White paper

Mitigare il rischio informativo, velocizzando delle trattative di M&A nel settore dei servizi finanziari

© 2022 Zscaler, Inc. Tutti i diritti riservati.

Introduzione

La piattaforma completa e nativa del cloud di Zscaler connette ogni cosa in modo sicuro, semplifica l'esperienza utente e l'onboarding e agevola la distribuzione e le procedure operative, proteggendo al contempo integralmente le risorse dalle minacce informatiche, in modo che l'azienda possa gestire le transazioni di M&A con un volume, una velocità e una sicurezza maggiori.

©2022 Zscaler, Inc. Tutti i diritti riservati.

Le sfide nelle operazioni di M&A/D nei servizi finanziari

Il settore bancario, dei servizi finanziari e delle assicurazioni (BFSI) sta assistendo a cambiamenti di vasta portata, che stanno stravolgendo i loro modelli di business, minacciandone in alcuni casi l'esistenza stessa. I bassi tassi di interesse, i controlli normativi e l'incertezza della politica monetaria, uniti ai profondi cambiamenti indotti dalla trasformazione digitale, quali la finanza decentralizzata e la tecnofinanza (FinTech), hanno spinto le organizzazioni del settore BFSI a dare la priorità a strategie di crescita inorganica, soprattutto nei casi in cui le loro capacità tecnologiche risultano carenti.

Le fintech con modelli di business maturi stanno intensificando le proprie operazioni di mercato, e stanno emergendo otto categorie di transazioni, tra cui:

1. Servizi bancari digitali (ad esempio, l'acquisizione di EVEN da parte di MoneyLion per 440 milioni di dollari)
2. Pagamenti (ad esempio, l'acquisizione di reti da parte di Mastercard per 3,2 miliardi di dollari)
3. Acquista ora, paga dopo (Buy Now, Pay Later, BNPL) (ad esempio, l'acquisizione di Afterpay da parte di Square per 29 miliardi di dollari)
4. Prestiti (ad esempio, l'acquisizione di Truebill da parte di Rocket Companies per 1,3 miliardi di dollari)
5. Gestione patrimoniale (ad esempio, l'acquisizione di Nutmeg da parte di JPMorgan Chase)
6. Assicurazione (ad esempio, l'acquisizione di Metromile da parte di Lemonade per 500 milioni di dollari)
7. Piattaforma Fintech (ad esempio, l'acquisizione di Tink da parte di Visa per 2,2 miliardi di dollari)
8. Finanza decentralizzata (ad esempio, l'acquisizione di Blockrize da parte di Gemini)
9. Consolidamento delle banche regionali (ad esempio, l'acquisizione di First Midwest da parte di Old National Bank per 2,5 miliardi di dollari)

La tesi dell'accordo alla base delle transazioni appena citate sembra essere:

1. Una grande organizzazione consolidata del settore BFSI che acquisisce una fintech per potenziare le proprie piattaforme tecnologiche (es. algoritmo proprietario, modelli di data science)
2. Una fintech in crescita che acquisisce un'altra fintech per rafforzare la propria posizione di leadership

Affinché le operazioni di M&A ottengano i risultati attesi, i responsabili dell'accordo e i dirigenti dovrebbero affrontare in modo proattivo tutte le aree che potrebbero influire negativamente sulla valutazione stimata e sulle sinergie.

© 2022 Zscaler, Inc. Tutti i diritti riservati.

Squilibrio nell'assetto tecnologico.
Le organizzazioni del settore BFSI hanno sviluppato un complesso mix di sistemi tecnologici, nel corso degli ultimi due decenni, che ha dato vita a un marcato debito tecnico. Molte organizzazioni hanno adottato tecnologie digitali senza prestare particolare attenzione al peso crescente del debito tecnico e funzionale, e ciò può comportare rischi critici nei contesti in cui si verificano M&A, in quanto diventa molto difficile valutare il profilo di rischio dell'organizzazione oggetto della fusione. Di conseguenza, le organizzazioni non raggiungono mai le sinergie stimate in termini di ricavi e costi.

Le policy di sicurezza informatica adottate dalle grandi organizzazioni, pensate per un'architettura di sicurezza tradizionale basata sul perimetro di rete, potrebbero non essere applicabili alle aziende Fintech nate sul cloud. Ad esempio, un grande istituto finanziario nordamericano che opera su un'architettura di sicurezza basata su un sistema castle-and-moat (ad esempio firewall, VPN) si è trovato in grave difficoltà quando ha dovuto integrare la piattaforma tecnologica nativa del cloud derivante dalle acquisizioni di realtà fintech, il che si è tradotto in un'esperienza scadente per l'utente finale.

Minacce alla sicurezza informatica e vulnerabilità dei dati.
Spesso, dopo l'annuncio di operazioni straordinarie, emergono problemi legati alla sicurezza informatica e alla vulnerabilità dei dati, questo perché gli utenti malintenzionati cercano di approfittarsi del periodo ambiguo di transizione, quando i dipendenti risultano particolarmente vulnerabili. Nelle organizzazioni BFSI, la necessità di proteggere rapidamente i dati, i processi e gli ecosistemi regolamentati di sedi e partner è fondamentale per rimanere conformi ed evitare attenzioni mediatiche indesiderate. Inoltre, la mancanza di uno scrupoloso processo di due diligence, volto a comprendere il profilo di rischio delle aziende acquisite, può trasformarsi in un incubo in termini normativi, per le aziende di questo settore. Ad esempio, PayPal ha dovuto sospendere i servizi di TIO Networks nove mesi dopo la sua acquisizione, a causa di una grave violazione che non era stata rilevata e segnalata in tempo.

Secondo un report pubblicato da Kroll, il 13% di tutti gli attacchi informatici è concentrato sul settore BFSI e comprende ransomware, ingegneria sociale e la compromissione della posta elettronica aziendale.

Zscaler fa in modo che le integrazioni delle M&A siano più sicure e veloci.
Zscaler offre un approccio moderno alle operazioni di integrazione e separazione che derivano dalle M&A/D, basato sull'implementazione di una soluzione Zero Trust Exchange fornita as-a-service, ossia come servizio, in una piattaforma cloud. Zscaler Zero Trust Exchange connette in modo sicuro gli utenti a sistemi, applicazioni, dispositivi e tra loro, senza connetterli alla rete dell'azienda acquirente oppure oggetto della separazione. Questa piattaforma offre un accesso immediato ai dati e garantisce l'operatività, proteggendo al contempo la rete aziendale dai potenziali rischi e dalle minacce informatiche. Il risultato è una sandbox di integrazione altamente scalabile, sicura e trasparente, riutilizzabile più e più volte.

Il time-to-value è calcolabile in termini di settimane, anziché mesi e trimestri
Zscaler semplifica il processo di integrazione con la sua soluzione Zero Trust Exchange distribuita sul cloud, che consente di ottimizzare quasi istantaneamente le architetture di rete e la standardizzazione della sicurezza in tutto l'ambiente. Le aziende che si affidano a Zscaler possono integrare solo ciò di cui hanno realmente bisogno, senza dover integrare per forza tutto e senza restare intrappolate nelle complessità tecnologiche tipiche delle operazioni di M&A (tempistica, prestazioni, costi, esperienza). La modalità as-a-service di Zero Trust Exchange consente di ottenere, già dal primo giorno, un'infrastruttura di rete e sicurezza pronta per il futuro. Completamente operativa in pochi giorni, la soluzione di Zscaler abbatte ogni barriera all'azione, consentendo alle organizzazioni di sfruttare le sinergie e generare valore più rapidamente.

© 2022 Zscaler, Inc. Tutti i diritti riservati.

I rischi vengono mitigati e tenuti sotto controllo con una policy di sicurezza unificata.
Zscaler protegge attivamente l'azienda dalle minacce informatiche note e in continua evoluzione, nonché dai rischi interni, grazie a una piattaforma cloud scalabile e semplice da utilizzare. Dato che tutto il traffico può passare attraverso la nostra piattaforma, le organizzazioni possono concentrarsi sulla protezione del traffico, anziché sul perimetro. Zscaler offre una visibilità completa e capacità di audit su tutti gli accessi all'interno dell'azienda, il tutto da un unico pannello di controllo, per individuare e neutralizzare tutte le minacce provenienti dalla rete.

Semplificazione dell'integrazione e ottimizzazione dei costi attraverso le operazioni amministrative, non ingegneristiche
La piattaforma consente alle operazioni IT e di sicurezza di connettere in modo sicuro qualsiasi dispositivo, applicazione o utente, indipendentemente da dove lavori, viaggi o da dove si connetta. L'accesso è garantito praticamente senza sforzo. Attraverso delle policy di logica aziendale, le organizzazioni riescono a controllare, connettere e verificare in modo sicuro l'accesso ad applicazioni, utenti e workload, senza la necessità di ricorrere a una rete privata o di una SD-WAN. Inoltre, possono sfruttare la potenza di Internet e il più grande data exchange sicuro a livello globale per trasportare il traffico aziendale e adattare in modo ottimale i sistemi on-demand, in base alla crescita e alle acquisizioni, grazie a un modello basato su utenti/a consumo. Le limitazioni delle soluzioni hardware vengono eliminate e non ci sono funzionalità da autogestire.

Potenziamento dell'agilità e della flessibilità aziendale
Zscaler elimina molti degli elementi tecnici complessi e dispendiosi in termini di tempo che caratterizzano le integrazioni, grazie alla sua piattaforma che aiuta a trasformare le operazioni di M&A in processi altamente ripetibili. Zscaler semplifica le integrazioni, consentendo agli amministratori di selezionare solo i sistemi di cui hanno realmente bisogno, e può aiutare a separare le risorse dismesse, senza ricorrere all'approccio "clona e vai".

Zscaler Zero Trust Exchange accelera in modo sicuro le operazioni di M&A/D

Zero Trust Exchange è il fulcro della piattaforma Zscaler e consente alle aziende di accelerare in modo sicuro la propria trasformazione digitale. Exchange amplia gli ambienti IT, in modo che i dipendenti possano lavorare ovunque, mantenendo al contempo una sicurezza standardizzata in tutta l'azienda. Consente inoltre una maggiore connettività e separa la sicurezza dalla rete.

Semplificazione delle trasformazioni di rete. Exchange passa da un approccio hub-and-spoke a un modello direct-to-cloud: si tratta di un approccio moderno e semplificato che elimina la maggior parte delle difficoltà associate alle integrazioni di rete, all'hardware e all'indirizzamento. Fornisce un unico pannello di controllo per supportare qualsiasi tipo di strategia cloud (ibrida, multi-cloud, multi-tenant, multi-VPC) e consente l'accesso diretto alle applicazioni per qualsiasi programma, ovunque sia ospitato.

Trasformazione e modernizzazione della sicurezza. Il tradizionale approccio perimetrale, basato sul modello castle-and-moat, sta venendo gradualmente abbandonato a favore del modello zero trust. Lo zero trust offre una connessione sicura e diretta che riduce le potenziali vulnerabilità legate all'archiviazione e allo spostamento dei dati, negli ambienti SaaS e su cloud pubblici, ed è applicabile a quasi ogni tipo di minaccia alla sicurezza. Con Zscaler, è possibile limitare la capacità delle minacce di muoversi lateralmente e la scalabilità della piattaforma reagisce alle minacce nuove e in evoluzione quasi in tempo reale.

© 2022 Zscaler, Inc. Tutti i diritti riservati.

Massimo supporto alla forza lavoro moderna e mobile. La forza lavoro di oggi è mobile e svincolata dagli spazi fisici. Zero Trust Exchange supporta questa nuova esigenza, offrendo agli utenti un accesso basato su policy, ovunque si trovino. Sono finiti i tempi in cui si doveva creare un tunnel verso le reti; ora, i problemi vengono risolti in modo proattivo grazie a una strategia di shift-left. La piattaforma può essere adattata per soddisfare le esigenze in evoluzione degli utenti, ovunque e qualsiasi sia il dispositivo utilizzato per accedere a Internet.

Zscaler è la nuova frontiera dell'integrazione

La capacità istantanea di condividere in modo ottimale processi e dati da qualsiasi luogo è un vantaggio competitivo che Zscaler introduce nelle M&A del settore BFSI. La semplicità offerta da Zscaler consente di completare le integrazioni in tempi molto più rapidi, con un impatto minimo sull'utente. Zscaler permette alle organizzazioni di avviare rapidamente le attività di acquisizione di valore, aumentando al contempo il volume delle operazioni straordinarie. Contattaci oggi stesso per una dimostrazione.

zscaler™ | Experience your world, secured.™

Informazioni su Zscaler
Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center nel mondo, Zero Trust Exchange, basata sul framework SASE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.com/it** o seguici su **X (precedentemente Twitter) @zscaler**.

©2022 Zscaler, Inc. Tutti i diritti riservati. Zscaler™, Zscaler Digital Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™ e ZPA™ sono (i) marchi commerciali o marchi di servizio registrati o (ii) marchi commerciali o marchi di servizio di Zscaler, Inc. negli Stati Uniti e/o in altri Paesi. Eventuali altri marchi commerciali appartengono ai rispettivi proprietari.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com/it