

Rete e sicurezza unificate

su oltre 150 siti produttivi.

Per proteggere i dati OEM su scala globale. Come un fornitore Tier 1 dell'automotive con oltre 30.000 dipendenti in 25 paesi ha consolidato una rete frammentata dalle acquisizioni, sostituito VPN e WAN legacy e governato l'adozione dell'AI su un'unica piattaforma SASE: Netskope One SD-WAN, Private Access e SSE.

150+	25	180	1
Siti produttivi globali	Paesi coperti	Siti SD-WAN entro fine anno	Piattaforma unica rete + sicurezza

IL CLIENTE

Fornitore Tier 1 Automotive Globale

Nato da una recente fusione tra due gruppi del settore, il cliente fornisce sistemi fluidi, tecnologie per interni ed esterni e air management a quasi tutti i principali OEM automotive. Conta circa 150 siti produttivi e 16 centri di ingegneria in 25 paesi: una catena di fornitura just-in-time in cui il downtime non e ammesso e in cui l'azienda custodisce dati di progettazione e proprieta intellettuale degli OEM, con precisi obblighi contrattuali di protezione.

SETTORE Manifatturiero — Automotive Tier 1	PRESENZA 25 paesi, operativita just-in-time
DIPENDENTI Oltre 30.000	CLIENTI Principali OEM automotive globali
FOOTPRINT ~150 siti produttivi, 16 centri di ingegneria	DATI CRITICI Progetti e IP degli OEM su una supply chain interconnessa

LE SFIDE

Quattro ostacoli critici

Le sfide che impedivano di garantire sicurezza operativa e conformita normativa.

01	Rete frammentata dalle acquisizioni Schemi di indirizzamento IP in conflitto, architetture non standardizzate e numerose soluzioni puntuali ereditate da fusioni e acquisizioni su oltre 150 stabilimenti.
02	VPN e firewall legacy Le reti firewall legacy degradavano prestazioni e connettivita; l'incoerenza e la mancanza di standardizzazione causavano problemi di accesso a dati e applicazioni per il personale.
03	Protezione dei dati OEM senza telemetria consolidata Dati di progettazione e proprieta intellettuale degli OEM distribuiti su una supply chain interconnessa, con obblighi contrattuali di protezione, ma strumenti di sicurezza isolati e privi di una telemetria completa.
04	Adozione dell'AI non governata La rapida diffusione di strumenti di AI generativa esponeva al rischio che dati di progettazione sensibili finissero in tool non autorizzati, senza visibilita su chi li usa e su quali dati vengono condivisi.

LA SOLUZIONE

Netskope One: SD-WAN + Private Access + SSE

Un'unica piattaforma SASE che converge rete e sicurezza: connettivita SD-WAN ad alte prestazioni, Zero Trust universale per IT, OT e dispositivi connessi, e servizi di sicurezza consolidati per web, cloud e applicazioni private, con intelligenza artificiale integrata.

Netskope One SD-WAN	SASE Branch: connettivita sicura e ad alte prestazioni con zero trust guidato dall'AI. E il backbone della nuova rete standardizzata su tutti i siti produttivi.
Netskope One Private Access	Universal ZTNA: sostituisce VPN legacy, NAC complessi e virtual desktop con un accesso unificato e sicuro a sistemi IT, OT e dispositivi connessi, incluso l'ERP on-premises.
Netskope One SSE	Security Service Edge: accesso sicuro a web, cloud e applicazioni private per la forza lavoro ibrida, con visibilita e governance sugli strumenti di AI (Netskope One AI Security).
Device Intelligence	Funzionalita agentless integrata nel Netskope One Gateway insieme a SD-WAN: visibilita sulle migliaia di dispositivi OT non gestiti sul plant floor e applicazione di policy basate sul rischio.

Fasi di Implementazione

01	Rollout SD-WAN sui primi 40 siti Deployment iniziale di Netskope One SD-WAN su 40 siti, poi esteso progressivamente a livello globale con un modello replicabile.
02	Standard di tiering per ogni sito Metodologia che definisce i requisiti per entrare nella rete unificata: indirizzamento IP, resilienza, ridondanza di rete, gestione dell'alimentazione, switch e router gestiti, dispositivi SD-WAN.
03	ZTNA e visibilita OT Attivazione di Private Access al posto delle VPN legacy e di Device Intelligence per la discovery e la governance dei dispositivi OT non gestiti in fabbrica.
04	Resilienza e governance AI Connettivita dual-path con backup cellulare terziario negli impianti critici a tutela del just-in-time; visibilita sui tool AI usati e sui dati condivisi, con indirizzamento degli utenti verso le soluzioni autorizzate.

I RISULTATI

Risultati raggiunti

1	Piattaforma unica Rete, firewall e sicurezza convergenti: meno strumenti standalone, operazioni semplificate	Day 1 Onboarding acquisizioni Accesso sicuro alle app critiche (incluso l'ERP on-premises) senza attendere l'integrazione completa della rete
180	Siti SD-WAN entro fine anno Rollout in linea con il piano, su uno standard di sito replicabile	Multi-path Resilienza di rete Connettivita ridondata e backup cellulare negli impianti critici just-in-time
AI	Visibilita e governance Controllo su quali strumenti di AI vengono usati e su quali dati vengono condivisi	OT Dispositivi non gestiti visibili Migliaia di device di fabbrica scoperti e governati con policy risk-based

"Prima era separato tra rete, firewall e sicurezza. Ora tutti abbiamo una piattaforma unica su cui possiamo collaborare e lavorare."

Vice President IT Infrastructure,
Fornitore Tier 1 automotive

Perche Netskope

- v Piattaforma unica che converge networking e sicurezza (SASE) con alte prestazioni
- v Universal ZTNA per IT, OT e dispositivi connessi, al posto di VPN e NAC legacy
- v Visibilita unificata su identita, dati e telemetria per un approccio zero trust
- v Onboarding rapido e standardizzato delle societa acquisite
- v Governance dell'AI generativa: visibilita sui tool utilizzati e sui dati condivisi

TRINITY LABS

sede_legale
Piazza IV Novembre 4, Milano

web
https://trinity-labs.it

linkedin
linkedin.com/company/trinity-labs-cyber

Tested. Trusted. Delivered.

© 2026 Trinity Labs S.r.l.s. · CONFIDENTIAL - All rights reserved

