



Skydda ert nätverk med världens säkraste utskrifter¹

94 %

av finansbolagen säger att säkerhet för skrivare och kopieringsapparater är mycket viktigt²



61 %

av företagen rapporterade minst ett dataintrång relaterat till enskilda utskrifter, under det senaste året³



43 %

av företagen ignorerar skrivare i sina säkerhetsrutiner för enheter⁴





Bara 18 % av företagen övervakar sina skrivare för att identifiera eventuella hot⁴. Hur gör ni?

Känn igen dolda risker

IT-personal får hela tiden i uppgift att skydda konfidentiell information, inklusive anställdas identiteter och kunddata, i och mellan olika enheter och miljöer. Många IT-avdelningar tillämpar rigorösa säkerhetsåtgärder för individuella datorer och nätverk, medan enheter för utskrift och bildhantering ofta förbises och förblir exponerade. När det finns osäkrade enheter kan hela nätverket bli utsatt för risk för cyberattacker.

Förstå potentiella kostnader

Ett enda säkerhetsintrång kan medföra stora kostnader. Om privat information utsätts för risk på grund av osäkra utskrifts- och bildenheter kan effekterna bli identitetsstöld, stulen företagsinformation, skadat rykte för varumärket och åtal. Om lagar och regler dessutom inte efterlevs kan det ge upphov till dryga böter.

HP hjälper er

Försva ert nätverk med världens säkraste utskrifter..¹ HPs skrivare är alltid på vakt och upptäcker och stoppar kontinuerligt hot medan de anpassar sig efter nya. HP kan hjälpa till att automatisera skydd av enheter, data och dokument med en bred uppsättning lösningar. Våra säkerhetsexperten kan hjälpa er att utveckla och implementera en genomgående säkerhetsstrategi för bildbehandling och utskrift.

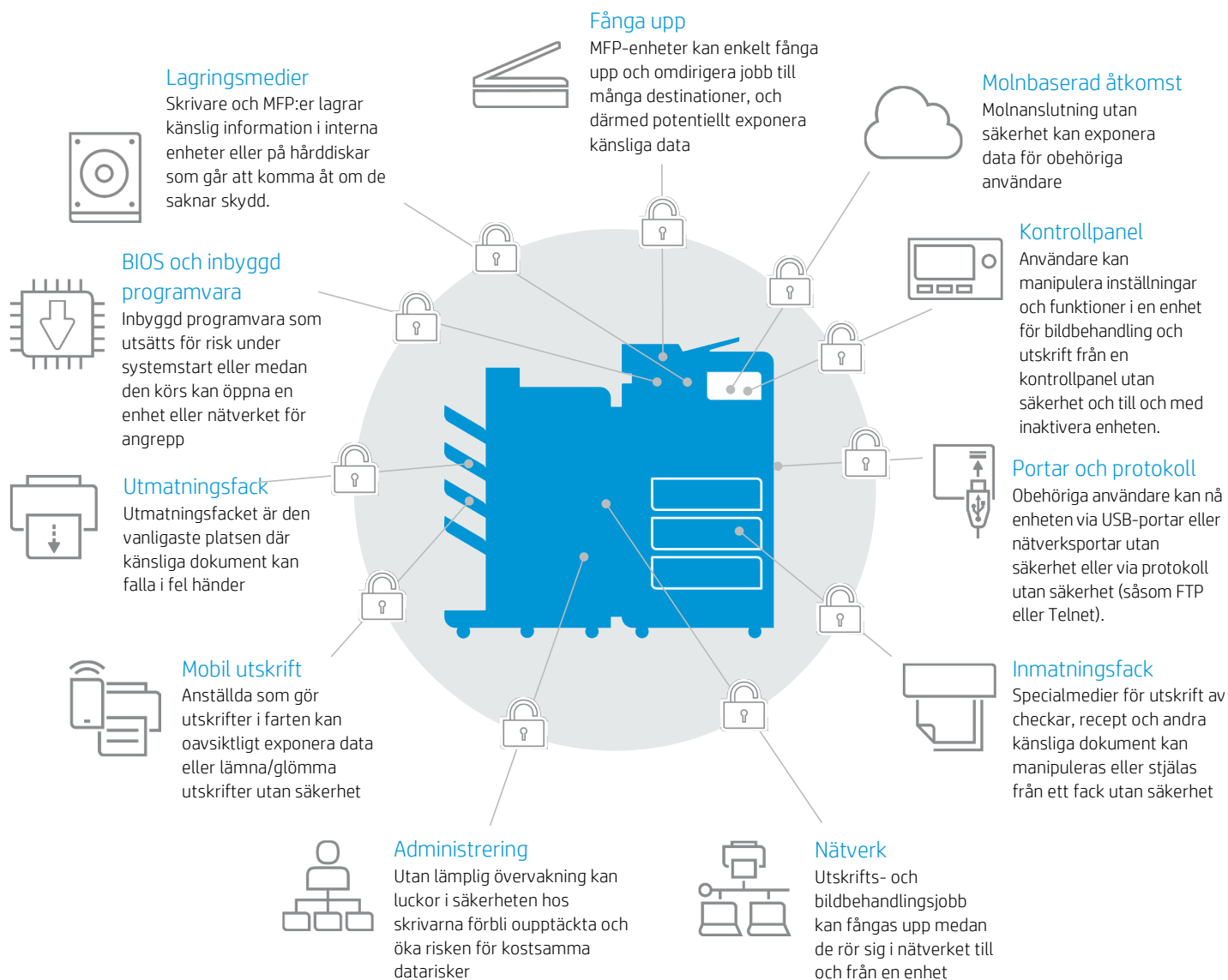
"Det är ett tecken på HPs långsiktiga investering i skrivarsäkerhet att de har den bredaste och djupaste uppsättningen lösningar och tjänster på marknaden."

– Quocirca, januari 2017⁵

Skyddar enheter, data och dokument

Kritiska luckor kan uppstå på flera platser i bildbehandlings- och utskriftsmiljön. När de sårbara punkterna har identifierats blir det lättare att minska riskerna.

Sårbara punkter vid bildbehandling och utskrift





Skydda enheten



Läs mer

HPs service för anpassad återvinning
hp.com/go/businessrecycling

HP Secure Managed Print Services (MPS) – Säkra
utskrifter
hp.com/go/securemps

HP-skrivare är utformade för att arbeta tillsammans med lösningar för säkerhetsövervakning och hantering för att minska riskerna, förbättra efterlevnaden och genomgående skydda ert nätverk. (Inte alla HP-enheter ger tillgång till alla funktioner och lösningar.⁶⁾)

Grundläggande säkerhetsrutiner

Krypterad lagring med säker radering

All känslig information som lagras på den interna enheten eller hårddisken är potentiellt sårbara för stöld. Många HP-enheter har inbyggd kryptering för att skydda data. När lagrade data inte behövs längre kan enhetens inbyggda funktioner användas för att skriva över data och ta bort känslig information på ett säkert sätt.

Säker kassering

Med HPs service för anpassad återvinning kan ni säkerställa att data raderas från hårddiskarna innan gamla produkter återvinns på ett ansvarsfullt sätt.

Säker åtkomst för reparation av skrivare

Att känna till säkerhetsrutinerna för leverantörers skivarunderhåll hjälper till att skydda känsliga data. Välj *HP Secure Managed Print Services (MPS)* eller HP-partners för att få experthjälp.

Avaktivera portar och protokoll som inte används

Minska den sårbara ytan genom ordentlig enhetskonfigurering. Avaktivera fysiska portar och osäkra protokoll (till exempel FTP eller Telnet) för att förhindra otillåten åtkomst eller användning.

Administratörers åtkomstkontroll för enheten

Ange administratörslösenord så att bara IT-personal eller annan behörig personal kan ställa in och konfigurera enhetens inställningar.

Vitlistning av kod för inbyggd programvara

Läs nästa sida för att se information om hur vitlistning kan skydda era enheter från skadlig programvara.

Avancerade säkerhetsrutiner

Common Criteria Certification

HPs skrivare för företag är certifierade som anpassade efter internationellt erkända säkerhetsstandarder, till exempel Common Criteria Certification (CCC) och FIPS 140. Se till att uppdateringar av inbyggd programvara i enheten är kodsignerade så att kodens autenticitet och integritet kan bekräftas, och efterlevnad säkerställas.



Läs mer

Inbäddade säkerhetsfunktioner för utskifter:

- HP Sure Start (BIOS-integritet)
- Vitlistning av kod för inbyggd programvara
- Intrångsidentifiering under körning
- HP Connection Inspector

hp.com/go/PrintersThatProtect

HP JetAdvantage Security Manager:

hp.com/go/securitymanager

Skrivarens säkerhetsfunktioner upptäcker och stoppar attacker automatiskt

HPs skrivare för företag har säkerhetsfunktioner som hjälper till att skydda dem från att bli en attackmöjlighet i ert nätverk. Bara HPs utskriftssäkerhet erbjuder identifiering i realtid, automatiserad övervakning och inbyggd programvaruvalidering för att stoppa hot i samma ögonblick som de uppstår.⁷

HPs skrivare för företag, från Pro⁸ till Enterprise,⁷ är alltid på vakt och upptäcker och stoppar kontinuerligt hot under alla delar av driften.

- **Under start.** Startkoden (för Pro-enheter) eller BIOS (för Enterprise-enheter) är en uppsättning instruktioner som används för att ladda nödvändiga hårdvarukomponenter och starta inbyggd programvara. Kodens integritet valideras vid varje startcykel, vilket hjälper till att skydda enheter mot attacker.
- **När inbyggd programvara läses in.** *Vitlistning* kontrollerar automatiskt programvara under start för att avgöra om det är säker kod – digitalt signerad av HP. Om en onormal händelse upptäcks startar enheten om i ett säkert offline-läge och IT meddelas.
- **Under körning.** HPs inbäddade funktioner hjälper till att skydda enhetens minne medan enheter är påslagna och anslutna till nätverket – när de flesta attacker sker. I händelse av en attack stängs enheten av.

HP Enterprise-enheter kan läka sig själva

Utöver att kunna upptäcka och stoppa attacker så självläker HP Enterprise-skrivare automatiskt efter attacker, så att IT inte behöver ingripa.⁷ De här funktionerna utlöser automatiskt en omstart i händelse av en attack eller en onormal händelse. Administratörer kan meddelas via verktyg för säkerhetsinformation och händelsehantering (SIEM) som ArcSight, Splunk och SIEMonster.

- *HP Sure Start* är branschens enda självläkande BIOS.⁷ Om BIOS skadas så startar HP Sure Start om med en säker kopia av BIOS.
- *Identifiering av intrång under körning* övervakar komplex drift av inbyggd programvara och minne, stoppar automatiskt intrånget och startar om i händelse av en attack.
- *HP Connection Inspector* utvärderar pågående nätverksaktiviteter för att bedöma vilka som är normala, stoppa misstänkta förfrågningar och stoppa skadlig programvara genom att automatiskt utlösa en omstart.

Med investeringsskyddet hos den uppgraderbara inbyggda programvaran HP FutureSmart går det att lägga till vitlistning, identifiering av intrång under körning och HP Connection Inspector till många befintliga HP Enterprise-skrivare.⁷

HP JetAdvantage Security Manager avslutar kontrollcykeln

När en enhet har startats om, eller varje gång en enhet läggs till i nätverket, bedömer *HP JetAdvantage Security Manager* enhetens säkerhetsinställningar och korregerar dem vid behov så att de följer på förhand fastställda företagspolicyer. IT-personalen behöver inte ingripa.⁹

Hur fungerar det?

De inbäddade säkerhetsfunktionerna hanterar fyra viktiga steg i en HP-enhets cykel.

Om HP Enterprise-enheter blir angripna kan de starta om och reparera sig själva.

HP JetAdvantage Security Manager avslutar kontrollcykeln.

Fyra. Kontinuerlig övervakning

Skyddar drift och stoppar attacker medan enheten körs. Inspekterar utgående nätverksanslutningar för att stoppa misstänkta förfrågningar (endast Enterprise).

Tre. Kontrollera inställningar

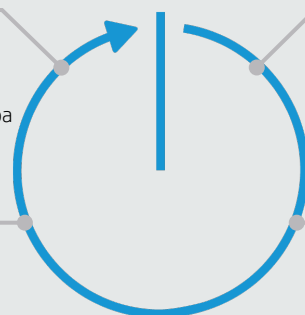
Efter en omstart kontrollerar och korregerar HP JetAdvantage Security Manager enhetens eventuella påverkade säkerhetsinställningar.

Ett. Kontrollera BIOS/startkod

Hindrar att skadlig kod körs under systemstart genom att endast tillåta att äkta HP-kod läses in.

Två. Kontrollera inbyggd programvara

Tillåter bara att autentisk, säker inbyggd programvara — som signerats digitalt av HP — läses in.





Skydda data



Läs mer

HP Web Jetadmin
hp.com/go/wja

HP Universal Print Driver med säker krypterad utskrift
hp.com/go/upd

Lösningar för HP JetAdvantage-arbetsflöde
hp.com/go/documentmanagement

HP Access Control
hp.com/go/hpac

Data behöver konstant skydd, både när de lagras och när de överförs. Här följer några grundläggande steg som bidrar till att säkerställa säkert mottagande och säker användning.⁶

Grundläggande säkerhetsrutiner

802.1x- eller IPsec-nätverksstandarder

Använd krypterade nätverksstandarder för att skydda data som förflyttas över nätverket mellan enheten och hanteringsverktyg, till exempel *HP Web Jetadmin* eller *HP Embedded Web Server*.

Kryptera data som överförs

Skydda utskriftsjobb som skickas till enheten, med kryptering som Internet Print Protocol over TLS (IPPS). Eller så ger *HP Universal Print Driver Secure Encrypted Print* symmetrisk AES256-kryptering och -dekryptering av utskrifter, från klient till sida, baserat på användardefinierade lösenord som använder FIPS 140-validerade krypteringsbibliotek från Microsoft®.

Vid skanning kan *Lösningar för HP JetAdvantage-arbetsflöde* hjälpa till att skydda känslig information, samtidigt som effektiviteten ökas. Till exempel integreras HP Capture och Route sömlöst med HP Access Control för att ge ökad säkerhet, med bekvämligheten med en enda autentisering och förmågan att övervaka innehåll för att ha kontroll över information.¹⁰

Kryptera data som inte används

Använd inbyggd kryptering för att skydda känslig affärsinformation som lagras på hårddisk. En extra säkerhetsnivå kan läggas till enheten genom det valbara tillbehöret HP Trusted Platform Module (TPM) för att stärka skyddet av krypterade autentiseringsuppgifter och data med hjälp av automatisk försegling av enhetens krypteringsnycklar för TPM. Tillbehöret ger enheten en säker identitet genom att generera och skydda certifierade privata nycklar.

Brandväggsskydd

Förhindra att virus och skadlig programvara kommer in i nätverket genom att begränsa skrivarens åtkomst till datorenheter på nätverket.

Inbyggd användarautentisering

Minska kostnaderna och säkerhetsriskerna genom att kräva att användare loggar in med PIN/PIC-, LDAP- eller Kerberos-autentisering. Dessa kan även integreras med Active Directory.

Rollbaserade åtkomstkontroller

HP Access Control Rights Management hjälper till att minska kostnader och säkerhetsrisker genom begränsningar av skriftfunktioner. Med rollbaserade åtkomstkontroller kan olika behörigheter ges till olika användare, eller till hela avdelningar, beroende på deras behov. Det går till exempel att begränsa vilka som faxar, skannar till e-post, eller skannar till fax.

Avancerade säkerhetsrutiner

Avancerad autentisering och spårning

Använd avancerad autentisering (till exempel lösenord, kontaktlösa kort, smartkort, biometrik) och spårningslösningar för ytterligare säkerhet och kontroll.



- *HP Access Control Secure Authentication* återställer kontroll, förstärker säkerhet och sänker kostnader. Skaffa flera avancerade kontroller och alternativ, inklusive pekautentisering med enheter med NFC-funktioner.
- *HP Access Control Job Accounting* hjälper till att noggrant följa och samla in data, analysera resultaten och sedan skapa och sända rapporter. Använd registrerade data för att tilldela skrivarkostnader, motivera anställda att skriva ut smartare och ge IT den information som krävs för att förbättra prognoser för alla enheter.

Läs mer

HP Access Control
hp.com/go/hpac

HP JetAdvantage Connect
hp.com/go/JetAdvantageConnect

HP Capture and Route
hp.com/go/hpcr

Mobila enheter inkluderade i nätverksåtkomst

Använd era mobila enheter som del av er totala säkerhetspolicy för skrivare och kontroll av skrivaråtkomst. HP erbjuder serverbaserade lösningar som ger säker pull printing och avancerade funktioner för administrering och rapportering.

- *HP JetAdvantage Connect* ger intuitiva och pålitliga mobilutskrifter för företag. Spara tid och pengar genom att smidigt utnyttja befintliga IT-nätverksverktyg och policyer för att hantera mobilutskrifter.¹¹ Användare kan säkert skriva ut från en mängd olika smarttelefoner och plattor, där och då de behöver, lika enkelt som från en dator.
- *HP Access Control* inkluderar funktioner för att hantera mobila utskrifter. Det utnyttjar den befintliga e-postinfrastrukturen och låter användare e-posta utskrifter till sin utskriftskö och sedan hämta dem från valfri skrivare eller multifunktionsskrivare (MFP) där lösningen är aktiverad. Skydda nätverkets utskriftsenheter med säkra autentiseringsfunktioner som Mobile Release.

Stoppa dataläckor innan de uppstår

HP-lösningar erbjuder funktioner som hjälper till att skydda dig mot dataförluster. Med *HP Capture and Route Data Loss Prevention* kan du förhindra att känslig information skannas eller faxas. *HP Access Control Print Data Loss Prevention* gör det möjligt för dig att förhindra att känsliga dokument skrivs ut. Spåra era viktigaste data för att förhindra läckor utan att arbetsflödet saktas ned. Få smarta säkerhetsvarningar baserade på villkor du själv väljer.

Använda digitala certifikat med skrivare

Förbättra säkerheten i utskriftsmiljön genom att använda digitala certifikat med nätverksskrivare och multifunktionsskrivare. Spara tid med HP JetAdvantage Security Manager för automatisk installation och förnyelse av certifikat.⁹



Skydda dokumentet



Läs mer

HP JetAdvantage Secure Print
hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Private Print
hp.com/go/JetAdvantagePrivatePrint

HP Access Control
hp.com/go/hpac

Dokumentskydd med HP och TROY
hp.com/go/HPandTROY

Integrera smarta hårdvaru- och programvarulösningar med den bredare IT-säkerhetsplanen för att skydda den känsliga informationen i utskrivna dokument.⁶

Grundläggande säkerhetsrutiner

Kontrollera åtkomst till förtryckta formulär

Utrusta era skrivare och multifunktionsskrivare med låsbara inmatningsfack som hjälper till att förhindra stöld av specialpapper som används för utskrift av checkar, recept eller andra känsliga dokument.

Använd en valfri PIN-kod eller pull printing för att skydda känsliga dokument

Användare kan välja att använda en PIN-kod eller pull printing för att minska både förlitandet på privata skrivare och risken för att utskriftsjobb faller i fel händer. De här säkerhetsåtgärderna minskar också oönskade utskrifter, vilket kan sänka kostnader och minska slöseri.

För utskrifter med PIN-kod tilldelas en PIN-kod när användare skickar konfidentiella utskriftsjobb. Koden måste användas vid enheten för att släppa förbi jobbet.

Pull printing lagrar utskriftsjobb i molnet eller på användarens dator. Användare autentiserar vid sin valda utskriftsplats för att hämta och skriva ut sitt jobb. HP erbjuder två molnbaserade pull print-lösningar:

- *HP JetAdvantage Secure Print* är en kostnadseffektiv lösning som är avsedd för små- och medelstora företag som lagrar utskriftsjobb i molnet eller på användarens dator. Den är lätt att ställa in och använda, gör att användare kan släppa förbi jobb från en mobil enhet, och har stöd för enheter för flera leverantörer.¹²
- *HP JetAdvantage Private Print* är HPs molnbaserade lösning som ger fördelarna med pull print, men utan komplexiteten. Den är enkel att konfigurera och kräver inte någon server, installation eller något underhåll.¹³

Avancerade säkerhetsrutiner

Kräv pull printing för alla utskrifter

HP Access Control Secure Pull Printing hjälper till att skydda konfidentiell information, förbättrar enhetssäkerheten och ökar effektiviteten. Den här robusta serverbaserade lösningen erbjuder flera former av autentisering, inklusive kortläsning, säkerhet på storföretagsnivå och administreringsfunktioner.

Använd MICR, vattenmärkning eller andra funktioner för att förhindra kopiering eller modifiering

HP- och TROY-lösningarna mot förfälskning innebär exempelvis användning av en säkerhetstoner som fläcker pappret om utskriften utsätts för kemisk manipulering, infogande av vattenstämplar med varierande data på utskrivna sidor och införande av maskinläsbara koder som spårar och kontrollerar individuella dokument. MFP:er kan integrera funktioner mot bedrägeri, till exempel anpassade signaturer, företagslogotyper och säkerhetstypsnitt i känsliga tryckta dokument som recept, personbevis och avskrifter.



Övervaka och hantera era utskriftsmiljöer



Läs mer

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Säkra lösningar för övervakning och hantering kan hjälpa till att upptäcka sårbarheter och etablera ett enhetligt, policybaserat dataskydd, minska risker och bibehålla efterlevnad.⁶ Förhindra luckor i skyddet och undvik dryga böter.

Grundläggande säkerhetsrutiner

Uppdatera enheter med den senaste inbyggda programvaran eller operativsystemet

Använd HP Web Jetadmin¹⁴ för att rulla ut uppdateringar till alla enheter och se till att enheter är uppdaterade med de senaste enhetsskydden och säkerhetsfunktionerna.

Granska aktivitetsloggar för skrivarsäkerhet

HP-enheter skickar skrivaraktiviteter/meddelanden till en syslog-server så att IT kan åtgärda problem om det behövs.

Bedöma och åtgärda enhetsinställningar

Hantera grundläggande säkerhetsinställningar för skrivare för alla enheter med *HP Print Manageability Integration Kit* (MIK), en plugin till Microsoft® System Center Configuration Manager (SCCM). Microsoft SCCM är en brett etablerad hanteringslösning för att på distans planera, installera, konfigurera och övervaka enheter. HP Print MIK kan upptäcka, bedöma och ändra de 15 vanligaste säkerhetsinställningarna och rapportera resultaten.

Välj *HP JetAdvantage Security Manager* för omfattande säkerhetshantering för alla enheter.⁹ Den här lösningen hjälper till att minska kostnader och resurser för att etablera en säkerhetspolicy för alla enheter, automatisera ändring av enhetsinställningar och installera och förnya unika certifikat medan ni får de rapporter som behövs för bevisa efterlevnad.



Läs mer

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Avancerade säkerhetsrutiner

Installera SIEM-programvara för att upptäcka och dokumentera hot

Händelsedata från HP FutureSmart-enheter kan skickas till verktyg för incidentupptäckt, till exempel ArcSight, Splunk och SIEMonster för övervakning i realtid. IT-säkerhetspersonal kan enkelt visa resultatmått för skrivare som en del av det bredare IT-ekosystemet och lösa varningar om skrivarsäkerhet.

Konfigurera automatiskt nya skrivarenheter när de läggs till i nätverket

Funktionen Instant-on Security som ingår med HP JetAdvantage Security Manager konfigurerar automatiskt nya enheter när de läggs till i nätverket eller efter en omstart.

Rapporter med granskning av säkerhetsefterlevnad för alla utskriftsenheter

Använd HP JetAdvantage Security Manager för att skapa rapporter med bevis på efterlevnad som demonstrerar applicering av säkerhetspolicyer hos skrivare och säkrande av kunders data.

Brist på efterlevnad kan skada er verksamhet

Enheter som är oskyddade eller har för dåligt skydd skapar fler tillfällen för cyberbrottslingar. För att möta det växande hotet implementerar regeringar över hela världen strikta säkerhetsregler som kräver att företag skyddar sina kunders information bättre.

Företag som inte har efterlevnad kan drabbas av höga kostnader, inklusive böter,

förlorade affärstillfällen, skadat rykte och stämningar.

Det är avgörande att installera enheter och lösningar som kan hjälpa er att klara efterlevnadskrav och skydda affärsinformation från säkerhetshot, till exempel HP Enterprise-skrivare och HP JetAdvantage Security Manager.



Få den hjälp ni behöver

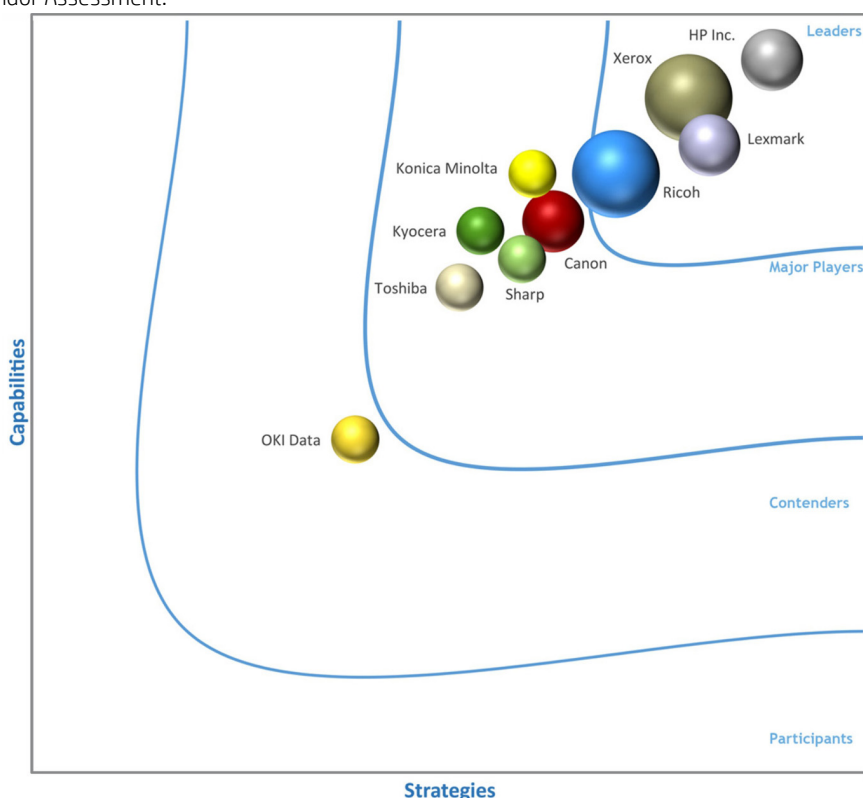
Ni behöver inte skydda och säkra på egen hand. Ett supportteam med konsulter kan visa hur man förbättrar säkerheten för data, enheter och dokument.

Samarbeta med experter på skrivarsäkerhet för att bedöma era nuvarande sårbarheter inom utskriftssäkerhet. Vi kan hjälpa er att bygga upp en omfattande säkerhetspolicy för utskrifter baserat på affärsbehov och bästa praxis, och skapa en plan för att uppnå förbättrad säkerhet i er unika miljö.

Erkända som branschledande

HP har utnämnts till ledande i den första IDC MarketScape-rapporten gällande Worldwide Security Solutions och Services Hardcopy 2017 Vendor Assessment. (Du hittar rapporten [här](#).) Enligt rapporten: "HP Inc. har ett angreppssätt gällande säkerhet som tar med hela utskrifts- och dokumentinfrastrukturen i beräkningen. Det börjar med att enheten läses och går vidare med alla aspekter av enhetsanvändning och innehållsskydd." Grafen som visas här är från IDC 2017 Vendor Assessment.¹⁵

IDC MarketScapes analysmodell för leverantörer har designats för att ge en översikt av ICT-leverantörers konkurrenskraft på en given marknad. Forskningsmetodiken använder sig av ett omfattande poängsystem som baseras både på kvalitativa och kvantitativa kriterier som resulterar i en enda grafisk illustration av varje leverantörs position inom en given marknad. Funktionspoängen mäter leverantörens produkt, go-to-market och verksamhetsgenomförande i det korta loppet. Strategipoängen mäter anpassning av leverantörsstrategier till kundkrav under en tidsram på 3-5 år. Leverantörens marknadsandel representeras av storleken på ikonerna.¹⁵



Komma igång

Kontakta en säljare för att få mer information om HPs säkerhetsfunktioner, lösningar och tjänster som kan ge er bättre skydd och ökad trygghet.

Läs mer

hp.com/go/printsecurity

¹ Påståendet "säkraste utskrifterna" är baserat på HPs granskning av publicerade säkerhetsfunktioner hos konkurrenternas likvärdiga skrivare, utförd 2017. Endast HP erbjuder en kombination av säkerhetsfunktioner som bevakar, upptäcker och automatiskt stoppar attacker för att sedan självvalidera programvarans integritet efter en omstart. För en lista över skrivare, besök: hp.com/go/PrintersThatProtect. Mer information: 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 undersökning som besvarades av 309 IT-proffs i Nordamerika, EMEA och APAC för HP, november 2016.

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

⁶ Vissa lösningar kanske inte stöds i alla HP-enheter. Vissa lösningar kan kräva ytterligare inköp.

⁷ HPs mest avancerade inbyggda säkerhetsfunktioner är tillgängliga på HP Enterprise-klassenheter med den inbyggda programvaran FutureSmart 4.5 eller senare, och baseras på HPs genomgång 2017 av publicerade inbyggda säkerhetsfunktioner hos konkurrerande skrivare i klassen. Endast HP erbjuder en kombination av säkerhetsfunktioner för integritetskontroll ned till BIOS med självläkande funktioner. En lista med kompatibla produkter finns på hp.com/go/PrintersThatProtect. Mer information finns på hp.com/go/printersecurityclaims.

⁸ Utvalda HP LaserJet Pro- och PageWide Pro-enheter har inbyggda funktioner som kan upptäcka och stoppa attacker. Mer information finns på hp.com/go/PrintersThatProtect.

⁹ HP JetAdvantage Security Manager måste köpas separat. Mer information finns på hp.com/go/securitymanager.

¹⁰ Ett extra lösenord krävs när information skickas till en lösenordsskyddad lagringsplats.

¹¹ HP JetAdvantage Connect fungerar med ledande mobila enheter. En engångs-plugin måste installeras för enheter som kör operativsystemen Android™, Google Chrome™ och Microsoft®. Mer information och en lista över operativsystem som stöds finns på hp.com/go/JetAdvantageConnect.

¹² HP JetAdvantage Secure Print: Pull printing fungerar med alla nätverksanslutna skrivare eller multifunktionsskrivare. Autentisering på enheterna är tillgänglig för många modeller av HP LaserJet, PageWide och OfficeJet Pro samt även vissa enheter från andra tillverkare. På vissa enheter måste den inbyggda programvaran uppdateras. Internetanslutning krävs för molnlagring och hämtning av utskriftsjobb. Aktivering av utskriftsjobb från en mobil enhet kräver nätverksanslutning och en QR-kod. Mer information och för att se en lista över skrivare och multifunktionsskrivare som stöds finns på hp.com/go/JetAdvantageSecurePrint.

¹³ HP JetAdvantage Private Print är tillgängligt utan kostnad och kräver att skrivaren är ansluten till internet med webbtjänsten aktiverad. Inte tillgängligt i alla länder. Läs mer på hp.com/go/JetAdvantagePrivatePrint.

¹⁴ HP Web Jetadmin kan hämtas utan extra kostnad från hp.com/go/webjetadmin.

¹⁵ Baserat på IDC:s granskning av fysiska leverantörer och åsikt gällande HPs ledarskap: "HP har en fördel med sin starka IT-service och -funktioner... och de tillhandahåller en omfattande och integrerad säkerhets strategi över hela IT-infrastrukturen." KÄLLA: [IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment](#), av Allison Correia och Robert Palmer, oktober 2017, IDC Doc #US41988517.

Registrera dig för att få uppdateringar

hp.com/go/getupdated



Dela med kollegor

© Copyright 2014–2018 HP Development Company, L.P. Informationen i detta dokument kan komma att ändras utan föregående meddelande. HP lämnar inga andra garantier för HPs produkter eller tjänster än de uttryckliga garantier som medföljer sådana produkter och tjänster. Ingenting i detta dokument ska anses utgöra en ytterligare garanti. HP ansvarar inte för tekniska eller redaktionella fel i detta dokument.

Android och Google Chrome är registrerade varumärken som tillhör Google Inc. Microsoft är ett registrerat varumärke i USA som tillhör Microsoft-koncernen.

4AA3-1295SVE, januari 2018, Rev. 11

