Il futuro delle reti è “user-centrico”

L’evoluzione delle tecnologie di rete, con l’ascesa di architetture come SASE e SSE, segna una svolta verso un approccio “user-centrico”. Una sfida per i network manager, chiamati a garantire prestazioni elevate, sicurezza robusta e un’esperienza utente senza intoppi, attraverso l’adozione di DEX e soluzioni innovative

Data creazione documento: 28 luglio 2025
Autore: Alessandro Lavarra
Versione: 1
Data Ultimo Aggiornamento: 28 luglio 2025

C'è un discreto fermento nel panorama delle tecnologie di rete. Abbiamo assistito a movimenti societari importanti come l'acquisizione da 16 miliardi di dollari di Juniper da parte di HPE e all'affermarsi di nuovi trend come le architetture SASE (Secure Access Service Edge) e le soluzioni SSE (Secure Service Edge).

Qualcosa è cambiato nel modo in cui pensare la rete e una nuova prospettiva si apre per i responsabili delle infrastrutture, chiamati a garantire non solo prestazioni e sicurezza, ma anche un'esperienza d'uso digitale impeccabile.

La centralità della rete come supporto attraverso cui si fruisce dei servizi digitali e la sua relativa staticità tecnologica ce l'hanno fatta apparire quasi come una commodity acquisita. "Avere rete" è una condizione che gli utenti percepiscono come scontata in qualsiasi luogo e verso qualsiasi risorsa. Quello che fa la differenza è la qualità dell'esperienza d'uso che sperimentiamo nell'utilizzo delle applicazioni.

I network manager, quindi, non solo devono garantire un alto grado di accessibilità e il giusto livello di sicurezza ma devono farlo garantendo un'esperienza d'uso fluida. Rallentamenti, interruzioni o procedure complesse per accedere alle risorse saranno percepite come disservizi, con ripercussioni negative sulla produttività e sul livello di soddisfazione.

La Digital Employee Experience (DEX) o Digital UX si configura come la nuova metrica dei servizi di networking ponendo l'accento sull'esperienza utente e sulla fluidità delle procedure. I network manager assumono un ruolo attivo di primaria importanza nel supportare il futuro della trasformazione digitale potendo incidere direttamente sull'esperienza d'uso delle procedure e indirettamente rendendo visibili i colli di bottiglia, le performance delle applicazioni o il reale utilizzo dei diversi servizi e applicativi.

Oggi poche aziende hanno la reale comprensione delle interazione dei propri utenti con le applicazioni e i servizi ma una infrastruttura di rete ben architettata e progettata con i giusti strumenti agisce su 4 livelli ai fini dell'esperienza d'uso

1. garantisce alte performance di rete con ottimizzazione e prioritizzazione del traffico.
2. dà visibilità sul reale accesso alle risorse locali, a quelle distribuite nella rete geografica e a quelle in cloud o SaaS.
3. In fase di troubleshooting permette di identificare i reali colli di bottiglia e di identificare se gli eventuali disservizi sono da ricercare sulla rete, sugli apparati di rete, sugli applicativi o sugli endpoint.
4. Utilizza meccanismi di sicurezza zero trust per rendere l'esperienza d'uso, degli utenti, fluida e omogenea mantenendo al contempo la sicurezza.

Le soluzioni

Una rete predisposta a soddisfare la nuova metrica della Digital Employee Experience deve garantire visibilità su quello che accade non perdendo di vista la sicurezza.

Le soluzioni per la WAN e per l'accesso alle risorse in Cloud sono le architetture SASE.

Un servizio di WAN as a Service come CATO Networks, oltre ai generici benefici del SASE, permette di:

- gestire in modo fluido e con la stessa tecnologie gli utenti quando sono in sede e quando sono in mobilità,
- misurare in modo capillare e di immediata consultazione, il reale uso delle applicazioni e gli accessi alle risorse in tutta la propria rete,
- avere visibilità e controllo proattivo sulle performance delle connessioni internet, latenze, perdita di pacchetti o jitter
- incidere sull'efficienza della rete attraverso, QoS, prioritizzazione, accelerazione, routing proprietario performance-driven, singolo punto di gestione dei pacchetti dati, stabilità del backbone.
- garantire capacità di calcolo senza limiti per firewalling e IPS
- superare i compromessi tra sicurezza e performance della VPN grazie alle logiche zero trust degli utenti mobili SDP (Software Defined Perimeter) e rendere l'esperienza d'uso più fluida.

Nella rete locale, invece, le soluzioni attente all'esperienza d'uso degli utenti partono dalla visibilità di quello che accade in rete per supportare i team IT nelle fasi di detection, diagnosis e remediation e dalle logiche ZTNA per garantire esperienze d'uso fluide anche in contesti sicuri. Un esempio efficiente in questo senso sono le reti adattive di Extreme Networks con le quali si ottiene:

- visibilità capillare sui tempi di risposta della rete, dell'applicazione o del dispositivo dell'utente permettendo di individuare subito le inefficienze,
- mappa dinamica della rete con link e allarmi immediatamente identificabili,
- visibilità dei tempi di risposta dei servizi di rete (DHCP, DNS, LDAP, RADIUS)
- visibilità immediata delle applicazioni e delle risorse di rete a cui gli utenti accedono,
- visibilità dei dispositivi collegati con informazioni arricchite (utente, tipologia, sistema operativo, rischi di sicurezza, localizzazione)
- Sicurezza fino a L7 applicativo all'edge (switch e AP) di modo da distribuire la capacità di calcolo su più apparati e non occupare la rete con traffico non consentito fermandolo direttamente alla periferia.
- Erogazione all'utente dei servizi di rete a cui è abilitato in modo dinamico al momento della sua connessione

Le sfide della sicurezza e della carenza di risorse.

Assecondare l'agilità e le performance richieste dagli utenti molto spesso spinge le organizzazioni a scontrarsi con problemi di sicurezza e di risorse.

La trasformazione digitale richiede alla rete di essere un elemento abilitante e il business si aspetta che i team IT siano in grado di gestire:

- **cambiamenti di assetto:** Le aziende si evolvono velocemente, con acquisizioni, fusioni, ristrutturazioni e aperture di nuove sedi o semplicemente con maggiore mobilità degli utenti o centralizzazione dei processi gestionali.

- **Accesso ai servizi in cloud:** Il cloud computing è diventato un elemento chiave. L'architettura incentrata su sicurezza perimetrale firewall-centrica e le reti a centro stella non sono più funzionali quando le risorse sono così distribuite. Servizi in cloud e applicazioni SaaS sono scelte strategiche anche per garantire alti livelli di usabilità ma comportano un aggiornamento adeguato dell'ecosistema di servizi di rete.
- **Utenti mobili, reti geografiche, Iot e OT:** Le aziende operano a livello globale, con reti che si estendono su più continenti, con utenti in mobilità, con interazioni profonde con fornitori e clienti, con dispositivi intelligenti distribuiti e l'equilibrio tra disponibilità dei servizi, sicurezza e usabilità è sempre più globale e sfidante.

A causa della troppa apertura e permissività dei sistemi che aumenta il rischio di incidenti di sicurezza e della rincorsa alle prestazioni si tende a procedere con aumenti di banda e di capacità di elaborazione e a sovrapposizione di strati e tecnologie di sicurezza portando complessità in un contesto che già soffre di mancanza di tempo e di risorse.

Molto raramente è stata messa in discussione l'architettura di rete, disegnata per condizioni di utilizzo e di rischio del tutto differenti dalle attuali e che quindi lascia esposti a rischi informatici, a volte anche banali, nonostante i forti investimenti in sofisticate soluzioni di cybersecurity o servizi esterni .

Le architetture SASE con la convergenza in un unico punto della sicurezza e della gestione di tutti gli edge, oltre ai benefici descritti, alzano di molto il livello di sicurezza con approcci realmente privi di complessità e molto trasparenti. I servizi per le reti geografiche cloud native si prestano, tra l'altro, ad essere fruiti anche completamente as a service appoggiandosi a partner tecnologici MSP così da ridurre ulteriormente l'effort per i team IT.

Il nuovo approccio alle reti abilitato da tecnologie come Extreme Networks, da parte loro, garantiscono la stessa trasparenza e gestibilità per le reti locali cablate e wireless e portano ad un livello superiore il concetto di security by design grazie ai principi di microsegmentazione, controllo accessi, fabric e sicurezza alledge.

Anche questi approcci sono requisito abilitante per servizi di Network Operation Center capaci di aumentare l'efficienza della rete e ridurre l'impatto sulle attività dei team interni. Le funzioni di configurazione automatica dei servizi e degli apparati, la gestione da console, lo spostamento delle capacità sul software e non sull'hardware completano il quadro in termini di flessibilità e gestibilità.

https://www.gartner.com/en/doc/758833-top-use-cases-for-digital-employee-experience-tools

Farei i conti con la sicurezza

Soffermarsi sui dati dell'attualità in tema sicurezza risulta perfino scontato. I responsabili della sicurezza hanno perfettamente chiaro il rischio a cui sono esposte le organizzazioni. e l'affidabilità di un'azienda non è più determinata solo dalla sua capacità di produrre ricchezza e garantire stabilità ma anche dalla sua capacità di proteggere il proprio business e i dati che custodisce dalle minacce esterne.

La mancanza di cultura della sicurezza che il nostro paese si è trovato a fronteggiare ha fatto sì che, molto di frequente, la sicurezza non è maturata all'interno delle organizzazioni con un processo evolutivo graduale e radicato, ma è stata vissuta come un'urgenza o un ritardo a cui porre rimedio spingendo verso l'acquisizione di servizi o tecnologie senza una strategia alla base.

Molto raramente è stata messa in discussione l'architettura di rete, disegnata per condizioni di utilizzo e di rischio del tutto differenti dalle attuali e che quindi lascia esposti a rischi informatici, a volte anche banali, nonostante i forti investimenti in sofisticate soluzioni di cybersecurity o servizi esterni .

Il proliferare di intelligenza distribuita sul campo mediante dispositivi IoT e OT introduce nuovi rischi e nuove complessità in termini di segmentazione della rete, di soluzioni di sicurezza dedicate e di distribuzione geografica degli apparati da raggiungere e gestire.

Il cronico problema dello "skill shortage".

La richiesta di sempre maggiore agilità e le sfide di sicurezza sono certamente impegnative ma, senza le risorse adeguate, risultano impossibili.

Da un sondaggio svolto dalla mia azienda il 29% degli intervistati ha dichiarato che "gestire ambienti complessi con poco tempo e risorse ridotte" è l'affermazione che più rappresenta il loro stato mentre al terzo posto con il 17% (dopo la necessità di contenere i costi *ça va sans dire*) si riconoscono nella frase "nella mia azienda c'è scarsa o nulla possibilità di formazione e scouting per nuove tecnologie".

Anche nel panorama internazionale le cose non cambiano e un simile questionario di Gartner, che descrive le sfide degli infrastructure manager, ha tutte e 5 le prime posizioni occupate da questioni relative alla mancanza di competenze (Insufficient skill, lack of maturity, technical debt, inability to keep pace, lack of innovation)

Per contro, i network e security manager cercano nei partner soprattutto un aiuto operativo su tecnologie già acquisite in autonomia (27% ricerca competenze tecniche su una determinata tecnologia e il 21% si rivolge ad un partner per capacity interna insufficiente).

Non riconoscendo, di fatto, il ruolo di contributo alle scelte e all'innovazione dei propri partner tecnologici.

Su questo tema e sulle possibili motivazioni, nell'ultimo report sulla **roadmap strategica per le reti,** Gartner solleva un elemento su cui molto abbiamo discusso anche con i vendor con cui collaboriamo. Troppo spesso i fornitori di tecnologie si limitano ad interpretare il loro ruolo commerciale portando dai clienti l'ultima tecnologia disponibile, senza poi essere in grado di mettere a terra progetti guidati da precisi outcome attesi e capaci di generare effettivo impatto.

La soluzione a questo scenario complesso si deve giocare su tre livelli; tecnologico, culturale e organizzative.

1. **Tecnologiche**. Per inseguire agilità e facilità di manovra con scarse risorse è necessario dotarsi di tecnologie che possiedano alcune caratteristiche abilitanti. Semplificare è la parola d'ordine e per farlo è necessario centralizzare più funzioni, essere as a service per garantire flessibilità e scalabilità, essere curate nel'usabilità e lineari nel licenscing per non nascondere complessità in fase di evoluzione, devono possedere strumenti di analisi e visibilità delle performance e dell'uso della rete.
   Nel mondo delle reti queste sono tipicamente le architetture single vendor SASE (Con in testa CATO che ha fatto della convergenza, della trasparenza, del single pane of glass e dell'usabilità e del licesnsing lineare il cardine della propria value proposition o, per le reti locali , l'offerta Extreme Network che con con la piattaforma di gestione XIQ pilota apparati proprietari e di terze parti con una unica licenza svincolata all'hardware senza

complessità garantendo Visibilità e controllo degli accessi oltre alle funzionalità FABRIC native su tutto l'hardware e una "obsevability" capillare sull'uso della rete.

2. **Culturale - Convergenza rete e sicurezza**. i team infrastruttura e sicurezza devono dialogare e condividere obiettivi comuni con al centro l'esperienza utente e non la rincorsa a tecnologia per tecnologia. Oggi ognuno dei due dipartimenti per perseguire i propri risultati tende a portare in casa o a rinnovare le tecnologie e ad aggiungere. di fatto rendendo più complesso e stratificato e quindi meno trasparente e gestibile con l'effetto paradosso di rendere meno efficiente e meno sicuro.
3. Organizzativo: **Outcome di business e collaborazione con i fornitori**. l'organizzazione interna deve lavorare per outcome chiari e condivisi mantenere la direzione e il controllo dei propri ambienti tecnologici e dei progetti ma affidarsi e fidarsi di partner tecnologici maturi e competenti non solo per strappare un punto percentuale di sconto sulla fornitura ma per co-progettare e far co-evolvere le infrastrutture in una roadmap chiara e condivisa. Niente il gioco delle parti cliente e fornitore in cui non si svelano i reali progetti ma si chiede una specifica tecnologia è necessario stringere alleanze con fornitori capaci di colmare il loro skill-gap, portare semplificazione, trasparenza e sfruttamento completo delle tecnologie adottate.

Non acquisire tecnologie puntuali per rispondere a un singolo pain e cercare di integrarle ma acquisire e adottare quelle architetture di rete capaci di integrare in modo elegante più funzioni di rete e più funzioni di sicurezza in un unico scenario. Questo determina la difficoltà di fare scelte "future proof" condannando le aziende al debito tecnologico e ad una scarsa maturità nell'evoluzione dei sistemi (neri primi 3 posizioni nelle risposte ad un sondaggio di Gartner del 2022 assieme a competenze insufficienti) e relegare i fornitori a semplici prestatori d'opera anziché alleati per il raggiungimento di obiettivi di business chiari.

La soluzione a questi bisogni è data dalle architetture SASE possibilmente gestite con servizi *single vendor* cloud native come CATO Networks che sono in grado di garantire:

- Attivazione interamente remotizzata di un sito (connettività SD-WAN, rete locale, servizi e regole di sicurezza di si
- curezza) in tempi che possono variare dall'ora alla mezza giornata a seconda della complessità, applicazione di regole per tutta la propria organizzazione da console centralizzata e con effetto immediato (pochi minuti).
- Ottimizzazione delle rotte da e per tutti gli edge della rete. La gestione del traffico all'interno del backbone proprietario garantisce la possibilità di ottimizzare le rotte senza generare backhaul e colli di bottiglia. Ogni pacchetto indirizzato ad un servizio in cloud, alla navigazione, ad una risorsa di rete interna sarà instradato e prioritizzato nel modo più efficiente.
- Gestione mediante software defined perimeter e con logiche di ZTNA di tutti gli utenti mobili e per tutte le risorsi di rete con la stessa teconologia e dalla stessa console di gestione di tutta la WAN

Farei i conti con la sicurezza

Soffermarsi sui dati dell'attualità in tema sicurezza risulta perfino scontato. I responsabili della sicurezza hanno perfettamente chiaro il rischio a cui sono esposte le organizzazioni. In qualche caso manca la piena consapevolezza, o il giusto coinvolgimento, di proprietà e direzioni generali meno sensibili, ma sempre più spesso la catena del valore

(clienti e fornitori) o i fondi quando presenti, impongono scelte adeguate per la sicurezza. Anche le normative, a partire dalla NIS2, sono sempre più chiare e perentorie sugli obblighi e i requisiti necessari per garantire sicurezza informatica e integrità dei dati.

L'affidabilità di un'azienda non è più determinata solo dalla sua capacità di produrre ricchezza e garantire stabilità ma anche dalla sua capacità di proteggere il proprio business e i dati che custodisce dalle minacce esterne.

La mancanza di cultura della sicurezza che il nostro paese si è trovato a fronteggiare ha fatto sì che, molto di frequente, la sicurezza non è maturata all'interno delle organizzazioni con un processo evolutivo graduale e ben radicato, ma è stata vissuta come un'urgenza o un ritardo a cui porre rimedio e le strategie adottate spesso sono state in sostanza due:

- il ricorso a servizi di sicurezza terzi,
- l'inserimento di tecnologie on top alle proprie infrastrutture.

Molto raramente è stata messa in discussione l'architettura di rete, disegnata per condizioni di utilizzo e di rischio del tutto differenti dalle attuali e che quindi lascia esposti a rischi informatici, a volte anche banali, nonostante i forti investimenti in sofisticate soluzioni di cybersecurity o servizi esterni . A riguardo dei quali, tra l'altro, vale la pena sottolineare che la consapevolezza dei propri bisogni e delle proprie condizioni in termini di sicurezza non è un affare delegabile a terzi o alle tecnologie per quanto evolute.

Traffico in rete dei dispositivi non IT.

Il proliferare di intelligenza distribuita sul campo mediante dispositivi IoT e OT introduce nuove complessità in termini di segmentazione della rete, di introduzione di soluzioni di sicurezza dedicate, di distribuzione geografica di apparati da raggiungere e gestire.

Il cronico problema dello "skill shortage".

La richiesta di sempre maggiore agilità e le sfide di sicurezza sono certamente impegnative ma, senza le risorse adeguate, risultano impossibili.

Da un sondaggio svolto dalla mia azienda il 29% degli intervistati ha dichiarato che "gestire ambienti complessi con poco tempo e risorse ridotte" è l'affermazione che più rappresenta il loro stato mentre al terzo posto con il 17% (dopo la necessità di contenere i costi *ça va sans dire*) si riconoscono nella frase "nella mia azienda c'è scarsa o nulla possibilità di formazione e scouting su nuove tecnologie".

Anche nel panorama internazionale le cose non cambiano e un simile questionario di Gartner, che descrive le sfide degli infrastructure manager, ha tutte e 5 le prime posizioni occupate da questioni relative alla mancanza di competenze (Insufficient skill, lack of maturity, technical debt, inability to keep pace, lack of innovation)

Per contro, i network e security manager cercano nei partner soprattutto un aiuto operativo su tecnologie già acquisite in autonomia (27% ricerca competenze tecniche su una determinata tecnologia e il 21% si rivolge ad un partner per capacity interna insufficiente).

Non riconoscendo, di fatto, il ruolo di contributo alle scelte e all'innovazione dei propri partner tecnologici.

Su questo tema e sulle possibili motivazioni, nell'ultimo report sulla **roadmap strategica per le reti,** Gartner solleva un elemento su cui molto abbiamo discusso anche con i vendor con cui collaboriamo. Troppo spesso i fornitori di tecnologie si limitano ad interpretare il loro ruolo commerciale portando dai clienti l'ultima tecnologia disponibile, senza poi essere in grado di mettere a terra progetti guidati da precisi outcome attesi e capaci di generare effettivo impatto.

La soluzione a questo scenario complesso si deve giocare su tre livelli; tecnologico, culturale e organizzative.

4. **Tecnologiche**. Per inseguire agilità e facilità di manovra con scarse risorse è necessario dotarsi di tecnologie che possiedano alcune caratteristiche abilitanti. Semplificare è la parola d'ordine e per farlo è necessario centralizzare più funzioni, essere as a service per garantire flessibilità e scalabilità, essere curate nel'usabilità e lineari nel licenscing per non nascondere complessità in fase di evoluzione, devono possedere strumenti di analisi e visibilità delle performance e dell'uso della rete.
   Nel mondo delle reti queste sono tipicamente le architetture single vendor SASE (Con in testa CATO che ha fatto della convergenza, della trasparenza, del single pane of glass e dell'usabilità e del licesnsing lineare il cardine della propria value proposition o, per le reti locali , l'offerta Extreme Network che con con la piattaforma di gestione XIQ pilota apparati proprietari e di terze parti con una unica licenza svincolata all'hardware senza complessità garantendo Visibilità e controllo degli accessi oltre alle funzionalità FABRIC native su tutto l'hardware e una "obsevability" capillare sull'uso della rete.
5. **Culturale - Convergenza rete e sicurezza**. i team infrastruttura e sicurezza devono dialogare e condividere obiettivi comuni con al centro l'esperienza utente e non la rincorsa a tecnologia per tecnologia. Oggi ognuno dei due dipartimenti per perseguire i propri risultati tende a portare in casa o a rinnovare le tecnologie e ad aggiungere. di fatto rendendo più complesso e stratificato e quindi meno trasparente e gestibile con l'effetto paradosso di rendere meno efficiente e meno sicuro.
6. Organizzativo: **Outcome di business e collaborazione con i fornitori**. l'organizzazione interna deve lavorare per outcome chiari e condivisi mantenere la direzione e il controllo dei propri ambienti tecnologici e dei progetti ma affidarsi e fidarsi di partner tecnologici maturi e competenti non solo per strappare un punto percentuale di sconto sulla fornitura ma per co-progettare e far co-evolvere le infrastrutture in una roadmap chiara e condivisa. Niente il gioco delle parti cliente e fornitore in cui non si svelano i reali progetti ma si chiede una specifica tecnologia è necessario stringere alleanze con fornitori capaci di colmare il loro skill-gap, portare semplificazione, trasparenza e sfruttamento completo delle tecnologie adottate.

   Non acquisire tecnologie puntuali per rispondere a un singolo pain e cercare di integrarle ma acquisire e adottare quelle architetture di rete capaci di integrare in modo elegante più funzioni di rete e più funzioni di sicurezza in un unico scenario. Questo determina la difficoltà di fare scelte "future proof" condannando le aziende al debito tecnologico e ad una scarsa maturità nell'evoluzione dei sistemi (neri primi 3 posizioni nelle risposte ad un sondaggio di Gartner del 2022 assieme a competenze insufficienti) e relegare i fornitori a semplici prestatori d'opera anziché alleati per il raggiungimento di obiettivi di business chiari.

Conclusioni:

Per i punti 1 e 2 I dispositivi firewall di ultima generazione stanno diventando l'ultima generazione di dispositivi firewall

Da un lato l'approccio Secure Service Edge (SSE-SASE) sta sostituendo i firewall e i proxy con Secure Web Gateway in cloud, CASB e Zero Trust, offrendo sicurezza da qualsiasi luogo.

Dall'altro lato, per la sicurezza della rete (anche OT e IoT) è necessaria una segmentazione on-premise e per questo i servizi di sicurezza vengono erogati direttamente all'edge (negli access point, negli switch, nei gateway SD-WAN, nei data center a livello L4- L7.

Sempre maggiore convergenza tra temi di sicurezza e di rete

Le architetture SASE, il Software-Defined Perimeter e le strategie Zero Trust richiedono una accelerazione nell'allineamento tra obiettivi di sicurezza e di rete.

Nella maggior parte delle aziende i team sicurezza e rete hanno obiettivi diversi (a volte in conflitto) ma devono convergere per offrire una migliore esperienza d'uso agli utenti.

Quindi le reti dovrebbero essere

Network operation dovrebbero essere assistite digitalmente (anche grazie ad AI e ML)

SASE dovrebbe essere la prima scelta per le reti geografiche

Le capacità dell'infrastruttura di campus dovrebbero essere garantite dal software e non dall'hardware

i concetti zero trust dovrebbero essere alla base della progettazione delle reti

i team di rete e sicurezza dovrebbero avere focus e obiettivi comuni sul DEX (digital experience) degli utenti

Inceve le reti attuali sono;
configurazioni e gestioni manuali

gli upgrade e gli investimenti sono focalizzati a rinnovamenti puntuali di singoli apparati o tecnologie

la WAN è tradizionale e non flessibile

la rete di campus è hardware centrica

le VPN tradizionali sono la modalità preferita per gli utenti remoti

strumenti e progetti sono "network centrici" e non user centrici

bibliografia

• *Market guide for single vendor SASE (Gartner 2022)*

• *Strategic Roadmap for Enterprise Networking (Gartner 2023)*

Market Guide for Digitale Experience Monitoring (Gartner 2023

.