

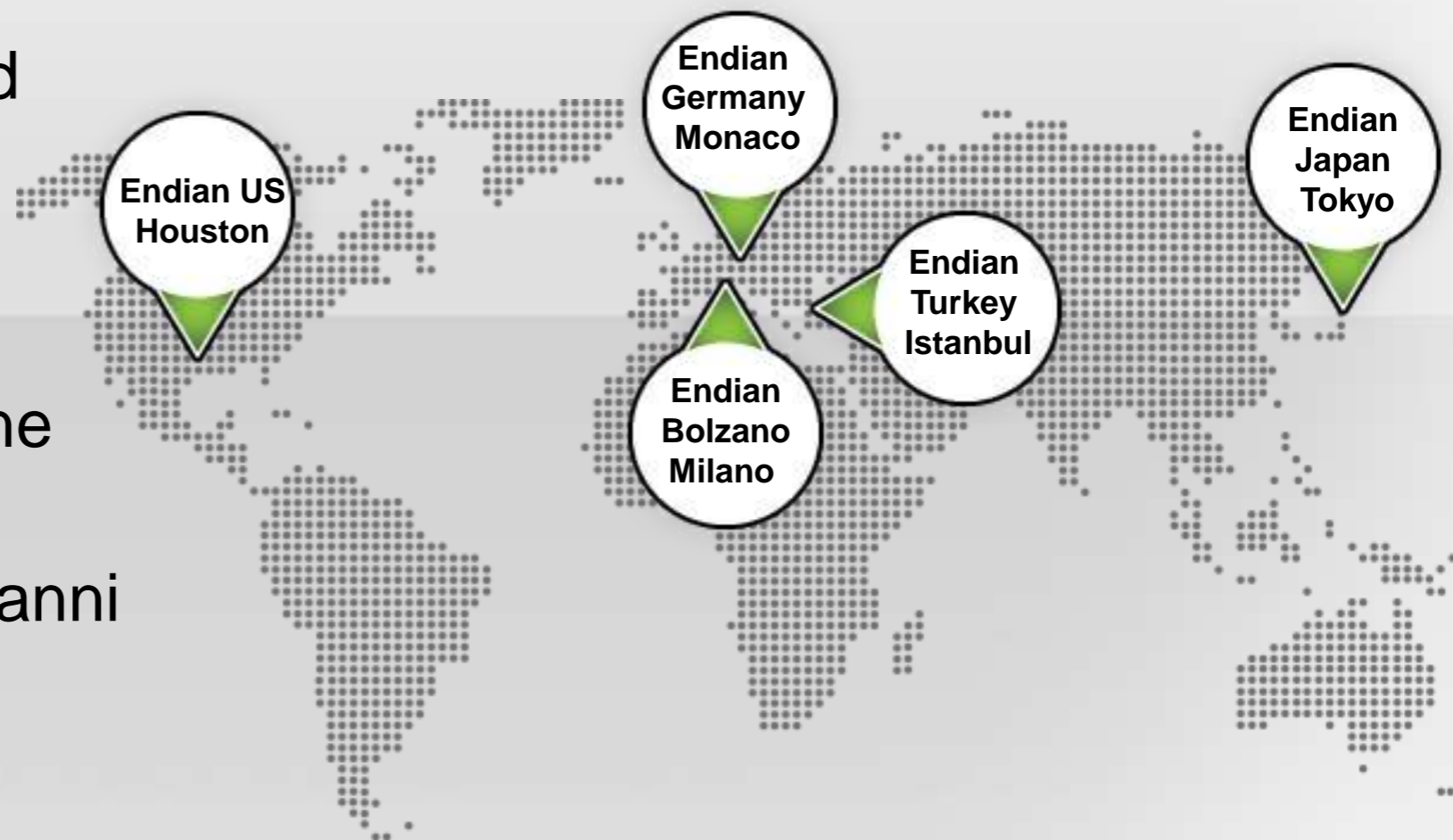


Endian 4i – VPN Switchboard

Alfredo Cusin – Sales Manager Endian
a.cusin@endian.com - Mob. 333 936711

Chi è Endian?

- Endian nasce nel 2003 ad Appiano, Italia
- Focus: Sicurezza della infrastruttura
- Nel 2005 nasce la versione community UTM.
- 1.200.000 download in 9 anni
- 25.000 contatti mensili
- 4.000 clienti WW.



Le Soluzioni Endian

Sicurezza dei dati nell'infrastruttura



Security Gateways
(UTM)



Hotspot
BYOD

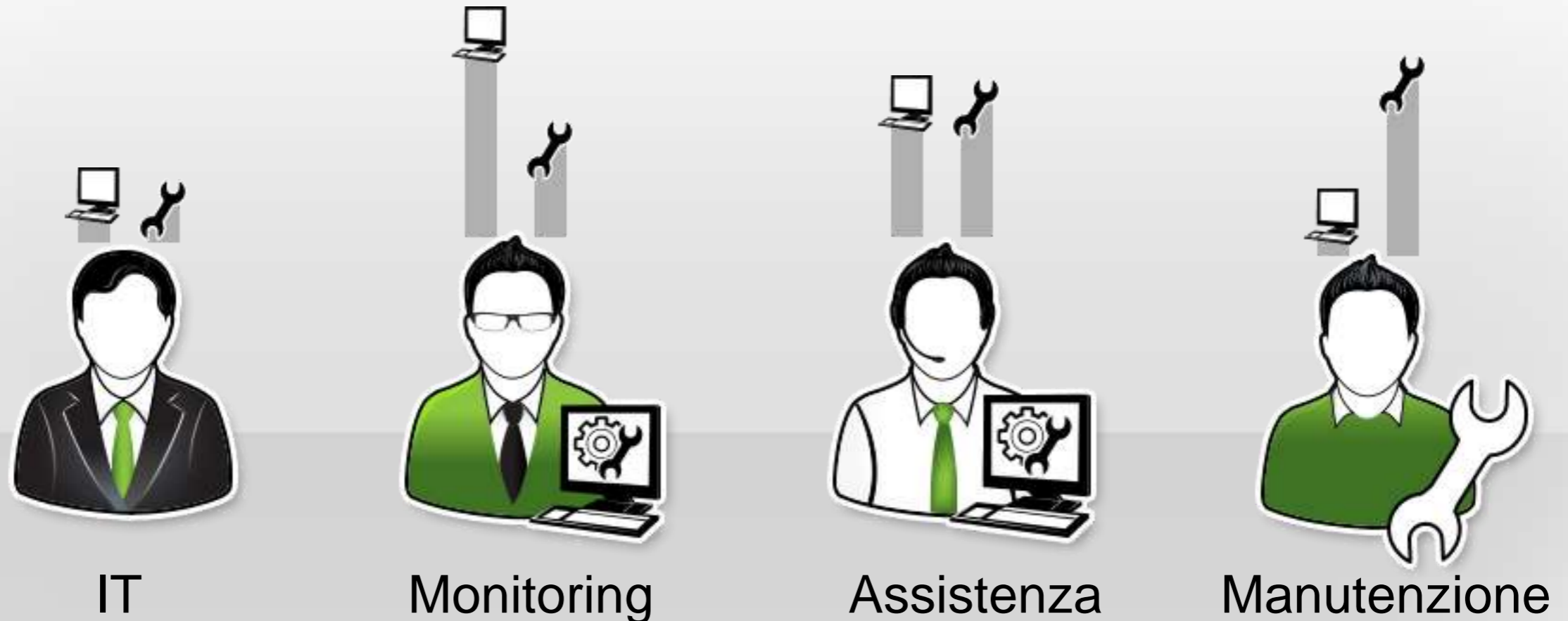


M2M 4i - Industrial

I nuovi rischi per i sistemi SCADA

- Ricerca di dispositivi nella rete, port scanning
- Invio di comandi non autorizzati
- Attacchi Man in the Middle
- Password breaking
- Viruses/Cyberweapons

**MOTIVAZIONI:
Hacking, Spionaggio,
Sabotaggio, Cyberterrorismo**



- Issues: necessità di rendere accessibili i sistemi a più utenti, alcuni di questi privi di competenza IT



IT



Monitoring



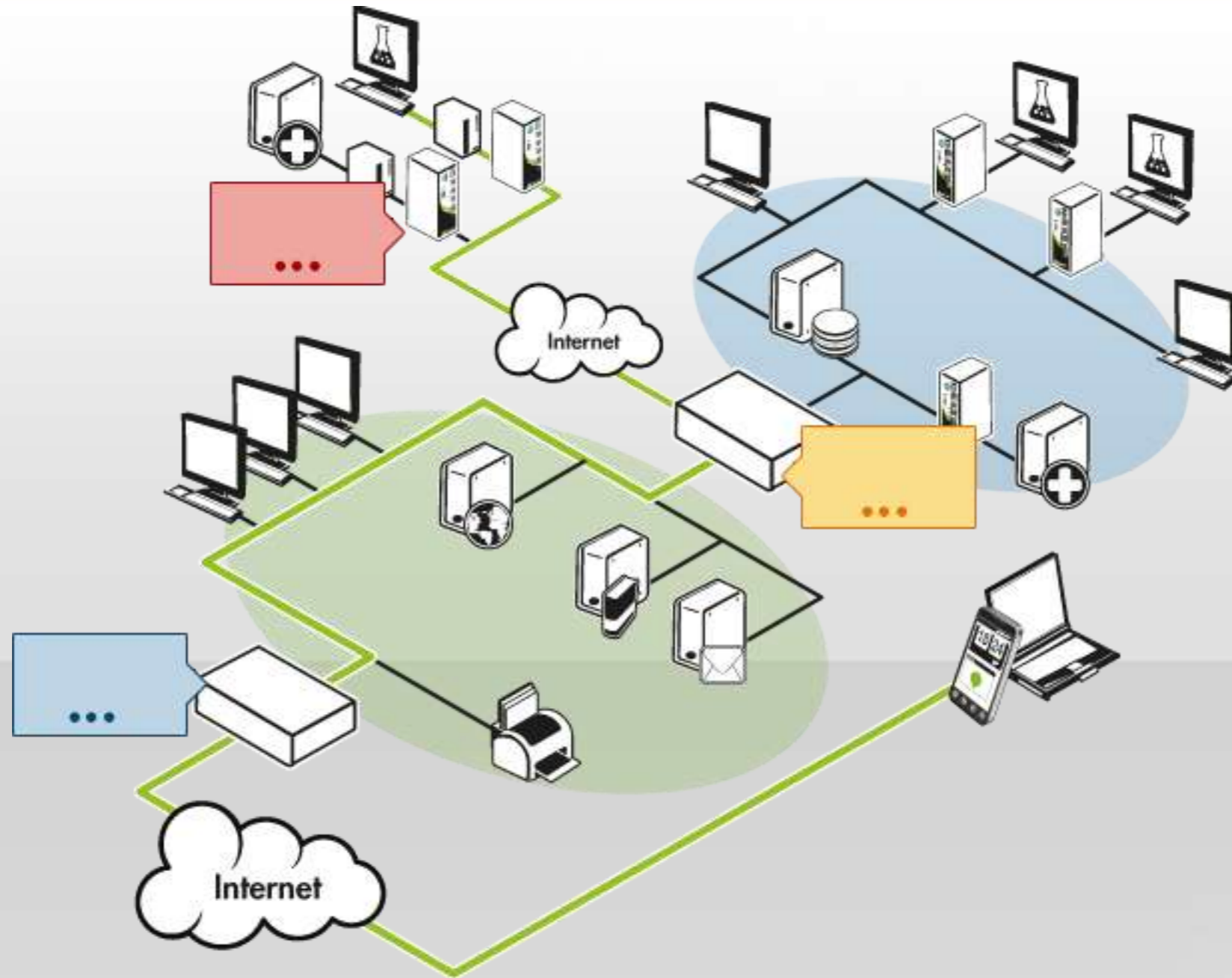
Assistenza



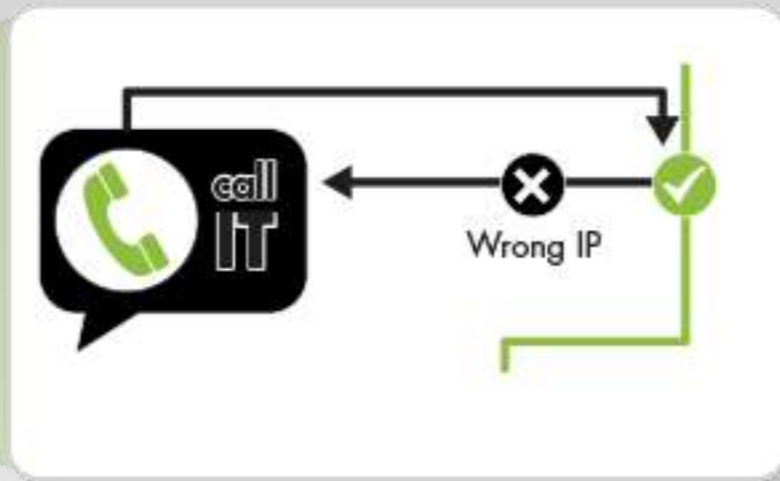
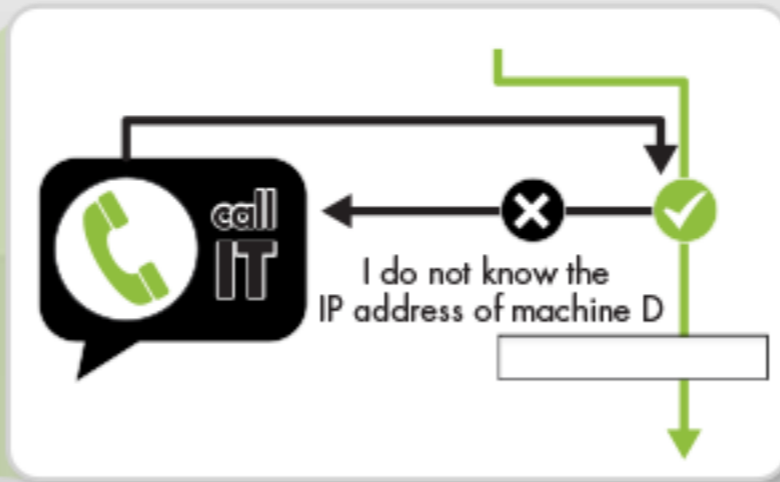
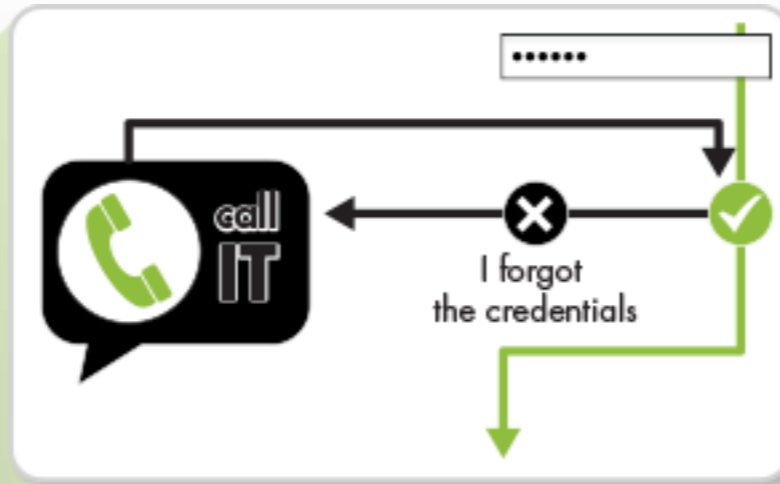
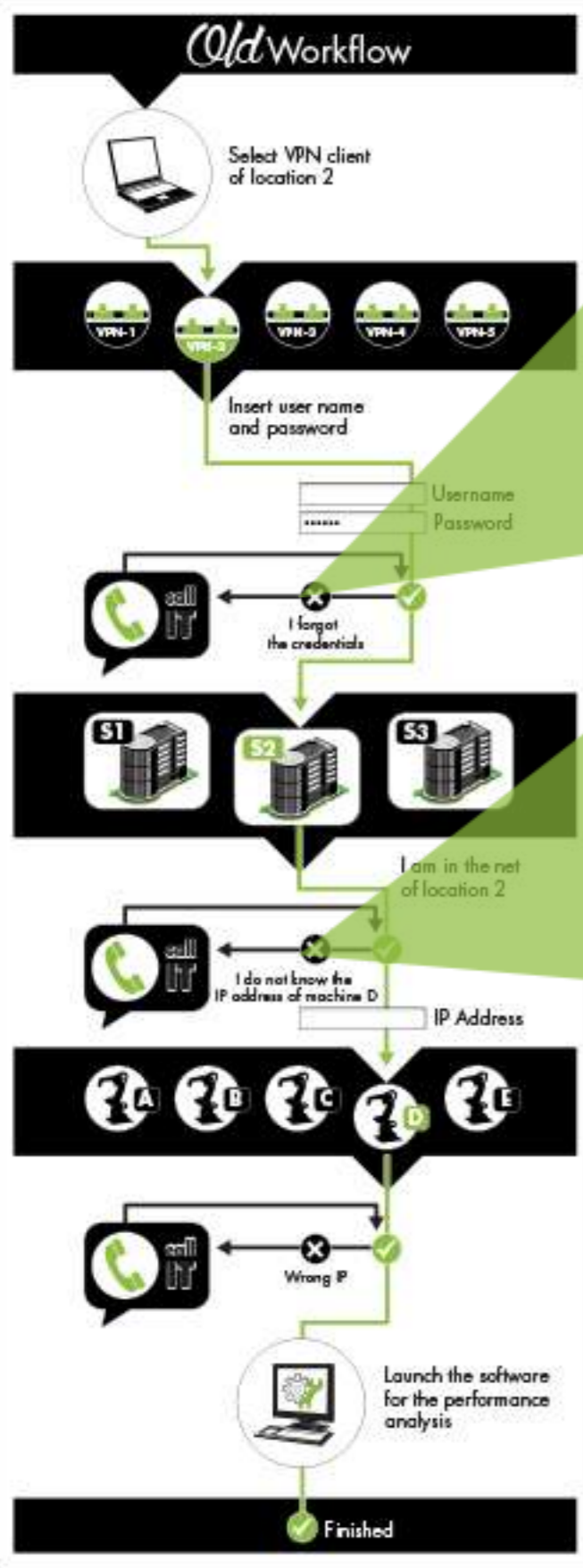
Manutenzione



Issues: Multi accesso



- Issues: esistenza di diversi sistemi VPN lato remoto richiede coinvolgimento con l'IT remoto e locale



Issues: complessità di accesso



ACCESSIBILITA SICURA

Endian 4i series e VPN Switchboard

ACCESSO sicuro e granulare

Il tecnico manutentore deve accedere agli impianti per dare supporto da remoto. L'utente finale vuole, tramite dispositivo mobile, consultare i dati prodotti da alcune di queste macchine. E strumenti per l'analisi della performance devono poter essere collegati per rilevare eventuali variazioni.

Endian VPN Switchboard è l'unico tool in grado di garantire accessi differenziati alle macchine per singolo utente o gruppo, abilitando solo i comandi necessari ed autorizzati per l'utilizzatore specifico.

SECURITY THROUGH OBSCURITY? NO, KEEP IT SIMPLE!

Grazie alle autorizzazioni personalizzate puoi in qualsiasi momento escludere l'accesso di un collaboratore che dovesse cambiare mansione o azienda, senza temere che egli porti via con sé le credenziali di accesso. Inoltre, grazie ai log che vengono scambiati tra periferia e sistema centrale, puoi sapere in qualsiasi momento cosa succede nella tua rete.



Integrazione con strutture già esistenti

I tuoi tecnici non hanno estese conoscenze informatiche ed esitano ad interfacciarsi con un nuovo strumento? Non c'è problema, perché grazie all'integrazione con le API, puoi accedere a tutte le funzionalità del VPN Switchboard direttamente dal tuo portale di supporto.



USB PROVISIONING

Le sedi periferiche in gateway che si collegano a Endian VPN Switchboard sono riconfigurare firewall a mano?

Certo che no! Con Endian VPN Switchboard il provisioning dei settaggi è comodo e semplice da realizzare tramite chiavetta USB. Le impostazioni scelte a livello centrale si trasferiscono ai gateway con un solo clic.



EASY DROP IN

Nessun problema nel caso in cui ci siano già degli endpoint in campo.

Con il VPN Switchboard è infatti possibile gestire qualsiasi device che utilizzi la tecnologia Open VPN (SSL).

Riduci costi e tempi di implementazione grazie all'integrazione del VPN Switchboard con tecnologie eterogenee.



...E inoltre:

- Il risparmio sulla gestione delle squadre dei tecnici è notevolissimo. Con un sistema di monitoraggio, gestione e manutenzione da remoto sicuro puoi limitare i costi di trasferta fino al 90%.
- Endian basa la realizzazione dei suoi prodotti su tecnologia open source: ciò significa che non possono esserci backdoor nascoste. I dati sensibili che tratti per il tuo business restano sempre assolutamente al sicuro.



La soluzione?

Endian 4i series e VPN Switchboard

La soluzione completa per la sicurezza dei sistemi....
anche SCADA

Cosa significa protezione IT in una rete aperta?

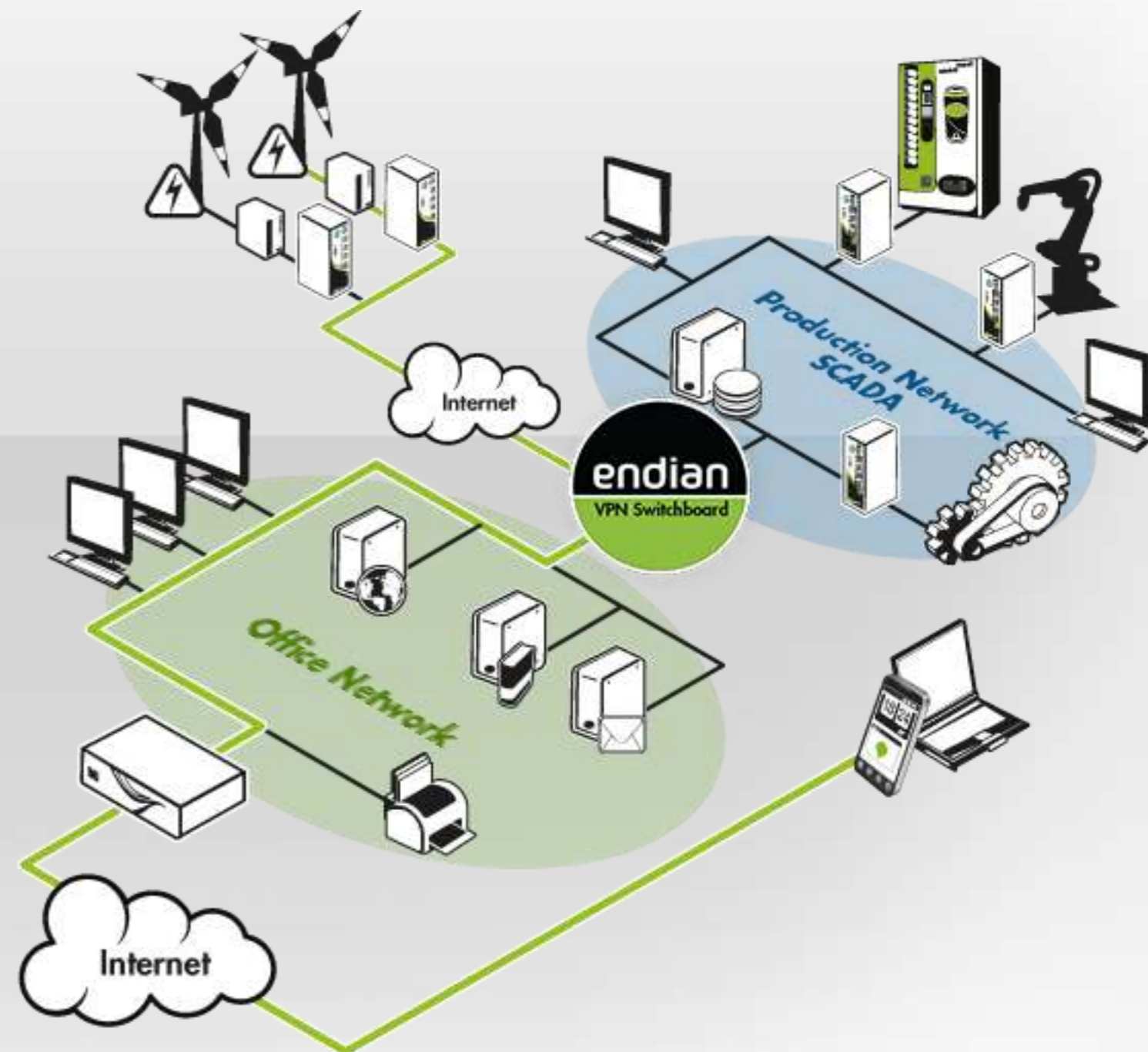
- Firewall
- VPN sicura
- Intrusion Detection / Prevention
- Regolazione e filtraggio del traffico dati
- AntiVirus

ASSOLUTAMENTE NON INTRUSIVA SUGLI IMPIANTI



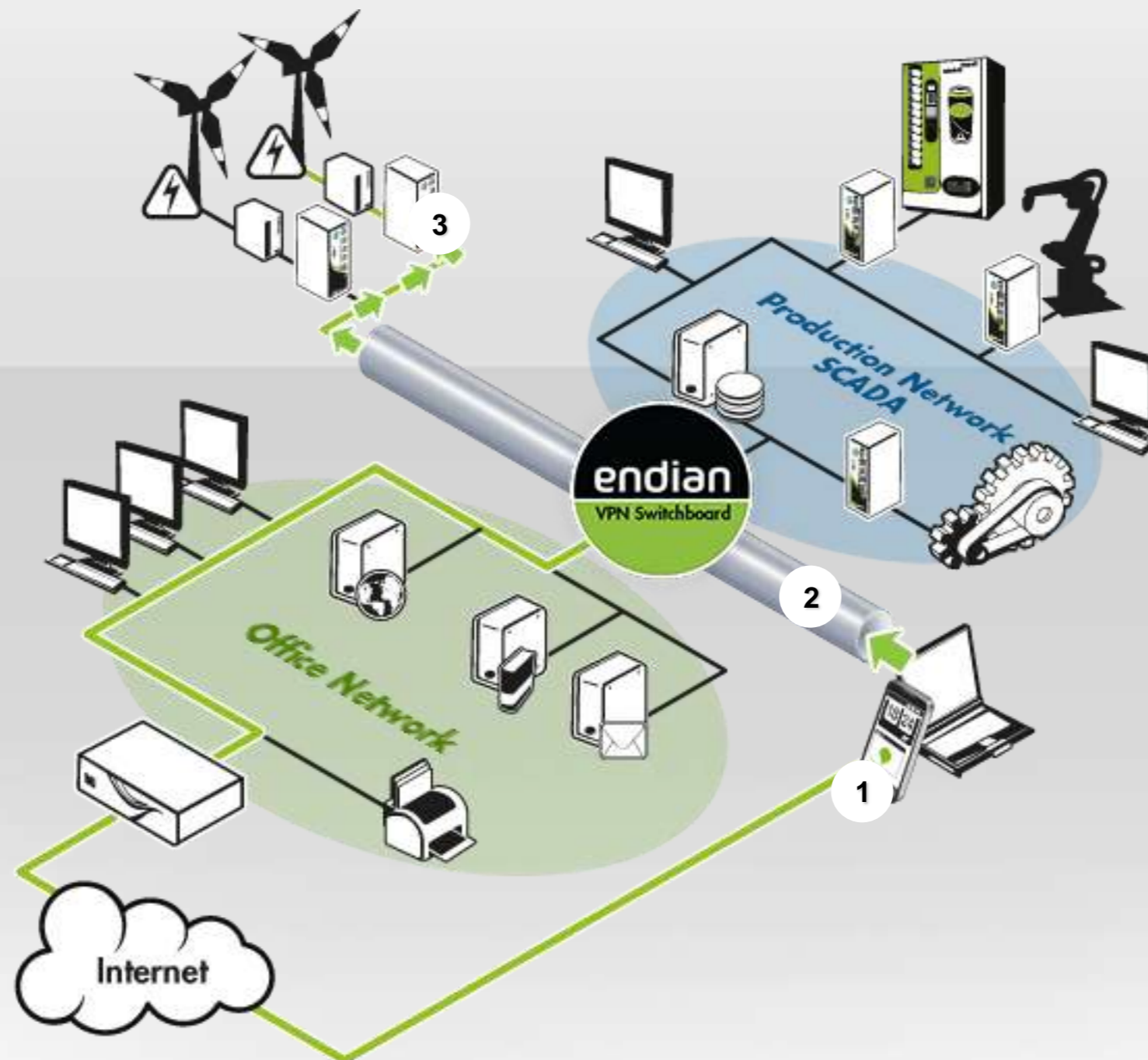
Endian 4i e la sicurezza industriale: la struttura

1. Appliance Endian UTM per la sicurezza perimetrale (vedi serie UTM)
2. Endian VPN Switchboard: concentratore VPN e gestione dei permessi
3. Device Endian 4i Edge per la protezione degli endpoint
4. Il Client dello Switchboard: Endian 4i Connect



Endian VPN Switchboard

Controlla il traffico con 2 tunnel



- 1 Invio richiesta
- 2 Contatto
- 3 Gestione

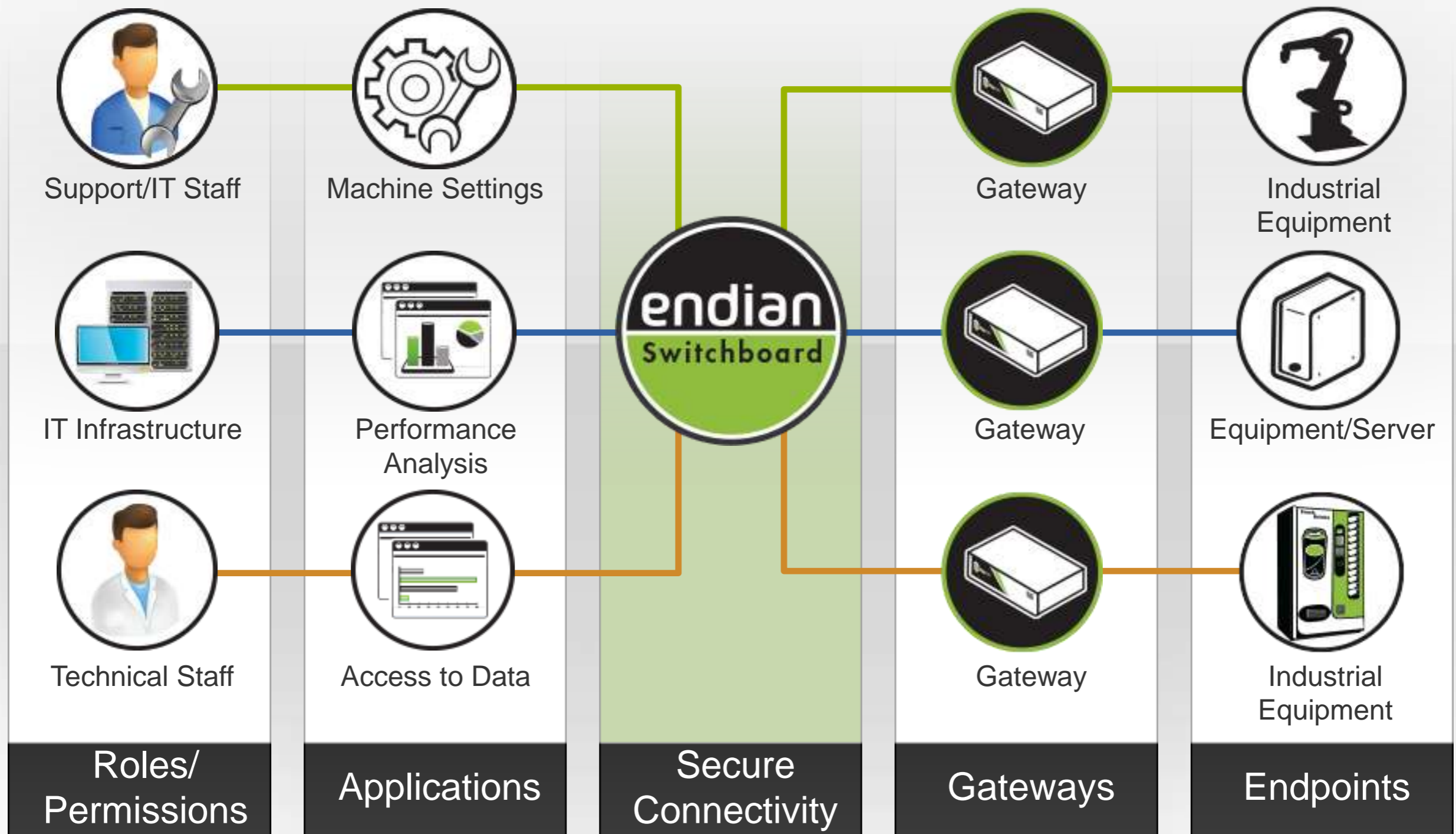
Un tunnel sicuro per tutte le applicazioni

Diversamente dalle altre soluzioni M2M Endian non pone limitazioni ai protocolli utilizzabili

- Modbus / SPS protocol
- Web Frontend
- VOIP
- File System
- Applications



Solution: Role based access to Endpoints and Applications



Endian VPN Switchboard Featurelist

Connections

- Connect to single endpoints or remote networks
- Establish connections by executing actions directly from the 4i Connect client
- Logs for every gateway
- Export Logs for each gateway as CSV file
- Exclusive access on gateway/endpoint level (see settings)

Users

- ** Users are created as VPN users (Endian 4i Connect client)
- Can be member or administrator of an unlimited number of user groups
- Can connect to single gateways or all gateways in a group they have access to
- Can modify and create single gateways or gateway groups
- Permissions:
 - Superuser, Group creation, Action management, API usage,
 - Pushing routes to configured networks
 - Endian Network account data for machine registration (provisioning)

Users groups

- Can contain an unlimited number of users
- Gateway/Gateway group permission management (connect/manage)
- User permission management (member/administrator of group)

Gateways

- ** Gateways are created as VPN user (native OpenVPN implementation of the machine)
- Provisioning
- configuration for Endian gateways (network configuration, VPN tunnel configuration, Upstream proxy configuration)
- automated registration on Endian Network
- User/User group permission management (connect/manage)
- Can be part of an unlimited number of gateway groups
- Network size configuration
- Endpoint configuration

Gateway groups

- Can have their own virtual IP pool (configurable)
- Can contain an unlimited number of gateways
- User/User group permission management (connect/manage)

Endpoints

- Configurable for each gateway
- Custom parameters (important for API as additional data might be stored there)
- Virtual IP addresses are assigned for every endpoint and mapped to the physical IP address -> simultaneous connections to many endpoints with same IP address possible

Actions

- Program calls
- URL calls
- Wildcards for program paths, URLs and IP addresses

Action Profiles

- Group multiple actions
- Can be assigned to Endpoints

Settings/Provisioning

- Virtual IP subnets
- IP Pools / group / global
- Model configuration (provisioning, also encrypted if wanted)
- Exclusive access configuration (gateway level, device level, disabled)
- OpenVPN NAT
- Automatic gateway registration in EN

API

- Enable/disable API -> secured with API Token (in Settings tab)
- Superuser+API (can run commands as any other user)
- User+API (can run commands for himself)
- Activate/deactivate user-gateway connections
- Activate/deactivate user-endpoint connections
- Read all user/gateway/endpoint/action-data

4i Connect Client

- Application management for actions
- Automatic VPN connection on program start
- Automatic reconnection
- Only available functionalities are shown (based on user permissions)
- Support for connection through HTTP Proxy (basic/NTLM authentication)
- Multilanguage (English, German as of now)
- Integrated Downloader (logs and provisioning files)
- Installs a Windows service and a graphical interface - no admin privileges needed after installation

Endian 4i offre multipli livelli di protezione



- 1 Layer 1 – Access Restricted:**
Solo le connessioni pre – approvate (M2M, P2M, D2M) possono essere stabilite
- 2 Layer 2 - Service/Port Restriction:**
Decidendo quale porta deve essere bloccata si garantisce un ulteriore livello di protezione da virus e minacce di altro genere
- 3 Layer 3 - Denial of Service Protection:**
La nostra soluzione intercetta gli attacchi e vi protegge dalle interruzioni di servizio
- 4 Layer 4 - Malformed Packet Rejection:**
Il firewall stateful vi protegge dai cosiddetti “malformed packets” che possono arrecare gravi danni ai sistemi
- 5 Layer 5 - Intrusion Detection Alerts:**
Il costante monitoraggio di network e sistemi ci consente di dare un allarme istantaneo in caso di attività sospetta o violazione delle policy
- 6 Layer 6 - SCADA Protocol Filtering:**
Su richiesta, possiamo fornire il protocollo di filtraggio Modbus TCP per gli appliance 4i Edge.

Sommario:

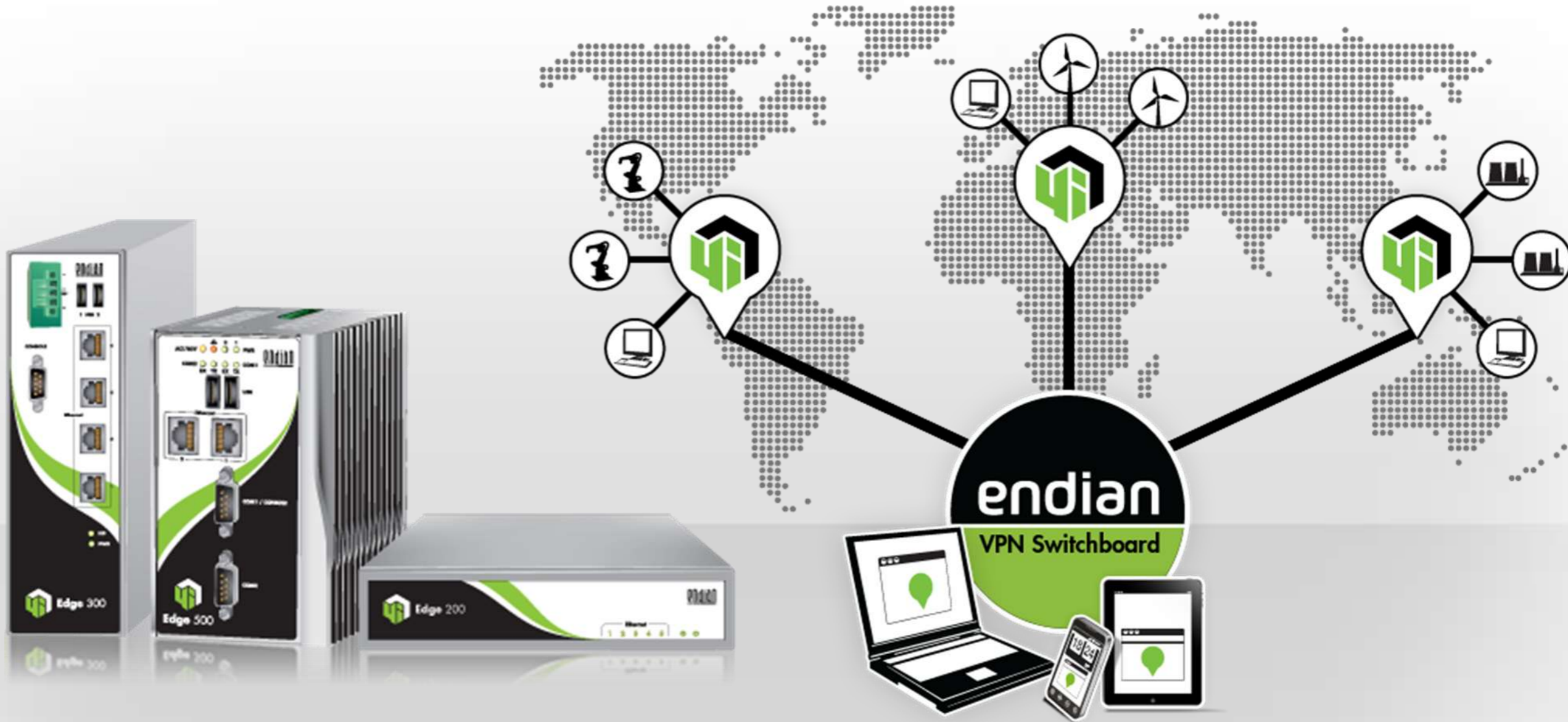
Che cos'è il VPN Switchboard?

- Pannello di controllo
- Concentratore VPN Endian 4i Series o 3° Party
- Add-on per qualsiasi soluzione Endian server



Cosa posso fare con il VPN Switchboard?

- Dare accesso a molti utenti (singoli o gruppi) secondo regole differenti
- Bloccare rapidamente l'accesso divenuto indesiderato (ad es. al termine del rapporto di lavoro)
- Impedire tentativi di intrusione su macchinari importanti
- Avere un rapporto dettagliato sugli accessi (regole di compliance)
- Assicurare agli utenti accesso semplice agli endpoint protetti (HMI, PLC, ecc)
- Sicurezza UTM



GRAZIE!
DOMANDE?