Enterprise Strategy Group | Getting to the bigger truth.™

REPORT ESG RESEARCH INSIGHTS

Valutazione dei benefici tangibili del SASE

Identificazione delle aree in cui le aziende che scelgono un approccio convergente migliorano i risultati d'impresa e la sicurezza

Di John Grady, ESG Senior Analyst
Adam DeMattia, Director of Research

Marzo 2021

Questo white paper di ESG è stato commissionato da Forcepoint e viene distribuito su licenza da ESG.

Sommario

Prefazione

Il concetto di SASE (Secure Access Service Edge) è comparso da poco sul mercato, eppure ha immediatamente riscosso un enorme interesse e risvegliato la curiosità degli utenti. Tutta questa attenzione non dovrebbe sorprendere, considerati i cambiamenti profondi apportati dal cloud e dalla mobilità nel mondo imprenditoriale dell'ultimo decennio a fronte di un'innovazione relativamente modesta delle tecnologie per la sicurezza di rete.

La pandemia, inoltre, ha costretto le imprese a prendere atto della realtà: i modelli di sicurezza informatica in uso da decenni non sono più adeguati in un mondo altamente distribuito. E questa realizzazione non ha fatto che attirare ancor più l'attenzione sul SASE.

La pandemia ha costretto le imprese a prendere atto della realtà: i modelli di sicurezza informatica in uso da decenni non sono più adeguati in un mondo altamente distribuito. E questa realizzazione non ha fatto che attirare ancor più l'attenzione sul SASE.

Se, da un lato, i potenziali vantaggi di un modello SASE (migliore sicurezza, migliore esperienza per gli utenti e maggiore efficienza operativa) per le aziende sono chiari, il fatto che il mercato rimanga a uno stadio iniziale lascia una carenza di informazioni sui benefici reali sperimentati dalle aziende che hanno adottato il SASE. Per fare chiarezza sull'impatto che la maturità dell'approccio al SASE ha sugli obiettivi imprenditoriali e di sicurezza di un'azienda, Forcepoint ha commissionato uno studio di ricerca all'Enterprise Strategy Group (ESG). I punti chiave messi in luce dallo studio includono i seguenti:

- Le aziende con un approccio SASE maturo sono meglio preparate a supportare una forza lavoro distribuita. Grazie all'agilità e alla flessibilità rese possibili da soluzioni distribuite nel cloud, insieme all'adozione di strategie Zero Trust, le aziende mature nutrono molta più fiducia nelle loro capacità di proteggere gli utenti remoti.
- Le aziende SASE mature stanno espandendo le loro funzionalità di sicurezza e, allo stesso tempo, riducendo il numero di fornitori a cui si affidano. Relazioni più strategiche e solide con un numero inferiore di fornitori e una migliore qualificazione anticipata delle soluzioni consentono alle aziende più mature di utilizzare gli strumenti di sicurezza con maggiore efficienza.
- Il SASE riduce gli attriti associati all'adozione di servizi cloud nei reparti commerciali. La visibilità coerente offerta dal modello SASE sulle risorse cloud gestite e non gestite significa che i team di sicurezza possono adottare un approccio più favorevole all'adozione del cloud, in ultima analisi aumentando la soddisfazione degli utenti.
- Il SASE supporta la resilienza aziendale. Grazie al modello SASE, le considerazioni di sicurezza non costituiscono un ostacolo all'adozione di soluzioni cloud e, in questo modo, le aziende possono supportare un maggior numero di applicazioni nel cloud, migliorando agilità e adattabilità in modo da superare gli ostacoli presentati da crisi sociali e macroeconomiche.
- Le aziende che danno priorità al SASE riducono i costi per la sicurezza. La riduzione del numero di fornitori e di strumenti abbassa la spesa sia per le soluzioni che per gli abbonamenti, nonché i costi operativi.

L'ascesa del SASE (Secure Access Service Edge)

La tendenza alla decentralizzazione continua a definire la strategia IT di molte aziende. Oggi più che mai, applicazioni e dati risiedono nel cloud e gli utenti che accedono a tali risorse sono sempre più spesso fuori dagli uffici aziendali.

Eppure, nonostante questi cambiamenti radicali nelle architetture di rete, molte aziende continuano ad affidare la loro sicurezza ai tradizionali approcci perimetrali, spesso basati sul backhaul del traffico dagli utenti remoti allo stack di sicurezza locale, dove viene sottoposto a ispezione. Le problematiche poste da questo approccio sono molteplici:

- Quando gli utenti accedono alle applicazioni cloud in questo modello, il percorso più lungo che il traffico deve seguire per passare attraverso gli strumenti di sicurezza locali può causare latenza e avere un impatto negativo sull'esperienza degli utenti.
- Nel caso delle applicazioni on-premise, il problema non è il backhaul ma l'impiego di soluzioni VPN incentrate sull'hardware, troppo permissive riguardo agli accessi di rete, prive della scalabilità necessaria per adeguarsi ai picchi nella domanda e spesso bersaglio degli hacker a causa della loro visibilità sulla rete Internet pubblica.
- Nell'accesso ad applicazioni locali o su cloud, la prevalenza di soluzioni di terze parti e dispositivi personali dei dipendenti complica ulteriormente la messa in sicurezza sistematica di questa matrice di connettività.

Nella ricerca di ESG, il 64% degli intervistati ha dichiarato che la sicurezza di rete lungo il perimetro è più complessa rispetto a due anni fa.

Anche in seguito a queste difficoltà, per molte aziende la sicurezza informatica è diventata più difficile e meno efficace. Specificamente, il 64% degli intervistati per la ricerca ESG ha dichiarato che la sicurezza di rete lungo il perimetro è più complessa rispetto a due anni fa.[1]

Per affrontare meglio queste dinamiche in evoluzione, è emersa una nuova architettura detta SASE (Secure Access Service Edge), nella quale più controlli di sicurezza convergono in un modello implementato nel cloud, con gestione centrale e applicazione distribuita. Non esiste un elenco definito di strumenti che devono essere inclusi nel SASE, ma molte aziende hanno optato per funzionalità SWG (Secure Web Gateway), CASB (Cloud Access Security Broker), ZTNA (Zero Trust Network Access), DLP (Data Loss Prevention) e FWaaS (Firewall-as-a-Service). Se all'inizio il SASE era prevalentemente utilizzato per filiali e uffici distaccati, la diffusione del lavoro da remoto forzata dalla pandemia ha messo in evidenza la necessità fondamentale di proteggere sistematicamente gli accessi a prescindere dalla posizione dell'utenza.

Maturità SASE: identificazione delle fasi

Per meglio comprendere i vantaggi di cui godono le aziende che hanno adottato architetture SASE, Forcepoint ha affidato a ESG l'incarico di condurre uno studio su 400 professionisti del settore IT e della sicurezza informatica. In base alle risposte a cinque domande fondamentali[2] sulle tecnologie, i controlli e i processi adottati per la sicurezza di rete, le aziende che hanno partecipato allo studio sono state suddivise in tre coorti in base al loro livello di maturità SASE:

[1] Fonte: ESG Master Survey Results, *Transitioning Network Security Controls to the Cloud*, luglio 2020.
[2] Maggiori informazioni sono disponibili nell'Appendice II: Domande del sondaggio utilizzate da ESG per valutare la maturità SASE.

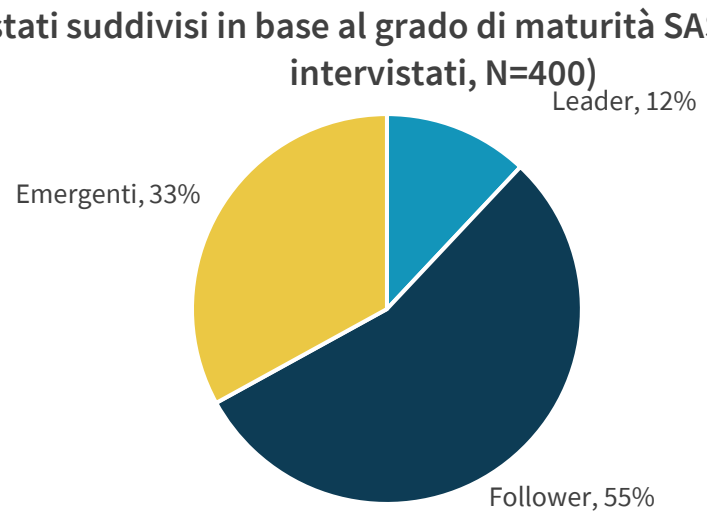
1. **Emergenti:** le aziende nella coorte "Emergenti" presentano da zero a due caratteristiche di maturità SASE. Queste aziende tendono ad avere un approccio più reattivo alla sicurezza in quanto non sempre incorporano le funzionalità di sicurezza e monitoraggio durante il processo di progettazione della rete. È improbabile che abbiano adottato strategie Zero Trust o che riducano attivamente il numero dei fornitori di soluzioni di sicurezza; è inoltre possibile che utilizzino un minor numero di controlli di sicurezza perimetrale.

2. **Follower:** i partecipanti classificati nella categoria "Follower" presentano da tre a quattro caratteristiche di maturità SASE. Queste aziende tengono ad avvalersi di svariati strumenti per i quali mostrano di avere un certo livello di integrazione e visibilità. Possono, tuttavia, essere indietro riguardo all'adozione di strategie Zero Trust, alla riduzione del numero di fornitori o alla progettazione proattiva della rete e della sicurezza.

3. **Leader:** le aziende identificate come "Leader" presentano tutte e cinque le caratteristiche di maturità SASE. Integrano sempre i controlli di sicurezza nella progettazione della rete, hanno implementato modelli Zero Trust, usano un ampio set di controlli di sicurezza di rete riducendo allo stesso tempo il numero di fornitori, hanno definito un sistema fortemente integrato di controlli perimetrali, sui quali hanno ampia visibilità.

Non sorprende che solo poche aziende abbiano raggiunto il terzo stadio di maturità SASE conquistandosi a buon diritto una posizione tra i Leader (v. Figura 1). I Leader identificati come tali possono utilizzare questo report internamente per confermare i vantaggi attesi in base ai benefici ottenuti dalle altre aziende che hanno adottato architetture SASE. La maggioranza (il 55%) degli intervistati rientra nella categoria dei Follower. Si tratta di aziende che possono contare su una solida base di partenza per evolvere verso un approccio SASE più maturo e che possono avvalersi dei dati del report per colmare le lacune che le separano dal gruppo dei Leader. La categoria Emergenti conta un terzo delle aziende partecipanti. Sebbene queste abbiano ancora del lavoro da fare riguardo al SASE, già capire i vantaggi dell'approccio e conoscere le best practice adottate dai Leader offre loro un vantaggio in quanto mostra le aree cui dare priorità per implementare un modello SASE nel tempo.

Figura 1. Distribuzione degli stadi di maturità SASE



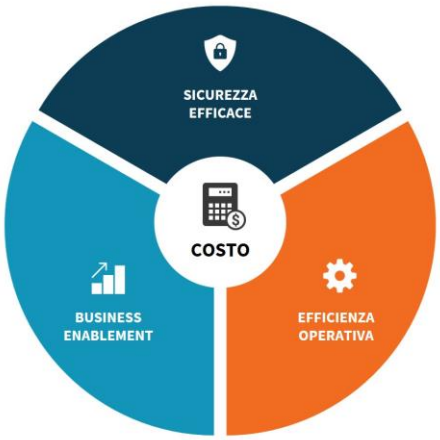
Fonte: Enterprise Strategy Group

Il valore del modello SASE

Le attribuzioni dei team responsabili della sicurezza informatica si sono evolute nel tempo. In passato i responsabili della sicurezza avevano la facoltà di imporre controlli rigidi e inflessibili. L'impatto sugli utenti non era considerato una priorità e la natura centralizzata dell'IT garantiva al team responsabile della sicurezza tutta la visibilità necessaria per svolgere il proprio ruolo senza ostacolare l'attività aziendale. Ma la diffusione crescente della tecnologia nei reparti aziendali non tecnici, accelerata dal modello self-service del cloud, ha obbligato i team di sicurezza a garantire che le misure di controllo attuate non limitassero le innovazioni necessarie alle funzioni amministrative e commerciali e non compromettessero l'esperienza o la produttività degli utenti.

Allo stesso tempo, nonostante la priorità riconosciuta in molte aziende alla spesa per il settore della sicurezza informatica, i vincoli finanziari restano reali. Diciamolo chiaramente: una strategia di sicurezza efficace, efficiente sotto il profilo operativo e funzionale agli obiettivi aziendali, che sia anche realizzabile con un investimento limitato, può comportare notevoli difficoltà (v. Figura 2). Eppure la nostra ricerca dimostra che le aziende che hanno raggiunto la maturità SASE sono in grado di ottenere risultati positivi in tutte queste aree.

Figura 2. I team di sicurezza informatica devono produrre risultati funzionali sia per la sicurezza sia per il business



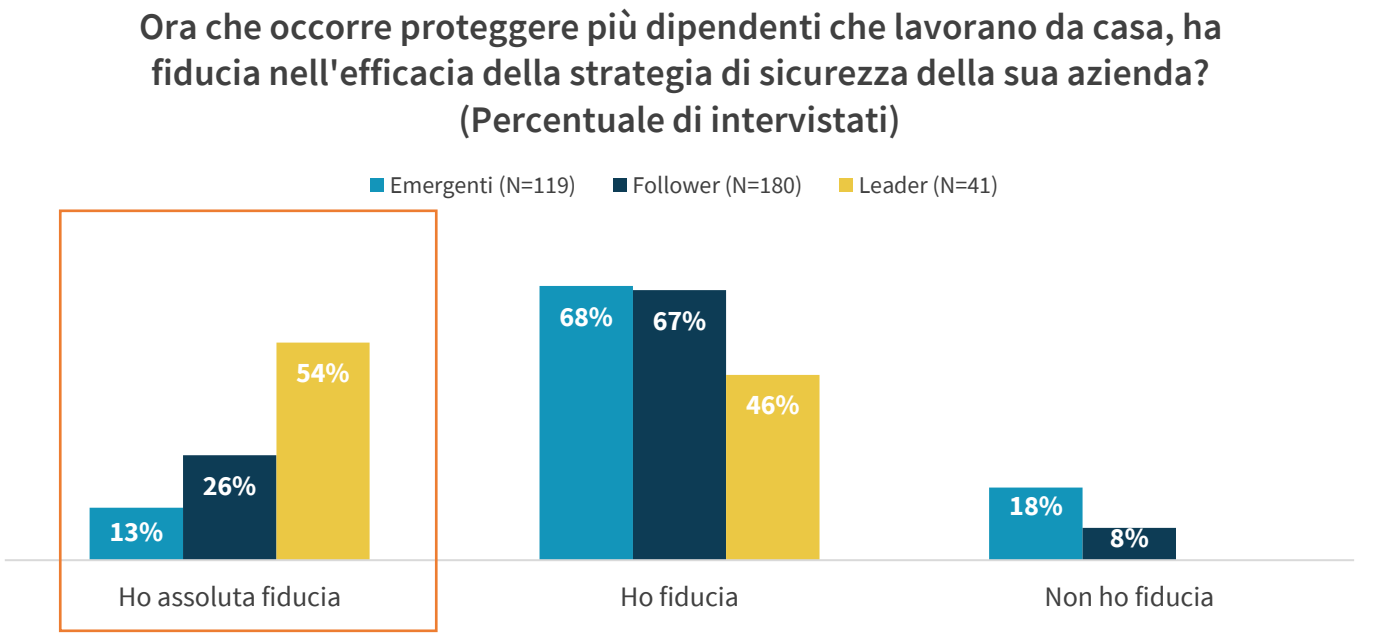
Fonte: Enterprise Strategy Group

Sicurezza efficace

Il SASE migliora l'efficacia della sicurezza negli ambienti distribuiti.

Come già detto, un fattore trainante essenziale del SASE è stato il bisogno di migliorare l'architettura della sicurezza per rispondere al paradigma dell'accesso invertito: utenti e applicazioni sono oramai più spesso all'esterno che all'interno di uffici e data center aziendali. La pandemia ha semplicemente esacerbato una tendenza già in atto: gli intervistati hanno dichiarato che la percentuale dei dipendenti che lavorano da remoto è passata dal 20% del periodo pre-COVID all'attuale 53%. Le aziende Leader si sono mostrate più propense a caratterizzare come "estremamente fluidi" gli sforzi per direzionare la sicurezza verso gli utenti remoti (39% rispetto all'8% delle aziende Emergenti). Ancora più importante dell'attrito (o assenza di attrito) nella protezione degli utenti remoti è l'efficacia dell'approccio. Anche in questo ambito i Leader hanno ottenuto risultati nettamente migliori rispetto alla controparte degli Emergenti, dichiarandosi con una probabilità di 4,2 volte maggiore molto fiduciosi nella loro capacità di proteggere i dipendenti che lavorano da casa (v. Figura 3).

Figura 3. La fiducia nelle capacità di proteggere una forza lavoro distribuita aumenta con la maturità SASE



Fonte: Enterprise Strategy Group

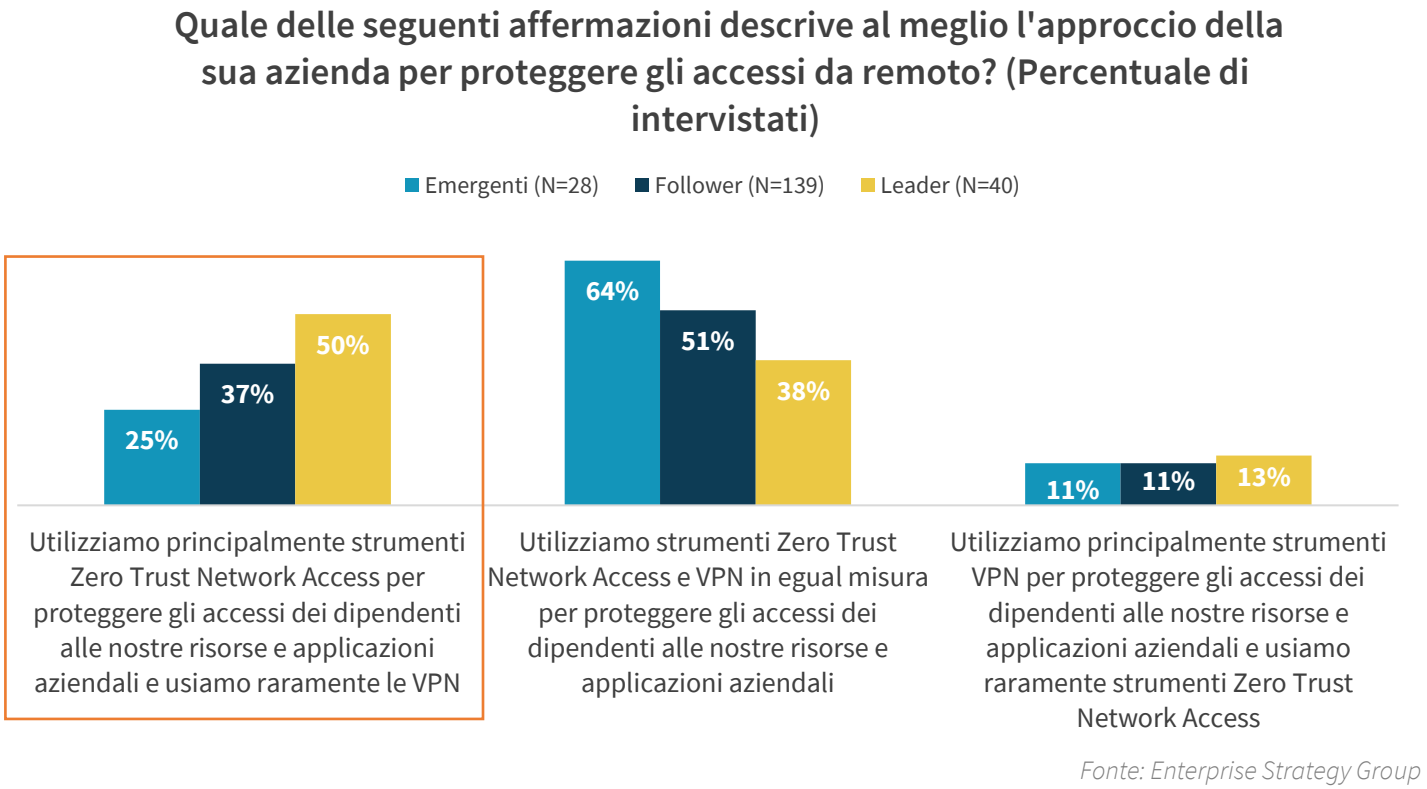
Perché questo aspetto assume importanza in questa fase della pandemia? In parole semplici, lo scenario del lavoro agile, che fino a un anno fa era sconosciuto ai più, oramai è destinato a restare. Se da un lato gli intervistati ritengono che il numero dei lavoratori da remoto sia destinato a calare con la fine della pandemia, dall'altro prevedono che si attesterà comunque sull'80% in più rispetto all'era pre-COVID. L'emergere di questa tipologia di lavoro ibrida significa che le aziende devono adottare un punto di vista più lungimirante riguardo alla protezione della forza lavoro distribuita ed evitare soluzioni estemporanee che nel tempo potrebbero finire per aumentare la complessità.

Partendo da questi presupposti, quali sono gli elementi per cui le aziende SASE mature sono meglio posizionate per supportare questo modello? Sebbene vi siano diversi motivi che giustificano il maggiore successo di tali aziende, un elemento che emerge su tutti è la prioritizzazione e l'adozione precoce degli strumenti di accesso alla rete Zero Trust come componente cruciale del SASE. Il modello Zero Trust si caratterizza per il fatto che ignora la posizione e considera ogni possibile contesto quando valuta l'affidabilità di chi accede alle risorse aziendali. Nato originariamente per le reti tradizionali, questo approccio è ideale per gli ambienti in cui utenti, dispositivi e applicazioni sono disseminati tra varie reti pubbliche e private.

Quasi tre quarti (il 73%) dei Leader hanno piani definiti per ridurre sensibilmente o eliminare del tutto le VPN per gli accessi da remoto, rispetto a un esiguo 30% delle aziende Emergenti.

Secondo i nostri risultati, i Leader hanno già completato una parte significativa della transizione da VPN a ZTNA e sono pertanto meglio posizionati per offrire un accesso sicuro e continuo a una forza lavoro remota (v. Figura 4). Questo passaggio andrà senz'altro avanto, dato che quasi tre quarti (il 73%) dei Leader hanno piani definiti per ridurre sensibilmente o eliminare del tutto le VPN per gli accessi da remoto, rispetto a un esiguo 30% delle aziende Emergenti. Il fatto che molte delle aziende che impiegano già una soluzione ZTNA abbiano in programma di proseguire la dismissione delle VPN dovrebbe servire da chiara conferma della validità di queste soluzioni.

Figura 4. Le aziende Leader hanno prioritizzato le soluzioni Zero Trust Network Access



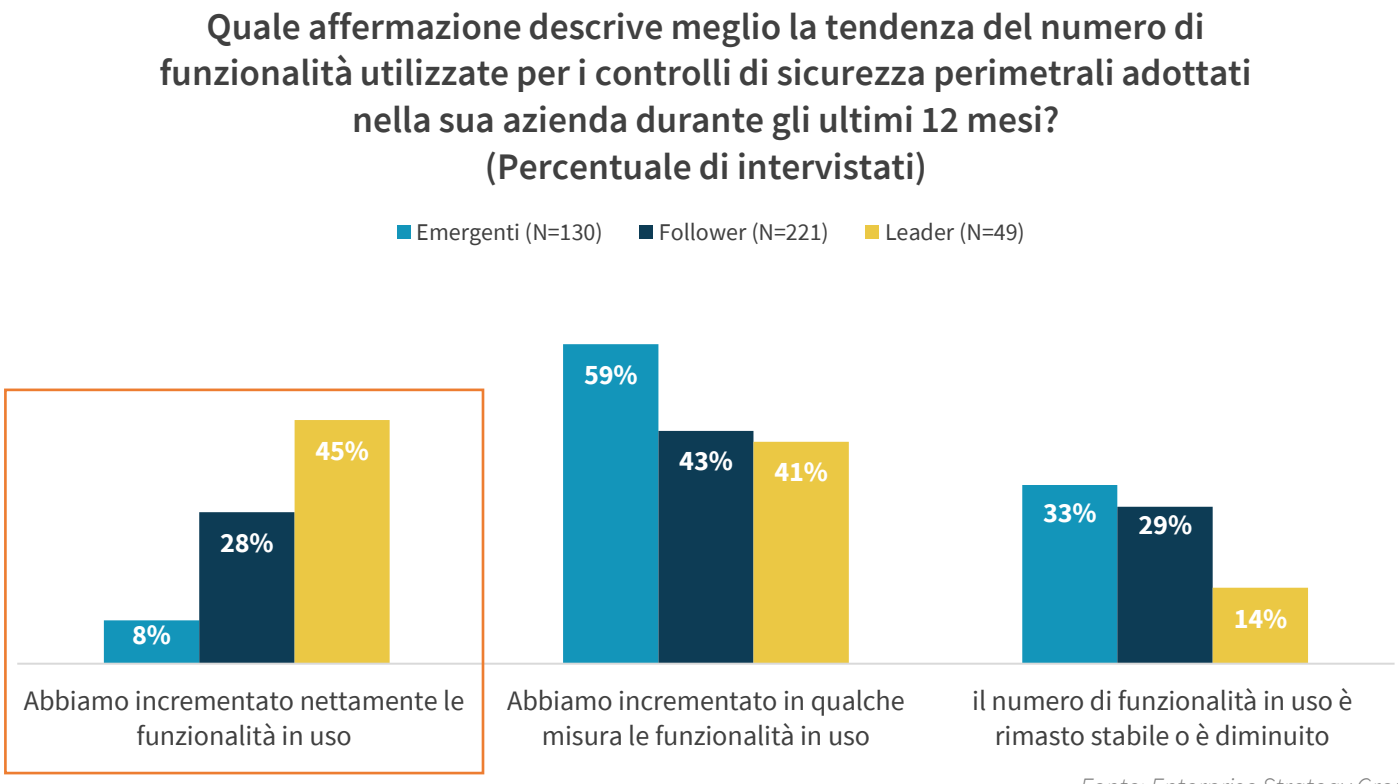
Fonte: Enterprise Strategy Group

Efficienza operativa

Il SASE incoraggia l'impiego di funzionalità di sicurezza ampliate.

Un aspetto essenziale del SASE è la riduzione del numero dei fornitori e lo snellimento dell'infrastruttura di sicurezza perimetrale tramite un approccio convergente. Un minor numero di fornitori comporta svariati vantaggi per l'ambiente di rete, ad esempio migliore efficienza, maggiore semplicità e una gestione più coerente. Questa riduzione, in ogni caso, non richiede sacrifici sul versante della funzionalità. Di fatto, le aziende Leader dichiarano di avere incrementato nettamente capacità e funzionalità in uso sul perimetro di rete, con una frequenza 5,6 volte maggiore rispetto alle aziende Emergenti (v. Figura 5).

Figura 5. Le aziende SASE mature sono in grado di sfruttare più funzionalità della soluzione

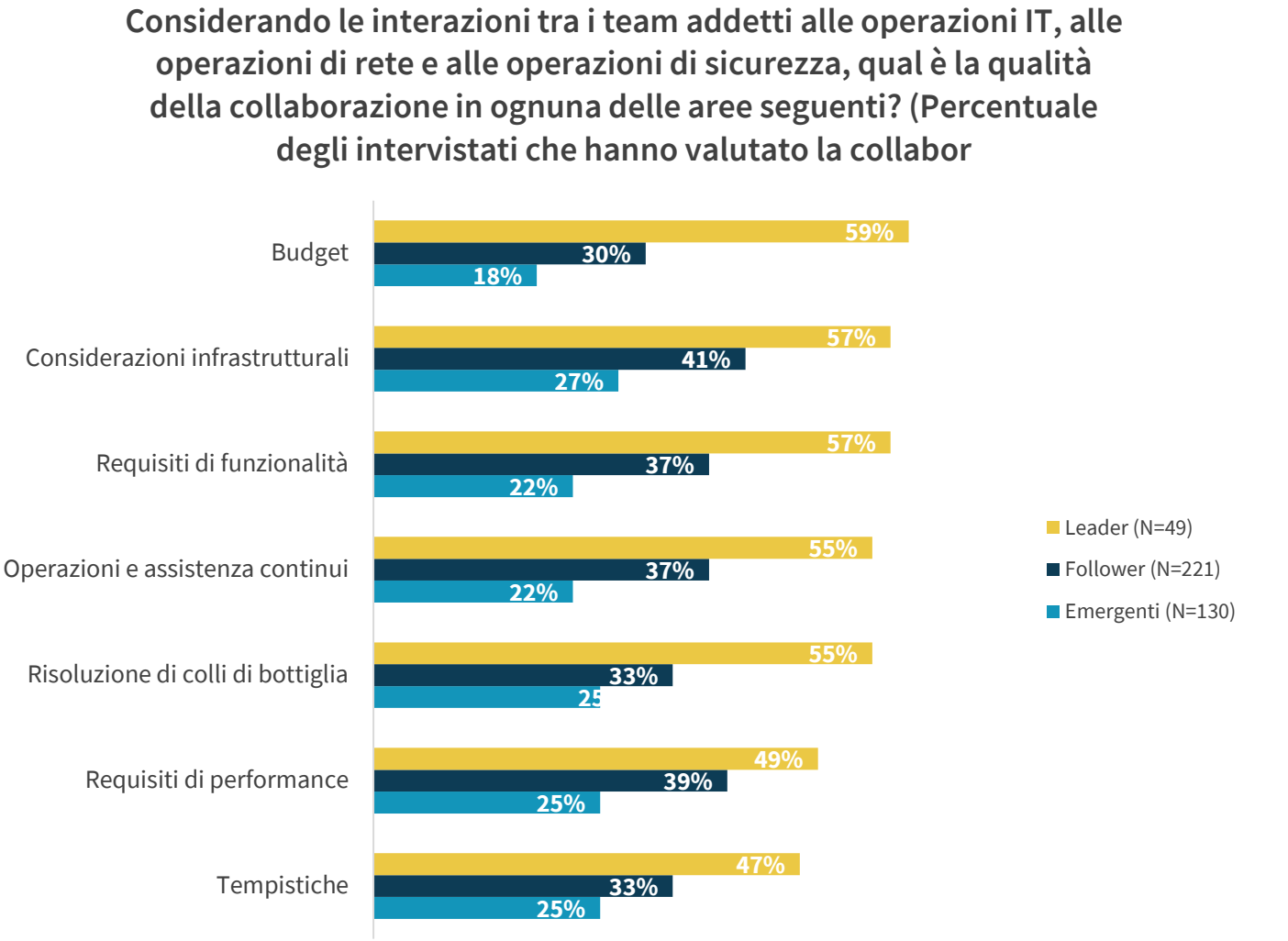


Fonte: Enterprise Strategy Group

Le aziende SASE mature riferiscono una collaborazione sensibilmente migliore fra tutti i gruppi coinvolti nelle attività di gestione, distribuzione e procurement della sicurezza perimetrale.

Le dinamiche aziendali svolgono un ruolo fondamentale per il conseguimento di questo risultato. Il procurement, la distribuzione e la gestione degli strumenti di sicurezza sono un gioco di squadra che richiede la collaborazione tra una varietà di gruppi, che includono le operazioni IT, di sicurezza e di rete. Tradizionalmente, i reparti IT hanno un'influenza enorme sulla scelta e sull'acquisto degli strumenti di sicurezza. Sta però aumentando il peso dei reparti responsabili della rete e della sicurezza, i cui specialisti guadagnano influenza e intendono assicurarsi che gli strumenti selezionati rispondano meglio alle loro specifiche esigenze. La combinazione tra meno venditori e una migliore qualificazione preventiva delle soluzioni assicura che le capacità funzionali dei prodotti adottati siano sfruttate fino in fondo e che le aziende non si ritrovino con software destinato a restare inutilizzato. Considerate tali premesse, non sorprende che le aziende Leader indichino una collaborazione sensibilmente migliore tra tutti i vari gruppi coinvolti nelle operazioni di procurement, distribuzione e gestione delle soluzioni di sicurezza perimetrali (v. Figura 6).

Figura 6. Una solida collaborazione interfunzionale è cruciale per il successo del SASE



Fonte: Enterprise Strategy Group

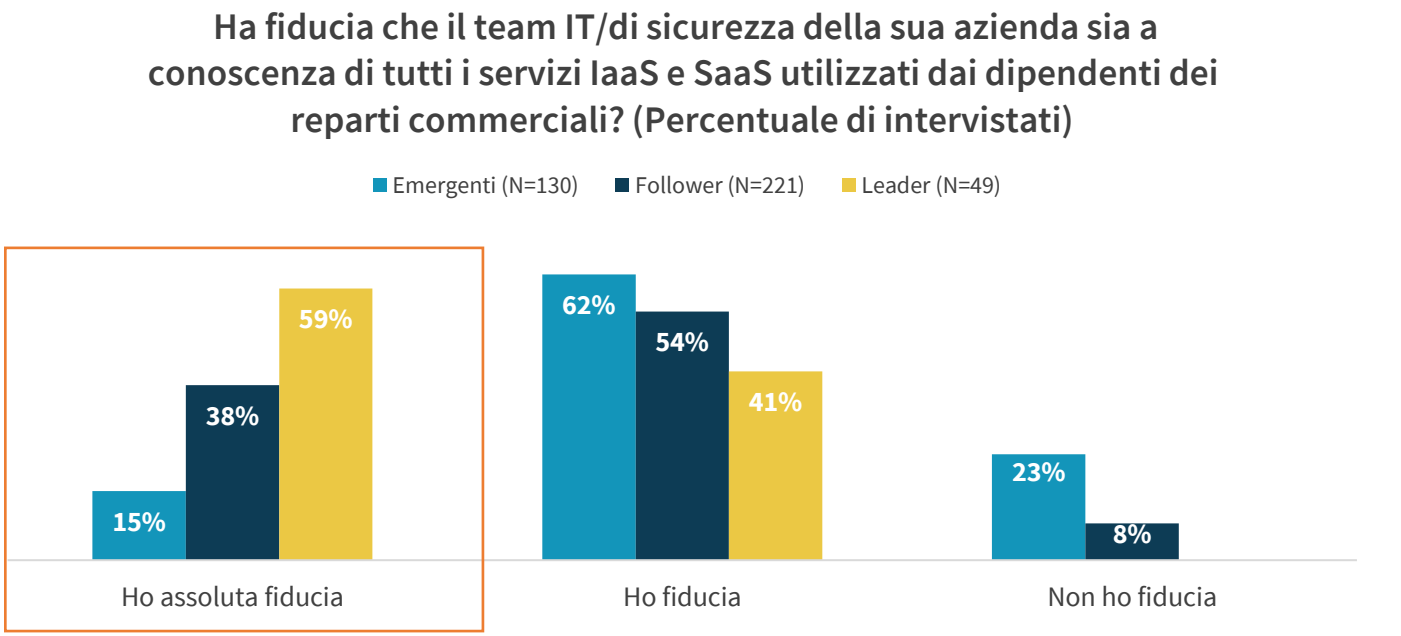
Business Enablement

Il SASE offre una visibilità multi-cloud uniforme.

La convergenza di strumenti prima isolati, la riduzione del numero di fornitori e l'utilizzo più efficace delle funzionalità dei prodotti concorrono anche a migliorare la visibilità sull'uso dei servizi cloud. La maggior parte delle aziende ha risorse disseminate tra una moltitudine di fornitori SaaS e IaaS. CASB, ZTNA e anche strumenti VPN tradizionali possono tutti, in maggiore o minore misura, supportare l'accesso a queste applicazioni. La gestione della visibilità su tutti questi strumenti eterogenei è un'impresa faticosa quanto vana.

E questo vale ancora di più nel modello IT decentralizzato descritto prima. Il team responsabile della sicurezza spesso rimane all'oscuro dei servizi cloud utilizzati dai reparti commerciali. Una visibilità granulare sull'utilizzo del cloud può garantire che i team di sicurezza siano a conoscenza delle risorse cloud usate, possano assegnare la priorità alla protezione delle risorse business-critical o che contengono dati aziendali sensibili e, in generale, restino aggiornati sulle modalità operative dei reparti commerciali. Secondo la nostra ricerca, la probabilità che le aziende Leader si dichiarino molto fiduciose della loro visibilità sul cloud è di 3,9 volte maggiore rispetto a quelle Emergenti (v. Figura 7).

Figura 7. Il SASE aiuta a ridurre le lacune di visibilità sul cloud



Fonte: Enterprise Strategy Group

Un aspetto critico di questa visibilità è la protezione dei dati e specificamente la DLP. Mentre utenti, dispositivi e applicazioni sono tutti fattori importanti nel controllo degli accessi, in ultima analisi sono la tipologia e la sensibilità dei dati in uso a fare la differenza. E questo è reso ancora più complicato dal fatto che spesso set di strumenti diversi offrono visibilità su parti diverse dell'infrastruttura a supporto della DLP. CASB, endpoint, rete e strumenti Secure Web Gateway possono avere tutti un certo livello di funzionalità DLP. Le aziende Leader lo sanno e infatti sono 3 volte più propense a utilizzare almeno 4 strumenti con funzionalità DLP rispetto alla categoria Emergenti. In ogni caso, come abbiamo visto, queste aziende stanno riducendo attivamente il numero di fornitori nei loro ambienti e riescono a integrare meglio la visibilità su tutti questi controlli in modo da garantire uniformità e ridurre i punti ciechi. Rispetto alla prevenzione della perdita dei dati, questo aspetto è critico per garantire che la policy aziendale sia applicata correttamente, a prescindere da dove risiedono i dati o da dove si trovi l'utente quando vi accede.

Il SASE promuove la resilienza aziendale.

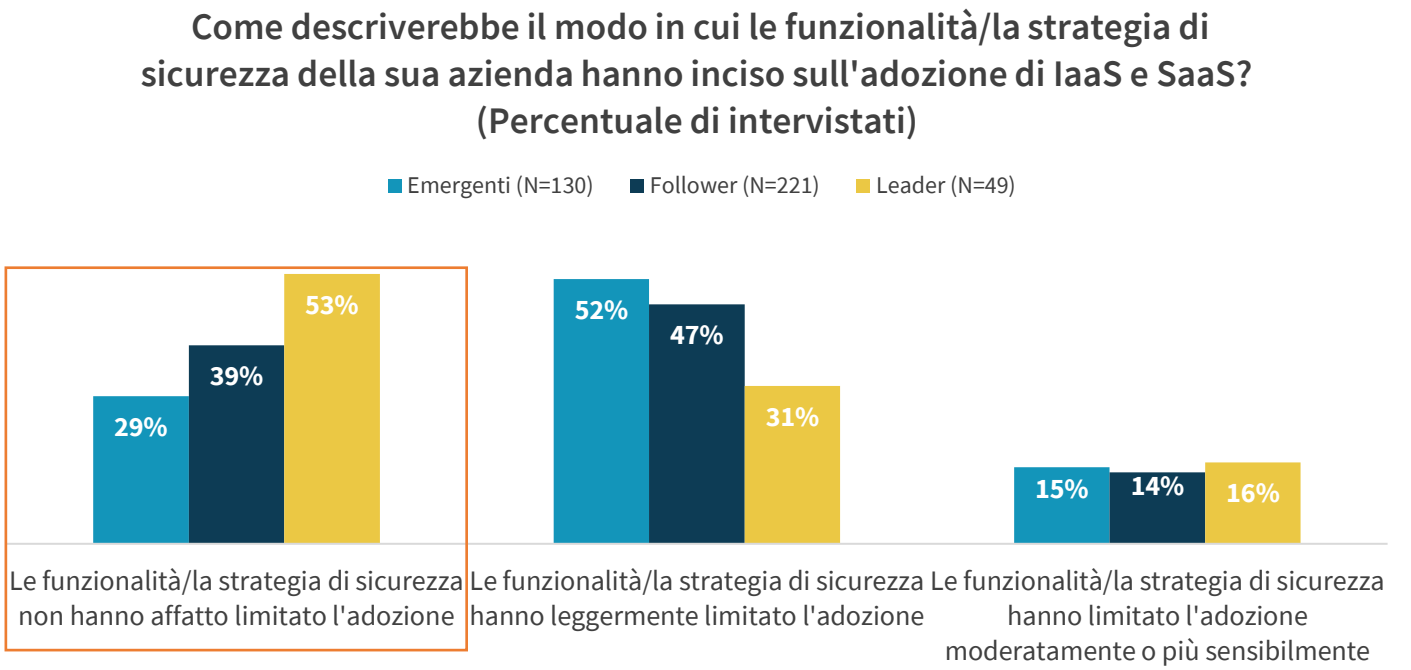
Come già detto, la sicurezza informatica non va considerata soltanto dal punto di vista della protezione, ma anche sotto il profilo dell'enablement: l'azienda deve essere messa in condizione di operare. Il SASE rappresenta l'evoluzione della sicurezza per le risorse di rete, per affrontare meglio la realtà degli ambienti dell'impresa moderna. Questo significa andare oltre le architetture incentrate sui firewall, per considerare approcci che integrano la sicurezza di applicazioni private, SaaS, Web e dati. L'obiettivo deve essere un'esperienza che elimini gli attriti tra responsabili commerciali e sviluppatori, consentendo loro di concentrarsi sulla generazione di profitti e di un'esperienza positiva per i loro clienti.

Grazie al migliore livello di visibilità offerto dal SASE, la maggioranza (53%) delle aziende Leader ha riferito che la sicurezza non limita l'adozione del cloud. Solo il 29% del gruppo Emergenti ha dichiarato lo stesso (v. Figura 8). Più specificamente, i Leader utilizzano una media di 128 applicazioni cloud business-critical, mentre le controparti del gruppo Emergenti arrivano a una media di 81. Ancora più

Le aziende che hanno dato priorità al SASE e ottenuto i vantaggi offerti dall'accelerazione cloud hanno maggiori probabilità (4,4 volte in più) di avere utenti estremamente soddisfatti nei reparti commerciali.

significativo è che le aziende che hanno dato priorità al SASE e ottenuto i vantaggi offerti dall'accelerazione cloud hanno maggiori probabilità (4,4 volte in più) di avere utenti estremamente soddisfatti nei reparti commerciali. Riepilogando: con il modello SASE la sicurezza non costituisce un ostacolo all'adozione di soluzioni cloud, le aziende possono supportare un maggior numero di applicazioni nel cloud e, in ultima analisi, gli utenti sono più soddisfatti.

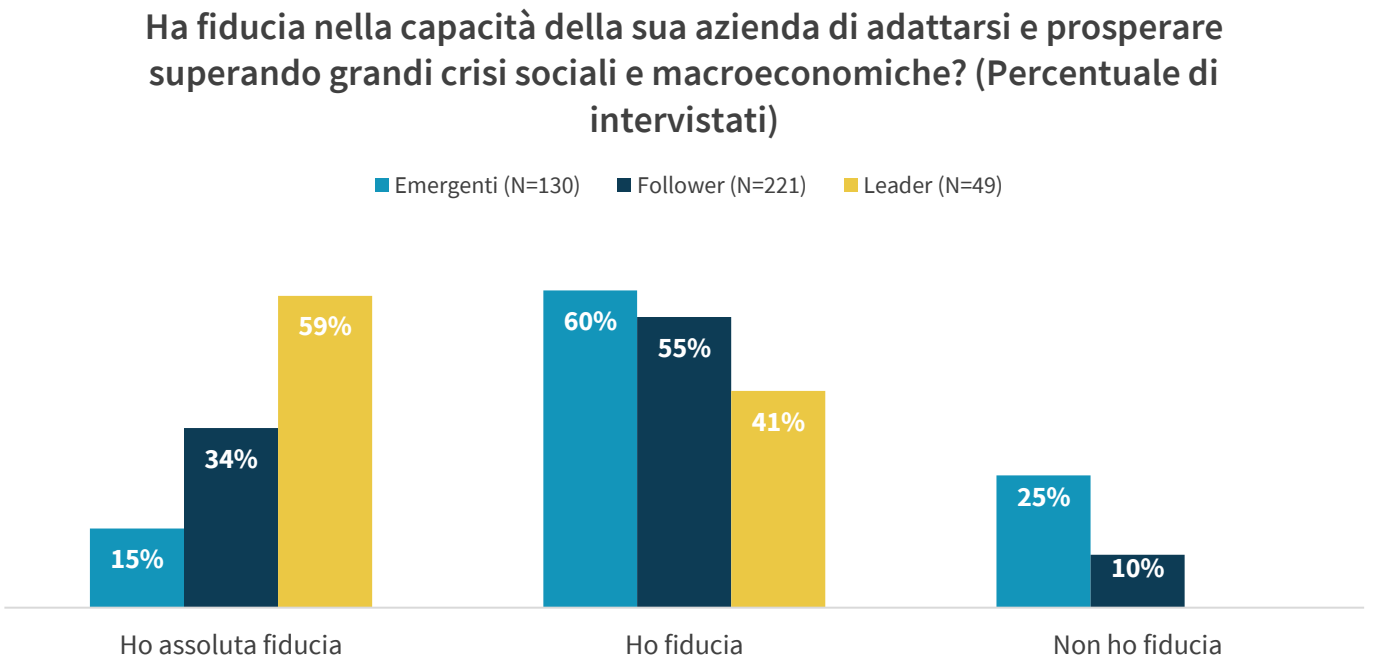
Figura 8. Il SASE riduce gli ostacoli all'adozione di SaaS e IaaS



Fonte: Enterprise Strategy Group

I motivi per il passaggio delle risorse al cloud sono stati identificati chiaramente negli anni e, per molti, il fattore principale è stato la resilienza. La scalabilità e la flessibilità del cloud consentono alle aziende di essere più agili e adattive, caratteristiche che tendono ad assumere più importanza nell'ottica della pandemia. Qual è l'impatto del SASE sulla resilienza? La probabilità che le aziende Leader ripongano una grande fiducia nella loro resilienza è di 3,9 volte maggiore rispetto alle controparti Emergenti (v. Figura 9).

Figura 9. Le aziende SASE mature hanno più fiducia nella loro resilienza



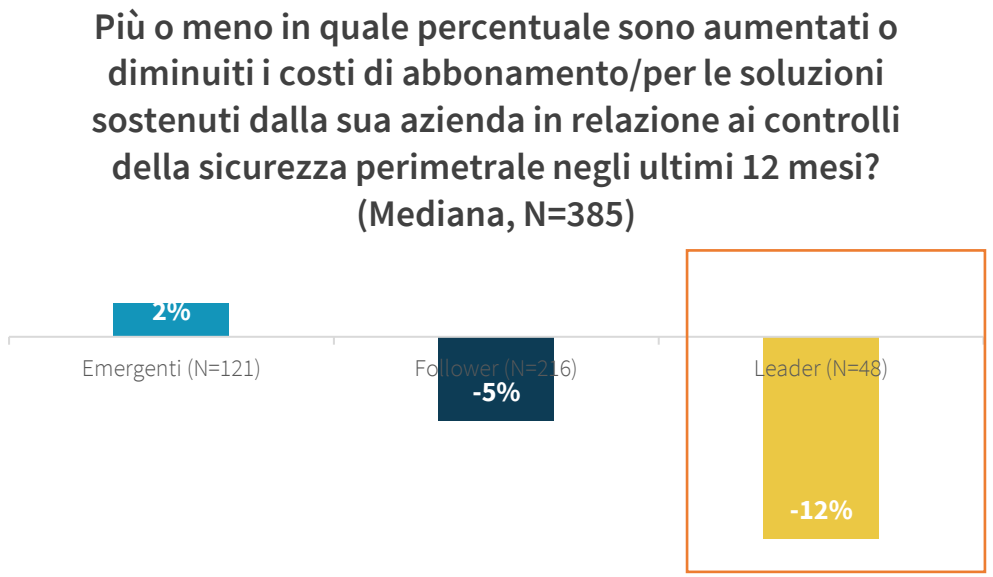
Fonte: Enterprise Strategy Group

Costo

Il SASE aiuta le aziende a tagliare i costi.

Nonostante l'apprezzamento di tutti i vantaggi summenzionati, le aziende con un approccio più maturo al SASE hanno maggiori probabilità di riferire risparmi sui costi sia di abbonamento/per le soluzioni, sia operativi (v. Figura 10). La riduzione del numero di fornitori e lo sviluppo con loro di partnership più strategiche consentono di ottimizzare preventivamente i costi di procurement. Tuttavia, un aspetto forse ancora più importante riguarda il calo dei costi operativi del 14% riferito dalle aziende Leader rispetto all'esiguo 1% del gruppo Emergenti. I vantaggi diretti del SASE, che in ultima analisi conducono a un risparmio sui costi operativi, sono: meno sistemi di gestione che gli amministratori devono imparare a usare, eliminazione di strumenti duplicati di gestione delle policy su sistemi diversi, con conseguente riduzione del rischio di errore umano, nonché maggiore efficacia nell'individuazione delle minacce e nelle capacità di risposta.

Figura 10. Nonostante utilizzino più strumenti e funzionalità, le aziende SASE mature riportano costi inferiori



Fonte: Enterprise Strategy Group

Conclusioni: la grande verità

Come ha mostrato la nostra ricerca, l'attenzione che il modello SASE ha riscosso sul mercato è più che giustificata. Le aziende Leader hanno riferito vantaggi sensibilmente maggiori in tema di sicurezza, operazioni, business e costi rispetto al gruppo delle Emergenti. In particolare:

- La probabilità che i Leader esprimano grande fiducia nella loro capacità di proteggere i dipendenti che lavorano da remoto sono di 4,2 volte maggiori.
- La probabilità che i Leader abbiano nettamente aumentato capacità e funzioni utilizzate sul perimetro di rete è di 5,6 volte maggiore.
- La probabilità che i Leader esprimano grande fiducia nella visibilità dei loro ambienti cloud distribuiti è più alta di 3,9 volte.
- Oltre la metà (53%) dei Leader ha dichiarato che le considerazioni di sicurezza non hanno affatto ostacolato l'adozione di servizi cloud nella loro azienda.
- I Leader riportano una riduzione del 12% nei costi di abbonamento/per le soluzioni e del 14% nei costi operativi.

Una riorganizzazione radicale delle architetture di sicurezza informatica aziendali non è cosa da poco e nessuno dovrebbe affrontarla con leggerezza. Tuttavia, sebbene il modello SASE proponga proprio una ristrutturazione di questa natura, ci sono due fattori importanti da ricordare quando si comincia a valutare la possibilità di adottare il SASE. In primo luogo il passaggio al SASE non deve necessariamente verificarsi dall'oggi al domani. Molte aziende, infatti, hanno optato per un approccio basato su casi d'uso, con un piano di espansione nel tempo. In secondo luogo, i vantaggi che comportano le architetture SASE possono aiutare le aziende a migliorare agilità e resilienza, contribuendo a elevare le iniziative SASE da un piano di mera sicurezza informatica a uno di più ampio respiro aziendale.

Studiando i passaggi intrapresi dalle aziende SASE mature, analizzando i benefici che ne hanno tratto e correlandoli alle priorità e capacità della propria azienda, diventa più facile trovare un punto di partenza, cominciare questo viaggio e iniziare a cogliere i frutti tangibili del SASE a breve termine.

Appendice I: Metodologia della ricerca e caratteristiche demografiche degli intervistati

Per raccogliere i dati per questo report, ESG ha condotto un sondaggio online completo tra i professionisti IT e della sicurezza informatica responsabili di valutare, acquistare e gestire servizi e prodotti per la sicurezza nel cloud e in rete. Oltre due terzi degli intervistati ricoprivano ruoli senior nel settore IT o della sicurezza (CIO, CISO, VP di IT/IS o equivalenti), mentre gli altri avevano incarichi dirigenziali o inferiori. Gli intervistati erano distribuiti in modo omogeneo tra Nord America (50%) ed Europa (50%). Tutti erano alle dipendenze di aziende con 500 o più dipendenti. In particolare, l'11% lavorava per aziende nella fascia media di mercato (cioè con 500-999 dipendenti) e l'89% per imprese (ovvero aziende con 1.000 o più dipendenti). Gli intervistati rappresentavano numerosi segmenti del settore privato e pubblico; la maggioranza proveniva da tecnologia/comunicazioni (20%), sevizi commerciali e finanziari (18%), manifattura (14%), salute e scienze della vita (13%), vendita all'ingrosso/al dettaglio (10%) ed enti pubblici (9%).

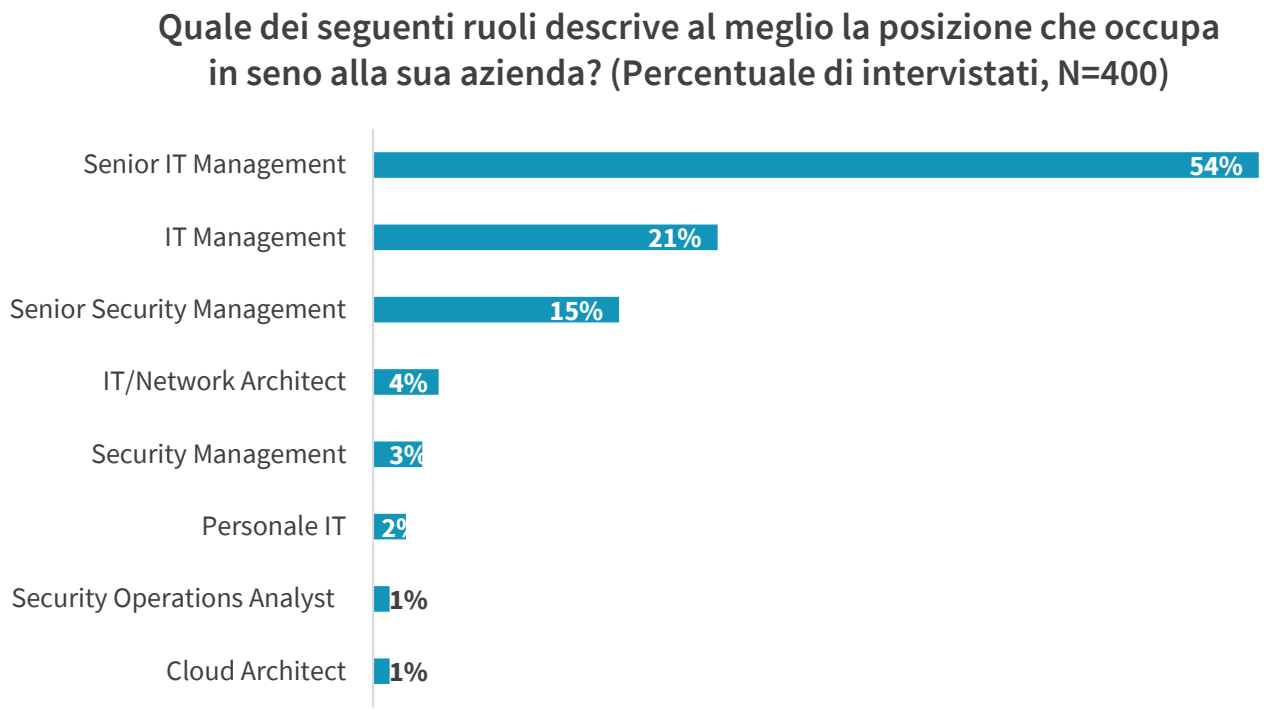
Il sondaggio è stato svolto tra il 13 e il 30 novembre 2020.

Dopo avere escluso i partecipanti non idonei, eliminato le risposte duplicate e vagliato le restanti risposte complete (utilizzando diversi criteri) in base all'integrità dei dati, è rimasto un campione finale di 400 intervistati.

Per completare il sondaggio, tutti gli intervistati hanno ricevuto un incentivo sotto forma di denaro contante e/o equivalenti. Nota: le percentuali che compaiono nelle figure e nelle tabelle del report sono state arrotondate per cui, se sommate, potrebbero non raggiungere il 100%.

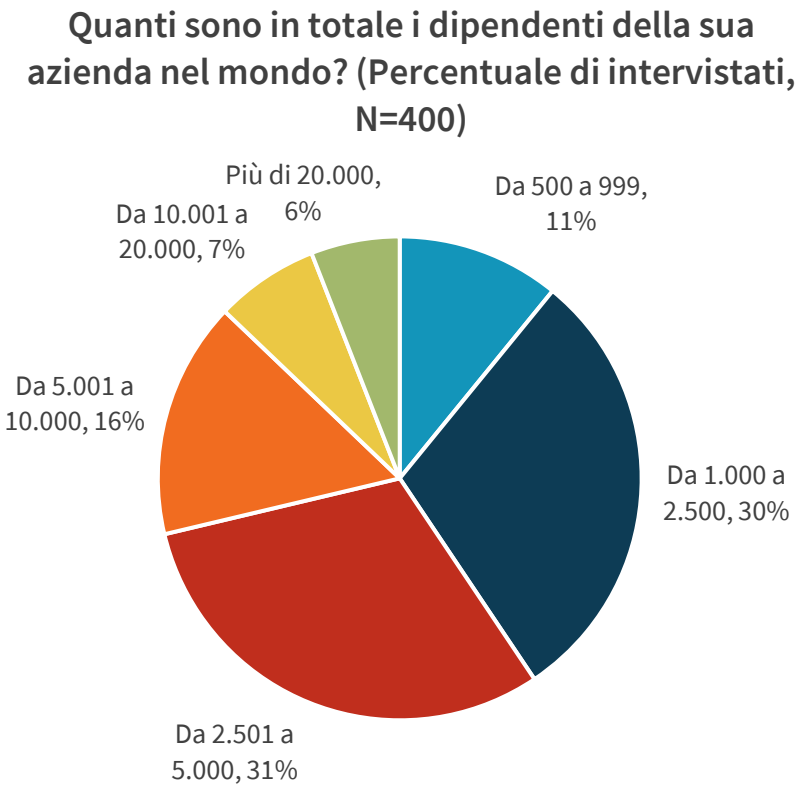
Le figure da 11 a 14 illustrano i dettagli demografici della base degli intervistati: i ruoli dei singoli intervistati, il numero totale di dipendenti delle aziende degli intervistati, il loro fatturato annuo e il loro settore primario.

Figura 11. Intervistati del sondaggio, in base al ruolo attuale



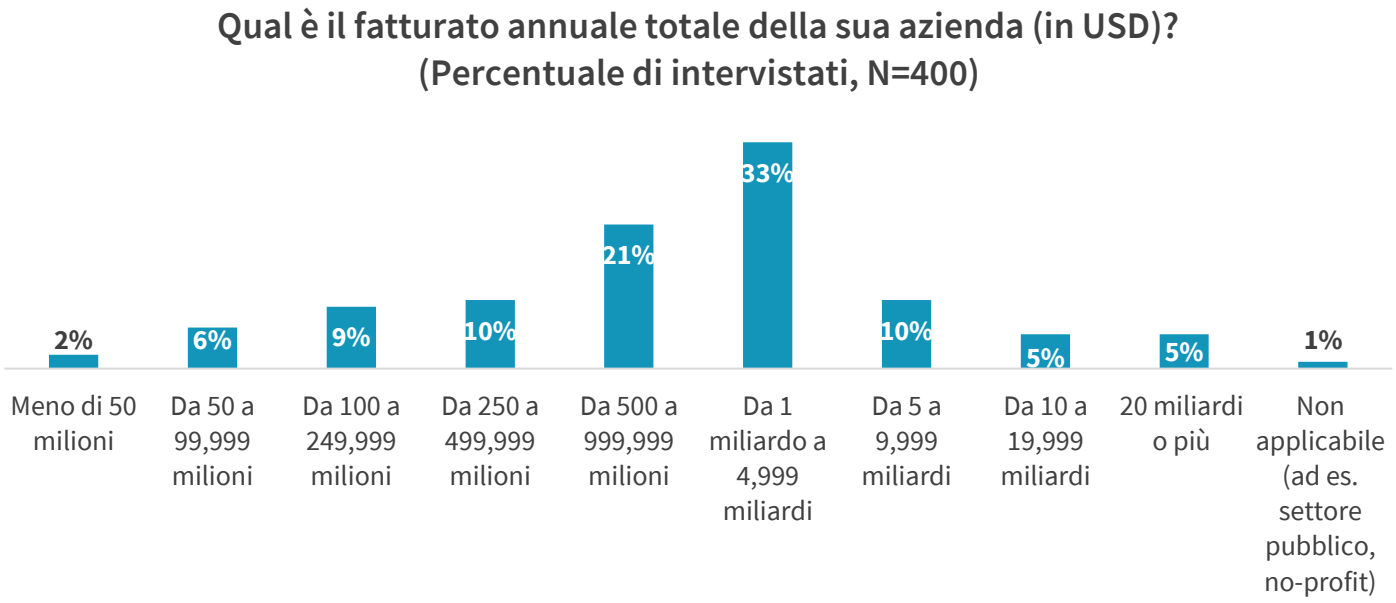
Fonte: Enterprise Strategy Group

Figura 12. Intervistati del sondaggio, in base alle dimensioni dell'azienda (numero di dipendenti)



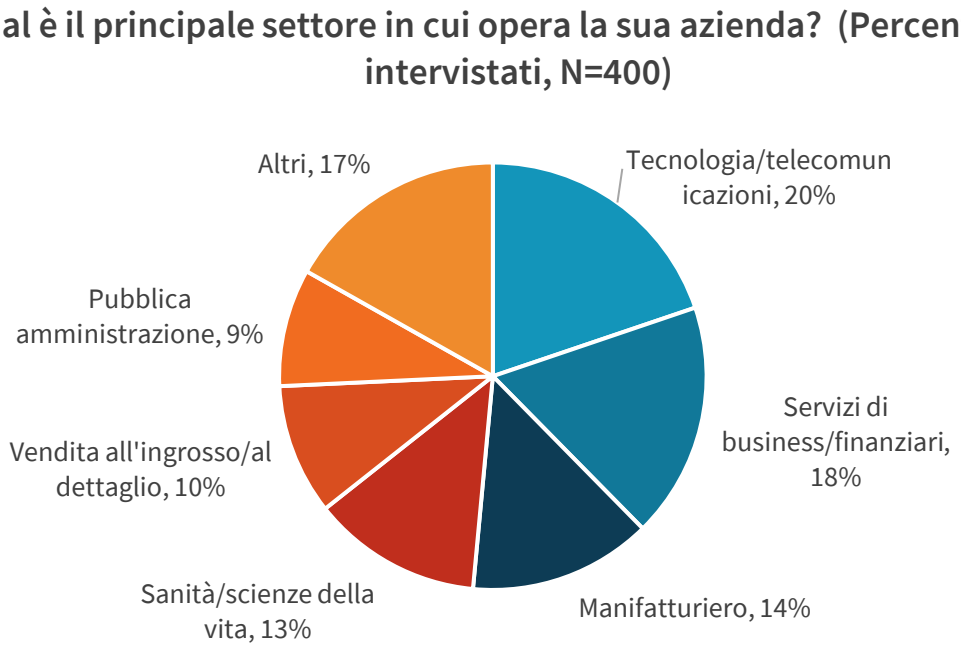
Fonte: Enterprise Strategy Group

Figura 13. Intervistati del sondaggio, in base alle dimensioni dell'azienda (fatturato annuale)



Fonte: Enterprise Strategy Group

Figura 14. Intervistati del sondaggio, in base al settore

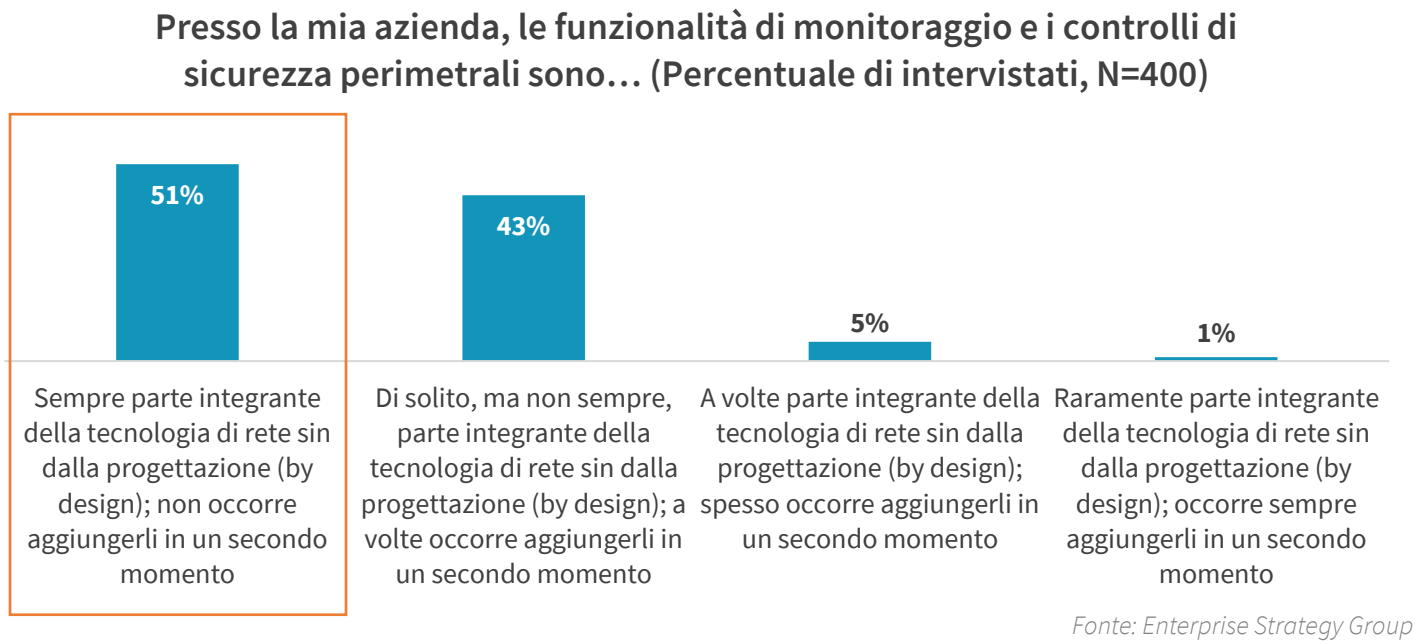


Fonte: Enterprise Strategy Group

Appendice II: Domande del sondaggio utilizzate da ESG per valutare la maturità SASE

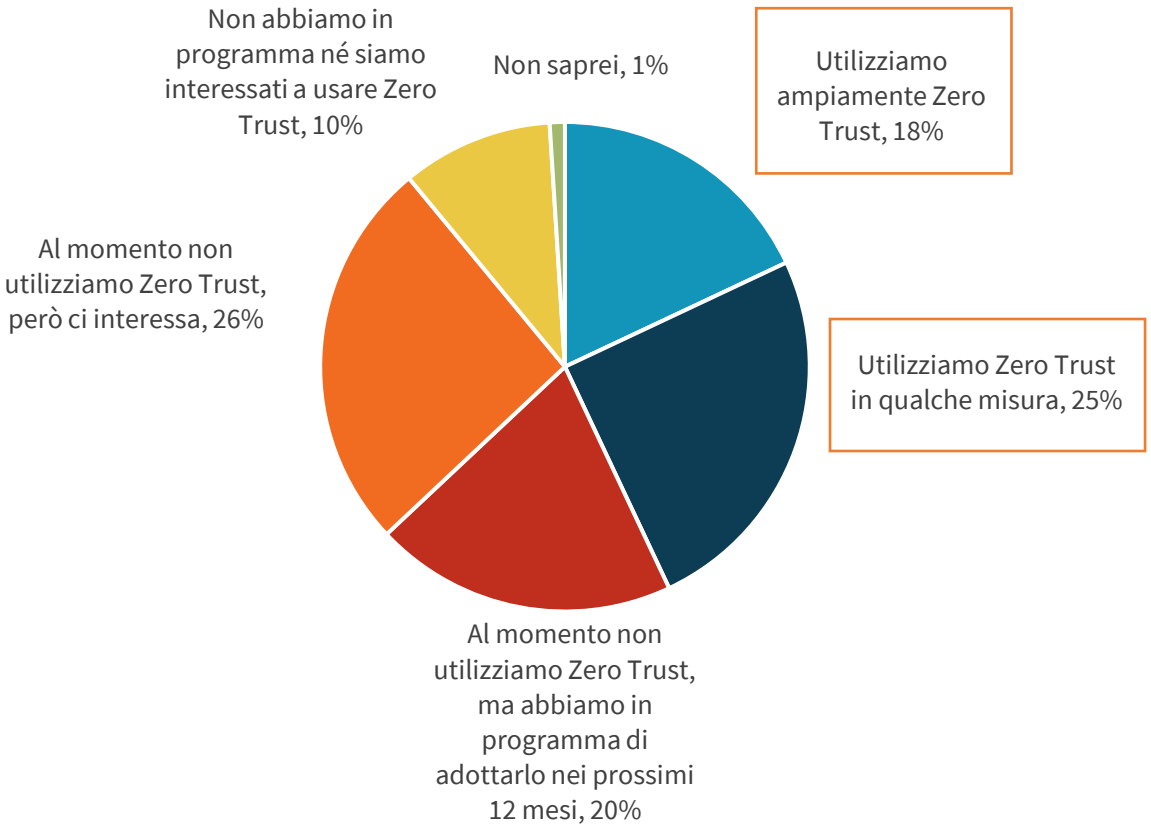
ESG ha valutato la maturità SASE delle aziende che hanno partecipato al sondaggio di ricerca in base alle loro risposte a cinque domande chiave su processi, controlli e tecnologie di sicurezza di rete. Le figure da 15 a 19 riprendono in dettaglio queste domande; le risposte evidenziate indicano quelle che ESG ha valutato come più mature.

Figura 15. Caratteristica di maturità 1: architettura di sicurezza perimetrale proattiva



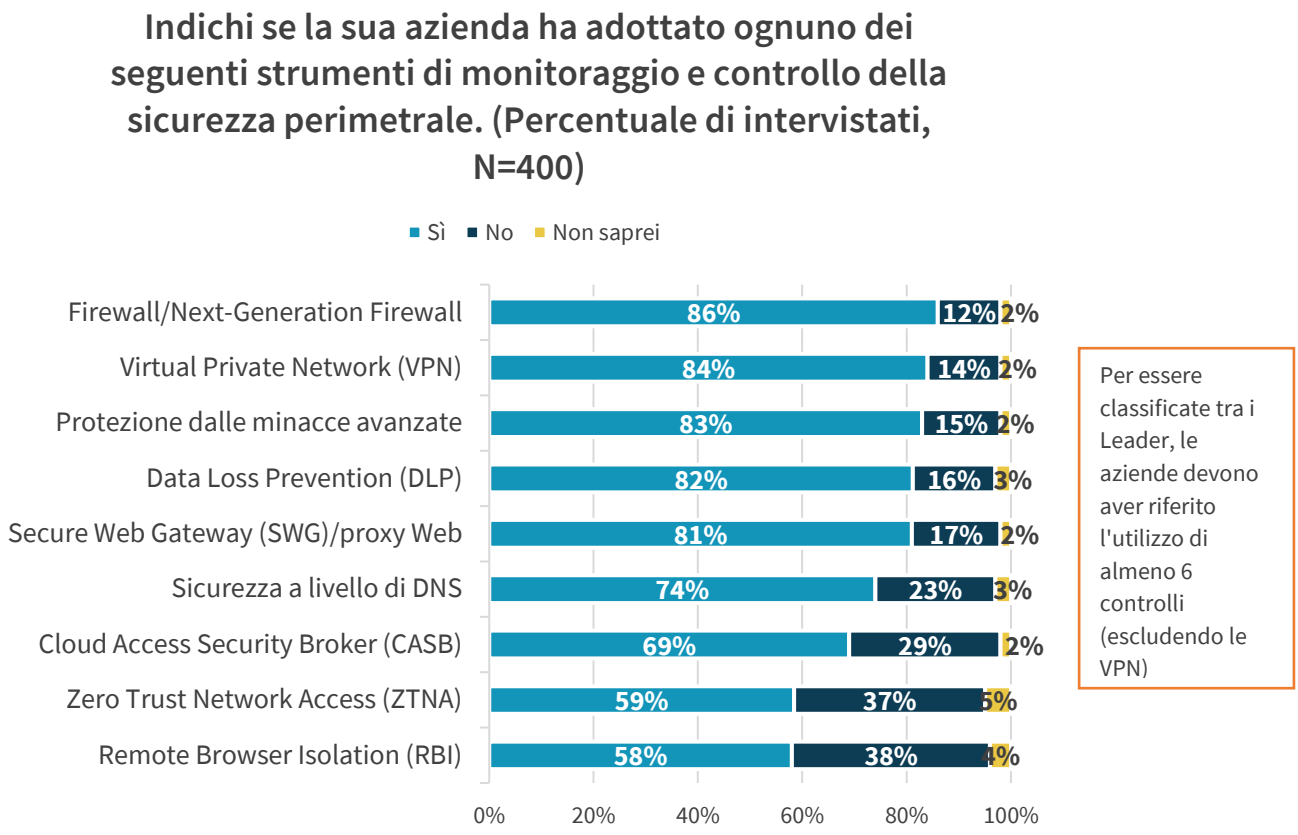
Fonte: Enterprise Strategy Group

Figura 16. Caratteristica di maturità 2: filosofia di sicurezza Zero Trust



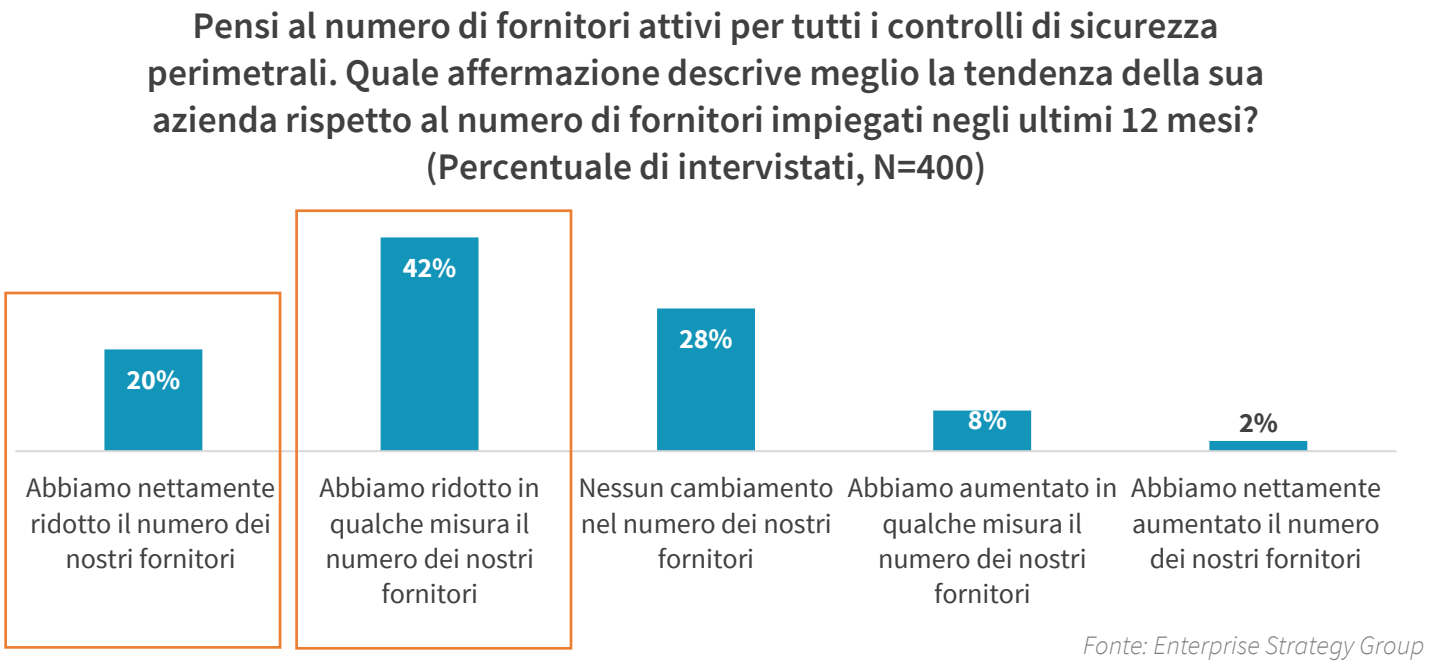
Fonte: Enterprise Strategy Group

Figura 17. Caratteristica di maturità 3: distribuzione di un solido set di controlli e funzionalità di sicurezza



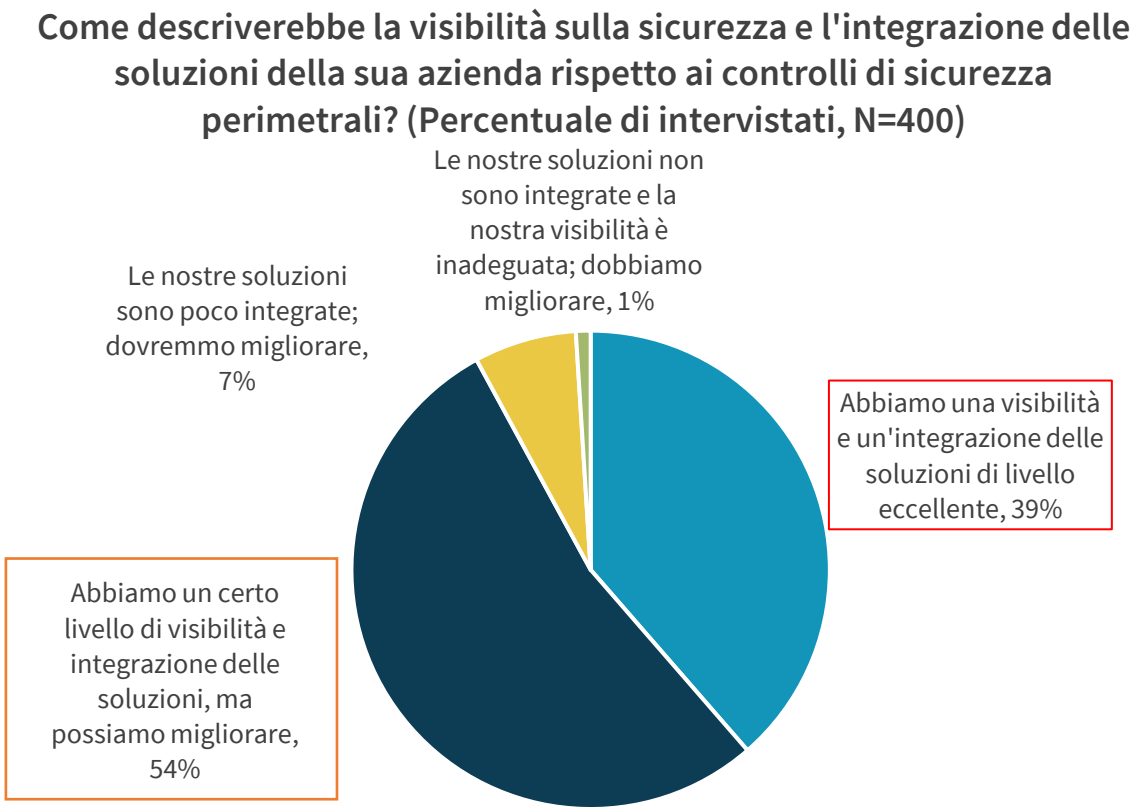
Fonte: Enterprise Strategy Group

Figura 18. Caratteristica di maturità 4: riduzione attiva dei fornitori di soluzioni di sicurezza perimetrale



Fonte: Enterprise Strategy Group

Figura 19. Caratteristica di maturità 4: riduzione attiva dei fornitori di soluzioni di sicurezza perimetrale



Fonte: Enterprise Strategy Group