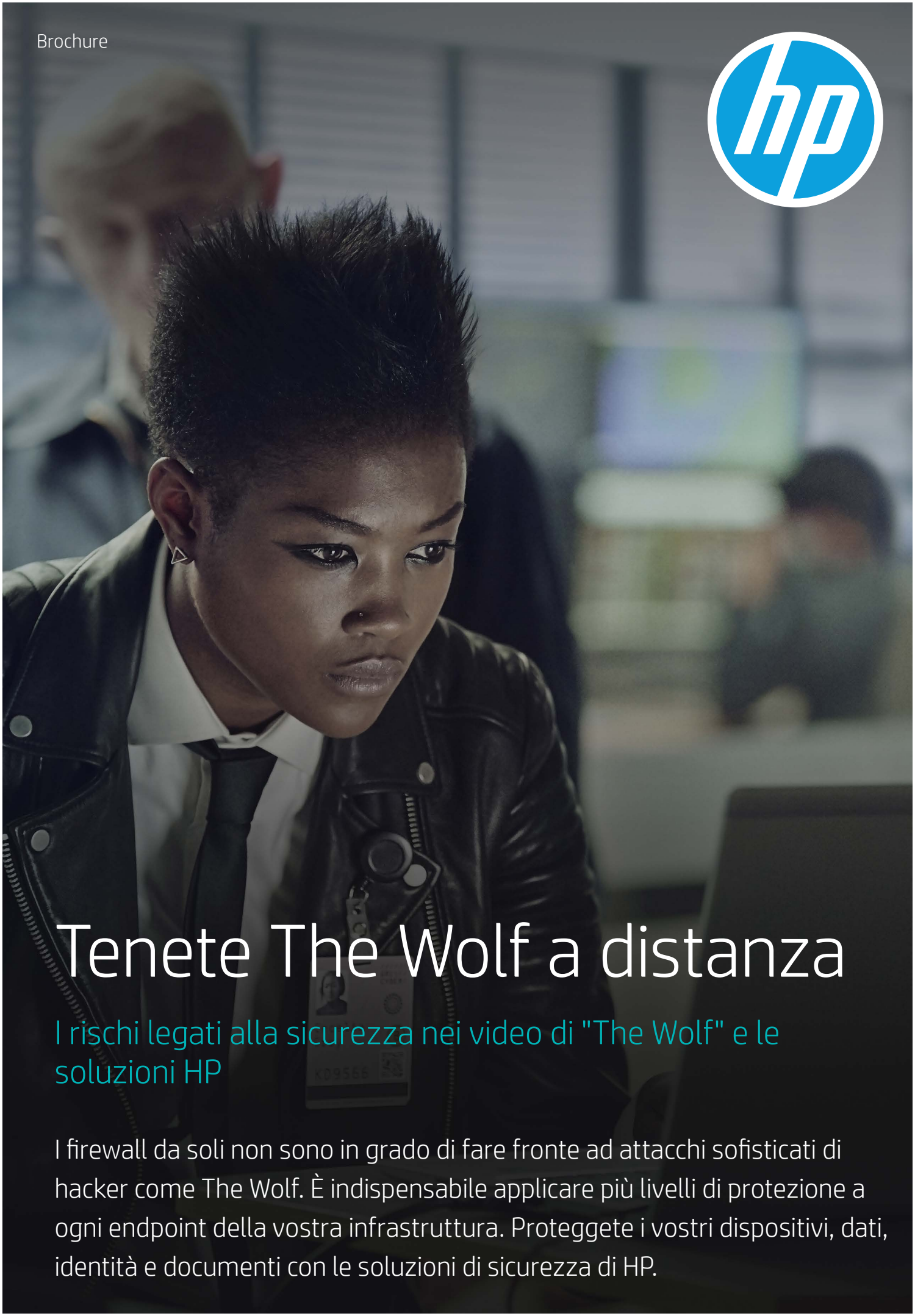
Brochure



Tenete The Wolf a distanza

I rischi legati alla sicurezza nei video di "The Wolf" e le soluzioni HP

I firewall da soli non sono in grado di fare fronte ad attacchi sofisticati di hacker come The Wolf. È indispensabile applicare più livelli di protezione a ogni endpoint della vostra infrastruttura. Proteggete i vostri dispositivi, dati, identità e documenti con le soluzioni di sicurezza di HP.

Stagione 1 The Wolf

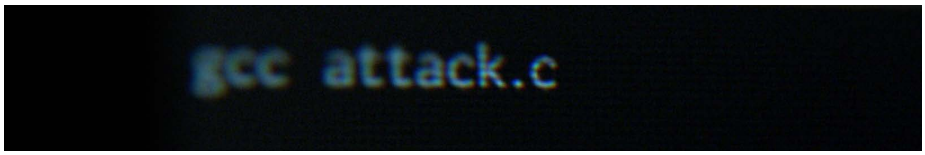
The Wolf mette fuori gioco un istituto finanziario internazionale sfruttando le vulnerabilità degli endpoint. Utilizza un dispositivo mobile per accedere a una stampante e installare un malware per intercettare e leggere i dati. Con un'e-mail di "phishing", The Wolf induce con l'inganno un utente a inviare a una stampante un codice dannoso nascosto in un file PDF.

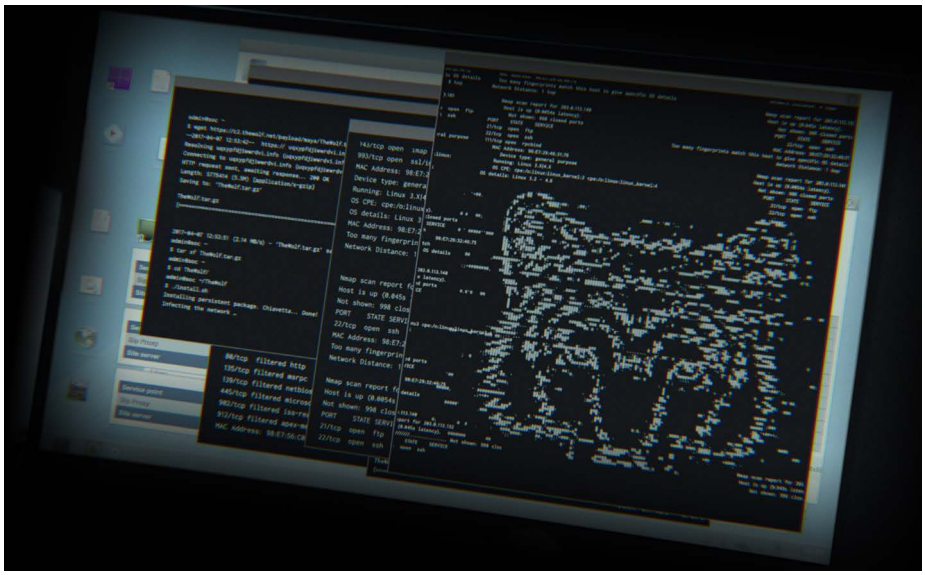
Il malware supera il firewall della stampante e raggiunge i PC dell'azienda compromettendone il BIOS, raccogliendo i dati e persino ripristinandosi dopo l'implementazione delle difese della rete.

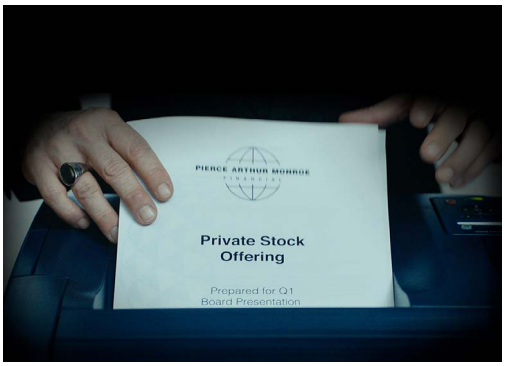
The Wolf si impadronisce di una stampa abbandonata prelevandola dal vassoio di raccolta della stampante e compromette la successiva negoziazione di Borsa della società, annientando in questo modo la fiducia degli azionisti.

Vulnerabilità

- Il Wi-Fi o il Bluetooth® della stampante sono aperti e non richiedono l'autenticazione degli utenti
- I file di dati della stampante non sono crittografati
- Gli utenti non riconoscono le e-mail e i file di stampa sospetti
- Le stampanti e i PC non sono dotati di protezione da malware a livello del BIOS
- I documenti riservati rimangono incustoditi nei vassoi di raccolta







Stagione 2 La caccia continua

The Wolf prende di mira i dati e le informazioni di pazienti archiviati in una delle più grandi società di gestione di cartelle cliniche al mondo. Viola un PC, quindi utilizza la porta USB di una stampante per caricare il malware superando il firewall, alla ricerca di dispositivi connessi da compromettere.

Poiché la stampante non risiede su una rete dedicata, The Wolf può accedere ai server e ai database contenenti dati sensibili. Si impadronisce di milioni di cartelle cliniche di pazienti, leggibili in quanto non crittografate.

L'ospedale e la società informatica sono entrambi responsabili e subiscono sanzioni pecuniarie significative, oltre ad aver compromesso la propria reputazione.

Vulnerabilità

- La porta USB della stampante non richiede l'autenticazione
- I file di dati non sono crittografati
- Le stampanti e i PC non sono dotati di protezione da malware
- Le stampanti non sono monitorate per rilevare eventuali problemi alla sicurezza

Stagione 3 True Alpha

The Wolf compromette l'operatività di una delle più grandi compagnie di navigazione e di un aeroporto internazionale.

Inviando per e-mail un file PDF apparentemente innocuo, fa in modo che un impiegato della compagnia di navigazione mandi in stampa un file infetto. Il malware nascosto si diffonde in tutta la rete quando il file viene inviato alla stampante, dove rimane inosservato. Ben presto The Wolf riesce ad accedere alla presentazione di un'importante conferenza del CEO, prendere il controllo delle operazioni di carico delle merci in un porto e del software del pilota automatico utilizzato dalle navi in mare.

In seguito, The Wolf prende di mira uno dei maggiori aeroporti, ostentando la propria capacità di controllare le luci, e potenzialmente i sistemi critici nella rete dell'aeroporto. Con il contributo delle stampanti HP, lo staff IT ha individuato e bloccato l'attacco.

Vulnerabilità

- Le stampanti installate temporaneamente vengono aggiunte alla rete senza un'adeguata configurazione che tenga conto della sicurezza
- I PC non sono dotati di sistemi di protezione da download accidentali durante l'esplorazione del Web
- I dispositivi IoT non sono monitorati né dotati di funzionalità di rilevamento dei malware
- I syslog delle stampanti non sono collegati agli strumenti di monitoraggio delle minacce

Come proteggersi da simili attacchi?

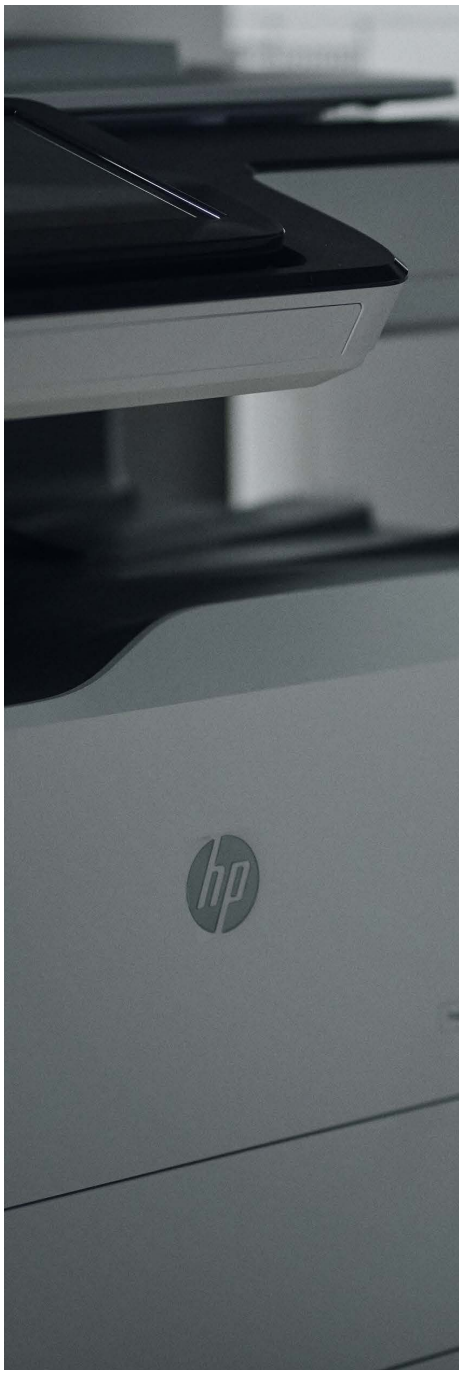
Protezione dell'identità: migliorare la sicurezza degli accessi con l'autenticazione avanzata sui PC HP Elite.

Protezione dei dispositivi: scegliere i PC HP Elite, le stampanti e le multifunzione HP Enterprise dotate di protezione da malware per rilevare, bloccare e ripristinare il sistema automaticamente in seguito a un attacco. Disabilitare le porte USB inutilizzate o gestire l'accesso mediante controlli utente. Isolare fisicamente le schede del browser con HP Sure Click per impedire che il dispositivo subisca attacchi malware web-based, che possono conaminare il resto dell'hardware.[1]

Protezione dei dati: applicare una soluzione per l'autenticazione e la crittografia come HP Access Control.[2] Richiedere l'autenticazione dell'utente e la crittografia dei dati quando si utilizzano stampanti con funzionalità Wi-Fi e Bluetooth. Implementare una soluzione di autenticazione e crittografia per dispositivi mobile come PrinterOn Enterprise. Crittografare i dati archiviati e in transito sulla rete.

Protezione dei documenti: implementare una soluzione di pull print, come HP Access Control.[2]

Ottimizzazione del monitoraggio e della gestione: configurare automaticamente le policy di sicurezza del parco dispositivi con HP JetAdvantage Security Manager[3] o HP Printer Security Plug-in for Microsoft® SCCM per stampanti e HP Manageability Integration Kit (MIK)[4] per PC. Abilitare i syslog per monitorare gli eventi legati alla sicurezza e connettere i dispositivi agli strumenti Security Information and Event Management (SIEM) per gli avvisi in tempo reale. Rivolgersi a un fornitore di soluzioni HP MPS esperto in sicurezza per la configurazione e la manutenzione delle stampanti, con particolare attenzione alla sicurezza.



Proteggete la vostra azienda con la sicurezza completa di HP

La stampa più sicura al mondo[5]

Le stampanti e le multifunzione HP Enterprise sono in grado di rilevare, bloccare ed effettuare il ripristino automatico in seguito a un attacco senza alcun intervento da parte dell'IT, grazie a funzionalità quali il rilevamento delle intrusioni durante l'operatività, HP Sure Start e HP Connection Inspector. Le altre protezioni includono le unità disco rigido crittografate, il firmware aggiornabile e la possibilità di inviare avvisi di sicurezza agli strumenti SIEM.

hp.com/go/PrintersThatProtect

I PC più sicuri e gestibili al mondo[6]

I PC HP Elite offrono protezione dalle minacce più diffuse proteggendo il sistema operativo ad ogni livello. L'autenticazione multifattoriale potenzia la protezione delle identità e il kit HP Management Integration[4] semplifica la gestione della sicurezza di tutto il parco PC. Altri sistemi di sicurezza includono la crittografia del disco rigido, HP Sure Recover,[7] HP Sure Click [1] e HP Sure View.

hp.com/go/ComputerSecurity

PrinterOn Enterprise

Stampa da mobile in rete affidabile e sicura per le aziende. Permette di collegare virtualmente tutti i dispositivi desktop o mobile alle stampanti di fornitori diversi all'interno e all'esterno di una rete affidabile.

hp.com/go/businessmobileprinting

HP Access Control[2]

Consente di ripristinare il controllo, potenziare la sicurezza e ridurre i costi fornendo autenticazione della stampa basata su ruoli, funzionalità di autorizzazione e pull print sicura in tutta l'azienda.

hp.com/go/hpac

HP JetAdvantage Security Manager[3]

Consente di ridurre costi e risorse assicurando nel contempo la sicurezza del parco dispositivi, grazie a uno strumento completo di conformità alla policy di sicurezza della stampa. Permette di definire una policy di sicurezza valida per tutto il parco stampanti, di automatizzare la correzione delle impostazioni dei dispositivi, di installare ed esaminare i certificati univoci e creare report sulla conformità per tutti i dispositivi.

hp.com/go/securitymanager

Per saperne di più:
hp.com/go/hpsecure

[1] HP Sure Click è disponibile sulla maggior parte delle piattaforme HP e supporta Microsoft® Internet Explorer e Chromium™. Gli allegati supportati includono Microsoft Office (Word, Excel, PowerPoint) e i file PDF in modalità di sola lettura, quando sono installati Microsoft Office o Adobe Acrobat.

[2] HP Access Control deve essere acquistato separatamente. Per maggiori informazioni consultare hp.com/go/hpac.

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

[4] HP Manageability Integration Kit non è preinstallato ed è disponibile all'indirizzo hp.com/go/clientmanagement.

[5] In base a una verifica HP del 2018 sulle funzionalità di sicurezza integrate nelle stampanti della stessa categoria pubblicate dalla concorrenza. 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.

[6] In base alle funzionalità di sicurezza uniche e complete di HP senza costi aggiuntivi, e alla gestione da parte di HP Manageability Integration Kit di ogni aspetto di un PC, compresi hardware, BIOS e software, tramite Microsoft® System Center Configuration Manager, tra venditori con vendite annue >1 milione di unità a novembre 2016 su PC HP Elite con processori Intel® Core® di settima generazione e superiori, scheda grafica Intel® integrata e Intel® WLAN.

7 HP Sure Recover è disponibile su PC HP Elite con processori Intel® o AMD di ottava generazione e richiede una connessione di rete aperta e cablata. Non disponibile su piattaforme con più unità di archiviazione interne, Intel® Optane™. È necessario eseguire il backup di file, dati, foto, video e altri documenti importanti per prevenire la perdita di dati.

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

Condividete questo documento con i colleghi

4AA7-0231ITE, agosto 2018, Rev. 1