CLOUD
CONFERENCE
ITALIA

HANDBOOK

Proteggere dati aziendali e identità sensibili: il modello Zero Trust

L'adozione di una strategia Zero Trust end-to-end è fondamentale per modernizzare il livello di sicurezza e superare gli standard normativi e di conformità richiesti.

Ad oggi, le imprese vanno incontro ad una sfida importante: **bilanciare l'accesso alle informazioni con la privacy di consumatori e utenti**.
La difficoltà sta nel trovare le soluzioni e le misure GDPR compliant, per poter legittimamente accedere ai dati e sfruttarli per innovare e rimanere competitivi.

Con il passaggio al modello di lavoro ibrido, chi si occupa di sicurezza informatica deve **rafforzare e proteggere i confini in crescita**.

Non solo, con l'evolversi dei requisiti normativi e di conformità in risposta alle trasformazioni tecnologiche, le organizzazioni devono **modernizzare il loro livello di sicurezza** per proteggere i dati e i processi sensibili.

Un framework Zero Trust è una strategia di sicurezza completa che consente di preparare l'organizzazione alle minacce future.

Introduzione

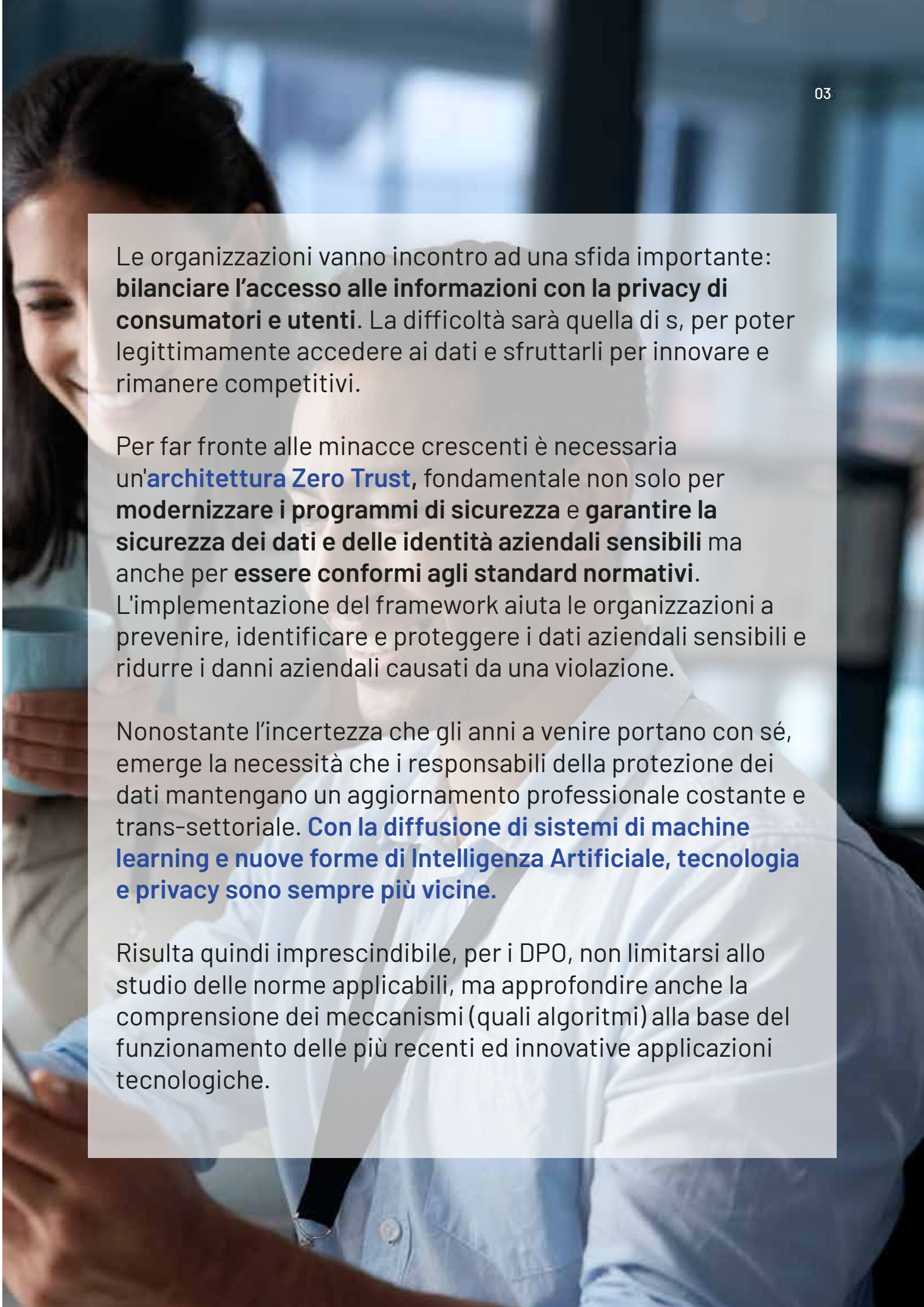
Il 2023 ha visto un record complessivo di ammende comminate, ai sensi del GDPR, dalle Autorità di controllo privacy di tutta Europa: per un totale di 1,78 miliardi di euro, con un incremento netto del 14% rispetto ai 1,64 miliardi di euro del 2022.

La protezione delle persone fisiche e giuridiche dai pericoli che possono celarsi dietro ad una rete internet è infatti una delle principali preoccupazioni dell'UE, che nel 2018 ha sviluppato il GDPR (General Data Protection Regulation).

L'aumento delle ammende dimostra la crescente attenzione di consumatori e imprese rispetto alle violazioni del Regolamento, la cui corretta attuazione viene accertata dall'EDPB, l'European Data Protection Board.

Allo stesso tempo, i dati riportati sono stati influenzati dall'impatto inflazionistico del comitato che nei casi in cui è stato attivato il meccanismo di coerenza del GDPR, ha chiesto in media un aumento del 630% rispetto all'ammenda originaria.

Al centro della questione, l'accordo tra i fornitori di servizi online e i consumatori: social media, motori di ricerca e altri servizi innovativi vengono offerti al pubblico anche gratuitamente in cambio dei dati personali dei consumatori. **Consentire ai fornitori di raccogliere i dati personali, è diventato un prerequisito per finanziare l'innovazione e lo sviluppo di molte tecnologie avanzate, con tangibili benefici per la società**.



Le organizzazioni vanno incontro ad una sfida importante: **bilanciare l'accesso alle informazioni con la privacy di consumatori e utenti**. La difficoltà sarà quella di s, per poter legittimamente accedere ai dati e sfruttarli per innovare e rimanere competitivi.

Per far fronte alle minacce crescenti è necessaria un'**architettura Zero Trust,** fondamentale non solo per **modernizzare i programmi di sicurezza** e **garantire la sicurezza dei dati e delle identità aziendali sensibili** ma anche per **essere conformi agli standard normativi**. L'implementazione del framework aiuta le organizzazioni a prevenire, identificare e proteggere i dati aziendali sensibili e ridurre i danni aziendali causati da una violazione.

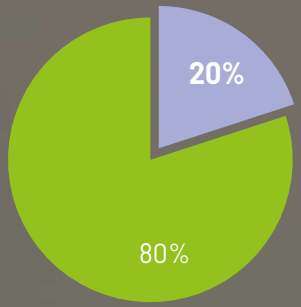
Nonostante l'incertezza che gli anni a venire portano con sé, emerge la necessità che i responsabili della protezione dei dati mantengano un aggiornamento professionale costante e trans-settoriale. **Con la diffusione di sistemi di machine learning e nuove forme di Intelligenza Artificiale, tecnologia e privacy sono sempre più vicine.**

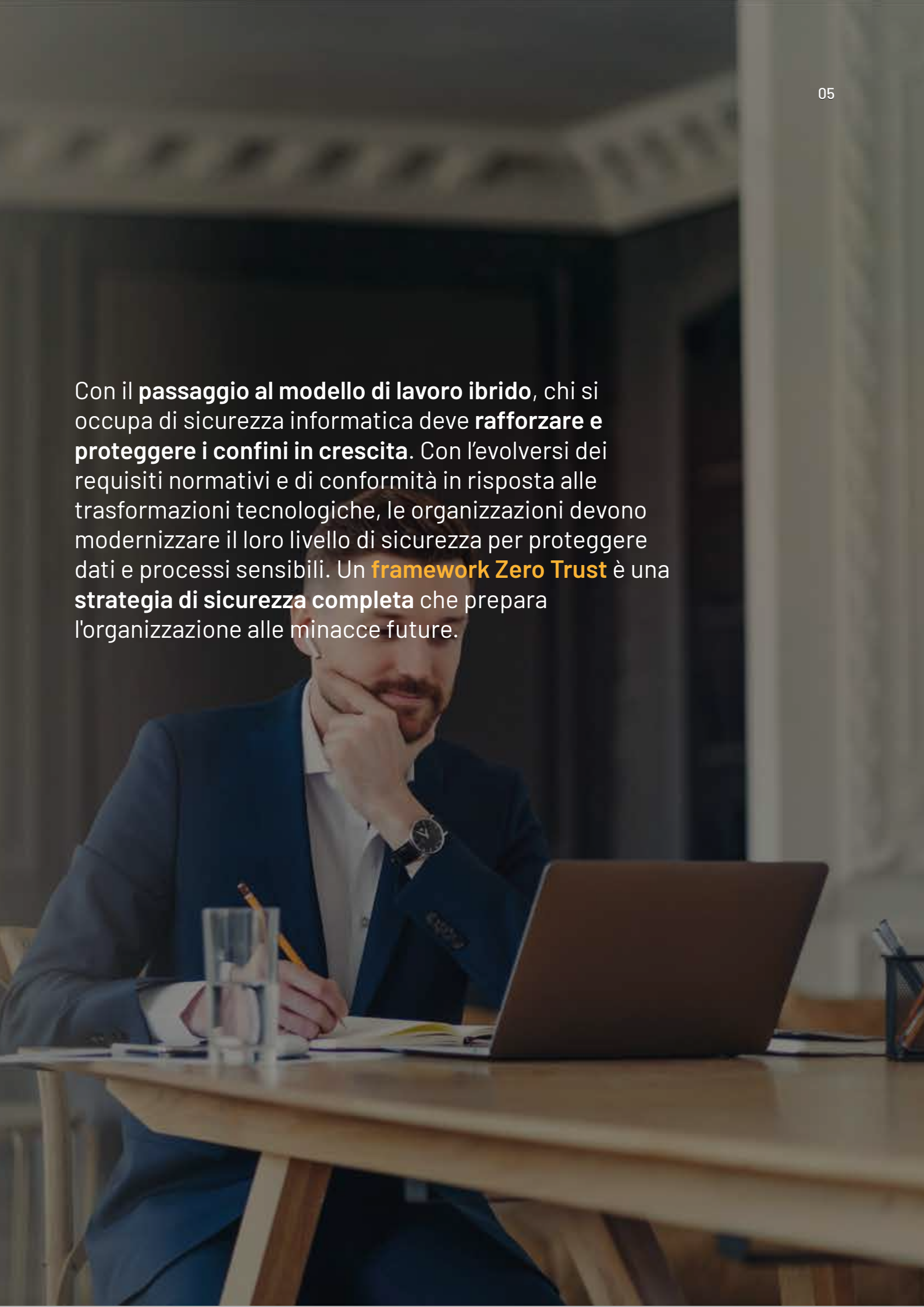
Risulta quindi imprescindibile, per i DPO, non limitarsi allo studio delle norme applicabili, ma approfondire anche la comprensione dei meccanismi (quali algoritmi) alla base del funzionamento delle più recenti ed innovative applicazioni tecnologiche.

Conformità e protezione dei dati sensibili

Gli standard normativi cambiano e si rafforzano frequentemente, soprattutto con l'aumento degli ambienti di lavoro ibridi e secondo il Cost of a Data Breach Report 2023 di IBM, l'82% delle organizzazioni ha subito più di una violazione dei dati nel corso della propria vita.

Di questi casi, il **20% delle violazioni dei dati** è dovuto ad **attori interni malintenzionati**. Se questa statistica non è sufficiente per illustrare il panorama delle minacce in evoluzione, quasi il **40%** delle organizzazioni ha riferito che il costo medio di una singola violazione dei dati da un evento interno è stato superiore a **500.000 dollari**, con una media di **20 eventi all'anno**, secondo il report **Building a Holistic Insider Risk Management Program.**





Con il **passaggio al modello di lavoro ibrido**, chi si occupa di sicurezza informatica deve **rafforzare e proteggere i confini in crescita**. Con l'evolversi dei requisiti normativi e di conformità in risposta alle trasformazioni tecnologiche, le organizzazioni devono modernizzare il loro livello di sicurezza per proteggere dati e processi sensibili. Un **framework Zero Trust** è una **strategia di sicurezza completa** che prepara l'organizzazione alle minacce future.

Cattivi attori interni o esterni: prevenire l'impatto di una violazione

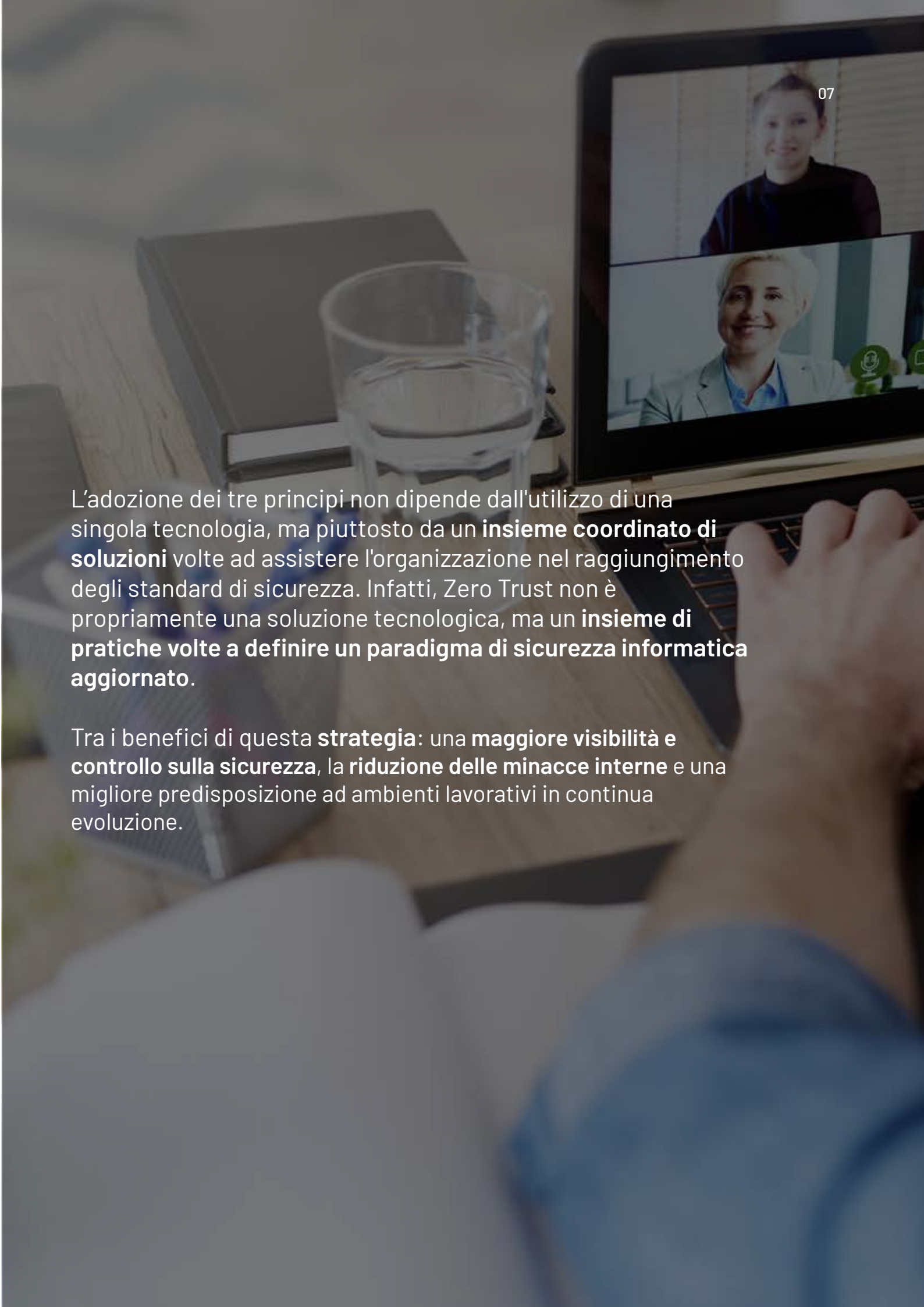
Il concetto di Zero Trust si fonda sul principio che ogni tentativo di accesso alla rete aziendale possa essere potenzialmente pericoloso:
ogni accesso deve essere accuratamente controllato.

Questo approccio si basa su **tre principi cardine**:

1. **Verifica esplicita**: le richieste provenienti da sistemi interni all'azienda non vengono più considerati sicuri, ma ogni richiesta di accesso è trattata come potenzialmente insicura ed è soggetta a verifica.

2. **Principio del privilegio minimo**: le identità che accedono ai dati aziendali devono operare con il più basso livello di privilegi utili al completamento dei loro compiti e questi privilegi devono essere assegnati esclusivamente per la durata delle specifiche operazioni.

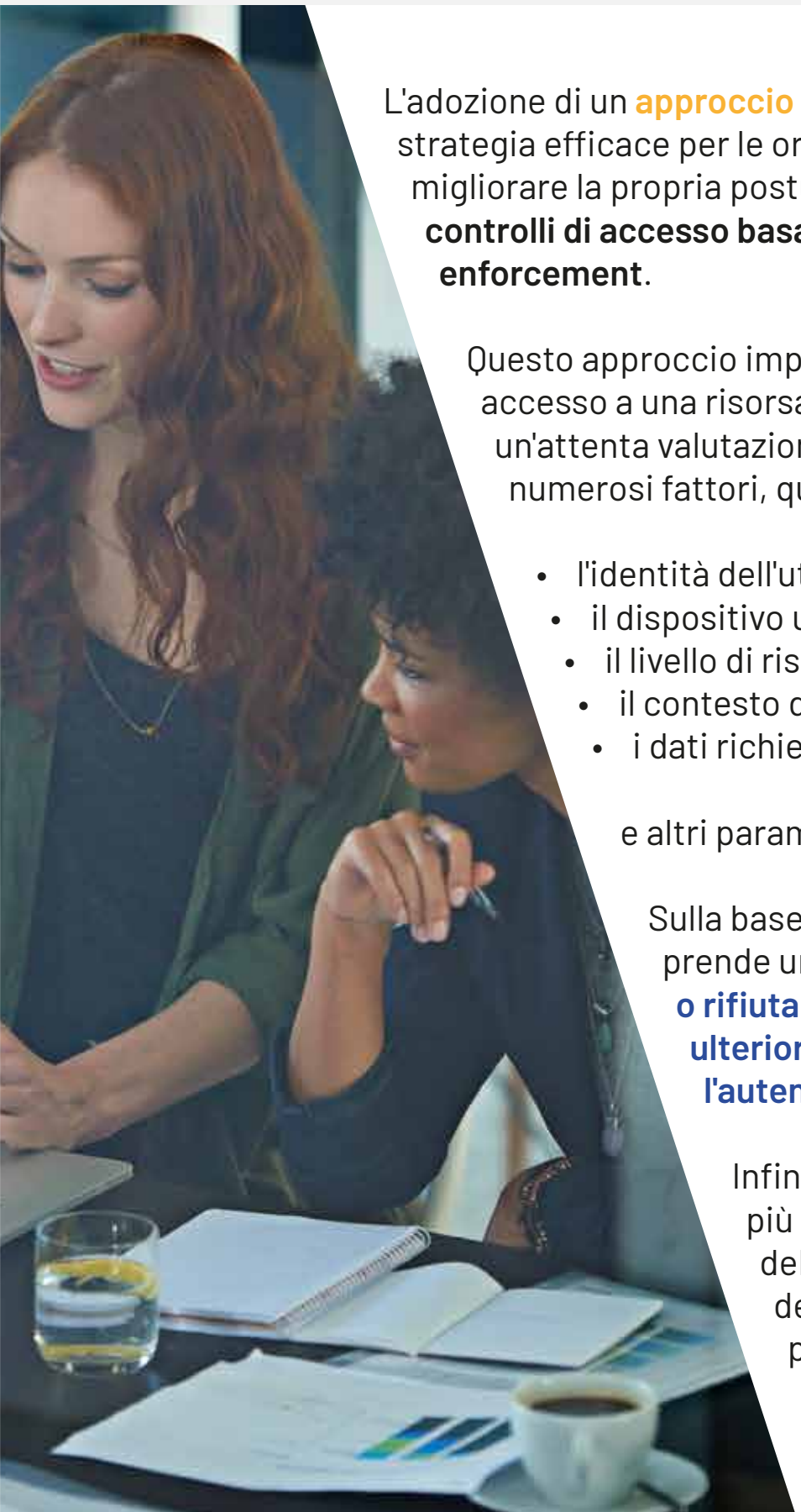
3. **Presunzione di compromissione**: operando sotto l'assunzione che possano esserci minacce già all'interno del network aziendale, vengono effettuati continui monitoraggi sulle attività per rilevare eventuali azioni sospette o non autorizzate.



L’adozione dei tre principi non dipende dall'utilizzo di una singola tecnologia, ma piuttosto da un **insieme coordinato di soluzioni** volte ad assistere l'organizzazione nel raggiungimento degli standard di sicurezza. Infatti, Zero Trust non è propriamente una soluzione tecnologica, ma un **insieme di pratiche volte a definire un paradigma di sicurezza informatica aggiornato**.

Tra i benefici di questa **strategia**: una **maggiore visibilità e controllo sulla sicurezza**, la **riduzione delle minacce interne** e una migliore predisposizione ad ambienti lavorativi in continua evoluzione.

Identificare e proteggere le identità aziendali sensibili



L'adozione di un **approccio Zero Trust** rappresenta una strategia efficace per le organizzazioni che vogliono migliorare la propria postura di sicurezza attraverso **controlli di accesso basati su segnali, decisioni e enforcement**.

Questo approccio implica che ogni richiesta di accesso a una risorsa sensibile sia sottoposta a un'attenta valutazione, tenendo conto di numerosi fattori, quali

- l'identità dell'utente,
- il dispositivo utilizzato,
- il livello di rischio associato,
- il contesto della richiesta,
- i dati richiesti

e altri parametri pertinenti.

Sulla base di questi segnali, il sistema prende una decisione di **autorizzare o rifiutare l'accesso, o di richiedere ulteriori verifiche, come l'autenticazione multifattore**.

Infine, il sistema applica l'azione più adeguata, come l'isolamento della sessione, la crittografia dei dati o la revoca dei privilegi.

Per identificare le risorse che necessitano di essere salvaguardate, le organizzazioni devono innanzitutto effettuare un **inventario di tutti i loro asset digitali**, concentrandosi su:

- **Identità**, che comprende sia gli account degli utenti sia quelli dei vari carichi di lavoro, come le applicazioni usate per accedere alle risorse d'impresa
- **Endpoint**, ovvero i dispositivi che consentono l'accesso alle risorse
- **Applicazioni**, insieme agli endpoint, abilitano l'accesso alle informazioni aziendali
- **Infrastruttura di rete**, la rete interna dell'organizzazione e le reti distribuite attraverso i vari servizi cloud impiegati
- **Dati**, che costituiscono l'asset digitale più prezioso dell' impresa

/ Va quindi valutato il livello di sensibilità e criticità di ciascuna risorsa, in base al valore che riveste per l'organizzazione, al grado di esposizione a potenziali minacce e alla normativa vigente.

Questa valutazione richiede di analizzare diversi aspetti, come la frequenza e la modalità di accesso alla risorsa, il tipo e la quantità di dati che essa contiene o elabora, il livello di protezione attuale e le possibili conseguenze di una violazione.

/ Inoltre, le organizzazioni dovranno considerare le norme e le regolazioni applicabili alla risorsa, in relazione al settore di attività, alla localizzazione geografica, al tipo di dati e alle richieste degli stakeholder.

Questo processo consente di classificare le risorse in base al loro livello di rischio e di priorità, e di definire le misure di sicurezza più appropriate per ciascuna di esse.

Implementare le strategie di protezione delle risorse sensibili

Una volta individuate le risorse critiche da difendere, la loro vulnerabilità e le conseguenze potenziali su di esse a seguito di un cyber attacco, si potrà procedere alla valutazione delle misure di protezione più idonee per assicurare l'integrità dell'ambiente.

Le strategie di protezione da implementare si baseranno sulle 5 aree principali discusse nel paragrafo precedente:

Identità: è necessario utilizzare un meccanismo di autenticazione forte, che preveda almeno l'autenticazione a più fattori o, ancora meglio, l'autenticazione passwordless.

Endpoint: è importante che gli endpoint siano mantenuti sempre in uno stato di salute e che avvenga un controllo continuo sulla loro conformità rispetto agli standard aziendali. Dispositivi non gestiti come i dispositivi personali non dovrebbero accedere alle risorse, e nel caso in cui fosse necessario, è importante imporre limitazioni per evitare fughe di dati.

Applicazioni: fondamentale verificare periodicamente lo stato di vulnerabilità delle applicazioni e prevedere un piano di patching.

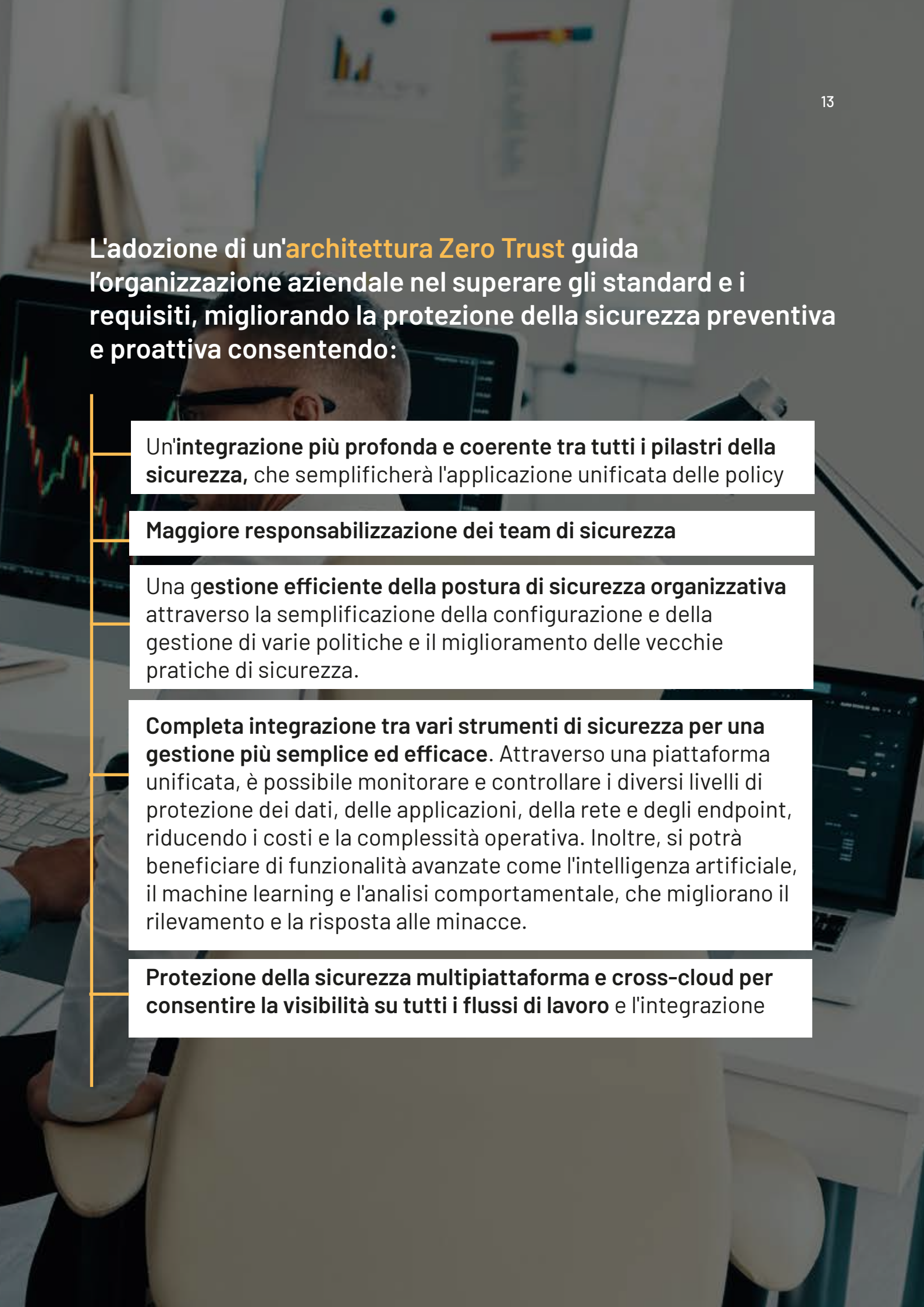
Infrastruttura di rete: una segmentazione della rete permette di rallentare un eventuale attore malevolo nei movimenti laterali in caso di infiltrazione all'interno dei propri sistemi.

Dati: devono essere categorizzati, etichettati e protetti mediante crittografia sia at rest che in transito. Sulla base di queste caratteristiche deve poi essere applicata una strategia di accesso.

Soddisfare i requisiti normativi: un approccio proattivo

Il framework di sicurezza Zero Trust di Microsoft supporta le aziende nel soddisfare gli standard normativi e di conformità per impostazione predefinita, inclusi i requisiti di conformità relativi a dati e legge.

In questo senso, si proteggono dati e informazioni di identificazione personale, dati finanziari, informazioni sanitarie e proprietà intellettuale, tutti ad alto rischio di furto, perdita o esfiltrazione.



L'adozione di un'architettura Zero Trust guida l'organizzazione aziendale nel superare gli standard e i requisiti, migliorando la protezione della sicurezza preventiva e proattiva consentendo:

- Un'**integrazione più profonda e coerente tra tutti i pilastri della sicurezza,** che semplificherà l'applicazione unificata delle policy
- **Maggiore responsabilizzazione dei team di sicurezza**
- Una g**estione efficiente della postura di sicurezza organizzativa** attraverso la semplificazione della configurazione e della gestione di varie politiche e il miglioramento delle vecchie pratiche di sicurezza.
- **Completa integrazione tra vari strumenti di sicurezza per una gestione più semplice ed efficace**. Attraverso una piattaforma unificata, è possibile monitorare e controllare i diversi livelli di protezione dei dati, delle applicazioni, della rete e degli endpoint, riducendo i costi e la complessità operativa. Inoltre, si potrà beneficiare di funzionalità avanzate come l'intelligenza artificiale, il machine learning e l'analisi comportamentale, che migliorano il rilevamento e la risposta alle minacce.
- **Protezione della sicurezza multipiattaforma e cross-cloud per consentire la visibilità su tutti i flussi di lavoro** e l'integrazione

Un **modello Zero Trust** aiuta a comprendere i criteri necessari per soddisfare i requisiti di governance.

Consente valutazioni continue, dall'inventario dei rischi dei dati all'implementazione dei controlli e al mantenimento dell'aggiornamento con normative e certificazioni.

L'adozione di una strategia Zero Trust end-to-end è un passo fondamentale da intraprendere per **modernizzare il livello di sicurezza e superare gli standard normativi e di conformità richiesti**.

Fonti:

- La normativa GDPR in sintesi (gdprset.it)
- Sicurezza dei dati e privacy nel 2023: una guida per DPO (assodpo.it)
- GDPR: il testo aggiornato del Regolamento 2023

+39 049 636 5600
hello@cloudconferenceitalia.it
www.linkedin.com/company/cloud-conference-italia/
www.cloudconferenceitalia.it

CLOUD CONFERENCE ITALIA
Powered by Resolve