L'Internet of Thing nelle imprese

Costruire una base sicura per sfruttare le opportunità di business dell'IoT

Solution Brief

Alcatel·Lucent Enterprise

L'IoT cambia radicalmente l'equazione del business

L'Internet of Things (IoT) ha il potenziale di trasformare il business modificando profondamente il modo in cui le organizzazioni raccolgono dati e informazioni, riunendo le principali tendenze tecnologiche e commerciali di mobilità, automazione e analisi dei dati. L'IoT si basa sul collegamento in rete di oggetti fisici che utilizzando sensori, attuatori e altri dispositivi integrati possono raccogliere e trasmettere informazioni sull'attività in tempo reale nella rete stessa. I dati raccolti da questi dispositivi possono poi essere analizzati dall'organizzazione per:

- **Ottimizzare prodotti e processi,** riducendo i costi operativi, aumentando la produttività e sviluppando nuovi prodotti e servizi
- **Acquisire nuove conoscenze sui bisogni e sulle preferenze dei clienti,** permettendo alle aziende di offrire prodotti e servizi più personalizzati.
- **Rendere le aziende più smart ed efficienti,** monitorando in modo proattivo le infrastrutture critiche e creando processi più efficienti.
- **Migliorare le esperienze degli utenti,** offrendo prodotti e servizi nuovi o migliorati per differenziare dalla concorrenza un'azienda guidata dai dati.

La diffusione dell'IoT continua a crescere

I professionisti IT di diversi settori hanno già in programma un maggiore uso di soluzioni IoT nel prossimo futuro. Nel 2022, si prevede che il mercato dell'Internet of Things (Internet delle cose) crescerà del 18% fino a raggiungere 14,4 miliardi di connessioni attive. Si prevede che entro il 2025, con l'allentamento dei vincoli di fornitura e l'ulteriore accelerazione della crescita, ci saranno circa 27 miliardi di dispositivi IoT connessi.

Fonte https://iot-analytics.com/number-connected-iot-devices

Le sfide della diffusione dell'IoT

L'IoT produce flussi di dati senza precedenti, presentando sfide di performance, operative e di gestione per l'infrastruttura di rete insieme a maggiori rischi di sicurezza da tutti gli endpoint. Per affrontare questi problemi, le organizzazioni devono adattare i progetti di rete tradizionali per fornire nuovi livelli di intelligenza, automazione e sicurezza.

Alle organizzazioni occorre un'infrastruttura di rete economica che possa controllare in modo sicuro grandi flussi di dati, ma che sia anche semplice da gestire e far funzionare. L'infrastruttura deve:

- **Fornire un processo semplice e automatizzato per l'onboarding dei dispositivi IoT.** I grandi sistemi IoT possono contenere migliaia di dispositivi o sensori, e il provisioning e la gestione manuale di tutti questi endpoint sono complessi e soggetti a errori. L'onboarding automatico consente all'infrastruttura di rete di riconoscere dinamicamente i dispositivi e di assegnarli alla rete protetta appropriata.
- **Fornire le giuste risorse di rete affinché il sistema IoT funzioni in modo corretto ed efficiente.** Molti dispositivi del sistema IoT forniscono informazioni fondamentali che richiedono un livello specifico di QoS. Ad esempio, alcuni casi d'uso richiedono riserve di larghezza di banda adeguate su un'infrastruttura di rete ad alte prestazioni per garantire la fornitura del servizio e l'affidabilità.
- **Garantire un ambiente sicuro contro gli attacchi informatici e la perdita di dati.** Poiché i molti dispositivi e sensori collegati in rete nell'IoT portano a una corrispondente abbondanza di potenziali vettori di attacco, la sicurezza è fondamentale per mitigare i rischi del crimine informatico. La sicurezza è necessaria a più livelli, compresa la segmentazione delle reti IoT stesse.

L'IoT aumenta l'esposizione ai crimini informatici

La crescita dell'IoT porta anche un'esplosione di minacce alla sicurezza informatica, dato che la proliferazione di sensori e dispositivi connessi espande notevolmente la superficie di attacco della rete. L'IoT è particolarmente sensibile perché molti dispositivi IoT sono concepiti senza sicurezza, o progettati da aziende che non conoscono gli attuali requisiti di sicurezza. Di conseguenza, i sistemi IoT possono potenzialmente rappresentare l'anello debole della sicurezza informatica aziendale.

Steve Turner, analista di Forrester, ha dichiarato che dalla sua ricerca emerge una distribuzione relativamente uniforme degli attacchi con riscatto tra i vari settori verticali. Tuttavia, tendono a fare più notizia gli incidenti di ransomware in alcuni comparti, come le infrastrutture critiche e la sanità.[1]

I dispositivi IoT comportano rischi per le risorse in tutta la rete. Creando questi segmenti attraverso la segmentazione virtuale di rete, i dispositivi IoT e le applicazioni che li controllano vengono isolati, riducendo le minacce senza dover prevedere costi aggiuntivi o complessi sistemi di reti separate.

[1]https://www.techtarget.com/searchsecurity/feature/Top-10-ransomware-targets-in-2021-and-beyond

Creare un'infrastruttura di rete IoT sicura

Proteggere traffico e dispositivi IoT è una sfida che non può essere risolta da una qualunque singola tecnologia di sicurezza. Questo richiede un approccio strategico che sfrutta molteplici livelli di protezione.

Per aiutare le organizzazioni a trarre vantaggio dai benefici e mitigare i rischi dell'implementazione dell'IoT, Alcatel-Lucent Enterprise (ALE) fornisce una strategia di rete di tipo zero trust con sicurezza a più livelli.

La strategia di ALE offre protezione ad ogni livello dell'infrastruttura, dal singolo utente e dispositivo fino alla rete stessa. La macro e microsegmentazione della rete garantisce un approccio semplice e affidabile all'onboarding sicuro dei dispositivi e fornire le giuste risorse di rete per far funzionare il sistema in modo corretto ed efficiente, il tutto in un ambiente sicuro per salvaguardare le organizzazioni dagli attacchi informatici.

Segmentazione IoT

Per consentire la segmentazione IoT, vengono assegnati profili a tutti gli utenti, i dispositivi e le applicazioni all'interno della rete ALE. Questi profili, che definiscono ruoli, autorizzazioni di accesso, livelli di QoS e altre informazioni sulle normative, vengono trasmessi a tutti gli switch e agli access point della rete.

- Con la macrosegmentazione, i dispositivi sono collocati in "segmenti virtuali" mediante tecniche di virtualizzazione della rete che consentono a più dispositivi e reti di utilizzare la stessa infrastruttura fisica rimanendo isolati dal resto della rete.
- Con la microsegmentazione, è possibile applicare regole di QoS e sicurezza diverse ai dispositivi all'interno di ciascun segmento virtuale. Questa soluzione aggiunge una maggiore granularità e aumenta la sicurezza della rete, impedendo a diversi tipi di dispositivi nello stesso segmento di interagire tra loro quando non sono stati strutturati per farlo.
- Grazie alla segregazione della rete con macro e microsegmentazione, se un dispositivo viene compromesso in una parte della rete, non solo la violazione non influisce sui dispositivi o sulle applicazioni in altri segmenti virtuali, ma non può propagarsi ad altri tipi di dispositivi all'interno del segmento interessato.
- Quando un nuovo dispositivo IoT viene collegato, la rete riconosce automaticamente il suo profilo e assegna il dispositivo all'ambiente virtuale appropriato.
- La comunicazione è limitata ai dispositivi all'interno di quell'ambiente virtuale e all'applicazione nel data center che controlla questi dispositivi.
- Poiché tutti gli utenti hanno anche profili all'interno della rete ALE, l'accesso ai segmenti virtuali IoT può essere limitato a persone e gruppi autorizzati.

Sicurezza avanzata

- Oltre alla segmentazione IoT, le tecnologie di rete di ALE forniscono una sicurezza su più livelli della rete.
- A livello di utente, i profili garantiscono che gli utenti siano autenticati e autorizzati con gli opportuni diritti di accesso.
- A livello di dispositivo, la rete assicura che i dispositivi siano autenticati e conformi alle regole di sicurezza stabilite.
- A livello di applicazione, la rete può stabilire regole per ogni applicazione o gruppo di applicazioni, tra cui il blocco, la limitazione della larghezza di banda e il controllo di chi può accedere a quali applicazioni.
- A livello di rete, gli switch ALE beneficiano di un codice sicuro e diversificato. Questo codice protegge le reti da vulnerabilità intrinseche, code exploits, malware e potenziali back door che potrebbero compromettere switch, router e altro hardware mission critical.
- L'analisi dei dati intelligente di ALE utilizza la tecnologia deep packet inspection e altre tecnologie per rilevare il tipo di dati e applicazioni che si muovono attraverso la rete, rendendo possibile l'identificazione di schemi di traffico insoliti, attività non autorizzate e intrusioni nella rete.

Opertatività e gestione di rete end-to-end

Le soluzioni di rete ALE offrono anche significativi vantaggi operativi e di gestione.

- ALE consente a più reti virtuali separate di operare su una singola infrastruttura comune, eliminando l'esigenza di investimenti CAPEX in infrastrutture fisiche multiple.
- La soluzione Unified Access di ALE permette alle tecnologie cablate e wireless di lavorare insieme come un'unica rete robusta, con un insieme comune di servizi di rete, una struttura di policy, uno schema di autenticazione comune e un unico database di autenticazione.
- Le soluzioni di rete ALE hanno anche un unico sistema di gestione per tutti gli elementi dell'infrastruttura, compresa la gestione unificata delle reti LAN cablate e WLAN wireless. Le soluzioni Alcatel-Lucent OmniVista® 2500 Network Management System e Alcatel-Lucent OmniVista® Cirrus Network Management as a Service per la gestione basata sul cloud forniscono un'unica finestra per gestire ambienti virtuali, switch, access point e tutti gli altri componenti di rete.

Un portafoglio disoluzioni di rete ad alte prestazioni

Gli switch, gli access point e i controller ALE supportano l'ultima generazione di funzionalità ad alta larghezza di banda e bassa latenza e possono gestire un gran numero di dispositivi in ambienti a elevata densità. I prodotti e le soluzioni di rete ALE sono in grado di soddisfare le esigenze di rete di organizzazioni di qualsiasi dimensione. ALE fornisce anche una selezione di switch, access point e router di livello industriale per l'implementazione in ambienti esterni o difficili.

Scenari IoT nei principali settori verticali

Le soluzioni IoT promettono di rendere le organizzazioni più intelligenti e vincenti nelle loro attività. Questi benefici sono particolarmente evidenti in alcuni settori verticali.

Settore sanitario

L'IoT ha il potenziale di trasformare il settore sanitario modificando profondamente il modo in cui ospedali, cliniche e altre strutture sanitarie raccolgono e utilizzano i dati, riunendo le principali tendenze tecnologiche e commerciali in termini di mobilità, automazione e analisi dei dati per migliorare le prestazioni sanitarie. I dati raccolti da questi dispositivi possono poi essere analizzati dall'organizzazione per:

- Migliorare la cura del paziente e offrire trattamenti e servizi nuovi o migliorati, contribuiendo così a differenziare un'organizzazione sanitaria basata sui dati da quelle tradizionali.
- Ottimizzare i processi, sviluppando nuovi servizi e flussi di lavoro nonché soluzioni che aumentano l'efficienza e riducono i costi operativi.
- Acquisire nuove conoscenze sulle esigenze e le preferenze dei pazienti, consentendo alle organizzazioni sanitarie di offrire cure ed esperienze più personalizzate.
- Rendere le reti ospedaliere più smart, monitorando in modo proattivo le infrastrutture critiche e automatizzando l'implementazione e la gestione dell'infrastruttura IT.

La crescita dell'IoT nel settore sanitario porta un'esplosione di minacce alla sicurezza informatica, dato che la proliferazione di sensori e dispositivi connessi espande notevolmente la superficie di attacco della rete. L'IoT per il settore sanitario è particolarmente vulnerabile perché molti dispositivi IoT sono concepiti senza sicurezza, o progettati da aziende che non conoscono gli attuali requisiti di sicurezza. Di conseguenza, i sistemi IoT possono potenzialmente rappresentare l'anello più debole della sicurezza informatica di ospedali, cliniche e strutture di assistenza.

Istruzione

Le istituzioni scolastiche non fanno eccezione nel mondo dell'IoT 'anywhere', un mondo in cui le tecnologie vengono progettate in ogni prodotto immaginabile. L'IoT apporta numerosi vantaggi alle università e alle scuole, contribuendo con una nuova generazione di oggetti intelligenti che possono migliorare immensamente l'esperienza di apprendimento e rafforzare in misura significativa la sicurezza e la protezione del campus. I dispositivi IoT, da quelli piccoli come un sensore luminoso a quelli grandi come lavagne intelligenti, comportano grandi cambiamenti nella gestione degli ambienti scolastici e nel modo in cui gli studenti apprendono. I dispositivi IoT:

- Creano nuove modalità di apprendimento per gli studenti per esperienze più personalizzate e dinamiche, come i libri di testo digitali immersivi e l'apprendimento basato sul gioco.
- Cambiano il modo in cui gli insegnanti svolgono le lezioni e verificano i risultati con apparecchiature audiovisive intelligenti, videoregistratori digitali per l'acquisizione di lezioni e test online.
- Semplificano le operazioni del personale amministrativo monitorando in modo proattivo le infrastrutture critiche e creando processi più efficienti ed economici per la gestione di HVAC, illuminazione e paesaggio.
- Garantiscono un ambiente più sicuro per studenti e insegnanti grazie a telecamere di sorveglianza digitale, serrature intelligenti e autobus scolastici connessi.

In queste scuole e università rimodellate, gli amministratori possono raccogliere, archiviare e analizzare enormi quantità di dati sull'ambiente e sulle prestazioni degli studenti. Questo fornirà alle scuole le informazioni necessarie per migliorare i processi che portano gli studenti ad avere successo e consentirà loro di individuare le lacune da colmare.

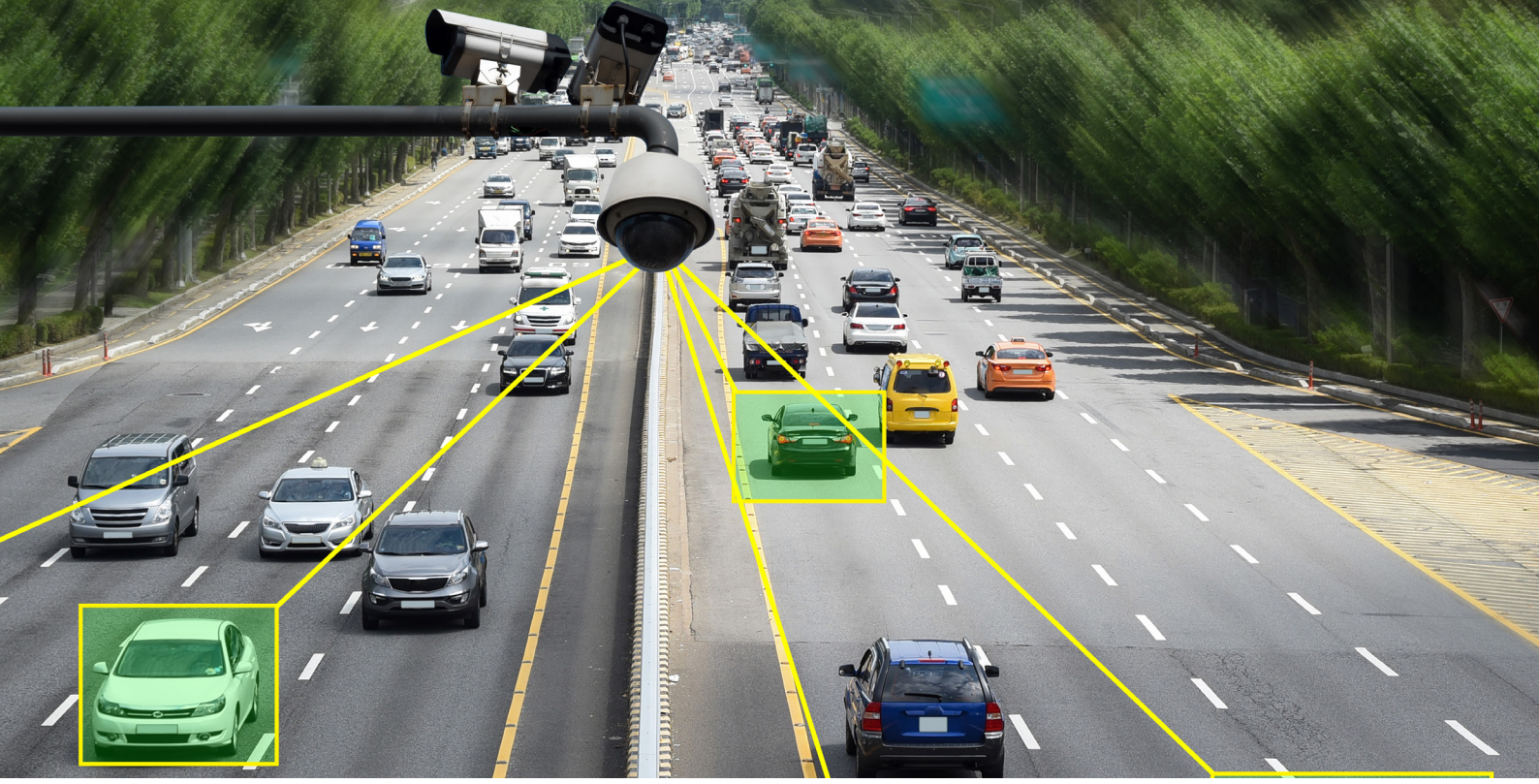
Queste trasformazioni comportano sia opportunità che minacce. È indispensabile adottare una strategia di difesa in profondità che fornisca connessioni sicure ai dispositivi IoT e prevenga le violazioni che possono colpire la privacy dei dati degli studenti e la sicurezza della ricerca o mettere a rischio l'autenticità e l'integrità dei dati.

Enti pubblici

I governi e i comuni si stanno unendo al flusso dell'IoT. Le città intelligenti offrono grandi opportunità commerciali e nuovi mezzi per servire e proteggere il pubblico. In queste città connesse, le aziende di servizi pubblici sollecitano l'uso di contatori intelligenti per creare sistemi di tariffazione adattabili e gli sviluppatori introducono sensori e componenti di automazione nelle nuove proprietà. I parcheggi intelligenti fanno risparmiare tempo ai cittadini e li rendono più efficienti, mentre i cestini intelligenti invitano all'azione quando stanno per traboccare. L'IoT aiuta i comuni e le amministrazioni a raccogliere informazioni sulla mobilità e sui trend dei dati, fornendo analisi dei dati fondamentali per la formulazione delle strategie cittadine e la pianificazione a lungo termine. L'IoT si traduce in:

- Cittadini ed enti pubblici meglio connessi per fornire servizi e risorse di alta qualità, sicuri e reattivi, che migliorino l'impegno e la fiducia tra pubblica amministrazione e cittadini, aumentando la vivibilità, la lavorabilità e la sostenibilità.
- Aumento della sicurezza dei trasporti grazie a una migliore comprensione delle operazioni del sistema di trasporto attraverso i dati dei sensori che tengono traccia di tutte le anomalie, dalla velocità dei treni della metropolitana leggera alla temperatura delle strade, fino alla posizione in tempo reale degli autobus del trasporto pubblico.
- Congestione ridotta e minore consumo di energia grazie alle tecnologie Smart City che sfruttano i dati in tempo reale per migliorare il modo in cui i funzionari utilizzano le risorse per soddisfare le richieste, fornendo l'agilità per reagire in tempi rapidi a modelli di traffico in continua evoluzione, variazioni nel consumo di acqua o energia, o cambiamenti nella qualità dell'aria.
- Miglioramento delle prestazioni operative e della manutenzione tramite il monitoraggio proattivo delle infrastrutture pubbliche critiche e la creazione di processi più efficienti per ridurre i costi operativi e rafforzare la capacità del sistema.
- Potenziamento della sicurezza pubblica grazie a una risposta più rapida ed efficace alle emergenze.

L'asticella della sicurezza informatica, tuttavia, deve essere posta in alto, molto in alto. Nelle città IoT, dove non tutte le applicazioni, i sensori e i dispositivi sono progettati tenendo conto della sicurezza, occorre un'infrastruttura intelligente e automatizzata in grado di classificare questi dispositivi in categorie separate, impedendo la comunicazione con ciò con cui non devono interfacciarsi. Questa containerizzazione rafforzerà in misura notevole la sicurezza e metterà l'ente pubblico sulla strada giusta per muoversi verso un ambiente basato su un approccio 'zero trust', creando più livelli di protezione in una strategia informatica di difesa in profondità.



Trasporti

L'Internet of Thing (IoT) trasforma il settore dei trasporti, modificando profondamente il modo in cui i sistemi raccolgono dati e informazioni, unendo automazione e analisi dei dati. Sensori, attuatori e altri dispositivi integrati raccolgono e trasmettono informazioni sull'attività in tempo reale nella rete stessa. Questi dati possono essere analizzati dalle autorità di trasporto per migliorare l'esperienza dei passeggeri e la sicurezza, ridurre la congestione e il consumo di energia e, allo stesso tempo, ottimizzare le prestazioni operative.

L'IoT è il fulcro delle forze che rimodellano i trasporti per fornire maggiore sicurezza, viaggi più efficienti, manutenzione più adeguata di veicoli e aerei e gestione del traffico più strategica. Tra gli esempi di applicazioni IoT per i trasporti figurano:

- Efficienza, per aumentare la capacità del sistema e migliorare la sicurezza e il comfort dei passeggeri, riducendo al contempo i costi e i rischi.
- Segnaletica stradale dinamica, per sistemi di trasporto intelligenti che visualizzano in tempo reale lo stato delle strade, le tariffe dei pedaggi, la chiusura delle corsie e i viaggi.
- Veicoli autonomi, con la capacità di percepire l'ambiente circostante, prevedere il comportamento, comunicare con altri veicoli e con l'ambiente circostante e reagire all'istante a scenari autostradali reali.
- Videosorveglianza, per garantire il movimento delle persone e delle folle, per automatizzare e rilevare tempestivamente comportamenti sospetti e bagagli abbandonati.

Gli attacchi informatici possono avere un impatto sulle operazioni quotidiane per periodi prolungati. Non solo l'interruzione del servizio, ma anche l'esposizione di dati altamente sensibili è un rischio enorme quando si tratta di questo settore. Mentre alcuni attacchi alla sicurezza informatica sono un tentativo di guadagno, altri sono studiati per causare caos e scompiglio, mettendo fuori uso interi sistemi. L'interruzione dei semafori, il blocco dell'accesso a file e a dati importanti, l'interruzione dei servizi dei libri paga e la compromissione dei distributori automatici di biglietti e dei tornelli sono solo alcuni di questi casi.

- Nel 2018, l'azienda Bay & Bay Transportation è stata vittima di un massiccio attacco ransomware che ha bloccato i sistemi utilizzati per gestire la sua flotta di 300 autocarri.
- Nel 2018, gli hacker hanno bloccato 2.000 computer del Dipartimento dei trasporti del Colorado, interrompendo le operazioni per settimane. Più di recente, i criminali informatici si sono infiltrati in tre dei 18 sistemi informatici della Metropolitan Transit Authority di New York.
- La prima metà del 2020 ha rivelato un aumento vertiginoso degli incidenti ransomware, con un incremento complessivo del 715% rispetto all'anno precedente.
- Nel 2020 sono stati rubati gli indirizzi e-mail e i dati di viaggio di 9 milioni di clienti EasyJet. A 2.208 di questi sono stati violati i dati delle carte di credito. Questo attacco informativo, unito allo scoppio della pandemia globale, ha fatto sì che la società aerea perdesse il 45% del suo valore azionario e registrasse la sua prima perdita annuale in 25 anni di esistenza.

Oggi reti e strategie IoT sicure sono una realtà

I prodotti e le soluzioni ALE costruiscono una base di rete sicura per aiutare le organizzazioni a implementare sistemi IoT che possono fornire le informazioni necessarie per ottimizzare prodotti e processi, rendere le aziende più intelligenti ed efficienti e migliorare le esperienze dei clienti. Le strategie di contenimento IoT e di sicurezza stratificata di ALE riducono i rischi e semplificano la configurazione delle reti IoT, facilitando l'onboarding dei dispositivi, fornendo operazioni più efficienti e aumentando notevolmente la sicurezza. ALE aiuta le organizzazioni a usufruire di tutti i benefici potenziali dell'IoT fornendo livelli avanzati di intelligenza di rete, automazione e sicurezza.

Vuoi saperne di più?

Per ulteriori informazioni sulle soluzioni IoT di ALE, vai su Sicurezza IoT ALE.

Alcatel·Lucent Enterprise