



# PROTEGGETE IL VOSTRO UFFICIO

**Canon**

---



# QUANTO SONO AL SICURO LE INFORMAZIONI NEL TUO UFFICIO?

Oggi, le aziende si affidano alle informazioni per creare reti complesse di tecnologie, processi, persone e organizzazioni che valicano i confini nazionali. Emergono nuove pratiche operative che ridefiniscono il lavoro d'ufficio e i processi di creazione, condivisione e utilizzo delle informazioni. In un contesto tanto intricato è difficile proteggere adeguatamente i dati. La maggior parte delle aziende pensa di risolvere il problema investendo in firewall, antivirus e software di sicurezza, ma spesso trascura di estendere la protezione anche alle stampanti, che invece svolgono un ruolo importante nella catena di sicurezza.



## PENSA ALLE TUE STAMPANTI

Le stampanti multifunzione (MFP) si sono evolute in strumenti potenti che, come i PC e i server, incorporano sistemi operativi e dischi fissi particolarmente capienti, si collegano alla rete e a Internet, e sono condivisi dagli utenti per elaborare enormi quantità di documenti di importanza critica per l'azienda.



## QUALI SONO I RISCHI?

- Visualizzazione da parte di utenti non autorizzati delle informazioni sensibili memorizzate su una MFP non protetta
- Compromissione della disponibilità dell'infrastruttura di stampa a causa di errori operativi
- Utilizzo della stampante quale via di accesso alla rete aziendale da parte di utenti esterni con intenti dolosi
- Visione dei documenti riservati lasciati nei vassoi di consegna al termine della stampa
- Prelievo involontario di materiale stampato appartenente ad altri utenti
- Trasmissione dei documenti via fax o via e-mail ai destinatari sbagliati a causa di errori di digitazione
- Intercettazione da parte degli hacker dei dati in transito
- Perdita dei dati dovuta a una gestione disattenta dello smaltimento della stampante alla fine del suo ciclo di vita.

"È necessario adottare degli standard di base per la sicurezza informatica in ufficio, dove potenzialmente si gestiscono enormi quantità di dati. Oggi la stampante non è più una macchina stupida, è un server che stampa carta".

(CISO, Publicis Groupe)

# SOLUZIONI DI STAMPA SICURE PER LA TUA AZIENDA

## Soluzioni progettate per la sicurezza e la privacy

Quando progettiamo o selezioniamo le tecnologie, i prodotti e i servizi per i nostri clienti, valutiamo l'impatto che possono esercitare sul loro ambiente operativo in termini di sicurezza delle informazioni. Per questo motivo le nostre stampanti multifunzione sono dotate di una serie di funzioni di sicurezza, sia standard che opzionali, che consentono alle aziende di ottenere il livello di protezione desiderato per:



DISPOSITIVI



RETI



DOCUMENTI



AZIENDA NEL SUO  
COMPLESSO



### STANDARD E CERTIFICAZIONI RICONOSCIUTI A LIVELLO INTERNAZIONALE

Le nostre stampanti multifunzione imageRUNNER ADVANCE vengono abitualmente valutate e certificate utilizzando la metodologia Common Criteria, in conformità ai requisiti degli standard IEEE2600 per la sicurezza dei dispositivi di stampa.



### TEST DI SICUREZZA

Canon esegue i propri test di sicurezza attenendosi a un regime che è considerato tra i più rigorosi nel settore delle apparecchiature per ufficio. Le tecnologie adottate nel nostro portafoglio di prodotti sono sottoposte agli stessi elevati standard di prova che ci aspettiamo vengano applicati alla nostra azienda.

Canon, leader nello sviluppo di soluzioni innovative per la gestione delle informazioni e della stampa, collabora con i propri clienti per aiutarli ad adottare un approccio inclusivo alla sicurezza dei dati. Un approccio che prenda in considerazione l'impatto che la nostra tecnologia può esercitare sul loro sistema di gestione delle informazioni, in termini di sicurezza.



# PROTEGGETE IL VOSTRO DISPOSITIVO

## Protezione completa per le risorse fisiche



### SOLUZIONI DI AUTENTICAZIONE UTENTE

Proteggi il tuo dispositivo dall'uso non autorizzato implementando il controllo dell'accesso tramite autenticazione. Oltre a ottimizzare il controllo e l'affidabilità del sistema, questa soluzione consente agli utenti di accedere più rapidamente alle impostazioni preferite e ai lavori di stampa. Le nostre stampanti dipartimentali sono dotate di Universal Login Manager, una soluzione di login flessibile che si avvale di un metodo di autenticazione locale basato su un database di utenti creato sul dispositivo, cui si aggiunge l'autenticazione del dominio tramite Active Directory o il server uniFLOW. Le aziende hanno così la possibilità di controllare l'accesso ai dispositivi senza trascurare la praticità d'uso.



### CONTROLLO DELL'AMMINISTRAZIONE DEL DISPOSITIVO

Solo gli utenti con privilegi di amministratore possono accedere alla configurazione del dispositivo, che include le impostazioni di rete e altre opzioni di controllo, così da prevenire modifiche intenzionali o accidentali.



### SISTEMA DI GESTIONE DEGLI ACCESSI

Questa funzione consente di controllare l'accesso alle funzioni del dispositivo. Gli amministratori possono utilizzare i ruoli standard oppure creare nuovi ruoli personalizzati attribuendo il livello di privilegi desiderato. Per esempio, ad alcuni utenti può essere impedito di copiare i documenti o di usare la funzione di invio.



### IMPOSTAZIONE DELLA POLICY DI SICUREZZA

I modelli imageRUNNER ADVANCE di ultima generazione sono dotati di una funzione che consente all'amministratore di accedere a tutte le impostazioni riguardanti la sicurezza da un unico menu e di modificarle prima di attivarle sulla periferica. Una volta attivate, l'uso del dispositivo e le modifiche alle impostazioni dovranno rispettare i criteri impostati. La policy di sicurezza può essere protetta da apposita password, in modo da limitare l'accesso al solo responsabile della sicurezza IT.



### PROTEZIONE DEI DATI SUL DISCO FISSO

La stampante multifunzione contiene un'elevata quantità di dati che necessitano di protezione: lavori in attesa di essere stampati, fax ricevuti, dati acquisiti, rubriche, registri attività e cronologia dei lavori. I dispositivi Canon offrono una serie di misure pensate per proteggere i dati durante l'intero ciclo di vita della periferica e assicurare la loro riservatezza, integrità e disponibilità.



### PROTEZIONE PREVENTIVA

I prodotti imageRUNNER ADVANCE offrono una serie di impostazioni di sicurezza che consentono di proteggere le stampanti dagli attacchi. La funzionalità Secure Boot garantisce l'integrità del dispositivo, mentre il monitoraggio syslog fornisce in tempo reale dati sulle condizioni di sicurezza del dispositivo (i dati possono essere letti da un apposito sistema SIEM di terze parti).



## I TUOI DISPOSITIVI SONO SICURI?

**1**

I tuoi dispositivi sono utilizzati da più utenti e installati in aree aperte al pubblico?

**2**

Gli utenti possono accedere liberamente ai dispositivi?

**3**

Hai implementato delle misure per proteggere le informazioni memorizzate sul disco fisso del dispositivo?

**4**

Gli utenti non autorizzati possono modificare le impostazioni del dispositivo?

**5**

Hai considerato il ciclo di vita del dispositivo e il suo smaltimento?

### CRITTOGRAFIA DEL DISCO FISSO

I nostri dispositivi imageRUNNER ADVANCE garantiscono il massimo livello di sicurezza criptando tutti i dati presenti sul disco fisso. Il chip di sicurezza responsabile della crittografia dei dati è conforme agli standard FIPS 140-2 Livello 2 stabiliti dal governo degli Stati Uniti e ha conseguito sia la certificazione CMVP (Cryptographic Module Validation Program), rilasciata negli USA e in Canada, sia la certificazione JCMVP (Japan Cryptographic Module Validation Program).

### CANCELLAZIONE DEL DISCO FISSO

Alcuni dati, come le immagini acquisite o copiate e i documenti stampati da computer, vengono temporaneamente memorizzati nel disco fisso della stampante ed eliminati al termine dell'operazione. Per assicurare che nessun dato rimanga nel disco fisso del dispositivo, è prevista un'opzione di cancellazione che elimina tutti i dati residui durante il processo di elaborazione del lavoro.

### INIZIALIZZAZIONE DI TUTTI I DATI E DELLE IMPOSTAZIONI

Per prevenire la perdita di dati in occasione della sostituzione o dello smaltimento del disco fisso, è possibile sovrascrivere i documenti e i dati memorizzati e ripristinare le impostazioni predefinite della periferica.

### MIRRORING DEL DISCO FISSO\*

Le aziende possono eseguire il backup dei dati su un secondo disco fisso opzionale. La procedura di mirroring comporta anche la crittografia di tutti i dati presenti su entrambi i dischi fissi.

### RIMOZIONE DEL DISCO FISSO\*

Questa funzione consente di rimuovere il disco fisso dalla periferica per conservarlo in un luogo sicuro.

\*Opzionale. Per informazioni dettagliate sulla disponibilità delle funzioni e delle opzioni sui nostri sistemi di stampa per l'ufficio, contatta il tuo rappresentante Canon locale



# PROTEGGETE LE VOSTRE RETI



## LA STAMPANTE PUÒ METTERE IN PERICOLO LA TUA RETE?

- La tua rete è vulnerabile ad attacchi malevoli?
- I visitatori possono eseguire stampe e scansioni senza mettere a rischio la tua rete?
- I criteri adottati per il lavoro BYOD sono sicuri e sostenibili?
- I flussi di dati di stampa tra PC e dispositivo sono crittografati?
- I dati di stampa e scansione sono protetti in fase di trasferimento?

# Canon offre numerose soluzioni di sicurezza pensate per proteggere la rete e i dati da attacchi interni ed esterni.

## FILTRO INDIRIZZI IP E MAC

Proteggi la tua rete da accessi non autorizzati consentendo la comunicazione, sia inbound che outbound, solo con i dispositivi che hanno un determinato indirizzo IP o MAC.

## CONFIGURAZIONE DEL SERVER PROXY

Imposta un proxy per gestire le comunicazioni e utilizzalo per collegarti con i dispositivi esterni alla rete.

## AUTENTICAZIONE IEEE 802.1X

L'accesso non autorizzato alla rete è impedito da uno switch LAN che concede i privilegi di accesso ai soli dispositivi client che sono autorizzati dal server di autenticazione.

## COMUNICAZIONE IPSEC

La comunicazione IPsec impedisce a terzi di intercettare o alterare i pacchetti IP trasportati sulla rete IP.

Utilizza la comunicazione criptata TLS per prevenire l'intercettazione, la manipolazione e l'alterazione dei dati che vengono scambiati tra la periferica e altri dispositivi, come per esempio i computer.

## CONTROLLO DELLE PORTE

Configura le porte nel rispetto delle policy di sicurezza aziendale.

## AUTO ENROLLMENT DEI CERTIFICATI

Grazie a questa funzionalità, i problemi relativi ai certificati di sicurezza sono drasticamente ridotti. Utilizzando una tecnologia riconosciuta nel settore, un amministratore di sistema può aggiornare e rilasciare automaticamente i certificati, facendo in modo che i criteri di sicurezza siano sempre rispettati.

## MONITORAGGIO DEL REGISTRO

Vari registri consentono di monitorare l'attività del dispositivo e le richieste di comunicazione che sono state bloccate.

## WI-FI DIRECT

Questa funzione consente di abilitare la connessione peer-to-peer per la stampa mobile senza che il dispositivo mobile debba accedere alla rete.

## CRITTOGRAFIA DEI DATI IN TRANSITO DA E VERSO IL DISPOSITIVO

Questa opzione cripta i lavori di stampa inoltrati dal computer dell'utente alla stampante multifunzione. Attivando la funzione di sicurezza universale, la crittografia viene estesa anche ai dati acquisiti in formato PDF.

## STAMPA MOBILE PER OSPITI

Il nostro software di rete sicuro per la gestione della stampa e delle scansioni affronta i comuni rischi di sicurezza per la stampa da dispositivi mobili da parte di ospiti fornendo percorsi esterni per l'invio dei lavori via e-mail, web e app. Collegando l'MFD a una fonte sicura si riducono al minimo i vettori di attacco.



# PROTEGGETE I VOSTRI DOCUMENTI

Tutte le aziende trattano informazioni sensibili come contratti, informazioni sugli stipendi, dati dei clienti e piani di ricerca e di sviluppo. Se queste informazioni dovessero cadere nelle mani sbagliate, le conseguenze potrebbero spaziare dal danno d'immagine a pesanti sanzioni, per arrivare fino ad azioni legali.

**Canon offre una gamma di soluzioni di sicurezza pensate per proteggere i documenti sensibili nel corso del loro intero ciclo di vita.**



## RISERVATEZZA DEL DOCUMENTO STAMPATO

### Stampa sicura

L'utente può impostare un codice PIN che dovrà essere inserito sul dispositivo per poter stampare il documento. Questa opzione consente agli utenti di proteggere i documenti riservati.

### Messa in attesa di tutti i lavori di stampa

Le stampanti imageRUNNER ADVANCE prevedono un'opzione che consente agli amministratori di configurare il sistema in modo che trattienga tutti i lavori inviati per la stampa, così da proteggerne la riservatezza. Per poterli stampare, gli utenti dovranno prima autenticarsi sul sistema.



## SCORAGGIARE O PREVENIRE LA DUPLICAZIONE DEI DOCUMENTI

### Stampa con filigrane visibili

È possibile stampare i documenti con un testo che appare sovrapposto al contenuto del documento oppure sul suo sfondo. Si scoraggia quindi la copiatura sensibilizzando l'utente sulla riservatezza del documento.

### Stampa/copia con filigrane invisibili

Attivando questa opzione è possibile eseguire copie o stampare documenti con un testo nascosto incorporato nello sfondo. Quando i documenti vengono copiati, il testo appare sul documento e agisce da deterrente.

### Prevenzione della perdita di dati a livello aziendale

Aggiorna il tuo sistema di prevenzione della perdita di dati usando iW SAM Express in combinazione con uniFLOW. Questa soluzione basata su server consente di acquisire e

### Mailbox

I lavori di stampa o i documenti acquisiti vengono inviati a una cartella cui l'utente può successivamente accedere. Le mailbox possono essere protette con un codice PIN per garantire che solo il proprietario possa visualizzarne il contenuto. Questo spazio sicuro sulla periferica è ideale per conservare i documenti che devono essere stampati con una certa frequenza (come i form) ma che richiedono una gestione molto attenta.

### uniFLOW Secure Printing\*

Con uniFLOW MyPrintAnywhere, gli utenti inviano i lavori tramite il driver universale e ritirano la stampa su qualsiasi stampante collegata in rete.

archiviare i documenti inviati da e verso la stampante, analizzare e interpretare dati utilizzando testo o attributi con l'obiettivo finale di agire contro le minacce alla sicurezza.

### Blocco scansione\*

Questa opzione incorpora un codice nascosto all'interno dei documenti copiati o stampati in modo da impedirne la duplicazione sulle periferiche sulle quali la funzione è attivata. L'amministratore può scegliere di applicare questa funzione a tutti i lavori o a discrezione dell'utente. È possibile incorporare un codice TL o QR.

### Tracciamento dell'origine del documento\*

Il codice incorporato nel documento consente di tracciare la sua origine.



## I TUOI DOCUMENTI SONO DAVVERO SICURI?

**1**

Hai implementato delle misure atte a impedire agli utenti non autorizzati di accedere ai documenti sensibili presenti nella stampante?

**2**

Puoi assicurare la riservatezza di tutti i documenti che passano attraverso il dispositivo condiviso?

**3**

Puoi tracciare l'origine dei documenti stampati?

**4**

Qualcuno può impossessarsi delle stampe contenenti dati sensibili?

**5**

Puoi impedire che i documenti vengano inviati al destinatario sbagliato?



### CONTROLLO DEGLI INVII DI DOCUMENTI E FAX

#### Limitazione delle destinazioni

Per ridurre il rischio di fuga di informazioni, gli amministratori possono limitare le destinazioni di invio a quelle contenute nella rubrica o sul server LDAP, agli indirizzi degli utenti registrati o a determinati domini.

#### Disattivazione del completamento automatico dell'indirizzo

Disattivando il completamento automatico degli indirizzi e-mail si può impedire l'invio dei documenti ai destinatari sbagliati.

#### Protezione della rubrica

Imposta un codice PIN per proteggere la rubrica del dispositivo da modifiche non autorizzate.

#### Conferma del numero fax

Puoi impedire che i documenti vengano inviati ai destinatari indesiderati impostando il sistema in modo che gli utenti debbano digitare due volte il numero di fax, per confermarlo, prima di procedere con l'invio.

#### Riservatezza dei fax ricevuti

Imposta il dispositivo in modo che memorizzi i documenti senza stamparli. Puoi anche proteggere la riservatezza dei fax ricevuti impostando dei codici PIN o applicando delle condizioni per la loro archiviazione sicura in una casella riservata.



### VERIFICA DELL'ORIGINE E DELL'AUTENTICITÀ DEL DOCUMENTO ATTRAVERSO FIRME DIGITALI

#### Firma del dispositivo

È possibile applicare una firma del dispositivo ai documenti acquisiti in formato PDF o XPS, utilizzando una chiave e un certificato, di modo che il destinatario possa verificare l'origine del documento e la sua autenticità.

#### Firma utente\*

Questa opzione consente agli utenti di inviare un file PDF o XPS aggiungendo una firma digitale univoca ottenuta da un'autorità di certificazione. I destinatari possono in tal modo verificare chi ha sottoscritto il documento.



### APPLICAZIONE DELLE POLICY GRAZIE ALL'INTEGRAZIONE DI ADOBE LIFECYCLE MANAGEMENT ES

Gli utenti possono proteggere i file PDF e applicare policy persistenti e dinamiche al fine di controllare i diritti di accesso e di utilizzo per proteggere le informazioni sensibili da divulgazioni accidentali o con intento doloso.

Poiché le policy vengono mantenute a livello del server, gli utenti possono modificare i diritti anche dopo la distribuzione di un file. La serie imageRUNNER ADVANCE può essere configurata per l'integrazione di Adobe® ES.

\*Opzionale. Per informazioni dettagliate sulla disponibilità delle funzioni e delle opzioni sui nostri sistemi di stampa per l'ufficio, contatta il tuo rappresentante Canon locale



# SICUREZZA DEI DATI AZIENDALI

Canon può contribuire alla protezione delle informazioni all'interno della tua azienda.

## **CONTROLLO TOTALE PER SODDISFARE LE TUE ESIGENZE DI ACQUISIZIONE E OUTPUT END-TO-END**

Il software modulare per la gestione dell'output permette alle aziende di condividere i dispositivi in tutta sicurezza, consentendo di stampare i lavori su qualsiasi stampante collegata al server di gestione dell'output senza correre alcun rischio. Gli utenti mobile sono supportati da un servizio controllato centralmente che assicura l'accesso alla stampa dai dispositivi mobili sia agli utenti interni che ai visitatori. Per le esigenze di acquisizione, il modulo di scansione consente di acquisire, comprimere, convertire e distribuire i documenti dal dispositivo multifunzione a un'ampia gamma di destinazioni, inclusi sistemi cloud. È anche possibile reindirizzare i lavori alla stampante più idonea, ottimizzando il costo di stampa di ogni documento.

La nostra soluzione incrementa la sicurezza dei documenti all'interno dell'azienda e, grazie al modulo di contabilizzazione, consente di controllare l'attività per utente, dispositivo e reparto.

## **GESTIONE CENTRALIZZATA DEL PARCO MACCHINE**

Il nostro software di gestione IW MC consente di aggiornare e di inviare ai dispositivi Canon in rete le impostazioni dispositivo, le policy di sicurezza, le password, i certificati e i firmware. La centralizzazione di queste attività consente al team IT di risparmiare tempo prezioso e garantisce il continuo aggiornamento della sicurezza dell'infrastruttura di stampa.

## **AUDIT COMPLETI**

L'architettura dei nostri servizi documentali per l'ufficio può essere ottimizzata con l'installazione di sistemi opzionali che consentono di acquisire un record completo (scansione e metadati del lavoro) di tutti i documenti elaborati dai dispositivi imageRUNNER ADVANCE.

## **SERVIZI DI STAMPA GESTITI**

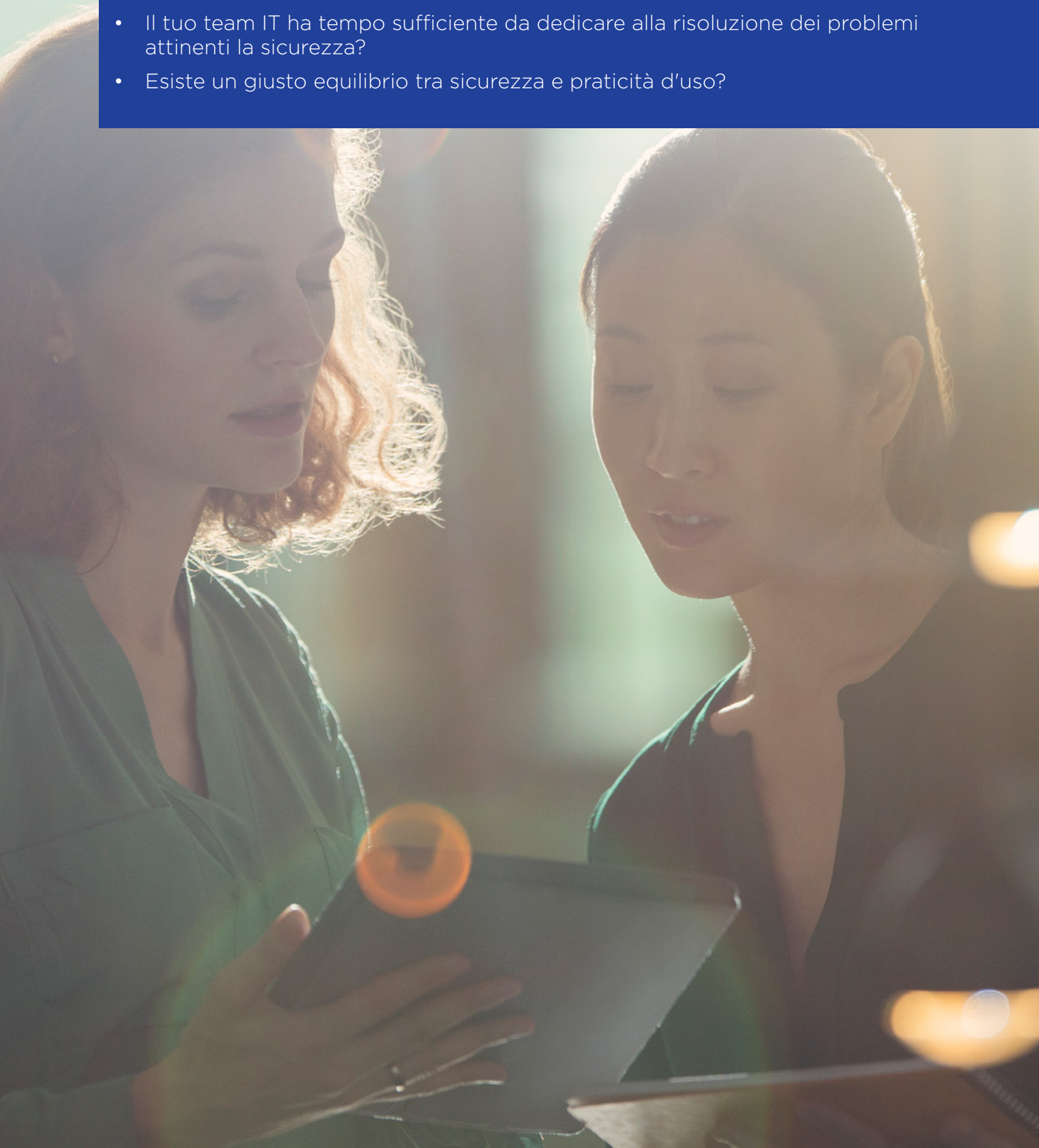
Canon MPS combina tecnologie e software innovativi con i servizi più adeguati, per soddisfare qualsiasi esigenza di stampa e di gestione dei documenti senza gravare in alcun modo sul carico di lavoro del team IT. Grazie alla gestione proattiva e alla continua ottimizzazione dell'infrastruttura di stampa e dei processi di gestione dei documenti, possiamo aiutarti a realizzare i tuoi obiettivi di sicurezza, ottimizzando i costi e incrementando la produttività della tua azienda.

## **SVILUPPO PERSONALIZZATO**

Disponiamo di sviluppatori interni che possono proporre e sviluppare una soluzione personalizzata in funzione delle tue specifiche esigenze.

## IL TUO APPROCCIO ALLA SICUREZZA AZIENDALE È INCLUSIVO?

- La tua policy di sicurezza si applica anche ai dispositivi multifunzione?
- In che modo garantisci l'aggiornamento e l'ottimizzazione della tua infrastruttura di stampa e la tempestiva ed efficiente correzione dei bug?
- I visitatori possono eseguire stampe e scansioni senza mettere a rischio la tua rete?
- Le policy BYOD sono sicure e compatibili con l'intero parco stampanti?
- Il tuo team IT ha tempo sufficiente da dedicare alla risoluzione dei problemi attinenti la sicurezza?
- Esiste un giusto equilibrio tra sicurezza e praticità d'uso?



# PERCHÉ CANON?



## ESPERIENZA

L'integrazione hardware e software riduce il rischio di violazioni del sistema.



## PARTNERSHIP

Aiutiamo i clienti nelle loro attività affrontando in modo proattivo le minacce alla sicurezza dei dati.



## SERVIZIO

Lo stesso team di sicurezza informatica dedicato ai clienti gestisce la nostra sicurezza informatica interna.

Prendiamo in considerazione tutte le potenziali minacce, sia all'interno che all'esterno del firewall aziendale.



## INNOVAZIONE

I nostri prodotti e servizi offrono modi più intelligenti per ridurre al minimo le probabili minacce alla sicurezza delle informazioni.



Abbiamo ricevuto il premio **"Highly commended"** per il miglior team addetto alla sicurezza agli **SCA Awards Europe 2017**, che riconoscono l'esperienza nel campo della cybersicurezza.

Canon U.S.A. ha vinto due premi ai **BLI PaceSetter Awards 2017** (Document Imaging Security and Mobile Print).

Canon Inc.  
Canon.com

Canon Europe  
canon-europe.com

Italian edition  
© Canon Europa N.V., 2018

**Canon**