande seg inn.⁷ Disse funksjonene utløser automatisk en omstart i tilfelle et angrep eller et avvik. Administratorer kan varsles via sikkerhetsinformasjons- og hendelseshåndteringsverktøy (SIEM) som ArcSight, Splunk og SIEMonster.

- *HP Sure Start* er bransjens eneste selvreparerende BIOS.⁷ Hvis BIOS settes i fare, starter HP Sure Start på nytt med en sikker "gyllen kopi" av BIOS.
- *Run-time intrusion detection* overvåker komplekse fastvare- og minneoperasjoner, stopper automatisk inntrengningen og starter på nytt i tilfelle et angrep.
- HP Connection Inspector evaluerer utgående nettverkstilkoblinger for å fastslå hva som er normalt, stanser mistenkelige forespørsler og hindrer skadelig programvare ved automatisk å utløse en omstart.

Med investeringsbeskyttelsen fra oppgraderbar HP Future Smart-fastvare kan du legge til hvitelisting, run-time intrusion detection og HP Connection Inspector til mange eksisterende HP Enterprise-skrivere.⁷

HP JetAdvantage Security Manager fullfører kontrollsyklusen

Etter en omstart inntreffer eller når en ny enhet legges til nettverket vurderer *HP JetAdvantage Security Manager* automatisk og, om nødvendig, retter på enhetens sikkerhetsinnstillinger for å samsvare med forhånds etablerte selskapsretningslinjer.⁹ IT-avdelingen behøver ikke å gripe inn.

Hvordan fungerer det?

De innebygde sikkerhetsfunksjonene håndterer fire hovedtrinn i syklusen til en HP-enhet.

HP Enterprise-enheter kan starte på nytt og reparere seg selv hvis de angripes.

HP JetAdvantage Security Manager fullfører kontrollsyklusen.

Fire. Uavbrutt overvåking

Beskytter operasjoner og stopper angrep mens enheten kjører.

Inspiserer utgående nettverkstilkoblinger for å stoppe mistenkelige forespørsler (kun Enterprise).

Tre. Sjekk innstillinger

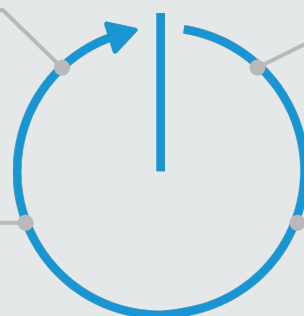
Etter ny oppstart kontrollerer og fikser HP Jet Advantage Security Manager sikkerhetsinnstillinger for eventuell berørt enhet.

En. Sjekk BIOS-/oppstartskode

Forhindrer utøvelse av ondsinnet kode under oppstart ved kun å tillate lasting av HP-signert, ekte kode.

To. Sjekk fastvare

Tillater kun at ekte, godkjent fastvare som er digitalt signert av HP, lastes.





Beskytt dataene

Dataene dine trenger konstant beskyttelse, både lagret og i transit. Her er noen viktige trinn for å bidra til å sikre trygge ankomster og bruk.⁶

Grunnleggende sikkerhetspraksiser

802.1x- eller IPsec-nettverksstandarder

Bruk krypterte nettverksstandarder for å beskytte data som reiser over nettverket mellom enheten og administrasjonsverktøyene som *HP Web Jetadmin* eller *HP Embedded Web Server*.

Krypter data i transit

Beskytt utskriftsjobber som reiser til enheten med kryptering som Internet Print Protocol over TLS (IPPS). *HP Universal Print Driver Secure Encrypted Print* leverer ekte symmetrisk AES256-utskriftsjobb-kryptering og dekryptering fra klienten til siden basert på et brukerdefinert passord som bruker FIPS 140-validerede kryptografiske biblioteker fra Microsoft®.

Under skanning kan *HP JetAdvantage Workflow Solutions* bidra til å beskytte sensitiv informasjon samtidig som effektiviteten økes. HP Capture and Route integreres for eksempel sømløst med HP Access Control for forbedret sikkerhet, med praktisk enkeltgodkjenning og mulighet for å overvåke innhold for informasjonsstyring.¹⁰

Krypter data i hvile

Beskytt sensitiv forretningsinformasjon lagret på harddisken, med innebygd kryptering. For et ekstra sikkerhetsnivå kan HP Trusted Platform Module (TPM)-tilbehøret legges til enheten for å styrke beskyttelse av kryptert informasjon og data ved automatisk å forsegle enhetens krypteringsnøkler til TPM. Den gir sikker enhetsidentitet ved å generere og beskytte private nøkler for sertifikater.

Brannmurbeskyttelse

Forhindre at skadelig programvare og virus kommer inn i nettverket ditt ved å begrense skrivertilgang til databehandlingsenheter i nettverk.

Innebygd brukergodkjenning

Reduser kostnader og sikkerhetsrisiko ved å kreve at brukere logger på med PIN/PIC-, LDAP- eller Kerberos-godkjenning. Du kan også integrere disse med Active Directory.

Rollebaserte tilgangskontroller

HP Access Control Rights Management bidrar til å redusere kostnader og sikkerhetsrisiko gjennom skriverfunksjonsbegrensninger. Rollebaserte tilgangskontroller gjør at du kan tilordne forskjellige funksjoner til forskjellige brukere, eller til og med hele avdelinger, avhengig av behovet. Du kan for eksempel begrense hvem som kan faks, skanne til e-post eller skanne til faks.



Finn ut mer

HP Web Jetadmin
hp.com/go/wja

HP Universal Print Driver med sikker kryptert utskrift
hp.com/go/upd

HP JetAdvantage-arbeidsflytløsninger
hp.com/go/documentmanagement

HP Access Control
hp.com/go/hpac

Avanserte sikkerhetspraksiser



Finn ut mer

HP Access Control
hp.com/go/hpac

HP JetAdvantage Connect
hp.com/go/JetAdvantageConnect

HP Capture and Route
hp.com/go/hpcr

Avansert godkjenning og sporing

Distribuer avansert godkjenning (som passord, nærhetskort, smartkort eller biometri) og sporingsløsninger for ekstra sikkerhet og kontroll.

- *HP Access Control Secure Authentication* gjenoppretter kontroll, forsterker sikkerhet og reduserer kostnader. Få et mangfold av avanserte kontroller og alternativer, inkludert berøring for å godkjenne med NFC-aktiverte mobilenheter.
- *HP Access Control Job Accounting* hjelper deg med nøyaktig sporing og innsamling av data, analyse av resultatene og deretter oppretting og sending av rapporter. Anvend utvunnede data til å fordele utskriftskostnader, motivere medarbeidere til å skrive ut smartere og gi IT-avdelingen nødvendig informasjon for å forbedre prognoser for hele flåten.

Mobile enheter inkludert i nettverkstilgang

Ta i bruk mobilenhetene dine som del av den samlede utskriftssikkerhetspolicyen for skrivertilgangskontroll. HP tilbyr serverbaserte løsninger som leverer sikker pull-utskrift, så vel som avanserte administrasjons- og rapporteringsmuligheter.

- *HP JetAdvantage Connect* leverer intuitiv og pålitelig mobil utskrift laget for bedrifter. Bidra til å spare tid og penger gjennom sømløs påvirkning av eksisterende IT-nettverksverktøy og policyer for å administrere mobil utskrift.¹¹ Brukere kan sikkert skrive ut fra en rekke smarttelefoner og nettbrett, hvor og når de måtte trenge det, like enkelt som utskrift fra en PC.
- *HP Access Control* inkluderer muligheter for å administrere mobil utskrift. Det benytter eksisterende e-postinfrastruktur, lar mobile brukere sende e-post med en utskriftsjobb til utskriftskøen og deretter dra den fra en løsningsaktivert skriver eller MFP. Beskytt nettverksutskriftsenheter med sikre godkjenningsfunksjoner, inkludert Mobile Release.

Stopp datalekkasjer før de skjer

HP-løsninger gir muligheter for å beskytte mot datatap. Med *HP Capture and Route Data Loss*-forebygging, kan du forhindre at sensitiv informasjon blir skannet eller fakset. *HP Access Control utskriftsdatatap*-forebygging kan forhindre at sensitive dokumenter blir skrevet ut. Spor de viktigste dataene for å avskrekke og forhindre brudd, uten å gjøre arbeidsflyten tregere. Få smarte sikkerhetsvarsler basert på vilkår du velger.

Anvend digitale sertifikater på skrivere

Forbedre sikkerheten til utskriftsmiljøet ditt ved å anvende digitale sertifikater på nettverksskrivere og MFP-er. Du sparer tid ved å bruke HP JetAdvantage Security Manager til å installere og fornye sertifikatene automatisk.⁹



Beskytt dokumentet



Finn ut mer

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

Integrer smarte maskinvare- og programvareløsninger med den overordnede IT-sikkerhetsplanen for å beskytte den sensitive informasjonen i dokumentene du skriver ut.⁶

Grunnleggende sikkerhetspraksiser

Kontroller tilgang til forhåndsstrykte skjemaer

Utstyr skriverne og MFP-ene dine med låsbare innskuffer for å bidra til å forhindre tyveri av spesialpapir brukt til å skrive ut sjekker, resepter eller andre sensitive dokumenter.

Bruk valgfri PIN- eller pull-utskrift for å beskytte sensitive dokumenter

Brukere kan velge PIN eller pull-utskrift, og redusere avhengighet av personlige skrivere så vel som risikoen for at utskriftsjobber faller i gale hender. Disse sikkerhetstiltakene reduserer også utskrift av ukjente, noe som kan kutte kostnader og søppel.

PIN-utskrift: Når brukere sender konfidensielle utskriftsjobber, tilordner de et PIN som de må skrive inn på enheten for å utløse jobben.

Pull-utskrift lagrer utskriftsjobber i skyen eller på brukerens PC. Brukergodkjenning på det valgte utskriftsstedet henter og og skriver ut jobbene. HP tilbyr to skybaserte pull-utskriftsløsninger:

- *HP JetAdvantage Secure Print* er en rimelig løsning designet for SMB som lagrer utskriftsjobber i skyen eller på brukerens datamaskin. Det er enkelt å konfigurere og bruke, lar brukere utløse jobber fra en mobil enhet og støtter enheter fra flere leverandører.¹²
- *HP JetAdvantage Private Print* er HPs kostnadsfrie skybaserte løsning som gir fordelene av pull-utskrift uten kompleksiteten. Den er enkel å konfigurere og krever ikke server, installasjon eller vedlikehold.¹³

Avanserte sikkerhetspraksiser

Krev pull-utskrift for alle utskriftsjobber

HP Access Control Secure Pull Printing bidrar til å beskytte konfidensiell informasjon, forbedrer enhetssikkerhet og øker effektivitet. Denne robuste serverbaserte løsningen gir flere godkjenningsmåter, inkludert skiltutløsning, så vel som sikkerhets- og administrasjonsfunksjoner på bedriftsnivå.

Bruk MICR, vannmerker eller andre funksjoner til å forhindre kopiering eller endring

HP og TROY forfalskningsavskrekkende løsninger inkluderer å bruke sikkerhetsstener som lager flekker hvis papiret utsettes for kjemisk manipulering, å legge til ulike datavannmerker på trykte sider og å inkorporere maskinlesbare koder som sporer og kontrollerer individuelle dokumenter. MFP-er kan legge inn funksjoner som forhindrer svindel, inkludert tilpassede signaturer, selskapslogoer og sikkerhetsskrifter, i sensitiv trykt dokumentasjon som resepter, fødselsattester eller avskrifter.



Overvåk og administrer utskriftsmiljøet



Finn ut mer

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Sikkerhetsovervåkings- og administrasjonsløsninger kan hjelpe deg med å identifisere sårbarheter og etablere en samlet, policybasert tilnærming til å beskytte data, redusere risiko og opprettholde samsvar.⁶ Hindre beskyttelseshull og unngå kostbare bøter.

Grunnleggende sikkerhetspraksiser

Oppdater enheter med den nyeste fastvaren/OS

Bruk HP Web Jetadmin¹⁴ til fastvareoppdatering over hele flåten, og sørg for at enhetene er oppdaterte med den nyeste enhetsbeskyttelsen og de nyeste sikkerhetsfunksjonene.

Gjennomgå hendelseslogger for skriftersikkerhet

HP-enheter sender skriverhendelser/-varsler til en syslog-server slik at IT-avdelingen om nødvendig kan korrigere problemer.

Vurder og rett opp enhetsinnstillinger

Administrer grunnleggende skriftersikkerhetsinnstillinger i flåten med *HP Print Manageability Integration Kit* (MIK), en plugin-modul for Microsoft® System Center Configuration Manager (SCCM). Microsoft SCCM er en mye brukt administrasjonsløsning for ekstern planlegging, distribuering, konfigurering og overvåking av endepunkter. HP Print MIK kan oppdage, vurdere og rette opp "topp 15"-sikkerhetsinnstillingene og rapportere om resultatene.

For omfattende sikkerhetsadministrasjon i flåten velger du *HP JetAdvantage Security Manager*.⁹ Denne løsningen hjelper deg med å redusere kostnader og ressurser for å etablere en sikkerhetspolicy for hele flåten, automatisere retting av enhetsinnstillinger og installere og fornye unike sertifikater samtidig som du får rapportene du trenger for å vise samsvar.



Finn ut mer

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Avanserte sikkerhetspraksiser

Distribuer SIEM-programvare for å oppdage og dokumentere trusler

Hendelsesdata fra HP FutureSmart-enheter kan sendes til hendelsesoppdagingsverktøy som ArcSight, Splunk og SIEMonster for overvåking i sanntid. IT-sikkerhet kan enkelt se skriverendepunkter som del av det bredere IT-økosystemet for å oppdage og løse skritersikkerhetsvarsler.

Konfigurer automatisk nye utskriftsenheter når de legges til i nettverket

Sikkerhetsfunksjonen Instant-on inkludert med HP JetAdvantage Security Manager, konfigurerer automatisk nye enheter når de legges til i nettverket eller etter en omstart.

Samsvarsrevisjonsrapportering av utskriftsflåtesikkerhet

Bruk HP JetAdvantage Security Manager til å lage rapporter som viser samsvar, bruk av sikkerhetspolicyer på skrivere og sikring av kundedata.

Samsvarsavvik kan skade virksomheten din

Ubeskyttede eller underbeskyttede endepunkter skaper flere muligheter for nettkriminalitet. For å bidra til å demme opp for den økende trusselen implementerer statlige organer over hele verden strenge sikkerhetsreguleringer som krever at organisasjoner beskytter kundeinformasjon på en bedre måte.

Organisasjoner som ikke overholder dette, kan få store omkostninger, inkludert bøter, tapte

forretninger, skadet rykte og gruppesøksmål.

Det er avgjørende å distribuere enheter og løsninger, som HP Enterprise-skrivere og HP JetAdvantage Security Manager, som kan hjelpe deg å oppfylle samsvarskrav og beskytte forretningsinformasjonen din mot sikkerhetstrusler.



Få hjelpen du trenger

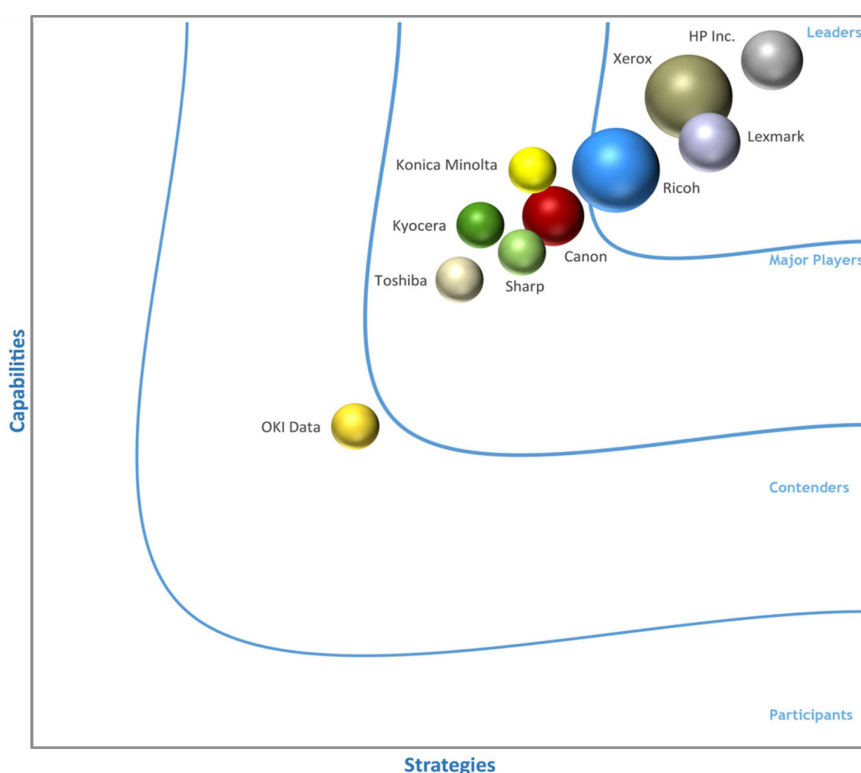
Men du trenger ikke å stå for beskyttelsen og sikkerheten på egen hånd. Et team med sikkerhetskonsulenter kan vise deg hvordan du forbedrer sikkerheten for data, enheter og dokumenter.

Samarbeid med utskriftssikkerhetsekspertene for å vurdere nåværende utskriftssikkerhetssårbarheter. Vi kan hjelpe deg med å bygge en omfattende utskriftssikkerhetspolicy basert på forretningsbehov og anbefalte fremgangsmåter, og lage en plan for å oppnå bedre sikkerhet innenfor ditt unike miljø.

Anerkjent som ledende i bransjen

HP har blitt kalt ledende i den første IDC MarketScape-rapporten om verdensomspennende sikkerhetsløsninger og Services Hardcopy 2017 Vendor Assessment. (Finn rapporten [her](#).) Ifølge rapporten "tar HP Inc.s tilnærming til sikkerhet hensyn til hele utskrifts- og dokumentinfrastrukturen, og starter med å låse ned enheten og utvide den i alle aspekter av enhetsbruk og innholdsbeskyttelse." Grafen som vises her er fra IDC 2017 Vendor Assessment.¹⁵

IDC MarketScape leverandøranalysemodell er designet for å gi en oversikt over konkurransedyktigheten til ICT-leverandører i et gitt marked. Forskningsmetodikken tar i bruk en sterk poengmetodikk basert på disse kvalitative og kvantitative kriterier som resulterer i en enkelt grafisk illustrasjon av hver leverandørs posisjon i et gitt marked. Evner-resultatet måler leverandørprodukt, gå til marked og forretningsutførelse på kort sikt. Strategi-resultat måler justering av leverandørstrategier med kundekrav i en tidsramme på 3 til 5 år. Leverandørmarkedsandel er representert av størrelsen på ikonene.¹⁵



Komme i gang

Kontakt salgsrepresentanten for å få mer informasjon om HP-sikkerhetsfunksjoner, -løsninger og -tjenester som kan få deg på vei mot større beskyttelse og trygghet.

Lær mer

hp.com/go/printsecurity

¹ Påstanden om "Sikreste utskrift" basert på en HP-vurdering av sikkerhetsfunksjoner fra 2017 for konkurransedyktige skrivere i sin klasse. Kun HP tilbyr en kombinasjon av sikkerhetsfunksjoner som kan overvåke for å automatisk registrere og stoppe angrepet, og så selvbekrefte programvarens integritet i en omstart. Du finner en liste over skriverne på: hp.com/go/PrintersThatProtect. Mer informasjon: 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-undersøkelse blant 309 IT-beslutningstakere i Nord-Amerika, EMEA og APAC, på vegne av HP, november 2016.

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

⁶ Det er ikke sikkert at alle løsninger støttes på alle HP-enheter; løsninger kan kreve tilleggskjøp.

⁷ HPs mest avanserte innebygde sikkerhetsfunksjoner er tilgjengelig på HP Enterprise-klasse enheter med FutureSmart-fastvare versjon 4.5 eller nyere, og er basert på HPs gjennomgang av 2017 om publiserte innebygde sikkerhetsfunksjoner i konkurransedyktige skrivere i samme klasse. HP er det eneste selskapet som tilbyr en kombinasjon av sikkerhetsfunksjoner for integritetskontroll, inkludert BIOS med muligheter for selvreparasjon. Du finner en liste over kompatible produkter på hp.com/go/PrintersThatProtect. Du finner mer informasjon på hp.com/go/printersecurityclaims.

⁸ Utvalgte HP LaserJet Pro- og PageWide Pro-enheter inkluderer innebygde funksjoner som kan oppdage og stoppe et angrep. Du finner mer informasjon på hp.com/go/PrintersThatProtect.

⁹ HP JetAdvantage Security Manager må kjøpes separat. Du får mer informasjon ved å gå til hp.com/go/securitymanager.

¹⁰ Et ekstra passord kreves når du sender informasjon til et passordbeskyttet sluttlager.

¹¹ HP JetAdvantage Connect fungerer med ledende mobilenheter. En engangsplugin-modul må være installert for enheter som kjører operativsystemene Android™, Google Chrome™ og Microsoft®. Du finner flere detaljer og en liste med støttede operativsystemer på hp.com/go/JetAdvantageConnect.

¹² HP JetAdvantage Secure Print: Pull-utskrift fungerer med alle nettverkstilsluttede skrivere eller MFP-er. Godkjenning på enhet er tilgjengelig for mange HP LaserJet-, PageWide- og OfficeJet Pro-enheter og utvalgte enheter som ikke er fra HP. Enkelte enheter kan kreve en fastvareoppgradering. Internett-tilkobling kreves for skybasert lagring og henting av utskriftsjobber. Utløsning av utskriftsjobber fra en mobilenhet krever nettverkstilkobling og QR-kode. Hvis du vil ha mer informasjon og en liste over støttede skrivere og MFP-er, kan du gå til hp.com/go/JetAdvantageSecurePrint.

¹³ HP JetAdvantage Private Print er kostnadsfritt, og krever at skriveren er tilkoblet Internett med netjtjenester aktivert. Ikke tilgjengelig i alle land. Lær mer på hp.com/go/JetAdvantagePrivatePrint.

¹⁴ HP Web Jetadmin kan lastes ned uten ekstra kostnad fra hp.com/go/webjetadmin.

¹⁵ Basert på IDC-gjennomgang av utskriftsleverandører og meninger om HP-lederskap: "HP har en fordel med sin sterke IT-service og -muligheter ... og fasilitering av en omfattende og integrert sikkerhetsstrategi på tvers av hele IT-infrastrukturen." KILDE: IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment, av Allison Correia og Robert Palmer, oktober 2017, IDC Doc #US41988517.

Få oppdateringer

hp.com/go/getupdated



Del med kolleger

© Copyright 2014-2018 HP Development Company, L.P. Informasjonen i dette dokumentet kan endres uten varsel. De eneste garantiene for HPs produkter og tjenester fremsettes i de uttrykkelige garantierklæringer som følger med slike produkter og tjenester. Ikke noe i dette dokumentet skal tolkes som noen form for tilleggsgaranti. HP skal ikke holdes ansvarlig for redaksjonelle feil eller utelatelser som finnes i dette dokumentet.

Android og Google Chrome er registrerte varemerker for Google Inc. Microsoft er et registrert varemerke i USA for Microsoft-konsernet.

4AA3-1295N0E, januar 2018, rev. 11

