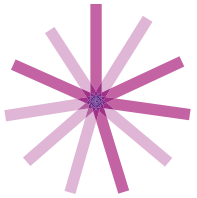
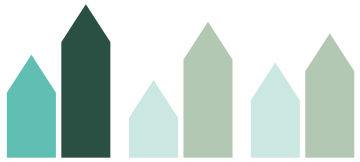
L'IMPERATIVO DELLA SICUREZZA: PROMUOVERE LA CRESCITA DEL BUSINESS NELL'APPLICATION ECONOMY >>

Sponsorizzato da ca technologies

COLEMAN PARKES RESEARCH

Sommario





USO DI QUESTO PDF INTERATTIVO

Le funzioni di interattività variano su tablet e smartphone, a seconda del lettore PDF utilizzato. È possibile che le funzioni di interattività non funzionino quando visualizzi il PDF in modalità di anteprima del messaggio e-mail. È consigliato l'utilizzo di Adobe Acrobat Reader.

HOME (prima pagina) | **SOMMARIO** | **INDIETRO** pagina precedente | **AVANTI** pagina successiva

Executive summary

L'application economy ha cambiato il volto della sicurezza IT. La linea di demarcazione tra l'interno e l'esterno dell'azienda si è praticamente dissolta. Il perimetro della rete aziendale si è non solo spostato; ma anche frammentato. La nuova frontiera della sicurezza si colloca oggi ovunque le persone decidano di accedere alla rete.

Ma questo non è l'unico problema. Clienti, dipendenti e partner si aspettano accesso always-on, senza soluzione di continuità, su qualsiasi device o piattaforma utilizzata.

In questo scenario complesso, le strategie di sicurezza IT tradizionali non saranno più adeguate. Le aziende devono essere in grado di autenticare identità altamente distribuite da più fonti, pur mantenendo una user experience senza attrito. Il punto di equilibrio, tra protezione robusta e soddisfazione degli utenti, è delicato e complesso da ottenere, e richiede un nuovo approccio alla sicurezza, basato sull'identità, che utilizza l'analisi comportamentale e contestuale e approcci maggiormente predittivi per offrire una customer experience coinvolgente, proteggendo al contempo le identità e i dati.

In ultima analisi, la sicurezza basata sull'identità consente di costruire le relazioni digitali affidabili con i clienti che costituiscono la principale risorsa del business nell'application economy.

A partire da questi presupposti, CA Technologies ha commissionato a Coleman Parkes Research un sondaggio condotto su 1.770 dirigenti senior di business e IT, inclusi oltre 100 CSO e CISO. Abbiamo chiesto loro delle pratiche di sicurezza IT che impiegano e di come si pongono circa l'adozione degli elementi chiave della sicurezza basata sull'identità.

Questo ci ha consentito di identificare le pratiche che caratterizzano gli utenti avanzati della sicurezza basata sull'identità, e quale impatto questo loro approccio alla sicurezza sta avendo sui rispettivi business.

Dai nostri risultati emerge chiaramente il valore di business di un nuovo modello di sicurezza digitale: un modello in sintonia con le esigenze dell'application economy, e in grado di trainare miglioramenti reali, che vanno a vantaggio dei ricavi.

La sicurezza basata sull'identità consente di costruire le relazioni digitali affidabili con i clienti che costituiscono la principale risorsa del business nell'application economy.

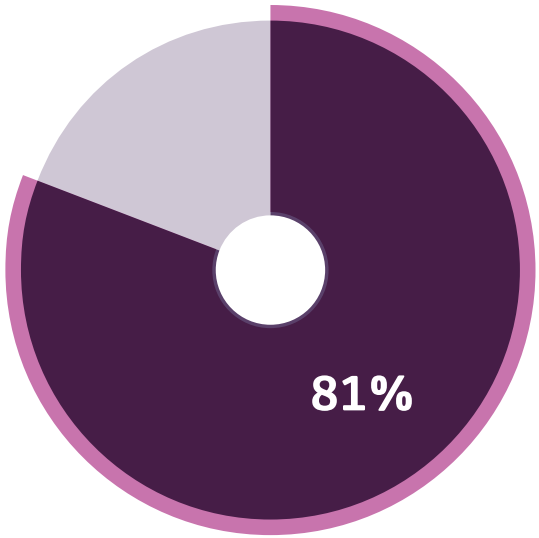
La nostra analisi ha rivelato quanto segue:

- **L'81%** delle imprese concorda sul fatto che la sicurezza deve essere priva di attrito, in modo da non gravare sugli utenti con requisiti di sicurezza eccessivamente onerosi.
- **L'82%** afferma che la sicurezza basata sull'identità è un fattore critico per il proprio business, ma solo **il 25%** può essere classificato come utente avanzato di un approccio alla sicurezza basato sull'identità.
- Il doppio degli utenti avanzati della sicurezza basata sull'identità hanno visto una riduzione delle violazioni dei dati, rispetto agli utenti di base: **41% contro 21%**.
- **Il 91%** degli utenti avanzati della sicurezza basata sull'identità hanno visto un miglioramento della portata digitale; **l'87%** della customer experience; e **l'87%** nella fidelizzazione dei clienti.
- Gli utenti avanzati della sicurezza basata sull'identità stanno anche ottenendo i risultati di business misurabili:
  - **Miglioramento del 47%** della crescita di business
  - **Miglioramento del 50%** della produttività dei dipendenti
  - **Miglioramento del 45%** della soddisfazione della clientela

"La sicurezza è il driver principale del nostro percorso digitale".

Direttore tecnologia, ente pubblico degli Stati Uniti

L'81% delle imprese concorda sul fatto che la sicurezza deve essere priva di attrito, in modo da non gravare sugli utenti con requisiti di sicurezza eccessivamente onerosi.



Introduzione: Una nuova frontiera

La rivoluzione digitale ha spostato, e continua a spostare, i paletti di confine della sicurezza IT. Ha creato un mondo multi-canale, multi-piattaforma e multi-device. Un mondo dove clienti, partner e dipendenti sono costantemente operativi, e si aspettano che lo sia anche tu.

Nell'application economy, i clienti si aspettano download veloci, accesso rapido, esperienze senza soluzione di continuità e protezione robusta. Se le funzioni di sicurezza li rallentano, ti abbandoneranno, e si rivolgeranno altrove se non riuscirai a salvaguardare i loro dati.

Il perimetro di rete tradizionale è un concetto ormai superato. Gli utenti accedono alla rete in qualsiasi momento, ovunque desiderano e su qualsiasi device o piattaforma. L'identità di un utente, non il firewall, rappresenta oggi l'ultima frontiera nella battaglia per proteggere i dati.

Questo impone un rapporto di reciproca fiducia tra l'utente e il business.

In questo scenario diventa imperativa una visione della sicurezza maggiormente orientata all'identità, che mette al centro della scena l'identità dell'utente. La sicurezza basata sull'identità utilizza contesto, analisi comportamentale e approcci più predittivi, per garantire che gli utenti siano chi dicono di essere. Questo consentirà loro di accedere in modo sicuro ai dati aziendali sul device che preferiscono, sempre e ovunque.

"La sicurezza è uno dei principali ostacoli per soddisfare le richieste dei clienti in termini di rapidità".

Direttore IT, associazione dell'amministrazione locale USA

Gli utenti accedono alla rete in qualsiasi momento e ovunque desiderano, e su qualsiasi device o piattaforma.

Tuttavia, la sicurezza basata sull'identità è più di un metodo efficace per proteggere i dati. Se realizzata correttamente, può essere un prezioso enabler di business. Può consentire di fornire nuovi servizi in modo più rapido. Può anche aumentare il coinvolgimento e la fidelizzazione dei clienti, entrambi elementi in cui la fiducia ha un ruolo importante. E, in un mondo digitale, la sicurezza è il driver principale della fiducia.

"La sicurezza basata sull'identità diventerà il principale approccio alla sicurezza tra le società del settore telecomunicazioni".

Direttore marketing, fornitore europeo di servizi di telecomunicazioni

Come parte della nostra ricerca sul modo in cui le imprese stanno evolvendo nell'era digitale, abbiamo esaminato i loro sforzi verso l'adozione di un approccio alla sicurezza maggiormente basato sull'identità. Abbiamo interpellato dirigenti senior di business, IT e della sicurezza di tutto il mondo su argomenti come:

- la loro percezione della sicurezza come enabler di opportunità di business
- i KPI critici utilizzati per valutare l'impatto della sicurezza IT, e i risultati ottenuti
- la loro adozione della sicurezza basata sull'identità necessaria per l'application economy
- in che modo un impiego uso avanzato della sicurezza basata sull'identità ha effetto sulla performance di business

Questo report riassume i nostri risultati. Esso esamina il modo in cui le aziende possono far evolvere la propria sicurezza IT per trainare un aumento della performance, della competitività e della crescita nell'application economy.

La sicurezza basata sull'identità è più di un metodo efficace per proteggere i dati. Se realizzata correttamente, può essere un prezioso enabler di business.

01. Lo stato della sicurezza nell'application economy

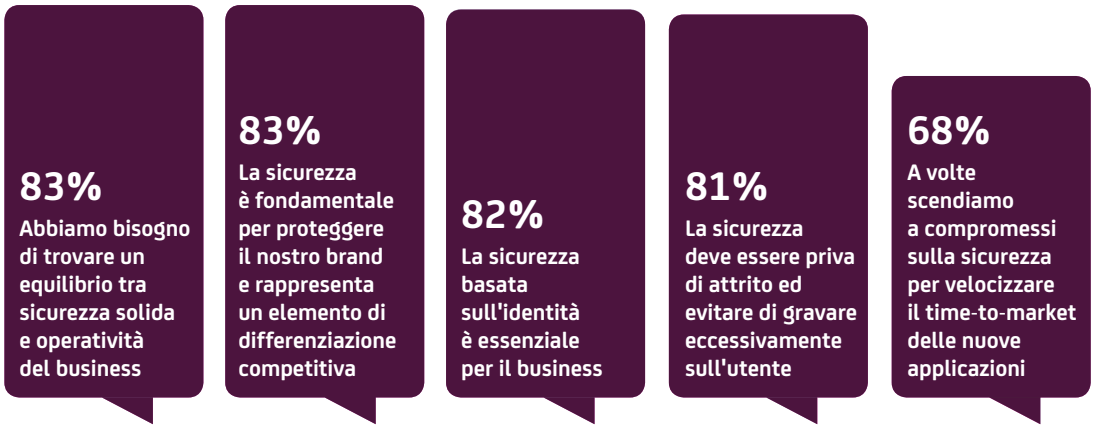
La nostra ricerca suggerisce che le aziende riconoscono il ruolo potenziale della sicurezza nell'ambiente di business di oggi. Esse rimangono focalizzate sugli obiettivi di sicurezza tradizionali, come la protezione dalle violazioni e la garanzia della compliance. Allo stesso tempo, tuttavia, i nostri intervistati vedono la sicurezza come un'opportunità di espandere il proprio business, e di competere in modo più efficace nell'application economy.

Oltre quattro quinti degli intervistati concordano sul fatto che la sicurezza può rendere possibili nuove opportunità di business; fornire un vantaggio competitivo; e offrire a dipendenti e clienti l'accesso rapido, comodo e always-on che ormai si aspettano (consultare la figura 1).

Questo si riflette negli indicatori di performance chiave (KPI) utilizzati per valutare l'impatto della sicurezza IT. Le metriche di performance di business esterne, come portata digitale, customer experience e soddisfazione della clientela saranno utilizzate quanto o più delle misure di sicurezza tradizionali, come violazioni e mancata riuscita dei controlli di compliance (consultare la figura 2).

Oltre quattro quinti degli intervistati concordano sul fatto che la sicurezza può concretizzare nuove opportunità di business; fornire un vantaggio competitivo; e offrire a dipendenti e clienti l'accesso rapido, comodo e always-on che ormai si aspettano.

FIG. 1 L'APPLICATION ECONOMY IMPONE ALLA SICUREZZA DI ASSUMERE IL NUOVO RUOLO DI ENABLER DI BUSINESS



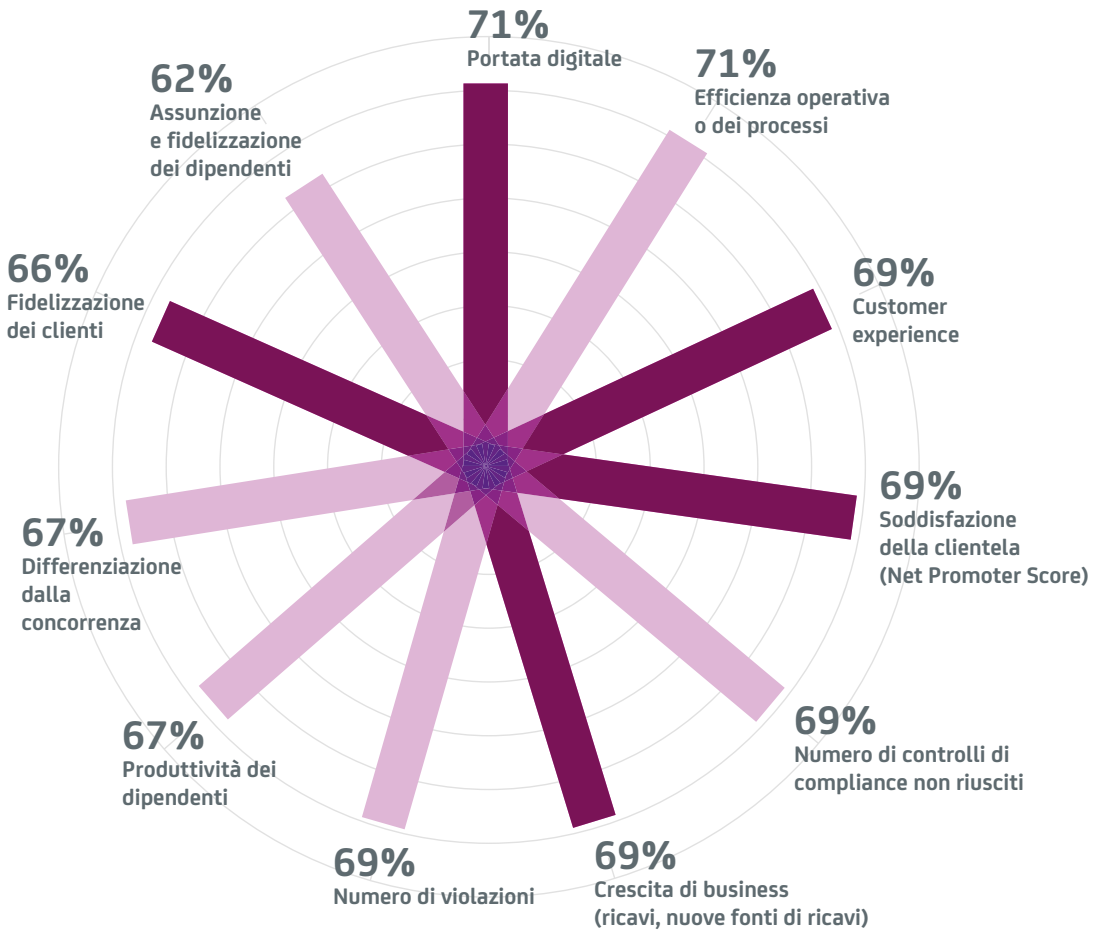
"Esiste un conflitto continuo tra sicurezza robusta, da un lato, e interfacce di clienti e dipendenti, dall'altro".

Direttore IT, associazione dell'amministrazione locale USA

I business vedono chiaramente la sicurezza IT come enabler di business critico, così come un modo per proteggere i dati. Tuttavia, l'application economy porta molti di loro a prendere scorciatoie. Un preoccupante 68% ammette di compromettere la sicurezza per portare le app sul mercato più rapidamente.

Ridurre la priorità della sicurezza nell'application economy è un rischio enorme. La gestione delle identità e degli accessi su migliaia di applicazioni, servizi e device richiede oggi un approccio molto più sofisticato alla protezione delle identità e dei dati, rispetto al passato.

FIG. 2 LE METRICHE DI BUSINESS ESTERNE SONO TRA I PRIMI KPI UTILIZZATI PER MISURARE L'IMPATTO DELLA SICUREZZA IT



02. Un nuovo approccio alla sicurezza

La sfida, nell'application economy, consiste nel verificare identità altamente distribuite da una vasta gamma di fonti, che includono applicazioni, sistemi, il cloud e le piattaforme social media.

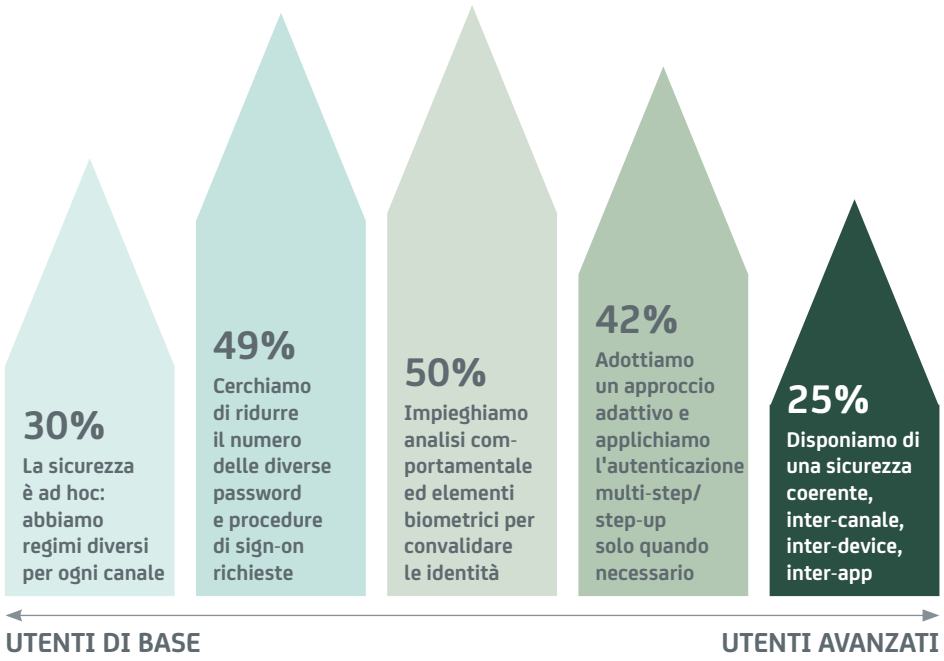
Ma tutto questo deve avvenire in modo totalmente invisibile agli utenti. I clienti vogliono sicurezza totale e un'esperienza senza attrito. Processi di registrazione e autenticazione incoerenti e faticosi raffredderanno il loro entusiasmo, ostacolando gli sforzi verso la creazione di relazioni digitali improntate alla fiducia.

La sicurezza basata sull'identità è un approccio che aiuta a garantire che le pratiche di sicurezza non incidano sulla user experience complessiva. Essa richiede inoltre di adottare controlli IAM (Identity and Access Management) maggiormente adattivi; e di applicare un approccio più proattivo e predittivo alla prevenzione e all'individuazione delle violazioni dei dati.

Abbiamo creato un modello di maturità per valutare l'adozione e l'impiego corrente, da parte delle aziende, di tre elementi chiave della sicurezza basata sull'identità:

1. **Customer experience** (consultare la figura 3). Approcci alla sicurezza coerenti e intercanale, mediante analisi comportamentale e tecniche adattive, si tradurranno in una sicurezza meno invasiva. Solo un quarto delle aziende utilizza una sicurezza coerente, inter-canale, inter-device e inter-app, per mantenere una user experience di qualità elevata. Una minoranza (il 42%) adotta un approccio adattivo, mentre la metà utilizza l'analisi comportamentale.

FIG. 3 APPROCCI COERENTI E INTERCANALE ALLA SICUREZZA TRAINANO LA CUSTOMER EXPERIENCE, MA POCHE AZIENDE LI HANNO ADOTTATI



"La sicurezza deve diventare più user-friendly, senza sacrificare la robustezza. La chiave consiste nel garantire che sia possibile identificare se un utente è un cliente, un dipendente o un hacker; salvaguardare i dati dei clienti e dei dipendenti; e fare in modo che le transazioni non vengano compromesse".

VP tecnologia e compliance, azienda bancaria statunitense

2. **Identity and Access Management** (consultare la figura 4). La sicurezza basata sull'identità richiede anche un approccio maggiormente adattivo ai controlli IAM. Quasi il 70% ha centralizzato e automatizzato i controlli IAM; ma solo un'azienda su dieci è in grado di adattarli in risposta ai rischi.

"La gestione dell'identità e degli accessi sarà le problematica di sicurezza principale nel futuro".

Direttore marketing, fornitore europeo di servizi di telecomunicazioni

3. **Rilevazione delle violazioni** (consultare la figura 5): I processi proattivi e predittivi possono migliorare notevolmente la capacità di un'azienda di individuare e prevenire le violazioni dei dati. Eppure, solo il 37% delle aziende impiega l'analisi per rilevare proattivamente e prevenire le violazioni dei dati; e meno della metà di queste ultime (16%) è in grado di predire il rischio di violazioni prima che si verifichino.

Dopo aver posto ai partecipanti domande su questi tre elementi della sicurezza basata sull'identità, abbiamo attribuito un punteggio alle loro risposte. Sulla base dei risultati, abbiamo classificato le rispettive aziende come utenti avanzati, di base o limitati della sicurezza basata sull'identità.

Ne è emerso che solo il 25% delle imprese è definibile come utente avanzato. La categoria di gran lunga più popolosa (64%) è quella degli utenti di base, mentre in poco più di un'azienda su dieci (11%) le funzionalità basate sulla sicurezza sono limitate o addirittura nulle.

FIG. 4 CONTROLLI DI IDENTITY AND ACCESS MANAGEMENT ADATTIVI MIGLIORANO LA SICUREZZA BASATA SULL'IDENTITÀ, MA POCHI LI HANNO ADOTTATI

20%
I controlli sono prevalentemente manuali

69%
I controlli sono prevalentemente centralizzati e automatizzati

11%
I controlli sono adattivi in base al rischio

UTENTI DI BASE — **UTENTI AVANZATI**

FIG. 5 L'ANALISI PREDITTIVA E PROATTIVA PUÒ MIGLIORARE NOTEVOLMENTE LA CAPACITÀ DI INDIVIDUARE E PREVENIRE LE VIOLAZIONI DEI DATI, MA POCHE AZIENDE LA UTILIZZANO

13%
Solo revisione occasionale dell'attività di reporting

34%
Alcune attività di analisi con reporting intelligente e avvisi

37%
Proattività: analisi approfondita con risposta in tempo reale eventi e incidenti

16%
Predittività: capacità di anticipare il rischio prima che si verifichi una violazione

UTENTI DI BASE — **UTENTI AVANZATI**

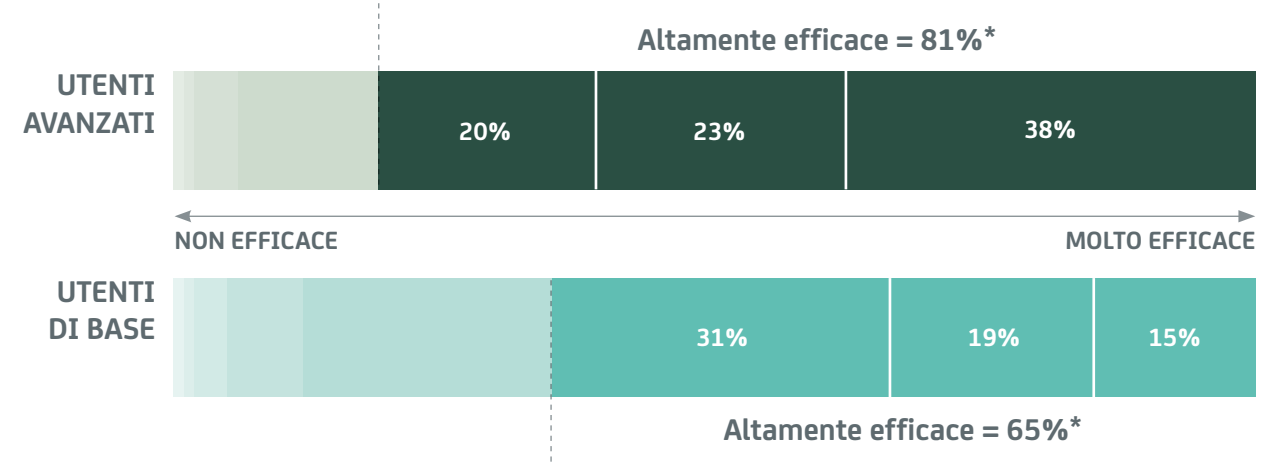
03. Il significativo impatto di business della sicurezza basata sull'identità

Nella fase successiva della nostra analisi abbiamo verificato l'eventuale correlazione tra impiego maturo della sicurezza basata sull'identità e risultati di business. A questo scopo, abbiamo confrontato la performance di business degli utenti avanzati e di base.

La nostra analisi ha rilevato che gli utenti avanzati della sicurezza basata sull'identità sono molto più propensi a credere che le proprie funzioni di sicurezza li differenzino dalla concorrenza. Circa l'81% lo dichiara in relazione alla propria strategia di sicurezza, rispetto al 65% degli utenti di base (consultare la figura 6).

Gli utenti avanzati attribuiscono anche una priorità molto più elevata a tutti gli obiettivi di sicurezza oggetto del sondaggio (disponibile a pagina 8). Ancora più significativo, è molto più probabile che questi utenti, rispetto agli utenti di base, utilizzino la sicurezza per rendere possibili nuove iniziative e relazioni di business (55% contro 34%).

FIG. 6 LA SICUREZZA BASATA SULL'IDENTITÀ AVANZATA MIGLIORA LA DIFFERENZIAZIONE COMPETITIVA

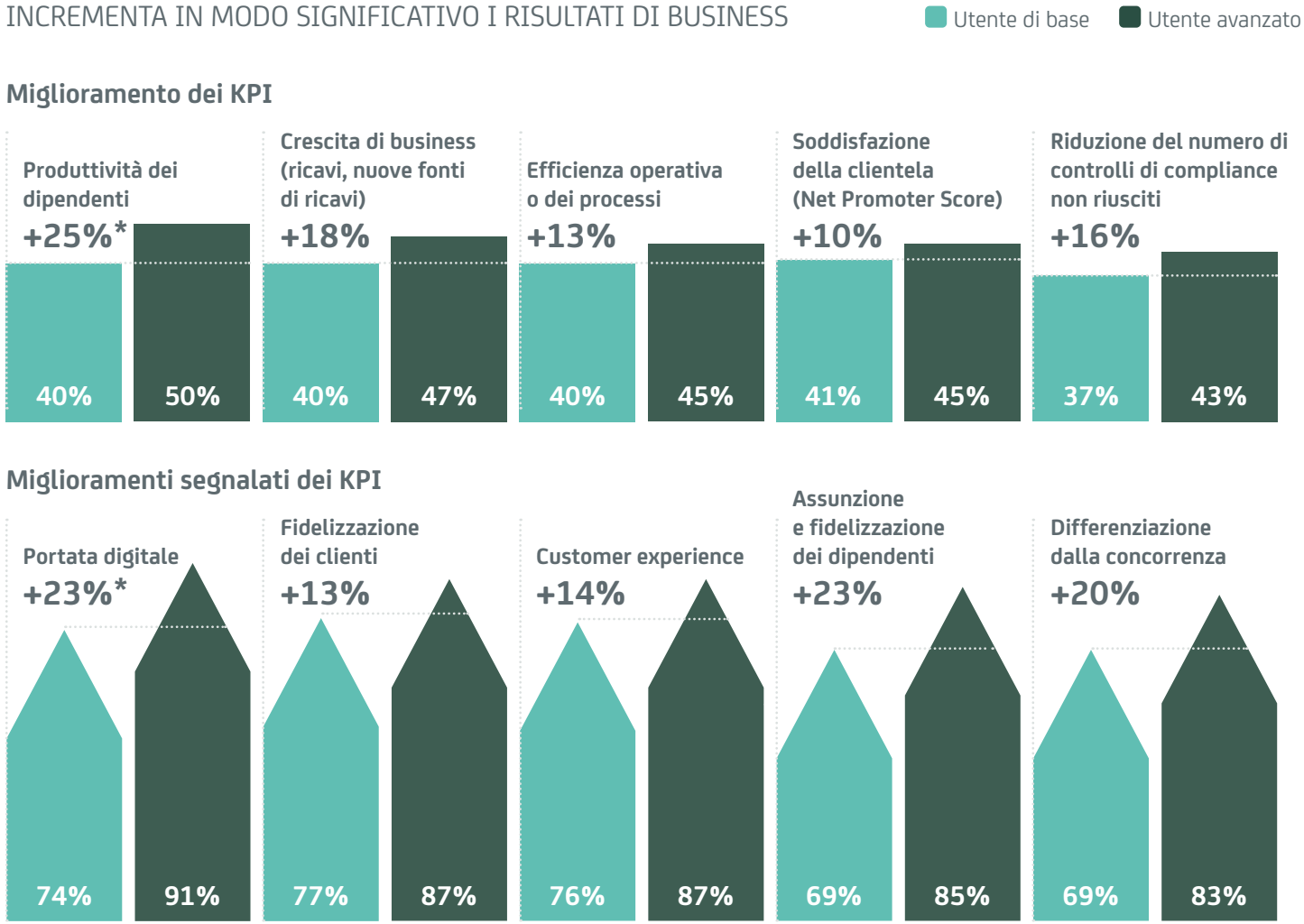


*% primi tre punteggi su 10, dove 10 equivale a "molto efficace" e 1 a "non efficace"

Un quadro analogo è emerso quando abbiamo esaminato l'impatto della sicurezza IT sui KPI utilizzati per valutarla. Gli utenti avanzati della sicurezza basata sull'identità dichiarano miglioramenti più significativi di tutti parametri di sicurezza e di business oggetto del sondaggio.

I differenziali tra utenti di base e avanzati variano tra il 10 e il 25% (consultare la figura 7). Ad esempio, l'87% degli utenti avanzati segnala un significativo miglioramento della customer experience, contro il 76% degli utenti di base. Un impatto ancora maggiore viene rilevato sulla capacità di acquisizione e fidelizzazione dei dipendenti: l'85% degli utenti avanzati segnala un miglioramento, contro il 69% degli utenti di base.

FIG. 7 LO SPOSTAMENTO DALLA SICUREZZA DI BASE ALLA SICUREZZA AVANZATA BASATA SULL'IDENTITÀ INCREMENTA IN MODO SIGNIFICATIVO I RISULTATI DI BUSINESS



* Miglioramento in % dei KPI passando dall'utente di base all'utente avanzato

In termini di protezione dei dati, mentre circa un terzo di tutti gli utenti continua a vedere un aumento delle violazioni della sicurezza, è significativo che per gli utenti avanzati esista quasi il doppio delle probabilità, rispetto agli utenti di base, di ottenere una riduzione del numero di violazioni dei dati riscontrate. Due quinti (41%) degli utenti avanzati sono riusciti a ottenere questo risultato l'anno scorso, nonostante un clima di sicurezza sempre più impegnativo. Questa cifra scende a meno di un quarto (21%) per gli utenti di base (consultare la figura 8).

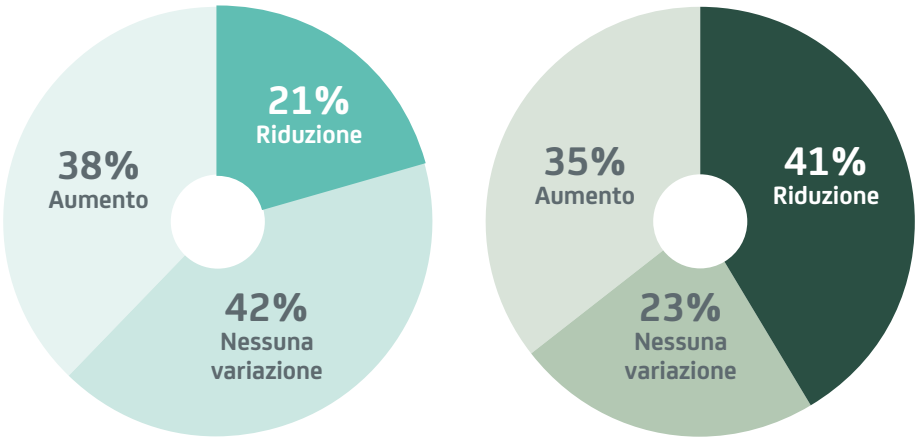
Digital Transformation Business Impact Scorecard

Abbiamo inoltre valutato l'impatto della sicurezza basata sull'identità sugli sforzi di digital transformation degli intervistati.

A questo scopo, abbiamo utilizzato la Digital Transformation Business Impact Scorecard, da noi creata come parte della nostra ricerca sugli sforzi di digital transformation delle imprese. La scorecard valuta l'effetto complessivo delle iniziative digitali delle aziende, sulla base di 14 KPI di business essenziali per il successo della trasformazione.

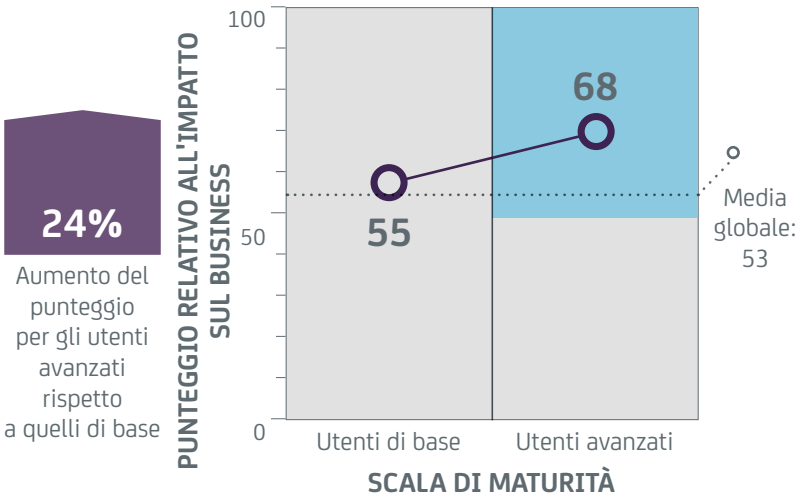
Abbiamo confrontato i risultati della scorecard per gli utenti avanzati e di base della sicurezza basata sull'identità. Il punteggio medio per gli utenti avanzati è stato di 68 su 100, rispetto al 55 per gli utenti di base: un miglioramento del 24% (consultare la figura 9).

FIG. 8 LA TRANSIZIONE DALLA SICUREZZA DI BASE ALLA SICUREZZA AVANZATA BASATA SULL'IDENTITÀ RIDUCE LE VIOLAZIONI DEI DATI



La percentuale delle imprese che riportano violazioni dei dati è aumentata, è rimasta invariato o è diminuita
(La somma delle percentuali non è pari a 100 a causa degli arrotondamenti)

FIG. 9 L'UTILIZZO AVANZATO DELLA SICUREZZA BASATA SULL'IDENTITÀ INCREMENTA I RISULTATI DI BUSINESS DELLA DIGITAL TRANSFORMATION



04. La lezione degli utenti avanzati della sicurezza basata sull'identità

Il messaggio è chiaro: gli utilizzatori maturi della sicurezza basata sull'identità stanno ottenendo maggiori benefici di business in ogni ambito. Cosa caratterizza l'operato di questi utenti e rende la loro sicurezza tanto più efficace?

In primo luogo, attribuiscono maggiore importanza alla sicurezza IT: L'81% investe di più nella prevenzione delle violazioni, contro il 55% degli utenti di base. E sono meno propensi a prendere scorciatoie: Il 58% degli utenti avanzati scende a compromessi sulla sicurezza per velocizzare il time-to-market delle proprie app, rispetto al 70% degli utenti di base.

Sono anche più propensi a fare uso delle cosiddette "DevSecOps". La maggioranza degli utenti avanzati della sicurezza basata sull'identità (54%) adotta questa pratica, contro il 33% degli utenti di base.

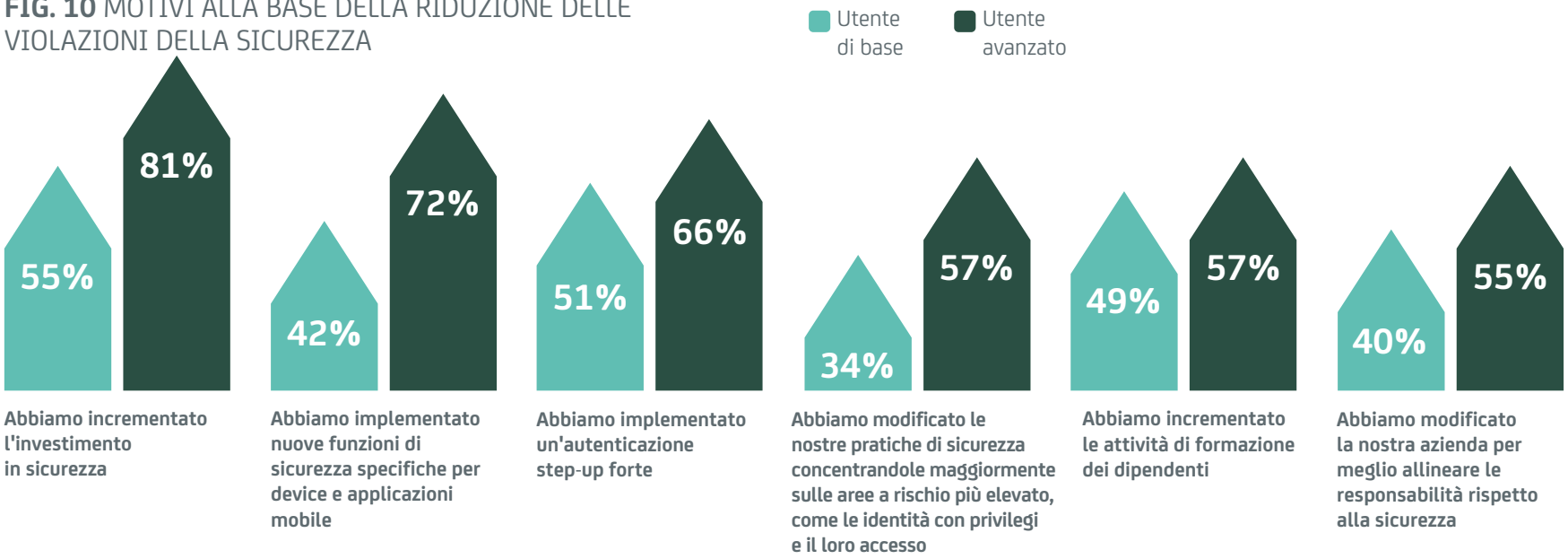
DevSecOps è essenziale nell'application economy. Quando il business dipende dalla tecnologia digitale, la sicurezza delle applicazioni non può essere un elemento secondario. Simile a DevOps, che inserisce le Operations IT in una fase anticipata del ciclo di sviluppo del software, DevSecOps anticipa l'integrazione della sicurezza nel processo di sviluppo. Questo assicura che la sicurezza sia integrata nelle applicazioni digitali fin dall'inizio.

Infine, gli utenti avanzati si attivano maggiormente per allineare il proprio approccio alla prevenzione delle violazioni rispetto agli aspetti pratici dell'application economy (consultare le figura 10).

È molto più probabile che implementino sicurezza dedicata per i device mobile e le applicazioni (72% contro 42%); che riconfigurino le pratiche di sicurezza per proteggere le aree ad alto rischio, come le identità con privilegi (57% contro 34%); che distribuiscano autenticazione step-up forte (66% contro 51%); e che riorganizzino il business per rafforzarne la responsabilità rispetto alla sicurezza (55% contro 40%).

> **"La nostra più grande preoccupazione di sicurezza è l'accesso remoto oggi praticamente onnipresente. L'autenticazione è stata al centro della sicurezza IT della nostra azienda negli ultimi due anni".**
>
> **Direttore R&S,** produttore farmaceutico statunitense

FIG. 10 MOTIVI ALLA BASE DELLA RIDUZIONE DELLE VIOLAZIONI DELLA SICUREZZA



05. Sicurezza efficace basata sull'identità: una tabella di marcia

Il nostro studio supporta fortemente il valore per il business dell'adozione di approcci alla sicurezza basati sull'identità. Ma da dove cominciare? Come fare in modo che funzioni per il tuo business? E come fare per garantire che migliori la performance e alimenti la crescita?

Nella nostra esperienza, le azioni che seguono sono cruciali per il successo della sicurezza basata sull'identità:

1. **Far coincidere identità e perimetro.** Oggi sono gli utenti il tuo confine di sicurezza e accedono alla rete ovunque e in ogni momento. È necessario poter verificare con certezza la loro identità e che possano accedere solo alle informazioni e ai servizi necessari. Questo significa considerare l'autenticazione basata sul rischio in combinazione con approcci analitici alla valutazione delle identità.
2. **Considerare la sicurezza come un enabler di business.** Nell'application economy, la sicurezza non si limita a ridurre il rischio, ma rende anche possibile una nuova crescita del business. La nostra ricerca mostra che un approccio basato sull'identità può apportare una serie di benefici in grado di migliorare la redditività. Lo stesso effetto ha l'integrazione degli indicatori della performance di business nel framework di valutazione della sicurezza.
3. **Attenzione prioritaria alla creazione di relazioni digitali affidabili**. Le risorse principali a tua disposizione sono le relazioni digitali con i singoli clienti. Hanno bisogno di essere certi che capisci le loro esigenze quando interagiscono con l'azienda, e che la loro identità e i loro dati rimangono protetti nel modo più lineare possibile.
4. **Proteggere le esperienze, non solo i dati**. La sicurezza deve essere solida, ma non deve creare ostacoli o rallentamenti. I clienti vogliono interazioni lineari ed esperienze di qualità: qualsiasi interruzione avrà come unico effetto quello di allontanarli. Questo significa offrire accesso Single Sign-On, funzionalità self-service e meccanismi di autenticazione coerenti ma flessibili, che seguono gli utenti tra le diverse applicazioni e device.
5. **Adottare un approccio adattivo allo IAM**. La nostra ricerca mostra che gli utenti maturi della sicurezza basata sull'identità dispongono di controlli IAM facilmente adattabili in risposta ai rischi, e offrono così una user experience notevolmente migliorata.
6. **Essere proattivi e predittivi**. Le analisi avanzate possono aiutare a respingere in modo proattivo i rischi per la sicurezza, anziché essere costretti a rimanere costantemente in modalità di emergenza. E possono anche far compiere alla sicurezza un ulteriore passo avanti, aiutando a rilevare, reagire e adattare i processi di sicurezza per gestire il rischio di violazioni prima che si verifichino.
7. **Non compromettere la sicurezza per ottenere velocità**. L'application economy ha aumentato la pressione alla release sempre più rapida di nuove applicazioni. Ma è più importante che mai garantire che la sicurezza sia integrata fin dall'inizio del processo, e non compromessa nella sue fasi finali. Un approccio DevSecOps può essere una valida opzione per assicurare che tutte le considerazioni di sicurezza siano valutate nelle prime fasi del processo di sviluppo.

Ulteriori informazioni

Metodologia di indagine

CA Technologies ha commissionato a Coleman Parkes Research un sondaggio, rivolto a dirigenti, sulla portata e sull'impatto delle attività di digital transformation delle rispettive aziende.

Coleman Parkes Research ha intervistato 1.770 decision-maker di business e IT senior (inclusi 106 CSO/CISO) di grandi aziende con sede in 21 paesi nelle Americhe, nell'area EMEA e nell'area APJ (Asia-Pacifico e Giappone). Il fatturato annuo delle aziende interpellate è superiore a 1 miliardo di dollari (o 0,5 miliardi di dollari in alcune economie meno sviluppate).

I paesi inclusi nel sondaggio sono:

America	**EMEA**	**APJ**
Brasile	Francia	Australia
Stati Uniti	Germania	Cina
	Italia	Hong Kong
	Paesi Bassi	India
	Sud Africa	Indonesia
	Spagna	Giappone
	Svezia	Corea
	Svizzera	Malesia
	Regno Unito	Singapore
		Tailandia

I settori inclusi nel sondaggio sono:

- Automotive
- Energia e utenze
- Mezzi di comunicazione e intrattenimento
- Produzione industriale
- Sanità
- Servizi bancari e finanziari
- Settore pubblico
- Telecomunicazioni
- Trasporti e logistica
- Vendita retail

La ricerca e l'analisi sono state condotte nei mesi di maggio e giugno 2016.

Informazioni su CA Technologies

CA Technologies (NASDAQ: CA) crea software che promuove l'innovazione all'interno delle aziende, consentendo loro di cogliere le opportunità offerte dall'application economy. Il software rappresenta il cuore di qualsiasi business, in ogni settore. Dalla pianificazione allo sviluppo, dalla gestione alla sicurezza, CA Technologies lavora con le aziende di tutto il mondo per cambiare il nostro modo di vivere, interagire e comunicare, in ambienti mobile, cloud pubblici e privati, distribuiti e mainframe. www.ca.com/it

Informazioni su Coleman Parkes Research

Coleman Parkes Research è specializzata nella selezione e nell'inclusione di operatori di livello senior in ricerche all'interno di diversi mercati globali, settori verticali e aree funzionali, per una vasta gamma di clienti. Opera con un approccio a 360° che include, tra l'altro, ricerche su leader di pensiero per PR e campagne di marketing, analisi di opportunità win/loss, test di messaggi di prodotto e colloqui approfonditi con dirigenti senior. Coleman Parkes Research collabora con i clienti alla definizione di strategie comprovate in grado di far emergere informazioni preziose sul mercato sulla base di singoli requisiti e ipotesi chiave. colemanparkes.com/

Informazioni su Grist

Servizi editoriali e creativi. Grist è una pluripremiata agenzia di content marketing e leadership di pensiero B2B, del cui DNA fa parte il patrimonio editoriale di The Economist e Financial Times, insieme a una chiara visione del futuro digitale. www.gristonline.com