Panoramica della soluzione

Proteggete la vostra rete con la stampa più sicura al mondo[1]

Il 94%

delle imprese finanziarie afferma che la sicurezza di copiatrici/stampanti è importante o molto importante[2]

Il 61%

delle aziende ha segnalato almeno una violazione di dati nell'ambiente di stampa nell'ultimo anno[3]

Il 43%

delle aziende ignora le stampanti nell'ambito delle proprie pratiche di sicurezza degli endpoint[4]

Solo il 18% delle aziende monitora le proprie stampanti alla ricerca di minacce.[4]

Riconoscere i rischi nascosti

Il settore IT è costantemente impegnato nella protezione delle informazioni riservate, inclusi i dati relativi all'identità di dipendenti e clienti, in dispositivi e ambienti eterogenei. Sebbene molti reparti IT applichino misure di sicurezza rigorose ai singoli computer e alla rete, l'ambiente di imaging e stampa è spesso trascurato e pericolosamente esposto. In presenza di dispositivi non protetti, l'intera rete può essere esposta a un attacco informatico.

Riconoscere i costi potenziali

Anche una sola violazione della sicurezza può essere potenzialmente dispendiosa. La compromissione di informazioni private attraverso operazioni di stampa e imaging non protette potrebbe dare luogo a furti di identità, sottrazione di informazioni riservate, danni alla reputazione e all'immagine del brand e controversie legali. Inoltre, la mancata conformità normativa e legale potrebbe generare pesanti sanzioni.

HP può aiutarvi

Proteggete la vostra rete con la stampa più sicura al mondo..[1] Le stampanti HP sono costantemente protette: rilevano e bloccano le minacce continuamente, aggiornandosi per rispondere a nuove minacce. HP può aiutarvi ad automatizzare la protezione di dispositivi, dati e documenti con un ampio portfolio di soluzioni. I nostri esperti della sicurezza di stampa sono in grado di aiutarvi a sviluppare e implementare una strategia end-to-end per la sicurezza di imaging e stampa.

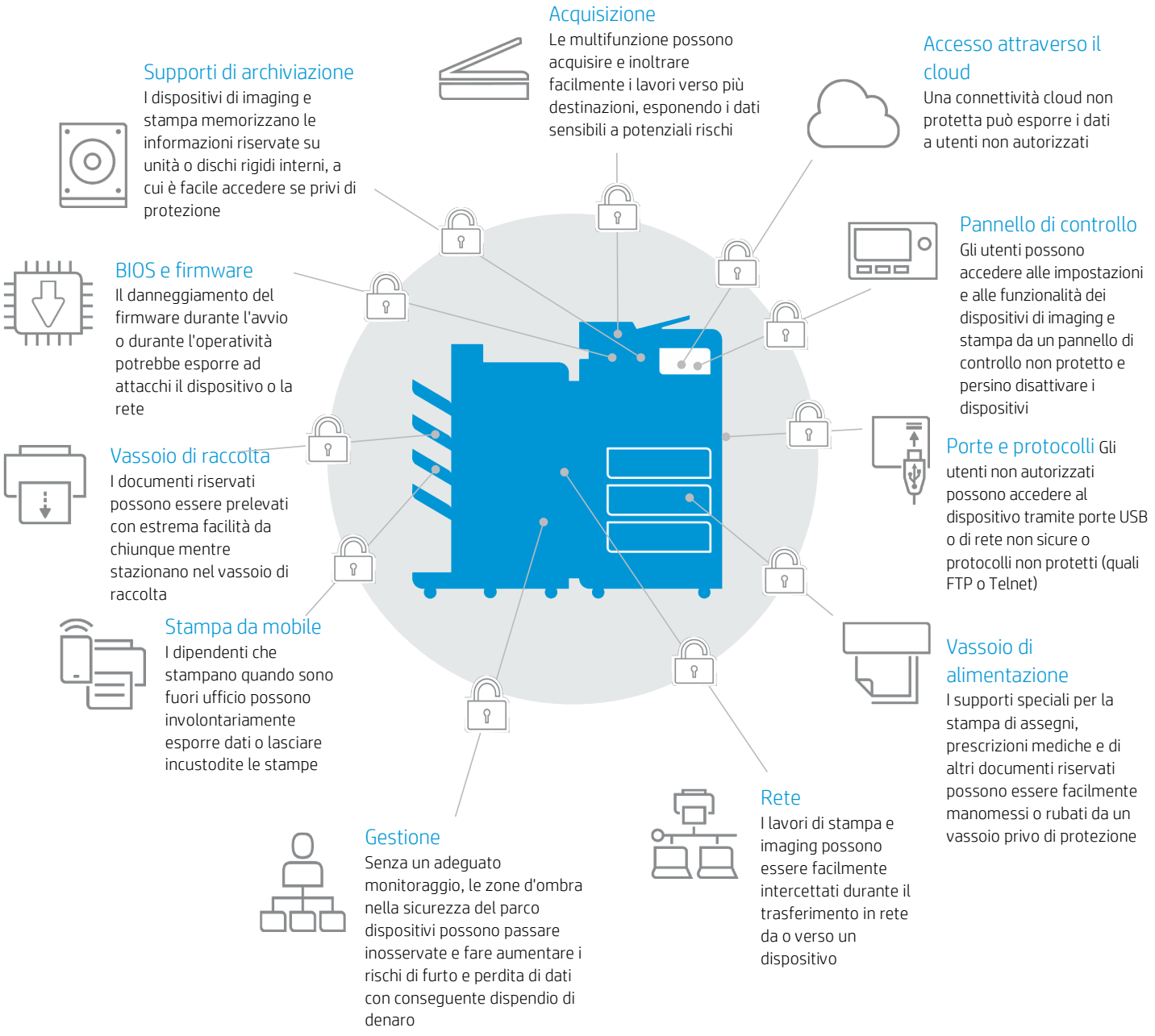
"A testimonianza del proprio investimento a lungo termine nella sicurezza di stampa, HP dispone del portfolio di soluzioni e servizi più ampio e dalle più avanzate funzionalità in materia di sicurezza presente sul mercato".

– Quocirca, gennaio 2017[5]

Proteggete dispositivi, dati e documenti.

Gravi criticità possono svilupparsi in più punti del vostro ambiente di imaging e stampa. Una volta individuati i punti vulnerabili, è più facile contenere i rischi.

Punti vulnerabili in ambiente di imaging e stampa



Acquisizione
Le multifunzione possono acquisire e inoltrare facilmente i lavori verso più destinazioni, esponendo i dati sensibili a potenziali rischi

Accesso attraverso il cloud
Una connettività cloud non protetta può esporre i dati a utenti non autorizzati

Supporti di archiviazione
I dispositivi di imaging e stampa memorizzano le informazioni riservate su unità o dischi rigidi interni, a cui è facile accedere se privi di protezione

Pannello di controllo
Gli utenti possono accedere alle impostazioni e alle funzionalità dei dispositivi di imaging e stampa da un pannello di controllo non protetto e persino disattivare i dispositivi

BIOS e firmware
Il danneggiamento del firmware durante l'avvio o durante l'operatività potrebbe esporre ad attacchi il dispositivo o la rete

Porte e protocolli
Gli utenti non autorizzati possono accedere al dispositivo tramite porte USB o di rete non sicure o protocolli non protetti (quali FTP o Telnet)

Vassoio di raccolta
I documenti riservati possono essere prelevati con estrema facilità da chiunque mentre stazionano nel vassoio di raccolta

Vassoio di alimentazione
I supporti speciali per la stampa di assegni, prescrizioni mediche e di altri documenti riservati possono essere facilmente manomessi o rubati da un vassoio privo di protezione

Stampa da mobile
I dipendenti che stampano quando sono fuori ufficio possono involontariamente esporre dati o lasciare incustodite le stampe

Rete
I lavori di stampa e imaging possono essere facilmente intercettati durante il trasferimento in rete da o verso un dispositivo

Gestione
Senza un adeguato monitoraggio, le zone d'ombra nella sicurezza del parco dispositivi possono passare inosservate e fare aumentare i rischi di furto e perdita di dati con conseguente dispendio di denaro

Protezione del dispositivo

Le stampanti HP sono progettate per lavorare in sinergia con le soluzioni di gestione e monitoraggio della sicurezza per contribuire a ridurre i rischi, migliorare la conformità e proteggere tutta la rete (non tutte le funzionalità e le soluzioni sono disponibili su tutti i dispositivi HP[6]).

Principali pratiche di sicurezza

Archiviazione crittografata con cancellazione sicura
Tutti i dati sensibili archiviati nell'unità o nel disco rigido interni sono potenzialmente esposti al furto. Numerosi dispositivi HP sono dotati di crittografia integrata per la protezione dei dati. Quando i dati archiviati non sono più necessari, le funzionalità integrate nei dispositivi consentono di sovrascrivere i dati e rimuovere i dati sensibili in tutta sicurezza.

Smaltimento sicuro
Con *HP Custom Recycling Services* è possibile garantire l'eliminazione dei dati dai dischi rigidi prima del riciclo responsabile dei prodotti obsoleti.

Accesso sicuro per la riparazione della stampante
La conoscenza delle pratiche di sicurezza dei fornitori di assistenza alle stampanti contribuirà a proteggere i dati sensibili. Affidatevi ad *HP Secure Managed Print Services (MPS)* o ai partner HP per usufruire dell'assistenza di esperti.

Disabilitazione di porte e protocolli inutilizzati
Riducete lo spazio vulnerabile con una configurazione adeguata dei dispositivi. Disabilitate le porte fisiche e i protocolli non sicuri (come FTP o Telnet) per impedire l'accesso o l'uso non autorizzato.

Controllo dell'accesso al dispositivo da parte dell'amministratore
Impostate password di amministratore affinché solo il personale IT o altro personale autorizzato possa configurare le impostazioni del dispositivo.

Whitelisting del codice del firmware
Alla pagina seguente sono disponibili le informazioni sull'utilizzo del whitelisting per proteggere il parco dispositivi dai malware.

Per saperne di più

HP Custom Recycling Services
hp.com/go/businessrecycling

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

Per saperne di più

Funzionalità integrate per la sicurezza di stampa:
- HP Sure Start (integrità del BIOS)
- Whitelisting del codice del firmware
- Rilevamento delle intrusioni durante l'operatività
- HP Connection Inspector

hp.com/go/PrintersThatProtect

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

Pratiche di sicurezza avanzate

Certificazione Common Criteria

Le stampanti aziendali HP sono dotate di certificazione di conformità agli standard di sicurezza riconosciuti a livello internazionale, come Common Criteria Certification (CCC) e FIPS 140. Assicuratevi che gli aggiornamenti del firmware del dispositivo siano firmati a livello di codice al fine di confermare l'autenticità e l'integrità dello stesso, mantenendo così la conformità.

Le funzionalità per la sicurezza di stampa rilevano e bloccano automaticamente gli attacchi

Le stampanti aziendali HP offrono funzionalità di sicurezza in grado di proteggere la stampante, impedendo che diventi un punto di accesso per gli attacchi in rete. Solo la sicurezza di stampa HP offre rilevamento in tempo reale, monitoraggio da remoto e convalida del software integrata per bloccare le minacce al loro verificarsi.[7]

Le stampanti aziendali HP, dalle Pro[8] alle Enterprise,[7] sono costantemente protette; rilevano e fermano continuamente le minacce durante tutte le fasi operative:

- **All'avvio.** Il codice di avvio (per i dispositivi Pro) o BIOS (per i dispositivi Enterprise) è rappresentato da una serie di istruzioni utilizzate per caricare i componenti hardware fondamentali e avviare il firmware. L'integrità del codice viene convalidata a ogni ciclo di avvio, consentendo la protezione del dispositivo dagli attacchi.
- **Al caricamento del firmware.** Il *whitelisting* verifica automaticamente il firmware durante l'avvio per determinare l'autenticità e la validità del codice con firma digitale di HP. In caso di rilevamento di anomalie, il dispositivo viene riavviato in uno stato offline sicuro, e l'IT viene avvisato.
- **Durante l'operatività.** Le funzionalità integrate di HP consentono la protezione della memoria dei dispositivi mentre sono accesi e connessi alla rete, ossia quando si verifica la maggior parte degli attacchi. Al verificarsi di un attacco, il dispositivo si arresta.

I dispositivi HP Enterprise hanno capacità di auto-riparazione

Oltre alla capacità di rilevare e fermare le minacce, le stampanti HP Enterprise eseguono l'auto-riparazione in seguito a un attacco, eliminando la necessità di intervento del personale IT.[7] Queste funzionalità generano automaticamente un riavvio al verificarsi di un attacco o un'anomalia. Gli amministratori possono riceverne notifica tramite strumenti SIEM (Security Information and Event Management) quali ArcSight, Splunk e SIEMonster.

- *HP Sure Start* è l'unico BIOS del settore con capacità di auto-riparazione.[7] Se il BIOS viene compromesso, HP Sure Start riavvia il dispositivo con una copia sicura del BIOS.
- Il *rilevamento delle intrusioni durante l'operatività* monitora le operazioni complesse legate al firmware e alla memoria, blocca automaticamente le intrusioni e riavvia il dispositivo al verificarsi di un attacco.
- *HP Connection Inspector* valuta le connessioni di rete in uscita per verificare il normale svolgimento delle attività, bloccare le richieste sospette e generare automaticamente un riavvio eseguendo l'auto-riparazione.

La protezione dell'investimento offerta dal firmware aggiornabile HP FutureSmart vi permette di aggiungere il whitelisting, il rilevamento delle intrusioni durante l'operatività e HP Connection Inspector a molte stampanti HP Enterprise esistenti.[7]

HP JetAdvantage Security Manager completa il ciclo di controllo

Una volta effettuato il riavvio, o in qualsiasi momento in cui venga aggiunto un nuovo dispositivo alla rete, *HP JetAdvantage Security Manager* esegue una valutazione automatica e, se necessario, ripristina le impostazioni di sicurezza del dispositivo conformemente ai criteri di configurazione aziendali prestabiliti.[9] L'intervento del personale IT non è più necessario.

Come funziona?

Le funzionalità di sicurezza integrate gestiscono i quattro passaggi fondamentali del funzionamento di un dispositivo HP.

In caso di attacco, i dispositivi HP Enterprise possono riavviarsi ed eseguire l'auto-riparazione.

HP JetAdvantage Security Manager completa il ciclo di controllo.

Uno. Verifica del codice BIOS/di avvio

Previene l'esecuzione di codice dannoso durante l'avvio consentendo solo il caricamento di codice autentico firmato da HP.

Due. Verifica del firmware

Consente di caricare solo firmware autentico e valido,— firmato digitalmente da HP

Tre. Verifica delle impostazioni

Dopo un riavvio, HP JetAdvantage Security Manager verifica e corregge tutte le impostazioni di sicurezza del dispositivo oggetto di attacco.

Quattro. Monitoraggio continuo

Protegge le operazioni e blocca gli attacchi mentre il dispositivo è in funzione.

Ispeziona le connessioni di rete in uscita per bloccare le richieste sospette (solo Enterprise).

Protezione dei dati

Archiviati o in transito, i dati richiedono una protezione costante. Di seguito vengono elencate alcune misure essenziali per la sicurezza dei dati durante il loro trasferimento e il loro utilizzo.[6]

Principali pratiche di sicurezza

Standard di rete 802.1x o IPsec
Utilizzate standard di rete crittografati per proteggere i dati che in transito sulla rete tra il dispositivo e gli strumenti di gestione, come *HP Web Jetadmin* o *HP Embedded Web Server*.

Crittografia dei dati in transito
Proteggete i processi di stampa inviati al dispositivo con protocolli di crittografia quali Internet Print Protocol over TLS (IPPS). In alternativa, *HP Universal Print Driver Secure Encrypted Print* offre autentiche funzioni di crittografia e decrittografia AES256 simmetrica dei processi di stampa, dal client alla pagina, sulla base di una password definita dall'utente, utilizzando librerie crittografiche conformi ai requisiti FIPS 140 di Microsoft®.

Durante la scansione, con *HP JetAdvantage Workflow Solutions* è possibile facilitare la protezione dei dati sensibili incrementando l'efficienza. Ad esempio, HP Capture and Route si integra perfettamente con HP Access Control per offrire maggiore sicurezza, con la praticità di un'unica autenticazione e la possibilità di monitorare il contenuto per la governance delle informazioni.[10]

Crittografia dei dati stazionari
Proteggete le informazioni aziendali riservate archiviate sul disco rigido avvalendovi della crittografia integrata. Per un livello supplementare di sicurezza, è possibile aggiungere al dispositivo l'accessorio opzionale HP Trusted Platform Module (TPM), per rafforzare la protezione delle credenziali e dei dati crittografati sigillando automaticamente le chiavi di crittografia del dispositivo nel modulo TPM. Il modulo garantisce la protezione dell'identità del dispositivo generando e proteggendo le chiavi private del certificato.

Protezione del firewall
Impedite l'accesso alla rete da parte di malware e virus, limitando l'accesso alla stampante ai computer in rete.

Autenticazione utente nativa
Riducete i costi e i rischi associati alla sicurezza imponendo agli utenti di accedere con autenticazione Kerberos, PIN/PIC o LDAP. È inoltre possibile integrare queste funzionalità con Active Directory.

Controlli di accesso basati su ruoli
HP Access Control Rights Management contribuisce a ridurre i costi e i rischi legati alla sicurezza attraverso restrizioni alle funzionalità della stampante. I controlli di accesso basati su ruoli consentono di attribuire a utenti differenti, o persino a interi reparti, capacità differenti a seconda delle rispettive necessità. Ad esempio, è possibile limitare gli utenti che possono inviare fax o inviare scansioni tramite e-mail o fax.

Per saperne di più

HP Web Jetadmin
hp.com/go/wja

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

Soluzioni per flussi di lavoro HP JetAdvantage
hp.com/go/documentmanagement

HP Access Control
hp.com/go/hpac

Per saperne di più

HP Access Control
hp.com/go/hpac

HP JetAdvantage Connect
hp.com/go/JetAdvantageConnect

HP Capture and Route
hp.com/go/hpcr

Pratiche di sicurezza avanzate

Autenticazione e monitoraggio avanzati

Implementate soluzioni avanzate di autenticazione (password, badge di prossimità, smart card o funzioni biometriche) e monitoraggio per offrire maggiore sicurezza e controllo.

- *HP Access Control Secure Authentication* vi consente di riassumere il controllo, potenziare la sicurezza e ridurre i costi. Ottenete un ampia gamma di opzioni e controlli avanzati, tra cui la funzione touch-to-authenticate per i dispositivi mobile con funzioni NFC.
- *HP Access Control Job Accounting* permette di monitorare e raccogliere i dati con precisione, analizzare i risultati e quindi creare e inviare rapporti. I dati estratti possono essere utilizzati per ripartire i costi di stampa, motivare i dipendenti a stampare in modo più razionale e fornire all'IT le informazioni necessarie per migliorare le previsioni relative al parco dispositivi.

Dispositivi mobile inclusi nell'accesso alla rete

Inserite i dispositivi mobile nelle vostre policy di protezione della stampa per ottenere il controllo degli accessi alla stampante. HP offre soluzioni basate su server che forniscono una stampa pull sicura, oltre a funzionalità avanzate di gestione e creazione di rapporti.

- *HP JetAdvantage Connect* offre una stampa da mobile intuitiva e affidabile, progettata per il business. Consente di risparmiare tempo e denaro sfruttando direttamente gli strumenti e le policy di rete IT esistenti per gestire la stampa da mobile.[11] Gli utenti possono stampare in tutta sicurezza da un'ampia gamma di smartphone e tablet (ovunque e in qualsiasi momento, in base alle proprie esigenze) con la stessa facilità della stampa da PC.
- *HP Access Control* include funzionalità per la gestione della stampa da mobile. Sfrutta l'infrastruttura di posta elettronica esistente, consentendo agli utenti mobili di inviare tramite e-mail un lavoro alla coda di stampa, quindi di recuperarlo da una qualsiasi stampante o multifunzione abilitata alla soluzione. Proteggete i dispositivi di stampa in rete con funzionalità di autenticazione sicura quali Mobile Release.

Blocco della fuga di dati prima ancora che si verifichi

Le soluzioni HP offrono funzionalità di protezione per scongiurare la perdita di dati. Con la prevenzione di *HP Capture and Route Data Loss*, è possibile impedire l'acquisizione o l'invio tramite fax di informazioni riservate. La funzionalità di *HP Access Control per la prevenzione* della perdita dei dati durante i processi di stampa impedisce la stampa di documenti riservati. Monitorate i dati più importanti per scoraggiare e prevenire le violazioni, senza rallentare i flussi di lavoro. Mostrate avvisi di sicurezza intelligenti, basati sulle condizioni specificate dall'utente.

Applicazione di certificati digitali alle stampanti

Migliorate la sicurezza dell'ambiente di stampa applicando certificati digitali alle stampanti e ai dispositivi multifunzione in rete. Risparmiate tempo utilizzando HP JetAdvantage Security Manager per installare e rinnovare automaticamente i certificati.[9]

Protezione dei documenti

Integrate soluzioni hardware e software intelligenti con il vostro ampio piano di sicurezza IT al fine di proteggere le informazioni riservate della vostra documentazione stampata.[6]

Principali pratiche di sicurezza

Controllo dell'accesso ai moduli prestampati
Dotando stampanti e multifunzione con vassoi di alimentazione con blocco potrete evitare che i supporti speciali utilizzati per stampare assegni, prescrizioni mediche o altri documenti riservati vengano rubati.

Stampa pull o con PIN opzionale per proteggere i documenti riservati
Gli utenti possono scegliere la stampa pull o con PIN per ridurre sia il ricorso alle stampanti personali sia i rischi legati al prelievo dei documenti stampati da parte di persone non autorizzate. Queste misure di sicurezza riducono anche il problema delle stampe non ritirate, con conseguente riduzione di costi e sprechi.

Per la stampa con PIN, gli utenti che stampano documenti riservati assegnano loro un PIN, che successivamente dovrà essere immesso sul dispositivo per sbloccare il processo.

La stampa pull memorizza i processi di stampa nel cloud o sul PC dell'utente. Gli utenti eseguono l'autenticazione presso il punto di stampa prescelto per recuperare e stampare i loro processi. HP propone due soluzioni di stampa pull basata su cloud:

- *HP JetAdvantage Secure Print* è una soluzione conveniente progettata per PMA, che memorizza i processi nel cloud o sul desktop dell'utente. È facile da configurare e utilizzare, permette agli utenti di avviare la stampa da un dispositivo mobile e supporta i dispositivi multivendor.[12]
- *HP JetAdvantage Private Print* è la soluzione gratuita di HP basata sul cloud, che offre i vantaggi della stampa pull eliminando le complessità. È di facile configurazione e non richiede server, installazione o manutenzione.[13]

Pratiche di sicurezza avanzate

Necessità di stampa pull per tutti i processi di stampa
HP Access Control Secure Pull Printing contribuisce a proteggere le informazioni riservate, offre maggiore sicurezza dei dispositivi e incrementa l'efficienza. Questa efficace soluzione basata su server offre più forme di autenticazione, tra cui l'emissione di badge e funzionalità di protezione e gestione di livello enterprise.

MICR, filigrane e altre funzionalità per evitare copie e modifiche
Le soluzioni anti-contraffazione HP e TROY includono l'impiego di toner di sicurezza che macchia la carta se viene alterato con sostanze chimiche, l'aggiunta di filigrane con dati variabili alle pagine stampate e l'inserimento di codici che il computer sia in grado di leggere per tenere traccia dei singoli documenti e verificarne l'autenticità. Le multifunzione possono integrare funzionalità anti-frode, quali firme personalizzate, loghi societari e font di sicurezza, nei documenti stampati che contengono dati sensibili, come prescrizioni mediche, certificati di nascita o copie autenticate.

Per saperne di più

HP JetAdvantage Secure Print
hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Private Print
hp.com/go/JetAdvantagePrivatePrint

HP Access Control
hp.com/go/hpac

Protezione dei documenti con HP e TROY
hp.com/go/HPandTROY

Monitoraggio e gestione dell'ambiente di stampa

Le soluzioni di gestione e monitoraggio della sicurezza sono in grado di aiutarvi a individuare le vulnerabilità e a definire una strategia unificata basata su policy per proteggere i dati, ridurre i rischi e mantenere la conformità.[6] Potrete così evitare criticità nella protezione e costose sanzioni.

Principali pratiche di sicurezza

Aggiornamento dei dispositivi con gli ultimi firmware/sistemi operativi
Utilizzate HP Web Jetadmin[14] per inserire aggiornamenti firmware all'interno del parco stampanti, assicurando che i dispositivi siano aggiornati con le ultime funzionalità di protezione e di sicurezza.

Revisione dei registri eventi per la sicurezza della stampante
I dispositivi HP inviano eventi e notifiche della stampante a un server syslog per consentire all'IT di risolvere eventuali problemi.

Valutazione e correzione delle impostazioni dei dispositivi
Gestite le impostazioni di sicurezza di base delle stampanti del parco dispositivi con *HP Print Manageability Integration Kit* (MIK), un plug-in per Microsoft® System Center Configuration Manager (SCCM). Microsoft SCCM è una soluzione di gestione ampiamente utilizzata per pianificare, implementare, configurare e monitorare gli endpoint da remoto. HP Print MIK può individuare, valutare e correggere le 15 impostazioni di protezione più importanti e comunicare i risultati.

Per una gestione completa della sicurezza del parco dispositivi, scegliete *HP JetAdvantage Security Manager*.[9] Questa soluzione consente di ridurre i costi e le risorse necessari per definire criteri di sicurezza di tutto il parco dispositivi, automatizzare la correzione delle impostazioni dei dispositivi, installare e rinnovare i certificati univoci e fornire i rapporti necessari per dimostrare la conformità.

Per saperne di più

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Per saperne di più

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Pratiche di sicurezza avanzate

Implementazione del software SIEM per rilevare e documentare le minacce
I dati relativi agli eventi dei dispositivi HP FutureSmart possono essere inviati a strumenti di rilevamento degli incidenti, quali ArcSight, Splunk e SIEMonster, per il monitoraggio in tempo reale. La sicurezza IT può in tal modo visualizzare gli endpoint di stampa nell'ambito di un più ampio ecosistema IT, per rilevare gli avvisi e risolvere le criticità relative alla sicurezza delle stampanti.

Configurazione automatica dei nuovi dispositivi di stampa aggiunti alla rete
La funzionalità Instant-on Security di HP JetAdvantage Security Manager permette di configurare automaticamente i dispositivi aggiungi alla rete, sia durante l'aggiunta sia dopo un riavvio.

Rapporto di conformità alle normative della sicurezza del parco stampanti
HP JetAdvantage Security Manager consente di creare rapporti sulla conformità per dimostrare l'applicazione dei criteri di sicurezza alle stampanti e proteggere i dati dei clienti.

Una violazione della conformità può danneggiare il business

Gli endpoint non protetti, o protetti in modo non efficace, offrono maggiori opportunità alla criminalità informatica. Per contribuire a contrastare la minaccia crescente, gli enti governativi di tutto il mondo stanno implementando norme di sicurezza più rigorose che impongono alle aziende di proteggere meglio i dati dei clienti.

Le aziende non conformi potrebbero trovarsi ad affrontare costi elevatissimi, dovuti a sanzioni, perdita di affari, danni alla reputazione e azioni legali collettive.

È fondamentale implementare dispositivi e soluzioni, come le stampanti HP Enterprise e HP JetAdvantage Security Manager, in grado di fornire la conformità normativa e proteggere le informazioni aziendali dalle minacce alla sicurezza.

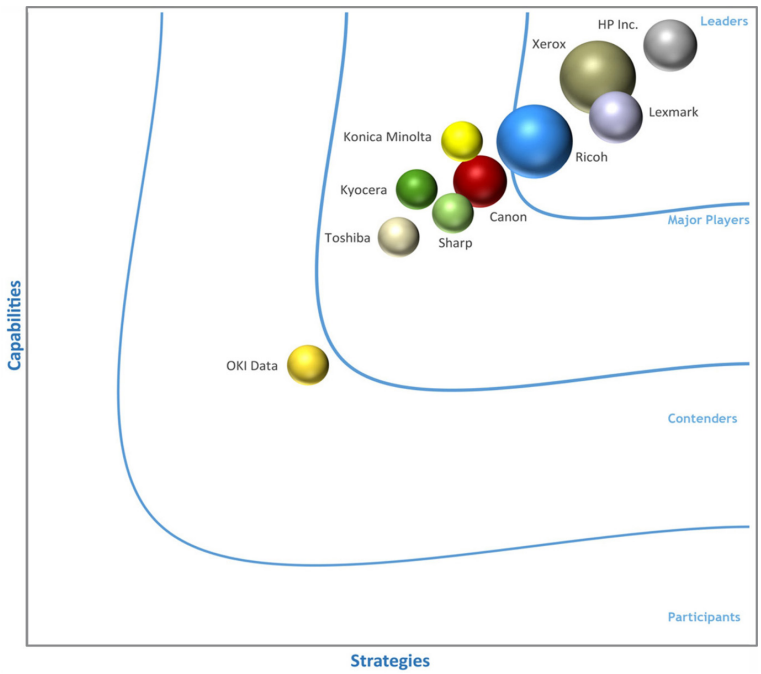
Tutto l'aiuto di cui avete bisogno

Non dovete essere voi a proteggere e rendere sicuri i dispositivi. Un team di assistenza composto da consulenti esperti può mostrarvi come migliorare la sicurezza dei vostri dati, dispositivi e documenti.

Collaborate con gli esperti della sicurezza di stampa per valutare le vostre attuali vulnerabilità. Possiamo aiutarvi a creare policy complete per la protezione dei vostri dispositivi basate sulle esigenze aziendali e le best practice, e a elaborare un piano per ottenere una sicurezza ottimizzata all'interno del vostro ambiente.

Leader riconosciuto nel settore

HP è stata inserita fra i leader nel primo report IDC MarketScape Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment (il report è consultabile qui). In base al report, "l'approccio di HP Inc. alla sicurezza tiene conto dell'intera infrastruttura di gestione documenti e stampa, cominciando dal blocco del dispositivo e continuando con tutti gli aspetti del suo utilizzo e della protezione dei contenuti." Il grafico qui riportato è tratto dall'IDC 2017 Vendor Assessment.[15]



Il modello analitico dei fornitori IDC MarketScape è progettato per fornire una panoramica della competitività dei fornitori ICT in un determinato mercato. La metodologia di ricerca utilizza un rigoroso metodo di assegnazione dei punteggi basato su criteri sia qualitativi che quantitativi, risultante in un'illustrazione grafica della posizione di ciascun fornitore all'interno di un determinato mercato. Il punteggio Capacità analizza il prodotto del fornitore, l'immissione sul mercato e l'esecuzione commerciale nel breve termine. Il punteggio Strategia analizza l'allineamento delle strategie del fornitore ai requisiti dei clienti in un periodo di tempo da 3 a 5 anni. La quota di mercato dei fornitori è rappresentata dalla dimensione delle icone.[15]

Per iniziare

Contattate il vostro referente commerciale per maggiori informazioni sulle funzionalità, le soluzioni e i servizi per la sicurezza HP e per definire il vostro percorso verso una maggiore protezione e serenità.

Per saperne di più
hp.com/go/printsecurity

[1] La stampa più sicura al mondo. Sulla base di verifiche HP pubblicate nel 2017 sulle funzionalità di sicurezza nelle stampanti della stessa categoria di produttori concorrenti. Solo HP offre una combinazione di funzionalità di sicurezza in grado di eseguire il monitoraggio, rilevare e bloccare automaticamente un attacco, quindi di convalidare automaticamente l'integrità del software mediante il riavvio. Per un elenco di stampanti, consultare hp.com/go/PrintersThatProtect. Per maggiori informazioni: hp.com/go/printersecurityclaims.

[2] InfoTrends, "Designing Hardware & Solutions", Brendan Morse, ottobre 2016.

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

[4] Sondaggio Spiceworks su 309 decision-maker IT in Nord America, EMEA e APAC per conto di HP, novembre 2016.

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

[6] Le soluzioni potrebbero non essere supportate da tutti i dispositivi HP; alcune soluzioni potrebbero richiedere l'acquisto separato.

[7] Le più avanzate funzionalità di sicurezza integrate di HP sono disponibili sui dispositivi HP di classe Enterprise con firmware FutureSmart 4.5 o superiore; l'affermazione si basa su analisi HP, pubblicate nel 2017, sulle funzionalità di sicurezza nelle stampanti concorrenti della stessa categoria. Solo HP offre una combinazione di funzionalità di sicurezza per la verifica dell'integrità del BIOS con capacità di auto-riparazione. Per un elenco dei prodotti compatibili, consultare hp.com/go/PrintersThatProtect. Per maggiori informazioni, consultare hp.com/go/printersecurityclaims.

[8] Una selezione di dispositivi HP LaserJet Pro e PageWide Pro include funzionalità integrate in grado di rilevare e bloccare un attacco. Per maggiori informazioni, consultare hp.com/go/PrintersThatProtect.

[9] HP JetAdvantage Security Manager deve essere acquistato separatamente. Per maggiori informazioni, consultare hp.com/go/securitymanager.

[10] Per l'invio di informazioni a un repository finale protetto da password è necessaria una password supplementare.

[11] HP JetAdvantage Connect è compatibile con i principali dispositivi mobile. È necessario installare un plug-in iniziale nei dispositivi con sistemi operativi Android™, Google Chrome™ e Microsoft®. Per maggiori informazioni e per un elenco dei sistemi operativi supportati, consultare hp.com/go/JetAdvantageConnect.

[12] HP JetAdvantage Secure Print: la stampa pull è compatibile con qualsiasi stampante o multifunzione collegata in rete. L'autenticazione sul dispositivo è disponibile per numerosi dispositivi HP LaserJet, PageWide e OfficeJet Pro e per alcuni dispositivi non HP. Alcuni dispositivi potrebbero richiedere un aggiornamento del firmware. Connessione Internet richiesta per l'archiviazione e il recupero dei lavori di stampa dal cloud. La stampa da un dispositivo mobile richiede una connessione di rete e un codice QR. Per maggiori informazioni e per un elenco di stampanti e multifunzione supportate, consultare hp.com/go/JetAdvantageSecurePrint.

[13] HP JetAdvantage Private Print è disponibile gratuitamente e richiede la connessione della stampante a Internet con i servizi Web attivati. Non è disponibile in tutti i paesi. Per maggiori informazioni, consultare hp.com/go/JetAdvantagePrivatePrint.

[14] HP Web Jetadmin è disponibile gratuitamente per il download all'indirizzo hp.com/go/webjetadmin.

[15] In base all'analisi di IDC sui resoconti dei fornitori e sulle opinioni riguardanti la leadership di HP: "Il vantaggio di HP è dovuto alla validità del servizio e delle funzionalità IT...che agevola una strategia di protezione completa e integrata nell'intera infrastruttura IT." FONTE: IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment, by Allison Correia and Robert Palmer, ottobre 2017, IDC Doc #US41988517.

Registratevi per ricevere gli aggiornamenti
hp.com/go/getupdated

Condividete questo documento con i colleghi

4AA3-1295ITE, gennaio 2018, Rev. 11