



Suojaa verkkoasi maailman turvallisimman tulostuksen avulla¹

94 %

rahoitusalan yrityksistä on sitä mieltä, että kopiokoneen/tulostimen ja monitoimilaitteen suojaaminen on tärkeää tai hyvin tärkeää.²



61 %

organisaatioista ilmoitti vähintään yhdestä tulostamiseen liittyvästä tietoturvaloukkauksesta a kuluneen vuoden aikana.³



43 %

yrityksistä jättää tulostimet ja monitoimilaitteet huomiotta päätelaitteiden tietoturvakäytännöissä.⁴





Vain 18 % yrityksistä valvoo tulostimia tai monitoimilaitteita uhkien varalta.⁴ Miten on laita sinun yrityksessäsi?

Tunnista piilevät riskit

IT-yksikkö joutuu jatkuvasti suojaamaan luottamuksellisia tietoja, kuten henkilöstön identiteettejä ja asiakkaiden tietoja, useissa laitteissa ja ympäristöissä. Vaikka monet IT-yksiköt suojaavat yksittäiset tietokoneet ja verkon huolellisesti, verkotetut monitoimilaitteet ja tulostimet lyödään usein laimin, joten ne jäävät alttiiksi. Kun laitteita ei ole suojattu, koko verkko voi altistua hyökkäykselle.

Ota huomioon mahdolliset kustannukset

Yksikin tietoturvaloukkaus voi käydä kalliiksi. Jos suojaamaton verkotettu monitoimilaitte tai tulostin vaarantaa luottamukselliset tiedot, voi aiheutua identiteettivarkaus, kilpailutietoja voidaan varastaa, yrityskuva ja maine voivat tahrinua tai seurauksena voi olla juridisia seurauksia. Lisäksi säädösten ja lainsäädännön noudattamatta jättämisestä voidaan määrätä suuret sakot.

HP voi auttaa

Suojaa verkkoasi maailman turallisimman tulostuksen avulla.¹ HP:n tulostimet ja monitoimilaitteet valvovat jatkuvasti tunnistuen ja pysäyttäen uhat sekä mukautuen uusiin. HP voi auttaa automatisoimaan laitteiden, tietojen ja asiakirjojen suojaamisen laajan ratkaisuvälikomansa avulla. Toimistolaitteiden suojausasiantuntijamme voivat auttaa laatimaan ja ottamaan käyttöön kattavan verkotettujen monitoimilaitteiden ja tulostinten suojausstrategian.

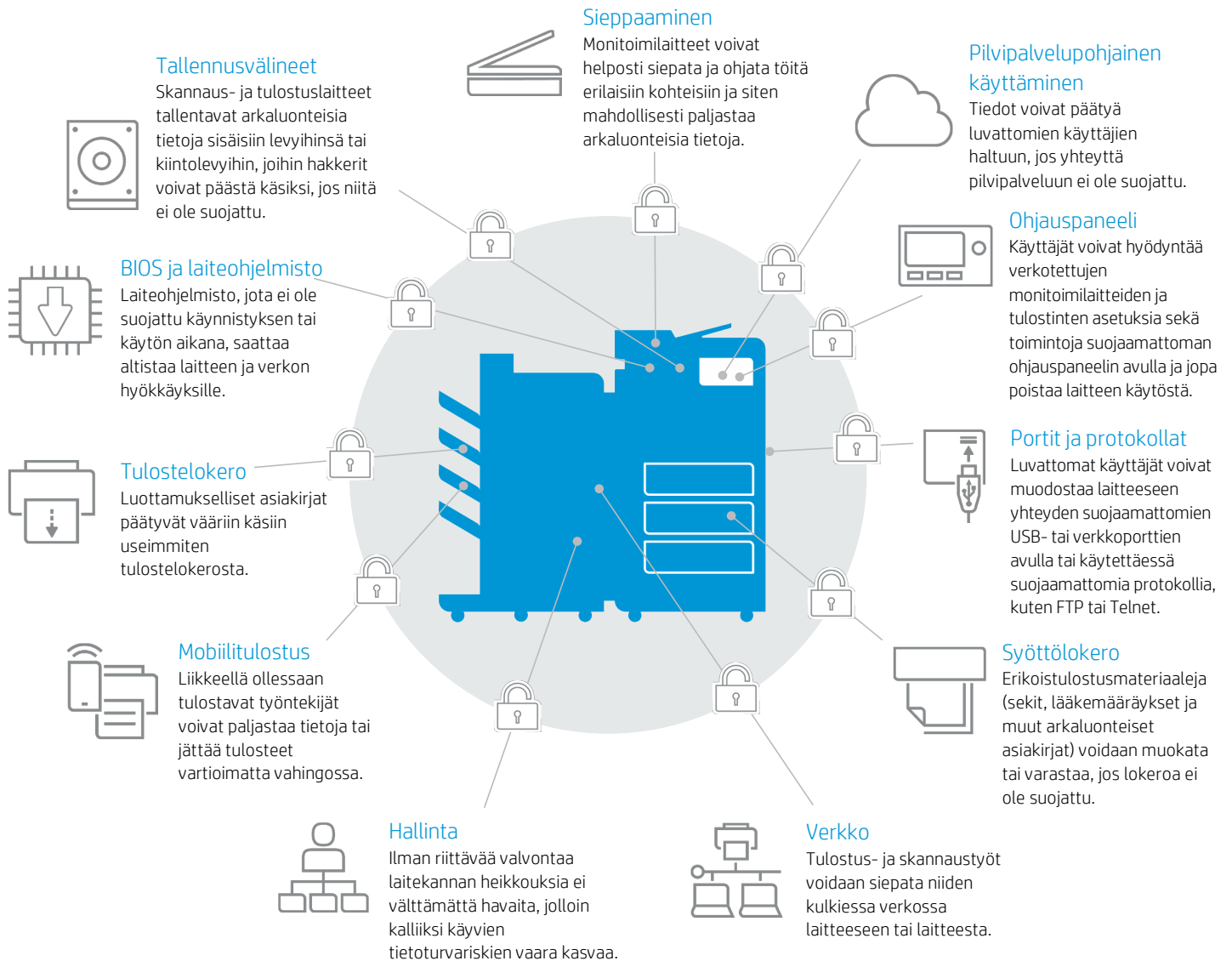
"HP:n pitkäaikaisesta panostamisesta toimistolaitteiden suojaukseen kertoo se, että yrityksellä on markkinoiden laajin ja monikerroksisin tietoturvaratkaisujen ja -palvelujen valikoima."

– Quocirca, tammikuu 2017⁵

Puolusta laitteitasi, tietojasi ja asiakirjojasi

Toimistolaiteympäristön useilla alueilla voi olla vakavia puutteita. Kun haavoittuvuudet saadaan selville, riskejä voidaan vähentää.

Verkotettujen monitoimilaitteiden ja tulostimien haavoittuvuudet





Suojaa laite



Lisätietoja

HP:n mukautetut kierrätyspalvelut
hp.com/go/businessrecycling

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

HP:n tulostimet ja monitoimilaitteet on suunniteltu toimimaan yhdessä tietoturvan valvonta- ja hallintaratkaisujen kanssa. Näin vähennetään riskejä, kohennetaan vaatimustenmukaisuutta sekä suojataan verkko kattavasti. (Kaikki ominaisuudet ja ratkaisut eivät ole käytettävissä kaikissa HP:n laitteissa.⁶⁾)

Perustason suojauskäytännöt

Salattu tallennus ja suojattu poisto

Kaikki sisäiseen levyyn tai kiintolevyyn tallennetut luottamukselliset tiedot ovat alttiina varkauksille. Monissa HP:n laitteissa tiedot suojataan salaamalla ne. Kun tallennettuja tietoja ei enää tarvita, ne poistetaan turvallisesti kirjoittamalla niiden päälle.

Suojattu hävittäminen

HP:n mukautettujen kierrätyspalveluiden avulla voidaan varmistaa, että tiedot poistetaan kiintolevyistä ennen käytöstä poistettujen laitteiden kierrättämistä vastuullisesti.

Tulostimien ja monitoimilaitteiden suojaaminen huollon ajaksi

Tulostimen ja monitoimilaitteen kunnossapitopalvelujen toimittajan tietoturvakäytäntöjen tunteminen auttaa suojaamaan luottamukselliset tiedot. Saat asiantuntevaa apua valitsemalla *HP Secure Managed Print Services (MPS)* -palvelun tai kääntymällä HP:n kumppanien puoleen.

Tarpeettomien porttien ja protokollien poistaminen käytöstä

Kun laitteen asetukset määritetään oikein, hyökkäyksille jää vähemmän mahdollisuuksia onnistua. Poista fyysiset portit ja suojaamattomat protokollat käytöstä, kuten FTP ja Telnet, jotta luvaton käyttö estetään.

Järjestelmänvalvojen pääsy käsiksi laitteeseen

Valitse järjestelmänvalvojan salasana siten, että vain IT-henkilöstä tai muut valtuutetut henkilöt voivat ottaa käyttöön ja määrittää laiteasetukset.

Sallittujen käyttäjien luettelointi laiteohjelmistossa

Seuraavalla sivulla on lisätietoja laitteiden suojaamisesta haittaohjelmilta sallittujen käyttäjien luettelon avulla.

Täydentävät suojauskäytännöt

Common Criteria Certification

Yrityskäyttöön tarkoitetuilla HP:n tulostimilla ja monitoimilaitteilla on kansainvälisesti tunnustettujen tietoturvastandardien mukaiset sertifioinnit, kuten Common Criteria Certification (CCC) ja FIPS 140. Varmista, että laiteohjelmistopäivitysten koodi on allekirjoitettu, että sen aitous ja eheys varmistetaan ja että vaatimustenmukaisuus säilytetään.

Toimistolaitteiden suojausominaisuudet tunnistavat ja pysäyttävät hyökkäykset automaattisesti.

Yrityskäyttöön tarkoitettujen HP-tulostimien ja -monitoimilaitteiden tietoturvaominaisuudet auttavat suojaamaan ne, jotta niitä ei käytetä astinlautoina verkkoon kohdistuvia hyökkäyksiä varten. Vain HP Print Security tarjoaa reaaliaikaisen tunnistuksen, automaattisen valvonnan ja sisäinen ohjelmiston tarkistuksen, jotta uhat pysäytetään heti kun niitä ilmenee.⁷

Yrityskäyttöön tarkoitettut HP-tulostimet ja -monitoimilaitteet Pro-tasolta⁸ Enterprise-tasolle⁷ valvovat jatkuvasti tunnistaen ja pysäyttäen uhat sekä mukautuen uusiin.



Lisätietoja

Tulostimien ja monitoimilaitteiden upotetut suojausominaisuudet:

- HP Sure Start (BIOSin eheys)
 - Sallittujen käyttäjien luettelointi laiteohjelmistossa
 - Ajonaikaisten hyökkäysten tunnistus
 - HP Connection Inspector
- hp.com/go/PrintersThatProtect

HP JetAdvantage Security Manager:
hp.com/go/securitymanager

- **Käynnistyksen aikana.** Käynnistyskoodi (Pro-laitteissa) tai BIOS (Enterprise-laitteissa) on sarja käynnistysohjeita, joiden avulla ladataan laitteiston kannalta kriittisiä komponentteja ja käynnistetään laiteohjelmisto. Koodin eheys tarkastetaan jokaisella käynnistysjaksolla, jotta laite suojataan hyökkäyksiltä.
- **Kun laiteohjelmisto ladataan.** Laiteohjelmisto tarkastetaan käynnistyksen aikana *sallittujen luettelon* avulla. Näin varmistetaan, että sen koodi on hyvä ja aito – HP:n digitaalisesti allekirjoittama. Jos havaitaan poikkeama, laite käynnistetään uudelleen suojattuun offline-tilaan ja IT-tuelle ilmoitetaan.
- **Kun laite on käytössä.** HP:n upotetut ominaisuudet auttavat suojaamaan muistia, kun laitteisiin on kytketty virta ja ne on yhdistetty verkkoon — juuri silloin kun useimmat hyökkäykset tapahtuvat. Jos laitteeseen kohdistuu hyökkäys, siitä katkaistaan virta.

HP Enterprise -laitteet osaavat korjata itse itsensä

Uhkien tunnistamisen ja pysäyttämisen lisäksi HP Enterprise -tulostimet ja -monitoimilaitteet korjaavat itsensä automaattisesti hyökkäyksen tapahduttua, joten IT-tuen ei tarvitse puuttua asiaan.⁷ Jos tapahtuu hyökkäys tai epänormaalia toimintaa, nämä toiminnot laukaisevat uudelleenkäynnistyksen automaattisesti. Järjestelmänvalvojille voidaan ilmoittaa tietoturvatietojen ja -tapahtumien hallintatyökalujen (SIEM) avulla, kuten ArcSight, Splunk ja SIEMONster.

- *HP Sure Start* on toimialan ainoa itsestään korjautuva BIOS.⁷ Jos BIOS vaarantuu, HP Sure Start käynnistää laitteen uudelleen turvallisen BIOS-kopion avulla.
- *Ajonaikaisten hyökkäysten tunnistus* valvoo monimutkaisia laiteohjelmisto- ja muistitoimintoja. Se pysäyttää hyökkäyksen automaattisesti ja käynnistää laitteen uudelleen, jos siihen on hyökätty.
- HP Connection Inspector arvioi lähtevät yhteydet tunnistaen, mikä on normaalia, estäen epäilyttävät pyynnöt ja torjuen haittaohjelmat laukaisemalla uudelleenkäynnistyksen automaattisesti.

Kun suojaat investoinnin päivitettävän HP FutureSmart -laiteohjelmiston avulla, voit ottaa käyttöön suojattujen luettelon, ajonaikaisten hyökkäysten tunnistuksen ja HP Connection Inspector -toiminnon monissa aiemmin hankituissa HP Enterprise -tulostimissa ja -monitoimilaitteissa.⁷

HP JetAdvantage Security Manager viimeistelee tarkastusjakson

Uudelleenkäynnistyksen tai uuden laitteen verkkoon lisäämisen jälkeen *HP JetAdvantage Security Manager* arvioi ja tarvittaessa korjaa laitteen suojausasetukset automaattisesti yrityksen ennalta laadittujen käytäntöjen mukaisiksi.⁹ IT-työntekijöiden ei tarvitse puuttua asiaan.

Miten se toimii?

Upotetut suojausominaisuudet toimivat HP:n laitteessa nelivaiheisesti.

Jos laitteeseen kohdistuu hyökkäys, HP Enterprise -laitteet osaavat käynnistää uudelleen ja korjata itse itsensä.

HP JetAdvantage Security Manager viimeistelee tarkastusjakson.

Neljä. Jatkuva valvonta

Suojaaj toiminnan ja pysäyttää hyökkäykset, kun laite on toiminnassa.

Tarkistaa lähtevät yhteydet ja estää epäilyttävät pyynnöt (vain Enterprise-laitteet).

Kolme. Tarkistaa asetukset

Uudelleenkäynnistyksen jälkeen HP JetAdvantage Security Manager tarkastaa laitteen suojausasetukset ja korjaa ne.

Yksi. Tarkistaa

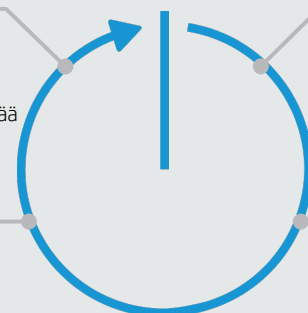
BIOSin/käynnistyskoodin

Estää haitallisen koodin suorittamisen käynnistettäessä sallimalla vain aidon HP:n allekirjoittaman koodin lataamisen.

Kaksi. Tarkastaa

laiteohjelmiston

Vain aidon—HP:n digitaalisesti allekirjoittaman—laiteohjelmiston lataaminen sallitaan.





Tietojen suojaaminen



Lisätietoja

HP Web Jetadmin
hp.com/go/wja

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

HP JetAdvantage -työnkuluratkaisut
hp.com/go/documentmanagement

HP Access Control
hp.com/go/hpac

Tietosi on suojattava jatkuvasti, kun niitä säilytetään tai siirretään. Tässä on muutamia vihjeitä turvallisen vastaanoton ja käyttämisen varmistamiseksi.⁶

Perustason suojauskäytännöt

802.1x- tai IPsec-verkkostandardit

Suojaa verkossa laitteiden välillä siirrettävät tiedot käyttämällä salattuja verkkostandardeja ja hallintatyökaluja, kuten *HP Web Jetadmin* tai *HP:n sulautettu Web-palvelin*.

Salaa siirrettävät tiedot

Suojaa laitteeseen siirrettävät tulostustiedot salaamalla. Ota käyttöön esimerkiksi IPPS (Internet Print Protocol over TLS). *HP Universal Print Driver Secure Encrypted Print* antaa käyttöön aidosti symmetrisen tulostustiedon AES256-salauksen ja salauksen purkamisen. Se ulottuu työasemasta tulostettavaan sivuun saakka ja perustuu käyttäjän määrittämään salasanaan ja Microsoftin® salauskirjastoihin, joissa käytetään FIPS 140 -validointia.

Skannaamisen aikana *HP JetAdvantage Workflow Solutions* voi auttaa suojaamaan luottamuksellisia tietoja ja parantamaan tehokkuutta. Esimerkiksi HP Capture and Route integroituu saumattomasti HP Access Control -toimintoon, joten tietoturva paranee kätevän yhden todennuksen avulla. Sisältöä voidaan valvoa tiedonhallinnan mahdollistamiseksi.¹⁰

Salaa säilytettävät tiedot

Suojaa kiintolevyyn tallennetut luottamukselliset tiedot sisäisen salauksen avulla. Suojausta laitteessa voidaan vahvistaa lisäämällä HP Trusted Platform Module (TPM) -lisävaruste. Se parantaa salattujen tietojen suojausta sulkemalla laitteen salausavaimet automaattisesti TPM-moduuliin. Se suojaa laitteen identiteetin luomalla varmenteen yksityiset avaimet ja suojaamalla ne.

Suojaaminen palomuurin avulla

Estä haittaohjelmien ja virusten pääseminen verkkoon sallimalla vain verkkoon liitettyjen laitteiden käyttää tulostimia ja monitoimilaitteita.

Alkuperäisen käyttäjän todennus

Säästä kustannuksia ja vähennä tietoturvariskejä edellyttämällä käyttäjiltä PIN/PIC-, LDAP- tai Kerberos-todennusta. Ne voidaan integroida Active Directoryyn.

Roolipohjaiset käytönvalvonnat

HP Access Control Rights Management auttaa säästämään kustannuksia ja vähentämään tietoturvariskejä rajoittamalla tulostimien ja monitoimilaitteiden ominaisuuksien käyttämistä. Roolipohjaisen käytön hallinnan avulla voit antaa eri käyttäjille tai jopa kokonaisille osastoille erilaisia oikeuksia tarpeiden mukaan. Voit esimerkiksi rajoittaa, kuka voi faksata, skannata sähköpostiin tai skannata faksiin.

Täydentävät suojauskäytännöt

Kehittynyt todennus ja seuranta

Tehosta tietoturvaa ja hallintaa ottamalla käyttöön kehittynyt todennus, kuten salasana, etälukukortit, älykortit tai biometrinen tunnistus.



- *HP Access Control Secure Authentication* palauttaa hallinnan, vahvistaa tietoturvaa ja vähentää kustannuksia. Saat käyttöösi useita kehittyneitä hallintavaihtoehtoja, kuten todennuksen koskettamalla NFC-yhteensopivan mobiililaitteen avulla.
- *HP Access Control Job Accounting* auttaa seuraamaan ja keräämään tietoja tarkasti, analysoimaan tuloksia sekä laatimaan ja lähettämään raportteja. Tiedonlouhinnan avulla tulostuskustannukset voidaan kohdentaa ja motivoida henkilöstöä tulostamaan fiksummin sekä tuottaa IT-yksikön tarpeisiin tietoja koko laitekannan kattavien ennusteiden laatimiseksi.

Mobiililaitteet mukaan verkon käytön valvontaan

Ota mobiililaitteet osaksi tulostamisen tietoturvakäytäntöä. HP tarjoaa palvelin pohjaisia ratkaisuja suojattuun turvatulostamiseen sekä kehittyneitä hallinta- ja raportointiominaisuuksia.

- *HP JetAdvantage Connect* tarjoaa yrityksille helppokäyttöistä ja luotettavaa mobiilitulostusta. Aikaa ja rahaa säästyy, kun mobiilitulostusta hallitaan saumattomasti nykyisten IT-verkkotyökalujen ja käytäntöjen avulla.¹¹ Käyttäjät voivat tulostaa turvallisesti erilaisista älypuhelimista ja tablet-tietokoneista yhtä helposti kuin tietokoneista mistä ja koska tahansa.
- *HP Access Control* mahdollistaa mobiilitulostuksen hallinnan. Se hyödyntää nykyistä sähköposti-infrastruktuuria, joten mobiilikäyttäjät lähettävät tulostustyön tulostusjonoon sähköpostitse ja turvatulostavat sen tämän ratkaisun kanssa yhteensopivan tulostimen tai monitoimilaitteen avulla. Suojaa verkotetut tulostimet ja monitoimilaitteet todennusominaisuuksilla, kuten Mobile Release.

Pysäytä tietovuodot ennen kuin niitä ilmenee

HP tarjoaa ratkaisuja, joiden avulla voit suojautua tietojen häviämiseltä. *HP Capture and Route Data Loss Prevention* -ratkaisun avulla voit estää tärkeiden tietojen skannaamisen tai faksaamisen. *HP Access Control Print Data Loss Prevention* -ratkaisun avulla voit estää tärkeiden asiakirjojen tulostamisen. Kun seuraat tärkeimpiä tietojasi, estät tietomurrot hidastamatta työnkulkua. Saat älykkäät tietoturvaravitukset valitsemiesi ehtojen perusteella.

Ota tulostimissa ja monitoimilaitteissa käyttöön digitaaliset varmenteet

Paranna tulostusympäristön tietoturvaa ottamalla digitaaliset varmenteet käyttöön verkon tulostimissa ja monitoimilaitteissa. Säästä aikaa käyttämällä HP JetAdvantage Security Manageria varmenteiden automaattista asennusta ja uusimista varten.⁹

Lisätietoja

HP Access Control
hp.com/go/hpac

HP JetAdvantage Connect
hp.com/go/JetAdvantageConnect

HP Capture and Route
hp.com/go/hpcr



Suojaa asiakirja

Integroi älykkäät laitteet ja ohjelmistoratkaisut osaksi laajempaa tietoturvasuunnitelmaa, jotta tulostettujen asiakirjojen sisältämät luottamukselliset tiedot suojataan.⁶



Lisätietoja

HP JetAdvantage Secure Print
hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Private Print
hp.com/go/JetAdvantagePrivatePrint

HP Access Control
hp.com/go/hpac

HP ja asiakirjojen TROY-suojus
hp.com/go/HPandTROY

Perustason suojauskäytännöt

Valvo esipainettujen lomakkeiden käyttämistä

Kun varustat tulostimet ja monitoimilaitteet lukittavilla syöttölokeroilla, estät sekkejä, lääkemääryksiä ja muita suojausta vaativia asiakirjoja tulostettaessa käytettävien erikoispaperien varastamisen.

Suojaa luottamukselliset asiakirjat edellyttämällä PIN-koodia tai turvatulostusta

Kun käyttöön otetaan PIN-koodi tai turvatulostus, riippuvuus henkilökohtaisista tulostimista ja tulostustöiden väärin käsiin joutumisen riski vähenevät. Nämä tietoturvatimet estävät myös turhat tulostukset, mikä voi säästää kustannuksia ja vähentää jätteen määrää.

Kun luottamuksellisia asiakirjoja tulostettaessa edellytetään PIN-koodia, se täytyy syöttää laitteeseen, jotta työ tulostetaan.

Pull Printing -tulostustyöt tallennetaan pilvipalveluun tai käyttäjän tietokoneeseen. Käyttäjien on todentauduttava, jotta he voivat turvatulostaa työnsä. HP tarjoaa kahta pilvipalvelupohjaista turvatulostusratkaisua:

- *HP JetAdvantage Secure Print* on edullinen pienille ja keskisuurille yrityksille tarkoitettu ratkaisu. Tulostustyöt tallennetaan pilvipalveluun tai käyttäjän tietokoneeseen. Se on helppo ottaa käyttöön ja käyttää. Käyttäjät voivat vapauttaa työt mobiililaitteen avulla, ja se tukee useiden valmistajien laitteita.¹²
- *HP JetAdvantage Private Print* on HP:n maksuton pilvipalvelupohjainen ratkaisu, joka tuo tullessaan turvatulostuksen edut helposti. Se on helppo ottaa käyttöön, eikä se edellytä palvelinta, asenusta tai ylläpitoa.¹³

Täydentävät suojauskäytännöt

Ota turvatulostus pakolliseksi kaikille tulostustöille

HP Access Control Secure Pull Printing auttaa suojaamaan luottamuksellisia tietoja, suojaamaan laitteen tehokkaammin ja parantamaan tehokkuutta. Tämä vankka palvelin pohjainen ratkaisu tarjoaa useita todennusvaihtoehtoja, kuten tulostustyön vapautus etälukukortin avulla, suuryritystason tietoturva ja hallintaominaisuudet.

Estä kopioiminen ja muutosten tekeminen MICR-, vesileima- tai muiden ominaisuuksien avulla.

HP ja TROY ehkäisevät väärinkäytöksiä esimerkiksi suojaavan värijauheen avulla, joka tahraa paperin, jos sitä käsitellään kemiallisesti, lisäämällä tulostettaviin sivuihin muuttuvilla tiedoilla varustettuja vesileimoja ja sisällyttämällä asiakirjoihin koneellisesti luettavia koodeja, joiden avulla yksittäisiä asiakirjoja voidaan seurata ja auditoida. Monitoimilaitteissa voidaan ottaa käyttöön väärentämistä ehkäiseviä ominaisuuksia, kuten mukautettavia allekirjoituksia, yritysten logoja ja turvakirjasimia esimerkiksi lääkemääryyksissä, syntymätodistuksissa ja muissa todistuksissa.



Valvo ja hallitse tulostusympäristöäsi



Lisätietoja

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Tietoturvan valvonta- ja hallintaratkaisut voivat auttaa tunnistamaan haavoittuvuudet sekä ottamaan käyttöön yhdenmukaisen käytäntöihin perustuvan lähestymistavan tietojen suojaamiseksi, riskien vähentämiseksi ja vaatimustenmukaisuuden varmistamiseksi.⁶ Estä suojauspuutteet ja auta välttämään kalliiksi käyvät sakot.

Perustason suojauskäytännöt

Päivitä laitteisiin uusimmat laiteohjelmisto- ja käyttöjärjestelmäversiot.

Asenna laiteohjelmistopäivitykset laitteisiin HP Web Jetadmin¹⁴ -ohjelmiston avulla, jotta laitteiden suojaus- ja tietoturvaominaisuudet ovat ajan tasalla.

Tarkastele tulostimen ja monitoimilaitteen tietoturvatapahtumalokeja

HP:n laitteet lähettävät tulostimen ja monitoimilaitteen tapahtumat ja ilmoitukset syslog-palvelimeen, jotta IT-yksikkö voi tarvittaessa korjata ongelmat.

Arvioi laiteasetuksia ja tee tarvittaessa muutoksia

Hallitse tulostinten ja monitoimilaitteiden perustason suojausasetuksia *HP Print Manageability Integration Kit* (MIK) -lisäohjelman avulla. Se toimii yhdessä Microsoft® System Center Configuration Managerin (SCCM) kanssa. Microsoft SCCM on laajalti käytetty hallintaratkaisu, jonka avulla suunnitellaan, otetaan käyttöön, määritetään ja valvotaan päätelaitteita etäyhteydellä. HP Print MIK pystyy löytämään, arvioimaan ja korjaamaan tärkeimmät 15 suojausasetusta ja raportoimaan tulokset.

Valitse *HP JetAdvantage Security Manager* koko laitekannan tietoturvan hallintaan.⁹ Tämä ratkaisu auttaa vähentämään kustannuksia ja resurssien tarvetta, jotta saadaan aikaan koko laitekannan kattava tietoturvakäytäntö, automatisoidaan laitteiden asetusten korjaaminen, asennetaan ja uudistetaan yksilöllisiä varmenteita sekä saadaan tarvittavat raportit vaatimustenmukaisuuden osoittamiseksi.



Lisätietoja

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Täydentävät suojauskäytännöt

Ota käyttöön SIEM-ohjelmisto uhkien tunnistamiseksi ja dokumentoimiseksi

HP FutureSmart -laitteista peräisin olevat tapahtumatiedot voidaan lähettää ArcSightin, Splunkin ja SIEMonsterin kaltaisiin tapahtumientunnistustyökaluihin reaaliaikaista valvontaa varten. IT-yksikön tietoturva-asiantuntijat voivat helposti tarkkailla tulostimia ja monitoimilaitteita laajemman IT-ekosysteemin osana, jotta laitteiden tietoturvahälytykset tunnistetaan ja ratkaistaan.

Määritä uusien tulostuslaitteiden asetukset automaattisesti, kun ne lisätään verkkoon

HP JetAdvantage Security Managerin pikasuojausominaisuus määrittää uusien laitteiden asetukset automaattisesti, kun ne lisätään verkkoon tai käynnistetään uudelleen.

Vaatimustenmukaisuuden raportointi kattaa koko toimistolaitekannan suojauksen

Laadi HP JetAdvantage Security Managerin avulla vaatimustenmukaisuuden osoittavia raportteja, jotta osoitetaan tietoturvakäytäntöjen soveltaminen tulostimiin ja monitoimilaitteisiin sekä asiakkaiden tietojen suojaaminen.

Jos vaatimustenmukaisuutta ei saavuteta, liiketoiminta voi kärsiä

Suojaamattomat tai puutteellisesti suojatut päätelaitteet houkuttelevat kyberrikollisia. Tämän kasvavan uhan kukistamiseksi viranomaiset eri puolilla maailmaa säättävät tietosuojamääräyksiä, jotta organisaatiot suojaavat asiakkaiden tiedot tehokkaammin.

Jos niitä ei noudateta, seuraukset voivat olla ikäviä: sakkoja,

liiketoiminnan kärsimistä, mainevahinkoja ja syytteitä.

On tärkeää ottaa käyttöön laitteet ja ratkaisut — kuten HP Enterprise -tulostimet ja -monitoimilaitteet sekä HP JetAdvantage Security Manager — jotka voivat auttaa täyttämään vaatimukset ja suojaamaan yrityksen tiedot turvallisuusuuhkia vastaan.



Saat tarvitsemasi avun

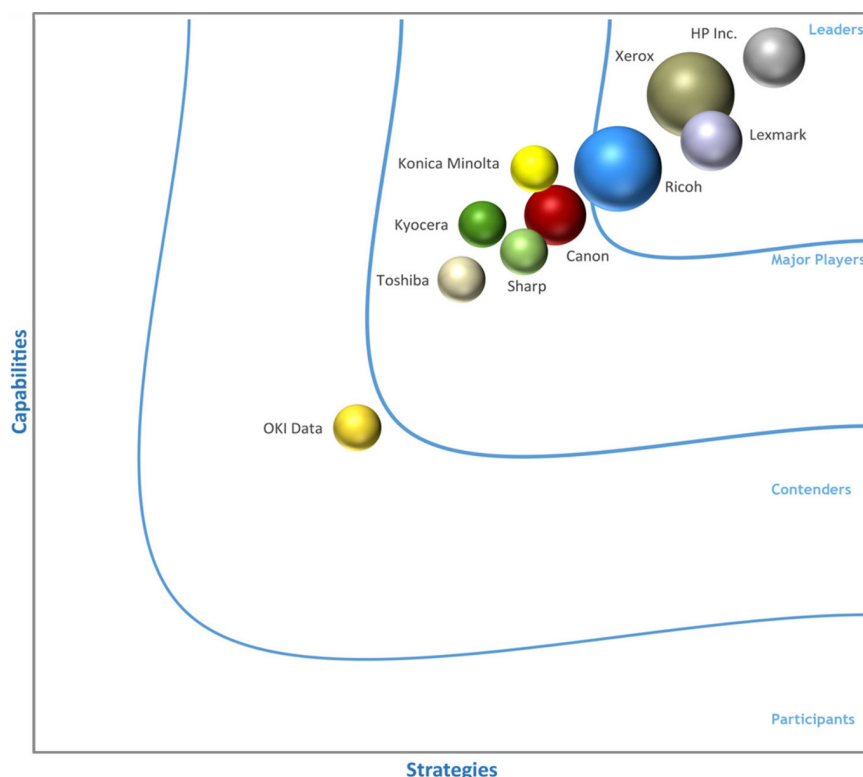
Sinun ei tarvitse huolehtia tietoturvasta ja suojauksesta omin päin. Konsultit voivat osoittaa, kuinka tietojen, laitteiden ja asiakirjojen suojausta parannetaan.

Arvioi toimistolaitteiden tietoturva yhteistyössä laitteiden tietoturva-asiantuntijoiden kanssa. Voimme auttaa laatimaan kattavan toimistolaitteiden tietoturvakäytännön, joka perustuu liiketoiminnan tarpeisiin ja parhaisiin käytäntöihin, sekä laatimaan suunnitelman tietoturvan parantamiseksi nykyisessä ympäristössä.

Tunnustettu alansa johtavaksi yritykseksi

HP on nimetty alansa johtavaksi yritykseksi ensimmäisessä IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment -raportissa. (Raportti löytyy [täältä](#).) Raportin mukaan ”HP Inc. huomioi tietoturva-asioissa koko tulostus- ja asiakirjainfrastruktuurin alkaen laitteen lukitsemisesta ja sisältäen kaikki laitteen käyttöä ja sisällön suojausta koskevat osa-alueet”. Tässä esitetty kuva on IDC 2017 Vendor Assessment -raportista.¹⁵

IDC MarketScapen tuotetoimittajia koskeva analyysimalli on suunniteltu siten, että se antaa yleiskuvan IT-toimittajien kilpailukyvyistä tietyllä markkinalla. Tutkimusmenetelmässä hyödynnetään tarkkaa arviointimenetelmää, joka pohjautuu sekä laadullisiin että määrällisiin kriteereihin ja jonka tuloksena on graafinen esitys jokaisen tuotetoimittajan asemasta kyseisellä markkinalla. Valmiudet-pistemäärä mittaa tuotetoimittajan tuotetta, markkinoille tuontia ja liiketoimintaa lyhyellä aikavälillä. Strategia-pistemäärä mittaa tuotetoimittajan strategian soveltamista asiakasvaatimuksiin 3–5 vuoden aikajaksossa. Kuvakkeiden koolla kuvataan tuotetoimittajan markkinaosuutta.¹⁵



Aloittaminen

Pyydä yhteyshenkilöltäsi lisätietoja HP:n suojausominaisuuksista, ratkaisuista ja palveluista, jotta lähdet matkalle kohti tehokkaampaa suojausta ja mielenrauhaa.

Lisätietoja

hp.com/go/printsecurity

¹ Turvallisin tulostus -väite perustuu HP:n vuonna 2017 tekemään arvioon julkistetuista suojausominaisuuksista saman luokan kilpailevissa laitteissa. Vain HP tarjoaa yhdistelmän suojausominaisuuksia, jotka voivat tarkkailla järjestelmää hyökkäyksen havaitsemiseksi ja pysäyttämiseksi automaattisesti ja sen jälkeen varmistaa ohjelmiston eheyden uudelleenkäynnistyksen yhteydessä. Luettelon tulostimista ja monitoimilaitteista näet osoitteessa: hp.com/go/PrintersThatProtect. Lisätietoja: hp.com/go/printersecurityclaims.

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

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

⁴ Spiceworksin HP:n puolesta tekemä kartoitus, joka koski 309:ää IT-alan päätöksentekijää Pohjois-Amerikassa sekä EMEA- ja APAC-alueilla marraskuussa 2016.

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

⁶ Ratkaisuja ei ehkä tueta kaikissa HP:n laitteissa; ratkaisujen ottaminen käyttöön voi edellyttää lisätarvikkeiden hankkimista.

⁷ HP:n kehittyneimmät sisäänrakennetut suojausominaisuudet ovat saatavina HP Enterprise -luokan laitteissa, joiden laiteohjelmisto on FutureSmart 4.5 tai uudempi. Perustuu HP:n vuosina 2017 tekemään arvioon julkistetuista suojausominaisuuksista saman luokan kilpailevissa laitteissa. Vain HP tarjoaa suojausominaisuusyhdistelmän, joka kattaa sekä eheystarkistuksen että BIOS-järjestelmän itsekorjaustoiminnot. Katso luettelo yhteensopivista tuotteista osoitteesta hp.com/go/PrintersThatProtect. Lisätietoja on osoitteessa hp.com/go/printersecurityclaims.

⁸ Tiettyjen HP LaserJet Pro- ja PageWide Pro -laitteiden upotetut ominaisuudet voivat tunnistaa ja pysäyttää hyökkäyksen. Lisätietoja on osoitteessa hp.com/go/PrintersThatProtect.

⁹ HP JetAdvantage Security Manager on hankittava erikseen. Lisätietoja on osoitteessa hp.com/go/securitymanager.

¹⁰ Kun tietoja lähetetään salasanalla suojattuun lopulliseen säilöön vaaditaan täydentävä salasana.

¹¹ HP JetAdvantage Connect toimii yleisimpien mobiililaitteiden kanssa. Android™-, Google Chrome™- ja Microsoft®-käyttöjärjestelmiä käyttäville laitteille on asennettava lisäohjelma (yhden kerran). Katso tiedot ja luettelo tuetuista käyttöjärjestelmistä osoitteesta hp.com/go/JetAdvantageConnect.

¹² HP JetAdvantage Secure Print: Pull printing -tulostus toimii minkä tahansa verkkoon liitetyn tulostimen tai monitoimilaitteen kanssa. Laitetason todentaminen on käytettävissä monissa HP:n LaserJet-, PageWide- ja OfficeJet Pro -laitteissa ja tietyissä muiden valmistajien laitteissa. Jotkin laitteet voivat vaatia laiteohjelmiston päivityksen. Pilvitallennus ja tulostustöiden noutaminen edellyttävät internetiyhteyttä. Tulostustöiden lähettäminen mobiililaitteesta edellyttää verkkoyhteyttä ja QR-koodia. Lisätietoja ja luettelo tuetuista tulostimista ja monitoimilaitteista: hp.com/go/JetAdvantageSecurePrint.

¹³ HP JetAdvantage Private Print on saatavilla maksutta, mutta sen käyttö edellyttää, että tulostin tai monitoimilaitte on yhteydessä Internetiin ja verkkopalvelut ovat käytössä. Ei saatavana kaikissa maissa. Lisätietoja on osoitteessa hp.com/go/JetAdvantagePrivatePrint.

¹⁴ Maksuton HP Web Jetadmin on ladattavissa osoitteesta hp.com/go/webjetadmin.

¹⁵ Perustuu IDC:n arvioon tulostustuotteiden toimittajista ja näkemykseen HP:n johtavasta asemasta: "HP:n etuna on sen vahvat IT-palvelut ja valmiudet ... se helpottaa myös kattavan ja integroidun, koko IT-infrastruktuuria koskevan tietoturvastrategian luontia." LÄHDE: [IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment](#), Allison Correia ja Robert Palmer, lokakuu 2017, IDC Doc #US41988517.

Tilaa päivitysilmoitukset

hp.com/go/getupdated



Jaa kollegoille

© Copyright 2014–2018 HP Development Company, L.P. Tämän asiakirjan sisältöä voidaan muuttaa ilman erillistä ilmoitusta. Ainoat HP:n tuotteita ja palveluja koskevat takuut mainitaan erikseen kyseisten tuotteiden ja palveluiden mukana toimitettavissa takuuehdoissa. Mitään tämän asiakirjan sisältöä ei tule käsittää lisätakuuksi. HP ei ole vastuussa asiakirjan teknisistä tai toimitusvirheistä tai puutteista.

Android ja Google Chrome ovat Google Inc:n rekisteröimiä tavaramerkkejä. Microsoft on Microsoft-yritysyhdyksen Yhdysvalloissa rekisteröimä tavaramerkki.

4AA3-1295FIE, tammikuu 2018, versio 11

