

Presentazione del modello Zero Trust Edge per la sicurezza e i servizi di rete

Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE)

A cura di David Holmes e Andre Kindness

28 gennaio 2021

Perché leggere questo report

Per supportare la digitalizzazione di un'azienda tramite il cloud e l'Internet of Things (IoT), molti team di networking si sono affidati alla SD-WAN. Tuttavia, la SD-WAN non soddisfa i nuovi requisiti di sicurezza o la funzione di forzatura che i mondi della sicurezza e del networking devono unificare. Questo report può aiutare i professionisti dei settori I&O e S&R a comprendere meglio i vantaggi di una nuova soluzione Zero Trust che permetterà di unificare l'infrastruttura di sicurezza e di rete al fine di supportare i sistemi di networking a livello aziendale.

Concetti chiave

I casi d'uso relativi alla sicurezza indurranno le aziende ad adottare il modello ZTE

Il caso d'uso iniziale per la maggior parte delle aziende che intraprendono un percorso di transizione al modello Zero Trust Edge consisterà nel garantire la sicurezza dei lavoratori da remoto, eliminando al tempo stesso la necessità di utilizzare le complicate VPN che attualmente imperversano nel settore.

Lo stack di sicurezza ospitato nell'edge Internet è il Santo Graal, ma siamo ancora agli inizi

Il modello ZTE aspira a essere uno stack di sicurezza completo ospitato su cloud o edge, ma la tecnologia non è ancora totalmente disponibile in quanto esistono altre dipendenze. Finché la larghezza di banda costituirà un fattore limitante in molte parti del mondo, alcuni elementi dovranno risiedere necessariamente in locale.

L'efficienza dell'edge on-premise intelligente non va sottovalutata

I casi d'uso relativi alla capacità di adottare decisioni intelligenti dall'edge on-premise sono ancora validi, in particolare per l'IoT/OT, l'assistenza sanitaria e gli ambienti che fanno uso intensivo della rete.

Presentazione del modello Zero Trust Edge per la sicurezza e i servizi di rete

Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE)

A cura di [David Holmes](#) e [Andre Kindness](#)

Con la collaborazione di [Glenn O'Donnell](#), [Joseph Blankenship](#), [Paul McKay](#), [Renee Taylor](#) e [Peggy Dostie](#)

28 gennaio 2021

Sommario

- 2 **La convergenza di sicurezza e networking è la chiave per il futuro delle aziende**
Gli approcci tradizionali alla sicurezza e al networking non supportano l'azienda distribuita
- 5 **L'emergere del modello Zero Trust Edge**
Sorpresa! Il modello ZTE inizia nel cloud
Uso delle soluzioni ZTE per distribuire 18 servizi di sicurezza e networking
- 10 **I casi d'uso determinano le tipologie e le ubicazioni dei servizi ZTE**
- 15 **Il mercato offre diverse tipologie di soluzioni ZTE**
Stack multi-vendor o soluzioni single-vendor a seconda delle esigenze
La scelta di un overlay basato su agenti o di un gateway senza agenti dipende dalla complessità
- 17 **Ostacoli sulla strada verso l'approccio Zero Trust Edge**

Che cosa significa

- 17 **La sicurezza e il networking si alleano contro un nemico comune**
- 18 **Materiale supplementare**

Documenti di ricerca correlati

[Evaluate SDWAN Services Based On Branch Office Goals, Not Hardware Data Sheets](#)

[Now Tech: Software-Defined WAN Hardware/Software, Q3 2020](#)

[Now Tech: Software-Defined WAN Services, Q3 2020](#)



Condividi i report con i colleghi.

Migliora la tua partecipazione con Research Share.

FORRESTER

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 Stati Uniti
+1 617-613-6000 | Fax: +1 617-613-5000 | [forrester.com](#)

© 2021 Forrester Research, Inc. Le opinioni espresse riflettono il giudizio al momento della redazione del documento e sono soggette a modifiche. Forrester®, Technographics®, Forrester Wave, TechRadar e Total Economic Impact sono marchi di Forrester Research, Inc. Tutti gli altri marchi sono di proprietà delle rispettive società. La copia o la distribuzione non autorizzata costituisce una violazione della legge sul copyright. Citations@forrester.com oppure +1 866-367-7378

Presentazione del modello Zero Trust Edge per la sicurezza e i servizi di rete

Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE)

La convergenza di sicurezza e networking è la chiave per il futuro delle aziende

Il networking e la sicurezza hanno una lunga e complessa storia, che può essere definita cordiale nell'ipotesi migliore o decisamente ostile nel peggiore dei casi. Tuttavia, questo approccio separato non è un modo accettabile di operare e spesso compromette i vantaggi derivanti dalle iniziative digitali. Le infrastrutture e le operazioni di rete e sicurezza rigidamente separate stanno rapidamente scomparendo per i motivi illustrati di seguito.

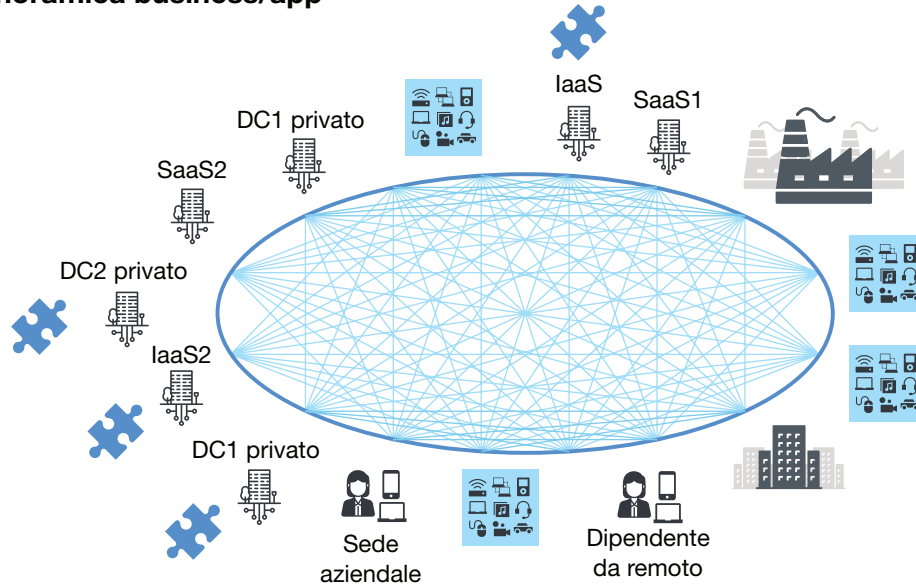
- **Le applicazioni e i dati distribuiti nel cloud si trovano al di fuori del "castello" del data center.** Non soltanto il cloud, l'edge e l'IoT stanno ridefinendo la posizione dei dati e delle applicazioni, ma questi componenti della digitalizzazione hanno definitivamente mandato in pensione il tradizionale modello di rete hub-and-spoke.¹ Ora un'infrastruttura di rete a livello aziendale interconnette asset, clienti, partner e risorse digitali per collegare tutti gli elementi dell'ecosistema aziendale (vedere la Figura 1).² Come sottolineato nel report di Forrester "[Build Security Into Your Network's DNA: The Zero Trust Network Architecture](#)", ciò può avvenire soltanto se la sicurezza è parte integrante del DNA della rete.
- **Il COVID-19 ha spinto i dipendenti fuori dal controllo della LAN aziendale.** Basti pensare al semplice fatto che molte applicazioni aziendali ora risiedono nel cloud e il loro numero è in costante aumento. Anche gli utenti hanno ormai abbandonato il tradizionale perimetro aziendale; dal sondaggio realizzato da Forrester sull'esperienza pandemica, è emerso che il 53% dei lavoratori in modalità agile desiderava continuare a lavorare da remoto anche dopo il superamento della crisi.³ Poiché sia le applicazioni sia gli utenti non sono più protetti, l'utilità e il valore di uno stack di sicurezza "fortificato" sono venuti meno.

Presentazione del modello Zero Trust Edge per la sicurezza e i servizi di rete

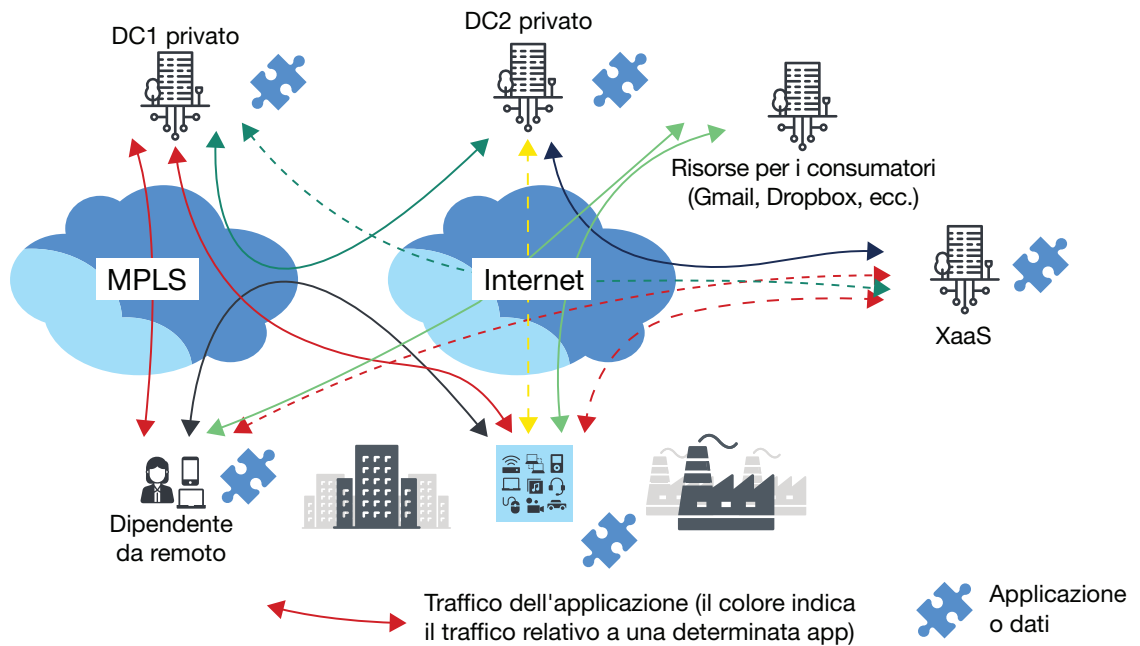
Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE)

FIGURA 1 La dispersione delle applicazioni e dei dati tra le risorse aziendali

Panoramica business/app



Panoramica I&O



Presentazione del modello Zero Trust Edge per la sicurezza e i servizi di rete

Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE)

Gli approcci tradizionali alla sicurezza e al networking non supportano l'azienda distribuita

A causa della pandemia del 2020, milioni di dipendenti sono stati costretti ad abbandonare il comodo rifugio del perimetro aziendale per entrare nella giungla selvaggia del lavoro da remoto. Un CISO di una grande compagnia assicurativa europea ci ha riferito che, prima della pandemia del 2020, solo il 5% dei dipendenti lavorava da remoto. La pandemia ha capovolto la percentuale e, ora, i dipendenti che lavorano da casa costituiscono il 95% dell'organico. Per questo tipo di società, l'infrastruttura VPN, già poco sicura, non è in grado di sostenere il carico. La tecnologia VPN è solo un'altra crepa nelle mura già erose del castello. I team di networking e sicurezza hanno avuto difficoltà a soddisfare i nuovi requisiti necessari per utilizzare il cloud e supportare i telelavoratori, dal momento che gli approcci tradizionali si basavano sui presupposti seguenti:

- **Appliance software o hardware dedicate in loco.** Sono ormai lontani i giorni in cui si adottava una soluzione specifica per risolvere un determinato problema tecnologico. Trent'anni di dispositivi connessi alla rete, come gli ottimizzatori WAN o i firewall, hanno comportato maggiori problemi di sicurezza, livelli di complessità più elevati, minore flessibilità ed efficienza ridotta. Ogni nuovo dispositivo aumenta esponenzialmente la complessità e i potenziali problemi di sicurezza.
- **Repository di policy e controlli on-premise inaffidabili.** Il software di gestione in loco necessita di hardware specifico e personale dedicato affinché sia sempre aggiornato con le funzionalità, le correzioni di bug e i miglioramenti di sicurezza più recenti. Il software di gestione che risiede all'interno di un'infrastruttura privata non soltanto è oneroso per l'azienda, ma ne ostacola le capacità di resilienza. Il software, in genere, non è stato progettato per essere trasferito sulle piattaforme cloud, il che limita la sua efficacia e la flessibilità delle opzioni di disaster recovery.
- **Un approccio incentrato sull'hardware che presenta dei limiti.** Aerei, automobili e treni devono rispettare delle restrizioni progettuali a causa dei vincoli di peso o dimensioni. Anche in assenza di questi vincoli, i team tecnologici non possono pensare di installare hardware in ogni parte di un sito di produzione, di un punto vendita o di uno stadio. È impossibile ipotizzare che l'hardware possa essere costruito in modo da soddisfare i requisiti di forma, prestazioni e funzionalità necessari per inserirlo tra un estrusore di plastica e la camera di riscaldamento o per resistere alle temperature di funzionamento di apparecchiature installate in luoghi come una sottostazione elettrica a Dubai o una torre cellulare nella Death Valley.
- **Sicurezza frammentaria e networking in silos.** La pratica di relegare determinate operazioni e tipologie di hardware a gruppi specifici non fa che accrescere le inefficienze operative, ridurre la resilienza dell'infrastruttura e aprire potenzialmente la porta a nuovi problemi di sicurezza. Molti dispositivi discreti, come firewall e router, possono essere combinati per ridurre la latenza utilizzando un'unica tabella per la ricerca delle regole per i pacchetti e applicando policy di sicurezza e di rete al punto di ingresso.

Presentazione del modello Zero Trust Edge per la sicurezza e i servizi di rete

Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE)

L'emergere del modello Zero Trust Edge

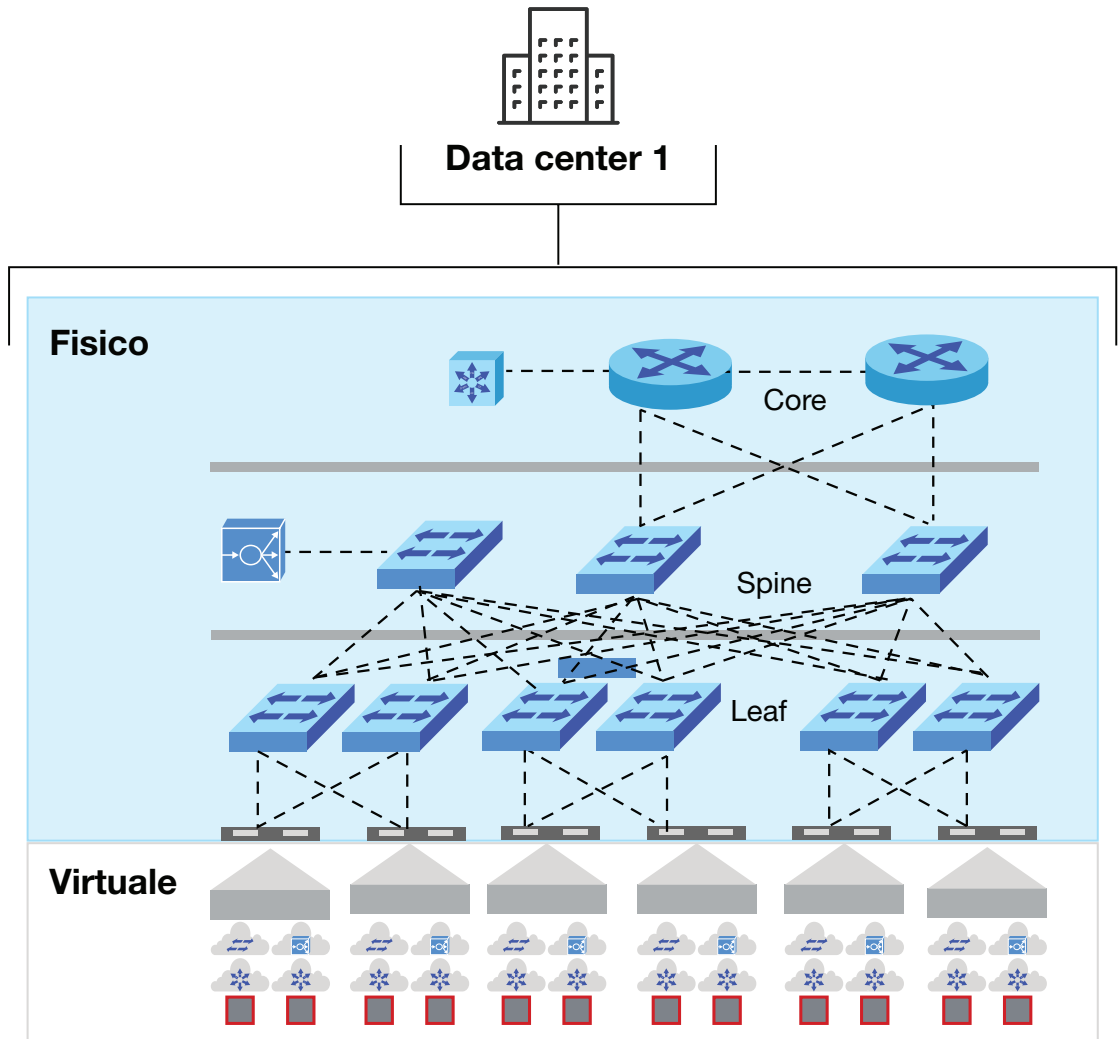
Quando la pandemia da COVID-19 ha costretto i dipendenti a lavorare da casa, una minoranza lungimirante di professionisti della sicurezza, convinti che la tecnologia VPN non fosse la scelta migliore, ha investito in soluzioni Zero Trust Network Access (ZTNA) per aggirare i problemi riscontrati con le VPN; tra coloro che avevano scelto di seguire il percorso ZTNA, alcuni si sono chiesti se esistessero altri approcci ZT che avrebbero potuto adottare, dal momento che molti professionisti della sicurezza e dell'I&O consideravano il modello Zero Trust come un concetto prevalentemente legato ai data center (vedere la Figura 2).⁴ Tuttavia, il framework di sicurezza illustrato nel report di Forrester "The Zero Trust eXtended (ZTX) Ecosystem" mostra perché il modello ZT è un concetto che non riguarda soltanto i data center. ZT protegge le aziende da clienti, dipendenti, collaboratori e dispositivi che si connettono da remoto attraverso la rete WAN a un ambiente più aggressivo, aperto, pericoloso e turbolento (vedere la Figura 3). Forrester esprime questo concetto con il termine "Zero Trust Edge" (ZTE) e lo definisce nel modo seguente:

Una soluzione Zero Trust Edge permette di connettere e trasportare il traffico in modo sicuro, sia in entrata che in uscita, da siti remoti utilizzando i principi di accesso Zero Trust e sfruttando prevalentemente i servizi di sicurezza e networking basati su cloud.






Presentazione del modello Zero Trust Edge per la sicurezza e i servizi di rete

Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE)






FIGURA 2 I primi ad adottare il modello ZT creavano microperimetri di sicurezza solo a protezione delle macchine virtuali (VM)



Servizi virtuali

-  Macchina virtuale
-  Appliance di sicurezza virtuale
-  Switch virtuale
-  Router virtuale
-  Hypervisor

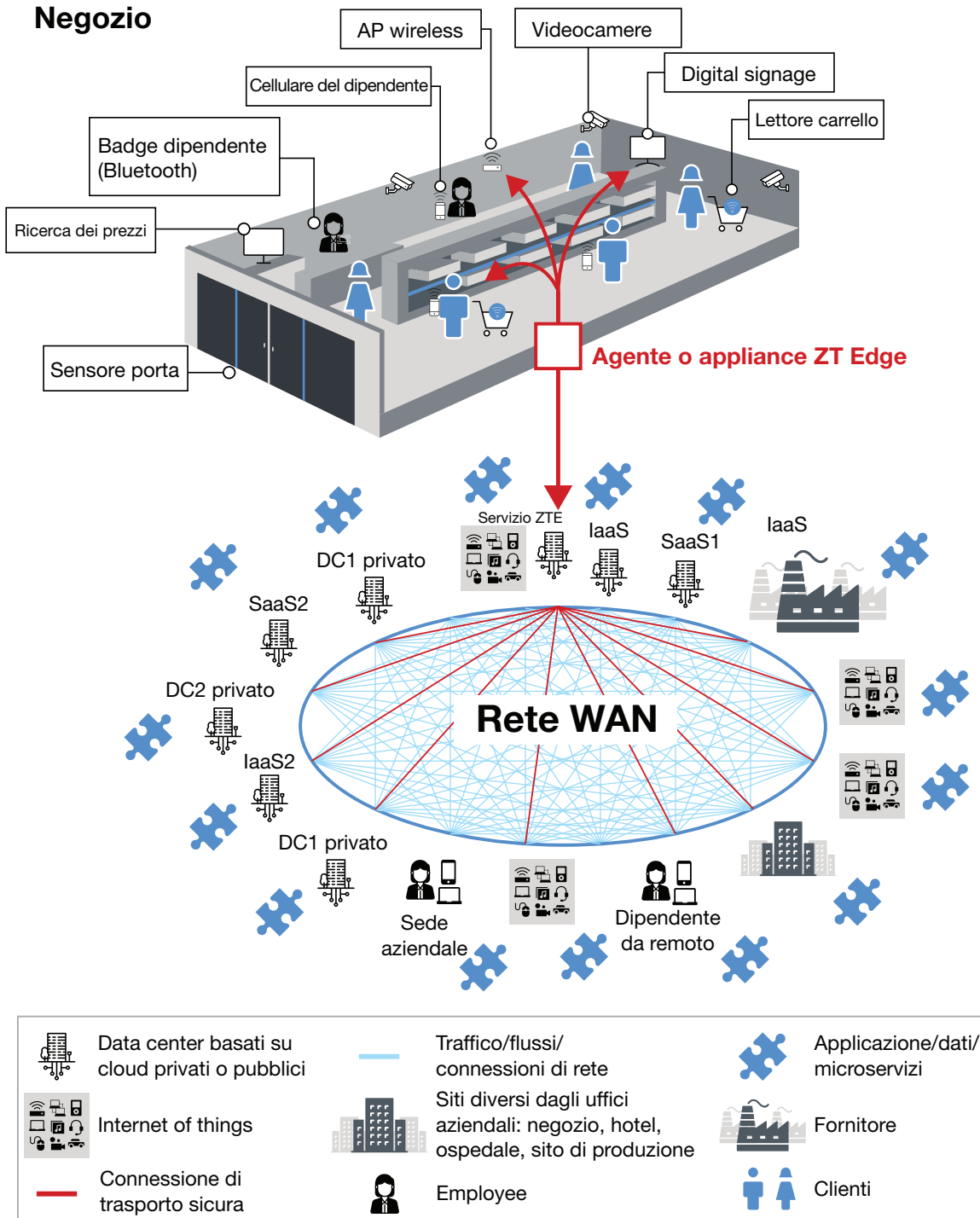
Infrastruttura fisica

-  Switch
-  Servizio di rete avanzato (gateway di segmentazione, bilanciamento del carico e altri servizi)
-  Server
-  Componente di rete (gateway del router)
-  Controlli di sicurezza

Presentazione del modello Zero Trust Edge per la sicurezza e i servizi di rete

Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE)

FIGURA 3 ZTE fornisce i controlli di sicurezza e le policy di rete necessari per proteggere tutte le connessioni in loco



Presentazione del modello Zero Trust Edge per la sicurezza e i servizi di rete

Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE)

Sorpresa! Il modello ZTE inizia nel cloud

L'approccio ZTE costruisce il framework di sicurezza e networking intorno al flusso di traffico e servizi proveniente da postazioni remote e in entrata nelle aziende e al flusso di servizi che viene ritrasmesso agli utenti o alle postazioni. Anche se il modello ZTE è concepito in funzione delle esigenze di un'azienda distribuita, le soluzioni, che garantiscono una serie di servizi più rapidi e agili, devono essere basate su due elementi fondamentali:

- **Gestione della sicurezza e della rete basata su cloud.** In passato, le configurazioni dei dispositivi e le policy di sicurezza erano contenute in strumenti diversi. Ad esempio, i controlli dell'accesso alla rete fornivano le policy di sicurezza per gli utenti, mentre le soluzioni di gestione per i firewall e i componenti di rete contenevano le configurazioni dei dispositivi. Questa situazione comporta un maggior rischio di errori di configurazione e riduce l'efficienza operativa, in quanto il personale deve impostare policy analoghe in più sistemi diversi. La gestione basata su cloud consente di unificare questi sistemi back-end diversi e di modificare, aggiungere o eliminare le configurazioni in base a un'unica soluzione di gestione della configurazione.
- **Monitoraggio e analisi basati su cloud.** In genere, il monitoraggio della rete e quello della sicurezza sono reciprocamente indipendenti ed entrambi sono requisiti essenziali per il funzionamento del modello ZTE. Google è un buon esempio: utilizza la sua WAN definita dal software per incrementare l'utilizzo dei link fino al 100%. Il monitoraggio identifica eventuali irregolarità nel traffico, spesso dovute a problemi di sicurezza, fino ai nodi metro di peering e in posizioni distanti dai data center aziendali.⁵ La quantità di informazioni da raccogliere e sintetizzare richiede che il monitoraggio ZTE sia basato sul cloud. Necessita di una piattaforma di calcolo molto estesa per supportare l'intera gamma di analisi.

Uso delle soluzioni ZTE per distribuire 18 servizi di sicurezza e networking

Da qualsiasi angolo del mondo le organizzazioni possono gestire, monitorare e analizzare centralmente la serie di servizi di sicurezza e networking disponibili nelle soluzioni ZTE (vedere la Figura 4). Alcuni dei servizi risiederanno esclusivamente nel cloud (o nell'edge del cloud), mentre altri dovranno essere ospitati in una posizione remota.

Presentazione del modello Zero Trust Edge per la sicurezza e i servizi di rete

Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE)

FIGURA 4 Tipi di servizi disponibili in una soluzione ZTE

Rete	
Larghezza di banda garantita	Imposta una quantità minima di larghezza di banda per un determinato tipo di traffico
Memorizzazione dei contenuti nella cache	Fornisce copie localizzate dei dati
Bilanciamento e utilizzo dei collegamenti	Utilizza più collegamenti contemporaneamente per aumentare la larghezza di banda del traffico e l'utilizzo complessivo della WAN
Qualità del servizio	Assegna la priorità al traffico di rete
Resilienza	Fornisce e mantiene un livello di servizio accettabile in caso di guasti e difficoltà di funzionamento.
Routing/percorso migliore	Seleziona il percorso corretto per il trasporto di livello 3 anche dal telelavoratore a un'applicazione ospitata su cloud
WAN definita da software (SD-WAN)	Consente di scegliere i percorsi, i collegamenti o le connessioni migliori in base a metriche di livello superiore, come jitter, pacchetti interrotti e affinità con un profilo di applicazione
Connessione WAN	Stabilisce il collegamento fisico verso/da una struttura
Ottimizzazione WAN	Fornisce deduplicazione, unione dei pacchetti e altre funzioni di ottimizzazione della WAN

Presentazione del modello Zero Trust Edge per la sicurezza e i servizi di rete

Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE)

FIGURA 4 Tipi di servizi disponibili in una soluzione ZTE (Continua)

Sicurezza	
Firewall di base	Offre semplici funzionalità firewall di rete (regole dei livelli 3 e 4) che possono essere separate e spostate localmente per ridurre la quantità di traffico in uscita dalla struttura remota
Cloud Access Security Broker (CASB)	Controlla e genera report sull'accesso alle applicazioni cloud
Firewall as-a-service (FWaaS)	Fornisce funzionalità firewall avanzate basate su cloud
Sistema di rilevamento delle intrusioni/Sistema di prevenzione delle intrusioni (IDS/IPS)	Analizza il traffico di rete in base alle firme per rilevare e deviare contenuti dannosi specifici
Crittografia del collegamento	Codifica e decodifica tutto il traffico di rete in ogni punto di diramazione
Gestione dell'identità e degli accessi (IAM)	Garantisce la corretta assegnazione ai dipendenti del diritto di accedere alle risorse tecnologiche appropriate
Gateway Web sicuro (SWG)	Impedisce che il traffico non protetto penetri nella rete interna di un'organizzazione. I filtri URL devono essere costantemente aggiornati e la tendenza è già quella di configurarli, ospitarli e mantenerli nel cloud
Analisi avanzata dei malware	Esegue programmi in un ambiente isolato (sandboxing) per filtrare e intercettare tipi di malware zero-day
Accesso alla rete Zero Trust (ZTNA)	Consente al telelavoratore di connettersi alle applicazioni aziendali in base alla propria identità, indipendentemente dal luogo in cui si trova il dipendente o l'applicazione. Si tratta del servizio di sicurezza basato su firme che deve essere presente nella soluzione ZTE.

I casi d'uso determinano le tipologie e le ubicazioni dei servizi ZTE

Gli architetti della rete e della sicurezza devono garantire la massima utilità nel momento in cui adottano una soluzione Zero Trust Edge. I tipi di servizi utilizzati dipendono dalla posizione, dai dispositivi, dalle persone e da altri elementi (vedere la Figura 5). Tre casi d'uso mostrano un incremento dei livelli delle funzioni di forzatura (il che significa che un maggior numero di servizi di networking e sicurezza vengono attivati all'interno della soluzione ZTE):

- **Garantire la sicurezza dei lavoratori remoti come primo caso d'uso.** La pandemia del 2020, con il conseguente esodo di massa dei lavoratori dagli uffici, ha costretto milioni di knowledge worker a lavorare da casa. La necessità di fornire un accesso sicuro ai servizi e alle applicazioni aziendali ai lavoratori da remoto è il primo caso d'uso che ha indotto le aziende ad adottare una

Presentazione del modello Zero Trust Edge per la sicurezza e i servizi di rete

Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE)

strategia Zero Trust Edge. Alla luce delle numerose difficoltà evidenziate nello studio di Forrester "[Key Considerations For Network And Capacity Management When Operationalizing A Home-Based Workforce](#)", gran parte delle aziende ha rinunciato a concentrare in sede tutte le sue risorse hardware e software. Al contrario, gli agenti software vengono distribuiti sui dispositivi di lavoro dei dipendenti, i quali si connettono ai servizi di sicurezza sull'edge del cloud (vedere la Figura 6).

- **Dare priorità al traffico generato dalle applicazioni aziendali che affolla la WAN delle filiali.**

Il numero di connessioni WAN è aumentato in modo esponenziale a causa dell'enorme diffusione del lavoro da remoto. Gran parte del traffico sulle WAN aziendali, tuttavia, è dovuto alle connessioni degli uffici remoti, in particolare quelle dei dipendenti, delle loro applicazioni e dei dispositivi aziendali. Il traffico SaaS, come quello di O365, è recentemente diventato un fattore importante e spesso comprende una parte del traffico dei clienti. Il traffico delle applicazioni basato su SaaS richiede connessioni dirette a Internet e i clienti possono avere la necessità di connettersi alle reti LAN degli uffici remoti. Per affrontare queste sfide, gli architetti aziendali stanno indirizzando sempre più questo traffico attraverso i firewall as-a-service (FWaaS). Ciò avviene mediante i router degli uffici remoti e/o le soluzioni SD-WAN illustrate nel report di Forrester "[Now Tech: Software-Defined WAN Hardware/Software, Q3 2020](#)" o tramite uno dei provider di servizi elencati nel report di Forrester "[Now Tech: Software-Defined WAN Services, Q3 2020](#)" (vedere la Figura 7). Alcuni fornitori, come Forcepoint, supportano la funzionalità SD-WAN integrata con più servizi di sicurezza.

- **Infine, garantire la sicurezza dell'Internet of Things.** Oltre ai lavoratori da remoto e agli uffici periferici in generale, la rete è utilizzata da dispositivi edge e IoT e dai partner aziendali. Gli architetti dei sistemi di controllo industriale (ICS, Industrial Control System) dovranno tenere conto di tutte le postazioni che richiedono una maggiore attenzione in termini di policy di sicurezza e di networking. Ad esempio, un ingegnere di uno stabilimento di produzione di auto deve considerare il traffico generato da dipendenti e appaltatori, ma deve anche tenere conto del traffico proveniente dai PLC (Programmable Logic Controller) di Siemens o dai sistemi di comunicazione del peso degli scaffali per il controllo dell'inventario di Bosch. A seconda dell'ubicazione e della disponibilità di banda presso il sito, alcuni elementi di sicurezza di base devono essere ospitati in loco, unitamente a tutti i servizi di networking, per ridurre il traffico indirizzato verso i servizi di sicurezza basati su cloud (vedere la Figura 8).

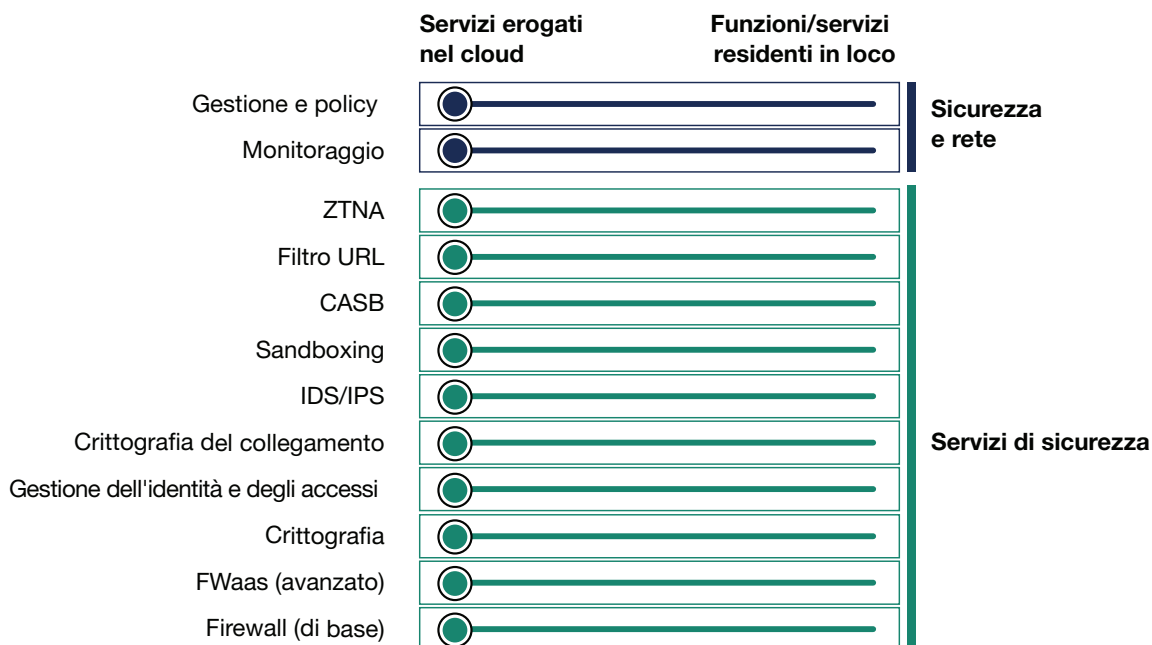
Presentazione del modello Zero Trust Edge per la sicurezza e i servizi di rete

Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE)

FIGURA 5 Per ogni caso è necessario considerare una serie di fattori diversi a livello di sicurezza e networking

	Lavoro da remoto	Piccolo ufficio	Qualsiasi sito
Risorse	Computer portatile	Desktop, stampanti, sale conferenze, webcam	Rete fisica eterogenea
Gateway alla soluzione ZTE	Agente endpoint	Dispositivo WAN con i servizi di rete in loco richiesti o overlay tramite agente	Dispositivo WAN con i servizi di rete in loco richiesti
IoT	No	Basso	Elevato
Elaborazione nell'edge	No	Basso	Elevato
Appaltatori	No	No	Sì
Fornitori di tecnologie e servizi aziendali	No	Basso	Elevato

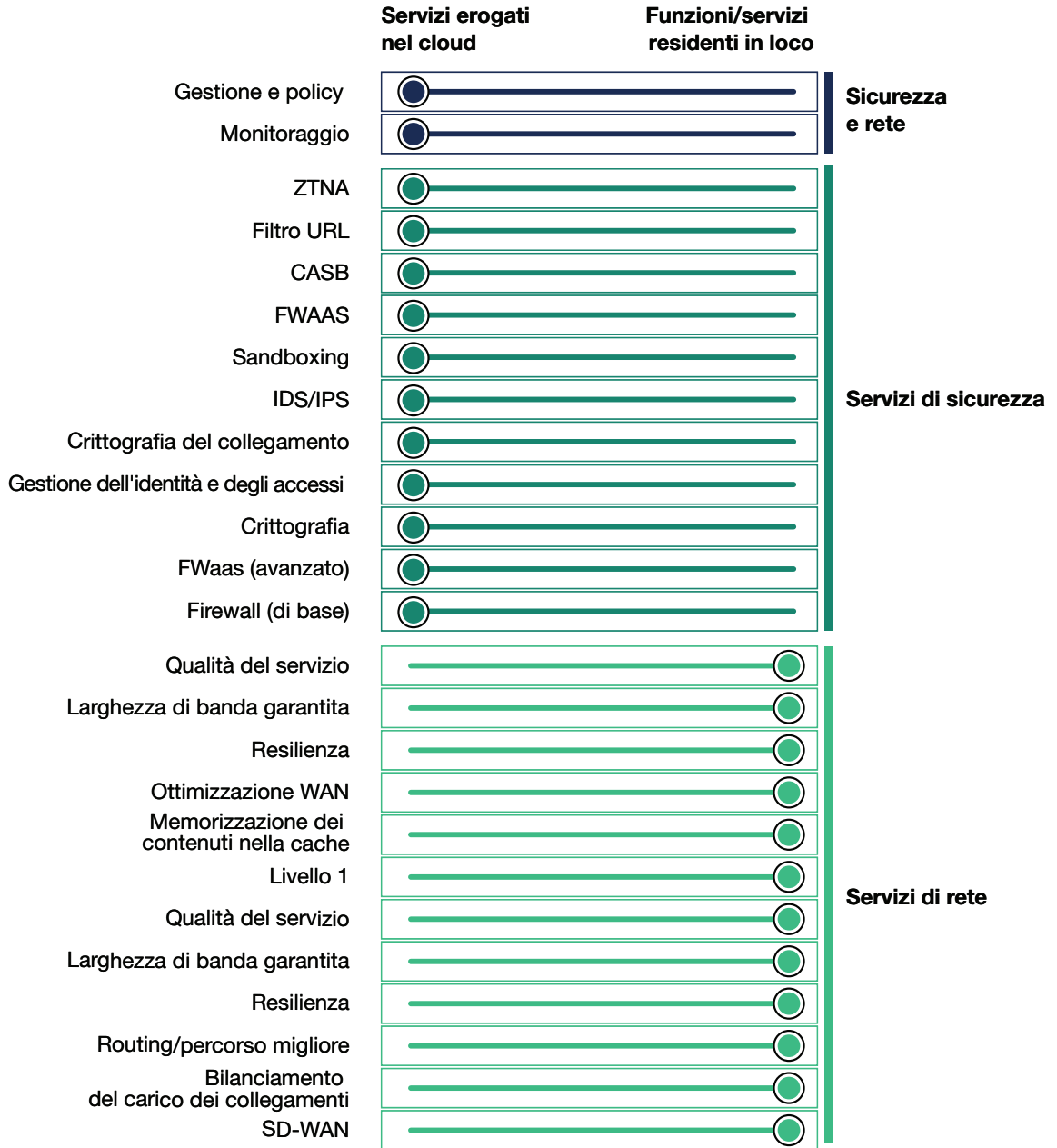
FIGURA 6 I telelavoratori beneficiano dei servizi di sicurezza ZTE basati su cloud



Presentazione del modello Zero Trust Edge per la sicurezza e i servizi di rete

Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE)

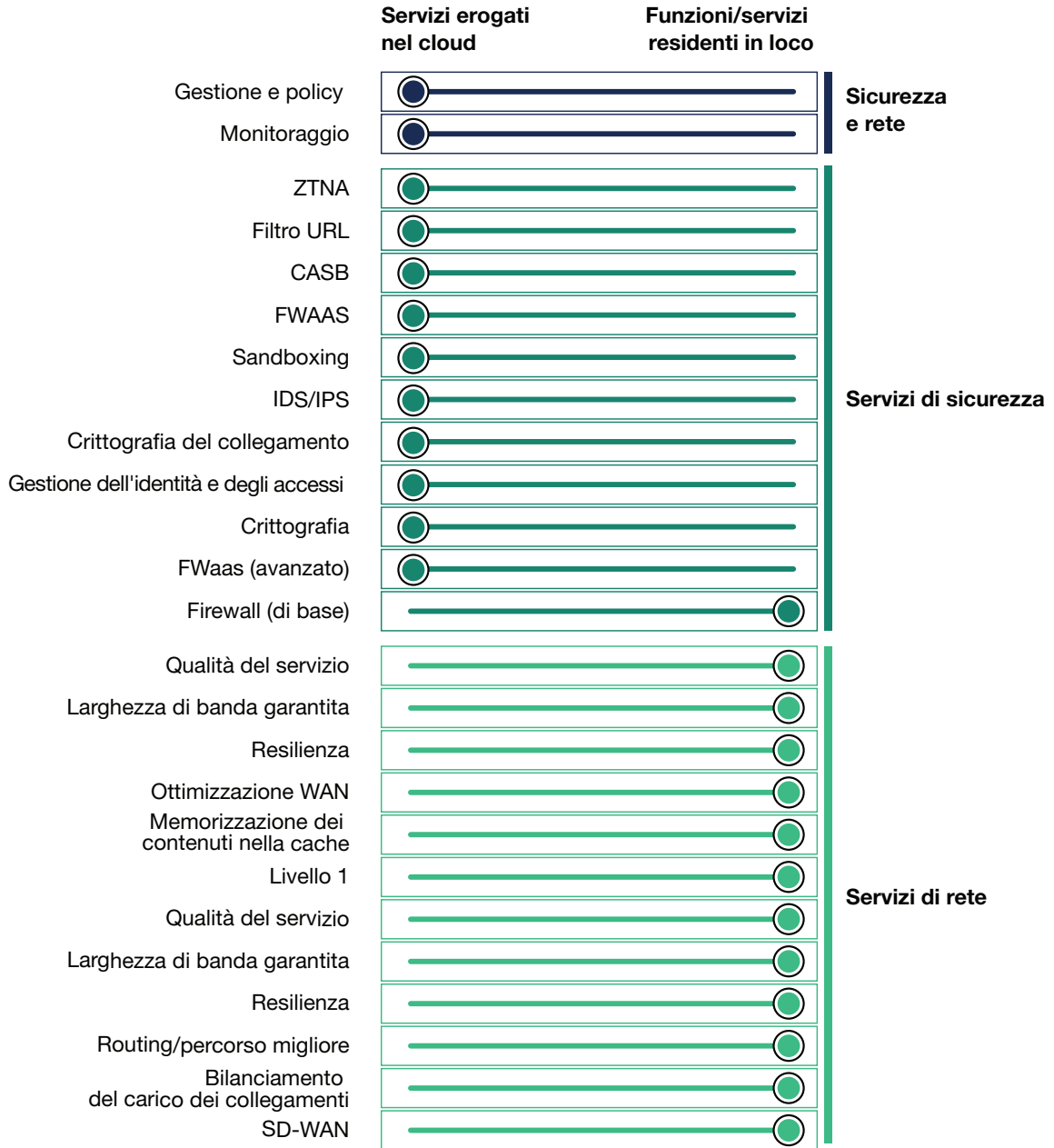
FIGURA 7 Gli uffici aziendali generici indirizzano il traffico verso servizi di sicurezza basati su cloud



Presentazione del modello Zero Trust Edge per la sicurezza e i servizi di rete

Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE)

FIGURA 8 Per i siti complessi con larghezza di banda WAN limitata, è necessario che alcune funzionalità di sicurezza risiedano in locale



Presentazione del modello Zero Trust Edge per la sicurezza e i servizi di rete

Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE)

Il mercato offre diverse tipologie di soluzioni ZTE

I professionisti della tecnologia possono utilizzare il modello ZTE in tre modalità diverse:

- **Servizio erogato tramite cloud.** Commercializzati da un numero relativamente ristretto di fornitori, i servizi ZTE basati su cloud sono erogati da provider di servizi gestiti, come Cato Networks, che utilizzano una rete di terze parti con decine, o in alcuni casi centinaia, di POP che offrono funzionalità ZTE cloud-edge. Questo approccio offre tutto il valore che le organizzazioni possono ottenere dalle soluzioni software as-a-service. Tuttavia, nessuna azienda è in grado di fornire tutte le funzionalità offerte dalle soluzioni migliori. Forrester ha riscontrato che le organizzazioni non utilizzano, in genere, tutte le funzionalità disponibili nelle soluzioni on-premise. Le soluzioni basate su cloud spesso sono in grado di soddisfare le esigenze di molte organizzazioni.
- **Servizi ZTE supportati da un servizio di connessione WAN.** Altre soluzioni includono un provider di reti di telecomunicazione già esistente che collega i propri clienti direttamente alle reti ZTE per le funzioni di sicurezza esternalizzate. Attualmente, Comcast Enterprise e Akamai già offrono questa funzione. Molti fornitori di hardware e software SD-WAN, come Versa Networks, collaborano con Zscaler o altri fornitori di sistemi di sicurezza. I team possono scegliere i prodotti migliori per ottenere il massimo dai servizi di sicurezza e networking. Tuttavia, questi team non otterranno l'agilità operativa o l'efficienza dei sistemi basati su cloud. Un approccio di tipo wrapper SD-WAN e ZTE richiede ulteriori interventi da parte dei team tecnologici, come l'impostazione di policy per ogni servizio indipendente. Non esiste un unico sistema di gestione e orchestrazione per una strategia wrapper SD-WAN e ZTE.
- **Un approccio "do-it-yourself" (DIY).** Un'organizzazione sufficientemente grande e agile potrebbe creare la propria piattaforma ZTE utilizzando provider di servizi cloud come POP e un servizio ospitato su cloud, ad esempio il firewall aziendale di Barracuda, come servizio di sicurezza nel cloud Azure di Microsoft. In questo modo, i servizi possono soddisfare meglio le esigenze aziendali, ma è necessario che i team abbiano un'ottima conoscenza dei requisiti aziendali e sappiano con chiarezza quali sono le competenze necessarie per creare e gestire l'infrastruttura. Dal report di Forrester "[Evaluate SD-WAN Services Based On Branch Office Goals, Not Hardware Data Sheets](#)" emerge che gran parte dei team è carente sotto alcuni aspetti.

Stack multi-vendor o soluzioni single-vendor a seconda delle esigenze

Poiché il modello ZTE rappresenta una minaccia per l'esistenza stessa di molte soluzioni di sicurezza on-premise, la strategia ZTE è ora diventata essenziale per questi fornitori. I fornitori ambiziosi puntano a vendere pacchetti completi "chiavi in mano" (se sono in grado di offrirli) e l'idea di servirsi di un fornitore unico per tutte le soluzioni di sicurezza su base OpEx può risultare allettante per le PMI e i clienti di fascia media. La scelta dipende dalle dimensioni e dalla complessità dell'azienda:

Presentazione del modello Zero Trust Edge per la sicurezza e i servizi di rete

Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE)

- **Le organizzazioni più grandi sceglieranno un approccio multi-vendor nel breve termine.** Le aziende di dimensioni più grandi hanno requisiti più complessi e servizi più eterogenei. Il peso più gravoso delle applicazioni legacy rende meno probabile l'adozione di un approccio basato su un singolo fornitore. Le persone intervistate nell'ambito di questa ricerca concordavano ampiamente su questa analisi. Per quanto riguarda le organizzazioni che hanno già avviato un percorso Zero Trust Edge, un tipico approccio multi-vendor può utilizzare Silver Peak Systems per la connessione SD-WAN a Zscaler per il filtraggio degli URL e lo ZTNA. Questa soluzione è funzionale per il caso d'uso iniziale (sicurezza dei lavoratori remoti), ma la migrazione di altri elementi dello stack di sicurezza in uno stack multi-vendor richiederà un'efficace concatenazione dei servizi; inoltre, è necessario che le API tra i componenti funzionino in modo coerente e affidabile.
- **Le organizzazioni più piccole potranno sperimentare un approccio completo allo stack di sicurezza.** Secondo Forrester, è possibile che le aziende più piccole si rivolgano a fornitori di soluzioni ZTE complete, come Netskope. In genere, i loro requisiti sono più limitati e la scelta di affidarsi a un fornitore unico potrebbe rivelarsi vantaggiosa. L'adozione di questo tipo di soluzioni richiede storicamente più tempo ai grandi gruppi tecnologici di livello enterprise. Ad esempio, ciò si è verificato nel mercato Wi-Fi con le soluzioni basate su cloud di Aerohive Networks, ora parte di Extreme Networks, e Meraki, oggi nel gruppo Cisco.

La scelta di un overlay basato su agenti o di un gateway senza agenti dipende dalla complessità

La connessione di tutti gli utenti e le applicazioni è l'ambizioso obiettivo finale della strategia Zero Trust Edge, che si tratti di sistemi che risiedono in ambienti on-premise, nel cloud, in un cloud privato o che lavorano in remoto. Tuttavia, la connessione a una rete complessa ed eterogenea è un'impresa tutt'altro che banale. Pertanto, il mercato attualmente supporta due tipi di implementazioni, una orientata a raggiungere l'obiettivo strategico e una finalizzata a facilitare l'accesso tattico al modello Zero Trust Edge. Alcuni fornitori, come Zscaler, possono supportare entrambi i modelli contemporaneamente e un numero sempre più consistente di fornitori si sta muovendo nella stessa direzione.

- **Modello uno: un gateway è l'unico punto di sicurezza.** Questo modello prevede un unico punto di accesso a Internet, come nel caso di un controller SD-WAN con un tunnel GRE che consente la connessione a una rete edge ospitata da un fornitore. Tutto il traffico in uscita viene convogliato sulla rete edge, che può quindi assegnare immediatamente delle policy di sicurezza al traffico di un determinato tenant nella rete. La superficie di esposizione alle minacce si riduce drasticamente, rendendo gli attacchi DDoS un problema altrui. È più probabile che questa opzione, sicuramente più lineare, venga adottata da un mercato di fascia media in quando non praticabile, nel breve termine, per ambienti eterogenei complessi.
- **Modello due: un overlay distribuisce le soluzioni di sicurezza, in genere tramite agenti.** In questo modello, gli endpoint si connettono alla rete edge tramite un overlay, generalmente supportato da un agente endpoint che stabilisce quali connessioni devono essere reindirizzate alla rete ZTE. Il modello overlay può essere implementato senza modificare la rete sottostante. Questa soluzione, tuttavia, presenta un serio inconveniente. L'installazione degli agenti, infatti, potrebbe non essere possibile a causa delle policy applicate in ambienti sensibili, come quello della sanità, della produzione e dell'IT/OT. Axis Security ha un approccio innovativo che utilizza il modello overlay senza richiedere la presenza di agenti sui dispositivi che desiderano connettersi alla rete. Abbiamo intervistato un cliente importante che ha scelto la soluzione Axis Security proprio per questo motivo.

Presentazione del modello Zero Trust Edge per la sicurezza e i servizi di rete

Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE)

Ostacoli sulla strada verso l'approccio Zero Trust Edge

Il modello Zero Trust Edge è rivoluzionario, o meglio trasformativo, rispetto all'approccio tradizionale alla sicurezza e al networking. Le funzioni di sicurezza informatica, in costante evoluzione, sono passate più rapidamente al modello Zero Trust Edge. Le reti legacy saranno molto più lente. Le aziende si stanno convertendo a un approccio Zero Trust Edge spinte dalla necessità di garantire la sicurezza dei telelavoratori, ma sono ancora molte le sfide da affrontare prima che questo modello possa mantenere appieno le sue promesse. Tra queste figurano le seguenti:

- **Applicazioni e servizi legacy.** Le moderne applicazioni Web supportano la federazione delle identità, rendendole (relativamente) semplici da configurare in un ambiente ZTE. Non sarà altrettanto semplice configurare le applicazioni basate su protocolli non Web, in particolare RDP/VDI e SIP/VoIP. Anche per questi due tipi di applicazioni molto comuni non esiste un metodo standardizzato di utilizzo nell'ambiente ZTE.
- **Dispositivi di rete esistenti.** Dopo aver collegato i laptop, i server e le applicazioni allo Zero Trust Edge, l'architetto dovrà prendere in considerazione le migliaia, se non centinaia di migliaia, di dispositivi OT e IoT su cui non può essere installato alcun software agente. Questi devono connettersi in massa, utilizzando protocolli di rete accettati, ed è proprio per questa necessità che i team di sicurezza e networking dovranno collaborare.
- **Capacità e fiducia.** Le organizzazioni possono utilizzare il modello ZTE per risolvere tatticamente alcuni problemi, come l'accesso sicuro per i lavoratori remoti, ma non sono ancora pronte a sostituire i servizi di sicurezza e networking ad alta capacità erogati dai loro data center esistenti. Le organizzazioni che hanno effettuato ingenti investimenti nei loro data center attenderanno il momento in cui dovranno compiere uno sforzo maggiore, come la migrazione al cloud delle loro applicazioni di importanza critica, prima di adottare la protezione Zero Trust Edge per questi servizi.

Che cosa significa

La sicurezza e il networking si alleano contro un nemico comune

Una volta che la sicurezza sarà integrata nella rete e diventerà parte del suo DNA, Forrester prevede che si verificherà la seguente situazione per le due organizzazioni:

1. **Organizzazioni di sicurezza che impostano le policy e i test di sicurezza.** I tipi di traffico e i servizi necessari per soddisfare livelli di fiducia accettabili saranno stabiliti dal team addetto alla sicurezza. Grazie agli strumenti di monitoraggio e analisi, i team lavoreranno insieme per assicurare il rispetto delle policy ed eseguire test e verifiche regolari del traffico e delle connessioni.
2. **Il networking dopo la sicurezza.** I professionisti del networking applicheranno le policy ZTE definite dal team di sicurezza. Se da un lato questo tipo di assetto imprimerà una forte accelerazione al concetto Zero Trust, dall'altro rappresenterà una netta inversione di tendenza rispetto all'approccio degli ultimi 25 anni in cui la sicurezza si sovrapponeva al networking.

Presentazione del modello Zero Trust Edge per la sicurezza e i servizi di rete

Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE)

3. **Internet diventerà infine un luogo più sicuro.** Se invitati a rispondere, gli ideatori di Internet ammetteranno in tutta franchezza che la sicurezza non era mai stata considerata nel progetto iniziale. Nei 30 anni successivi alla sua nascita, l'Internet globale è diventato una rete pericolosa da attraversare. Il modello Zero Trust Edge offre finalmente un percorso più sicuro.

Contatta un analista

Acquisisci maggiore fiducia nelle tue decisioni collaborando con i leader di Forrester per applicare la nostra ricerca alle tue specifiche iniziative aziendali e tecnologiche.

Contatta un analista

Per mettere in pratica i risultati della ricerca, contatta un analista per approfondire le tue domande in una sessione telefonica di 30 minuti oppure scegli di essere contattato tramite e-mail.

Per saperne di più.

Consulenza di un analista

Trasforma la ricerca in azione collaborando con un analista su un progetto specifico sotto forma di sessioni strategiche personalizzate, workshop o discorsi.

Per saperne di più.

Webinar

Partecipa alle nostre sessioni online sulle ultime ricerche che interessano il tuo settore di attività. Ogni chiamata include domande e risposte degli analisti e diapositive ed è disponibile su richiesta.

Per saperne di più.



App di ricerca Forrester per iOS e Android.

Mantieni il vantaggio sulla concorrenza, ovunque ti trovi.

Materiale supplementare

Aziende intervistate nell'ambito di questo report

Desideriamo ringraziare i collaboratori delle seguenti società per il tempo che ci hanno gentilmente dedicato durante l'attività di ricerca svolta per la realizzazione di questo report.

419 Consulting

Axis Security

Akamai

Barracuda

AT&T

BlackBerry

Presentazione del modello Zero Trust Edge per la sicurezza e i servizi di rete

Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE)

Cato Networks	Marriott Vacations Worldwide
Cisco Systems	Menlo Security
Citrix	Mentor Graphics
Deutsche Telekom	Netskope
Edelweiss Financial Services	Nuspire
Famous Supply	Palo Alto Networks
Fortinet	Silver Peak
Infoblox	SKF
IronNet	VMware
Jefferies	Windstream
Juniper	Zentera Systems
Lightstream	Zscaler

Note di chiusura

- ¹ Un data center privato è un hub di dati, applicazioni e sicurezza con sedi remote; ristoranti, centri per la cura di pazienti acuti, siti di produzione, per citare solo alcuni esempi, si collegano all'hub per accedere a tutte le risorse aziendali.
- ² Consultare il report Forrester "[Emerging Technology Spotlight: Businesswide Networking Fabric](#)".
- In un modello di business interconnesso, gli attori dell'ecosistema contribuiscono alla co-creazione di valore per i clienti in modo distribuito. Consulta il report Forrester "[Customer-Obsessed Businesses Need Digital Ecosystems](#)".
- ³ Nei nostri sondaggi sull'esperienza pandemica (PandemicEX) abbiamo chiesto agli intervistati in che misura la loro azienda/organizzazione stava adottando simili misure per gestire il rischio connesso al coronavirus. Fonte: sondaggio Q1 2020 US PandemicEX Survey 1 di Forrester (dal 3 al 6 marzo 2020); sondaggio Q1 2020 US PandemicEX Survey 2 di Forrester (dal 17 al 19 marzo 2020) e sondaggio Q2 2020 US PandemicEX Survey 1 di Forrester (dal 1° al 3 aprile 2020).
- Consulta il report Forrester "[The State Of Remote Work, 2020](#)".
- ⁴ I materiali di marketing dei fornitori, nei primi tempi della diffusione del concetto di ZT, presentavano soluzioni destinate esclusivamente ai data center privati. Ad esempio, Palo Alto evidenziava, in vari white paper, il modo in cui il modello ZT poteva proteggere le risorse dei data center. Fonte: "Best Practices - Data Center Security", Palo Alto Networks, 1° giugno 2016 (<https://www.paloaltonetworks.com/resources/whitepapers/best-practices-data-center-security>).
- ⁵ Fonte: Sushant Jain, Alok Kumar, Subhasree Mandal, Joon Ong, Leon Poutievski, Arjun Singh, Subbaiah Venkata, Jim Wanderer, Junlan Zhou, Min Zhu, Jonathan Zolla, Urs Hölzle, Stephen Stuart e Amin Vahdat, "B4: Experience with a Globally-Deployed Software Defined WAN", Proceedings of the ACM SIGCOMM 2013 Conference, Agosto 2013 (<https://storage.googleapis.com/pub-tools-public-publication-data/pdf/41761.pdf>).

Collaboriamo con i leader aziendali e tecnologici per sviluppare strategie focalizzate sul cliente che promuovono la crescita.

PRODOTTI E SERVIZI

- › Ricerca e strumenti di base
- › Dati e analisi
- › Collaborazione tra colleghi
- › Coinvolgimento degli analisti
- › Consulenza
- › Eventi

Le ricerche e gli approfondimenti di Forrester sono personalizzati in base al tuo ruolo e alle tue iniziative aziendali più importanti.

A CHI CI RIVOLGIAMO

Professionisti del marketing e di strategia

Direttori commerciali
Marketing B2B
Marketing B2C
Esperienza del cliente
Informazioni sui clienti
Strategia di eBusiness e di canale

Professionisti in gestione tecnologica

Direttori informatici
Sviluppo e distribuzione delle applicazioni
Architettura aziendale
Infrastruttura e operazioni

- Sicurezza e rischi

Approvvigionamento e gestione dei fornitori

Professionisti del settore tecnologico

Relazioni con gli analisti

ASSISTENZA CLIENTI

Per informazioni sulle ristampe cartacee o elettroniche, l'Assistenza clienti è disponibile al numero +1 866-367-7378 o +1 617-613-5730 oppure all'indirizzo clientsupport@forrester.com.
Offriamo sconti e prezzi speciali per istituzioni accademiche e non a scopo di lucro.