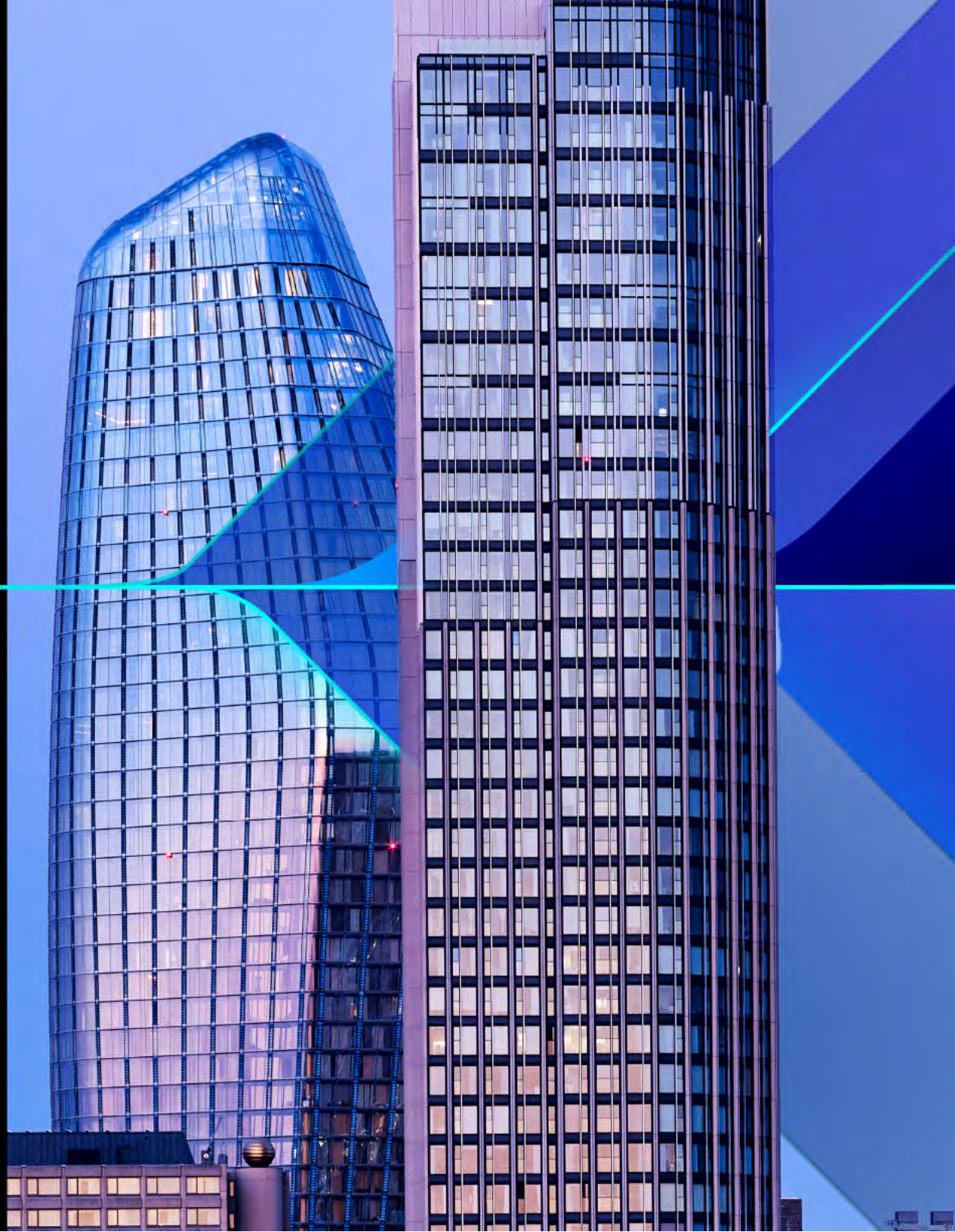
zscaler™

# ZSCALER

## PER IL SETTORE DEI SERVIZI BANCARI E FINANZIARI



# CONTENUTI


01 Uno scenario di tecnologia e business in rapida evoluzione.

02 Lo stato della trasformazione digitale.

03 Configurazione corretta o sbagliata del digitale.

04 Infrastruttura legacy: un fattore abilitante o un inibitore?

05 L'arte di bilanciare la sicurezza con l'esperienza utente.

06 Creare un equilibrio tra sicurezza ed esperienza utente con SASE e Zero Trust.

07 Zscaler: un'introduzione.

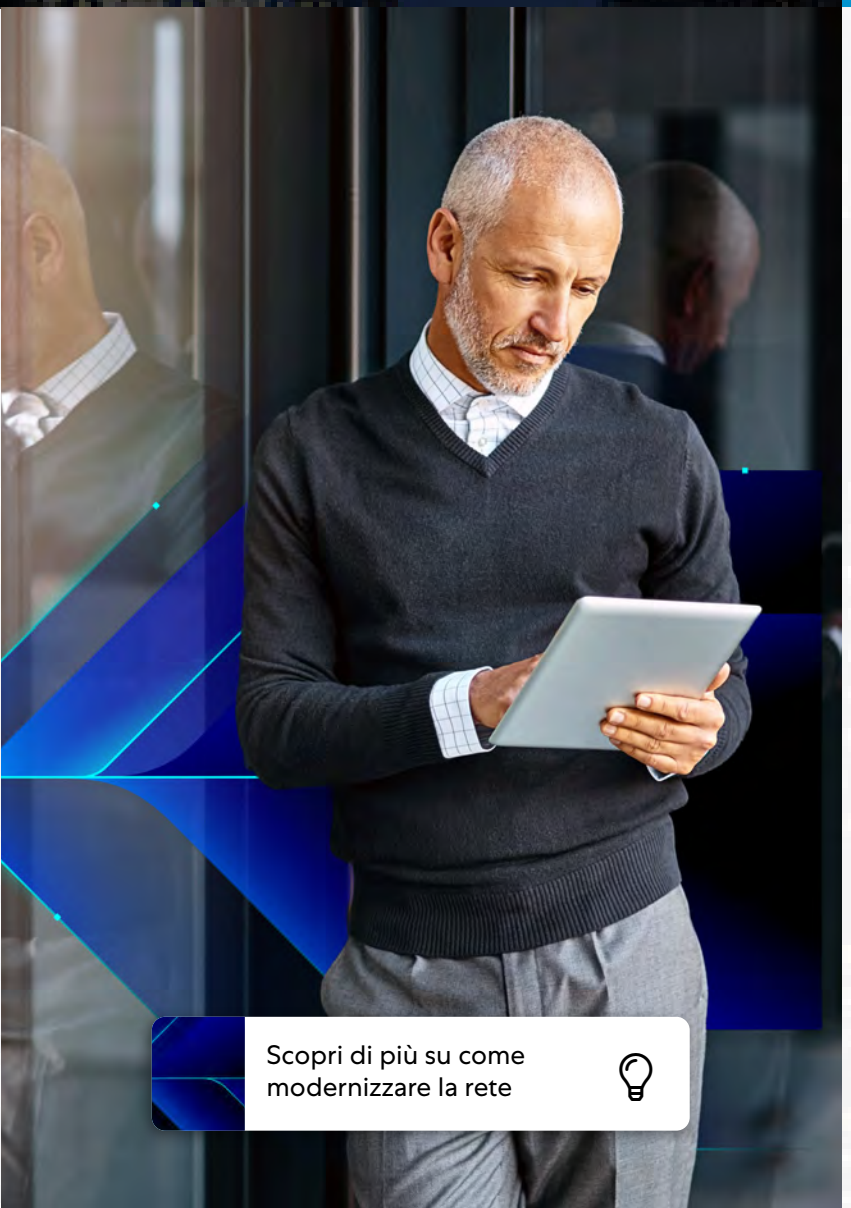
08 Fusioni e acquisizioni.

09 Quali sono le prospettive della trasformazione digitale?

10 Perché agire subito?


# 1 UNO SCENARIO TECNOLOGICO IN **RAPIDA EVOLUZIONE**

Quando si verifica un qualunque tipo di evento con effetti dirompenti in tutto il mondo, il misuratore più pertinente, quantitativo e sensibile della situazione globale è la salute del settore dei servizi finanziari.



Scopri di più su come modernizzare la rete

**Per sopravvivere e prosperare in uno scenario economico internazionale in rapida evoluzione, questo settore ha impiegato un approccio olistico e strategico, reinventandosi e adottando nuove piattaforme FinTech basate sul cloud computing, l'ubiquità mobile e gli ultimi progressi nell'automazione dell'Intelligenza Artificiale (IA).**

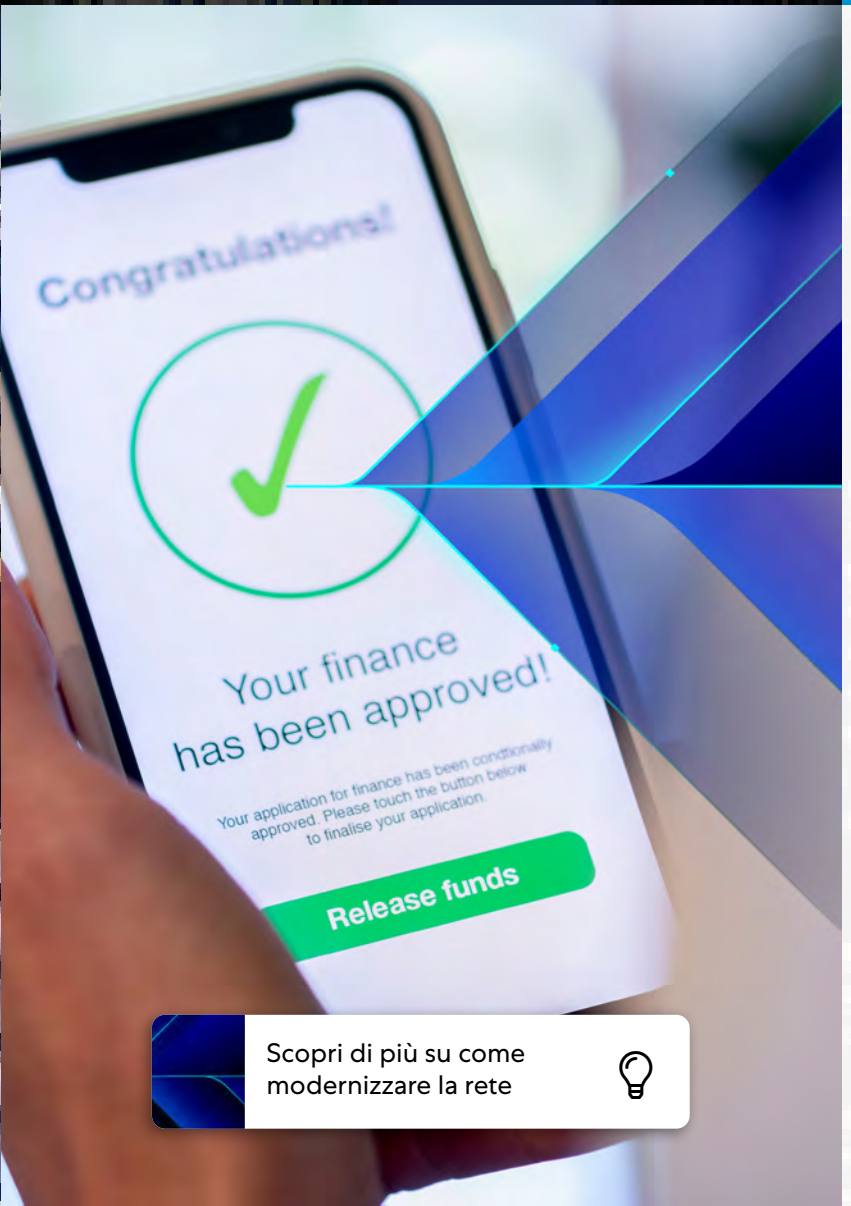
Fino al 2020, i giovani millennial erano i principali utenti delle nuove tecnologie bancarie, come i sistemi contactless "tap & pay", ma la curva di apprendimento si è appiattita e ampliata considerevolmente andando a includere tutti i gruppi di età, che ora si trovano a sperimentare la comodità del contactless. L'era del Covid-19 (Coronavirus) ha ovviamente accelerato ulteriormente il passaggio all'online banking e verso una società senza contanti.

Allo stesso tempo, i progressi tecnologici hanno aperto il mercato a una concorrenza digitale senza precedenti. L'ascesa delle cosiddette "challenger bank" si è sviluppata in linea con l'inclinazione dei consumatori ad abbracciare l'e-commerce attraverso l'uso di uno smartphone e l'utilizzo più ampio dei pagamenti elettronici.

Che qualcuno stia cercando un mutuo, una polizza assicurativa, un piano d'investimento o semplicemente trasferendo denaro e svolgendo le normali attività legate al conto corrente o di verifica, poterle svolgere in modo digitale sta diventando rapidamente una consuetudine. Il dinamismo del mercato e la possibilità di scelta senza precedenti hanno reso i clienti estremamente esigenti, che si aspettano esperienze in tempo reale e personalizzate senza soluzione di continuità.

# 2 LO STATO DELLA TRASFORMAZIONE DIGITALE

L'innovazione digitale e l'agilità aziendale sono fondamentali per attrarre nuovi clienti, aumentare la quota di mercato nei territori nazionali e affrontare le opportunità di crescita in nuovi segmenti commerciali.




Scopri di più su come modernizzare la rete

**Tuttavia, il cuore della maggior parte delle organizzazioni finanziarie mature sono i sistemi core, spesso basati su tecnologie on-premise proprietarie che sono state ampiamente personalizzate nel corso degli anni, creando più dipendenze e molti livelli di funzioni IT interconnesse. Facendo riferimento alle normative finanziarie, ai controlli di governance e alle leggi sulla privacy dei dati come altro inibitore chiave dell'adesione al cloud, è comprensibile il motivo per cui la maggior parte delle organizzazioni di servizi finanziari sia stata lenta o in ritardo nel riuscire a sfruttare l'efficienza e l'agilità fornite dal cloud pubblico.**

Fin dall'inizio, le autorità di regolamentazione finanziaria hanno stabilito standard e linee guida per l'uso del cloud computing per la sicurezza e la privacy. Ciò ha permesso al cloud di diventare un fattore che favorisse l'ottemperanza alle normative, consentendo agli istituti finanziari di sviluppare approcci efficaci alla gestione del rischio, all'integrità dei dati e alla riservatezza, senza soffocare l'innovazione.

Anche se la maggior parte delle istituzioni finanziarie ora adotta un ambiente ibrido con alcune infrastrutture legacy, il cloud sta pervadendo stabilmente nel panorama IT, attraverso piattaforme e applicazioni per qualsiasi cosa come ERP, dati di mercato, ricerca CRM, servizi ausiliari di marketing e rivendita e molto altro ancora. Persino la semplice formazione per le qualifiche FINRA è passata sul Web e **FINRA stessa ha trasferito il 100% delle proprie applicazioni sul cloud.**

Secondo un sondaggio condotto da Zscaler su 600 CIO EMEA nel 2020, la trasformazione digitale è in corso nel settore dei servizi finanziari. Molte organizzazioni hanno adottato una strategia cloud-first, sfruttando più cloud pubblici e applicazioni Software-as-a-Service (SaaS) per soluzioni rivolte ai clienti, operazioni di back-office e integrazione con i partner nell'ecosistema finanziario, quali shadow bank, provider di FinTech e così via.

**Il sondaggio riferisce che due terzi delle aziende ha spostato il 50% delle proprie applicazioni sul cloud, mentre un quarto ha raggiunto il 75%.**

# 3 CONFIGURAZIONE CORRETTA O SBAGLIATA DEL DIGITALE

Man mano che i servizi finanziari si evolvono, passando dalle sedi fisiche al Web, i fornitori si trovano ad affrontare la sfida di tentare di replicare, in un formato online, lo stesso livello di servizio per i clienti fornito di persona, offerto in precedenza nelle loro filiali.

**Per ridurre il rischio di perdita dei clienti, l'esperienza-utente è stata posizionata in cima alla lista delle priorità aziendali per la maggior parte delle organizzazioni finanziarie. Quando i servizi vengono erogati nel modo corretto e senza soluzione di continuità, il cliente chiede di più, interagisce sempre di più e potenzialmente acquista nuovi servizi. Se invece il servizio viene erogato male, è lento o manca la fiducia, il cliente se ne va rapidamente.**

Con un attento sguardo al futuro e alla concorrenza emergente, le organizzazioni progressive di servizi finanziari stanno guardando avanti verso le tecnologie basate su 5G, IA, blockchain, Robotic Process Automation (RPA) e l'uso più ampio di Internet delle cose (IoT).

I progressi compiuti nell'adozione, nell'implementazione e nella diffusione di queste tecnologie sono stati bruscamente interrotti a causa degli effetti della pandemia di Covid-19, che ha avuto un impatto dirompente sulle strategie di sviluppo commerciale e organizzativo a tutti i livelli. Le organizzazioni di tutto il mondo sono state rapidamente costrette a cambiare marcia e concentrarsi sulla continuità del business. Nel giro di pochi giorni, la maggior parte dei reparti IT ha risposto alla sfida, mostrando la capacità di gestione dei progetti, ridefinendo le priorità e accelerando quei progetti che permettevano alle economie locali e internazionali di continuare a muoversi. Migliaia di dipendenti, che operavano in uffici o filiali, sono stati messi in condizione di poter lavorare da remoto, mentre i pagamenti senza contanti e altre forme di **processi senza ostacoli e a distanza** sono stati implementati in anticipo, alcuni persino prima rispetto alle tempistiche di rilascio previste.

Scopri di più su come modernizzare la rete

# 4 INFRASTRUTTURA LEGACY: UN FATTORE ABILITANTE O UN INIBITORE?

Mentre da un lato le organizzazioni di servizi finanziari hanno compiuto progressi significativi, abbracciando il cloud e il mobile come parte del loro percorso di trasformazione digitale, l'evoluzione ha portato con sé diverse nuove sfide.

**Gli investimenti esistenti che continuano a servire quotidianamente le operazioni aziendali vengono spesso estesi alla loro durata massima, per ottenere il massimo ritorno sull'investimento. Il problema è che l'infrastruttura legacy non è mai stata progettata per le esigenze transazionali, analitiche e procedurali del mondo cloud e mobile di oggi. Queste inadeguatezze si sono mostrate in modo ancora più evidente durante la pandemia.**

Prima della crisi, la maggior parte del personale del settore dei servizi finanziari operava da una filiale o in ufficio. Una piccola percentuale viaggiava per affari, per riunioni sul campo o lavorava da casa, collegandosi ai principali sistemi bancari e assicurativi dell'organizzazione tramite reti private virtuali (VPN) o Virtualized Desktop Interfaces (VDI). Sulla scia della crisi, tuttavia, l'IT ha dovuto affrontare la sfida di consentire un accesso remoto sicuro per un numero record di lavoratori da remoto che dovevano rimanere chiusi in casa.

Anche se il personale mobile poteva comunque accedere ai sistemi aziendali e alle applicazioni cloud, le VPN non erano progettate per l'uso da parte di quasi la totalità del personale, richiedendo che il traffico attraversasse uno stack di apparecchi di applicazione, quali bilanciatori del carico, DDoS, firewall e concentratori VPN. Il backhauling del traffico attraverso l'infrastruttura esistente di rete e legacy e attraverso più apparecchi di applicazione ha causato latenza, frustrazione degli utenti e una minore produttività. Negli scenari peggiori, i dipendenti hanno ignorato le politiche di sicurezza e i controlli VPN, creando lacune e vulnerabilità all'interno della sicurezza stessa.

La tecnologia VDI ha consentito agli utenti da remoto di connettersi a sistemi di base, e-mail e altre applicazioni nell'utilizzo di dispositivi BYOD, riducendo i problemi classici, quali la visibilità dei dati e il furto. Queste soluzioni non sono solo notoriamente difficili da installare e costose da mantenere, ma sono anche diventate troppo utilizzate, e un ulteriore rischio per la sicurezza durante la pandemia.

Scopri di più su come modernizzare la rete

**In genere, le organizzazioni IT risolvono il problema di una rete poco performante con un'infrastruttura aggiuntiva. Questo non solo aggiunge ulteriore complessità e costi, ma aumenta anche i rischi per la sicurezza. Man mano che le organizzazioni percorrono questa strada verso un'infrastruttura sempre più ingombrante, diventano meno agili, meno innovative e meno competitive.**

**Negli ultimi mesi, questa tendenza è stata accelerata per via del Covid-19, che ha portato la maggior parte del personale a lavorare da remoto e il settore dei servizi finanziari ad accelerare la distribuzione di Microsoft 365.**

## COME CONSEGUENZA, SONO SCATURITE DELLE PROBLEMATICHE:

- Le soluzioni di accesso remoto basate su VPN non sono state in grado di fornire i livelli di servizio richiesti dall'azienda, con conseguente latenza ed esperienza utente di scarsa qualità
- L'accesso remoto basato su VPN, che mette i computer da remoto sulla rete aziendale, è da tempo noto come il vettore principale per l'infezione degli endpoint. Questo è stato esacerbato con l'aumento del lavoro da casa.
- Microsoft 365 è un protocollo che richiede maggiore larghezza di banda e latenza inferiore per offrire livelli di servizio accettabili.
- L'espansione dell'architettura "Hub and Spoke" è molto costosa e in definitiva non fornisce l'SLA necessario.
- L'espansione della superficie delle architetture di sicurezza esistenti rende le aziende più vulnerabili in particolare agli attacchi dei cosiddetti cavalli di Troia, inoltre questa strategia non protegge completamente dalle minacce interne.

Molti responsabili IT riconoscono che l'architettura hub and spoke non è più mappata sull'attuale ambiente cloud e mobile distribuito e fatica a supportare gli utenti da remoto o a mostrare una capacità di scalabilità per soddisfare la crescita del traffico di rete. Ma non si tratta solo delle problematiche e dei costi connessi alla protezione dell'infrastruttura legacy che sono determinanti nella necessità di trasformazione dell'architettura; in realta' l'IT si trova anche a dover progettare e implementare un'architettura che supporti una vasta gamma di innovazioni in ambienti diversi, dinamici e complessi. L'obiettivo è quello di creare un mondo digitale in grado di comprendere ed elaborare il linguaggio naturale, raccogliere grandi dati, identificare modelli, interpretare, percepire, ragionare e offrire consulenza in tempo reale per supportare l'apprendimento guidato di nuova generazione, la tecnologia operativa, la robotica, i dispositivi indossabili e altro ancora.

# 5 L'ARTE DI BILANCIARE LA SICUREZZA CON L'ESPERIENZA UTENTE

Banche, compagnie di assicurazione e altre organizzazioni di servizi finanziari sono ovviamente responsabili della detenzione e della gestione di grandi quantità di denaro dei clienti, nonché di informazioni finanziarie.

**Con una sfida in continua evoluzione per stare al passo con i criminali e le minacce informatiche e le rigorose normative finanziarie, non sorprende che le organizzazioni finanziarie siano tra i soggetti che investono di più nella sicurezza informatica.**

Gli sviluppi digitali generano delle opportunità per i criminali, che cercano di sfruttarne le vulnerabilità. In pochi secondi, il personale che risponde a un'e-mail di phishing può compromettere le proprie credenziali ed essere oggetto di una violazione dei dati, di un attacco ransomware o di entrambi. Tuttavia, vi è un equilibrio da raggiungere. Come si fa a spingere in modo economico e sicuro i processi e le applicazioni aziendali core verso una forza lavoro mobile e da remoto, senza compromettere l'esperienza utente?

Quando ci sono diversi passaggi di sicurezza si può andare a ledere l'esperienza utente, i clienti e i dipendenti possono sentirsi frustrati e – di conseguenza - la produttività può venirne colpita. I responsabili IT riconoscono di essere competenti nel fornire sia la sicurezza che l'esperienza utente, ma sanno anche quanto sia complesso offrire entrambi questi elementi contemporaneamente.

Scopri di più su Zscaler Zero Trust Exchange

# 6 CREARE UN EQUILIBRIO TRA SICUREZZA ED ESPERIENZA UTENTE CON **SASE E ZERO TRUST**

Secure Access Service Edge (SASE) è un modello di sicurezza definito da Gartner, specificamente per affrontare le sfide di sicurezza poste da app, dispositivi e utenti che si muovono al di fuori del perimetro di rete tradizionale.

Scopri di più su Zscaler Zero Trust Exchange

**L'architettura SASE combina funzionalità WAN complete e funzioni di sicurezza di rete, come Secure Web Gateway, CASB, firewall as a service e ZTNA (Zero Trust Network Architecture) per supportare le esigenze dinamiche di accesso sicuro delle imprese digitali.**

A differenza dell'accesso tradizionale alla rete, l'approccio Zero Trust si adatta al business, elabora le connessioni tramite broker e concede l'accesso in base all'utente, al dispositivo, alla posizione e all'app, fornendo un accesso veloce e sicuro agli utenti autorizzati, indipendentemente da dove si trovino e senza collocare gli stessi sulla rete. Con lo ZTNA, il web diventa un vettore non attendibile e l'accesso alle applicazioni avviene tramite un servizio cloud intermediario, controllato da un provider di terze parti o da un servizio self-hosted.

Dato che questo modello evita la necessità di hardware e processi VPN tradizionali, esso consente di creare un processo fluido per l'utente e migliora l'esperienza complessiva.

Lo ZTNA fornisce accesso controllato alle risorse, migliora la connettività ed elimina la necessità di esporre direttamente le applicazioni a Internet, il che riduce l'area della superficie di attacco. È diventato largamente adottato durante la pandemia, consentendo ai lavoratori da remoto e da casa di accedere alle applicazioni core con lo stesso livello di controlli di sicurezza dei dipendenti che operano in ufficio. Pertanto, oggi, lo ZTNA sta rapidamente diventando uno standard di best practice che le aziende stanno adottando in tutti gli ambiti di business. Che gli utenti accedano al data center, alle app private o al cloud pubblico, indipendentemente dal fatto che si trovino in ufficio o che lavorino da remoto, l'esperienza sarà quindi identica.

## ZERO TRUST EXCHANGE

Zscaler Zero Trust Exchange è una piattaforma SASE appositamente progettata e basata su cloud che connette in modo sicuro utenti, dispositivi e app utilizzando policy aziendali su qualsiasi rete. Una soluzione veloce, sicura e scalabile, che bilancia le priorità di sicurezza dell'organizzazione in base all'esperienza utente, per rendere il cloud un luogo sicuro per fare business.

# 7 PERCHÉ SCEGLIERE ZSCALER: UNA PRESENTAZIONE

Che si tratti di sviluppare nuove soluzioni bancarie che funzionino con la criptovaluta, nuovi servizi transfrontalieri, limitare le frodi o gestire nuovi processi di conformità normativa, le organizzazioni di servizi finanziari si trovano a dover supportare la propria strategia con una piattaforma moderna, solida, agile e scalabile, che consenta all'azienda di innovarsi rapidamente e mitigare la concorrenza.


Scopri di più su Zscaler Zero Trust Exchange

**Soluzione operativa da oltre dieci anni e distribuita su oltre 150 data center in tutto il mondo, Zero Trust Exchange di Zscaler, basata su SASA, è la piattaforma di sicurezza cloud in linea più grande al mondo, che blocca oltre 100 milioni di minacce al giorno. Questa piattaforma elabora oltre 150 miliardi di transazioni e 175 milioni di aggiornamenti di sicurezza al giorno, equivalenti a 10 volte il numero di ricerche quotidiane su Google a livello globale.**

Zscaler vanta un'esperienza consolidata nel settore dei servizi finanziari, con oltre 500 clienti operanti in questo ambito, sei delle prime dieci banche statunitensi, sette delle prime dieci banche europee e due delle prime cinque banche australiane che hanno supportato la propria infrastruttura bancaria con Zscaler Zero Trust Exchange. A livello generale, Zscaler è un partner di fiducia per 4.500 clienti in 185 Paesi, tra cui 450 delle 2.000 aziende leader di Forbes.

Zero Trust Exchange protegge migliaia di clienti da attacchi informatici e perdite di dati collegando in modo sicuro utenti, dispositivi e applicazioni, in qualsiasi luogo, utilizzando le policy aziendali.

I vantaggi principali della piattaforma sono la capacità di sovrapporsi all'architettura esistente per accelerare istantaneamente la trasformazione digitale e offrire servizi efficienti, sicuri, incentrati sul cliente e scalabili:

- **Efficienza:** semplifica l'IT, riduce la complessità e i costi.
- **Sicurezza:** migliora la resilienza e l'approccio alla sicurezza, attraverso un'unica visione per più divisioni, mitigando la perdita dei dati e i rischi per la sicurezza.
- **Focus sul cliente:** supporta l'ambiente di lavoro da qualsiasi luogo, aumenta la capacità, riduce la latenza e crea un'esperienza utente coerente per migliorare la produttività.
- **Scalabilità:** una piattaforma moderna e agile che sostiene l'innovazione e la trasformazione digitale, fornendo opportunita' di crescita.

National Australia Bank (NAB) offre una gamma completa e integrata di prodotti e servizi bancari e finanziari, inclusa la gestione patrimoniale, con operazioni in Australia, Nuova Zelanda, parte dell'Asia, Regno Unito e Stati Uniti.

## Steve Day

National Australia Bank, Melbourne, Australia

nab.com.au

**A causa del lockdown dovuto alla pandemia di Covid-19, questa banca si è trovata a dover consentire rapidamente al personale di lavorare da casa, continuando a fornire servizi a più di 9 milioni di clienti.**

"Prima della pandemia di Covid-19, non avevamo mai avuto più di 5.000 membri del nostro personale che lavorassero da remoto", ha dichiarato Steve Day, EGM Infrastructure, Cloud and Workplace presso NAB. "Dovevamo trovare rapidamente un modo per attrezzare il personale del centro di contatto, in modo che potesse gestire le chiamate da casa, accedere alle nostre app e ai nostri archivi di dati da remoto", ha dichiarato. "Tutto questo, gestendo al contempo quattro volte i normali volumi di chiamate".

Lavorando insieme a Zscaler, la NAB è riuscita a fornire accesso remoto sicuro a più di 32.000 dipendenti, inclusi i team del call center, in sole tre settimane. La NAB ha adottato Zero Trust per ridurre i costi e la superficie di attacco, creando un'infrastruttura in grado di supportare le operazioni future.

"Lo Zero Trust offre due grandi vantaggi. In primo luogo, non abbiamo più bisogno di gestire una rete aziendale separata, il che offre notevoli risparmi sui costi. Nel nuovo modello, offriamo l'accesso a Internet pubblico solo all'interno dei nostri uffici aziendali. In secondo luogo, abbiamo aumentato l'approccio alla sicurezza, non installando un'infrastruttura di sicurezza più costosa, ma rimuovendo tutti i dati e le applicazioni dall'ambiente aziendale per ridurre la superficie di attacco. Ora disponiamo di un'infrastruttura di rete sicura, in grado di supportare NAB durante la crisi attuale e quando le operazioni torneranno alla normalità".

"I dipendenti vanno a casa, accendono il loro PC e operano esattamente come se fossero in ufficio. Non devono preoccuparsi di ulteriori passaggi di accesso o gestire i token di sicurezza, funziona tutto da sé", ha riferito Steve Day, EGM Infrastructure, Cloud & Workplace.

# 8 FUSIONI E ACQUISIZIONI

Le fusioni, le acquisizioni e le scissioni sono prevalenti nel settore dei servizi finanziari, ma impegnative per i team di rete e sicurezza che sono responsabili di garantire la connettività degli utenti alle app interne e la sicurezza dei dati sensibili.

**La convergenza di reti disparate, la gestione di indirizzi IP sovrapposti e la creazione di standard di sicurezza coerenti sono solo alcuni esempi delle sfide che l'IT si trova a dover affrontare. I progetti sono dispendiosi in termini di tempo e risorse e spesso impiegano mesi e anni per essere completati.**

Velocità, sicurezza ed esperienza utente sono di primaria importanza durante tali transizioni complesse. Lavorando insieme a Zscaler, le organizzazioni possono semplificare notevolmente i progetti di M&A e di cessione:

- Implementando semplicemente il software e instradando gli utenti verso le app in pochi minuti, senza convergere minimamente le reti.
- Adottando una sicurezza standardizzata per tutte le risorse, con app visualizzabili solo per gli utenti autorizzati e con questi ultimi che non sono mai sulla rete.
- Offrendo agli utenti un'esperienza di accesso uniforme indipendentemente dal dispositivo, dall'app o dalla posizione.

Scopri di più su Zscaler Zero Trust Exchange

# 9 QUALI SONO LE PROSPETTIVE DELLA TRASFORMAZIONE DIGITALE?

Se da un lato le organizzazioni finanziarie sono riuscite a reagire rapidamente alla pandemia, i team IT e di sicurezza si stanno ancora adattando al meglio alla nuova normalità.

Consulta più Risorse sul lavoro da qualsiasi luogo

**Una volta risolte le soluzioni temporanee, l'attenzione si rivolge alla fase successiva del percorso di trasformazione digitale. Costruire un'infrastruttura moderna per sostenere l'innovazione futura è fondamentale.**

Man mano che il 5G si sviluppa e il settore dei servizi finanziari adotta una quota crescente di tecnologia operativa, robotica avanzata, dispositivi indossabili e altre innovazioni incentrate sul cliente, emergono nuove sfide e vulnerabilità per la sicurezza. La sicurezza informatica rimarrà sempre uno dei principali rischi che le istituzioni finanziarie si troveranno ad affrontare.

Con il passare del tempo, diventa sempre più importante collaborare con fornitori di infrastrutture affidabili che non solo siano ben attrezzati a gestire le esigenze di oggi, ma che abbiano anche la visione e la capacità di guidare il futuro delle organizzazioni finanziarie a livello globale.

Abbiamo posto ai responsabili IT più visionari una domanda: qual è il futuro del vostro percorso di trasformazione digitale?

# 10 PERCHÉ AGIRE SUBITO?

Il costo di non fare nulla è elevato, che si tratti di un semplice aumento dei costi di infrastruttura e MPLS, della perdita di produttività o del costo di ripristino dopo un attacco informatico.

**Agendo subito, l'organizzazione può ottenere immediatamente un aumento della sicurezza e una visione univoca della stessa in tutta l'azienda, supportando al contempo la nuova realtà del lavoro da remoto.**

Allo stesso tempo, gli investimenti IT diventano sempre più lungimiranti e vengono convogliati in una nuova architettura scalabile, in grado di accelerare le priorità aziendali e le nuove innovazioni.

## CONFORMITÀ NORMATIVA

Le autorità bancarie indipendenti si adoperano per garantire una regolamentazione e una vigilanza efficaci e coerenti del settore bancario e dei servizi finanziari. Tali organismi, con il contributo di organizzazioni leader del settore, hanno sviluppato linee guida e raccomandazioni sull'adozione di tecnologie cloud, sulla procedura e sulla pratica di outsourcing ai fornitori di servizi cloud (CSP) e sull'adozione di un approccio basato sui principi per la gestione e la misurazione del rischio negli ambienti con tecnologia cloud.

Zscaler si impegna ad aiutare i clienti nel loro percorso verso la conformità, offrendo una solida protezione della privacy e della sicurezza, nonché il supporto nel soddisfare gli attuali ed emergenti obblighi normativi di rischio e conformità. Zscaler fornisce informazioni trasparenti e supporto alle best practice per garantire che l'implementazione e la gestione delle proprie soluzioni soddisfino l'infrastruttura della governance.

Consulta più Risorse sul lavoro da qualsiasi luogo

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com