



WORKSPACE SECURITY

LA GESTIONE DEI RISCHI NEL
NUOVO MONDO DEL LAVORO

Canon

SOMMARIO

1. Introduzione

Introduzione	2
Prefazione	3

3. Una nuova concezione dell'ambiente di lavoro

Introduzione	14
Mobile working	16
Smart working	17
Co-working	18

5. Perché scegliere Canon

Panoramica	27
La nostra esperienza	29

2. Il panorama attuale

Introduzione	5
Minacce interne	6
Violazioni dei dati	9
Dispositivi connessi in rete	10

4. Tutela delle informazioni

Introduzione	21
Gestione della stampa	22
Gestione dell'acquisizione	23
Gestione dei documenti	24



SE I TEMPI DEL LAVORO DALLA 9 ALLE 6 NON FOSSERO ANCORA FINITI...

Anche se il lavoro a domicilio, remoto e mobile, era molto comune per alcune aziende, in pochissimo tempo è diventato una necessità per tutte e costituisce ormai la nuova normalità.

Per le organizzazioni di tutto il mondo, questo cambiamento a lungo termine delle modalità di lavoro ha improvvisamente creato nuove problematiche di sicurezza da affrontare. La diffusione dello smart working, il cambiamento degli schemi comportamentali e ambienti completamente nuovi sono tutti fattori che contribuiscono ad aumentare le responsabilità per la sicurezza delle informazioni.

Perché nonostante questi cambiamenti, le informazioni restano ancora la linfa vitale delle aziende e la loro protezione

costituisce un imperativo. E quindi, mentre il confine tra lavoro remoto e lavoro d'ufficio diventa sempre più sottile, come si può garantire la protezione costante dei dati? Come influisce l'evoluzione dell'utilizzo dei dati sulla sicurezza delle informazioni e sulle procedure di lavoro moderne? E come si può garantire la sicurezza richiesta da aziende e clienti anche in un ambiente di lavoro decentralizzato?

Le nuove esigenze di protezione delle informazioni impongono la definizione di strategie per la gestione dei processi, degli strumenti e dei criteri necessari al fine di prevenire, rilevare e contrastare le minacce alle informazioni digitali e cartacee nell'ambito di una forza lavoro decentralizzata e attivamente mobile.

...ORA LO SONO

In questo clima, un approccio completo e proattivo alla sicurezza si sta rapidamente trasformando in un fattore importante per distinguersi dalla concorrenza.

Per implementarlo correttamente è necessaria una visione più olistica del modo in cui i dati vengono utilizzati e archiviati, sia fisicamente che digitalmente, e per tutto il ciclo di vita dei documenti in cui si trovano.

Canon, riconosciuta da IDC MarketScape come leader mondiale nel campo dei servizi e delle soluzioni di sicurezza¹, ti aiuterà a comprendere le caratteristiche e le problematiche di una forza lavoro altamente flessibile e di un ambiente di lavoro che potrebbe trovarsi in qualunque parte del mondo.

PREFAZIONE DI QUENTYN TAYLOR

Direttore del reparto Information Security di Canon EMEA

All'inizio del 2020, mentre esaminavamo le prospettive per il nuovo anno, ben pochi avrebbero immaginato la portata del cambiamento che ci saremmo trovati di fronte. L'ambiente di lavoro si è trasformato e, in molti casi, è presente ovunque sia disponibile una connessione Internet, accelerando una visione del lavoro che stava solo iniziando ad apparire come normale.

Ma il lavoro a domicilio, remoto e mobile si è rapidamente imposto come standard aziendale, e in tutto il mondo le aziende si stanno adattando rapidamente, per garantire la sicurezza di operazioni distribuite fra paesi e continenti diversi. Ovunque si svolgano le attività, le aziende devono integrare la sicurezza nelle strutture, nei processi e nelle procedure di gestione delle informazioni utilizzati quotidianamente.

In questo documento vengono esaminate le problematiche generate dal cambiamento e le varie modalità di protezione delle informazioni, ovunque si trovi l'ambiente di lavoro dei dipendenti".



SEZIONE 1:

IL PANORAMA ATTUALE

I PROBLEMI DI SICUREZZA SONO ONNIPRESENTI, ALL'INTERNO E ALL'ESTERNO DELL'AZIENDA, E POSSONO ESSERE **INTENZIONALI O ACCIDENTALI**

L'evoluzione rapida degli ambienti di lavoro determina un incremento della probabilità di violazione. Ma l'impatto sull'utile e sulla reputazione dell'azienda rimane costante.

Le nuove procedure lavorative adottate da tutte le aziende aumentano l'esposizione al rischio, perché le imprese stanno accelerando il passaggio ai servizi basati su cloud che consentono di lavorare ovunque, continuando a incrementare il carico sull'infrastruttura esistente.

Ma le informazioni aziendali non sono minacciate solo dai pericoli esterni. Le nuove procedure, i nuovi comportamenti e i nuovi endpoint comportano tutti un rischio associato all'utente, che viene ulteriormente amplificato dalla natura stessa del lavoro fuori ufficio, potenzialmente privo di confini.

MINACCE INTERNE

Le minacce interne sono un rischio che si crea **all'interno dell'azienda stessa.**

Esse riguardano dipendenti, ex-dipendenti, collaboratori o partner commerciali, che dispongono di informazioni interne e hanno accesso alle procedure di sicurezza, ai dati e ai sistemi informatici dell'azienda.

Anche se tali minacce non costituiscono certo una novità, la loro natura si sta evolvendo.

Con persone che utilizzano le risorse hardware e software aziendali da posizioni sempre più distribuite e per periodi di tempo sempre più lunghi, la gestione, il recupero e la protezione remota dei dispositivi utilizzati e dell'accesso alle informazioni che contengono diventano sempre più problematici.

Come se non bastasse, possono verificarsi perdite interne causate da persone che desiderano danneggiare l'azienda o trarre profitto dalla violazione, ma anche perdite accidentali dovute all'errore umano. Le minacce possono costituire un problema quotidiano dovuto a una mancanza di attenzione alla sicurezza o all'introduzione di dispositivi di rete in ambienti con protocolli di protezione poco chiari.

Lavorare in ambienti non familiari, configurazioni domestiche inappropriate, aree pubbliche o spazi di co-working non fa che aumentare il rischio di perdita accidentale.



Il 51%

delle violazioni dei dati
viene attribuito a **criminali**
o **malintenzionati**²





Il 24%

è dovuto alla **negligenza** di dipendenti o collaboratori³

VIOLAZIONI DEI DATI

Le violazioni dei dati possono provocare enormi danni reputazionali ed economici, senza distinzione fra le persone che lavorano da casa o in ufficio.

Si verifica una violazione dei dati quando le informazioni personali conservate da un'azienda vengono perse, utilizzate in modo inappropriato oppure consultate, modificate o divulgate senza autorizzazione, a causa di un errore umano, della mancata applicazione delle misure di sicurezza o di azioni nocive compiute da parti esterne.

Anche in un momento di crisi internazionale, le aziende non sono immuni agli attacchi informatici che possono causare una violazione. Infatti, nelle prime fasi della pandemia di COVID-19 i criminali informatici hanno colpito aziende di tutti i settori, determinando un aumento del 38% negli attacchi alle banche o altri istituti finanziari e un notevole incremento di quelli rivolti ai settori sanitario e retail⁴.

Mentre il lavoro remoto si sta rapidamente imponendo come standard, i criminali informatici escogitano nuovi metodi per sfruttare le vulnerabilità della forza lavoro distribuita.

In particolare, mentre le strategie aziendali per l'ambiente di lavoro si evolvono, la configurazione errata di sistemi o applicazioni utente può determinare una violazione dei dati.



DISPOSITIVI CONNESSI IN RETE

L'hardware connesso alla rete aziendale può esporre ai malintenzionati i dati contenuti in tali dispositivi.

Anche i dispositivi privi di controlli di sicurezza appropriati possono essere utilizzati come punto di accesso all'ambiente aziendale e ai sistemi in cui sono conservate le informazioni sensibili.



Fino a poco tempo fa tale rischio era limitato all'hardware d'ufficio e ai dispositivi personali soggetti a protocolli di controllo rigorosi.

Con l'aumento dello smart working e del co-working, il numero degli endpoint connessi rappresenta una minaccia ancora sconosciuta.

Anche se l'85%⁵ adotta già iniziative BYOD (Bring Your Own Device), le reti e i protocolli in uso non sono in genere progettati per supportare l'intera forza lavoro. Solitamente tali criteri vengono applicati solo ai dispositivi più essenziali.

Tuttavia, prevedendo condizioni di lavoro da remoto più permanenti, un numero sempre crescente di dispositivi non protetti normalmente utilizzati in ufficio, come stampanti e scanner, comincerà a connettersi alla rete aziendale, senza essere soggetto alla governance e ai criteri di sicurezza centrali.



SEZIONE 1: IL PANORAMA ATTUALE

Come se non bastasse, l'aumento improvviso e imprevisto dei lavoratori remoti ha aumentato il ricorso a servizi consumer per le necessità quotidiane, come chiamate in conferenza, elaborazione di documenti e condivisione di file, in un intervallo di tempo incredibilmente breve.

Da un momento all'altro gli utenti hanno iniziato a condividere le informazioni aziendali tramite applicazioni consumer situate all'esterno della rete aziendale, che non sono monitorate dal reparto IT e che, presentando vulnerabilità alla sicurezza non verificate, espongono al rischio le informazioni elaborate.

Le aziende faticano a tenere il passo con questo improvviso aumento del numero e della varietà delle minacce alla sicurezza. Inoltre, questo clima di incertezza viene costantemente alimentato dal bombardamento mediatico, che attira l'attenzione sulle minacce rappresentate dagli hacker e da virus sempre più nocivi e sofisticati.

Questa pericolosa combinazione ha distratto i team di sicurezza, permettendo alle minacce di diffondersi senza controllo all'insaputa di tutti. In molti casi tali vulnerabilità sono rimaste aperte per giorni, settimane o addirittura mesi.

E mentre la gestione della sicurezza informatica è focalizzata soprattutto su computer e processi online, è importante sottolineare che le informazioni aziendali sono sparse ovunque e si spostano di continuo, oppure si trovano in ambienti sconosciuti e non monitorati.

La posizione in cui il personale interagisce con sistemi e documenti costituisce l'area più vulnerabile della sicurezza aziendale. Oggi tale interazione si verifica in un numero di luoghi e punti di contatto senza precedenti.



SEZIONE 2:

UNA NUOVA CONCEZIONE DELL'AMBIENTE DI LAVORO



UNA NUOVA CONCEZIONE DELL'AMBIENTE DI LAVORO

In un mercato costantemente interconnesso, è necessario un ambiente che consenta di lavorare senza temere alcuna violazione dei dati. **Ma non è sempre facile.**

Insieme al numero dei punti in cui i lavoratori condividono e richiedono dati, aumentano anche le vulnerabilità.

Da un recente sondaggio Gartner emerge che, dopo il COVID 19, quasi tre CFO su quattro prevedono di lasciare in posizioni remote permanenti il 5% dei dipendenti che in precedenza lavoravano in sede⁶. Le multinazionali di alto profilo, come Twitter, hanno adottato misure radicali per l'evoluzione dell'ambiente di lavoro, implementando una politica di smart working permanente nel maggio 2020⁷.

Tali misure, e tutto quello che influisce sulle modalità e sulle posizioni in cui i dipendenti interagiscono con i dati aziendali, comportano importanti problemi di sicurezza.



Che si lavori da casa, in viaggio o in ambienti di lavoro condivisi...

...ci saranno conseguenze di vasta portata sulla sicurezza e sulla gestione delle informazioni, che si protrarranno ancora per molto tempo nel futuro "dell'ufficio", qualunque esso sia.

OGGI LE PERSONE LAVORANO IN MOLTI LUOGHI DIVERSI

E ciascuno di essi comporta problemi di sicurezza unici, mentre il concetto di "ambiente di lavoro" sta diventando sempre più fluido.

In tutti questi ambienti, la protezione dei dati contenuti nei documenti fisici e digitali implicherà nuove problematiche e considerazioni:



MOBILE WORKING



Dispositivi facilmente persi o rubati



Procedure incoerenti per la protezione di hardware e software



Informazioni utilizzate e connesse tramite connessioni Internet pubbliche e a volte non sicure



SMART WORKING



Endpoint consumer non protetti, situati al di fuori della rete aziendale



Connessioni Internet consumer con difese variabili



Monitoraggio dell'utilizzo e controllo dell'accesso appropriati



CO-WORKING



Dispositivi e connessioni
Internet pubbliche



Dispositivi e connettività
controllati da terze parti
sconosciute



Mancanza di controllo
dell'accesso ad hardware e
strutture





Quale che sia la configurazione dell'ambiente di lavoro

aziendale, e probabilmente include una combinazione di tutti questi ambienti, è essenziale comprendere come mantenere lo stesso standard di sicurezza delle informazioni, sia che il personale lavori all'interno dell'ufficio sia che sia seduto sul divano di casa propria.





SEZIONE 3

PROTEZIONE DELLE INFORMAZIONI



PROTEZIONE DELLE INFORMAZIONI

Anche prima della decentralizzazione della forza lavoro in massa a cui stiamo assistendo oggi, il ciclo di vita dei documenti che contengono le informazioni fisiche e digitali alla base del business era spesso lungo e complesso, e pertanto caratterizzato da numerosi punti deboli.

Per loro stessa natura, nei moderni flussi di lavoro sempre più automatizzati i dati creati o acquisiti digitalmente vengono spesso memorizzati in più posizioni o elaborati più volte.

Il trasferimento non protetto dei dati fra sistemi degli utenti, aree di archiviazione cloud e dispositivi endpoint, come le stampanti, può introdurre più vulnerabilità, a cui si aggiunge il rischio che i documenti stampati fisicamente cadano nelle mani sbagliate, accidentalmente o intenzionalmente.

Quando tali endpoint non risiedono tutti nell'ambiente d'ufficio aziendale, in una rete gestita centralmente, tale rischio si amplifica.

Per evitare minacce come quelle illustrate in questa guida ed esaminare i potenziali punti deboli in un ambiente globale con più persone che lavorano da remoto, è essenziale che i dipendenti abbiano la possibilità di condividere agevolmente le informazioni in sicurezza tra i dispositivi edge (dispositivi consumer e così via) e il cloud.

Per contribuire all'eccellenza operativa delle iniziative di sicurezza nell'intera azienda, è essenziale adottare una strategia che preveda una sicurezza più profonda per progettazione nei processi di gestione dei documenti.

Anche se la tendenza a lavorare ed elaborare le informazioni da remoto sta accelerando, le aziende avevano già previsto tale evoluzione.

Proprio per questo, Canon ha sviluppato un approccio semplificato alla protezione delle informazioni, che permette di tutelarle indipendentemente dalla posizione in cui vengono consultate, gestite ed elaborate.

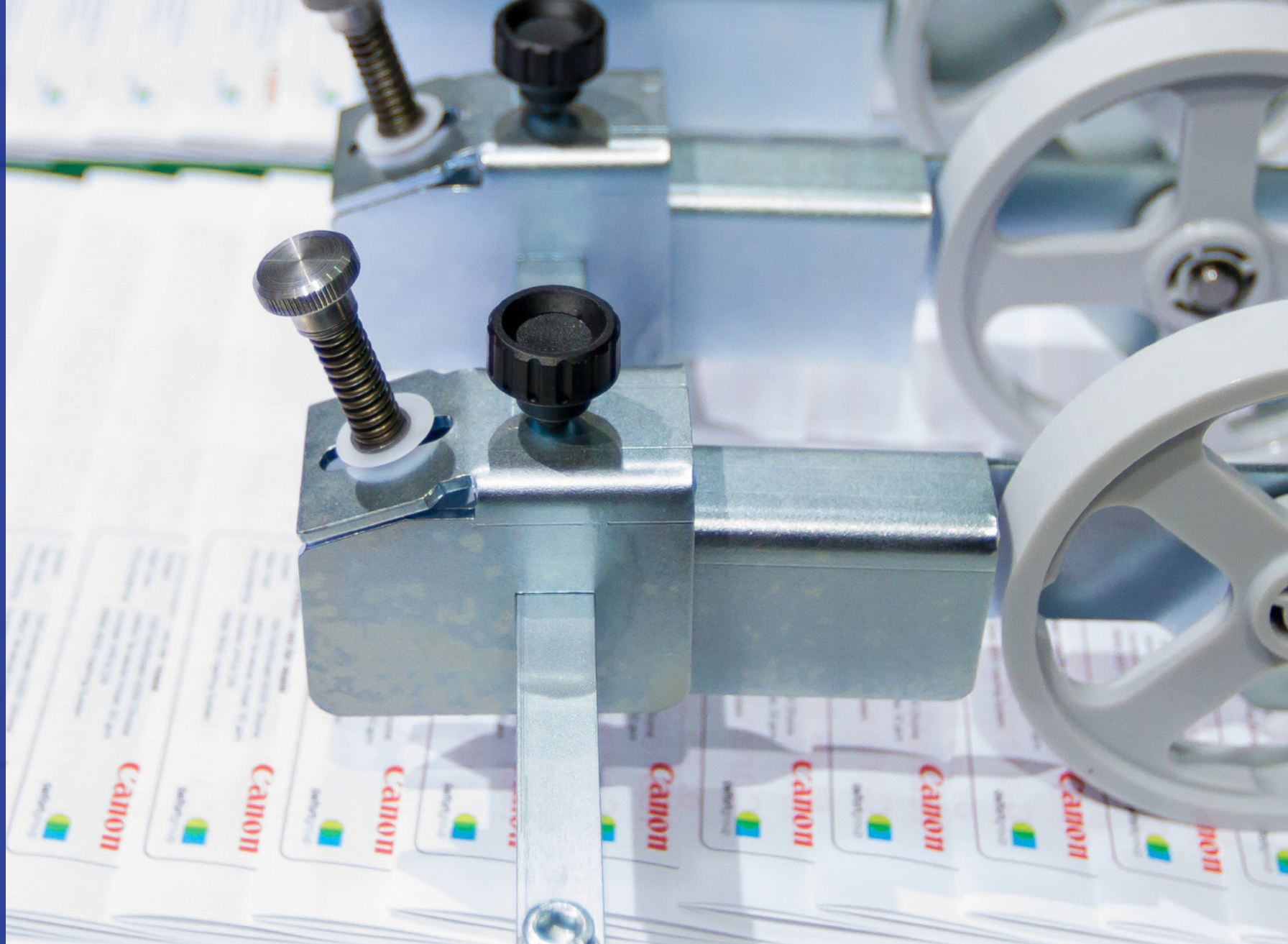
A tale scopo, è necessario garantire una sicurezza costante dei dati per tutto il ciclo di vita delle informazioni:



GESTIONE DELLA STAMPA

Proteggere il processo di invio dei documenti in stampa, fino al rilascio dell'output stampato presso il dispositivo.

Prevenire le violazioni dei dati proteggendo i dispositivi di stampa connessi alla rete e tutelando tutte le attività degli utenti correlate alla stampa.





GESTIONE DELL'ACQUISIZIONE

Proteggere la digitalizzazione dei documenti cartacei e la relativa distribuzione alla destinazione desiderata.

Migliorare la sicurezza dei documenti controllando l'accesso alle funzionalità di scansione e proteggendo i documenti digitalizzati.

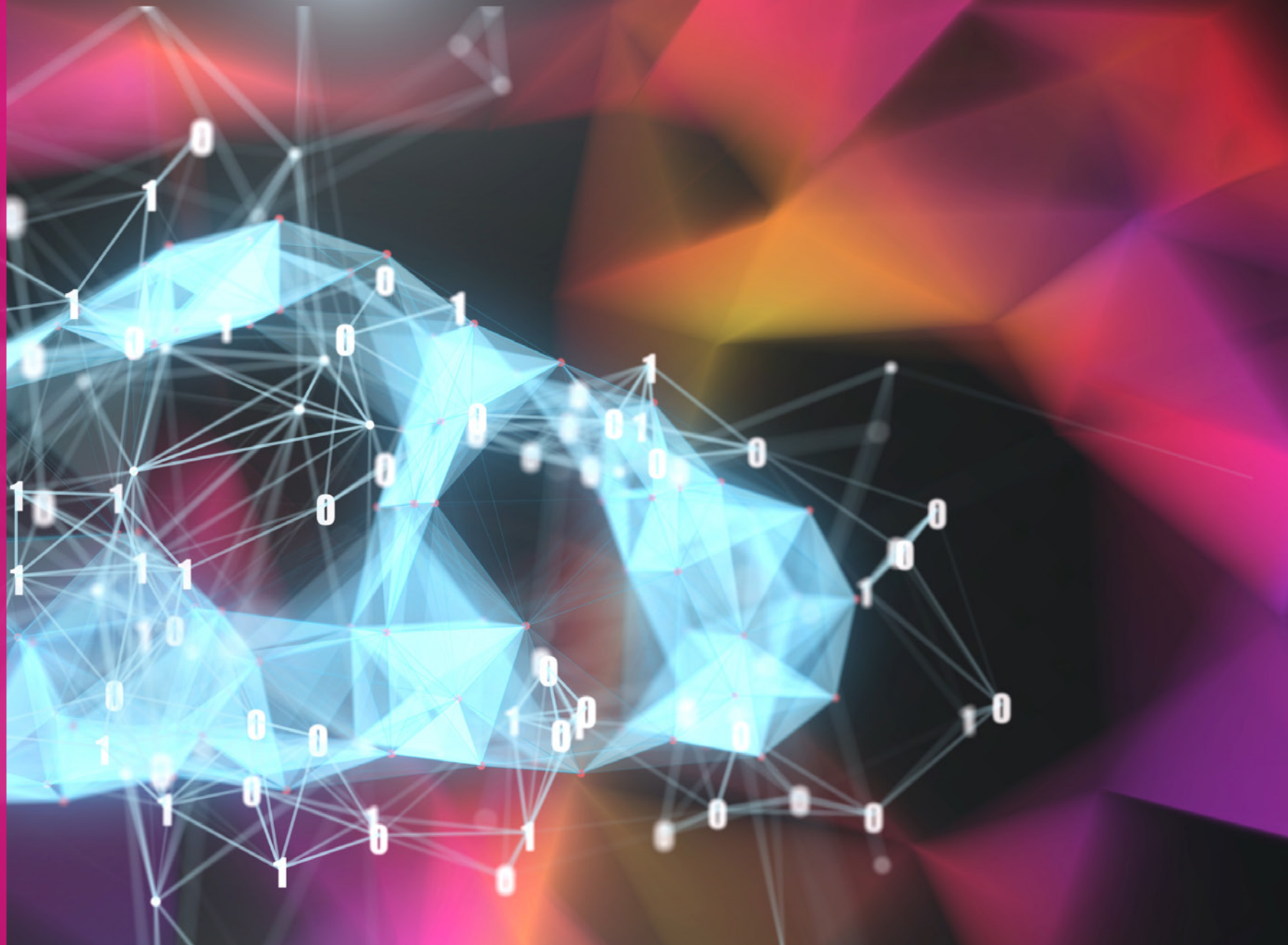




GESTIONE DI DOCUMENTI E CONTENUTI

Proteggere l'archiviazione e l'elaborazione dei documenti, sia nelle applicazioni on-premise che nel cloud. Assicurare la conformità alle normative sulla protezione dei dati e rafforzare le misure di sicurezza per documenti e contenuti.

Per garantire la coerenza fra queste fasi del ciclo di vita delle informazioni, ovunque si svolgano le attività, le aziende devono integrare la sicurezza nelle strutture, nei processi e nelle procedure di lavoro quotidiani.





SEZIONE 4

PERCHÉ SCEGLIERE CANON



PERCHÉ SCEGLIERE CANON



I nostri servizi e soluzioni consentono di proteggere tutti i documenti e i dati sensibili, in formato digitale o cartaceo, per tutto il ciclo di vita dei documenti, senza interferire sulla capacità degli utenti di accedere alle informazioni necessarie per svolgere il proprio lavoro.

Il nostro obiettivo è aiutare le aziende ad assumere il controllo delle informazioni e a mantenere un ambiente di lavoro sicuro.

GRAZIE A TALE APPROCCIO ALLA GESTIONE DELLE INFORMAZIONI, CANON È STATA RICONOSCIUTA DA IDC MARKETScape COME LEADER MONDIALE NEL CAMPO DEI SERVIZI E DELLE SOLUZIONI DI SICUREZZA⁸.

Per la nostra comprensione olistica dell'ecosistema di stampa, acquisizione e gestione delle informazioni, ci troviamo nella posizione ideale per aiutare le aziende a raggiungere i propri obiettivi cruciali di protezione dei documenti, nel loro percorso verso l'eccellenza operativa della sicurezza.

Mentre un documento viene creato, condiviso, stampato o memorizzato nel cloud, la nostra soluzione end-to-end permette alle aziende di gestire le informazioni in modo sicuro e conforme ai criteri interni, utilizzando funzionalità come l'autenticazione degli utenti, i controlli di manomissione del firmware e la crittografia dei dati archiviati e in transito.

Questo ci consente di distinguerci come partner, grazie a un approccio alla sicurezza esaustivo e a prova di futuro, che garantisce la protezione delle aziende e dei loro clienti.

PERCHÉ SCEGLIERE CANON



Per allineare efficacemente le operazioni aziendali e di sicurezza è spesso necessario l'aiuto di un partner che vanta una lunga esperienza globale.

Rivolgendosi a un partner affidabile e competente, si può avere la certezza che i processi e i sistemi aziendali per la gestione di informazioni e documenti supportino un'evoluzione dell'ambiente di lavoro incentrata sulla protezione, anziché esporre l'organizzazione a rischi per la sicurezza, persino quando l'azienda prevede di adottare velocemente procedure lavorative cloud-first.

In particolare, fornendo servizi che promuovono la trasformazione digitale, supportando il passaggio a procedure di lavoro che sono sicure per progettazione e vengono riviste regolarmente per far fronte a un panorama tecnologico, normativo e di sicurezza informatica in continua evoluzione, possiamo aiutare le aziende a garantire che i documenti vengano gestiti in sicurezza per tutto il loro ciclo di vita, in qualsiasi punto dell'azienda.

L'attenzione di Canon all'evoluzione dell'ambiente di lavoro ci permette di considerare tutti gli aspetti della sicurezza delle informazioni nell'ambito della fornitura di qualunque soluzione per il cliente.

In qualità di partner, Canon può fornire affidabili processi di gestione dei servizi, soluzioni integrate, una tradizione di innovazione e personale specializzato competente. Le nostre soluzioni hardware e software affidabili, collaudate e testate consentono di assumere il controllo delle informazioni per tutto il ciclo di vita dei documenti.



Queste soluzioni sono testate per misurare la vulnerabilità in termini di sicurezza nell'ambito delle nostre procedure di lancio standard, prima dell'introduzione sul mercato, allo scopo di garantire la sicurezza dell'ambiente di lavoro fin dal primo giorno e in qualsiasi ambiente di lavoro.



SECURE BY-DESIGN

Canon garantisce la conformità agli standard di settore per ridurre al minimo il rischio di violare le disposizioni GDPR fin dalla progettazione dei requisiti di sicurezza dei prodotti.

La governance centralizzata dell'infrastruttura di stampa e gestione dei documenti assicura un approccio coerente e semplifica l'amministrazione dei protocolli di sicurezza.



DEFINIAMO GLI STANDARD DI SETTORE

Canon Europe è certificata per la conformità allo standard ISO 27002 sulla sicurezza delle informazioni ed è orgogliosa di fare parte alle principali organizzazioni responsabili della regolamentazione del settore e di definirne l'orientamento futuro.



UN PARTNER PER LA SICUREZZA

L'approccio "secure by-design" garantisce la verifica della sicurezza di tutti i prodotti e servizi Canon prima della commercializzazione.

Canon fornisce inoltre indicazioni dettagliate su come configurare i dispositivi e il software per ottimizzarne la sicurezza, mentre un singolo team di sicurezza europeo protegge la nostra organizzazione e garantisce la sicurezza dei clienti.



LE PERSONE AL CENTRO DELLA SICUREZZA

Tutti i dipendenti sono tenuti a seguire corsi di formazione sui comportamenti consigliati per la sicurezza dei dati, mentre i nostri addetti vengono valutati individualmente in background prima di presentarsi presso la sede del cliente.

I nostri termini e condizioni includono un codice di condotta per la sicurezza dei dati dei clienti.

È proprio grazie a queste procedure e agli standard definiti dal personale che la nostra azienda viene riconosciuta da tutto il settore come leader nel campo della sicurezza delle informazioni.

LA NOSTRA ESPERIENZA

L'esperienza di Canon nella gestione dei flussi di lavoro, dell'ottimizzazione dei processi e delle informazioni può aiutare le aziende che desiderano contenere i rischi per la sicurezza, fornendo dispositivi e soluzioni che consentono agli utenti di proteggere e potenziare le difese degli asset, semplificare i processi, ridurre al minimo i punti di contatto e aumentare la protezione delle informazioni business-critical⁹.

ROBERT PALMER

VICEPRESIDENTE DEL REPARTO RICERCA, IDC



La portata globale di Canon, insieme alla sua capacità di operare a livello locale, offre all'azienda una base solida per l'adozione di un approccio olistico alla risoluzione dei problemi aziendali, inclusa l'esigenza di proteggere l'infrastruttura di stampa e documenti.

L'approccio Canon non si limita all'ambiente di lavoro, ma si estende all'evoluzione di servizi e soluzioni di sicurezza che includono la videosorveglianza, mentre i suoi esperti in materia internazionali aiutano attivamente i clienti ad affrontare i problemi di sicurezza e contenere i rischi in qualsiasi mercato verticale, reparto e applicazione.

Quando un documento viene creato, condiviso, stampato o memorizzato nel cloud, l'approccio completo di Canon alla protezione delle informazioni consente all'azienda di gestire le informazioni in tutta sicurezza, in conformità con i ai criteri interni.

CANON È SINONIMO DI IMAGING.



E noi utilizziamo l'imaging per fare la differenza e promuovere il cambiamento.

Per i nostri clienti che intraprendono la trasformazione digitale e hanno cambiato il loro modo di lavorare. Per il cambiamento sociale in generale, grazie un'attenzione continua alla sostenibilità che è parte integrante della tradizione e della cultura della nostra azienda.

Infine, stiamo cambiando il nostro modo di investire in nuovi mercati, prodotti e tecnologie al fine di continuare a lavorare ancora per molto tempo a beneficio di tutti: dei nostri clienti, dei nostri dipendenti e dell'intera società.



CANON SI BASA SU 4 VALORI PRINCIPALI:



Innovazione

Una lunga tradizione di innovazione incentrata sulle immagini, che ci permette di realizzare tecnologie all'avanguardia da più di 80 anni. Nel nostro settore siamo sempre i primi a sperimentare le nuove soluzioni e ci impegniamo al massimo per lo sviluppo futuro della tecnologia.



Supporto

Offriamo un portafoglio di servizi diversificato per garantire la massima qualità, assicurando la soddisfazione dei clienti. I nostri esperti interni fanno tutto il possibile per migliorare l'efficienza e aiutare i clienti a esprimere il loro potenziale.



Sicurezza

Le soluzioni e i servizi Canon consentono di proteggere tutti i documenti e i dati sensibili, in formato digitale o cartaceo, per l'intero ciclo di vita dei documenti. I nostri servizi e soluzioni sono sicuri per progettazione, perché vengono concepiti pensando alla sicurezza.



Sostenibilità

Canon ha allineato le sue procedure per la sostenibilità agli Obiettivi di sviluppo sostenibile delle Nazioni Unite, come l'impegno a ridurre le emissioni di CO2 nell'intero ciclo di vita dei prodotti, riducendo le dimensioni degli imballaggi e consolidando i centri di distribuzione.

Tutti insieme, questi elementi fanno di Canon **il partner ideale per la tua azienda.**

RIFERIMENTI

- 1 IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2019-2020 Vendor Assessment Doc #US44811119, dicembre 2019
- 2 IBM Security - Cost of a Data Breach Report 2019
- 3 IBM Security - Cost of a Data Breach Report 2019
- 4 Carbon Black
- 5 Bitglass
- 6 Comunicato stampa di Gartner "Gartner CFO Survey Reveals 74% Intend to Shift Some Employees to Remote Work Permanently", aprile 2020
- 7 The Guardian
- 8 IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2019-2020 Vendor Assessment Doc #US44811119, dicembre 2019
- 9 IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2019-2020 Vendor Assessment Doc #US44811119, dicembre 2019



Desideri ulteriori informazioni su come prepararti per il panorama aziendale del futuro?

Scarica la nostra guida all'ambiente di lavoro del futuro.

Oppure **visita il nostro sito** o **contatta il nostro team** per scoprire di più sulle soluzioni Canon per la sicurezza delle informazioni.

Canon Inc.
canon.com

Canon Europe
canon-europe.com

Italian edition /canon.it
© Canon Europa N.V. 2020

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
Richtstrasse 9
CH-8304 Wallisellen
Tel. +41 (0)22 567 58 58
canon.ch

Canon
