



Sicurezza per le stampanti HP DesignJet

Le minacce alla sicurezza evolvono di giorno in giorno. Tutti i dispositivi collegati a una rete aziendale, e quindi anche le stampanti di rete, comprese quelle per grandi formati, costituiscono un punto di vulnerabilità.



Il 64%

dei responsabili IT dichiara che le proprie stampanti sono probabilmente infette da malware¹



Il 73%

dei CISO (i responsabili della sicurezza delle informazioni) prevede una violazione significativa della sicurezza entro un anno²



Il 26%

di tutte le violazioni di dati di una certa importanza riferite dai responsabili IT interessava le stampanti³

Clienti destinatari

Organizzazioni di ogni dimensione, area geografica e settore, con l'esigenza di proteggere gli ambienti condivisi di imaging e stampa.

Contatti destinatari

- CISO (Chief Information Security Officer) o Responsabile della sicurezza IT
- CIO
- Responsabili sicurezza/conformità
- Responsabili e decision maker IT

Caratteristiche dei clienti ideali

- Requisiti di sicurezza sempre più complessi a causa delle minacce e della conformità alle normative
- Non possono accettare il rischio di violazioni causate da falle nella propria rete
- Stanno sborsando somme cospicue per sanzioni dovute alla mancata conformità normativa in materia di gestione dei dati dei clienti
- Usano dati strettamente riservati nel corso delle attività quotidiane

Situazione del mercato

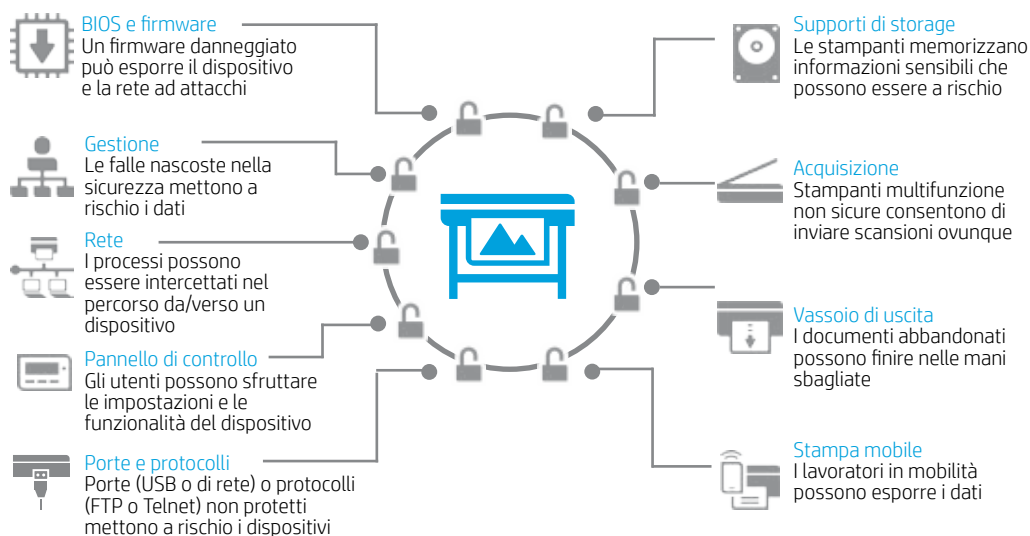
A causa della crescente sofisticazione e pervicacia dei criminali informatici, i firewall di rete si stanno dimostrando misure di sicurezza insufficienti. Le organizzazioni devono rafforzare gli end point che si trovano dietro il firewall, e ciò comprende anche le stampanti di rete.

Se si verifica un attacco informatico ostile, una violazione interna accidentale, una difformità rispetto alle norme o alle leggi in vigore, i costi per risolvere una violazione della sicurezza possono essere notevoli. Il costo annuo medio è pari a circa 4 milioni di dollari⁴, e può comprendere sanzioni, perdite in termini di business, danni alla reputazione e azioni legali collettive.

I requisiti normativi e relativi alla conformità stanno diventando sempre più complessi. Le organizzazioni necessitano di dispositivi e soluzioni in grado di aiutarle a rimanere conformi.

Sfide alla sicurezza dei clienti

Sebbene molti reparti IT applichino misure di sicurezza rigorose ai singoli computer e alla rete aziendale, i dispositivi di imaging e stampa sono spesso sottovalutati e pericolosamente esposti.



Esigenze di sicurezza dei clienti

I clienti necessitano di soluzioni semplici per proteggere dati, dispositivi e documenti. Desiderano anche poter gestire in modo agevole sicurezza e conformità per risparmiare tempo nelle operazioni legate all'IT.

Sicurezza dei dispositivi

- Protezione di BIOS e firmware da attacchi e malware
- Protezione degli aggiornamenti del firmware
- Protezione di impostazioni e password dei dispositivi

Sicurezza dei dati

- Crittografia dei dati che transitano da e verso la stampante, e a riposo quando memorizzati nella stampante
- Supporto di certificati digitali firmati CA (PKI)
- Cancellazione e smaltimento sicuri dei dischi rigidi
- Autenticazione degli utenti e controllo degli accessi
- Soluzioni per la sicurezza della stampa mobile

Sicurezza dei documenti

- Soluzioni di stampa sicura con PIN

Monitoraggio della sicurezza e conformità del parco stampanti

- Controllo della protezione del parco stampanti grazie a diverse funzioni di configurazione e monitoraggio
- Report avanzati per supportare la dimostrazione di conformità

Proposta di valore per il cliente

- Riduzione al minimo del rischio di costosi attacchi informatici
- Protezione di dati e documenti sensibili
- Risparmio di tempo grazie all'automazione della gestione della protezione del parco stampanti
- Garanzia di conformità alle normative di settore, con semplice accesso ai dati per il reporting della conformità

Proposta di valore per i partner

- Un'opportunità di crescita, poiché i clienti investono attivamente nella sicurezza della stampa
- Permette di intavolare una conversazione sul valore, così da poter vendere soluzioni a prezzi più elevati all'azienda; il tema della sicurezza può spostare l'attenzione dal prezzo al valore aggiunto

Domande di qualificazione

Poni ai clienti queste domande:

- Esiste una strategia di sicurezza per i dispositivi di stampa e imaging?
- Vengono gestite informazioni sensibili, ad esempio identità dei dipendenti o dati dei clienti?
- I processi di stampa vengono crittografati?
- Le stampanti sono protette da malware e virus?
- Quanto spesso vengono applicati gli

aggiornamenti del firmware delle stampanti?

- Sono state impostate password amministrative per le stampanti oppure chiunque può modificare le impostazioni dei dispositivi?
- Quanto tempo richiede all'IT la configurazione delle stampanti?

Offerte di sicurezza HP per stampanti HP DesignJet

Le funzionalità di sicurezza integrate nelle stampanti HP DesignJet possono aiutare le aziende a proteggere dispositivi, dati e documenti, oltre a semplificare la gestione della sicurezza e della conformità del parco stampanti.

Stampanti protette

- **Pacchetti firmware firmati da HP:** i pacchetti firmware sono firmati digitalmente dal gruppo HP Code Signing. Ogni nuova installazione di firmware viene verificata
- **UEFI Secure Boot:** convalida l'integrità del sistema operativo all'avvio
- **Crittografia dell'unità disco rigido:** HP utilizza la crittografia e la decifrazione dei dati AES (Advanced Encryption Standard) a 256 bit
- **Cancellazione di file e dischi sicura:** procedure per garantire che i dati archiviati nei sistemi di storage siano effettivamente eliminati, per impedirne il ripristino.
- **Blocco dell'accesso dal pannello di controllo:** permette di bloccare il pannello di controllo della stampante per impedire a utenti non autorizzati di accedervi e modificare le impostazioni della stampante.

Software protetto




Oltre ai dispositivi, HP offre soluzioni per rilevare, rendere sicuro, monitorare e gestire il parco dispositivi e proteggere dati e documenti nel tempo.

- **HP JetAdvantage Security Manager:** l'unico strumento di conformità della sicurezza basato su criteri del settore per automatizzare la gestione della protezione del parco stampanti⁶
 - Supporta la creazione e l'implementazione di criteri di sicurezza per il parco stampanti
 - Creazione di report basati sul rischio per aiutare l'IT a esaminare rapidamente lo stato del parco stampanti e dimostrarne la conformità
 - Applicazione e aggiornamento automatizzati di certificati dispositivo firmati CA univoci
- **HP Web Jetadmin:** una soluzione di gestione della stampa pluripremiata leader di settore per migliorare la produttività e contribuire a ridurre i costi operativi. HP Web Jetadmin, semplice da usare, offre un'intuitiva interfaccia basata su Web per installare, configurare, gestire dispositivi di stampa HP e non HP collegati in rete e a PC, nonché risolvere eventuali problemi.⁷

Dispositivi protetti

- **Servizi HP Custom Recycling:** permettono di eliminare definitivamente i dati dalle unità disco rigido prima che i prodotti obsoleti vengano riciclati in modo responsabile. Ulteriori dettagli alla pagina hp.com/go/businessrecycling.

Confronto tra sicurezza di HP DesignJet e prodotti concorrenti

		HP DesignJet (1)	Canon (2)	Epson (3)	Ricoh (4)
DISPOSITIVO 	Funzioni di sicurezza per la gestione della rete tramite SNMP v3	✓	✓	⊘	✓
	Secure File Erase	✓	⊘ (6)	⊘	✓
	Secure Disk Erase	✓	✓ (5)	✓	✓
DATI 	Compatibilità 802.1x	✓	⊘ (6)	✓	✓
	Crittografia unità disco fisso	✓	⊘	✓	✓
	Internet Protocol Security (IPsec)	✓	⊘ (6)	✓	✓
DOCUMENTI 	Stampa con PIN	✓	⊘	⊘	✓

- (1) Modelli confrontati: HP DesignJet T930, T1530, T2530 MFP, T3500MFP
 (2) Modelli confrontati: Canon iPF785, iPF770, iPF850, iPF770L36, M40 Scanner
 (3) Modelli confrontati: Epson SC-T5200/D, SC-T5200F MFP
 (4) Modelli confrontati: Ricoh MP CW2201SP
 (5) per modelli con unità disco rigido
 (6) Scanner M40: Sì

Elementi vincenti

Le aziende devono prendere la sicurezza della stampa sul serio. HP offre prodotti e soluzioni leader di settore che consentono di proteggere dispositivi, dati e documenti.

¹ Ponemon Institute, "Insecurity of Network-Connected Printers," ottobre 2015.

² Help Net Security, "Why enterprise security priorities don't address the most serious threats," luglio 2015.

³ Il 26,2% degli intervistati ha sperimentato gravi violazioni della sicurezza dell'IT che hanno richiesto misure risolutive, e oltre il 26,1% di tali incidenti ha interessato la stampa. IDC, "IT and Print Security Survey 2015" IDC #US40612015, settembre 2015.

⁴ Ponemon Institute, "Cost of Data Breach Study Global Analysis" 2016

⁵ Quocirca, Managed Print Services Landscapes for 2014 and 2015.

⁶ Affermazioni sulla concorrenza basate sulla ricerca interna condotta da HP sulle offerte della concorrenza (Device Security Comparison, gennaio 2015) e Solutions Report on HP JetAdvantage Security Manager 2.1 di Buyers Laboratory LLC, febbraio 2015. HP JetAdvantage Security Manager deve essere acquistato separatamente. Per maggiori informazioni, visita il sito hp.com/go/securitymanager.

⁷ HP Web Jetadmin è scaricabile gratuitamente all'indirizzo hp.com/go/wja

Condivisione con i colleghi

© Copyright 2017 HP Development Company, L.P. Le informazioni contenute in questo documento sono soggette a modifica senza preavviso. Le sole garanzie applicabili a prodotti e servizi HP sono quelle indicate nella dichiarazione di garanzia esplicita fornita con ciascun prodotto e servizio. Niente di quanto dichiarato nel presente documento dovrà essere interpretato come garanzia aggiuntiva. HP non è responsabile per errori tecnici o editoriali od omissioni contenuti nel presente documento.

Android e Google Chrome sono marchi di fabbrica di Google Inc. Microsoft è un marchio registrato negli Stati Uniti del gruppo di aziende Microsoft.

Riservato HP 2017. Il presente documento contiene informazioni riservate e/o soggette a tutela giuridica, ed è inteso solo per uso interno di HP e dei relativi partner di canale.

A chiunque non rientri tra i destinatari identificati nella copertina del presente documento è severamente vietato rivedere, redistribuire, divulgare, utilizzare in altro modo o fare affidamento sul contenuto del presente documento.

