Sostituzione della VPN

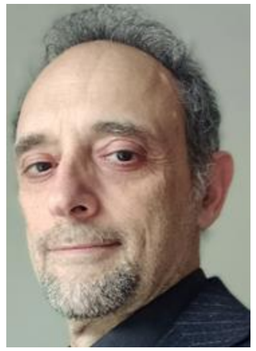
Perché è il momento giusto ?

Stefano Artioli | WW Solutions Architect, *Netskope*

Stefano Marzi | Technical Design Security Team Leader, *N&C*

Stefano Artioli
WW Solutions Architect, *Netskope*

Stefano Marzi
Technical Design Security Team Leader, N&C



Prima di tutto,
qualche definizione...

Security Service Edge (SSE) Vs Secure Access Service Edge (SASE)

Security service edge (SSE) **secures access to the web, cloud services and private applications**. Capabilities include access control, threat protection, data security, security monitoring, and acceptable-use control enforced by network-based and API-based integration. SSE is primarily delivered as a cloud-based service, and may include on-premises or agent-based components.

https://www.gartner.com/en/information-technology/glossary/security-service-edge-sse

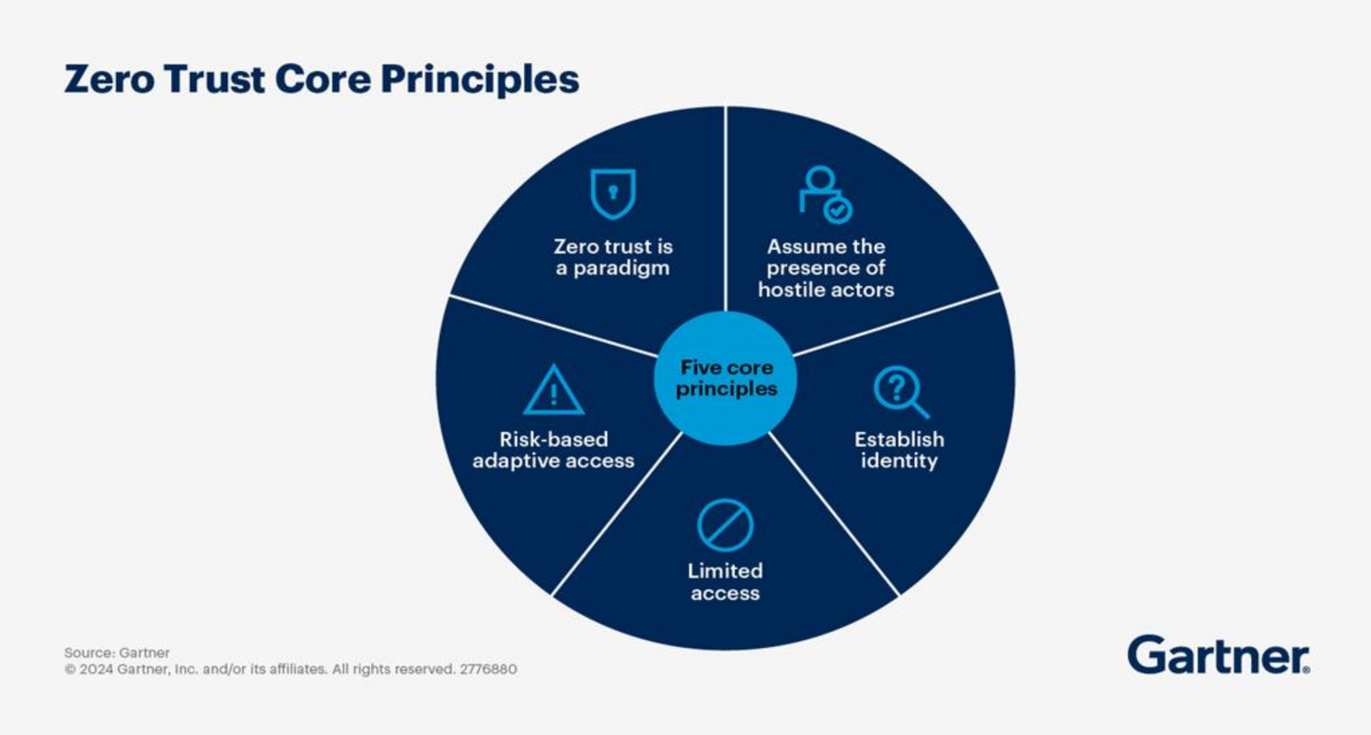
Secure access service edge (SASE) **delivers converged network and security as a service capabilities**, including SD-WAN, SWG, CASB, NGFW and zero trust network access (ZTNA). SASE supports branch office, remote worker and on-premises secure access use cases. SASE is primarily delivered as a service and enables zero trust access based on the identity of the device or entity, combined with real-time context and security and compliance policies.

https://www.gartner.com/en/information-technology/glossary/secure-access-service-edge-sase

Zero Trust

In contrast to the traditional “castle and moat” model of information security, where **everyone inside** the moat **is implicitly trusted**, **zero trust assigns access based on calculated risk and adapts the access as the calculated risk of the entity changes and the criticality of the accessed object**. The zero-trust approach delivers the resilience to mitigate cyber risk, enables modern business capabilities and a hybrid workforce, and provides the flexibility to enable appropriate access methods, while removing implicit access based on location.

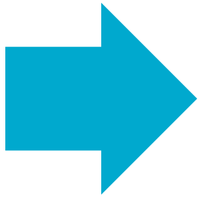
https://www.gartner.com/en/cybersecurity/topics/zero-trust-architecture



Zero Trust Network Access (ZTNA)

Zero trust network access (ZTNA) is a product or service that creates an identity- and context-based, logical access boundary around an application or set of applications. **The applications are hidden from discovery, and access is restricted via a trust broker to a set of named entities.** The broker verifies the identity, context and policy adherence of the specified participants before allowing access and prohibits lateral movement elsewhere in the network. This removes application assets from public visibility and significantly reduces the surface area for attack.

https://www.gartner.com/en/information-technology/glossary/zero-trust-network-access-ztna-



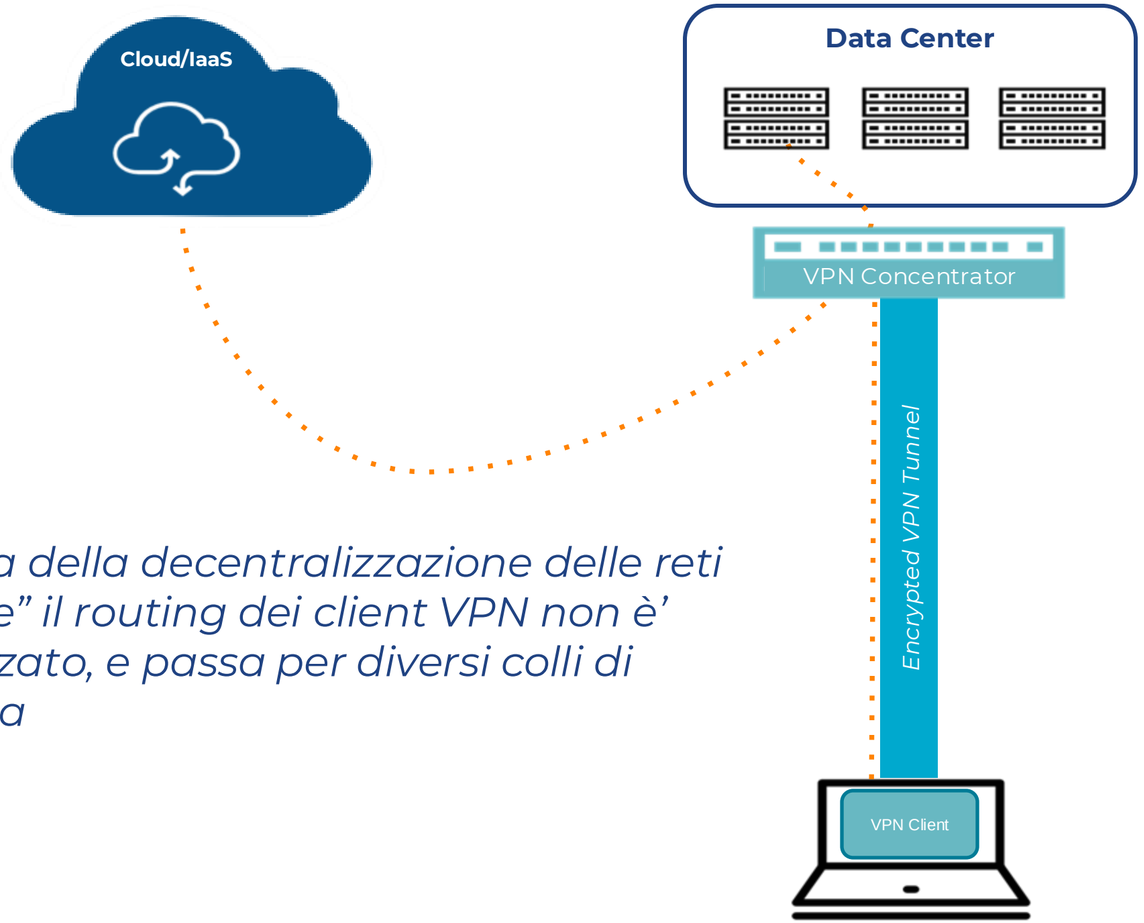
- ✓ Adattiva
- ✓ “Context-aware” e “Least-Privileged”
- ✓ Accesso alle Applicazioni, e non alla rete
- ✓ Configurata via Policies
- ✓ Le risorse interne non possono essere scoperte

Entro il 2025, come minimo il 70% degli accessi remoti verrà servito tramite Zero Trust Network Access (ZTNA), in grossa crescita rispetto al 10% stimato alla fine del 2021.[1]

1. Gartner Research

Cosa c’e’ di “sbagliato” nella VPN ?

Cosa c’e’ di “sbagliato” nella VPN ?



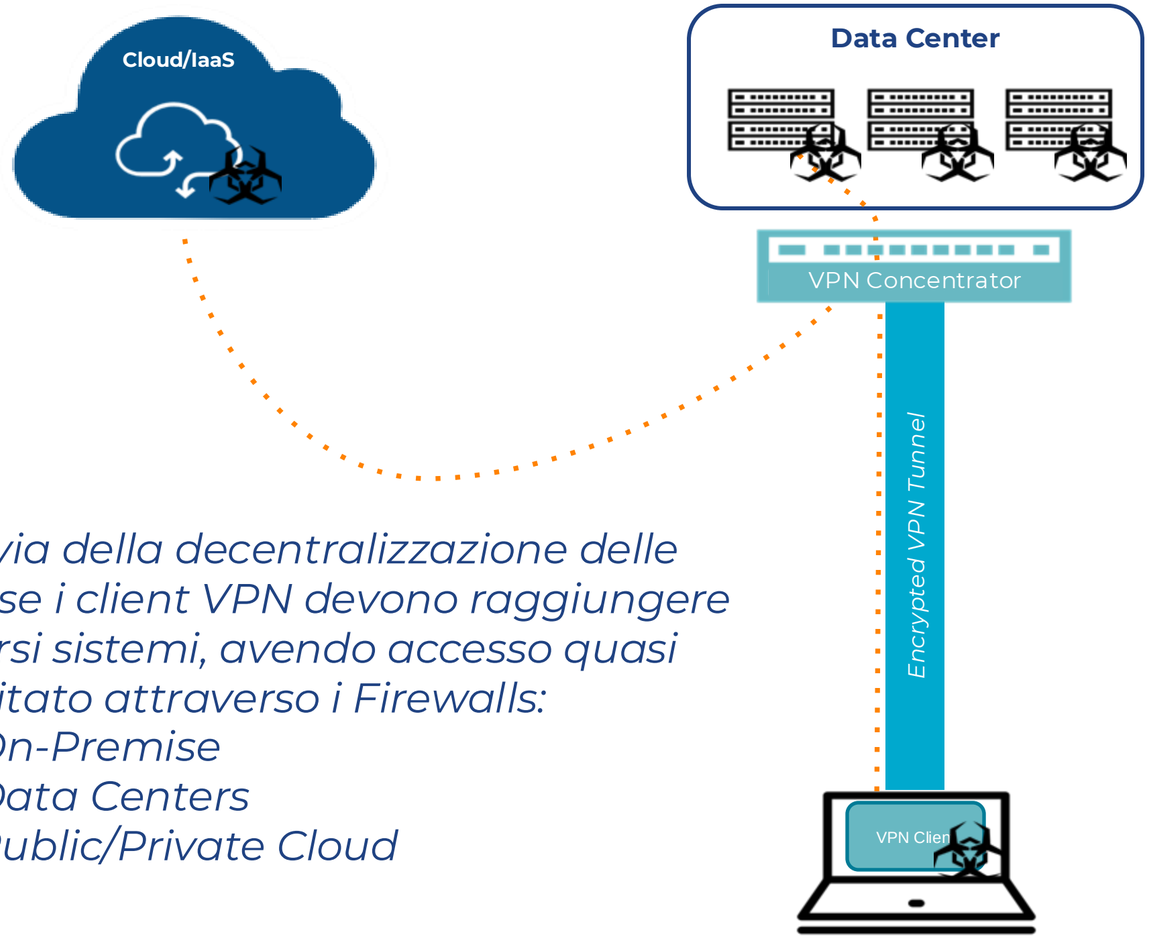
A causa della decentralizzazione delle reti “interne” il routing dei client VPN non è’ ottimizzato, e passa per diversi colli di bottiglia

La fiducia implicita garantisce accesso quasi illimitato ad utenti autenticati con la VPN

I VPN concentrators sono dispositivi complicati, costosi, che vanno tarati sulle crescenti necessità di lavoro remoto e che richiedono continuo patching

Le VPN richiedono la presenza di un client specifico, che spesso deve essere avviato dall’utente manualmente

VPN e considerazioni di Cyber Security



Per via della decentralizzazione delle risorse i client VPN devono raggiungere diversi sistemi, avendo accesso quasi illimitato attraverso i Firewalls:

- *On-Premise*
- *Data Centers*
- *Public/Private Cloud*

La “fiducia implicita”, o “implicit trust” che la VPN garantisce al dispositivo permette al malware di avere una presenza diretta all’interno della rete

Una volta che il Malware e’ nella rete ha la possibilità di effettuare “lateral movement”

In Sostanza…

Mancanza di Visibilità e Controllo

- Policies non consistenti
- Troppa libertà di accesso
- Nessuna Visibilità e Controllo delle applicazioni accedute

Pessima Esperienza Utente

- Necessità di convogliare tutto il traffico in un singolo punto
- Connessioni VPN multiple, o multiple connessioni interne
- Impossibilità di ottimizzare le rotte

Rischi sulla Sicurezza

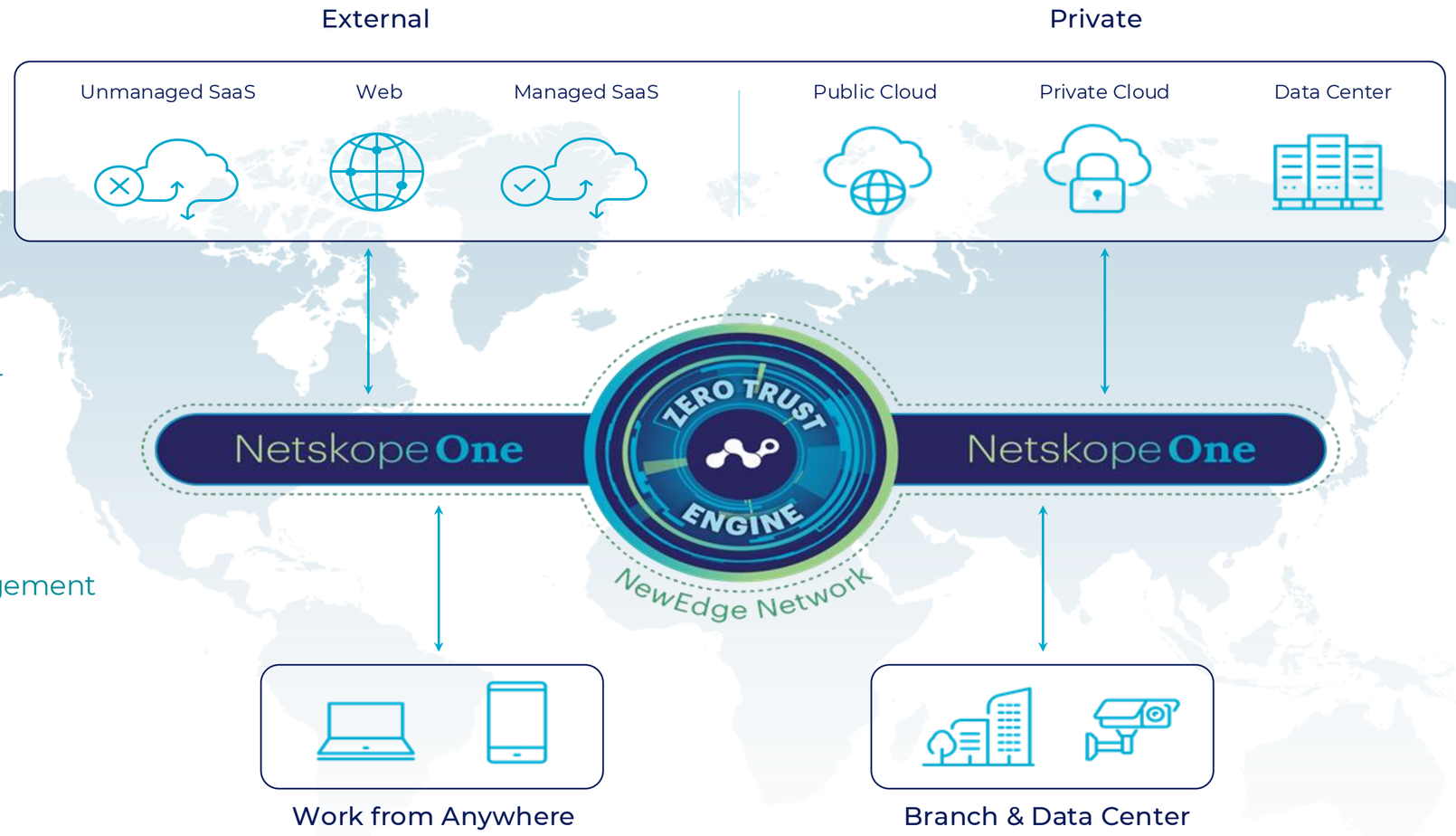
- Presenza IP nella rete
- Fiducia Implicita
- VPN esposta agli “Hackers”
- “Lateral Movement” non autorizzato

Complessità e costo

- Instradamento complesso
- Manutenzione
- Aggiornamento
- Soluzioni separate
- Alto volume di chiamate all’HelpDesk

Alternativa alla VPN - Netskope One Private Access

Netskope One Platform – Product View

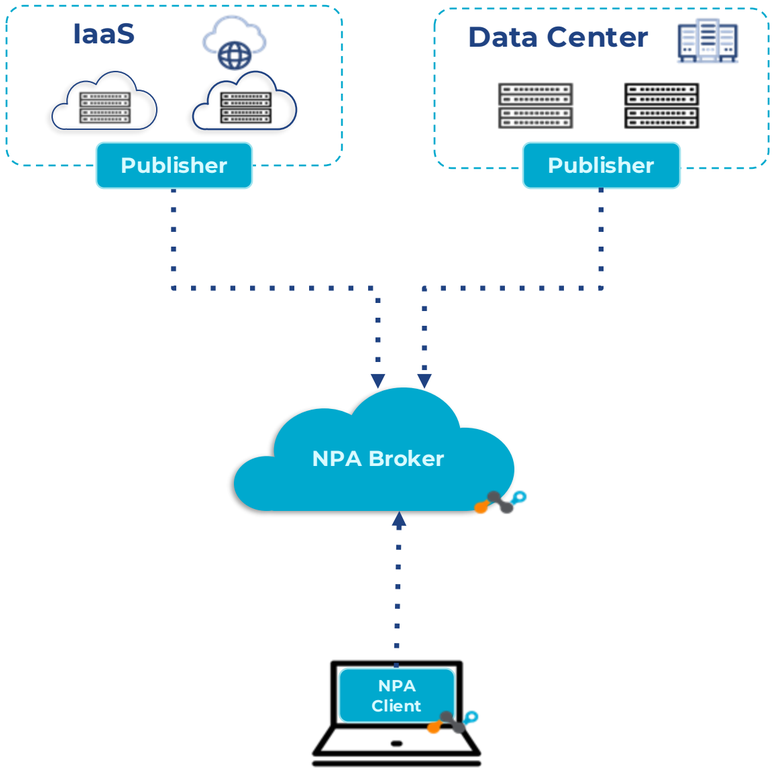


Cloud Access Security Broker
Secure Web Gateway
Zero Trust Network Access
Data Protection + DLP
Threat Protection
Data Security Posture Management

SD-WAN
SASE Client
Digital Experience Mgmt.
Firewall and IDS/IPS
Intelligent IoT

Alternativa alla VPN

Netskope One Private Application Access (NPA)



Vantaggi:

- Protezione superiore con accesso diretto alle applicazioni tramite policies “Zero Trust”
- L’architettura utilizza solo connessioni “outbound” riducendo la superficie di attacco
- Le applicazioni interne sono schermate da scansioni riducendo i “lateral movement”
- L’instradamento diretto verso le applicazioni garantisce performances superiori ed una migliore esperienza utente
- Riduzione del costo e della complessità
- Supporta sia dipendenti remoti che utenti esterni

Limiti:

- Non tutte le applicazioni interne sono compatibili con NPA. Applicazioni che richiedono connettività Server-to-Client richiedono un IP del Client remoto nella rete (Eg. VOIP)
- Per supportare queste applicazioni i clienti dovrebbero mantenere una VPN per questi casi specifici… MA…

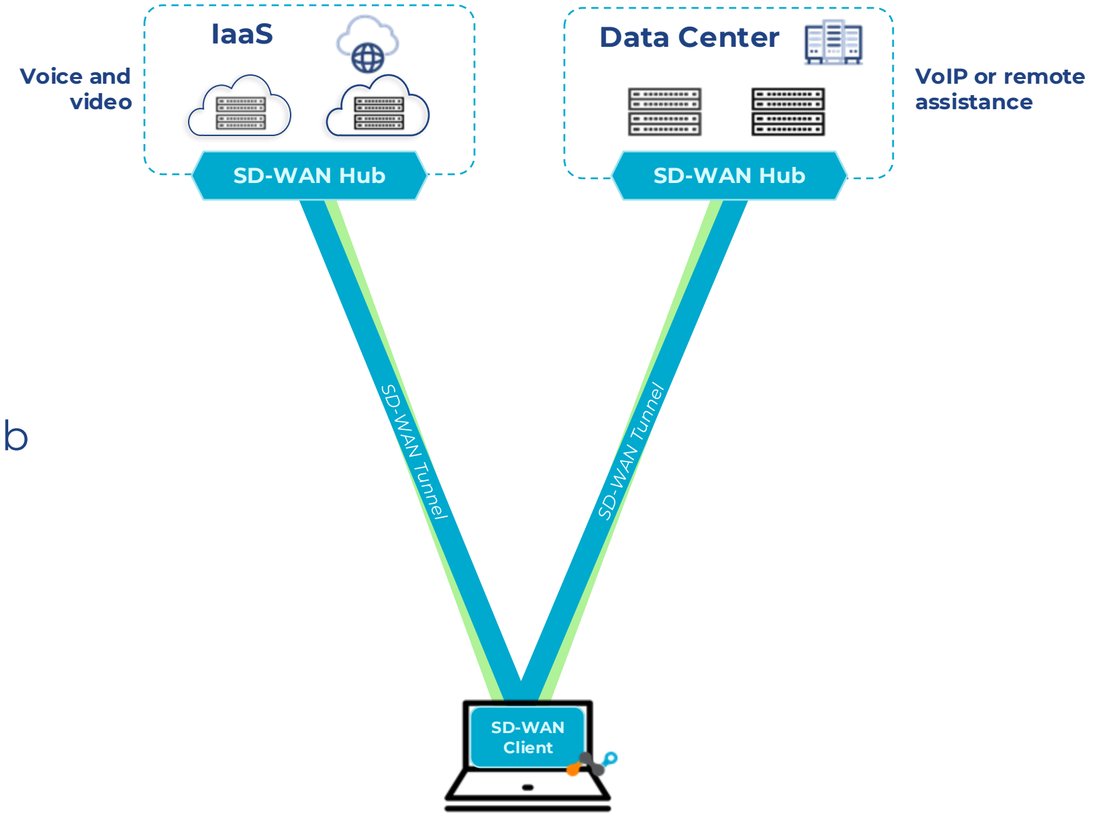
Alternativa alla VPN
Netskope One Private Optimized Access (SD-WAN Client)

Vantaggi:

- Accesso ad applicazioni che richiedono un IP per contattare il Client remoto (Server-to-Client, come VOIP)
- Connessione ad applicazioni, non a reti, con configurazione tramite policies
- Scelta del miglior instradamento, QoS ed “application assurance” tipici delle soluzioni SD-WAN
- Ottimizzazione Voice/Video per applicativi On-Prem (VoIP) & Cloud (e.g. UCaaS, come Zoom)
- Alte prestazioni per via della connessione diretta a multipli Hub (DC, IaaS)

Limiti:

- Non completamente allineato ai principi ZTNA per via della presenza dell’IP del Client nella rete (sebbene limitato alle singole applicazioni)



Use Cases supportati da Netskope One Private Access

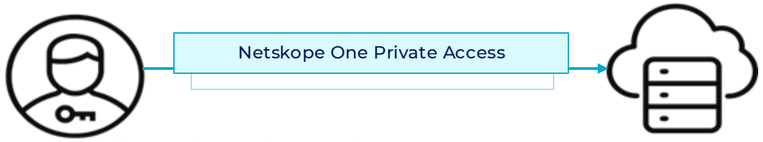
Sostituzione della soluzione VPN

- Strategia Zero Trust
- Riduce la superficie di attacco
- Minimizza il “lateral movement”
- Riduce i rischi

Lavoro Ibrido e Remoto

- Continua valutazione delle Policies
- Esperienza Utente superiore
- Gestisce l’accesso di utenti esterni

Movimento nel Cloud

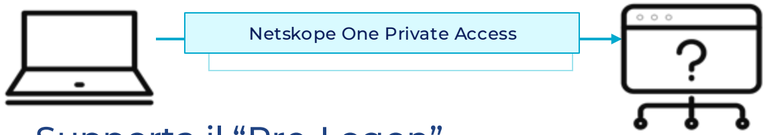


- Accelera la migrazione
- Mantiene un controllo costante
- Garantisce un accesso diretto
- Semplifica la connessione

“Mergers and Acquisitions”

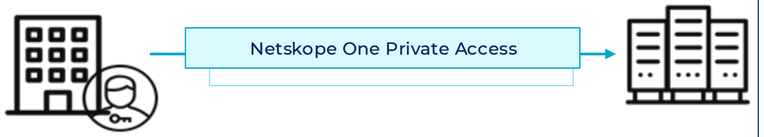
- Garantisce accesso immediato
- Elimina la ristrutturazione di rete
- Accelera l’integrazione

Supporta l’installazione remota



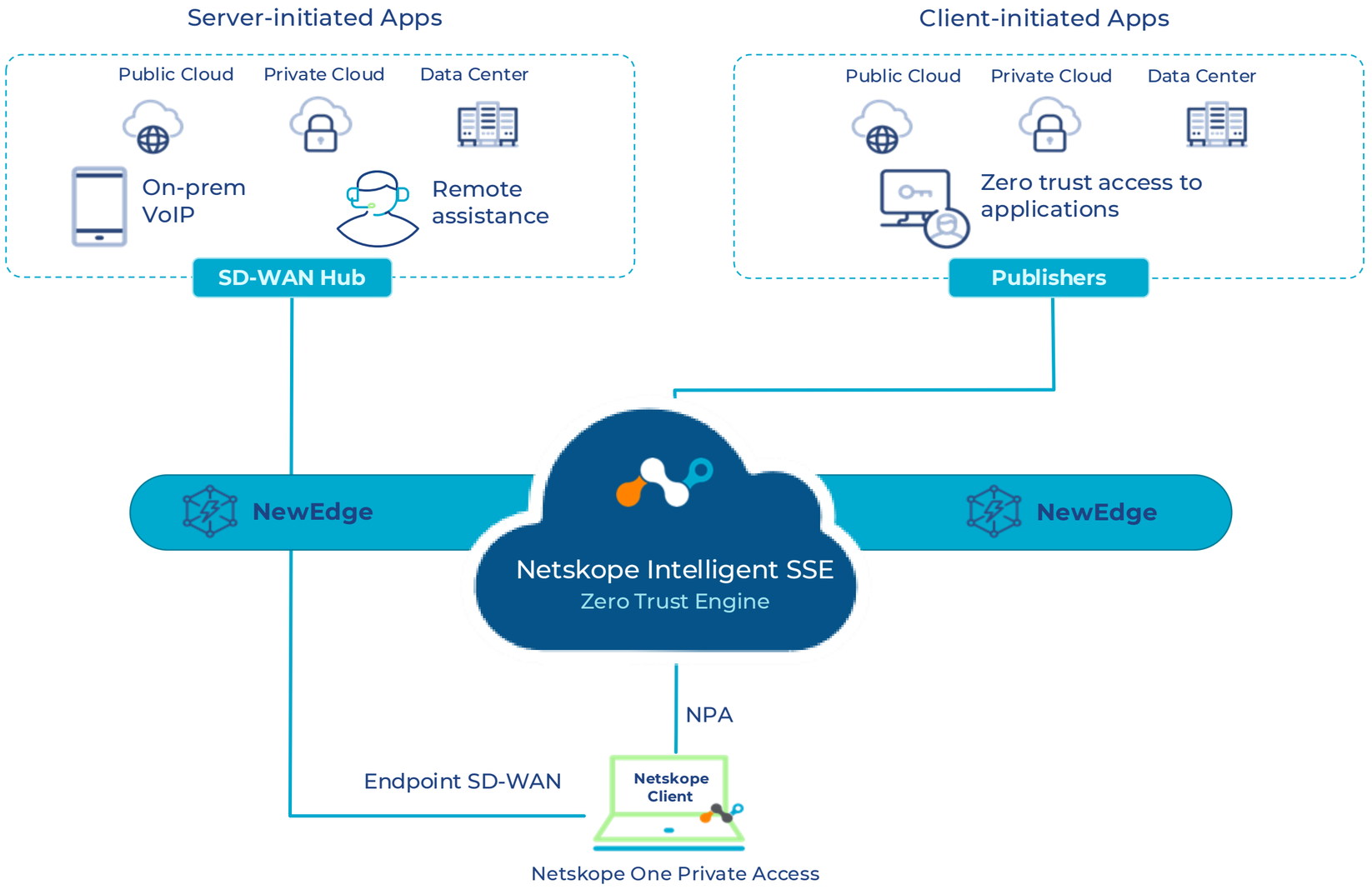
- Supporta il “Pre-Logon”
- Supporta il reset della password
- Supporta Windows Autopilot, anche ibrido

Supporta uffici remoti



- Continua valutazione delle Policies
- Riduce il bisogno di Site-to-Site VPN
- Esperienza utente superiore

Singola Soluzione - Netskope One Private Access



- Accesso diretto a tutte le Applicazioni
- Accesso “Context-aware” e “Least-Privileged” Grazie a ZTNA
- Supporto per applicazioni che richiedono traffico Server-to-Client
- Singolo Client
- Riduzione del costo e della complessità

I Benefici di Netskope One Private Access

Aggiorna la tua vecchia soluzione di Accesso Remoto basata su VPN ottimizzando la velocità e competitività del tuo business e riducendo la complessità ed i costi

Migliora l'esperienza utente e la produttività degli utenti ibridi e remoti

Migliora la sicurezza con principi di Zero Trust

Riduce i costi e la complessità con una soluzione distribuita, completa ed unificata

Esempi concreti - Clienti che sono migrati a Netskope One Private Access

“Ho un problema con la gestione degli accessi in VPN”

Cosa possiamo fare quando un cliente che opera nella pubblica amministrazione ci pone questa domanda?

Diventa fondamentale seguire una serie di passaggi chiave che garantiscano sicurezza e conformità alle normative del settore (come la NIS2)

- Comprendere il problema del cliente
- Analizzare l’infrastruttura
- Cercare la miglior soluzione in termini di sicurezza & costi
- Illustrarla al cliente
- Implementarla

Ma entriamo nel dettaglio del nostro primo cliente

300 dipendenti distribuiti su più sedi regionali

Utilizzo di client VPN con autenticazione standard

Utenti remoti che richiedono l’accesso alle risorse del Data Center

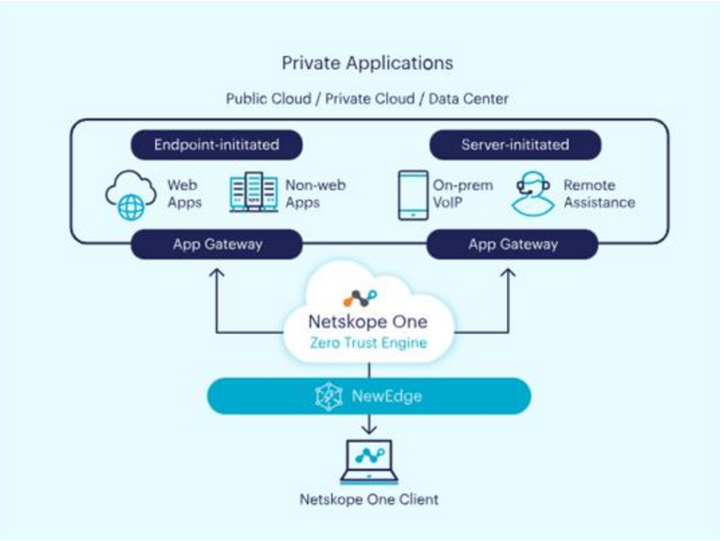
Necessità di raggiungere endpoint remoti dai server aziendali

Ha subito una violazione dei dati

La sfida del progetto

Soddisfare i requisiti, mantenendo l'operatività ed aumentando la sicurezza

Quale soluzione abbiamo implementato?
Netskope One Private Access



Cosa abbiamo ottenuto:

- Controllo sugli accessi, attivando il Multi Factor Authentication con Entra ID
- Aumento della visibilità degli endpoint e degli utenti
- Attivazione dello Zero Trust e granularità nelle policy di accesso ai servizi
- Protezione del traffico bidirezionale client <> server

Secondo cliente, Un caso.... un pò diverso

Questa volta siamo nella Pubblica Amministrazione Centrale,
un Ente con centinaia di sedi sul territorio nazionale, parcellizzazione delle risorse e delle policy di sicurezza.
Ci siamo trovati di fronte a delle esigenze diverse dal precedente.

Le richieste convergevano verso l'attivazione di:

- ZTNA su 10000 utenze e la protezione dell'accesso con MFA.
- Politiche di Zero Trust verso servizi in Housing e SaaS
  .
- Controllo della navigazione Web per gli utenti fuori sede

La soluzione è sempre Netskope One

E’ stata inoltre richiesta la funzionalità di “Posture check” per le risorse SaaS.

Questa soluzione, confrontando le impostazioni delle applicazioni SaaS con policy di sicurezza e benchmark del

settore come CIS, PCI-DSS, NIST, HIPAA, CSA, GDPR e ISO, aiuta ad identificare configurazioni errate ed allineare

la postura di sicurezza alle pratiche migliori e agli standard di conformità.

Tutto questo ha portato il cliente ad ottimizzare le sue risorse, aumentare il controllo sulle policy di accesso e la

visibilità su utenti, endpoint e risorse aziendali

Cosa dicono gli Analisti di Netskope ?

Netskope named a Leader in the 2024 Gartner Magic Quadrant for Security Service Edge

- Highest in *execution* and furthest in *vision*
- Netskope has been named a *Leader* by Gartner *eight years* in a row
- *THREE-peat Leader* for the SSE MQ
- Netskope received the *highest ranking* in TWO use cases in the 2024 Gartner SSE Critical Capabilities report

Gartner

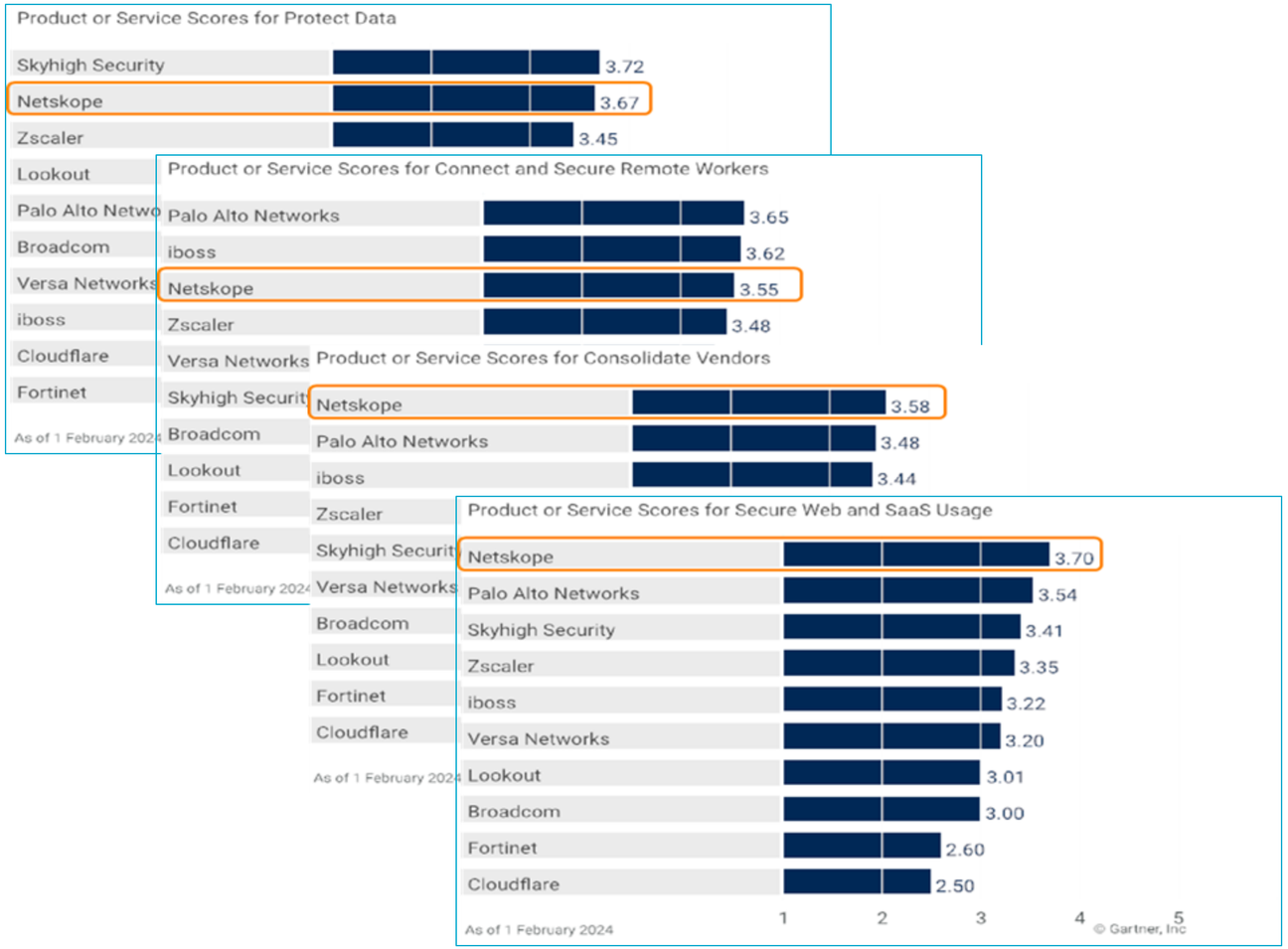
This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Netskope. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

*Gartner, Magic Quadrant for Security Service Edge, Charlie Winckless, Aaron McQuaid, John Watts, Craig Lawson, Thomas Lintemuth, Dale Koeppen, April 15, 2024

Netskope Excels in the 2024 Gartner SSE Critical Capabilities Report

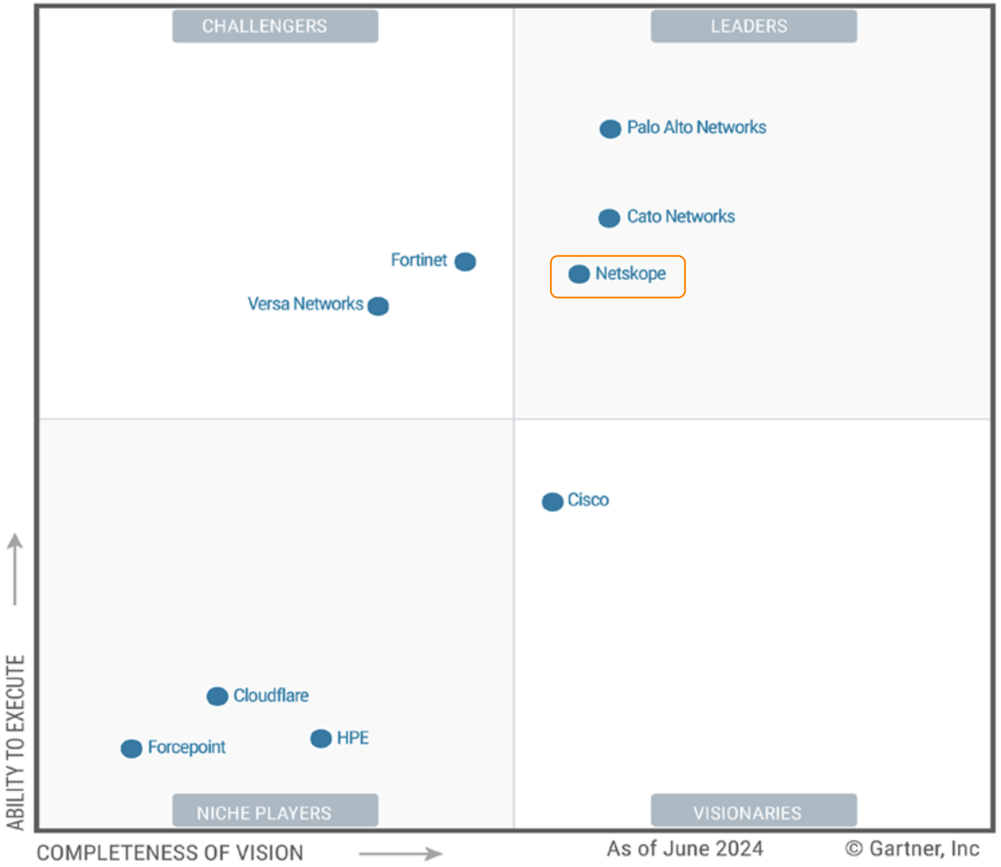
"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

The report is a reflection of vendors' capabilities today, not future looking plans.



Netskope named a Leader in the 2024 Gartner Magic Quadrant for Single-Vendor SASE

- Netskope *debuts* as a *Leader* in the first year of meeting Gartner's inclusion criteria
- Builds on Netskope's sustained *Leader* status for the *2024 SSE MQ*
- Netskope is the *only* vendor to be rated in the *top 3 spots for ALL 3 use cases* in the 2024 Gartner SASE Critical Capabilities



Gartner

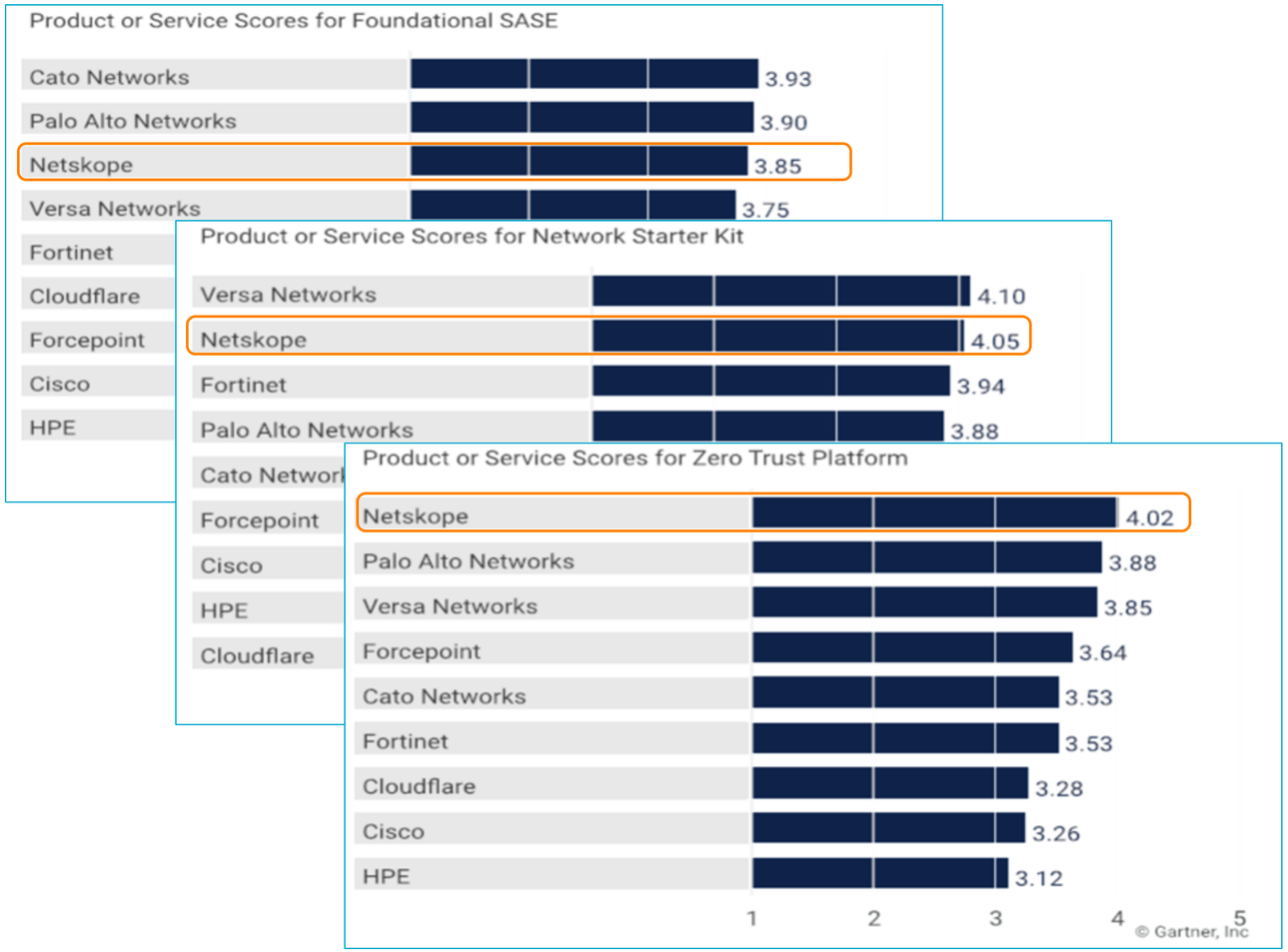
This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Netskope. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

*Gartner, Magic Quadrant for Single-Vendor SASE, Andrew Lerner, Neil MacDonald, Jonathan Forest, Charlie Winckless, July 3, 2024.

Netskope Excels in the 2024 Gartner Single-Vendor SASE Critical Capabilities Report

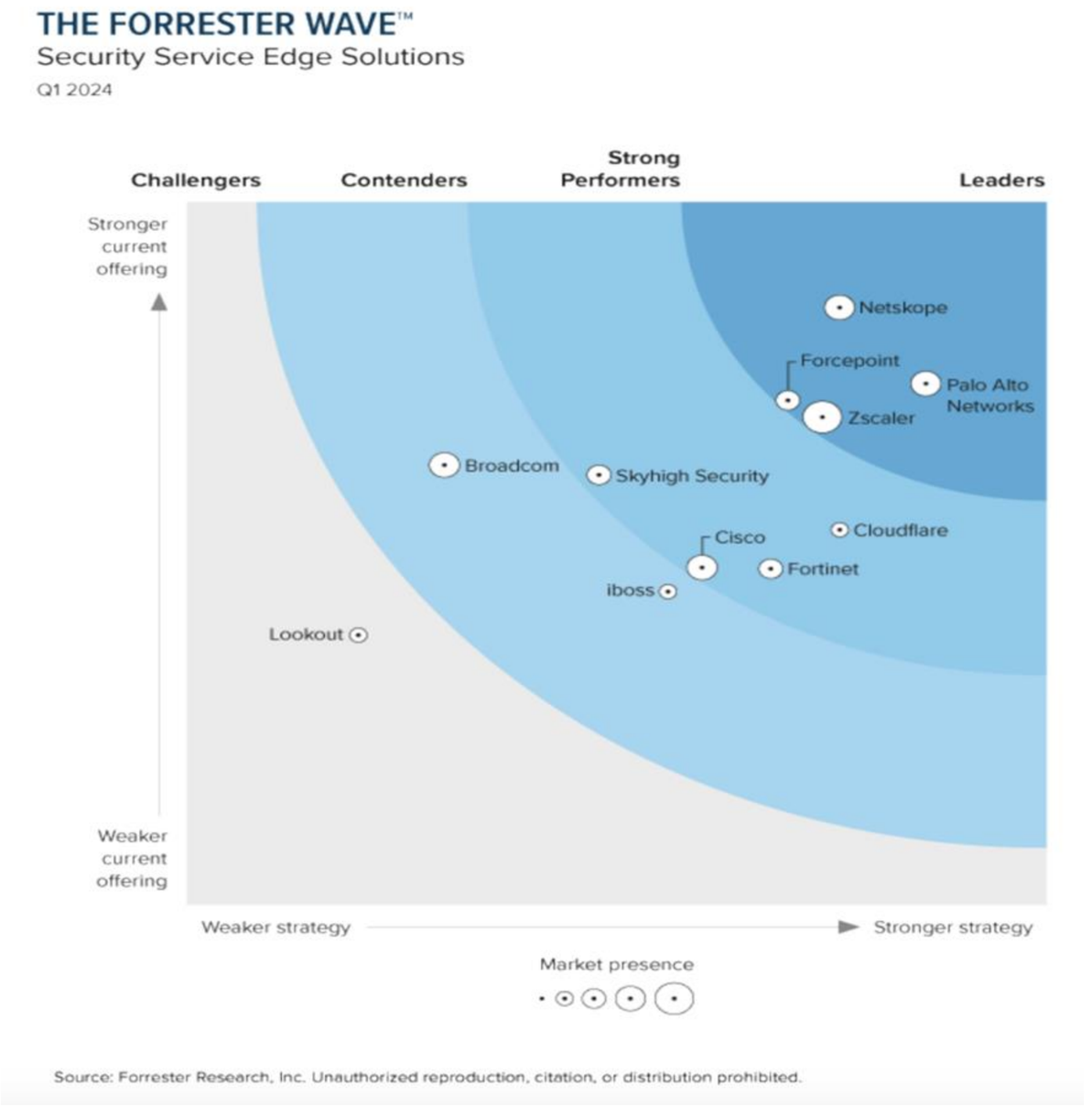
"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

The report is a reflection of vendors' capabilities today, not future looking plans.



Netskope Named a “Leader” in the 2024 Forrester Wave™ for Security Service Edge Solution

- Named a Leader
- Highest Ranking for in the current offering category
- First SSE WAVE with 25 criteria

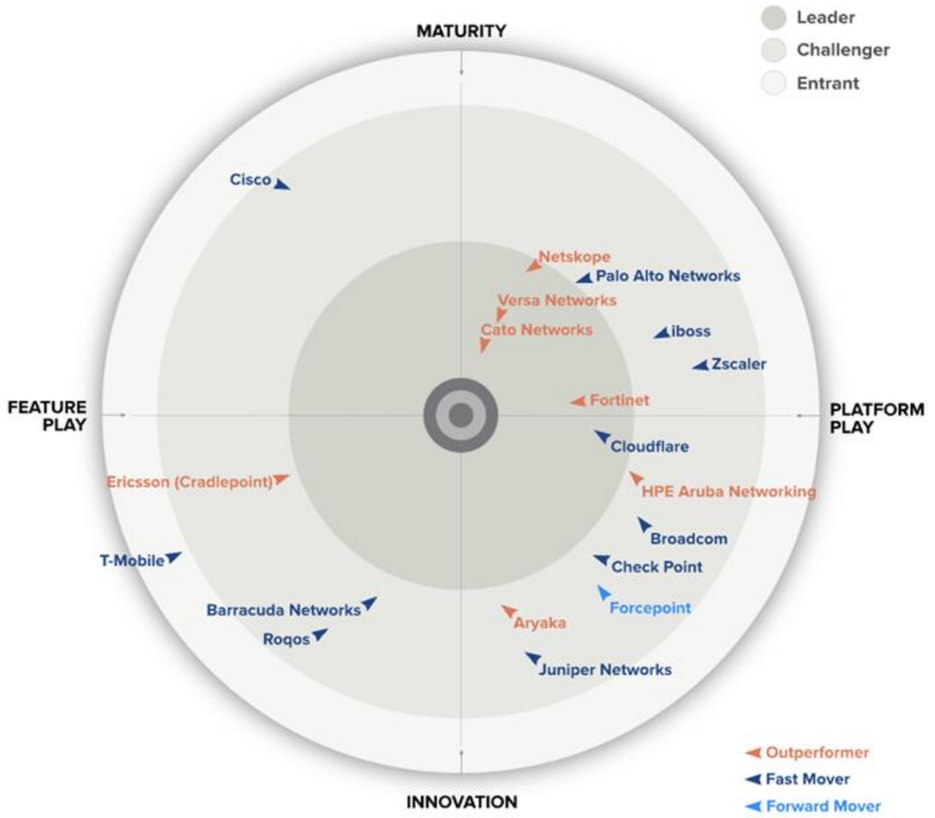


Netskope Named a “Outperformer” in the 2025 GigaOM Radar for Secure Access Service Edge (SASE)

Strengths

Netskope scored well on several decision criteria, including:

- Integrated SASE architecture: Netskope One SASE offers a fully converged, cloud-native platform that unifies core SASE components through its Zero Trust Engine. Incorporating best-in-class security and networking technologies into a converged solution with built-in zero-trust services, the architecture seamlessly integrates SD-WAN, SSE, CASB, cloud firewall, Next Generation Secure Web Gateway (NG-SWG), and ZTNA, providing context-aware functionalities for risk reduction and connectivity optimization.
- Next-generation security: The platform includes ML-powered DLP for accurate data detection and classification across all environments. The Zero Trust Engine provides contextual awareness across multiple variables, enabling adaptive, least-privileged access and real-time user coaching. This AI-driven approach allows for continuous monitoring and policy refinement based on emerging risks.
- Comprehensive threat prevention: Netskope Active Threat Protection offers a 360-degree view of cloud app usage, combining threat intelligence, static and dynamic analysis, and ML-based anomaly detection with prioritized threat protection, sandboxing, and zero-day threat intelligence feeds. It supports both standard and advanced threat engines, covering a wide range of threats from traditional malware to sophisticated advanced persistent threats (APTs) and fileless attacks, with real-time blocking capabilities and global threat sharing within the Netskope Cloud.
- Netskope is categorized as an Outperformer due to its consistent innovation and rapid integration of new capabilities, which outpace the general SASE market in feature development and strategic growth.



Q&A

Contatti:

Stefano Artioli - WW Solutions Architect, Netskope
sartioli@netskope.com

Stefano Marzi - Technical Design Security Team Leader, N&C
s.marzi@nectlc.com

Vieni a trovarci al nostro stand!