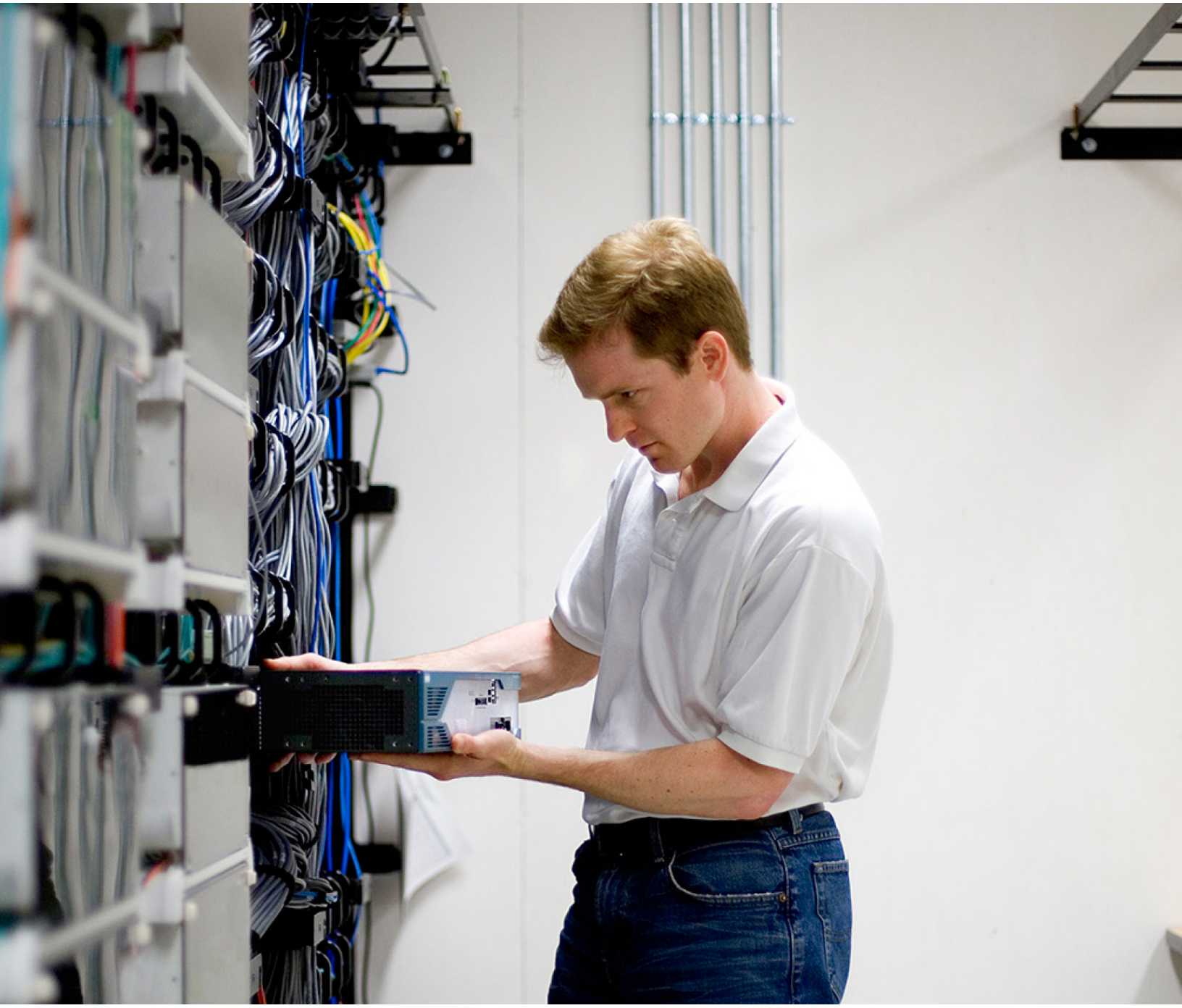
L'edge della rete diventa intelligente per soddisfare le esigenze attuali e future



Sintesi

Nella nuova realtà del business digitale, l'edge della rete non è mai stato più importante. Spesso trascurato, l'edge della rete è invece l'elemento fondamentale da cui dipende il successo digitale. Basta prendere in considerazione tutto ciò che succede all'edge della rete:

- È la prima linea di difesa contro le infiltrazioni di dispositivi non affidabili o dannosi.
- È il veicolo (su cui spesso si investe molto) tramite cui applicazioni e servizi raggiungono i destinatari.
- È il gateway strategico per connettere le aziende distribuite.
- È il ponte tra l'azienda e i clienti.
- È il punto in cui i nuovi dispositivi di Internet of Things (IoT) vengono connessi e gestiti.
- È il posto ideale per capire cosa succede veramente nell'azienda.

L'edge della rete talvolta viene implementato con la convinzione che tutte le soluzioni di rete siano essenzialmente le stesse. Al contrario, Cisco ritiene che il nuovo business digitale richieda la più ampia intelligence all'edge.

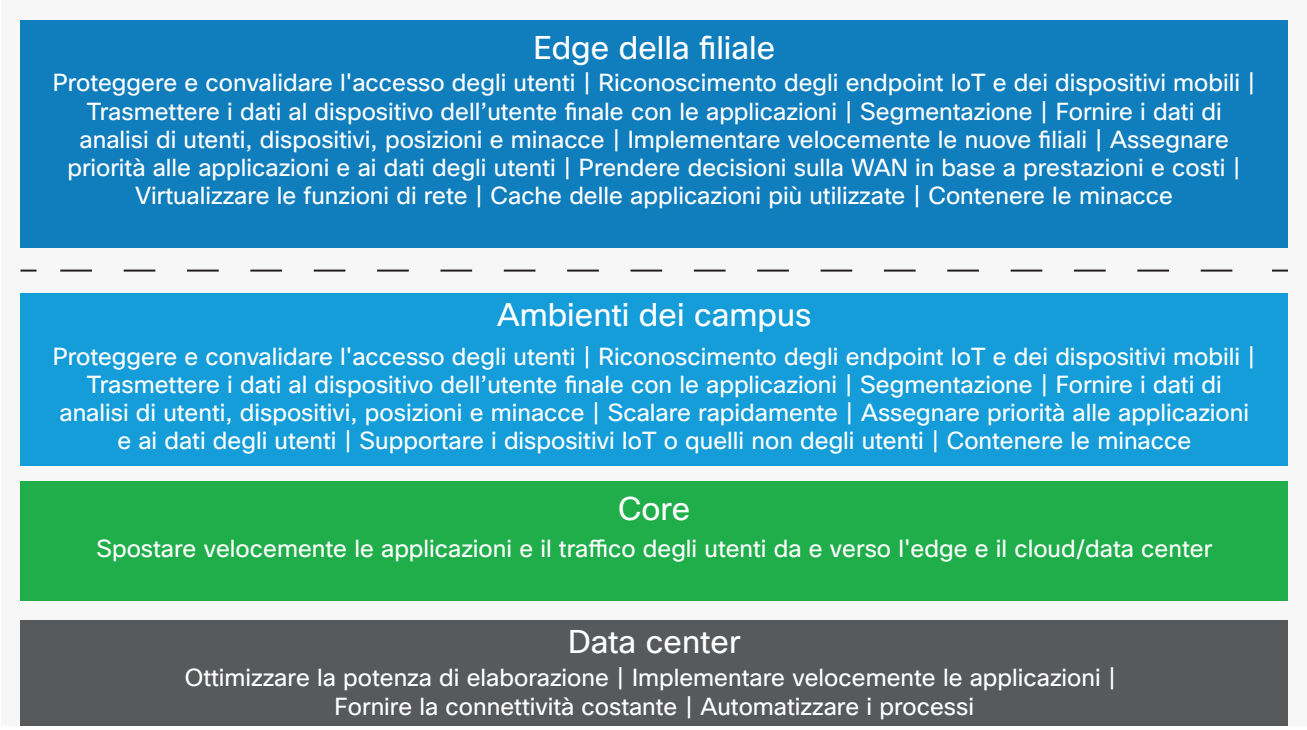
Forniamo soluzioni e funzionalità strategiche per sostenere il successo del business. La strategia di Cisco per l'edge della nuova rete digitale si basa su questi principi:

- La difesa delle risorse critiche all'edge. Le aziende possono evitare il 99,2% delle violazioni sfruttando la rete sia come sensore che come strumento di policy. Al tempo stesso è possibile fornire informazioni più dettagliate per migliorare la protezione e poter intervenire più rapidamente.
- Supportare il riconoscimento dei dispositivi e delle applicazioni con un roaming otto volte più rapido e la visibilità su più di 1200 applicazioni. Ciò è possibile grazie a una partnership strategica con Apple e tramite le innovazioni del Wi-Fi.
- Adattare continuamente la rete all'evoluzione dell'azienda tramite un approccio software-defined nelle LAN wireless, LAN e WAN. Ciò comporta un calo del 79% dei costi di implementazione dissociando il software dall'hardware e virtualizzando l'edge della WAN.
- Una piattaforma progettata per soddisfare le esigenze future implementando un'infrastruttura basata su standard e programmabile in grado di aggiungere rapidamente nuove funzionalità se necessario.
- Informazioni più approfondite e ottenute più velocemente dal commercio al dettaglio e dai servizi di accoglienza, con una granularità dei dati di localizzazione fino a un metro di distanza, in modo da consentire migliori decisioni di business.

Oggi la rete è essenziale per promuovere il cambiamento in quasi tutte le aziende che hanno intrapreso il percorso di trasformazione digitale. Questo processo di trasformazione consentirà alle aziende di migliorare l'agilità e la produttività, di interagire meglio con i clienti e proteggere la proprietà intellettuale e le risorse importanti.

L'edge della rete svolge un ruolo cruciale in questa trasformazione e ha responsabilità maggiori rispetto al core e alle reti dei data center. Come mostrato nella figura 1, quando si confronta ogni layer della rete, l'edge ha molte responsabilità nel campus. Lo stesso vale anche per le filiali.

Figura 1. Layer della rete e relative funzioni



Il ruolo dell'edge della rete

Con la trasformazione digitale l'edge della rete diventa ancora più importante. Si pensi a tutto ciò che succede all'edge della rete:

- **È la prima linea di difesa.** All'edge la policy viene applicata e convalidata, senza limitare la possibilità di accedere alle risorse necessarie. Se l'accesso non viene gestito correttamente, l'azienda può subire infiltrazioni o le minacce possono proliferare e la criticità aumenta con il continuo evolversi delle minacce. Il dispositivo, il firmware e perfino il sistema operativo sono potenziali punti di compromissione.
- **È il veicolo che fornisce le applicazioni su cui si è investito molto.** All'edge della rete vengono assegnate le priorità, quindi un'esperienza insoddisfacente a questo livello rallenterà l'adozione delle applicazioni, riducendo il ROI.
- **È un gateway strategico che permette la connessione delle aziende distribuite.** Fornire un'esperienza uniforme a dipendenti, partner e clienti, ovunque si trovino, è di fondamentale importanza. Una rete di seconda categoria offre livelli di servizi diversi ai destinatari principali.
- **È il ponte tra l'azienda e i clienti.** Se l'azienda appartiene al settore del commercio al dettaglio o dei servizi di accoglienza, un accesso inadeguato impedirà di interagire con i clienti a livello personale e avrà un impatto negativo sul brand.
- **Serve a supportare le esigenze sempre maggiori dei dispositivi IoT.** L'edge della rete adatta l'ambiente fisico consentendo alle aziende di praticamente tutti i settori di entrare nell'era digitale migliorando le operazioni e riducendo i costi. Senza le giuste funzionalità all'edge, le aziende possono rimanere indietro in termini di riduzione dei costi ed efficienza operativa.
- **È il posto ideale per capire cosa succede nell'azienda.** In una rete distribuita, solo l'edge ha la visibilità su tutto il traffico di dati, raccogliendo dati e informazioni analitiche dall'edge stesso. Dai dati su utenti, applicazioni, dispositivi e minacce, le aziende possono ottenere informazioni approfondite che consentono di prendere decisioni migliori per supportare i dipendenti, ridurre rischi e costi e offrire informazioni ai destinatari. Se la granularità non ha il giusto livello di coerenza, questi dati sono distorti e inaffidabili.

La commoditizzazione dell'edge è una buona scelta?

Molte soluzioni edge vengono commoditizzate usando componenti già disponibili per realizzare progetti e dispositivi per edge direttamente secondo gli standard del settore. Ciò avviene spesso per ridurre i costi di progettazione e produzione delle apparecchiature sfruttando i progetti già disponibili forniti dai produttori dei componenti. Ciò porta alla commoditizzazione dell'edge. L'approccio che privilegia i fattori dei costi e della gestione rispetto alle innovazioni necessarie per la crescita e la sicurezza espone l'azienda a rischi maggiori.

Quali sono i rischi?

I componenti e i progetti sono disponibili non solo ai produttori dei dispositivi, ma anche a chi vuole infiltrarsi nella rete. Ogni dispositivo che si collega alla rete è un potenziale punto di infiltrazione nella rete stessa. Oggi le aziende utilizzano un numero sempre maggiore di dispositivi mobili e dispositivi Internet of Things (IoT) connessi nella loro rete per il business. Le aziende devono cercare soluzioni che offrano un accesso sicuro, a partire dall'edge e continuando a controllare il traffico a ogni hop, dall'edge al data center.

C'è anche il rischio di dover riprogettare la rete se il business ha nuove esigenze. Le soluzioni standard sono progettate per soddisfare molti scenari d'uso generici, ma sono limitate in termini di flessibilità e personalizzazione. Un'altra limitazione è che non sono pronte per l'evoluzione imprevedibile della rete. La piattaforma di rete deve essere in grado di adattarsi alle continue evoluzioni del mondo digitale.

La maggior parte delle soluzioni standard sono progettate per allinearsi direttamente agli standard del settore che forniscono una base comune di requisiti e funzionalità. Tuttavia, gli standard possono cambiare. Il processo di standardizzazione è spesso lungo, mentre le esigenze dei produttori di dispositivi, degli sviluppatori di applicazioni e degli utenti cambiano continuamente. Le aziende che utilizzano un approccio basato sugli standard potrebbero non essere in grado di soddisfare maggiori aspettative degli utenti. A volte una soluzione soddisfa gli standard nella fase iniziale, ma permette di sviluppare funzionalità aggiuntive successivamente se necessario. In tal modo si soddisfano le nuove esigenze del mondo digitale senza essere vincolati agli standard, che potrebbero essere modificati o aggiornati anni dopo.

C'è anche il rischio che l'integrità dei dispositivi venga compromessa. I criminali informatici intercettano i dispositivi quando vengono distribuiti a livello mondiale, quindi alterano i componenti, ad esempio scambiando i processori o integrando i monitor per acquisire dati sensibili.

Qual è il costo reale?

Spesso l'edge viene commoditizzato per ridurre i costi di progettazione e produzione e quindi vendere alcune soluzioni a un prezzo inferiore. Tuttavia, quando si calcolano i costi non bisogna esaminare solo il semplice capitale o persino i costi operativi, ma anche il costo associato al rischio. Ogni azienda è diversa, quindi determinare i costi reali per ognuna è impossibile. Vanno però considerati questi fattori.

- Il costo di una violazione della sicurezza. La proprietà intellettuale e le risorse di molte aziende sono indispensabili per la loro sopravvivenza. Se cadono nelle mani sbagliate quali sono le conseguenze? I criminali informatici sono incredibilmente abili a capitalizzare la proprietà intellettuale tramite i riscatti del ransomware, l'estorsione e la rivendita al maggior offerente. Alcuni studi dimostrano che per le cartelle cliniche sono stati chiesti riscatti di 40,00 dollari ciascuna. Considerate le migliaia di cartelle degli ospedali, questi ultimi potrebbero trovarsi costretti a sborsare cifre astronomiche per riappropriarsene.
- Il costo di un'applicazione business-critical che non viene adottata dai dipendenti. Molte aziende investono gran parte del budget in nuove applicazioni e sistemi per migliorare la produttività. Se i dipendenti hanno delle esperienze negative con queste applicazioni o servizi, li abbandoneranno e il ROI precipiterà.
- Il costo delle opportunità perse. Un'azienda del settore del commercio al dettaglio o dei servizi di accoglienza interagisce con i clienti attraverso i loro dispositivi mobili. Ma se i clienti incontrano difficoltà a connettersi, l'azienda perde l'opportunità di interagire con loro e influenzare i comportamenti desiderati.
- Il costo della mancanza di visibilità. L'edge contiene numerose informazioni relative agli utenti, ai dispositivi, alle applicazioni che utilizzano, a dove vanno e persino informazioni sui punti in cui ci sono potenziali minacce. Senza questa visibilità l'azienda può passare una miriade di ore a cercare di capire in che modo gli utenti interagiscono con l'ambiente, come accedono e usano le informazioni e persino individuare troppo tardi una potenziale minaccia che poteva essere mitigata prima.

Cisco fornisce intelligence all'edge

Cisco adotta un approccio diverso rispetto alla commoditizzazione dell'edge. Investiamo moltissimo nello sviluppo di innovazioni volte a favorire l'ingresso delle aziende nell'era digitale. Puntiamo alla difesa delle risorse critiche per supportare un livello più elevato di riconoscimento delle applicazioni e dei dispositivi e per fornire informazioni più approfondite e più velocemente. Cisco aiuta le aziende ad adattarsi all'evoluzione del business e a prepararsi al futuro. Operiamo sviluppando da zero funzionalità uniche o migliorando le funzionalità di componenti ampiamente utilizzati. Cisco fornisce le funzionalità che consentono di soddisfare le esigenze dell'edge della rete sia oggi che in futuro.

La difesa delle risorse critiche all'edge

L'edge della rete è il punto principale per l'accesso non autorizzato dei malintenzionati perché è qui che avviene l'onboarding di utenti e dispositivi. Deve essere affidabile, poiché ha il compito di identificare e controllare quello che succede in rete.

La commoditizzazione della sicurezza dell'edge si basa sul presupposto che la sicurezza standardizzata sia efficace. Ma se ciò è vero, come è possibile che i furti, l'estorsione e il sequestro di informazioni stiano rapidamente creando un giro d'affari da 1.000 miliardi di dollari?

Gli attuali approcci alla sicurezza dell'edge non funzionano. Cisco è leader del mercato con tecnologie innovative che permettono di conoscere un dispositivo, il suo utente e lo stato di integrità prima di lasciarlo entrare nella rete e consentirgli di muoversi liberamente.

Si veda di seguito un elenco di innovazioni nella sicurezza dell'edge della rete introdotte da Cisco® per i suoi clienti e come vengono utilizzate.

- **Identità e integrità di dispositivi e utenti**. I dispositivi Cisco dell'edge integrano le più complete tecnologie di analisi dei profili degli endpoint. Inoltre, Cisco AnyConnect® Security Agent svolge un controllo dell'integrità della conformità alle policy e della postura della sicurezza prima di consentire l'accesso alla rete di produzione. L'accuratissima identità degli endpoint permette di escludere completamente dalla rete i dispositivi non autorizzati e pericolosi (infettati da malware) finché non si dimostra che sono puliti e autorizzati.
- **I privilegi di accesso cambiano in base al punteggio delle minacce**. Grazie all'integrazione con Cisco Identity Services Engine, i privilegi di accesso di utenti e dispositivi possono essere cambiati automaticamente di pari passo con l'evolvere del punteggio delle minacce STIX o delle vulnerabilità CVSS. STIX e CVSS sono espressioni usate comunemente per descrivere la gravità delle minacce e delle vulnerabilità della sicurezza.
- **Integrazione della segmentazione software-defined**. In genere è difficile creare e gestire la segmentazione con le LAN virtuali e le ACL (Access Control List) ed è ancora più difficile quando la segmentazione diventa fondamentale per proteggere le operazioni di IoT. I dispositivi Cisco dell'edge hanno la segmentazione software-defined di Cisco TrustSec® integrata nel sistema operativo nonché un ASIC per garantire identità e segmentazione semplici e ad alte prestazioni dal punto di accesso all'applicazione nel data center.
- **La rete come strumento di policy**. Si tratta della segmentazione software-defined integrata nei dispositivi periferici che consentono l'applicazione istantanea e coerente delle policy di sicurezza per controllare gli accessi e contenere le minacce. Usando l'integrazione con le tecnologie Identity Services Engine, Cisco StealthWatch e Cisco Security Technology Associate possono attivare una policy per contenere una minaccia, il tutto da un unico punto di controllo oppure da un solo prodotto.
- **La rete come sensore**. Si può ottenere una visibilità completa e avanzata grazie a NetFlow e al servizio di analisi di Cisco StealthWatch. Poiché tutti i dispositivi Cisco dell'edge includono Flexible NetFlow, si può avere una visibilità completa sui flussi per scoprire i comportamenti anomali. Con le tecnologie commoditizzate non si ha visibilità sui comportamenti degli utenti quando entrano in rete e su cosa fanno in Internet.
- **Integrazione di Stealthwatch Learning Network**. Questa innovazione consente a tutti i dispositivi delle filiali di condividere i dati sui comportamenti e adottare misure più intelligenti riguardo a ciò che è ammissibile, con una maggiore velocità, semplicità e scalabilità.
- **Applicazione di policy defcon zero-minute**. Ciò significa che è possibile disporre di policy prestabilite per rispondere a eventi catastrofici, come il malware zero-day o gli eventi di hacking che si diffondono rapidamente. Basta premere un tasto per attivare i cambiamenti delle policy di accesso per ciascun dispositivo sulla rete in modo da limitare o bloccare tutte le comunicazioni finché la minaccia non viene risolta.

- **Identità degli endpoint di IoT e segmentazione automatica**. Le analisi dei dispositivi Cisco dell'edge al momento aiutano a identificare la più grande raccolta di dispositivi medici IoT, ma la tecnologia si sta espandendo in molti altri settori. Attraverso l'integrazione con le tecnologie avanzate come Identity Services Engine, i dispositivi di rete dell'edge potranno identificare meglio e segmentare automaticamente gli endpoint più nascosti e aggiungerli automaticamente a segmenti di rete distinti per proteggerli dagli attacchi. Perciò quando un dipendente mette un dispositivo in rete, questo viene identificato, classificato e assegnato al segmento di rete di sicurezza corrispondente.
- **Contenimento delle minacce velocemente**. I dispositivi Cisco dell'edge sono integrati con Identity Services Engine e TrustSec, perciò quando un partner Cisco o un partner di integrazione della tecnologia rileva un attacco, può associare l'endpoint pericoloso a un segmento di rete, tramite un comando IT o automaticamente. Le minacce vengono rilevate più rapidamente e l'intervento di contenimento è immediato.
- **Rilevamento del malware nel traffico criptato**. Quando gli hacker trovano modi più nascosti per accedere alla rete, Cisco sfrutta la capacità di esaminare gli intervalli di rete per identificare il malware, persino nel traffico crittografato.
- **Difesa contro ransomware e malware e protezione nel cloud**. L'integrazione con Cisco Umbrella Branch rende i dispositivi Cisco dell'edge fondamentali per la soluzione Cisco contro il ransomware. Umbrella impedisce ai dipendenti di accedere ai siti Web sospetti, compromessi o contenenti malware. Impedisce inoltre ai bot di ransomware e malware di raggiungere la propria origine, senza cui in genere non possono funzionare.
- **Protezione dei dipendenti mobili**. I dipendenti mobili sono probabilmente i principali punti di infiltrazione del malware perché sono spesso liberi di accedere a Internet da remoto. Cisco AnyConnect Security Agent con VPN può essere potenziato con Cisco Advanced Malware Protection e Cisco Umbrella for Mobility per garantire la sicurezza quando si è fuori dalla rete. Consente inoltre la connessione tramite VPN a molti dispositivi Cisco dell'edge. Nessuna di queste soluzioni di sicurezza per dispositivi mobili con singolo agente funziona in un ambiente standard.
- **Integrità dei dispositivi di rete**. Per infiltrarsi nella rete e compromettere i sistemi, gli hacker non sfruttano solo le vulnerabilità di applicazioni e sistemi operativi. Possono attaccare gli stack software e hardware dei dispositivi di rete, perciò ai fini della sicurezza è fondamentale proteggere il dispositivo di rete. Come per i sistemi operativi e le applicazioni, le vulnerabilità dei dispositivi di rete probabilmente continueranno a essere scoperte. Cisco applica regole rigorose per lo sviluppo di software e hardware che comprendono test di regressione per fare in modo che i clienti Cisco possano continuare a utilizzare una rete sicura.

Dati più approfonditi e disponibili più velocemente

L'edge Cisco è una fonte preziosa di informazioni su ciò che succede veramente nell'azienda e offre dati sugli utenti, sui dispositivi che usano e sulle applicazioni a cui accedono. È in grado di capire e imparare dai dispositivi presenti nella rete per adattarsi automaticamente ai cambiamenti e alle diverse esigenze. Fornisce dati basati sulla posizione per comprendere meglio come gli utenti interagiscono con l'ambiente per permettere di prendere decisioni di business migliori e offre un'analisi forense delle minacce che permette di capire come le minacce si infiltrano nell'azienda.

Con Cisco IOx Fog Computing, l'edge può decidere il luogo ideale, on-premise o nel cloud, per elaborare i dati, consentendo all'azienda di migliorare le prestazioni e ridurre i costi. L'analisi della posizione disponibile in Cisco Connected Mobile Experiences (CMX) comprende la funzionalità di analisi della posizione granulare basata su BLE (Bluetooth Low Energy) e Wi-Fi per fornire una visione realistica di come le persone interagiscono con l'ambiente.

Le aziende B2C (business-to-consumer) come il commercio al dettaglio, i servizi di accoglienza e l'istruzione sono riuscite a raggiungere una localizzazione con un'accuratezza inferiore a un metro grazie alla combinazione di Wi-Fi e BLE e a incrementare il fatturato. Alcuni esempi includono il 20% del fatturato non associato alle prenotazioni delle stanze di Hyatt Regency, un aumento di tre volte del tempo di permanenza dei clienti e un miglioramento pari all'80% dell'esperienza utente al centro commerciale Stary Browar, il tutto offrendo al tempo stesso esperienze mobili personalizzate.

Inoltre, Cisco Prime™ offre una panoramica a 360 gradi degli utenti finali, dei loro dispositivi e delle applicazioni utilizzate in rete. Ciò permette di pianificare meglio le risorse della rete, misurare l'adozione delle applicazioni e ridurre i costi.

Adattarsi all'evoluzione del business con l'automazione

Con più utenti, dispositivi e sedi da gestire, la necessità di automatizzare i processi e i nuovi servizi con disponibilità immediata diventa molto più che una necessità. Negli ambienti con accesso via cavo e wireless, un fabric per campus e data center con overlay del software dissociato che usa ASIC (Application Specific Integrated Circuits) offre:

- Maggiore scalabilità
- Garanzia dei servizi
- Sicurezza
- Altri servizi sia per dispositivi fisici che virtuali, applicazioni e utenti

La virtualizzazione della rete consente di gestire la rete e le policy in base al tipo di utente per implementare e personalizzare le applicazioni velocemente e contenere le minacce con maggiore rapidità. Si tratta di un approccio centralizzato per implementare in modo sicuro nuove sedi remote in pochi minuti anziché alcuni giorni per qualsiasi tipo di connessione.

Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) offre la funzionalità plug-and-play (PnP) controllata centralmente e qualità del servizio (QoS) semplice per l'implementazione zero-touch all'edge. Consente inoltre l'assegnazione dinamica delle priorità per le applicazioni critiche.

Cisco offre l'agilità basata su software che consente la personalizzazione. Tramite le piattaforme hardware e software strettamente integrate, possiamo offrire vantaggi significativi alle aziende, che saranno evidenti a livello di WAN e di access edge. I componenti personalizzati della WAN includono un ASIC rapido e il software di gestione del cloud rende Cisco Enterprise Network Functions Virtualization (Enterprise NFV) una realtà, in cui è possibile attivare i servizi di rete in pochi minuti anziché alcuni mesi. Enterprise NFV offre funzionalità di elaborazione, archiviazione, infrastruttura di rete, gestione e qualità del servizio per eseguire i servizi di rete in modo da ridurre la complessità nelle filiali e abilitare nuovi servizi on-demand all'edge stesso.

Le aziende hanno registrato un calo del 79% dei costi di implementazione con APIC-EM PnP e un provisioning più rapido dell'85% con le applicazioni di Intelligent WAN di APIC-EM.

A causa dell'enorme quantità di utenti e dispositivi che si connettono dai luoghi più disparati, l'edge della rete può trovarsi in grandi campus o in piccole sedi remote. La visualizzazione globale della topologia con funzionalità PnP automatizzate riduce notevolmente il costo di integrazione o aggiornamento dei dispositivi di rete come switch, router o access point. Le applicazioni aggiuntive sul controller consentono il provisioning della QoS in tutta la rete, proteggendo rapidamente il traffico business-critical dai consumatori della larghezza di banda non critici. Le applicazioni specializzate come l'app Intelligent WAN (IWAN) consentono il provisioning, il monitoraggio e la risoluzione dei problemi di sicurezza, la crittografia, la selezione del percorso e Application Visibility and Control sulla WAN.

Inoltre, il software Cisco ONE™ rappresenta un metodo flessibile e vantaggioso per acquistare software per l'edge. In ogni fase del ciclo di vita dei prodotti, il software Cisco ONE consente di acquistare, gestire e aggiornare la rete con maggiore facilità. Si può realizzare un ROI solido di pari passo con la crescita dell'investimento grazie all'innovazione e agli aggiornamenti continui per le macchine fisiche e virtuali.

Riconoscimento di applicazioni e dispositivi

Cisco è l'unico fornitore a collaborare con Apple, il leader del settore dei dispositivi mobili, per offrire un'esperienza mobile migliore. Questa partnership strategica per entrambe le aziende sfrutta l'intelligence nella rete per offrire la migliore esperienza Wi-Fi tramite un roaming ottimale. In altre parole, si tratta di una corsia preferenziale per migliorare la produttività dei dipendenti con le applicazioni business-critical dei dispositivi Apple iOS utilizzati al lavoro.

Le aziende possono contare su un roaming fino a otto volte più rapido e chiamate tramite Wi-Fi più affidabili del 66% e un calo del 50% dei costi di gestione della rete grazie a un numero inferiore di SSID. Inoltre, gli utenti finali possono risparmiare la carica della batteria dei dispositivi iOS fino al 30%.

Da molti anni Cisco fornisce innovazioni Wi-Fi che superano lo standard attuale e rappresentano il punto di partenza per lo standard successivo. La tecnologia wireless Cisco Aironet® offre esperienze innovative e ad alta densità che migliorano le trasmissioni radio, le prestazioni dei dispositivi e l'esperienza applicativa. Cisco è stato anche pioniere della tecnologia Flexible Radio Assignment che ottimizza le prestazioni della rete Wi-Fi senza limitare la disponibilità radio. Questa funzionalità consente ai wireless access point di identificare le esigenze improvvise di larghezza di banda wireless e di adattarsi automaticamente alla rete wireless per soddisfare quella necessità. Ciò è fondamentale in aree affollate dove molti utenti competono per la larghezza di banda wireless.

Il business digitale dipende dalle applicazioni utilizzate per aumentare la produttività e interagire con i clienti. Cisco offre Application Visibility and Control che rileva le applicazioni all'edge della rete cablata e wireless. Utilizziamo il controllo intelligente dei percorsi per selezionare il percorso migliore della WAN ottimizzando al tempo stesso la trasmissione sulla LAN wireless o cablata, in modo che gli utenti possano usufruire della migliore esperienza applicativa possibile.

Le aziende possono ottenere una visibilità approfondita su oltre 1200 applicazioni e assegnare priorità alle applicazioni business-critical con un semplice clic con APIC-EM e Cisco Prime Infrastructure.

L'edge ha la capacità di monitorare e migliorare l'esperienza dei dipendenti nell'ambiente fisico. Cisco Digital Ceiling estende i vantaggi di IoT, facendo convergere diverse reti di edifici tra cui:

- Illuminazione
- Riscaldamento e raffreddamento
- Video IP
- Sensori IoT
- E molto altro tramite una piattaforma di rete intelligente e sicura

Digital Ceiling offre ai dipendenti nuove esperienze ed efficienza e riduce i costi operativi degli edifici.

Progettato per il futuro

Progettato tenendo presente il futuro, senza un sistema operativo Cisco IOS-XE che ha una programmabilità basata su standard e modelli, l'edge Cisco prepara la rete ad aggiungere nuove funzionalità e ad adattarsi ai cambiamenti dell'ambiente, del business o del settore. Ciò rende la rete periferica aperta, programmabile ed espandibile.

L'edge sta passando da un modello personalizzato a livello di dispositivo, in cui la segmentazione e il controllo degli accessi vengono aggiunti a una configurazione di rete, a una soluzione completamente automatizzata con policy. In futuro, non bisognerà effettuare il provisioning diretto delle reti. Si potranno esprimere le policy come una semplice finalità. Inoltre, è possibile stabilire quali utenti o gruppi hanno accesso a determinati gruppi privilegiati di applicazioni o di dati, sia on-premise che nel cloud. Il provisioning della rete per l'applicazione di questa policy avverrà in modo automatico, garantendo al contempo una grande flessibilità per monitorare, risolvere, correggere o applicare servizi aggiuntivi su un determinato traffico.

L'edge sta anche diventando completamente programmabile. Le soluzioni di orchestrazione possono interfacciarsi con l'edge utilizzando API basate su modelli standard, la creazione di script Python o altri strumenti di stile Linux. Ciò rende più semplice l'integrazione dell'edge nei metodi moderni di sviluppo software, garantendo un'agilità e una personalizzazione mai visti prima.

Innovazione continua all'edge della rete

Con il previsto boom della connettività che porta con sé opportunità significative, le aziende stanno iniziando a riconoscere che questa trasformazione richiederà cambiamenti fondamentali dell'infrastruttura di rete e la capacità di gestire e analizzare i dati. Svolgiamo un ruolo preminente in questa trasformazione sostenendo l'innovazione dell'infrastruttura di rete, la gestione dell'infrastruttura e l'analisi dei dati per estrarre informazioni utili.

Cisco si impegna per trasformare la risoluzione dei problemi da reattiva a proattiva e per ridurre i tempi di risoluzione da giorni interi a pochi minuti. Lo faremo trattando ogni dispositivo della rete come sensore e come elemento di elaborazione di dati distribuiti. Ottenendo i dati dai dispositivi dell'edge e spostandone l'elaborazione più vicino alla fonte dei dati, possiamo eseguire analisi a velocità di linea per generare informazioni utili con machine learning.

Potendo contare sul numero maggiore di dispositivi installati e soluzioni ASIC personalizzate, Cisco si trova in una posizione di vantaggio per progettare hardware e software ottimizzati per l'analisi. Sfruttiamo il potenziale dei dispositivi installati. L'integrazione di rete cablata e wireless significa che l'intelligence all'edge consente di risolvere i problemi, che si verifichino all'edge oppure no, nel giro di pochi secondi, e, nel corso del tempo, di correggere potenziali problemi anche prima che si manifestino. In questo modo i reparti IT possono rispettare i Service Level Agreement (SLA) per le prestazioni della rete e delle applicazioni anche in futuro.

Conclusioni

Con così tanti elementi che dipendono dall'edge della rete, la commoditizzazione di LAN e WAN cablate e wireless introduce rischi che potrebbero portare a violazioni della sicurezza, alla perdita di produttività del personale e di fatturato, alla perdita di opportunità e alla mancanza di visibilità. L'edge della rete Cisco va oltre l'approccio standardizzato e offre un'intelligence di alto valore all'edge.

Questo approccio consente alle aziende di:

- proteggere il business con una prima linea di difesa solida
- fornire le applicazioni ai destinatari in modo sicuro
- offrire un'esperienza ottimale ai dipendenti ovunque si trovino
- interagire con i clienti per generare nuovi flussi di entrate
- gestire meglio i dispositivi IoT e ottimizzare l'ambiente fisico
- fornire una visibilità ottimale di ciò che succede veramente nell'azienda

Maggiori informazioni

Per scoprire di più, visitare la pagina sulla tecnologia Cisco Unified Access all'indirizzo http://www.cisco.com/c/en/us/solutions/enterprise-networks/unified-access/index.html.

C11-737691-00 08/16