SMARTSHIELD

Tecnologie integrate di sicurezza per la stampa

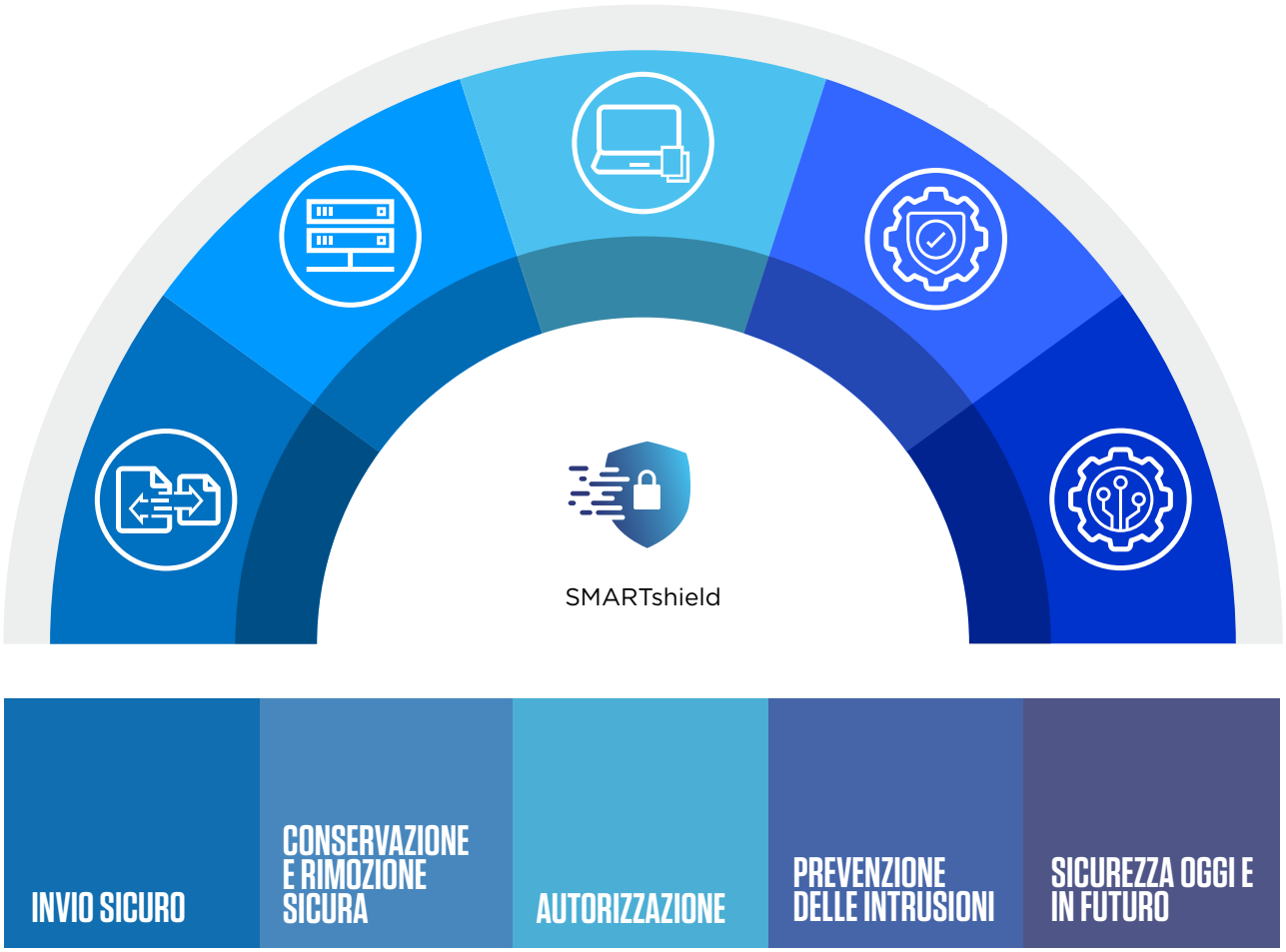
Per stampanti ColorWave e PlotWave

Canon

SICUREZZA DI STAMPA ECCEZIONALE

Le nostre stampanti Large Format, leader del mercato, rispondono alle preoccupazioni in merito alla sicurezza dei documenti che contengono dati riservati.

SMARTshield offre una serie di funzionalità di sicurezza integrate nel flusso di lavoro per i nuovi sistemi PlotWave e ColorWave. Progettato per la sicurezza dei tuoi sistemi, oggi e in futuro.



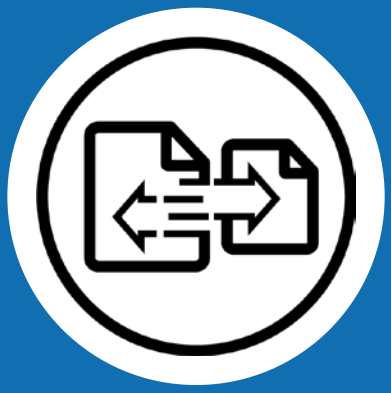
Ora più che mai, le aziende e le organizzazioni governative che utilizzano stampanti per grandi formati devono proteggere le informazioni più importanti, riservate e sensibili all'interno dei loro uffici e delle loro reti. Tra queste sono comprese le informazioni inviate dalle singole postazioni di lavoro e da altri dispositivi per la stampa, nonché i dati memorizzati nella stampante. È fondamentale che i sistemi siano protetti dagli accessi non autorizzati per salvaguardare i dati di stampa, le informazioni stampate e l'infrastruttura IT dell'utente finale. Per queste ragioni, alle organizzazioni serve una stampante Large Format sicura, in grado di semplificare la vita al responsabile IT, agli utenti e agli amministratori.

SMARTshield è una tecnologia di stampa sicura completamente integrata, presente in tutte le nostre stampanti per grandi formati e progettata specificamente per soddisfare tali esigenze.

La tecnologia SMARTshield è dotata di molteplici misure di sicurezza pensate per tenere i dati e le informazioni al sicuro dalle intrusioni.

SMARTshield affronta tutti i rischi per la sicurezza, in ogni fase del flusso di lavoro.

SMARTshield ti protegge oggi e in futuro.



INVIO SICURO

Protegge i dati durante l'invio alla stampante, da qualsiasi dispositivo.

Grazie alle applicazioni per il flusso di lavoro ClearConnect, gli utenti possono inviare file dal proprio PC o da qualsiasi dispositivo mobile. Con un tale livello di flessibilità e accesso mobile, è essenziale che i dati vengano trasmessi in modo sicuro alla stampante, in qualsiasi momento e da tutti i dispositivi.

- Compatibilità con Internet Protocol Security (IPSec)
- Compatibilità con IPv6 e IPv4
- HTTPS

SMARTshield

CONSERVAZIONE E RIMOZIONE SICURA

Protegge i dati sensibili memorizzati sul disco rigido della stampante.

È importante proteggere i dati sensibili memorizzati dalla stampante per evitare che vengano rubati o diffusi per errore dall'azienda o dal singolo ufficio. SMARTshield crittografa le informazioni e limita l'accesso con l'identificazione utente per proteggere tutti i tuoi dati. Cancellando correttamente i dati, l'utente si assicura che i file riservati siano inaccessibili ai colleghi non autorizzati.

- Eliminazione sicura dei file
- E-shredding
- Hard disk rimovibile
- Avvio protetto
- Crittografia dei dati
- Distruzione dell'hard disk al termine del contratto

SMARTshield

AUTORIZZAZIONE

Con l'autorizzazione utente, SMARTshield nega l'accesso ai file riservati agli utenti non autorizzati.

Inoltre, con l'autenticazione è possibile tenere sotto controllo le attività degli utenti, limitare le funzioni e i protocolli a cui possono accedere e monitorare le spese sostenute utente per utente.

- Blocco di accesso al pannello di controllo
- Stampa sicura con credenziali di dominio (Active Directory)
- Stampa sicura con smart card (senza lettore)
- Stampa file disponibili solo nella Smart Inbox
- Invia la scansione alla tua cartella principale
- Stampa dalla tua cartella principale
- Disabilita porte e interfacce
- Software di terze parti come uniFLOW

SMARTshield

PREVENZIONE DELLE INTRUSIONI

Per ogni business, una delle sfide maggiori in materia di sicurezza è tenere lontano gli hacker. Quando si stampano dati importanti è fondamentale limitare l'accesso alla stampante e ai dati memorizzati sul controller (o disco fisso).

È necessario assicurarsi che la stampante non subisca intrusioni o venga usata a danno della tua rete. SMARTshield affronta la sfida di prevenzione delle intrusioni su numerosi fronti:

- Disabilitando protocolli inutilizzati
- SNMP v3
- Compatibilità con IEEE 802.1x
- McAfee antivirus (opzionale)
- Whitelisting con McAfee Application Control (opzionale)

SMARTshield

SICUREZZA OGGI E IN FUTURO

La sicurezza non è una condizione statica. Gli hacker cercano costantemente nuove vie per accedere alle tue informazioni preziose. SMARTshield è progettato per proteggere le tue informazioni, oggi e in futuro.

I nostri esperti di sicurezza monitorano regolarmente la comparsa di nuovi pericoli, per proteggere i tuoi dati e le tue stampanti. Le funzioni attuali includono:

- Il software di controllo Windows 10 IoT Enterprise LTSC
- Supporto almeno fino al 2029 e oltre
- Aggiornamenti sulla sicurezza da remoto
- On Remote Service

Comprendiamo le tue preoccupazioni in ambito di sicurezza e per questo abbiamo elaborato una serie di funzioni per contenere i rischi che il tuo business affronta in ogni fase del flusso di lavoro. Non solo oggi, ma anche in futuro.

Canon è il partner ideale per un ambiente di stampa sicuro.

SMARTshield

COMPATIBILITÀ DI SMARTSHIELD

SMARTshield è integrato nei seguenti sistemi:

ColorWave 3600

ColorWave 3800

Serie PlotWave 3000

Serie PlotWave 5000

PlotWave 7500

SMARTSHIELD
NEL DETTAGLIO

INVIO SICURO

Compatibilità con Internet Protocol Security (IPsec)	IPsec è un protocollo che fornisce autenticazione, riservatezza dei dati e integrità nella comunicazione di rete fra il controller e gli altri dispositivi.
Compatibilità con IPv6 e IPv4	Internet Protocol version 4 (IPv4) è un protocollo fondamentale dei metodi di navigazione basati su standard, in Internet e in altre reti a commutazione di pacchetto. Usa indirizzi di 32 bit. IPv6 è la versione più recente e usa indirizzi di 128 bit, garantendo così un unico indirizzo a molti più dispositivi.
HTTPS	Per proteggere il traffico di rete verso WebTools Express, Publisher Express e Publisher Select dall'intercettazione e dall'alterazione, è possibile utilizzare il protocollo HTTPS al posto del normale traffico HTTP con il controller. Inoltre, i certificati attendibili CA possono essere incorporati nel controller per prevenire un attacco man-in-the-middle e quindi evitare che qualcuno sul percorso di rete si finga il controller.

CONSERVAZIONE E RIMOZIONE SICURA

Cancellazione sicura dei file	Rimuove automaticamente dalla Smart Inbox i lavori di stampa, scansione e copia dopo un limite di tempo definito dall'utente. La rimozione dei file è sicura se si abilita la funzione e-shredding.
E-shredding	E-shredding è una funzione di sicurezza che consente al sistema di sovrascrivere i dati di stampa/copia/scansione dopo che sono stati eliminati dal sistema. In caso di furto del disco, questa funzione impedisce il recupero di qualsiasi dato personale cancellato, compreso il contenuto e gli attributi dei file.
Hard disk rimovibile	Il Removable HDD Kit opzionale permette agli amministratori di rimuovere fisicamente l'hard disk interno del dispositivo, per poterlo riporre in un luogo sicuro al termine della giornata lavorativa. L'unità può essere facilmente reinstallata e utilizzata in orario di lavoro.
Avvio protetto	Avvio protetto è uno standard di sicurezza che consente al dispositivo di avviarsi usando solo software affidabili. All'accensione della stampante, il controller verifica la firma di ciascun software di avvio.
Crittografia dei dati	La crittografia dell'hard disk del controller POWERsync cripta tutti i file presenti sull'unità (inclusi il sistema operativo e i dati; crittografia dello spazio disco utilizzato). La procedura di crittografia si basa sul Trusted Platform Module (TPM) e sul meccanismo Microsoft BitLocker, conforme alla certificazione FIPS 140-2. Viene utilizzato il metodo di crittografia AES 256.
Distruzione dell'hard disk al termine del contratto	Su richiesta del cliente, l'hard disk interno del controller POWERsync può essere rimosso e distrutto fisicamente, garantendo così che nessun dato di stampa rimanga memorizzato nella stampante una volta che questa ha lasciato gli uffici del cliente.

AUTORIZZAZIONE

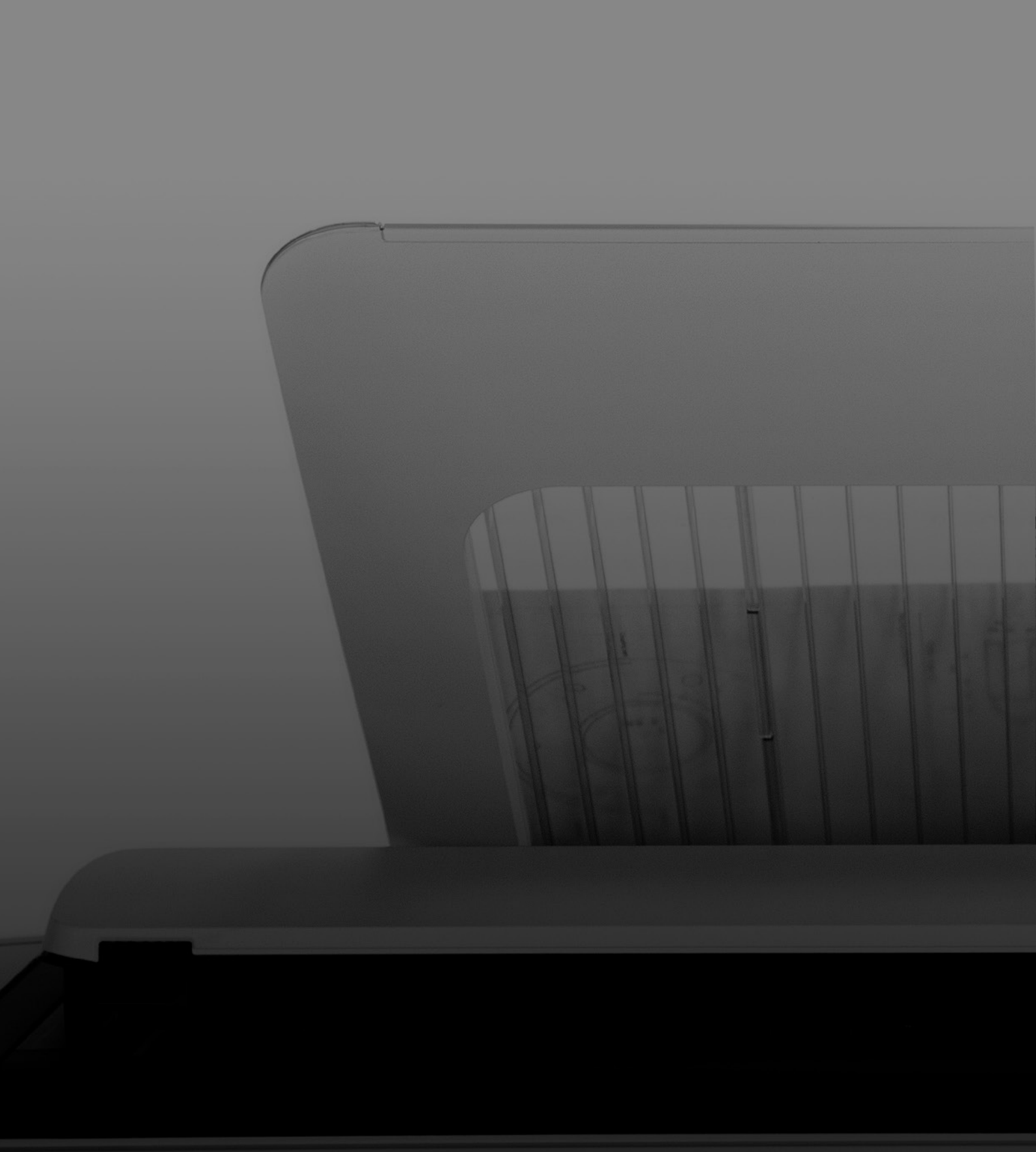
Blocco di accesso al pannello di controllo	Se si abilita la funzione di accesso alla gestione, è possibile accedere al pannello di controllo utente ClearConnect solo dopo averlo sbloccato con le credenziali di dominio o la smart card.
Stampa sicura con credenziali di dominio (Active Directory)	I documenti sensibili non vengono stampanti finché il proprietario del lavoro non si autentica nel panello utente del sistema con le credenziali utente corrette e avvia la stampa.
Stampa sicura con smart card (senza lettore)	I documenti sensibili non vengono stampanti finché il proprietario del lavoro non si autentica nel panello utente del sistema strisciando o inserendo la smart card e avvia la stampa.
Stampa file disponibili solo nella Smart Inbox	Disabilitando la funzione di stampa diretta in WebTools Express, il file per la stampa rimarrà nella tua Smart Inbox fino alla sua attivazione dal pannello utente ClearConnect o in WebTools Express. In questo modo eviti che il documento stampato venga preso accidentalmente da un collega.
Invia la scansione alla tua cartella principale	La funzione per inviare scansioni alla propria cartella principale è disponibile autenticandosi con nome utente e password. Dopo l'autenticazione nel pannello della stampante, l'utente può inviare la scansione alla propria cartella principale in rete, configurata per il suo account MS Active Directory (Windows).
Stampa dalla tua cartella principale	La funzione di stampa dalla propria cartella principale è disponibile autenticandosi con nome utente e password. Dopo l'autenticazione nel pannello della stampante, l'utente può stampare dalla propria cartella principale in rete, configurata per il suo account MS Active Directory (Windows).
Disabilita porte e interfacce	Per proteggere il controller POWERsync da accessi non autorizzati, tutte le porte e le interfacce di rete sono disabilitate.
Software di terze parti come uniFLOW	I sistemi di stampa PlotWave e ColorWave con un'interfaccia utente ClearConnect possono essere integrati negli ambienti uniFLOW del cliente. Gli utenti dispongono così di ulteriori funzionalità per aiutare il cliente a controllare e ridurre i costi di stampa, aumentare la protezione dei dati e migliorare la produttività dei dipendenti.

PREVENZIONE DELLE INTRUSIONI

Disabilita i protocolli inutilizzati	Gli amministratori di rete hanno la capacità di configurare protocolli accessibili specifici. Pertanto, è possibile bloccare efficacemente la comunicazione con dispositivi indesiderati e l'accesso al sistema, attraverso protocolli di trasporto specifici.
SNMP V3	È la versione sicura di SNMP che fornisce autenticazione e integrità tra la Network Management Station (NMS) e le stampanti gestite.
Autenticazione dispositivo IEEE 802.1X	Secondo lo standard IEEE 802.1X, la procedura di autenticazione è basata sulle porte e consente a un'autorità centrale di autenticare un dispositivo per comunicare in rete con altri dispositivi.
McAfee antivirus (opzionale)	La possibilità di installare l'antivirus McAfee sul controller POWERsync costituisce una misura di protezione aggiuntiva contro i virus.
Whitelisting con McAfee Application Control (opzionale)	Funzione di sicurezza opzionale da attivare con licenza. Se attivata e abilitata, crea un elenco dettagliato di tutti i file sul controller e impedisce modifiche non autorizzate da parte di malware, virus e utenti. Controlla regolarmente l'integrità dei file rispetto all'elenco e blocca qualsiasi manomissione o modifica non autorizzata.

SICUREZZA OGGI E IN FUTURO

Il software di controllo Windows 10 IoT Enterprise LTSC	Il controller POWERsync nelle stampanti usa Windows 10 IoT Enterprise LTSC.
Supporto fino al 2029 o oltre	Microsoft garantisce il supporto di Windows 10 IoT Enterprise LTSC fino al 2029 o oltre. Gli aggiornamenti di sicurezza sono garantiti per questo arco temporale.
Aggiornamenti sulla sicurezza da remoto	Attraverso WebTools Express, l'amministratore di sistema può caricare e installare da remoto gli aggiornamenti di sicurezza. In questo modo puoi fare affidamento su risposte rapide e tempi di funzionamento elevati, in quanto non è necessario l'intervento fisico di un tecnico alla stampante.
On Remote Service	On Remote Service è il servizio sviluppato da Canon che garantisce la più elevata continuità operativa per il tuo sistema Canon. In quanto applicazione integrata al controller, On Remote Service offre servizi di supporto a distanza, come la telediagnostica, la telelettura dei contatori e l'assistenza remota. Ciò comporta una maggiore disponibilità del sistema, una riduzione dell'amministrazione, prime riparazioni migliori, tempi di risposta più rapidi e, soprattutto, serenità.



Canon Italia Spa
Strada Padana Superiore, 2/B
20063 Cernusco sul Naviglio MI
Tel 02 82481
Fax 02 82484600
Pronto Canon 848800519
canon.it

Canon (Svizzera) SA
Richtistrasse 9
CH-8304 Wallisellen
Tel. +41 (0)22 567 58 58
canon.ch
Italian edition