



Trantor®

ACCESS POINT GESTITI · RETE SOVRANA

SecureWiFi

**Ogni dispositivo nel suo recinto,
ogni identità col suo certificato.**

Il WiFi aziendale con la segregazione facile: SSID e VLAN come recinti nominati, autenticazione con certificati al posto delle password condivise, e un server centrale — on-premise, a casa tua — che spinge la configurazione a tutti gli access point.



VLAN SENZA FATICA

CERTIFICATI, NON PASSWORD

PUSH DAL CENTRO

ON-PREMISE

LA DOMANDA GIUSTA

Chi può parlare con chi, sulla tua rete? Se la risposta è «tutti con tutti», SecureWiFi esiste per cambiarla — senza farne un progetto.

trantor.it

· info@trantor.it

La rete piatta è una scelta

Nelle aziende più attente alla sicurezza, il WiFi per i dipendenti spesso non esiste: troppo rischio collegare l'aria alle reti che contano. Così si vive col cavo — oppure si affronta un progetto da apparati blasonati, costoso e lungo. SecureWiFi è la terza via: una rete WiFi ad altissima sicurezza, in piedi con semplicità e in poco tempo, che porta i dipendenti anche sulle reti aziendali più critiche.

Il WiFi vietato

Dove i dati contano, la rete senza fili ai dipendenti è spesso proibita: nessuna fiducia, nessun WiFi — e la mobilità interna resta un desiderio.

Gli apparati blasonati

Le soluzioni avanzate — i Cisco della situazione — fanno fare tutto: al prezzo di licenze importanti e di un mestiere che pochi hanno in casa.

La password condivisa

Una chiave per tutti significa nessuna identità: chi entra non si distingue, e revocare l'accesso a uno solo è impossibile — si cambia la chiave a tutti.

L'IoT in salotto

Telecamere, sensori e stampanti — i dispositivi meno difendibili — siedono sulla stessa rete dei dati che valgono di più.

LA FILOSOFIA

«Segmentare non deve essere un progetto. Deve essere l'impostazione predefinita.»

Tre idee, un solo gesto

Recinti, non progetti

Nella console disegni i recinti — ospiti, IoT, uffici, sale riunioni — e ogni SSID vive nella sua VLAN. La segregazione non si costruisce: si dichiara. E la VLAN segue l'identità del dispositivo, non la presa a cui è vicino.

L'identità è un certificato

Autenticazione WPA-Enterprise su standard aperti (802.1X): ogni dispositivo ha il proprio certificato. Niente password condivise da far girare, nessuna chiave da cambiare quando qualcuno esce: si revoca il certificato di quel dispositivo, e gli altri non se ne accorgono. E dove il certificato non arriva — ospiti, dispositivi semplici — c'è la rete a password, singola o multipla, nel suo recinto separato.

La verità sta al centro

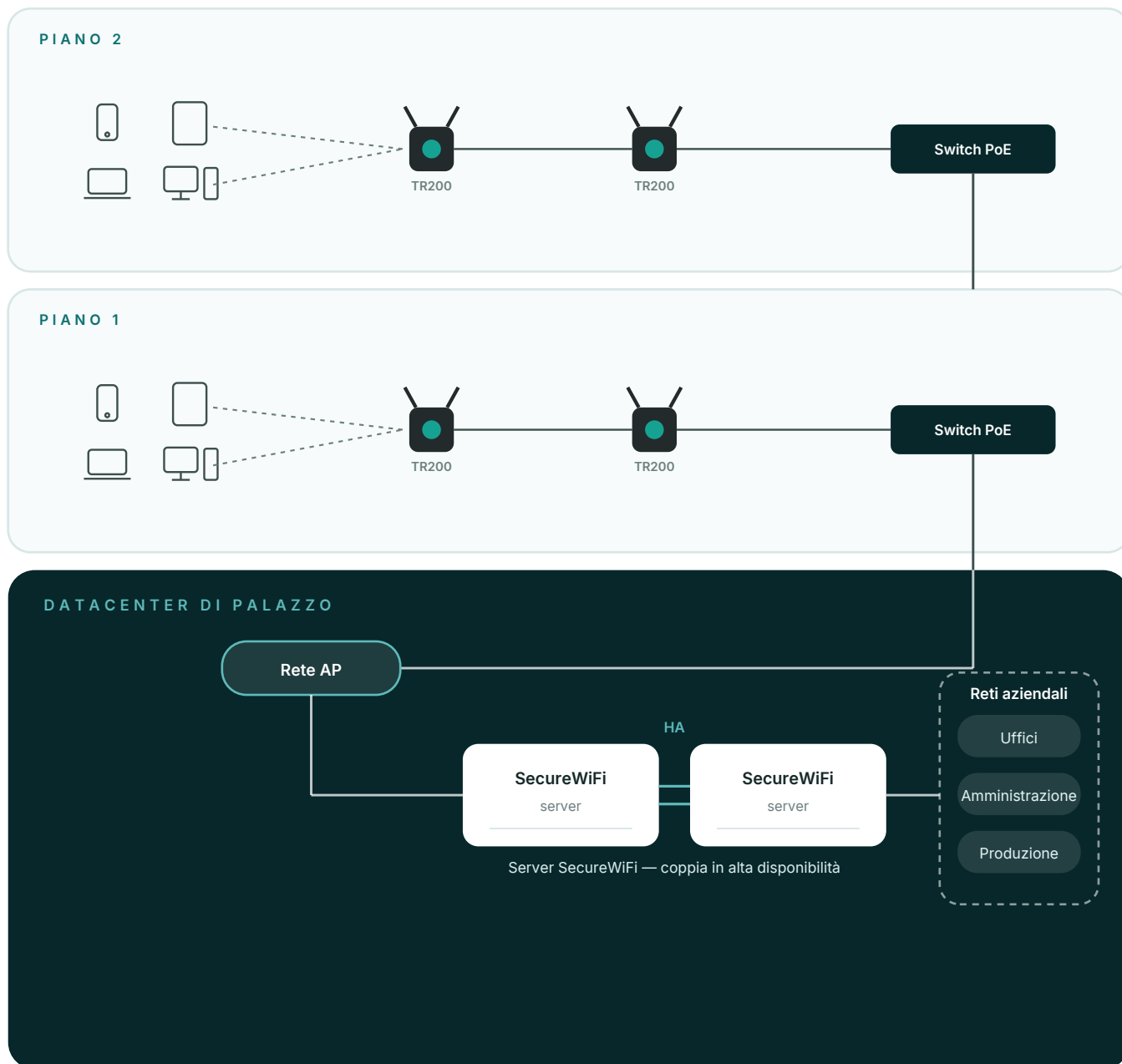
Il server centrale — on-premise, a casa tua — custodisce la configurazione e la spinge agli access point. Un AP nuovo si adotta e riceve tutto; uno sostituito riparte identico. Gli access point non custodiscono la verità: la ricevono.

NIENTE CLOUD OBBLIGATORIO

Il piano di controllo abita da te: la rete non dipende da un servizio esterno, dalle sue condizioni o dalla sua raggiungibilità. Sovranità significa anche questo.

Dal piano al datacenter

Un palazzo in sezione: su ogni piano i client — telefoni, tablet, portatili e PC fissi — parlano WiFi con gli AP; gli AP, alimentati e collegati dallo switch PoE di piano, confluiscono nel datacenter, dove il server SecureWiFi in alta disponibilità governa tutto.



Linea continua: collegamento cablato · linea tratteggiata: WiFi. Schema illustrativo — piani, AP e reti scalano a piacere.

LA STRADA DI UN ACCESSO

Il client si autentica sull'AP col certificato; la richiesta arriva al server dalla rete AP; il server verifica l'identità e apre il recinto giusto: da lì il client parla con le reti aziendali che gli spettano — e solo con quelle.

Di serie, dalla stessa console

Segregazione

- ✓ **Fino a due reti WiFi per access point:** tipicamente una a certificati per l'azienda, una a password per gli ospiti — ognuna nel suo recinto
- ✓ **Isolamento fra client** sulle reti ospiti: i visitatori non si vedono fra loro
- ✓ **VLAN dinamica per identità:** sulla rete a certificati, ogni utente atterra nella sua VLAN al momento del login
- ✓ **La rete ospiti non vede la rete dei dati** — e non è una regola da ricordare: è il disegno

Identità e accessi

- ✓ **Un certificato per dispositivo:** l'accesso è nominale, non una chiave di gruppo
- ✓ **Certificati via e-mail o portale self-service:** il dipendente scarica, e il resto è automatico
- ✓ **Standard aperti** (WPA-Enterprise, 802.1X): nessun client proprietario da installare
- ✓ **Revoca immediata del singolo device** — perso o dismesso — senza toccare gli altri
- ✓ **iOS importa da solo; Android con la nostra app** — il sistema non importa certificati nativamente, e lo diciamo prima noi
- ✓ **Autenticazione a scelta per ogni rete:** certificati, oppure password — singola o multipla, revocabile senza toccare le altre

Gestione dal centro

- ✓ **Configurazione dichiarata una volta,** spinta a tutti gli access point
- ✓ **Sostituzione senza riconfigurare:** l'AP nuovo riparte identico al vecchio
- ✓ **Adozione guidata del nuovo AP:** si collega, si adotta, riceve tutto
- ✓ **Aggiornamenti orchestrati dal centro,** su tutta la flotta

L'access point

- ✓ **Assemblato da noi,** su base Raspberry Pi 5 — hardware standard, sostituibile, dichiarato
- ✓ **Alimentazione PoE:** un cavo solo porta dati e corrente
- ✓ **Radio WiFi 6E tri-band:** 2,4, 5 e 6 GHz
- ✓ **Fino a 2 reti WiFi per AP,** ognuna col suo recinto e la sua autenticazione

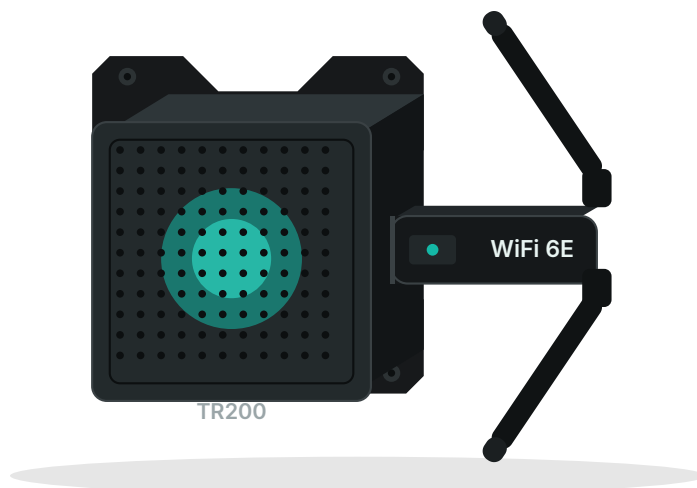
LA SEMPLICITÀ È IL PRODOTTO

Ogni voce di questa pagina si fa dalla console centrale, senza toccare gli AP uno a uno. È questo il punto: la sicurezza che non costa fatica è quella che si usa davvero.

AP TR200

05

Codice completo: **Trantor SecureWiFi AP TR200** — l'access point assemblato da noi, governato dal server centrale. Questo è il dispositivo, com'è davvero.



Specifiche del dispositivo	
Base	Raspberry Pi 5 — hardware standard, assemblato e collaudato da noi
Radio	Adattatore WiFi 6E tri-band: 2,4, 5 e 6 GHz
Alimentazione	Ingresso PoE: un solo cavo porta dati e corrente
Antenne	2 esterne snodate, orientabili
Montaggio	Piastra a parete o soffitto, inclusa
Reti WiFi	Fino a 2 per AP — a certificati, oppure a password (singola o multipla)
Segregazione	VLAN dinamica per identità: sulla rete a certificati ogni utente atterra nel suo recinto
Gestione	Adozione, configurazione e aggiornamenti in push dal server centrale

SI ADOTTA, RICEVE, LAVORA

Un AP nuovo o sostituito riparte identico, dal push del centro: la verità non abita sull'apparato.

In casa, per davvero

Il perimetro resta tuo

- ✓ **Server centrale on-premise:** come macchina dedicata, o come VM e container — ad esempio su Trantor TVirt
- ✓ **Nessuna telemetria obbligatoria:** idoneo agli ambienti isolati e classificati
- ✓ **I certificati nascono, si distribuiscono e si revocano** dalla stessa console, in casa
- ✓ **Standard aperti a ogni livello:** la rete resta leggibile e verificabile, anche senza di noi

Dentro il posto di lavoro sovrano

SecureWiFi chiude il perimetro della famiglia Trantor: **VDesk** è il posto di lavoro digitale, **TVirt** e **TVStor** sono il motore e lo storage, SecureWiFi è la porta d'ingresso — con l'identità nei certificati e ogni dispositivo nel suo recinto. Identità, rete e dati: tutti in casa, tutti sotto lo stesso interlocutore.

PER CHI NON PUÒ SBAGLIARE

Studi professionali, sanità, pubblica amministrazione, produzione: ovunque la rete ospiti convive con dati che valgono, la segregazione per costruzione non è un lusso — è il requisito. SecureWiFi la rende l'impostazione predefinita.

Governato, sostituibile, per iscritto

Come si compra, come si vive

- ✓ **Access point governati:** la flotta cresce adottando, non riconfigurando
- ✓ **Assistenza di chi scrive il codice:** un solo interlocutore per console, server e AP
- ✓ **Hardware sostituibile:** un AP guasto si rimpiazza e riparte identico, dal push del centro
- ✓ **Condizioni per iscritto:** funzionalità, compatibilità e assistenza — dichiarate prima della firma

Schede tecniche di dettaglio e listino completano il quadro — con la stessa regola di tutta la gamma Trantor: ogni riga verificabile, ogni promessa scritta.

LA PROSSIMA MOSSA

Disegniamo i tuoi recinti.

Una sessione con la mappa della tua rete: ospiti, IoT, uffici e sale — e il progetto di segregazione che diventa l'impostazione predefinita. Rispondiamo per iscritto.

trantor.it
info@trantor.it