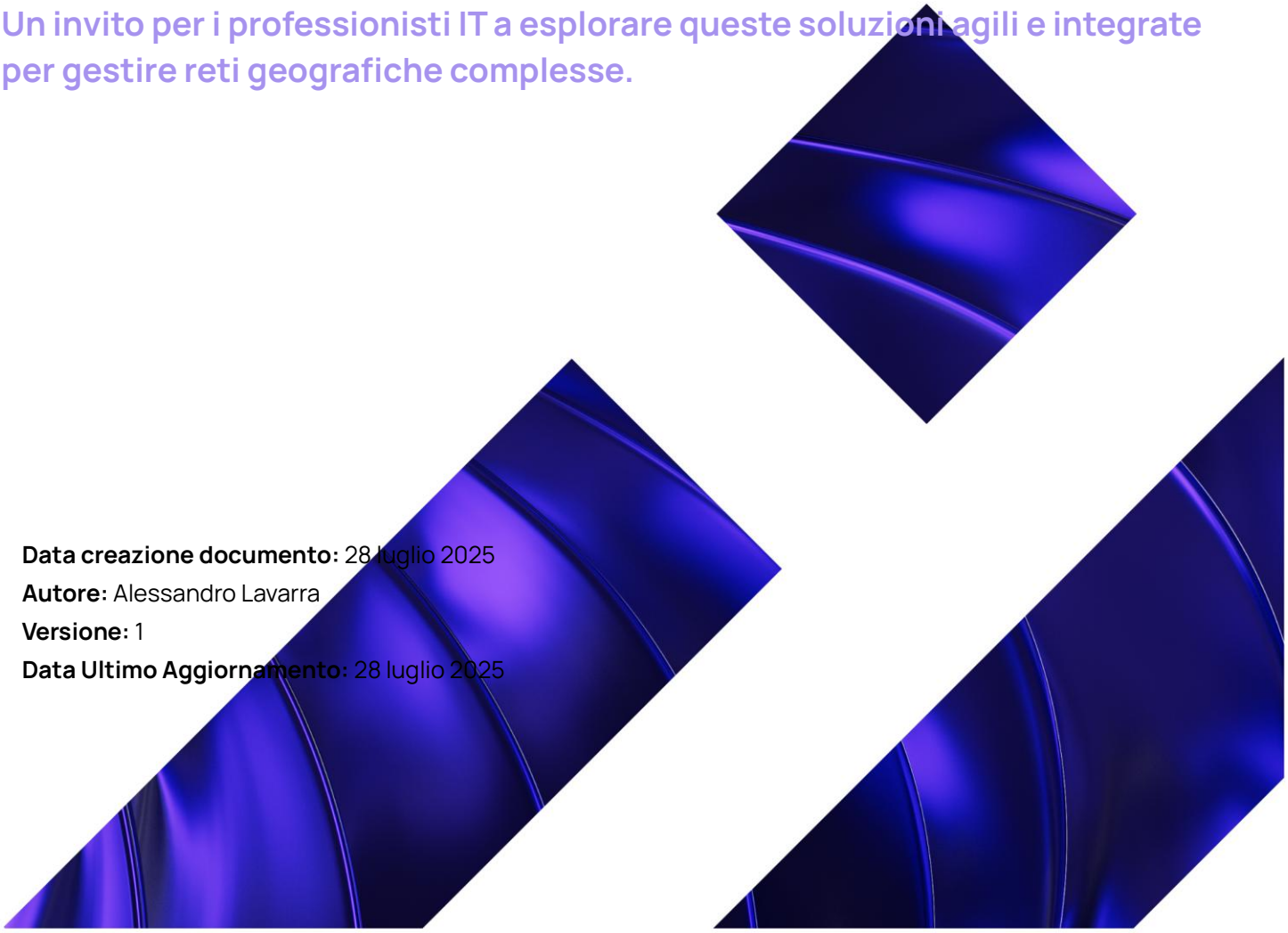
Scelta del fornitore nel mercato SASE

Una panoramica dettagliata del mercato attuale per le architetture SASE che esplora le offerte dei principali fornitori come PaloAlto e CATO Networks e fornisce elementi per l'adozione e la valutazione delle soluzioni.
Un invito per i professionisti IT a esplorare queste soluzioni agili e integrate per gestire reti geografiche complesse.



Data creazione documento: 28 luglio 2025
Autore: Alessandro Lavarra
Versione: 1
Data Ultimo Aggiornamento: 28 luglio 2025

Come orientarsi nella scelta del fornitore nel mercato SASE ancora molto dinamico e in via di definizione.

Le architetture SASE sono il modello che più si sta affermando per la gestione delle reti geografiche. L'approccio SASE (Security Access Service Edge) è stato descritto da Gartner che ne ha coniato la definizione, nel 2019 e, in pochi anni, si è meritato le attenzioni dei più grandi player del mercato delle reti.

Oggi si contano numerose soluzioni che si posizionano nella categoria SASE, alcune a pieno titolo altre con tecnologie non del tutto mature e altre ancora, in modo più forzato, per esigenze di marketing giusto per cavalcare l'hype che si è creato.

Hype giustificato dal fatto che questi modelli stanno dettando il passo sul modo di pensare la rete geografica e la relativa sicurezza oggi.

Come spesso accade sotto la bandiera di un nuovo acronimo o dietro ad una definizione di un nuovo paradigma architetturale si posizionano soluzioni con differenti modi di interpretare l'idea originale e, vista la rapidità con cui si alza il livello di interesse per SASE e con cui si evolvono le soluzioni di mercato, riteniamo utile fare chiarezza tra le differenti offerte.

Il mercato single vendor SASE

Il punto di partenza che utilizzeremo è il primo Magic quadrant di Gartner per il single-Vendor SASE pubblicato il 16 agosto di quest'anno che fornisce gli elementi di base per capire questo mercato emergente e molto dinamico.

Innanzi tutto è necessario un piccolo disclaimer. Essendo SASE una architettura di per sé eterogenea fondata sulla convergenza tra tecnologie di Software Defined WAN (SD-WAN) e un set di tecnologie di sicurezza basate sul cloud (Firewall as a Service, Secure Web Gateway, Zero Trust Network Access, Cloud Access Security Broker…) si potrebbe dire, in punta di definizione, che si è realizzata una architettura SASE anche aggregando soluzioni differenti di differenti vendor.

SASE però sottintende un'esperienza d'uso agile e trasparente sia da parte di chi gestisce le reti sia da parte delle organizzazione che lo adottano ed è per questo motivo che prenderemo in considerazione solo i prodotti e i servizi erogati da uno stesso vendor e, il più possibile, integrati e cloud-based.

Il mercato SASE dal lato dei produttori è ancora in via di definizione e si muove, in modo molto dinamico, tra sviluppo di soluzioni e, in quasi la totalità dei casi, in acquisizioni strategiche che vedono i differenti player impegnati nell'aggregare tecnologie e integrare i diversi componenti, vedremo su questo punto l'eccezione virtuosa.

Dal punto di vista degli utenti finali si tratta di un mercato ancora immaturo e il tasso di adozione in Italia è un po' più lento rispetto alle altre country e a quanto gli operatori si immaginassero nonostante i benefici di semplificazione, saving ed efficienza che garantisce. Nell'anno in corso comunque questo trend si sta invertendo e l'approccio SASE sta riscontrando l'attenzione che merita.

Le funzionalità di SASE e i protagonisti del mercato

SASE deve garantire l'accesso sicuro ai siti produttivi, ai branch office alle applicazioni nei data center on premises e in cloud da parte degli utenti interni e remoti e ai servizi SaaS.

I servizi base per poter parlare di SASE devono comprendere: secure web gateway (SWG), controlli in linea per l'accesso SaaS, accesso remoto alle applicazioni basato su identità, contesto e policy e un'appliance che supporti la gestione dinamica del traffico, prioritizzazione e aggregazione di banda.

Le funzionalità opzionali invece comprendono servizi di sicurezza come il remote browser isolation, data loss prevention, una sandboxing di rete, protezione DNS, interoperabilità basata su API.

Con questa premessa vediamo le offerte più significative selezionate da Gartenr nel primo quadrante su SASE.

Abbiamo alcuni vendor che partono dal mercato SD-WAN e hanno esteso la loro offerta ai servizi di sicurezza grazie all'integrazione di più tecnologie proprie o derivanti da acquisizioni. In questi casi è necessario fare attenzione all'integrazione delle diverse parti, al ruolo della componente hardware che in una buona architettura SASE dovrebbe essere marginale, al licensing e a come viene gestita e orchestrata la convivenza di più prodotti.

In questa categoria Gartner posiziona tra i visionari CISCO ma lo considera ancora debole in quanto ad "ability to execute" in particolare per l'orchestrazione tra i tanti prodotti che compongono la sua offerta SASE: Umbrella, Secure Connect, Meraki SD-wan, Catalyst e Duo oltre ad alcuni limiti geografici dei propri PoP.

Anche Versa Networks, classificato come Challenger, ha robuste funzionalità SD-wan e propone Versa Secure Access Fabric (VSAF) come piattaforma SASE unificata, con, in alternativa, Titan per incontrare i bisogni di clienti meno esigenti in termini di features e di conseguenza di investimento. Versa sembra avere una visione a lungo termine nel settore.

Altri vendor arrivano dal mondo della sicurezza più tradizionale e "hardware centrica" come Fortinet, lui pure classificato tra i "challengers". L'offerta però si compone di una serie di prodotti della famiglia *Forti-* che ruotano attorno all'appliance FortiGate che rimane centrale (Forti SD-wan, FortiManager, FortiCASB, FortiMonitor, FortiWeb, FortiSASE, Fortisolator) rendendo necessario gestire diversi componenti. Fortinet è arrivato da poco al mercato SASE ed è comprensibile visto l'ampio installato della sua offerta più tradizionale.

Altro vendor protagonista del mercato della sicurezza è PaloAlto, già leader nei quadranti SD-wan e SSE che sono i due componenti che convergono nelle architetture SASE, PaloAlto si piazza, solitario, tra i leader anche nel quadrante SASE.

L'offerta di PaloAlto è Prisma SASE, una piattaforma che integra SD-wan con CloudGenix e NGFWs e si appoggia a componenti virtuali come Access Prisma per ottimizzare il traffico WAN attraverso il cloud su infrastruttura Google. Prisma presenta difficoltà nell'integrazione dei suoi componenti risultando complessa da gestire.

Prisma SASE si basa su PoPs proprietari, ma non può adattarsi dinamicamente ai cambiamenti nell'ambiente di rete per la forte dipendenza con i servizi Google Cloud Platform (GCP) il che può compromettere anche le prestazioni in alcune aree come la Cina. La soluzione mostra debolezze nelle operazioni in ambienti nativi cloud e nella gestione di servizi come SaaS, con un impatto sulla performance delle applicazioni oltre a costi non propriamente accessibili.

Cato Networks: nata come startup senza vincoli pregressi di installato o di asset da salvaguardare, ha progettato da zero la sua soluzione SASE cloud native con tutte le funzionalità integrate by design. Ottima l'esperienza d'uso lato network and security.

Basata su un backbone proprietario per il trasporto del traffico unito ad uno stack applicativo per gestire regole di rete e sicurezza in un unico passaggio, la soluzione SASE di CATO, ha una distribuzione capillare grazie ai suoi PoP presenti in tutto il mondo (da menzionare in particolare l'efficacia della soluzione quando è necessario portare servizi in Cina).

CATO ha fatto della semplificazione dell'infrastruttura della WAN l'elemento fondante della propria proposta che si manifesta anche nella console di gestione estremamente friendly e immediata mantenendo la promessa di facilità d'uso e trasparenza e nell'estrema flessibilità.
Solidamente basata su una infrastruttura next generation SD-wan la roadmap di CATO è indirizzata all'evoluzione dei servizi di sicurezza. Gartner posiziona CATO prima soluzione tra i challengers perchè, dichiara, sconta una maggiore lentezza nel costruire la base installato e la rete di vendita e assistenza worldwide.

Menzioni

Fuori dal quadrante ma meritevoli di menzione sono rimasti Cradlepoint (acquisita da Ericsson) e Netskope perchè al momento dell'analisi non soddisfacevano i criteri di inclusione di Gartner.

Nel frattempo Netskope leader del mercato SSE con le sue soluzioni CASB, SWG e DLP ha acquisito tecnologia SD-wan (Infiot) per completare la propria offerta SASE e Cradlepoint leader del mercato wireless WAN 4G e 5G ha annunciato, dopo l'acquisizione di Ericom (per la componente di sicurezza), la sua roadmap in 12 mesi per il lancio della propria offerta 5G-optimized Secure Access Service Edge (SASE) che promette di estendere il concetto di rete geografica gestita anche agli impianti OT, IoT e mezzi in movimento.

La scelta di adottare architetture SASE

Per quanto riguarda l'adozione di SASE i responsabili delle reti, e della sicurezza assieme a CIO e responsabili delle operation dovrebbero collaborare nell'adozione di architetture SASE e, utilizzando anche gli spunti contenuti in questo articolo, valutare quali fornitori sono più adatti alle loro esigenze orientandosi verso soluzioni più robuste lato SD-wan o lato sicurezza a seconda delle caratteristiche della propria organizzazione o più equilibrate e attente alla facilità di implementazione per coprire in modo uniforme e agile tutti i bisogni della rete geografica.

In accordo con i principali analisti e come abbiamo già evidenziato in precedenti articoli, per le organizzazioni con reti geografiche da gestire, SASE deve rappresentare un'opzione immediata o di prossima valutazione.

A questo proposito si consiglia di non effettuare investimenti a lungo termine su tecnologie puntuali che coprano singoli casi d'uso e che precludano o rallentino l'adozione di soluzioni SASE complete.