

PUNTO DI VISTA

I costi nascosti (ma non troppo) delle LAN: è fondamentale che operatività e licenze siano semplici



Sintesi preliminare

La rete locale (LAN) cablata e wireless costituisce la spina dorsale dell'IT. Supporta le applicazioni di nuova generazione e può aumentare la produttività degli utenti. Per questo motivo, la LAN non solo influisce notevolmente sull'esperienza degli utenti, ma è anche là dove iniziano o terminano molti eventi di sicurezza.

Gli amministratori IT di oggi devono costruire le loro reti di nuova generazione puntando a garantire un'esperienza utente sicura e fluida. Lo switching Ethernet e il Wi-Fi sono tra le tecnologie più mature nello spazio IT. Tuttavia, con la crescita delle esigenze, sono aumentati anche i costi nascosti addebitati dai fornitori per il funzionamento di queste tecnologie di base.

Tendenze che aumentano i costi operativi

Complessità degli ambienti multi-vendor

Sono molte le ragioni per cui le organizzazioni hanno fornitori diversi per le loro reti cablate e wireless. Possono essere state fatte scelte in base a cicli di aggiornamento, conoscenza dei fornitori, cambiamenti nelle preferenze della leadership, costi o anche disponibilità. In ogni caso, le LAN multi-vendor tendono ad aumentare le spese operative a causa della maggiore complessità.

Ogni fornitore ha la sua interfaccia, quindi il team IT dovrà passare da un'interfaccia all'altra per individuare la causa originaria quando si verifica un problema. Inoltre, quando si cerca di trovare e risolvere la causa originaria, sarà necessario collaborare con i team di assistenza di fornitori diversi, poco motivati a collaborare tra di loro. Infine, la condivisione delle informazioni è limitata e quindi è più difficile cogliere le tendenze storiche.

Proliferazione delle licenze

Gli elementi di base di una LAN sono lo switch Ethernet e l'access point (AP) wireless. In un passato non troppo lontano, la maggior parte dei costi di questi componenti era costituita da spese di capitale (CapEx). Lo switch Ethernet veniva acquistato e, a parte l'assistenza, il costo era limitato all'acquisto dell'hardware. L'acquisto di un AP wireless era simile a quello dello switch Ethernet, fino all'introduzione del controller wireless LAN (WLC), quando al costo del WLC sono spesso state abbinate licenze per AP wireless. In entrambi i casi, l'amministratore IT poteva prevenire il costo della soluzione wireless attraverso la spesa CapEx iniziale.

“Il 78% dei responsabili decisionali IT ha dichiarato che preferisce usare come standard un unico brand per l'hardware di rete, invece di mettere insieme soluzioni di diversi fornitori.”¹

Gli amministratori IT di oggi, tuttavia, devono fare i conti con una serie vertiginosa di licenze e canoni di abbonamento per l'hardware e la gestione delle LAN cablate e wireless LAN. Queste licenze e i relativi canoni possono riguardare aspetti basilari, come il sistema operativo, e complessi, come la visibilità delle applicazioni. È ormai comune che un ordine di acquisto per una piccola rete di filiale possa contenere diverse pagine complesse e di difficile comprensione sulle licenze per funzioni che in precedenza erano incluse nell'acquisto dell'hardware. Questa tendenza ha aumentato in modo significativo le spese operative (OpEx).

“Il 69% delle aziende ha più dispositivi IoT che computer in rete.”²

Tre trappole da evitare in relazione alle licenze

Gestione

Il cloud è diventato il metodo di gestione preferito per le LAN. Questo metodo, accessibile ovunque e in qualsiasi momento, è efficiente dal punto di vista operativo, ma le licenze di abbonamento possono essere complesse e costose.

Le licenze hanno caratteristiche variabili di costi e funzionalità e in alcuni casi sono condizione imprescindibile per l'utilizzo dell'hardware acquistato come CapEx. Comprendere la natura delle licenze di gestione cloud di ciascun fornitore è fondamentale per limitare le spese operative. È anche importante assicurarsi che esistano opzioni locali, non penalizzanti, se i team IT vogliono staccarsi dal cloud.

Visibilità degli endpoint

È difficile gestire una rete senza sapere cosa vi è collegato. I sistemi di autenticazione possono dire agli amministratori IT chi è in rete, ma non cosa. Questo porta il personale IT a dover identificare manualmente ciò che è connesso, un processo lungo e impreciso che comporta costi operativi elevati. Molti fornitori richiedono una licenza e/o un abbonamento per abilitare la visibilità degli endpoint, spesso senza nemmeno includere l'onboarding sicuro. Queste sono esigenze di base che non dovrebbero comportare costi aggiuntivi.

Sicurezza

Molte violazioni hanno origine sul perimetro delle LAN cablate e wireless LAN, nel punto di connessione di utenti ed endpoint. Spesso le reti cablate e wireless non vengono costruite pensando alla sicurezza. Questo porta a soluzioni in cui le funzioni di sicurezza, aggiunte a posteriori in modo artificioso, sono ulteriormente isolate e limitate in quanto a efficacia. Per gli amministratori IT e di sicurezza che supportano la LAN, la mancanza di integrazione comporta un aumento del tempo necessario per rilevare e risolvere i problemi. Questo può aumentare significativamente i costi operativi quando si verificano eventi di sicurezza. I ritardi si traducono anche in un aumento dei danni causati dall'attacco.

Come scegliere una soluzione integrata per il perimetro LAN

Una soluzione LAN tradizionale, in cui i costi principali sono rappresentati dall'hardware e non dagli abbonamenti, non appartiene al passato. Cerca fornitori di soluzioni che comprendano già le funzionalità chiave necessarie, preferendoli a chi le fornisce solo dietro pagamento aggiuntivo. Una soluzione per il perimetro LAN deve includere come minimo:

- Gestione unificata di reti cablate e wireless sia in locale che nel cloud
- Hardware che funzioni anche se una licenza scade
- Funzionalità di intelligence che rilevano ciò che è connesso alla LAN e sono in grado di intervenire contro dispositivi non autorizzati
- Sicurezza integrata ed efficace

Per semplificare la distribuzione e la gestione del perimetro LAN e ridurre il più possibile il costo totale di proprietà (TCO), è necessaria una soluzione dove rete e sicurezza convergono. Un'architettura sicura e facile da gestire, con tutte le funzionalità necessarie incluse, ridurrà le spese operative e aumenterà le prestazioni.

¹ "Networking Technology Trends in 2020 and Beyond," SpiceWorks Ziff Davis, consultato il 1° febbraio 2022.

² "How Prepared Is Your IT Department for Attacks on IoT Devices?" Virginia Business Systems, consultato il 1° febbraio 2022.