RACONTEUR

Rivoluzioniamo la sicurezza informatica

Forcepoint

Forcepoint

Forcepoint è leader globale nel campo della sicurezza informatica per utenti e protezione dei dati. Le soluzioni di Forcepoint basate sul comportamento si adattano ai rischi in tempo reale e vengono fornite attraverso una piattaforma di sicurezza convergente che protegge gli utenti della rete e l'accesso al cloud, impedisce la fuoriuscita di dati riservati dalla rete aziendale ed elimina le violazioni interne. Con sede ad Austin, in Texas, Forcepoint crea ambienti sicuri e affidabili per migliaia di clienti aziendali e governativi, e i loro dipendenti, in oltre 150 paesi.

RACONTEUR

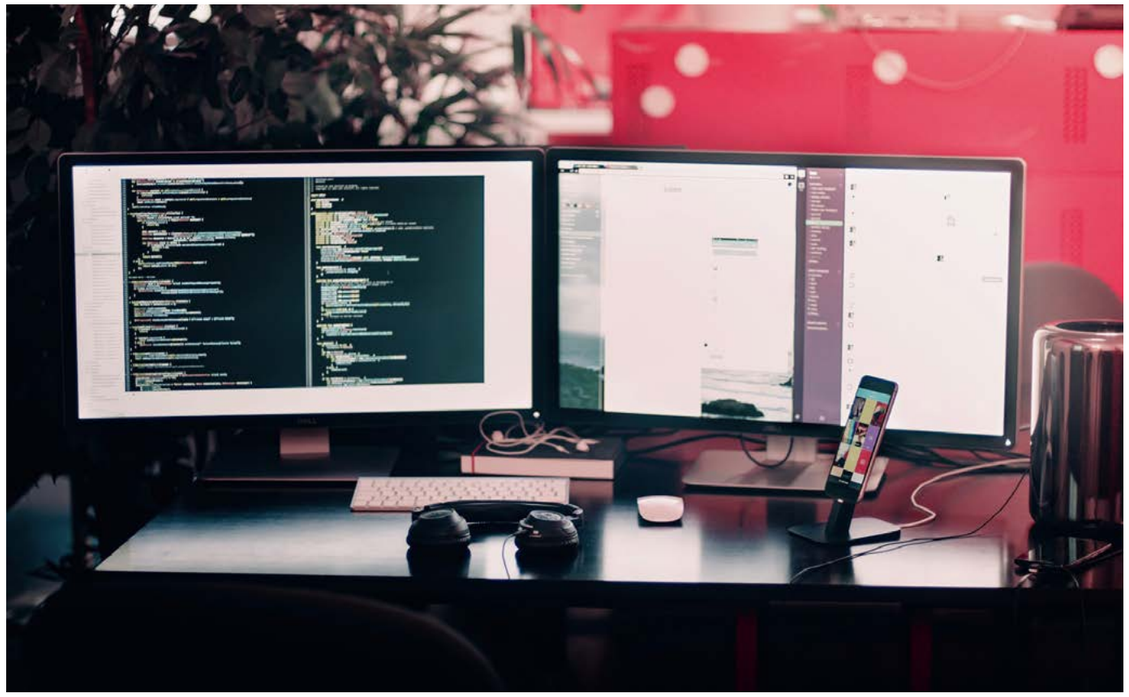
Sponsorizzato da
Forcepoint

Responsabile di progetto Georgie Cauthery
Redattore Peter Archer
Design Kellie Jerrard, Sara Gelfgren
Responsabile della produzione Hannah Smallman
Responsabile del Marketing digitale Kyri Rousou

Collaboratori
Christine Horton
Nick Ismail
Tamlin Magee

Sebbene questa pubblicazione sia finanziata attraverso la pubblicità e la sponsorizzazione, tutti gli editoriali sono privi di pregiudizi e le caratteristiche sponsorizzate sono chiaramente etichettate. Per una scadenza imminente, richieste di collaborazione o feedback, chiamare il numero +44 (0)20 3428 5230 o inviare un'e-mail a info@raconteur.net

Indice



TECNOLOGIA

La rivoluzione dell'implementazione tecnologica

SASE, acronimo di Secure Access Service Edge, è un servizio basato nel cloud e offre una soluzione olistica per fornire un ambiente protetto in cui la fiducia è pari a zero

Tamlin Magee

La gestione della sicurezza informatica a distanza presentava le sue difficoltà ancor prima dell'avvento della pandemia e che lo smart working diventasse la norma per molti. Il fatto che le imprese si fossero già spostate con entusiasmo verso modalità di lavoro basate su un cloud ha reso le vecchie forme di difesa della rete, il cosiddetto approccio "Castle-and-Moat", meno attuabile. Era necessario, pertanto, cedere un certo livello di controllo.

Negli anni, approcci quali CASB, o broker di sicurezza per l'accesso al cloud, firewall-as-a-service e gestione dell'identità e dell'accesso hanno in qualche modo contribuito ad aiutare le aziende a costruire difese migliori. Ma senza una strategia unificata di implementazione olistica, alle aziende mancava ancora la visibilità necessaria per gestire la sicurezza nel mondo del cloud "digital-first".

Queste tecnologie, e non solo, sono ora riunite sotto la dicitura Secure Access Service Edge, o SASE (pronunciato "sassy"), con un pacchetto di servizi facile da vendere e acquistare, afferma Martin Courtney, Principal Analyst di TechMarketView. Poiché il framework è nato sul cloud, i programmi guidati da SASE si prestano bene alle reti Zero Trust, assicurando che a nessuna persona vengano fornite credenziali inappropriate di default.

L'idea è di abilitare l'accesso protetto valutando caso per caso, fornendo agli utenti i permessi di cui hanno bisogno per svolgere un'azione specifica, piuttosto che permettere loro di accedere a tutta la rete. SASE promette di ridurre i costi, la complessità e le difficoltà di integrazione all'interno dell'azienda, garantendo una migliore visibilità.

Come afferma Martin Courtney, sebbene SASE non rappresenti l'unico approccio Zero Trust, propone comunque una soluzione ben confezionata che offre gli strumenti necessari per verificare gli utenti finali e i dispositivi in base alla posizione, all'apparecchiatura, all'indirizzo IP e alla rete.

Kevin Curran, professore di sicurezza informatica presso la Ulster University, afferma che SASE è una soluzione moderna per superare i problemi legati ai sistemi obsoleti, aggiungendo che la sicurezza tradizionale non è più adatta allo scopo e che i modelli Zero Trust sono semplicemente più pertinenti all'era digitale.

"SASE è la soluzione ideale per accogliere i modelli Zero Trust", continua Kevin Curran. "Le aziende stanno cercando di tappare i buchi già da un po', aggiungendo connessioni, sistemi e persone alle loro reti per fornire soluzioni rapide per la connettività".

> **SASE andrebbe introdotto lentamente e in fasi che prevedono progetti pilota e adeguamenti in un ambiente di prova prima dell'implementazione**

L'85%

delle aziende prevede di implementare una piattaforma SASE o SD-WAN entro l'estate del 2022

Accelerate Technologies 2020

Questo ha portato a un marasma in continua crescita, in cui le aziende non riescono nemmeno ad avere un quadro d'insieme di ciò che accade in un dato momento. "Essendo basato nel cloud, SASE offre una soluzione olistica per fornire un ambiente protetto in questi tempi difficili", conclude Kevin Curran.

Tuttavia, la misura in cui i componenti SASE vengono correttamente combinati in un'unica interfaccia gestibile varia notevolmente, poiché, secondo Martin Courtney, alcuni fornitori stanno "infilando nel calderone qualsiasi prodotto o soluzione gli capiti sotto mano".

Come per la maggior parte delle cose, a portare un valore aggiunto concreto è in realtà l'integrazione continua nelle pratiche aziendali. Le aziende dovrebbero smettere di vedere SASE come una soluzione pronta all'uso, ma dovrebbero invece allineare le loro attività a questo approccio in maniera continuativa.

Come sostiene Kevin Curran, affinché una strategia SASE sia efficace, tutti i touchpoint devono essere mappati e ciò significa che bisogna innanzitutto condurre una valutazione del rischio approfondita per esaminare ogni accesso ai dati archiviati e ogni autenticazione dei dipendenti, oltre al ruolo che parti terze assumono all'interno della rete.

Garantire la continuità è un fattore tanto culturale quanto tecnico. I responsabili della sicurezza dovrebbero iniziare istituendo dei solidi processi di governance a livello aziendale, cercando al contempo di vincere la diffidenza dei dipendenti tramite una formazione adeguata. È opportuno spiegare chiaramente ai dipendenti le motivazioni dietro questi cambiamenti radicali.

Forse, la cosa più importante resta però convincere la leadership, ma per fortuna esistono delle chiare linee di attacco per comunicare i benefici di questo approccio. I vantaggi del modello Zero Trust come strategia di mitigazione sono in qualche modo ovvi, ma la sicurezza e la convergenza di rete sono altrettanto importanti dal punto di vista strategico, poiché consentono alle imprese di ampliare le reti in modo più sicuro in linea con la propria crescita.

In questa opera di convincimento, va comunque messo in evidenza che SASE non è un esercizio meramente formale da svolgersi una tantum. I responsabili informatici e della sicurezza devono invece vedere SASE come una fase di un viaggio e tracciare un percorso che sia strategicamente allineato all'azienda nel suo complesso.

FORMAZIONE SCOLASTICA

Come rendere SASE una priorità a livello direttivo

I responsabili informatici e coloro incaricati della sicurezza devono educare i dirigenti sulla necessità di un'infrastruttura di protezione dei dati su un cloud, sostiene Nicolas Fischbach, Global Chief Technology Officer presso Forcepoint

Nicolas Fischbach, Global Chief Technology Officer, Forcepoint

Nonostante l'aumento degli attacchi informatici sferrati contro le aziende e l'impatto economico delle normative più severe in materia di protezione dei dati, i consigli di amministrazione continuano a mettere la sicurezza informatica in secondo piano.

Tuttavia, man mano che le aziende affrontano la loro trasformazione digitale, verso l'Industria 4.0, l'investimento nelle soluzioni di sicurezza del cloud e la loro comprensione deve diventare la massima priorità per l'alta dirigenza aziendale.

Nel 2019 Gartner ha citato SASE (Secure Access Service Edge) come il framework di sicurezza più appropriato per le imprese moderne. SASE riunisce le soluzioni esistenti per la sicurezza e la protezione dei dati, e le fa convergere nel cloud. Il fatto di avere una "finestra" unica consente ai responsabili di sicurezza e gestione dei rischi di abilitare e gestire i requisiti versatili di accesso a dati e app con controlli più coerenti delle policy.

La pandemia di coronavirus ha accelerato l'esigenza delle aziende di adottare questo framework di sicurezza e protezione dei dati poiché i dipendenti in ogni parte del mondo sono costretti a lavorare da remoto.

Per comprendere l'importanza di adottare l'approccio SASE e la sicurezza del cloud, i responsabili di informatica, gestione del rischio, protezione dei dati e sicurezza devono essere in grado di educare i dirigenti e comunicare in modo efficace i vantaggi in termini di protezione dei due asset più importanti di un'azienda: le persone e i dati.

La sfida di comunicare l'importanza della sicurezza alla dirigenza

Affrontare il tema della sicurezza con i dirigenti comporta due sfide principali.

La prima è che molti consigli di amministrazione non ricevono informazioni dettagliate in merito alla sicurezza e di conseguenza questa non figura mai tra le loro priorità, in particolare se non è guidata da fattori legati a conformità o rischio.

La seconda sfida sta nel cambiare la percezione della sicurezza e della protezione delle informazioni, che al momento sono viste come una sorta di polizza assicurativa per proteggere l'azienda da eventuali rischi, piuttosto che come qualcosa che determina i risultati aziendali.

In realtà, la sicurezza abilita la trasformazione digitale nel cloud e contribuisce a portare un valore aggiunto all'azienda. Questo aspetto si è forse dimostrato al meglio nelle prime fasi di chiusura totale a causa del COVID-19, che ha comportato uno spostamento di massa verso il lavoro da remoto. In questo ambiente le imprese hanno dovuto permettere ai dipendenti di lavorare da casa in maniera sicura, proteggendo le risorse e i dati aziendali e favorendo al contempo la produttività e l'innovazione.

I responsabili informatici e della sicurezza hanno ora un'ottima opportunità per presentare alla dirigenza una versione re-ingegnerizzata della sicurezza, indispensabile per un futuro di successo nel cloud, e devono sostenerla a gran voce.

Invece di vedere la sicurezza come un freno all'innovazione o un qualcosa senza contesto a cui non ci si può sottrarre, lo scopo dovrebbe essere quello di presentare SASE come un catalizzatore per ottenere un vantaggio competitivo e allinearlo agli obiettivi aziendali. Questi sono aspetti a cui la dirigenza saprà relazionarsi.

Andrebbe inoltre comunicato che, sebbene SASE abbia le potenzialità per contribuire a guidare l'eccellenza operativa, necessita comunque di una piattaforma e di un provider fidati, rispettabili e comprovati per essere messo in pratica.

Al momento, esiste un provider in grado di offrire un'esperienza di rete e sicurezza ottimale, compresa la transizione dallo stato attuale a quello futuro? I professionisti IT saranno propensi ad abbandonare i vantaggi effettivi o percepiti e la libertà del multi-sourcing in favore di un'unica soluzione da parte di un solo provider?

Nel decidere se adottare SASE o meno, è quindi opportuno porsi delle domande ben precise.

SASE è un viaggio

Prima ancora di spiegare i vantaggi di SASE, i responsabili informatici e della sicurezza devono iniziare dal basso e spiegare alla dirigenza il livello di maturità attuale dell'azienda in riferimento alla sicurezza. Dopo aver stabilito tutto ciò in linea con gli obiettivi di trasformazione digitali, allora si può cominciare a programmare il viaggio verso SASE. Si tratta di un percorso a fasi, che spesso prevede il passaggio da on-premise a ibrido a cloud-first o cloud-native.

Le aziende avranno già un modus operandi e delle implementazioni di sicurezza esistenti per quanto concerne la sicurezza di rete e del cloud e per la protezione dei dati, pertanto, con la progressiva eliminazione delle soluzioni precedenti e l'adozione di un approccio più dinamico al lavoro in ambienti virtuali, è essenziale che la dirigenza comprenda che SASE, così come la trasformazione digitale, è un viaggio che continuerà a evolversi.

È inoltre importante spiegare alla dirigenza che SASE andrà a toccare vari reparti dell'azienda. Per attuare questo programma è necessario, come minimo, un forte allineamento aziendale tra Chief Information Security Officer (CISO), Chief Information Officer e Data Protection Officer.

Il valore commerciale di SASE

Se SASE viene integrato nelle operazioni aziendali invece di essere trattato come un semplice elemento aggiuntivo, migliorerà l'esperienza dei dipendenti consentendo loro di lavorare in modo produttivo e sicuro, senza impedimenti dovuti a misure di sicurezza obsolete.

Questa convergenza sarà di aiuto, ad esempio, nella frammentazione delle policy affinché agli utenti vengano attribuite regole specifiche a seconda dell'applicazione o dei dati a cui provano ad accedere. Inoltre, l'esperienza dell'utente finale è spesso collegata direttamente a queste soluzioni di sicurezza disgiunte, il che provoca attrito invece di fungere da rete di sicurezza per l'utente.

SASE contribuisce anche a ridurre la complessità del toolbox del CISO. Attualmente ci sono troppi strumenti di sicurezza diversi che non sono integrati, ma riunendoli tutti sotto un unico framework, si ridurrà l'impatto operativo e si migliorerà il tempo medio per rilevare e reagire.

Dal punto di vista aziendale, è importante che la dirigenza comprenda che SASE consentirà alle imprese di restare produttive e innovative, assicurando allo stesso tempo la conformità e la sicurezza indipendentemente da dove si trovano i loro dipendenti o dispositivi, un aspetto cruciale non solo nell'era attuale dello smart working, ma anche per i modelli lavorativi flessibili che sono ormai diventati ordinari.

SASE aiuterà le imprese a ridurre il rischio, migliorare la visibilità sull'intera rete e creare un metodo di risposta più automatizzato alle minacce che potrebbero danneggiare gravemente l'azienda, sia dal punto di vista economico che della reputazione.

Infine, i responsabili informatici e della sicurezza devono educare la dirigenza sulla necessità di un framework per la sicurezza e la protezione dei dati nel cloud. L'IT ibrido è ora una realtà per le imprese e la maggior parte di esse ha infatti implementato parte della propria infrastruttura al di fuori della propria sede.

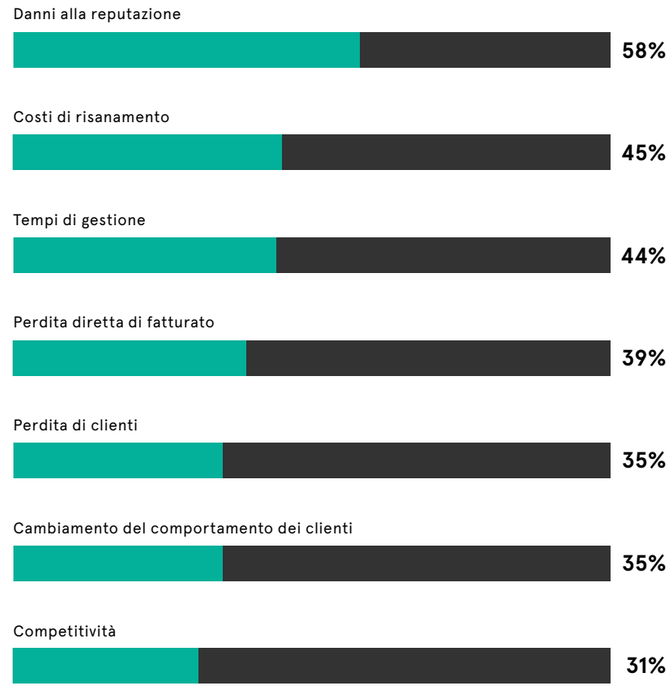
SASE aiuterà le imprese a ottenere visibilità e fornirà un accesso sicuro a endpoint, reti, applicazioni e dati, rendendo evidente il vantaggio principale dell'IT ibrido: sfruttare al massimo il cloud man mano che il tasso di adozione aumenta.

L'85%

delle aziende ha un membro del consiglio di amministrazione responsabile della sicurezza informatica

Grant Thornton 2019

IMPATTO DI UN ATTACCO INFORMATICO



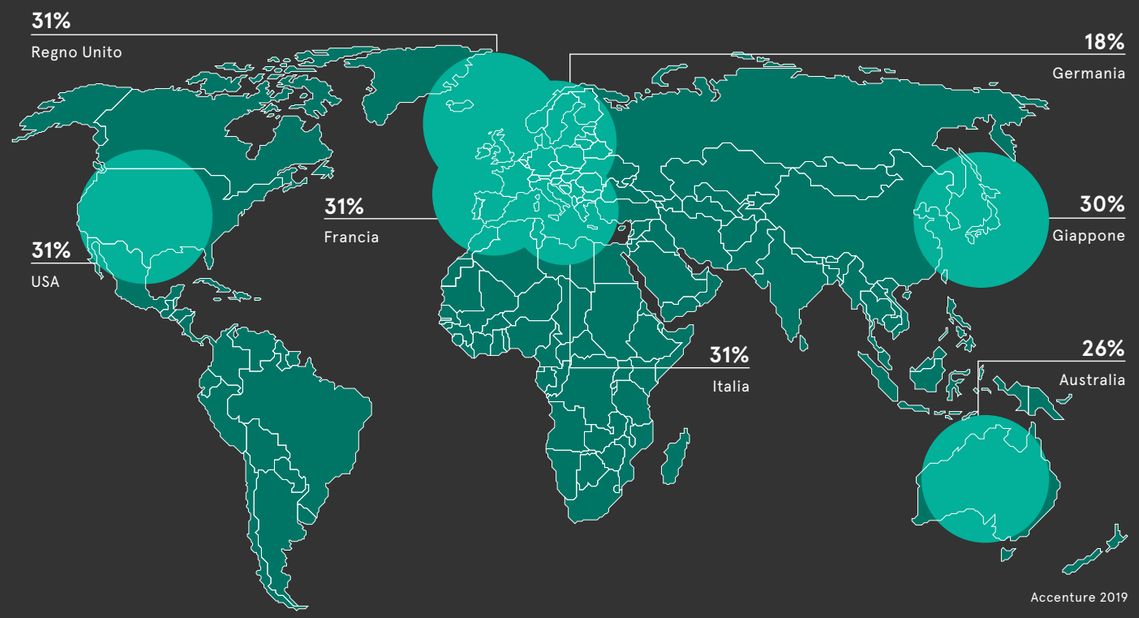
Ponemon Institute e Forcepoint 2020

MAI FIDARSI

Il costo derivato dal crimine informatico continua a crescere e spesso il rischio maggiore è posto dagli stessi dipendenti. Molte aziende hanno difficoltà a rilevare le minacce interne, ma un approccio Zero Trust può essere la soluzione

LE TECNOLOGIE ATTUALMENTE DISPONIBILI NON FAVORISCONO UNA RIDUZIONE DELLA CRIMINALITÀ INFORMATICA

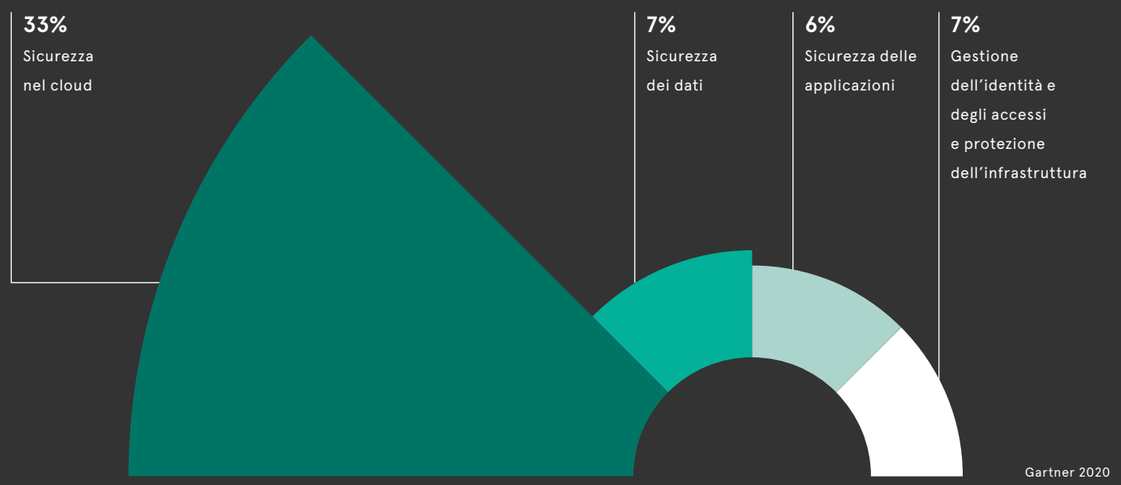
Aumento anno per anno del costo della criminalità informatica in base al paese



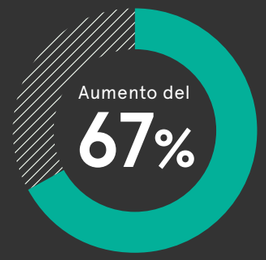
Accenture 2019

CON LA CRESCITA RAPIDA DELLA SICUREZZA BASATA SU CLOUD, LA RISPOSTA POTREBBE RISIEDERE NEL CLOUD STESSO

Crescita dei mercati della sicurezza nel 2020



Gartner 2020



delle violazioni della sicurezza informatica negli ultimi 5 anni

Accenture 2019

del costo della criminalità informatica negli ultimi 5 anni

Accenture 2019

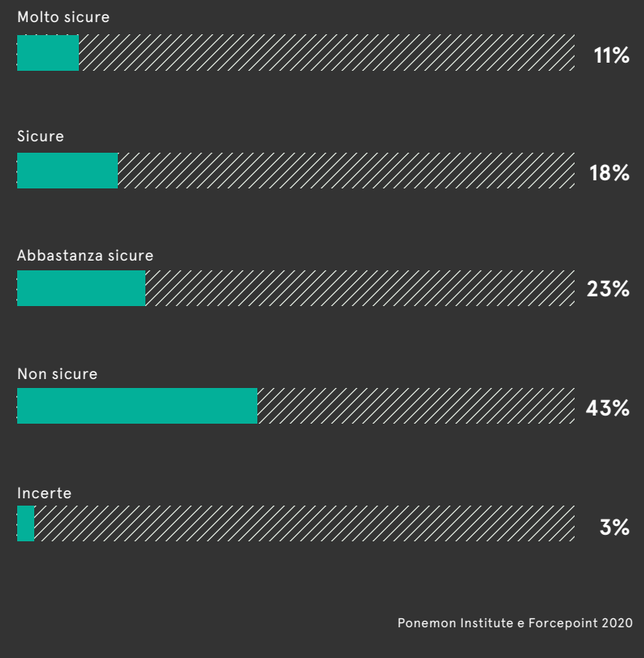
La spesa prevista per la sicurezza del cloud nel 2020 è di

$585m

Gartner 2020

LE IMPRESE HANNO DIFFICOLTÀ A DETERMINARE SE I LORO UTENTI SONO AFFIDABILI

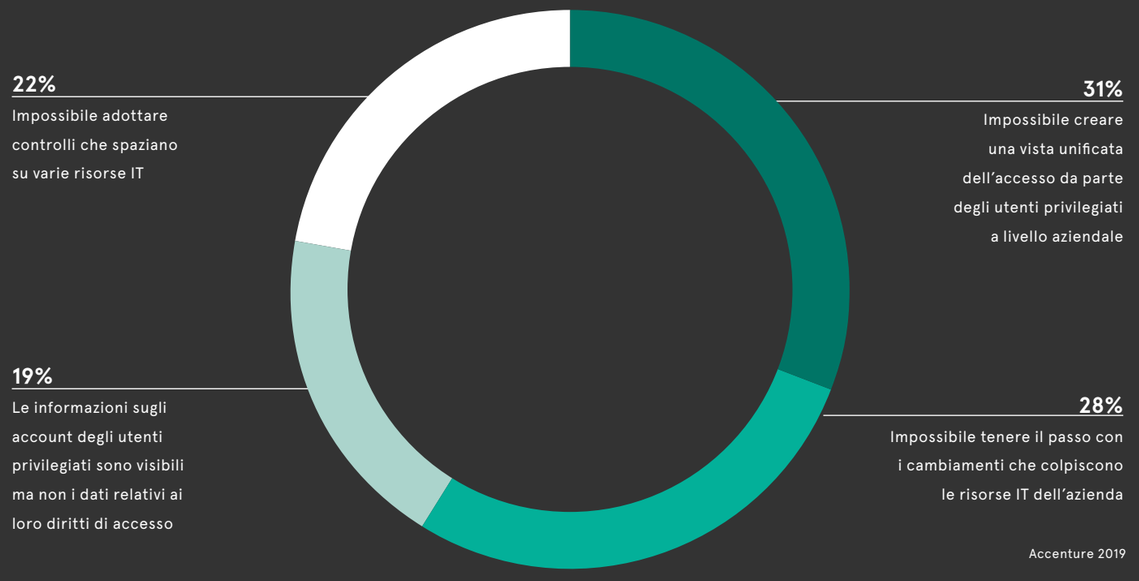
Quanto si sentono sicure le aziende di avere visibilità a tutti i livelli e di poter determinare se gli utenti privilegiati rispettano le policy



Ponemon Institute e Forcepoint 2020

...E GLI ATTUALI STRUMENTI DI SICUREZZA RENDONO DIFFICILE RILEVARE UN CASO DI MINACCIA INTERNA

Motivo principale della mancanza di fiducia delle imprese nei confronti degli utenti



Accenture 2019

CULTURA

Utilizzare lo stack di sicurezza per differenziarsi

Una user experience coerente e migliorata può differenziare un'azienda, aumentando il coinvolgimento e la fedeltà quando il personale lavora da casa

Nick Ismail

Quasi dal giorno alla notte, il disagio iniziale causato dalla pandemia di coronavirus ha portato a uno spostamento globale verso il lavoro da remoto. Questo cambiamento monumentale ha creato una serie di sfide tecnologiche e culturali a cui le aziende hanno dovuto adattarsi rapidamente.

Nonostante le sfide palesi, la forza lavoro del futuro – i millennial e la Generazione Z in primis – si aspettano questo tipo di flessibilità dai potenziali datori di lavoro e lo considerano spesso un requisito importante per attrarre e mantenere i talenti.

Il COVID-19 ha certamente accelerato questo passaggio al lavoro da remoto, ma si trattava comunque di una tendenza in crescita, guidata dal desiderio di una maggiore flessibilità da parte della forza lavoro rappresentata dai millennial e dalla Generazione Z. Con questa nuova normalità che diventa la realtà, sorge una domanda: in che modo le aziende possono scalare l'accesso remoto garantendo al contempo la sicurezza?

Matt Palmer, direttore di Cyberclaria, sostiene che non serve aggiungere ulteriore tecnologia, ma bisogna invece semplificarla. "Le aziende dovrebbero rimpiazzare le complesse tecnologie del passato con soluzioni integrate che offrano accesso ininterrotto indipendentemente da dove si trova l'utente, quale dispositivo utilizza e quali sistemi o applicazioni necessita per accedervi", aggiunge Palmer.

"Non ha senso mantenere l'autenticazione in sede, se l'utente lavora nel cloud; gli utenti devono poter essere in grado di accedere una volta su qualsiasi dispositivo e avere un'esperienza ininterrotta".

Creare una migliore user experience

Il passaggio accelerato al lavoro da remoto ha offerto ai responsabili informatici e della sicurezza l'opportunità di creare una migliore user experience con il proprio stack di sicurezza.

Attualmente, l'esperienza dell'utente in merito alla sicurezza è in genere scarsa e per ovviare a ciò le aziende dovrebbero adottare delle soluzioni integrate, incentrate sulla gestione dell'identità e la scalabilità nel cloud, al fine di garantire una user experience coerente e flessibile, un aspetto essenziale in un ambiente di smart working.

Kelly Bissell, responsabile presso Accenture Security, sostiene che dei framework di sicurezza come SASE (Secure Access Service Edge) consentono un'esperienza di accesso coerente sia in ufficio che da remoto, aderendo al contempo ai principi di Zero Trust.

"I controlli di sicurezza come il Trust Score possono semplificare le policy, riducendone il numero per lo stesso accesso, facendo meno affidamento sull'autenticazione basata sull'utente e fornendo una migliore user experience. I controlli di sicurezza degli endpoint come la containerizzazione possono consentire a un dipendente di utilizzare il proprio dispositivo personale per accedere in sicurezza alle risorse aziendali", aggiunge.

Facendo un passo avanti per attrarre la forza lavoro rappresentata dai millennial e dalla Generazione Z, le aziende dovrebbero pensare di integrare tecnologie, come dati biometrici e riconoscimento facciale, nel proprio stack di sicurezza, strumenti che fanno sempre più parte della vita sociale dei giovani.

Attirare e mantenere i talenti

Per attirare e mantenere i talenti, aumentando al contempo la produttività, è essenziale creare un framework di sicurezza accessibile che non solo riduca l'attrito con l'utente, ma arricchisca anche l'esperienza del dipendente.

Vince Warrington, Chief Executive di Dark Intelligence, sostiene che ciò sta diventando sempre più importante poiché ora i dipendenti devono avere lo stesso livello di user experience sia che lavorino da remoto che in ufficio.

"È quindi necessario sviluppare soluzioni che agevolino i loro progressi invece che limitarli", aggiunge. "Sappiamo che le frustrazioni legate all'attrezzatura informatica fanno crollare il morale, per cui le aziende che adattano la loro sicurezza alle nuove norme lavorative sono probabilmente più avvantaggiate in fatto di ritenzione e produttività dei dipendenti".

Un morale basso e una frustrazione costante possono anche avere serie ripercussioni sulla sicurezza. I dipendenti che hanno un'esperienza positiva in relazione all'approccio dell'azienda in fatto di sicurezza sono meno propensi a divulgare dati potenzialmente riservati tramite le applicazioni di consumo.

I responsabili possono sfruttare SASE per offrire una solida user experience nel loro stack di sicurezza in modo da differenziare il loro approccio e attrarre la forza lavoro del futuro.

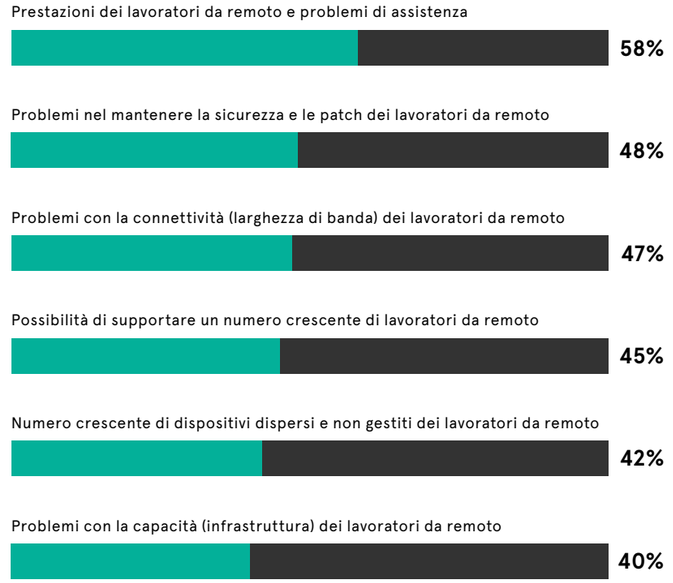
Il framework rappresenta il punto in cui convergono networking e sicurezza, e segna la fine di una percezione di quest'ultima come fonte di frustrazione per l'utente.

Con l'adozione di questa funzionalità di sicurezza integrata o "invisibile", come la descrive Charles Eagan, Chief Technology Officer presso BlackBerry, si migliorerà la user experience.

Palmer di Cyberclaria sostiene che nell'era dello smart working, fornendo ai dipendenti un perimetro di sicurezza incoerente, si dà l'idea che l'azienda non ritenga abbastanza importante offrire loro la stessa esperienza che si aspetterebbero come clienti. "SASE offre l'opportunità di smettere di usare la tecnologia per dire ai dipendenti che non contano e usarla invece per dimostrare loro quanto valgono", conclude.

> **SASE offre l'opportunità di smettere di usare la tecnologia per dire ai dipendenti che non contano e usarla invece per dimostrare loro quanto valgono**

SFIDE POSTE DAL LAVORO DA REMOTO COME CONSEGUENZA DEL COVID-19



Accelerate Technologies 2020

PRIVACY DEI DATI

Risolvere il dilemma della fiducia

Adottando nuovi approcci, le aziende possono garantire la sicurezza e la privacy dei loro dati e sistemi nel cloud

Christine Horton

Il cloud computing è stato un'ancora di salvezza per le aziende nel 2020, poiché ha permesso loro di mettere in piedi nuove forze lavoro da remoto e continua a sostenere le loro attività quotidiane.

Nonostante tutto, c'è un aspetto che continua a causare diffidenza riguardo all'adozione del cloud: la sicurezza.

Negli ultimi 12 anni, il Cloud Industry Forum ha redatto un report annuale che esamina il modo in cui le aziende utilizzano il cloud e le barriere alla sua adozione. "Ogni report, senza eccezioni, ha identificato la sicurezza come l'ostacolo e la causa di preoccupazione principale per le aziende che desiderano adottare la tecnologia cloud" afferma il Chief Executive Alex Hilton.

Analogamente, da uno studio recente condotto dalla società di consulenza sul cloud Contino è emerso che quasi la metà delle imprese (il 48%) è restia a migrare al cloud per via di preoccupazioni legate alla sicurezza. Michael Chalmers, Managing Director di Contino per Europa, Medio Oriente e Africa, ritiene che il problema non risieda tanto nel fatto che il cloud sia sicuro o meno, ma piuttosto nella differenza tra i modelli di sicurezza tradizionali e il nuovo mondo del cloud.

"In passato, l'attenzione era posta sulla difesa del perimetro del sistema e si presumeva che tutto ciò che si trovasse al suo interno fosse affidabile. Questo approccio non risulta però efficace perché offre agli hacker troppa libertà dopo che sono riusciti a violare un sistema. Di conseguenza, le violazioni e gli attacchi sono diventati molto più frequenti e seri", aggiunge.

Un guscio duro che racchiude un cuore tenero?

Il problema sta nel fatto che il cloud è un sistema distribuito, in cui utenti diversi accedono ad applicazioni e sistemi diversi da varie postazioni. Questo costringe ad adottare un approccio Defense in Depth alla pianificazione, che richiede una sicurezza stratificata per ciascun componente dell'architettura, non semplicemente un guscio duro che racchiude un cuore tenero.

Di conseguenza, si è venuto a creare un modello Zero Trust per cui nessun utente o sistema, sia all'interno che all'esterno del cloud, è considerato affidabile finché non viene verificato.

"Un esempio è dato dal principio dell'accesso meno privilegiato", aggiunge Chalmers. "Ciò significa che ciascun utente ha accesso solo ai sistemi di cui ha bisogno per svolgere il proprio lavoro. In questo modo si limita la portata dei possibili danni causati da un utente malintenzionato o da un criminale informatico qualora dovesse ottenere l'accesso a quell'account. La verifica degli utenti si svolge attraverso tecnologie come l'autenticazione a fattori multipli , la gestione dell'identità e dell'accesso, la crittografia e i sistemi di permessi.

Gartner afferma infatti che anche le aziende più restie dovrebbero mettere da parte le proprie preoccupazioni, puntando su tecnologie come SASE (Secure Access Service Edge), che offre una serie di servizi erogati su cloud, tra cui accesso alle reti Zero Trust e SD-WAN (Software-defined Wide Area Network) con supporto all'accesso protetto per filiali e lavoratori da remoto.

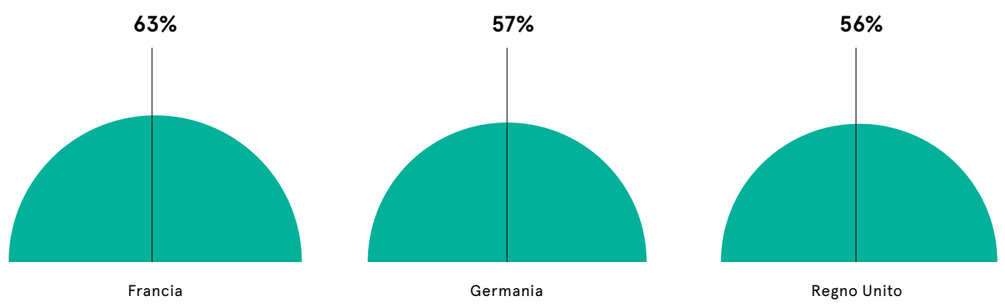
Fiducia e giurisdizione?

Una preoccupazione comune in Europa deriva dalla percezione che, con l'archiviazione nel cloud, i dati vadano a finire nelle mani di entità non europee, spesso presumendo erroneamente che questo sia meno affidabile e possa generare degli ostacoli in fatto di compliance.

Jim Reavis, Chief Executive della Cloud Security Alliance, sostiene tuttavia che il coronavirus ha perturbato la visione tradizionale del mondo definito da confini nazionali, poiché le aziende sono state costrette a re-inventare rapidamente la loro struttura in termini virtuali data l'esigenza dei dipendenti di lavorare da casa.

"Per sostenere questo mondo virtuale si assiste a un'implementazione massiccia di framework di sicurezza nel cloud, come SASE e Software Defined Perimeter", aggiunge. "Gli elementi chiave per rendere questi framework operativi e affidabili sono rappresentati da dipendenza sulle identità comprovate, autenticazione, crittografia robusta e key management con Root of Trust verificate. Poiché questi elementi vengono vagliati, i principali stakeholder convengono che la sicurezza tramite cloud sia superiore e più pratica rispetto ai controlli fisici".

AZIENDE CHE HANNO APPORTATO MODIFICHE IMPORTANTI ALLA GOVERNANCE DEL CLOUD DOPO L'INTRODUZIONE DEL GDPR IN BASE AL PAESE



Thales Group e Ponemon Institute 2019

GUARDANDO AVANTI

SASE potenzia ’azienda

SASE, che fa convergere nel cloud le soluzioni esistenti per la sicurezza e la protezione dei dati, ha tutto il potenziale per essere ampiamente adottato, rimpiazzando le precedenti misure di sicurezza ormai obsolete

Nick Ismail

Gartner, che ha coniato l’acronimo SASE nel 2019, ritiene che il 40% delle aziende adotterà questa strategia aziendale entro il 2024, da meno dell’1% alla fine del 2018.

Sei anni sembrano un’eternità in ambito tecnologico, ma Paul Rumsey, Operations Director presso VIVIDA, ritiene che SASE, sebbene sia ancora gli albori, rappresenti il passo successivo più logico per la sicurezza. “Nel giro di cinque anni mi aspetto che diventerà uno standard del settore per le aziende, soprattutto con l’enorme aumento dello smart working a causa del coronavirus, una politica che secondo me molte aziende adotteranno nel lungo termine”, aggiunge.

Con la diffusione sempre maggiore del framework SASE, le aziende dovranno trovare un modo per analizzare tutti i dati creati da questo set di tecnologie. In realtà, la responsabilità dovrebbe ricadere sul fornitore o sul proprietario della piattaforma. I fornitori SASE saranno meglio attrezzati per raccogliere tutti i dati telemetrici provenienti dall’utente finale, la sua posizione e il suo dispositivo, per creare delle dashboard pensate per il Chief Information Security Officer nell’ambito dell’offerta di sicurezza nel cloud.

“Oltre alla necessità di prestare attenzione ai problemi di riservatezza, è possibile comunque mantenere privati questi dati e al contempo utilizzarli per aumentare in modo esponenziale la sicurezza e ridurre l’attrito con l’utente. Inoltre, la valutazione di quando, dove e come gli utenti interagiscono con le applicazioni e le funzionalità può generare una vasta mole di informazioni utili per migliorare la user experience”, afferma Charles Eagan, Chief Technology Officer presso BlackBerry,

Zero trust

L’approccio Zero Trust, un componente chiave del framework SASE, mette al primo posto i dati e offre un’autorizzazione continua per qualsiasi tipo di accesso remoto, ricollegando la capacità di rischio dell’utente con le risorse a cui può accedere.

L’analisi comportamentale sarà essenziale per il successo del modello Zero Trust, fornendo profili di rischio degli utenti e punteggi aggiornati in tempo reale. “Ciò aiuterà le aziende a regolare il livello di accesso assegnato a una persona in base a quanto è rischioso il suo comportamento” afferma Rumsey. Così facendo, le aziende potranno adottare un approccio alla sicurezza basato sul rischio.

IL 54%

delle aziende dà la priorità a iniziative per migliorare la visibilità e la sicurezza per il lavoro da casa e l’infrastruttura cloud

Accelerate Technologies 2020

> **SASE risolverà un problema di attrito che si riscontra da tempo tra l’utente e i requisiti di sicurezza complicati**

Questo atteggiamento proattivo alla sicurezza influirà anche sull’abilità delle aziende di valutare il livello di rischio di ciascun individuo in base al comportamento. L’autenticazione continua abilitata dall’approccio Zero Trust, nell’ambito del framework SASE, faciliterà il modo in cui le aziende determinano automaticamente l’accesso di un utente finale.

Eagan aggiunge poi: “L’agilità è un beneficio importante dell’autenticazione continua poiché, anche dopo aver superato l’evento di autenticazione, sarà comunque possibile prendere una decisione di sicurezza e automatizzare il ripristino immediato. Nella maggior parte dei casi, ciò consente di prevenire, o perlomeno, di mitigare i danni”.

Ridurre l’attrito

Le aziende stanno ora iniziando a riconoscere i benefici di un approccio SASE o Zero Trust alla sicurezza.

Con la progressiva penetrazione del framework attraverso tutti i sistemi, si avrà un vantaggio evidente per i dipendenti e, nel lungo periodo, per i clienti. Riferendosi ai limiti di sicurezza attuali delle banche che cercano di rilevare e prevenire le frodi, Eagan afferma che con SASE e l’autenticazione continua sarà possibile “identificare prontamente gli utilizzi fraudolenti, anche se le credenziali sono state compromesse e usate da un altro dispositivo”.

Questa convergenza di soluzioni esistenti per la sicurezza e la protezione dei dati nel cloud ha le potenzialità per rivoluzionare il concetto stesso di sicurezza e risolverà un problema di attrito che si riscontra da tempo tra l’utente e i requisiti di sicurezza complicati, causando spesso frustrazioni tra i dipendenti e un numero maggiore di incidenti.

“Rendendo questa relazione più armoniosa, ci auguriamo di riscontrare una diminuzione del numero di incidenti legati alla sicurezza causati da errore umano”, conclude Rumsey.

RACONTEUR

Forcepoint