



Trantor®

ACCESS POINT GESTITI · RETE WIFI SICURA E ON-PREMISE

SecureWiFi

**Ogni dispositivo isolato,
ogni identità col suo certificato.**

Il WiFi aziendale con la segregazione facile: SSID e VLAN isolano le connessioni, l'autenticazione con certificati si porta via le password condivise, e un server centrale (on-premise, nella tua azienda) gestisce la configurazione di tutti gli access point.



SEGREGAZIONE RESA FACILE

CERTIFICATI, NON PASSWORD

GESTIONE CENTRALIZZATA

ON-PREMISE

LA WIFI PER LE RETI AZIENDALI

Trantor® SecureWiFi permette alle aziende di adottare le comunicazioni WiFi in maniera complementare a quelle cablate, anche per le reti aziendali, che solitamente per motivi di sicurezza vengono private del canale senza fili.

trantor.it · info@trantor.it

10 agosto 2026

I contenuti di questa brochure (testi, grafiche, loghi) sono proprietà della PetaBit S.r.l. e sono protetti dalle norme su diritto d'autore e proprietà industriale e non possono essere riprodotti senza autorizzazione scritta. Gli altri marchi citati appartengono ai rispettivi proprietari. Le informazioni pubblicate hanno scopo informativo e non costituiscono offerta contrattuale, e PetaBit non garantisce l'assenza di imprecisioni. Tutti i prezzi esposti sono soggetti a modifiche e non costituiscono offerta contrattuale.

Cosa risolve Trantor® SecureWiFi

Nelle aziende più attente alla sicurezza, il WiFi per i dipendenti spesso non esiste: troppo rischio esporre via WiFi le reti più confidenziali. Così si limita l'infrastruttura alla sola rete cablata, oppure si affronta un progetto usando le soluzioni complesse sul mercato, costoso e lungo. SecureWiFi è la terza strada: una rete WiFi ad alta sicurezza, in piedi con semplicità e in poco tempo, che porta i dipendenti anche sulle reti aziendali più critiche.

Il WiFi vietato

La rete senza fili ai dipendenti è spesso proibita: nessuna fiducia, nessun WiFi, e la mobilità interna resta macchinosa. Implementare una rete WiFi non deve essere sinonimo di mettere a rischio la sicurezza della rete, anzi, può aumentarne la sicurezza.

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. SecureWiFi adotta i certificati per gli utenti stabili della WiFi, e password multiple usa-e-getta per gli ospiti.

Soluzioni esistenti, ma difficili da praticare

Le soluzioni più avanzate sul mercato sanno fare tutto: al prezzo di licenze importanti e di mesi di integrazione in azienda. E l'usabilità degli utenti finali di solito non è tra le priorità.

L'IoT in azienda

Telecamere, sensori e stampanti, che sono i dispositivi più vulnerabili, sono quelli che più hanno bisogno di connessioni senza fili sicure.

LA FILOSOFIA

«La rete WiFi non è solo per gli ospiti, ma può contribuire alla messa in sicurezza delle reti aziendali più critiche. Le aziende hanno diritto a una soluzione che permetta di fare tutto ciò in semplicità e poco tempo.»

Panoramica tecnica di SecureWiFi

Appliance server basata su Linux

Il software centrale Trantor® SecureWiFi Appliance è basato su AlmaLinux 10 e può essere installato su macchine virtuali o su bare-metal x86 e ARM. È lì che risiede il centro di comando della soluzione. E dispone di pieno supporto all'alta affidabilità tramite ridondanza.

Interfaccia web per gestione e self-service

Trantor® SecureWiFi Appliance espone un'interfaccia web sia per gli amministratori di sistema, con la quale possono gestire l'infrastruttura WiFi, sia per gli utenti finali, che la usano per gestire in autonomia la configurazione della WiFi sui propri dispositivi.

Dispositivi access-point WiFi Trantor®

La soluzione richiede access point ad hoc, i Trantor® SecureWiFi AP, che si collegano alla SecureWiFi Appliance, ed erogano la WiFi dentro la tua azienda. Questi dispositivi supportano alimentazione via PoE, aggiornamenti e gestione 100% centralizzata, e protocollo fino a WiFi 7 2.4/5/6GHz, con antenne estendibili via cavo.

Autenticazione via password multiple o certificato

SecureWiFi permette di creare reti WiFi che accettano password pre-condivise (con WPA2/WPA3-PSK), che possono essere anche multiple e/o usa-e-getta. Inoltre per gli utenti più stabili e critici supportiamo l'autenticazione via certificati e username+password (con WPA2/WPA3-Enterprise e 802.1X), che garantisce standard di sicurezza molto più elevati e autenticazione bidirezionale. SecureWiFi può essere autosufficiente: gli utenti locali possono risiedere nell'appliance. Se vuoi collegarlo velocemente alla tua directory aziendale, SecureWiFi comunica via LDAP anche con Active Directory, così l'appartenenza a un gruppo LDAP diventa il permesso di accedere a una certa rete WiFi. Chi ha anche Trantor® Imago lo può usare come backend di identità al posto di LDAP così da sbloccare funzioni in più, fra cui l'enrollment del dispositivo tramite SSO (OIDC e SAML); l'identità resta comunque in azienda, senza passare da nessun cloud.

Segregazione dei client e supporto a VLAN multiple

Ogni rete WiFi può far atterrare i client su una rete aziendale (VLAN) diversa, e anche la stessa rete WiFi può far atterrare i client in reti (VLAN) diverse a seconda di chi si sta connettendo a quell'AP. Inoltre, i client possono essere isolati in modo che un eventuale client infetto non possa attaccare chi si trova nella sua stessa WiFi.

IN ROADMAP: Diagnostica avanzata

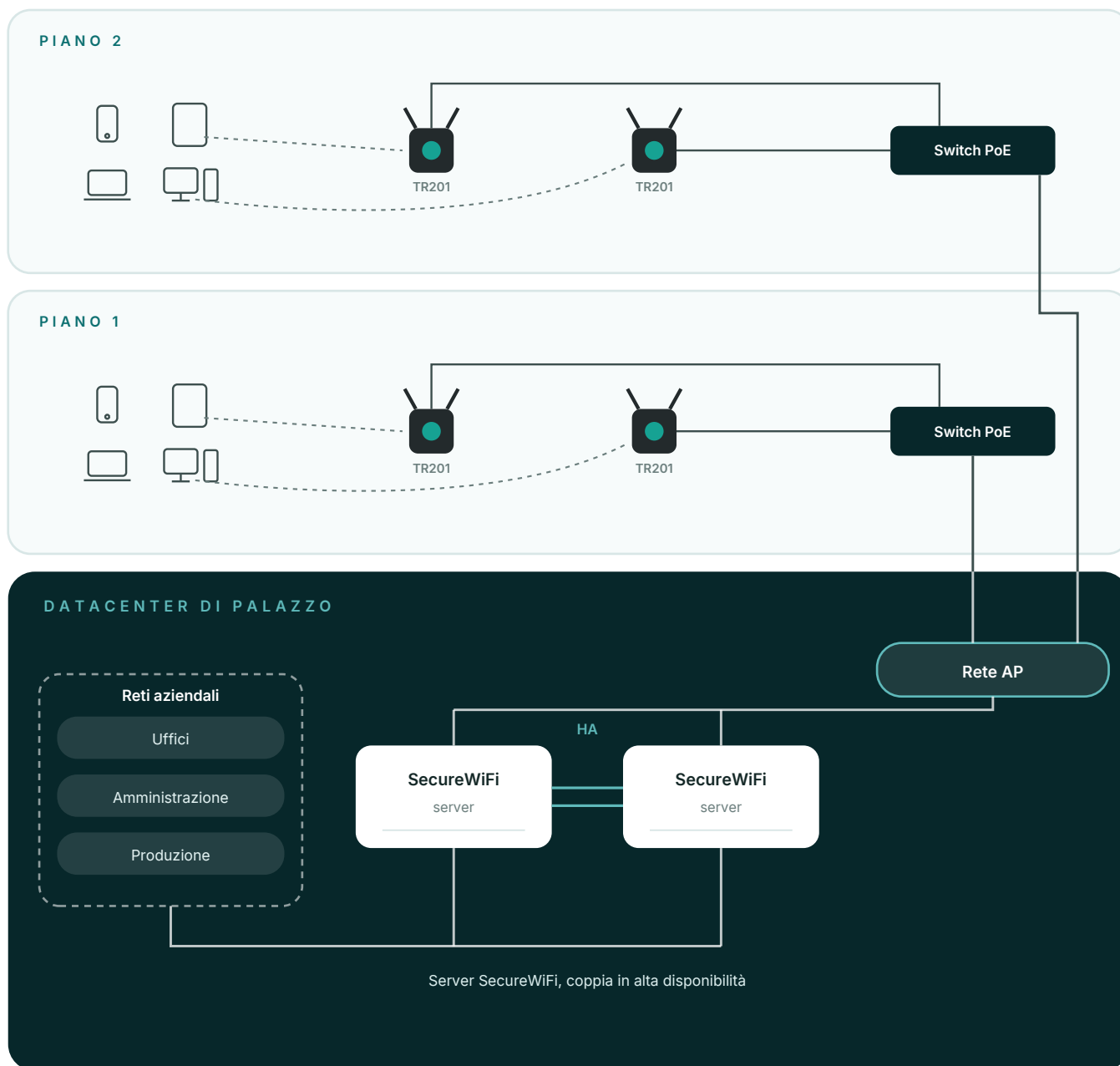
È in sviluppo un set di feature per la diagnostica avanzata dei problemi di connessione e stabilità, che include anche la raccolta del traffico di rete al momento del malfunzionamento in modo da permettere l'analisi anche di problemi intermittenti, e include anche statistiche predittive e testate sull'uso di software reali (es. le videochiamate). Come sempre, nessun dato esce fuori dalla tua azienda.

NIENTE CLOUD OBBLIGATORIO

Il controllo risiede on-premise nella tua azienda: la rete non dipende da un servizio esterno, dalle sue condizioni o dalla sua raggiungibilità. Anche gli ambienti air-gapped e confidenziali possono usufruire delle reti WiFi.

Dal piano al datacenter

A seguire lo schema di funzionamento della soluzione SecureWiFi: su ogni piano si trovano i client (telefoni, tablet, portatili, PC fissi, e dispositivi IoT/stampanti), che parlano WiFi con gli AP Trantor®; gli AP, collegati allo switch PoE di piano, confluiscono nel datacenter, dove l'appliance SecureWiFi in alta disponibilità governa tutto.



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

IL PERCORSO DI UN CLIENT

Il client si collega sull'AP di piano e si autentica col certificato parlando con il server centrale; il server verifica l'identità e fa atterrare il client nella rete aziendale (VLAN) corretta: da lì il client parla con il resto della rete seguendo le normali policy firewall e di sicurezza dell'azienda.

AP TR201

Nome completo: **Trantor SecureWiFi AP TR201**. L'access point assemblato da noi, e controllato dal server centrale. Di seguito le caratteristiche del dispositivo.



Specifiche del dispositivo	
Base	Scheda ARM64 con Linux
Protocolli WiFi	Due schede WiFi: una WiFi 5 (802.11ac) dual-band 2.4/5GHz e una WiFi 7 (802.11be) tri-band 2.4/5/6GHz (entrambe retro-compatibili con 802.11a/b/g/n e la scheda WiFi 7 retro-compatibile anche con 802.11ac/ax)
Alimentazione e rete cablata	Ingresso RJ45 1Gbit/s PoE+ (802.3at) 48V 20W: un solo cavo porta dati e corrente; nella confezione è anche incluso un iniettore PoE compatibile nel caso non si vogliano usare switch PoE
Antenne	Esterne, orientabili ed estendibili via cavo
Montaggio	Piastra a parete o soffitto, compatibile con standard VESA 100x100 e 75x75
Reti WiFi	Massimo 1 rete WiFi per ogni scheda (quindi massimo 1 rete WiFi 5, e massimo 1 rete WiFi 7)
Densità	Circa 25 client per access point, superficie variabile
Roaming	802.11r/k/v: il passaggio da un AP all'altro non interrompe la sessione
Trasmissione radio	Selezione automatica di canale e potenza, coordinata dal server centrale
Autenticazione WiFi	Supporto a WPA2/WPA3-PSK e WPA2/WPA3-Enterprise, sia con password singola/multiple, sia con certificati 802.1X
Segregazione e isolamento	VLAN statica per rete WiFi, oppure VLAN dinamica per utente
Gestione	Configurazione e aggiornamenti dal server centrale
Mesh	Non supportato, per scelta: ogni AP è collegato via cavo, così non esistono ponti radio invisibili dentro la rete

Trantor® SecureWiFi e le alternative

05

Ogni alternativa qui sotto è un prodotto serio, con punti di forza reali. Il confronto utile non è la lista delle funzioni: è dove risiede il controllo, se l'identità è compresa o è un secondo acquisto, e che cosa resta a carico tuo.

Soluzione	Dove risiede il controllo	Identità e onboarding	Da considerare
Trantor® SecureWiFi Trantor® · Italia	Appliance on-premise, su VM o bare metal: nessun cloud obbligatorio, funziona anche in ambienti isolati	Compresa e autosufficiente: RADIUS, CA e portale self-service, con utenti locali oppure LDAP verso la tua directory. Con Trantor® Imago si aggiunge l'enrollment via SSO (OIDC e SAML)	Access point Trantor® ad hoc per la piattaforma SecureWiFi, con possibilità di personalizzazione in base alle esigenze
Cisco Meraki Cisco · extra-UE	Cloud del costruttore, non opzionale	802.1X sì; la CA e l'onboarding richiedono Cisco ISE o un fornitore terzo	Il più diffuso e fra i più curati da usare; modelli solo pre-definiti
HPE Aruba Central e ClearPass HPE · extra-UE	Central è cloud, i controller on-premise restano disponibili	ClearPass copre identità e onboarding: prodotto e licenza separati	Fortissimo sulle installazioni dense; il costo si compone di più licenze, e la fusione con Juniper muove cataloghi e modelli di supporto
Juniper Mist HPE · extra-UE	Cloud obbligatorio: la diagnostica assistita è il prodotto	Access Assurance, a licenza separata, con SSO sul portale dell'utente finale	Diagnostica radio senza rivali; nessuna opzione on-premise, e il catalogo è in fase di consolidamento dentro HPE
Ubiquiti UniFi Ubiquiti · extra-UE	Controller on-prem oppure in cloud	RADIUS di base; i certificati e l'onboarding self-service non ci sono	Prezzo difficile da battere per gli uffici; manca la gestione avanzata delle identità, e il supporto non è di classe enterprise
PacketFence open source · con AP di terzi	On-premise	NAC completo: 802.1X, portale, VLAN dinamiche, certificati via SCEP	Software gratuito e maturo; integrazione con gli access point, dimensionamento e manutenzione restano a carico del cliente
SecureW2 · Portnox extra-UE · con AP di terzi	Cloud	È il loro mestiere: certificati, onboarding e RADIUS gestito, con SSO verso il tuo provider di identità	Non forniscono access point: si aggiungono a un'infrastruttura WiFi che possiedi già, e l'identità passa dal loro cloud

Posizionamento sintetico aggiornato ad agosto 2026, su fonti pubbliche. Ogni piattaforma citata è un prodotto valido nel proprio contesto d'uso; i marchi appartengono ai rispettivi proprietari.

LA PROSSIMA MOSSA

Progettiamo la tua WiFi.

Una sessione per mappare la tua rete: guest, IoT, uffici e sale, e il progetto di segregazione e autenticazione avanzata.

trantor.it
info@trantor.it