Garantire sicurezza alle soluzioni UCC (Unified Communication e Collaboration)

Cosa serve in un mondo in continua evoluzione

White paper

Alcatel·Lucent Enterprise

Indice

- Maggiore attenzione alla cybersecurity
- Cybersecurity end-to-end: sei aree chiave
- Meno rischi per raggiungere gli obiettivi di business
- Cybersecurity, come parte integrante del mindset del fornitore di tecnologia

Maggiore attenzione alla sicurezza informatica

Nel corso degli ultimi anni, quasi tutte le aziende e le organizzazioni della pubblica amministrazione hanno cambiato il modo in cui i dipendenti comunicano, collaborano e condividono le informazioni. Il rapido passaggio a soluzioni in grado di supportare il lavoro a distanza è stato fondamentale per assicurare la continuità di business durante il periodo di crisi sanitaria, ma con un prezzo da pagare: il perimetro della rete delle organizzazioni ora si estende ben oltre i confini tradizionali dell'ufficio causando un aumento significativo della superficie di rete vulnerabile.

I rischi associati ai perimetri di rete estesi non sono destinati a scomparire in tempi brevi. Secondo Gartner, entro la fine del 2023 il 39% dei knowledge worker a livello globale lavorerà con modelli ibridi, da remoto e in ufficio. Negli Stati Uniti, questo numero sale al 51%[1].

Le perturbazioni geopolitiche hanno ulteriormente aumentato i rischi della sicurezza informatica. L'Agenzia dell'Unione Europea per la sicurezza informatica ha definito l'invasione russa dell'Ucraina un "game changer" per il dominio informatico globale.[2] Secondo l'Associazione delle aziende di outsourcing IT ucraine e secondo Fortune 500 nel 2022 una su cinque aziende si è affidata a sviluppatori di software locali (del Paese di appartenenza).[3]

Allo stesso tempo, l'impatto sociale degli attacchi informatici è aumentato. Nel 2022 abbiamo assistito a importanti attacchi informatici a infrastrutture civili critiche, che hanno causato un'emergenza nazionale in Costa Rica 4 e a organizzazioni sanitarie.[5]

Le organizzazioni non possono permettersi ritardi nel migliorare la cybersecurity

Si stima che nel 2021 i crimini informatici siano costati all'economia globale 5,5 trilioni di euro, con danni che dovrebbero superare i 10 trilioni di euro entro il 2025.[6] Il problema è così grave che l'Unione Europea sta elaborando una legge sulla resilienza informatica e ha emanato una versione 2 significativamente migliorata della sua direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS) per salvaguardare i consumatori e le imprese che acquistano o utilizzano prodotti o software con una componente digitale.[7] Gli Stati Uniti stanno inoltre attuando misure per rafforzare la sicurezza informatica, tra cui l'Executive Order 14028, che incoraggia le agenzie ad adottare principi di sicurezza informatica incentrata sull'approccio zero trust e ad adeguare di conseguenza le architetture di rete.[8]

Poiché le aziende e le amministrazioni pubbliche si stanno trasformando digitalmente supportando modelli di lavoro flessibili, non hanno altra scelta se non quella di rafforzare la sicurezza informatica. Le soluzioni utilizzate dai team per comunicare, collaborare e condividere le informazioni devono pertanto incorporare le migliori pratiche di sicurezza informatica a ogni livello e in ogni aspetto della funzionalità.

1 Gartner Forecasts 39% of Global Knowledge Workers Will Work Hybrid by the End of 2023. Gartner, marzo 2023.
2 Volatile Geopolitics Shake the Trends of the 2022 Cybersecurity Threat Landscape. 2 European Union Agency for Cybersecurity. Novembre 2022.
3 Nel 2022 in Ucraina, secondo Fortune 500, un'azienda su cinque si è affidata a sviluppatori locali per esigenze di sviluppo software Ukrainian Hi-Tech Initiative, ottobre 2022.
4 I 13 cyberattacchi più costosi del 2022: uno sguardo al passato. Security Intelligence, dicembre 2022.
5 In Review 2022: An Eventful Cybersecurity Year Forbes, dicembre 2022.
6 New European Union cybersecurity proposal takes aim at cybercrime World Economic Forum, settembre 2022.
7 EU Cyber Resilience Act. European Commission, settembre 2022.
8 Executive Order on Improving the Nation's Cybersecurity. Cybersecurity & Infrastructure Security Agency.

Cybersecurity end-to-end: sei aree chiave

Le soluzioni di unified communication e collaboration devono rispondere alle esigenze di cybersecutity end-to-end in quanto questo è l'unico modo per assicurare che la sicurezza venga applicata in modo esaustivo. Un approccio end-to-end alla sicurezza informatica aiuta imprese e la pubblica amministrazione a:

- **Prevenire gli attacchi informatici** introducendo la cybersecurity in ogni aspetto della progettazione del prodotto per ridurre la superficie oggetto di attacchi informatici
- **Proteggersi dagli attacchi informatici** attuando gli standard di sicurezza e le best practice più recenti in tutte le componenti della soluzione per rafforzarne la resistenza
- **Reagire agli attacchi informatici** adottando azioni rapide e appropriate per limitare l'impatto e migliorare la resilienza, qualora si debba affrontare un attacco.

Per determinare se le soluzioni unified communication e collaboration rispondono alle esigenze di cybersecutity end-to-end è necessario valutare le soluzioni nelle aree descritte di seguito. Focalizzarsi su queste aree può essere d'aiuto per garantire che l'assessmnet delle soluzioni sia completo e mirato rispetto alle vulnerabilità principali del panorama delle minacce informatiche.

1 Sicurezza per progettazione

Storicamente, la progettazione delle soluzioni è stata guidata, per la maggior parte dei casi, dalla necessità di nuove funzionalità e la sicurezza è sempre stata un elemento importante, anche se non prioritario. Con il cambiamento del panorama, le priorità in fase di progettazione si sono invertite, oggi i progetti di soluzioni devono essere guidati dai requisiti di cybersecurity.

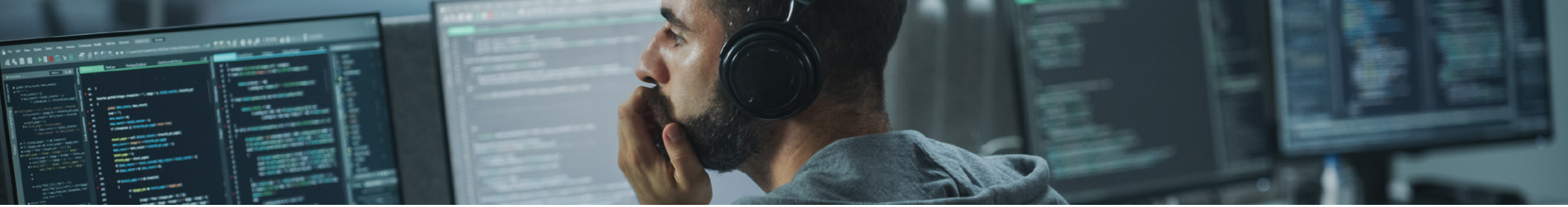
Le soluzioni hardware e software basate sulla sicurezza per progettazione tengono conto della sicurezza in ogni fase: definizione, implementazione e della consegna del prodotto. Tutti i sistemi hardware e operativi sono di tipo industriale, la protezione Denial of Service (DoS) è integrata e le soluzioni attuano le principali best practice di cybersecurity del settore. Ad esempio, una soluzione unified communication e collaboration per le aziende che si occupano di sicurezza interna dovrà soddisfare gli elevatissimi standard di resilienza e riservatezza richiesti da queste organizzazioni.

2 Sicurezza di accesso alla rete basato sul principio zero trust

Le strategie di sicurezza che basano l'affidabilità sulla posizione dell'utente all'interno del firewall aziendale, sulle credenziali di accesso o sull'applicazione o sul dispositivo utilizzato non sono più adeguate, anche quando si combinano più meccanismi di sicurezza. Oggi nessun utente, dispositivo o applicazione dovrebbe godere di fiducia incondizionata.

Le soluzioni di unified communication e collaboration che utilizzano un modello di sicurezza basato su Zero Trust Network Access (ZTNA) aiutano le organizzazioni a contrastare efficacemente le minacce in continua evoluzione. ZTNA non si fida di alcun utente, dispositivo o applicazione, indipendentemente dalla sua ubicazione. Si basa su cinque principi fondamentali:

- La rete è ostile
- Le minacce esterne e interne sono sempre presenti
- Posizione e identità non sono sufficienti per determinare la fiducia
- Ogni dispositivo, utente e flusso di rete deve essere autenticato e autorizzato.
- Le policy di rete e di sicurezza devono essere dinamiche e utilizzare il maggior numero possibile di fonti di dati.



3 Macro e microsegmentazione

La macro e la microsegmentazione consentono un approccio granulare e altamente controllato alla sicurezza informatica per tutti gli utenti, i dispositivi e le applicazioni che accedono alla rete.

La macrosegmentazione segrega utenti, dispositivi e applicazioni in base al loro dominio funzionale, in modo che non possano comunicare con gli elementi di altri macrosegmenti. Ad esempio, le applicazioni unified communication e collaboration di un macrosegmento non possono comunicare con le tecnologie adibite alla sicurezza, come le telecamere a circuito chiuso e i sistemi di chiusura delle porte, di un secondo macrosegmento o con i sensori e i controlli per l'illuminazione, il riscaldamento e il condizionamento dell'aria di un terzo macrosegmento.

La microsegmentazione definisce il modo in cui gli utenti, i dispositivi e le applicazioni all'interno di un macrosegmento possono interagire tra loro ed è in genere regolata da policy di sicurezza molto specifiche. Ad esempio, una telecamera di sorveglianza non dovrebbe potersi interfacciare con una serratura, nonostante si tratti dello stesso macrosegmento relativo alla sicurezza.

4 Crittografia nativa end-to-end

Nelle moderne oganizzazioni, dipendenti, clienti, partner e fornitori possono trovarsi in qualunque posto del mondo e le soluzioni che utilizzano per comunicare e collaborare possono essere installate nell'edificio in cui lavorano, dall'altra parte della città, o in un centro dati all'altro capo del mondo. In ogni caso, le persone devono essere in grado di scambiare informazioni in modo sicuro e riservato utilizzando voce, video e testo.

Per garantire che solo i partecipanti alla conversazione possano accedere alle informazioni scambiate, ogni conversazione deve essere completamente crittografata dall'origine alla destinazione. Ciò significa che ogni elemento hardware e software coinvolto nelle comunicazioni end-to-end deve essere dotato di meccanismi di crittografia nativamente integrati e approvati dalle agenzie di sicurezza.

5 Certificazioni e accreditamenti in materia di sicurezza e privacy

Solo pochi anni fa, le certificazioni e gli accreditamenti di sicurezza più rigorosi erano richiesti esclusivamente per prodotti quali i firewall, o settori particolari, come la difesa. Oggi gli standard di sicurezza specifici devono essere applicati a tutti i prodotti tecnologici, in qualsiasi settore.

È estremamente importante verificare che le dichiarazione di cybersecurity siano supportate da certificazioni e accreditamenti riconosciuti. Ecco alcuni esempi di conformità da ricercare:

- **Standard globali di sicurezza e privacy**, come ISO 27001 per la sicurezza delle informazioni, ISO 27017 per ambienti basati su cloud più protetti e più sicuri, ISO 27018 per la protezione delle informazioni di identificazione personale in ambienti basati sul cloud e Common Criteria Evaluation Assurance Level (EAL) 2 e superiori per la sicurezza dei sistemi informatici.
- **Standard di sicurezza e privacy specifici di settore**, come l'Health Insurance Portability and Accountability Act (HIPAA) negli Stati Uniti e l'Hébergeurs de Données de Santé (HDS) per l'hosting di dati sanitari in Francia.
- **Standard regionali di sicurezza e privacy**, come il regolamento generale sulla protezione dei dati (GDPR) nell'Unione Europea.

6 Continui e specifici test sulla sicurezza

Come gli standard di sicurezza, i processi dei test specifici sulla sicurezza, un tempo riservati ai prodotti di sicurezza, sono ora obbligatori ancehe per le soluzioni di unified communication e collaboration.

I test di penetrazione ne sono un esempio lampante. Questi test simulano gli attacchi informatici per rivelare le vulnerabilità della sicurezza, per poterle affrontare in modo proattivo prima che si verifichino i problemi. Per essere al passo con le minacce informatiche in un panorama in continua evoluzione, i test di penetrazione guidati esclusivamente dai requisiti di cybersecurity devono essere effettuati su base continuativa.

I fornitori di tecnologia che si impegnano ad aiutare i propri clienti a mantenere la massima sicurezza informatica devono fornire le risorse, le competenze e gli strumenti necessari per eseguire test di penetrazione continui.

Meno rischi per raggiungere gli obiettivi di business

Le soluzioni di unified communication e collaboration che implementano la gamma completa di misure di sicurezza informatica descritte nella sezione precedente offrono alle aziende e alle organizzazioni della pubblica amministrazione la libertà e la flessibilità fondamentali per portare avanti le attività riducendo al minimo i rischi e garantire la conformità. Possono inoltre:

- **Consentire ai dipendenti** di collaborare e condividere informazioni in modo sicuro e riservato utilizzando qualsiasi supporto e dispositivo, ovunque.
- **Migliorare l'esperienza del cliente** con comunicazioni arricchite, informative e coinvolgenti, velocizzare i processi decisionali, automatizzare i processi di business e rilevare proattivamente i problemi prima che si ripercuotano sul cliente.
- **Aumentare l'eccellenza operativa e l'agilità** utilizzando un'infrastruttura digitale, implementandola dove ha più senso per l'organizzazione, on premise o attraverso un modello di cloud ibrido, privato o pubblico, aderendo al contempo a rigorose policy di riservatezza dei dati e garantendo la conformità alle normative sulla privacy.

Gli esempi che seguono evidenziano solo alcune delle opportunità che si profilano e che possono essere facilmente adattate ad altre esigenze e ad altri settori.

Creare un luogo di lavoro flessibile e digitale per responsabilizzare i dipendenti

Con il giusto mix di soluzioni di comunicazione e collaborazione sicure, i dipendenti possono lavorare in modo più rapido e flessibile, mantenendo al contempo la piena conformità con le normative del settore.

- **Nel settore sanitario,** una forza lavoro altamente mobile può collaborare e condividere informazioni rimanendo del tutto conforme agli standard di sicurezza dei dati. Il personale può scambiare senza difficoltà gli aggiornamenti e ottenere rapidamente l'assistenza di cui ha bisogno. Il personale medico può utilizzare comunicazioni sicure e in tempo reale per migliorare il percorso di cura dei pazienti e l'efficienza del flusso di lavoro. Il personale non medico può accelerare i processi e le risposte ai problemi di manutenzione che potrebbero compromettere la sicurezza dei pazienti e del personale.
- **Nel settore dell'istruzione**, gli insegnanti possono offrire esperienze di apprendimento a distanza più ricche e coinvolgenti, con maggiori opportunità per gli studenti di partecipare alle attività, collaborare ai progetti e interagire utilizzando il mezzo di comunicazione preferito. Il controllo completo degli accessi e i criteri automatizzati mantengono l'integrità dei dati, mentre l'analisi dei dati consente di assegnare priorità alle comunicazioni critiche e alle risorse di rete.
- **Nelle organizzazioni governative**, il personale può scambiare informazioni in modo sicuro all'interno di team distribuiti. Può condividere schermi, controllare da remoto il desktop di un altro utente e scambiare file di grandi dimensioni per rafforzare la collaborazione. Inoltre può interagire in modo sicuro con i cittadini attraverso applicazioni web o mobili, utilizzando voce, video, chat o messaggistica istantanea.
- **Nel settore dei trasporti**, il luogo di lavoro digitale consente ai dipendenti di utilizzare i propri dispositivi mentre lavorano, di introdurre processi più efficienti e di fornire ai passeggeri servizi potenziati, come la possibilità di lavorare durante gli spostamenti. I protocolli di comunicazione sicuri, le installazioni di tipo industriale e il codice diversificato proteggono i dati in ogni punto della rete.

Connettere tutto per migliorare l'esperienza dei clienti

Connettere in modo sicuro persone, oggetti e applicazioni con comunicazioni in tempo reale consente alle aziende e alle organizzazioni pubbliche di:

- Offrire ai dipendenti i dispositivi, le tecnologie e i dati di cui hanno bisogno per assistere meglio i clienti, riducendo al minimo il rischio che l'errore umano o la mancanza di consapevolezza compromettano la sicurezza.
- Utilizzare dispositivi integrati e sicuri per comunicare e collaborare con i clienti mentre si è in viaggio, con accesso completo alle soluzioni di gestione delle relazioni con i clienti (CRM).
- Aumentare la protezione, il controllo e la visibilità su una gamma di dispositivi Internet of Things (IoT) in rapida crescita e diversificata.
- Mantenere aggiornati i sistemi di comunicazione e collaborazione per evitare il rischio che le applicazioni obsolete aumentino la superficie di attacco facendole diventare più vulnerabili.
- Implementare controlli di accesso efficaci e crittografia end-to-end su tutte le piattaforme.

La gestione unificata della rete consente di gestire in modo olistico tutte le piattaforme di comunicazione, le applicazioni e i dispositivi IoT. La gestione unificata della rete:

- Semplifica le attività di gestione delle reti cablate e wireless e dei dispositivi IoT per ridurre i costi di gestione, ottimizzare le prestazioni e potenziare l'efficienza operativa.
- Accelera la risoluzione dei problemi in ambienti tecnologici sempre più diversificati per ridurre il rischio di interruzioni del servizio e tempi di fermo.

La gestione unificata della rete in tutti i settori offre una serie di vantaggi. Ad esempio:

Nel settore sanitario, le soluzioni IoT possono tracciare la posizione di apparecchiature critiche come bombole di ossigeno, carrelli di emergenza, monitor dei pazienti, aste per flebo e sedie a rotelle migliorando la sicurezza e l'efficienza. Le connessioni tra persone, oggetti e applicazioni si possono utilizzare anche per attivare allarmi che segnalano al personale medico le necessità dei pazienti, i malfunzionamenti delle apparecchiature e possono avvisare tutti i membri della struttura in caso di situazioni non sicure.

Nel settore dell'istruzione, c'è un nuovo potenziale per connettere i dispositivi e le applicazioni del campus intelligente, grazie a diversi livelli di sicurezza è possibile proteggere le risorse dell'istituto dai dispositivi poco protetti che accedono alla rete. Gli istituti scolastici possono anche utilizzare il rilevamento delle impronte digitali dei dispositivi IoT per identificare le caratteristiche dei dispositivi, come il tipo, il produttore, il modello e il sistema operativo, per semplificare e accelerare la configurazione della rete IoT e l'onboarding dei dispositiv..

Aumentare l'eccellenza operativa e l'agilità

Grazie possibilità di implementare in modo flessibile e sicuro le soluzioni unified communication e collaboration, on premise o con un modello di cloud ibrido. privato o pubblico, le aziende e le organizzazioni pubbliche possono trarre vantaggio dalle tecnologie digitali nel modo che meglio si allinea ai loro obiettivi e mandati. Ogni organizzazione può raggiungere nuovi livelli di eccellenza operativa, soddisfacendo al contempo i requisiti specifici del settore, adottando modelli cloud per migliorare l'operatività e l'agilità in contesti quali:

- **Sanità**, dove le cartelle cliniche digitali possono essere utilizzate per migliorare l'assistenza ai pazienti e aumentare l'efficienza del personale medico, con la massima garanzia che le informazioni personali vengano archiviate in un centro dati sicuro e certificato nel cloud.
- **Istruzione**, dove docenti, personale e studenti hanno un accesso ad applicazioni e servizi basati sul cloud, sicuro e sensibile alla privacy, ovunque. E dove i reparti IT possono ridurre i tempi e i costi associati all'implementazione, al supporto e all'aggiornamento di un'ampia gamma di applicazioni.
- **Pubblica amministrazione**, dove le comunicazioni riservate possono essere supportate da un'elevata disponibilità e protette da meccanismi DoS integrati e da hardware e sistemi operativi sicuri e di tipo industriale.
- **Trasporti**, dove l'alterazione delle funzionalità di comunicazione può creare situazioni di pericolo, rendendo essenziali soluzioni di sovranità dei dati.

Cybersecurity, come parte integrante del mindset del fornitore di tecnologia

Sebbene molti fornitori di tecnologie promuovano la sicurezza informatica, non tutti dispongono di competenze complete per implementare funzionalità di sicurezza end-to-end.

Alcatel-Lucent Enterprise va ben oltre gli altri fornitori per implementare tutte le best practice necessarie per la sicurezza informatica end-to-end. In quanto:

- Applica le best practice e quanto raccomandato dal National Institute of Science and Technology (NIST) in sede di assesmnet del rischio di nuove funzionalità e in fase di implementazione della funzionalità di cybersecurity, come la crittografia nativa, nelle proprie soluzioni.
- Adotta la certificazione Common Criteria EAL2+
- Applica gli standard ISO 27001 a tutte le sue soluzioni basate sul cloud.
- Promuove l'approccio ZTNA, la segmentazione di rete granulare nonché criteri di sicurezza altamente specifici per ridurre il rischio di attività non autorizzate.
- Esegue test altamente specializzati e specifici per la sicurezza, come i test di penetrazione, su tutti i suoi prodotti.
- Garantisce che i propri prodotti ottengano le certificazioni chiave di settore, come HDS, HIPAA e Family Educational Rights and Privacy Act (FERPA).

Essendo riconosciuta tra le aziende esperte di sicurezza informatica, contribuisce alle proposte dell'Unione Europea per le direttive in materia. Inoltre, grazie alla propria esperienza aiuta i clienti nella scelta e nell'adozione del giusto mix di soluzioni di unified communication e collaboration sicure e adatte alle loro esigenze, supportandoli a formare i loro dipendenti sulle migliori pratiche di sicurezza informatica.

Alcatel-Lucent Enterprise è un partner affidabile a livello mondiale

Molte organizzazioni di diversi settori verticali si affidano alle soluzioni di comunicazione sicure e digitali di ALE per raggiungere i loro obiettivi, tra cui:

- Metropoli e città di Perpignan in Francia, dove i funzionari della pubblica amministrazione stanno attuando un piano strategico di transizione digitale che include sistemi di videoconferenze e comunicazioni vocali per i dipendenti, supporto per le applicazioni IoT e nuovi contenuti e servizi per i residenti, i turisti del capoluogo e i dipendenti comunali.
- Newman University negli Stati Uniti, un college cattolico di arti liberali che ha dotato il personale di funzionalità di telefonia mobile che non richiedono numeri di telefono diretti e il team IT di un'unica piattaforma intuitiva basata sul cloud per la gestione, il provisioning e il monitoraggio di tutta l'infrastruttura di rete.
- Kingsway Hospitals in India, che ha adottato un'infrastruttura di soluzioni di comunicazione che mantengono il personale clinico e amministrativo connesso, in tempo reale, con l'obiettivo di ottimizzare l'erogazione delle cure e migliorare l'esperienza del paziente.
- J. Malucelli Group in Brasile, che ha modernizzato la propria rete con una soluzione convergente di comunicazione e di rete che comprende la telefonia, reti LAN e Wi-Fi con gestione in cloud per semplificare e ridurre i costi delle comunicazioni per le diverse aziende del gruppo.

Ulteriori informazioni

Per saperne di più su come ALE può aiutare la tua organizzazione a beneficiare delle soluzioni Digital Age Communication, visita il nostro sito web o contattataci oggi stesso.

© 2023 ALE International, ALE USA Inc. Tutti i diritti riservati in tutti i paesi. Il nome e il logo Alcatel-Lucent sono marchi commerciali di Nokia utilizzati da ALE sotto licenza. Per visualizzare l'elenco dei marchi proprietari di ALE, visitare: https://www.al-enterprise.com/it-it/legal/trademarks-copyright.DID23042401IT (agosto 2023)

Alcatel·Lucent Enterprise