WHITE PAPER

aruba
a Hewlett Packard Enterprise company

UNA TRASFORMAZIONE DI SUCCESSO DI WAN E SICUREZZA È IL MOTORE DELL'IMPRESA DIGITALE

SOMMARIO

EXECUTIVE SUMMARY

Le aziende procedono sempre più spedite verso la trasformazione digitale allo scopo di migliorare l'efficienza, incrementare la soddisfazione del cliente, perseguire nuove opportunità di mercato, incrementare la redditività e mantenere un vantaggio competitivo. La migrazione delle applicazioni aziendali sul cloud è essenziale per qualsiasi iniziativa di trasformazione digitale di successo. Perché? Oggi ci sono più applicazioni in esecuzione nel cloud che nei tradizionali data center aziendali e la maggior parte di queste applicazioni viene consumata in modalità Software-as-a-Service (SaaS). Oltretutto, in un mondo incentrato sul cloud, le aziende devono assicurarsi che sia possibile accedere alle applicazioni in modo diretto e sicuro in qualsiasi momento, da qualsiasi luogo e con qualsiasi dispositivo. Un'ulteriore esigenza è che la rete offra sempre un'esperienza della massima qualità tanto ai dipendenti quanto ai clienti. Infine, l'esplosione dei dispositivi mobile e IoT nell'ambiente aziendale ha drammaticamente ampliato la superficie di attacco, esponendo l'azienda a violazioni della sicurezza in grado di comprometterne i dati e metterne fuori uso la rete.

Le reti aziendali di oggi non erano state progettate per un mondo basato sul cloud e non riescono assolutamente a garantire l'agilità e la sicurezza necessarie per abbracciare appieno la trasformazione digitale. Per le aziende è essenziale non soltanto mettere in sicurezza le proprie applicazioni nel cloud, ma anche proteggere gli utenti che si connettono a quelle applicazioni tramite la wide area network (WAN). Al tempo stesso, l'attuale, ambiente competitivo aziendale esige che le aziende offrano ai clienti un'esperienza della massima qualità, fornendo una rete in grado di mantenere sempre i livelli di prestazioni e disponibilità necessari per le loro attività.

Per realizzare appieno la promessa della trasformazione digitale, le aziende devono trasformare l'architettura sia della WAN sia della sicurezza: non possono limitarsi a quella dell'una o dell'altra soltanto. Le aziende hanno già compiuto investimenti significativi nel passaggio al cloud. Adesso la sfida più grande consiste nell'ottenere un effetto moltiplicatore da quegli investimenti. La soluzione consiste nel modernizzare le architetture della WAN e della sicurezza dell'azienda. L'imperativo strategico consiste quindi nell'adottare una software-defined wide area network (SD-WAN) più intelligente, altamente automatizzata e perfettamente integrabile con i servizi di sicurezza forniti nel cloud.

Poiché la trasformazione della WAN e della sicurezza rappresentano un percorso, l'azienda può iniziare dalla modernizzazione dell'una o dell'altra componente, ma per mettere pienamente a frutto gli investimenti compiuti nel cloud, bisogna modernizzarle entrambe. Ugualmente importante è evitare il vendor lock-in scegliendo partner di soluzioni tecnologiche che offrano flessibilità e libertà di scelta. Una volta trasformate le architetture della rete e della sicurezza, l'azienda può adottare tempestivamente le innovazioni per incrementare la produttività e accelerare la crescita e la redditività, contenendo al tempo stesso i costi.

Per realizzare appieno le promesse del cloud e della trasformazione digitale, le aziende devono trasformare l'architettura sia della WAN sia della sicurezza: non possono limitarsi a quella dell'una o dell'altra soltanto. Le aziende hanno già compiuto investimenti significativi nel passaggio al cloud. Adesso la sfida più grande consiste nell'ottenere un effetto moltiplicatore da quegli investimenti.

LE APPLICAZIONI SONO FORNITE NEL CLOUD: ANCHE LA SICUREZZA DOVREBBE ESSERLO

Tradizionalmente, tutto il traffico delle applicazioni proveniente dalle filiali verrebbe trasportato in backhaul tramite servizi MPLS privati al data center aziendale per verifiche e ispezioni di sicurezza (figura 1). Questa architettura ha senso se le applicazioni sono ospitate esclusivamente nel data center aziendale. Adesso, tuttavia, con la massiccia migrazione di servizi e applicazioni nel cloud, l'architettura di rete tradizionale risulta inadeguata: essa infatti riduce le prestazioni delle applicazioni e offre un'esperienza utente irregolare, poiché il traffico destinato al web deve passare per il data center e il firewall aziendale prima di giungere a destinazione.

Inoltre, con l'aumento del numero di dipendenti che lavorano al di fuori della rete aziendale connettendosi direttamente alle applicazioni sul cloud, la tradizionale sicurezza basata sul perimetro risulta insufficiente. Il cloud e il SaaS hanno cambiato per sempre il modo in cui gli utenti si connettono alle applicazioni e interagiscono con esse. Trasformando le architetture della WAN e della sicurezza, le aziende possono garantire un accesso diretto e sicuro alle applicazioni e ai servizi in ambienti multi-cloud indipendentemente da dove ci si connette e dal dispositivo usato.

Le soluzioni di sicurezza su cloud normalmente supportano una pluralità di funzionalità di sicurezza di rete, che possono includere il secure web gateway (SWG), il Firewall-as-a-Service (FWaaS), il cloud access security broker (CASB) e l'architettura di rete Zero Trust (ZTNA). In precedenza, queste erano tutte funzionalità implementate in locale, separate e dedicate. Ora possono essere fornite tramite cloud e in maniera unificata, come mostrato in figura 2.

Alcuni tra i primi ad adottare le soluzioni di sicurezza fornite tramite cloud non sono riusciti ad implementare anche una SD-WAN che permettesse di evitare di applicare l'adaptive Internet breakout direttamente dalle filiali. Pertanto, non erano in grado di indirizzare il traffico in uscita dalla filiale direttamente verso il cloud. Senza la componente SD-WAN, il traffico destinato al cloud doveva comunque passare dal data center, pregiudicando le prestazioni delle applicazioni.

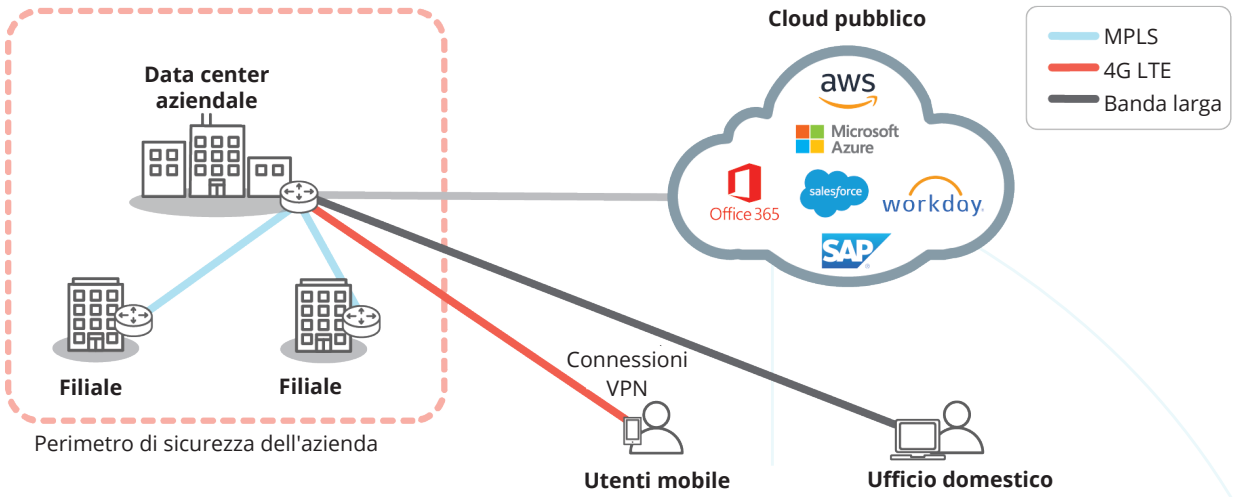

Figura 1: Le WAN aziendali tradizionali e gli approcci alla sicurezza basati sul perimetro non sono stati progettati per il cloud. Effettuare il backhaul del traffico di tutte le applicazioni dalle filiali al data center riduce le prestazioni delle applicazioni e offre un'esperienza utente irregolare.

L'adozione di una soluzione di sicurezza basata sul cloud e di una SD-WAN elimina i costi e le complessità associate alla gestione di più firewall di nuova generazione in locale, senza però escludere la necessità delle funzionalità dei firewall con stato basati sulla zona presso le filiali per bloccare le minacce in entrata. Come mostrato in figura 3, utilizzando una soluzione SD-WAN avanzata, le aziende possono connettersi direttamente al cloud grazie all'adaptive Internet breakout usando semplici connessioni a Internet a banda larga. L'applicazione di un'intelligenza in grado di riconoscere le applicazioni inserite nella white list permette di sfruttare il local breakout tra la filiale e il PoP (point of presence) più vicino, eliminando la latenza e fornendo un'esperienza della massima qualità per le applicazioni su cloud e SaaS fidate (Microsoft Office 365, 8x8, RingCentral, ecc.). L'application awareness permette inoltre di inviare i dati di altri tipi di traffico diretti verso il web a un servizio di sicurezza ospitato sul cloud in modo da consentirne un'ispezione avanzata prima di inoltrarli al fornitore SaaS di turno. Le avanzate funzionalità SD-WAN integrate con i moderni servizi di sicurezza basati sul cloud garantiscono un'applicazione coerente delle politiche e del controllo degli accessi da parte di utenti, dispositivi, applicazioni e IoT. Ciò permette alle aziende di rispettare le politiche ed eliminare i tempi morti e mitigare il rischio di compromissione dei dati associati alle violazioni della sicurezza.

METTERE IN SICUREZZA L'IOT DELL'AZIENDA CON L'SD-WAN

La proliferazione dei dispositivi IoT nelle aziende porta con sé nuovi modi di monitorare, automatizzare, ottimizzare e relazionare sui processi aziendali, nonché di generare gli avvisi e le notifiche del caso, e ciò vale tanto per le linee produttive quanto per l'automazione della climatizzazione e dell'illuminazione finalizzata al risparmio energetico. L'IoT rende le aziende più efficienti tramite l'automazione; tuttavia

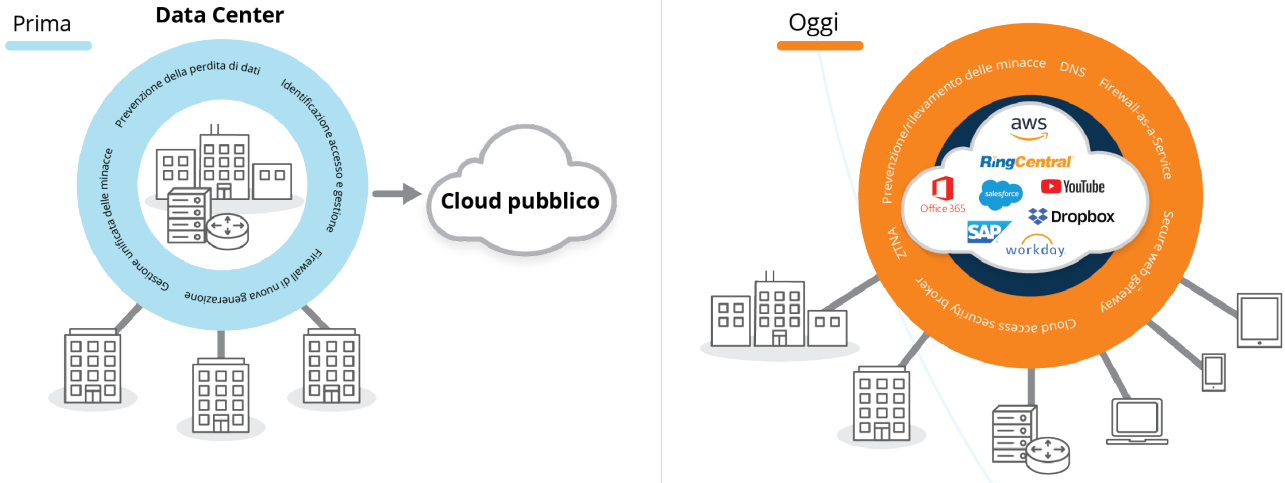

Figura 2: In passato l'importante era mettere in sicurezza il data center aziendale, l'unico luogo in cui erano ospitate le applicazioni. Ora che le applicazioni si sono spostate sul cloud e operano da lì, l'approccio alla sicurezza aziendale basata sul perimetro si sta rivelando sempre più inefficace. È essenziale pensare in maniera diversa e spostare sul cloud anche la sicurezza.

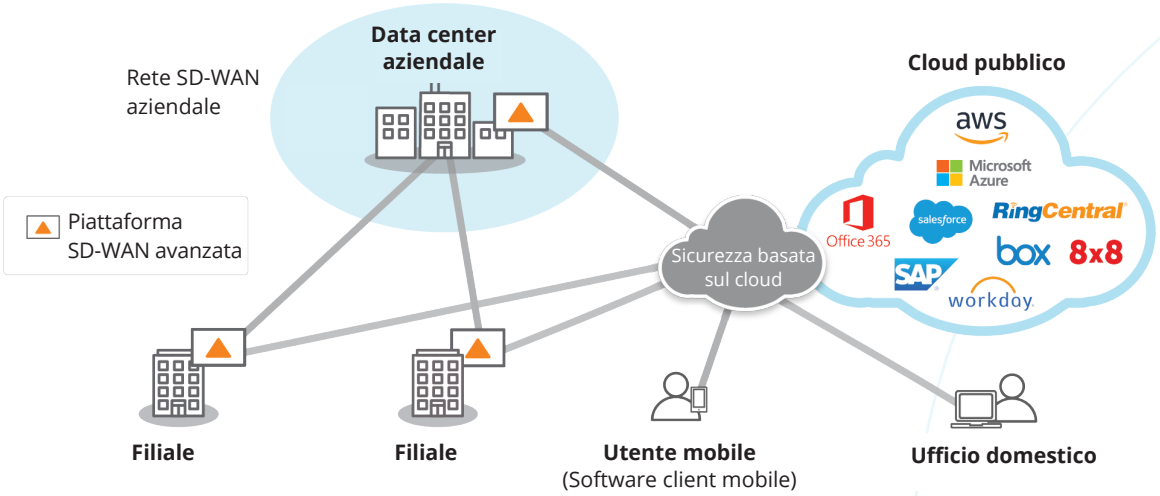

Figura 3: Una SD-WAN avanzata fornisce alle aziende un accesso sicuro al cloud. Le filiali possono usare connessioni a banda larga e l'adaptive Internet breakout per connettere direttamente gli utenti alle applicazioni sul cloud, ottimizzando le prestazioni delle applicazioni e l'esperienza utente. Unendo una SD-WAN avanzata e una soluzione di sicurezza basata sul cloud usando un approccio alla rete Zero Trust (ZTNA) basato sulle politiche si può garantire sempre la sicurezza della WAN aziendale, degli utenti, dei dispositivi e delle applicazioni.

amplia a dismisura la superficie d'attacco aggiungendo una nuova dimensione di complessità. Per affrontare la crescente sfida della sicurezza dei dispositivi mobili, l'IT guarda a soluzioni di accesso alla rete Zero Trust (ZTNA) basate sul modello Zero Trust. Le soluzioni ZTNA prevedono l'installazione di un agente di protezione dell'endpoint sul dispositivo dell'utente (portatile, tablet, cellulare). L'agente software fa in modo che il traffico in uscita dal dispositivo venga diretto a un servizio di sicurezza basato sul cloud prima di essere inoltrato verso l'applicazione SaaS o il fornitore IaaS. Tuttavia, a differenza dei tablet e degli smartphone, i dispositivi IoT non consentono l'installazione degli agenti software ZTNA (e di agenti software di terze parti in genere). Per questo, per neutralizzare la potenziale vulnerabilità dei dispositivi IoT, le aziende necessitano di una soluzione di sicurezza diversa se vogliono proteggere le proprie reti da violazioni in grado di compromettere l'operatività aziendale quotidiana.

I rischi associati all'impiego dei dispositivi IoT possono essere ridotti con l'adozione di una piattaforma SD-WAN avanzata e application-aware. Le piattaforme SD-WAN avanzate sono in grado di identificare e classificare il traffico delle applicazioni al primo pacchetto, intercettarlo all'edge della rete, spostarlo sul segmento appropriato e proteggerlo dal resto del traffico in transito sulla rete. Le piattaforme SD-WAN avanzate orchestrano la segmentazione end-to-end coprendo i percorsi LAN-WAN-LAN e LAN-WAN-Data center/Cloud. Di conseguenza, le politiche di sicurezza sono applicate in maniera automatizzata e coerente, per di più con una visibilità maggiore. Con la segmentazione end-to-end, le aziende possono creare segmenti isolati per il traffico dei dispositivi IoT. Per ciascun segmento è possibile definire una politica di sicurezza indipendente. Poiché il traffico di un segmento è isolato da quello negli altri segmenti, non è possibile che si verifichino accessi non autorizzati. Anche se sorgesse una minaccia, il suo impatto resterebbe limitato al segmento in cui è emersa. Inoltre, con un firewall con stato basato sulla zona unificato, le aziende possono proteggere dalle potenziali minacce, bloccandole, anche i siti remoti e i dispositivi IoT.

Facciamo un esempio. In un sito remoto in cui sono installati dispositivi IoT senza agente come sistemi PoS e di climatizzazione (figura 4, di seguito), una piattaforma SD-WAN avanzata identifica in modo univoco le applicazioni usate dai dispositivi. Una politica di sistema intercetta il traffico del PoS e lo trasmette al data center aziendale, che ospita l'applicazione di elaborazione della transazione con carta di credito. A questo traffico vengono applicati i servizi di sicurezza basati su firewall di nuova generazione già esistenti, implementati nel data center. Invece, le politiche del sistema di climatizzazione segmentano e trasmettono il traffico del sistema di climatizzazione al servizio di sicurezza basato sul cloud per un'ispezione di sicurezza aggiuntiva, per poi inoltrarlo al centro di comando dell'IoT ospitato nel cloud pubblico. Poiché in base alle politiche aziendali il traffico IoT è isolato dal resto, eventuali violazioni del segmento dedicato al traffico della climatizzazione non potranno compromettere o mettere a rischio i dati personali e delle carte di credito che transitano sul segmento dedicato al traffico del sistema PoS. La segmentazione aiuta inoltre le organizzazioni a soddisfare i requisiti di conformità PCI (payment card industry) o di altri settori eventualmente rilevanti. Come mostrato nell'esempio, l'implementazione congiunta di una soluzione di sicurezza completa e di una piattaforma SD-WAN avanzata offre alle aziende più dinamiche una protezione maggiore nel momento in cui decidono di affrontare la trasformazione finalizzata a godere dei benefici dell'IoT.

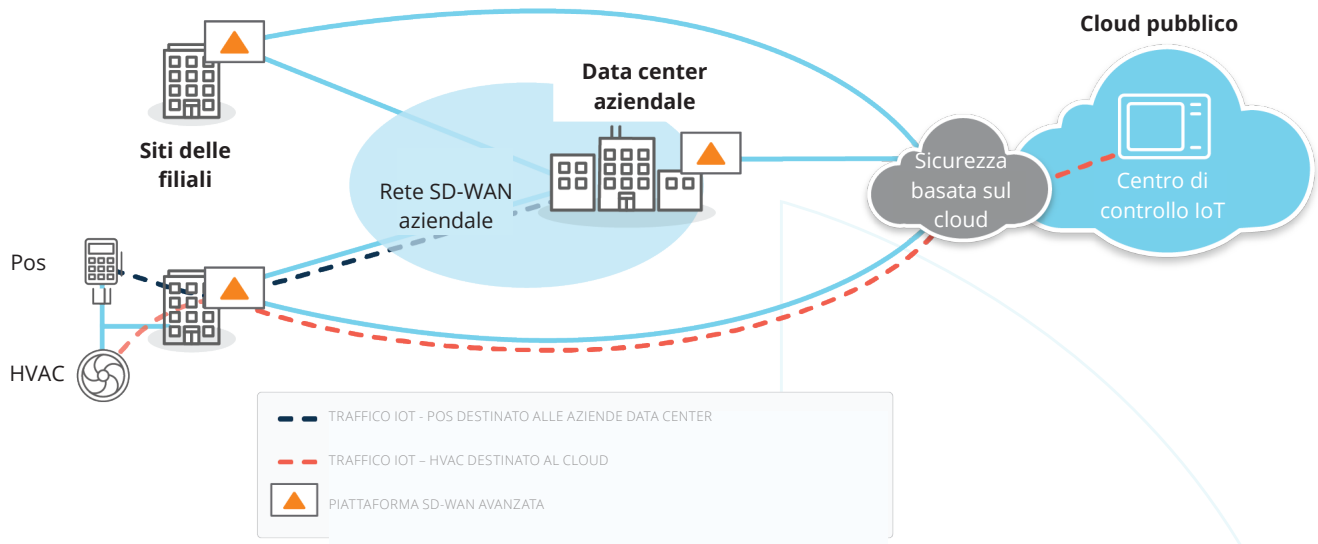

Figura 4: Gli endpoint dell'IoT si stanno moltiplicando, incrementando il rischio di violazioni della sicurezza. Usando una piattaforma SD-WAN avanzata, le aziende possono proteggere i dispositivi IoT con un firewall con stato basato sulla zona unificato in grado di identificare dinamicamente il traffico dei dispositivi IoT, applicare politiche individuali e segmentare la rete a un alto livello di dettaglio in modo da soddisfare i requisiti di conformità. Una SD-WAN avanzata fa in modo che il traffico IoT venga intercettato sull'edge della rete e inviato alla corretta destinazione (cloud incluso) senza compromessi e senza rischi di esposizione per l'azienda. Come mostrato nel diagramma, tutti i dati delle transazioni del sistema PoS provenienti dalla filiale vengono inoltrati al data center, mentre il traffico del sistema di climatizzazione viene indirizzato al centro di comando dell'IoT nel cloud.

LE SOLUZIONI MIGLIORI RENDONO L'AZIENDA PIÙ AGILE

Considerate la costante evoluzione degli approcci alla sicurezza di rete e la complessità insita nella creazione di soluzioni di rete complete, è importante prendere in considerazione le soluzioni di sicurezza e di rete migliori offerte da fornitori di provata esperienza e specializzazione nel campo. Se da un lato non è realistico pretendere di trovare un singolo fornitore in grado di offrire il meglio in entrambi i settori, dall'altro le aziende non dovrebbero essere costrette ad accontentarsi di soluzioni basiche né sull'uno, né sull'altro versante.

Il panorama delle minacce è in costante evoluzione e la sicurezza rappresenta perciò una delle principali preoccupazioni per le aziende. Queste devono perciò mantenere l'agilità necessaria per adottare rapidamente e a prezzi convenienti nuove soluzioni di sicurezza senza restare vittime del vendor lock-in. Disporre di una soluzione di rete indipendente dona alle imprese la fiducia e la serenità necessarie per scegliere e implementare le soluzioni di sicurezza basata sul cloud che meglio soddisfano le loro specifiche esigenze operative e di sicurezza, peraltro in costante evoluzione.

Potendo scegliere liberamente tra le soluzioni dei migliori fornitori che grazie all'automazione unificano l'SD-WAN e la sicurezza basata sul cloud, le aziende guadagnano in termini di velocità e agilità operativa e riducono le complessità e i costi grazie a un'architettura della sicurezza solida e di coerente applicazione in grado di minimizzare l'impatto dei cyber-attacchi. Tutto ciò, in ultima analisi, consente alle imprese di ottenere un effetto moltiplicatore sugli investimenti passati e in corso sui servizi e sulle applicazioni basati sul cloud.

LA TRASFORMAZIONE DELLA WAN È ESSENZIALE PER IL SUCCESSO DELLA TRASFORMAZIONE DIGITALE

Oltre a tutti i benefici derivanti dalla migrazione a una moderna architettura della sicurezza basata sul cloud, la trasformazione della WAN costituisce un valore enorme per le aziende principalmente basate sul cloud. Le tradizionali WAN incentrate sui router non sono state progettate per il cloud. Le aziende devono modernizzare la loro architettura WAN e ripensare all'architettura delle reti delle filiali per migliorare le prestazioni e la sicurezza delle applicazioni sul cloud. Le aziende utilizzano sempre più il cloud e il modello SaaS, con l'obiettivo di offrire un'esperienza utente della massima qualità.

La trasformazione della WAN consente di fornire un percorso utente-cloud più efficiente e un'esperienza migliore. Come anticipato in precedenza, l'implementazione dell'adaptive Internet breakout in relazione alle applicazioni ospitate sul cloud o SaaS direttamente dalle filiali non soltanto consente di ottimizzare la larghezza di banda disponibile, ma riduce anche la latenza e l'impatto negativo che questa potrebbe avere sulla produttività dell'utente.

Molte organizzazioni stanno trasformando l'edge delle proprie reti e stanno adottando l'SD-WAN per connettere le filiali con connessioni a Internet a banda larga. L'SD-WAN offre funzionalità di scelta intelligente del percorso basate sulle applicazioni e su politiche definite centralmente in grado di ottimizzare la distribuzione del traffico tra più connessioni WAN (MPLS, Internet a banda larga, LTE, ecc.). I vantaggi dell'SD-WAN sono:

- accesso conveniente alle applicazioni aziendali
- prestazioni, disponibilità e qualità dell'esperienza dell'utente finale migliori
- la soddisfazione delle esigenze dei moderni siti remoti e delle moderne filiali
- l'integrazione delle applicazioni e dei servizi SaaS e basati sul cloud
- il miglioramento dell'efficienza dell'IT nelle filiali grazie al provisioning automatico dei servizi

SODDISFARE I REQUISITI DEI SLA DELLE APPLICAZIONI

Tutto questo ha come risultato una produttività e un'agilità dell'azienda maggiori. Le aziende hanno bisogno di reti a elevate prestazioni costruite su fondamenta che ne garantiscano un'elevata disponibilità e in grado di supportare in modo affidabile le applicazioni critiche per l'azienda. La sicurezza, però, non deve mai essere messa in secondo piano. Il supporto di funzionalità che consentono la micro-segmentazione e l'applicazione delle politiche a un alto livello di dettaglio offre alle aziende la possibilità di rendere la propria WAN sicura, soddisfare i requisiti di conformità e proteggersi dalle violazioni.

Le aziende devono poter godere dell'agilità necessaria per aprire nuove filiali e regolare dinamicamente le politiche e le norme della sicurezza. La possibilità di propagare il contesto delle politiche è un elemento essenziale dell'automazione delle filiali. Tutto ciò rende le soluzioni SD-WAN avanzate una prospettiva molto attraente, poiché essa elimina la necessità per le aziende di implementare più appliance dedicate alla sicurezza e al tempo stesso consente loro di semplificare e consolidare (o "snellire") l'architettura WAN edge delle filiali. Le piattaforme SD-WAN edge avanzate consentono alle aziende di trasformare la propria WAN unificando SD-WAN, routing, ottimizzazione delle WAN, segmentazione e sicurezza delle filiali in un'unica piattaforma gestita centralmente.

L'orchestrazione dell'SD-WAN centralizzata e un approccio variabile in base alle applicazioni sono alla base di una rete il cui comportamento rifletta sempre le esigenze prioritarie dell'azienda. L'unificazione dell'orchestrazione della rete e delle politiche di sicurezza fa sì che i parametri di QoS e sicurezza vengano sempre e uniformemente applicati alle applicazioni (o alle classi di applicazioni) indipendentemente da come o dove vi si acceda. Gli obiettivi delle prestazioni delle applicazioni e della sicurezza sono dettati dall'alto dalle politiche aziendali, non dalle limitazioni tecnologiche provenienti dal basso.

Una SD-WAN avanzata monitora continuamente lo stato della rete e delle applicazioni, rileva i cambiamenti e attiva in tempo reale reazioni immediate e automatizzate volte a neutralizzare l'impatto di problemi, interruzioni e minacce alla sicurezza. Inoltre, l'automazione della connettività della piattaforma su cloud tramite l'integrazione delle API (application programmable interface) semplifica le operazioni IT, fornendo alle imprese un accesso tempestivo a IaaS, SaaS e servizi di sicurezza basati sul cloud.

Per garantire dinamicamente le prestazioni, la sicurezza e l'esperienza di altissima qualità richieste dagli ambienti multi-cloud, le reti di oggi devono essere caratterizzate da visibilità end-to-end, programmabilità e automazione. Una WAN intelligente architettata con le migliori soluzioni SD-WAN e di sicurezza basata sul cloud può accelerare le iniziative di trasformazione digitale e l'evoluzione delle aziende consentendo loro di accogliere più rapidamente le innovazioni senza impatti negativi sulla produttività o sulla crescita, il tutto riducendo al minimo l'esposizione alle minacce per la sicurezza.

CONCLUSIONE

Nel far migrare le proprie applicazioni dai data center al cloud, le moderne aziende basate sul cloud devono attuare la trasformazione della WAN e della sicurezza. Solo così potranno far rendere al massimo i loro investimenti nel cloud. Gartner ha coniato il termine SASE (Secure Access Service Edge) per indicare un'architettura che si muove in quella direzione. Come mostrato in figura 5, è importante che, nell'architettare un edge di servizi ad accesso sicuro, le aziende valutino di attuare una trasformazione sia della WAN sia della sicurezza per fornire un'esperienza senza interruzioni.

Realisticamente, nessun singolo fornitore potrà offrire le migliori tecnologie di rete e di sicurezza in un'unica piattaforma. Il panorama delle minacce è in costante evoluzione e le aziende devono perciò mantenere l'agilità necessaria per adottare rapidamente e a prezzi convenienti nuove soluzioni di sicurezza. È opportuno che le aziende prendano in considerazione piattaforme che consentano di integrare le migliori soluzioni di rete e di sicurezza. In questo modo possono evitare di dipendere dalle soluzioni proprietarie di un unico fornitore o di doversi accontentare di funzionalità basiche.

Una piattaforma SD-WAN avanzata che supporti l'integrazione delle API (application programmable interface) può offrire alle aziende nuovi livelli di automazione e la possibilità di connettersi a una varietà di servizi basati sul cloud di primissimo livello, ivi compresi quelli concernenti la sicurezza. Può inoltre supportare funzionalità di sicurezza di base necessarie per le filiali a complemento dei servizi di sicurezza forniti via cloud in modo da permettere un'applicazione delle politiche di sicurezza end-to-end, senza interruzioni e in tutta l'azienda. In questo modo, le aziende non ancora pronte a portare a compimento la trasformazione sia della WAN sia della sicurezza possono migrare verso un'architettura WAN moderna e basata sul cloud senza fretta, ma anche senza compromessi.

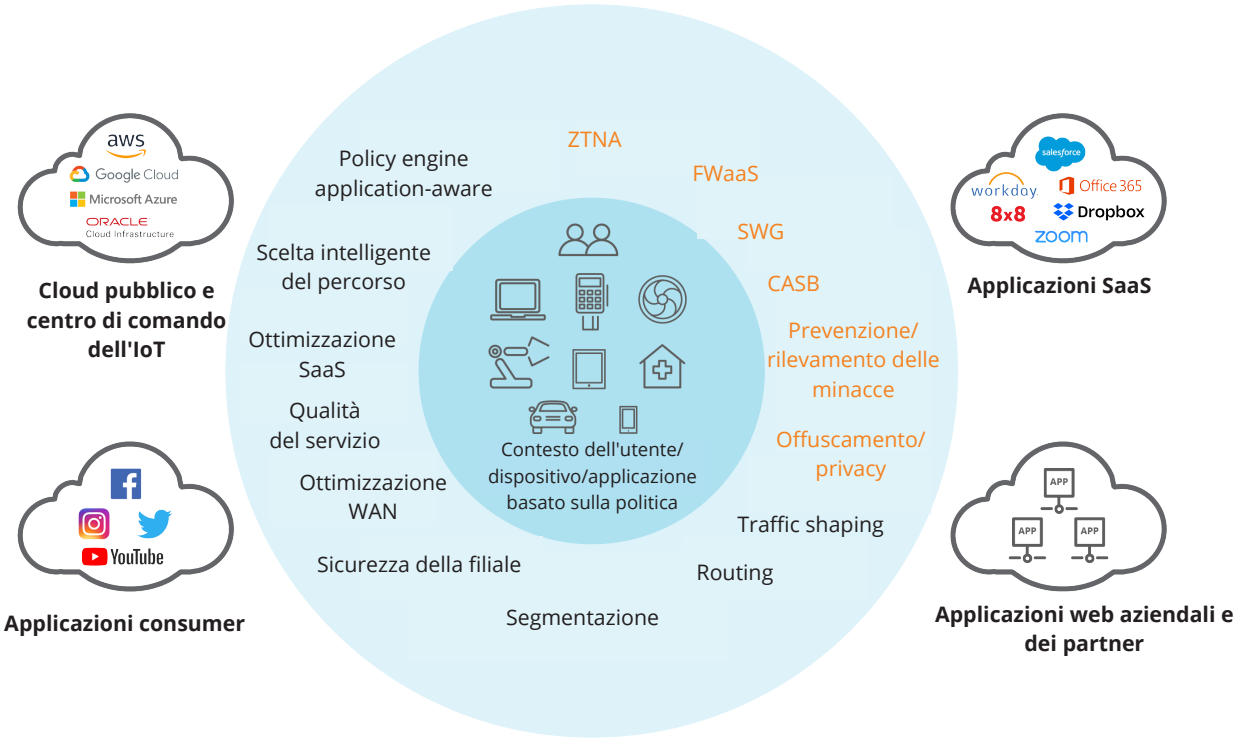

Figura 5: Per supportare le iniziative di trasformazione digitale dell'azienda (per es., strategia basata sul cloud, mobilità della forza lavoro), occorre un edge di servizi ad accesso sicuro. In un'architettura SASE robusta, una WAN ricca di funzionalità deve operare in congiunzione con una sicurezza di rete altrettanto completa per soddisfare l'esigenza di un accesso sicuro e dinamico da parte di utenti, dispositivi e applicazioni.

Infine, per le aziende non ancora pronte a mettere da parte i firewall delle filiali per affidarsi a una sicurezza completamente basata sul cloud, è importante trovare una piattaforma SD-WAN avanzata che offra la possibilità di scegliere liberamente tra le migliori soluzioni software UTM (unified threat management) di terze parti per adottarle come soluzione integrata presso le filiali. In questo modo possono eliminare i costi aggiuntivi e le complessità gestionali che normalmente comporta una moltitudine di firewall dedicati e separati, mantenendo però la flessibilità necessaria per poter implementare le migliori soluzioni sul mercato, garantendosi in ultima analisi la possibilità di migrare fluidamente verso un modello di sicurezza basata sul cloud.

Con l'aumentare degli investimenti delle aziende nel cloud, prendere in considerazione la trasformazione sia della WAN sia della sicurezza le metterà nelle condizioni di offrire la miglior esperienza possibile agli utenti, incrementare la produttività e sfruttare nuove fonti di entrate. In ultima analisi, avviare una trasformazione della WAN e della sicurezza accorta e senza compromessi consente alle imprese di ottenere un effetto moltiplicatore sui loro investimenti sul cloud, passati e in corso.

WP_Successful-WAN-and-Security-Transformation_EM_021621 a00110932enw