Considerazioni e soluzioni per la digitalizzazione del luogo di lavoro del settore pubblico

Alcatel·Lucent
Enterprise

eBook

Indice

Panoramica

In tutte le organizzazioni pubbliche ci sono dipendenti che svolgono delle attività critiche su cui tutti facciamo affidamento. Il loro ruolo non può essere sottovalutato. Spesso hanno un impatto diretto sulla vita di molte migliaia di persone.

La digitalizzazione è un processo in corso da tempo. Con la continua pressione per migliorare i servizi pubblici e tagliare i costi, la pandemia ha ulteriormente accelerato questa tendenza. Tuttavia, due anni fa non era possibile prevedere che una considerevole percentuale di lavoratori pubblici avrebbe dovuto lavorare da casa, né c'era modo di ipotizzare la conseguente necessità di distribuzione della forza lavoro che ne sarebbe emersa.

Le sfide dei lavoratori che necessitano di un mondo più digitale e le complesse esigenze di riuscire a sostenere una forza lavoro distribuita, hanno imposto alle organizzazioni pubbliche di passare da soluzioni temporanee a soluzioni permanenti in grado di supportare la modalità di lavoro ibrida.

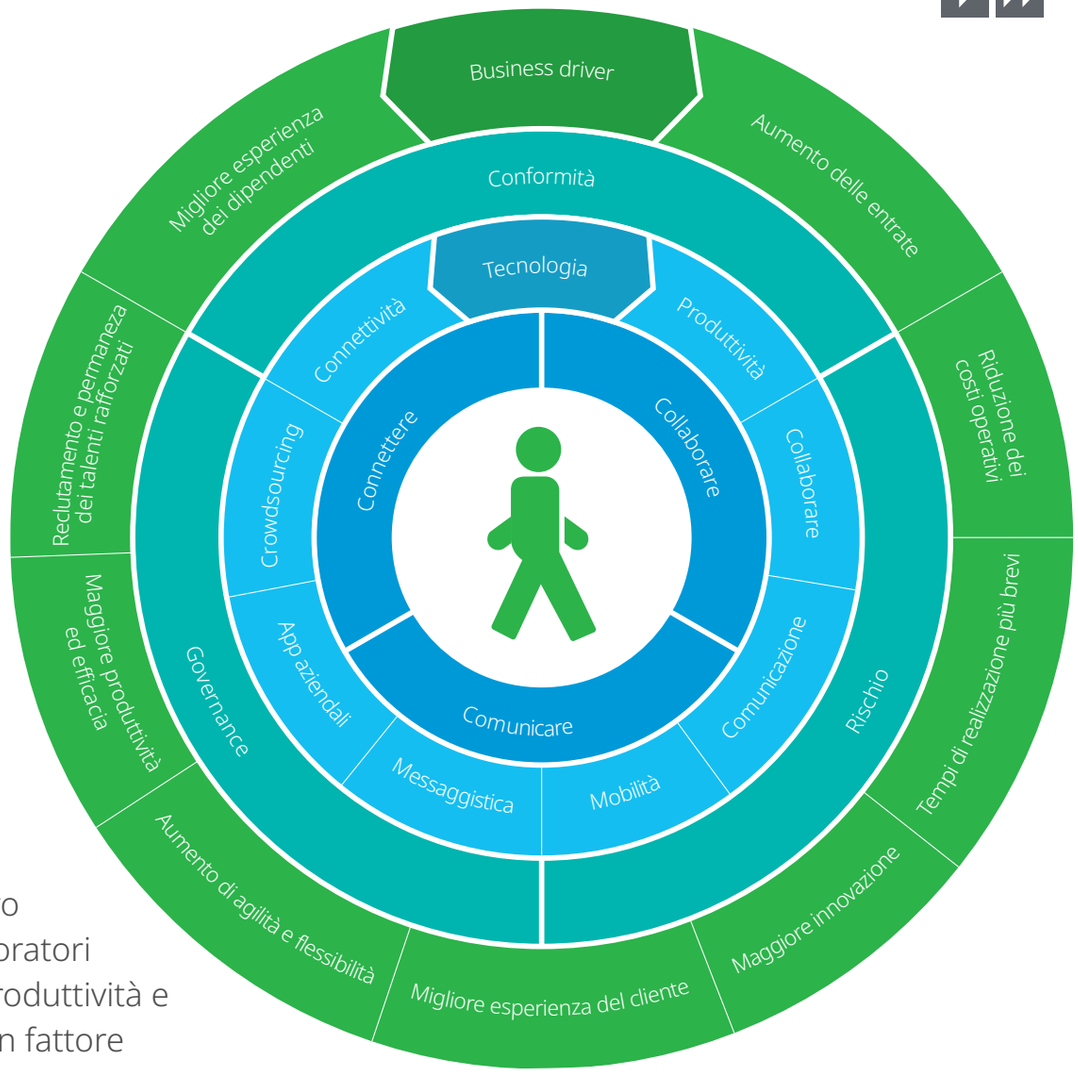
Deloitte[1] fornisce un eccellente grafico che spiega come il luogo di lavoro digitale si inserisce e quali vantaggi offre.

La tecnologia fornisce strumenti per migliorare le comunicazioni e la collaborazione ovunque e con qualsiasi dispositivo, tuttavia, assicurarsi di disporre della tecnologia adeguata per il risultato desiderato può non essere un'impresa così semplice.

Alcatel-Lucent Enterprise ha collaborato con clienti di tutto il mondo per comprendere le nuove sfide che questi devono affrontare e per fornire soluzioni di tecnologia digitale che consentano ai lavoratori di svolgere l'attività ovunque e con qualsiasi dispositivo. Il luogo di lavoro digitale ha creato efficienze per i lavoratori pubblici, favorendo una maggiore produttività e riducendo gli spostamenti, il che è un fattore positivo per l'intero pianeta.

Questo eBook evidenzia i tre elementi chiave per ottenere un ambiente di lavoro digitale di successo nel settore pubblico:

- Comunicazioni e collaborazione
- Connettività
- Sicurezza



Esamineremo le soluzioni di Alcatel-Lucent Enterprise che possono aiutare le organizzazioni pubbliche a digitlizzare con successo il posto di lavoro in maniera flessibile, agiile e sicura.

1 https://www2.deloitte.com/content/dam/Deloitte/be/Documents/technology/The_digital_workplace_Deloitte.pdf

Considerazioni chiave per ottenere un ambiente di lavoro digitale nel settore pubblico

Comunicazioni e collaborazione

Oggi i dipendenti dividono il loro luogo di lavoro tra casa, postazioni remote e ufficio. L'ufficio non è più il luogo dove si lavora quotidianamente, e viene spesso utilizzato per riunioni di gruppo, formazione e incontri con i cittadini. Gli impiegati non si recano più in un solo luogo per lavorare e incontrarsi con i loro colleghi e team e questo nuovo modo di lavorare ha impattato fortemente l'ambiente di lavoro tradizionale, rendendo le comunicazioni e la collaborazione più importanti che mai.

Le comunicazioni sono una componente critica per la digitalizzazione del luogo di lavoro, in quanto la sfida è riuscire a mantenere i dipendenti coinvolti, produttivi e motivati. Ai lavoratori occorrono strumenti di comunicazione che consentano loro di svolgere le attività quotidiane, di comunicare e collaborare con colleghi, team e cittadini ovunque si trovino e qualunque sia il dispositivo che utilizzano.

Per garantire comunicazioni connesse, raccomandiamo:

- Funzionalità di comunicazioni avanzate per i dipendenti, tra cui: voce di alta qualità, chat di gruppo, messaggi vocali e la possibilità di passare da una chiamata a un video qualunque sia il dispositivo
- Funzionalità di collaborazione quali la condivisione dello schermo, il controllo remoto del desktop e la condivisione di file di grandi dimensioni
- Comunicazioni e collaborazione con contatti esterni in totale sicurezza
- Continuità delle chiamate in tutta l'organizzazione con connessione istantanea e elenco di contatti coerente
- Un canale di trasmissione per le notizie, per tenere tutti aggiornati sugli ultimi annunci o regolamenti
- Soluzioni di comunicazione e collaborazione intuitive

Per assicurare che tutti i dipendenti dispongano di ciò di cui hanno bisogno, raccomandiamo di:

- Valutare i principali profili e i requisiti di comunicazione degli utenti tenendo conto dei ruoli e della loro necessità di mobilità, nonché dell'esigenza di accedere alle app aziendali
- Offrire ai dipendenti in prima linea dispositivi ottimizzati che consentano un accesso rapido alle informazioni e alle comunicazioni mentre sono in movimento

- Garantire che il personale del servizio clienti abbia un accesso ottimizzato per la gestione delle chiamate e delle interazioni integrato con il CRM o le app aziendali
- Consentire la collaborazione con il personale di back-office per migliorare i servizi per i cittadini e la risoluzione dei problemi sin dalla prima chiamata
- Valutare i requisiti giuridici locali/del paese per proteggere la privacy dei dati

Per garantire un lavoro ad alte prestazioni da casa raccomandiamo:

- Chat di gruppo, funzionalità audio e video meeting con condivisione dello schermo e file per collaborare su qualsiasi dispositivo
- Continuità delle chiamate utilizzando un'infrastruttura di base per connettere tutti i profili
- Un'opzione DeskPhone per i dipendenti che trascorrono più di un'ora al telefono e gestiscono chiamate importanti, come servizi ai cittadini, assistenza sanitaria e situazioni di emergenza
- Funzionalità di comunicazione integrate nell'app aziendale preferita per facilitarne l'adozione da parte dell'utente e mantenere il desktop libero da ingombri
- Accesso remoto protetto per consultare in totale sicurezza le informazioni sensibili

Connettività

Il luogo di lavoro digitale si basa su una connettività di alta qualità, resiliente e sicura. Man mano che i nuovi modi di lavorare si normalizzano e il luogo di lavoro digitale prende forma, è necessario predisporre l'infrastruttura digitale per connettere i dipendenti. Indipendentemente dall'ubicazione, si devono considerare alcuni punti chiave:

- La sicurezza deve essere una priorità assoluta. È necessaria una soluzione con diversi livelli di sicurezza all'interno della rete. Una struttura basata sull'approccio zero trust presuppone che ogni dispositivo o utente rappresenti un rischio per la sicurezza. Il controllo dell'accesso alla rete deve essere abilitato.
- L'accesso sicuro alle applicazioni da qualsiasi luogo crea la necessità di connessioni di accesso basate sull'utente. I profili basati sull'utente forniscono una connettività sicura e flessibile senza perdita di servizio, indipendentemente dalla posizione.
- I lavoratori remoti con elevati requisiti di sicurezza e privacy dei dati devono essere in grado di connettersi alla rete aziendale da casa o dalle filiali. Questo garantisce il rispetto delle policy e della sicurezza aziendali, nonché il controllo da parte del team IT.
- I lavoratori oggi utilizzano notebook per applicazioni in tempo reale (voce, video) in ufficio e a casa. Questo è un grande cambiamento per molte organizzazioni del settore pubblico. La rete wireless deve essere in grado di supportare un uso più intenso di applicazioni in tempo reale su un'area più ampia. È un aspetto che dovrebbe essere preso in considerazione quando si definisce la rete.
- La resilienza della rete wireless è passata in cima all'elenco delle priorità, in quanto molti più lavoratori si connettono col WiFi. In una rete wireless distribuita con access point intelligenti non esistono singol point of failure, in caso di non funzionamento di un access point, il servizio verrà assunto da altri access point della rete. Una rete wireless distribuita elimina anche la necessità di duplicare la rete, consentendo di risparmiare tempo e denaro.
- Il ritmo accelerato della trasformazione digitale crea pressione per il team IT che è già alle prese con sfide quotidiane, pertanto andrebbe valutato come ottenere ulteriori efficientamenti. La riduzione del numero di interfacce di gestione e di sistemi operativi sulla rete diminuirà i carichi di lavoro e il tempo di formazione, mentre l'automazione il tempo di implementazione e di gestione operativa della rete stessa
- È essenziale un accesso di alta qualità. Il luogo di lavoro digitale crea efficienze che consentono un aumento della produttività, ma se la connettività viene a mancare questo incremento si vanifica.

Sicurezza

Sicurezza delle comunicazioni

Il Governo e le organizzazioni del settore pubblico sono obiettivi significativi per gli attacchi informatici. Per questi enti è fondamentale utilizzare l'attrezzatura più sicura disponibile sul mercato. Gli strumenti di gestione integrata devono consentire la supervisione della sicurezza su tutti gli elementi della rete.

Da non sottovalutare il fatto che i dispositivi mobili stanno trasformando il panorama delle comunicazioni e aumentando il bisogno di sicurezza, in quanto gli aggressori informatici sfruttano i crescenti volumi di codice contenuti in ogni access point. La crittografia di tipo defense-grade, la privacy dei dati e gli ambienti di comunicazione sicuri necessitano di un'infrastruttura sicura e disponibile che sia efficiente e facile da gestire.

I nostri consigli

Aggiornare e controllare il proprio sistema di comunicazione:

- Gli aggiornamenti del sistema rivestono un'importanza critica in termini di sicurezza informatica. E' fondamentale mantenere i sistemi di comunicazione aggiornati per una maggiore protezione contro la vulnerabilità del software.
- Abilitare il monitoraggio del sistema di comunicazione per tracciare attività sospette configurando soglie d'uso e allarmi nel sistema di gestione della rete

Autenticare e criptare:

- Abilitare l'autenticazione reciproca tra tutti i dispositivi (telefoni e gateway) e il sistema di comunicazione
- La segnalazione deve essere criptata per prevenire attacchi di protocol poisoning e man in-the-middle
- Le comunicazioni IP devono essere criptate per evitare le intercettazioni

Rendere i sistemi ridondanti e aggiungere una componente di sicurezza:

- Il rischio non può mai essere uguale a zero. Se un gateway o il sistema di comunicazione principale è fuori uso, un sistema di back-up può subentrare senza problemi in presenza di ridondanza spaziale.
- Aggiungere i componenti necessari per proteggere il proprio sistema di comunicazione, come Session Border Controller (controller di fine sessione) o Reverse Proxy, mentre i server di notifica sono utilizzati per avvisare le persone di competenza

Educare:

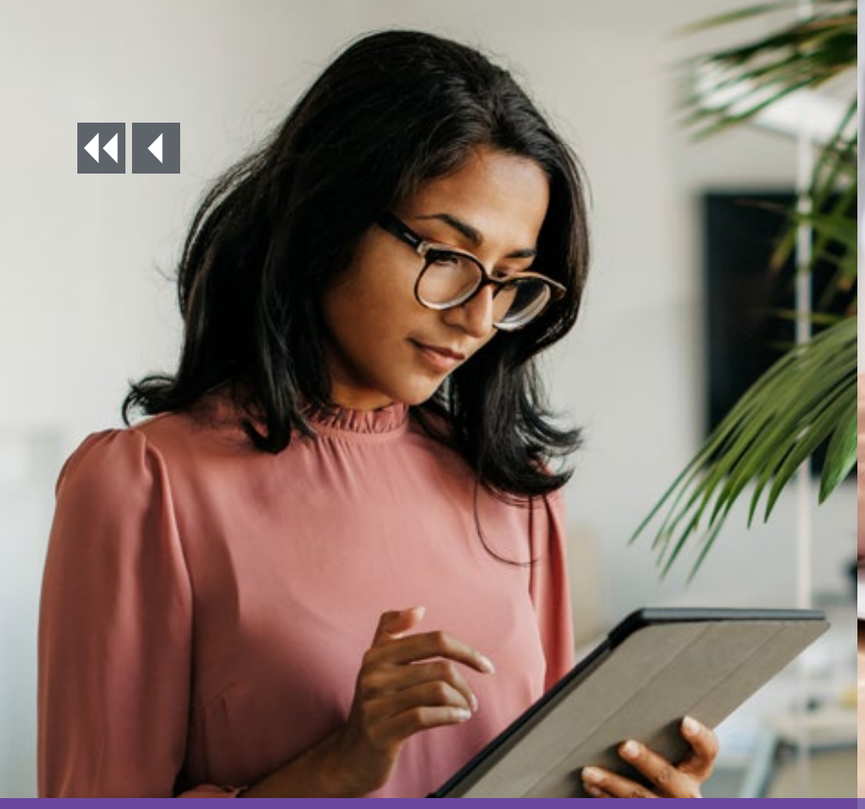
- Educare gli utenti e gli amministratori; applicare le migliori pratiche all'interno dei team, compresi i promemoria per l'aggiornamento delle password, formare gli utenti su come combattere il crimine informatico e come riconoscere una chiamata criptata con l'icona del lucchetto sul telefono

Sicurezza della rete

La sicurezza informatica è da tempo una priorità fondamentale per le organizzazioni della pubblica amministrazione. Tuttavia, le richieste relative ad essa stanno cambiando a causa della trasformazione digitale. Con l'accelerazione della trasformazione, i vecchi metodi di sicurezza della rete stanno diventando obsoleti. In quanto componente fondamentale dell'architettura di rete, la sicurezza deve essere incorporata sotto ogni aspetto e applicata universalmente in tutti gli accessi alla rete - cablata e wireless. Di seguito sono riportate alcune aree da considerare per rendere sicura la rete a tutti i livelli.

- **Livello utente:** verificare che gli utenti siano sempre autenticati e autorizzati con i corretti diritti di accesso (utilizzando policy e profili)
- **Livello dispositivo:** verificare che i dispositivi siano autenticati e conformi alle regole di sicurezza stabilite dall'IT. Questo obiettivo si può ottenere con agenti installati sui dispositivi che eseguono una rapida scansione di sicurezza prima che questi si connettano alla rete.
  Ad esempio, la scansione può garantire che i dispositivi che si aggiungono alla rete abbiano un software antivirus aggiornato e l'ultima versione del sistema operativo.
- **Livello applicazione:** impostare regole associate a specifiche applicazioni (compreso il blocco, la limitazione della larghezza di banda o l'identificazione di chi può usarle)
- **Analisi dei dati intelligente:** le capacità di analisi negli switch e negli access point aiutano a fornire visibilità e informazioni dettagliate riguardo a rete, utenti, dispositivi e applicazioni utilizzate in rete. Possono anche fornire funzonalità deep packet inspection che rilevano 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.
- **Tecniche di segmentazione della rete**: collocare dispositivi IoT in contenitori virtuali sicuri consente a più dispositivi e reti di utilizzare la stessa infrastruttura fisica, rimanendo isolati dal resto della rete. Se una violazione si verifica in una parte della rete virtuale, non colpisce altre aree o applicazioni.

Queste tecniche di sicurezza aiutano a costruire una struttura di architettura zero trust, il livello successivo nell'architettura di rete che opera secondo il principio "non fidarsi mai - verificare sempre", dove tutti gli utenti devono essere autenticati, autorizzati e continuamente convalidati prima di essere autorizzati ad accedere ad applicazioni e dati.



Luogo di lavoro digitale

Modelli cloud flessibili

Connettere tutto

Soluzioni ALE per il luogo di lavoro digitale del settore pubblico

Comunicazioni e collaborazione

Digital Age Communication (DAC) di Alcatel-Lucent Enterprise offre una gamma completa di soluzioni e servizi di comunicazione e collaborazione basati sul cloud per affrontare la trasformazione digitale. Il luogo di lavoro digitale si sta evolvendo verso un ambiente professionale distribuito, dove il lavoro a distanza è diventato normale, rendendo le comunicazioni in tempo reale essenziali per connettere colleghi, cittadini e partner. Le soluzioni di comunicazione Alcatel-Lucent Enterprise consentono la continuità delle chiamate ovunque, in qualsiasi situazione e su qualsiasi dispositivo.

Funzionalità di comunicazione chiave di Alcatel-Lucent Enterprise:

- **Connessione senza soluzione di continuità** all'interno e all'esterno dell'organizzazione. L'infrastruttura di comunicazione di base connette chi lavora in modalità ibrida al personale di back-office e in prima linea, indipendentemente dai dispositivi utilizzati, attraverso una varietà di tecnologie standard quali PSTN, TDM, IP, SIP, VoWIFI, DECT e fornisce anche metriche per l'IT per il controllo della Qualità del Servizio (QoS).
- **Il routing one number** attraverso il telefono professionale e il softphone è ideale per il lavoro ibrido. I dipendenti possono lavorare da casa o in ufficio senza perdere chiamate e senza la necesssità di effettuare trasferimenti di chiamata.

- I DeskPhones di ALE offrono **robusti portatili di qualità HD 3D Symphonic** e applicazioni per smartphone con notifiche e allarmi anche durante il roaming in loco e sono in genere destinati al personale mobile che lavora in prima linea.
- **Facile accesso** alle funzionalità di accoglienza clienti e agli agenti, ad esempio gruppi e code di chiamata aiutano il personale del servizio clienti a rispondere a tutte le chiamate in entrata
- **Conferenza di crisi per chiamate di emergenza**, consente ai contatti predefiniti di essere automaticamente inseriti in una conferenza per la gestione di disastri o crisi con la semplice pressione di un pulsante
- **La crittografia end-to-end** garantisce la sicurezza e la privacy richieste dalle organizzazioni del settore pubblico

- Le comunicazioni e la collaborazione per il luogo di lavoro digitale sono semplici, **basta un clic per chiamare** un contatto o avviare una conferenza, oppure è possibile utilizzare funzionalità più avanzate come la chat di gruppo, la condivisione dello schermo e dei file, le riunioni audio e video, tutto in una singola app, disponibile come client web. Nessuna installazione necessaria. Le applicazioni sono disponibili per dispositivi Android e iOS e per PC. I clienti con soluzioni ALE possono utilizzare i terminali esistenti con tecnologia WebRTC.
- I connettori per Microsoft® Teams e Google consentono ai dipendenti di **comunicare senza difficoltà** con tutta l'organizzazione dal rispettivo luogo di lavoro digitale. Con i connettori per SaaS CRM e ITSM, i dipendenti possono comunicare e collaborare dalle loro app aziendali.

eBook
Considerazioni e soluzioni per la digitalizzazione del luogo di lavoro del settore pubblico

Connettività

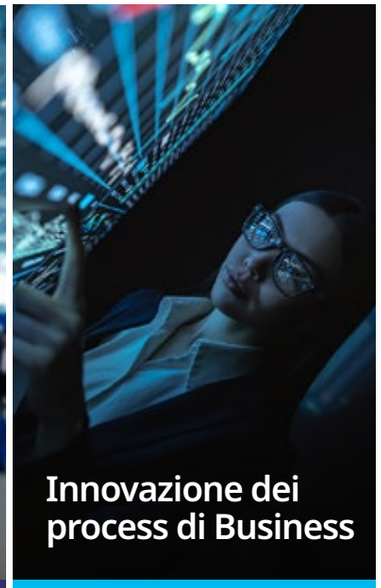
Digital Age Networking di Alcatel-Lucent Enterprise fornisce una rete autonoma con un'esperienza di connessione resiliente e senza soluzione di continuità grazie ad Alcatel-Lucent OmniSwitch® (LAN) e ad Alcatel-Lucent OmniAccess® Stellar (WLAN), con una convergenza ultra veloce, un controllo sicuro dell'accesso alla rete e QoS garantita. Il Wi-Fi aziendale di nuova generazione, con controllo WLAN integrato negli access point, elimina la necessità di dispositivi di controllo fisici centralizzati. Le soluzioni ALE possono essere gestite on premises e in cloud.

Caratteristiche chiave della connettività ALE:

- **Un singolo Network Management System (NMS)** fornisce un ulteriore livello di integrazione tra le reti cablate e wireless riducendo il carico di lavoro del manager IT, poiché non occorre controllare due sistemi di gestione con due serie di policy e regole di configurazione. La soluzione OmniVista® Network Management System di Alcatel-Lucent Enterprise offre una gestione unificata e la massima visibilità in tutta la rete per migliorare l'efficienza e l'agilità dell'IT.
- **Il provisioning automatizzato** di un'infrastruttura di rete sicura semplifica le aggiunte, gli spostamenti e le modifiche, riducendo il tempo necessario per mantenere e far funzionare la rete, creando efficienza operativa e diminuendo costi e rischi.
- **Shortest Path Bridging (SPB),** progettato per sostenere la creazione e il funzionamento di una rete meno complessa, costruisce dinamicamente e mantiene la tipologia di rete tra i nodi. L'SPB condivide il carico e utilizza tutte le connessioni fisiche disponibili con una maggiore larghezza di banda.
- **Lavoratori ibridi (opzione 1). L'accesso remoto sicuro** è abilitato con il Remote Access Point (RAP). La rete aziendale può essere facilmente estesa al di fuori della sede principale, fornendo connettività ai lavoratori remoti come se fossero nella LAN aziendale. A seconda del modello, il RAP può anche fornire connettività cablata per telefoni IP o per altri dispositivi IoT. L'accesso è supportato da policy di sicurezza centralizzate e unificate tra le reti cablate e wireless, garantendo una gestione semplice e una sicurezza altamente solida e coerente.
- **Lavoratori ibridi (opzione 2) SD-WAN e SASE**. Il Secure Access Service Edge (SASE) collega in modo sicuro siti remoti, filiali e lavoratori remoti. La soluzione SASE per i lavoratori remoti consiste in un software nel computer portatile dell'utente che fornisce un accesso sicuro alle applicazioni nel data center dell'azienda, in data center privati, Internet o in cloud pubblici, con una gestione centralizzata e senza richiedere hardware aggiuntivo presso il sito del lavoratore. SASE fornisce sicurezza avanzata con firewall di nuova generazione (NGFW), compreso il filtraggio degli URL e il firewall delle applicazioni Unified Threat Management (UTM, ossia la gestione unificata delle minacce), tra cui il Next Generation Intrusion Prevention System (NGIPS - sistema di prevenzione delle intrusioni di nuova generazione) antivirus e anti-malware.

Automatizzare le operazioni di rete mission-critical e migliorare l'esperienza degli utenti

Aumentare la digitalizzazione con onboarding e gestione sicure dell'IoT



Accelerare la trasformazione con flussi di lavoro automatizzati

Sicurezza

Sicurezza delle comunicazioni

Che tu sia responsabile di un piccolo ente di amministrazione locale o di un grande paese, la tua rete di comunicazione rischia di essere presa di mira dagli hacker.

Caratteristiche di sicurezza chiave di Alcatel-Lucent Enterprise:

- **Connettività sicura** tra il sistema di comunicazione on premises (PBX e telefoni) e l'infrastruttura cloud, completamente sviluppata e gestita da Alcatel-Lucent Enterprise, con autenticazione reciproca, crittografia e Security Border Element (SBC)
- **Alta disponibilità** con architetture ridondanti in termini spaziali, on premises, in cloud privati o pubblici, protezione contro gli attacchi denial of service (DoS), sicurezza integrata con hardware hardened e sistemi operativi
- **Riservatezza delle comunicazioni** con una forte crittografia basata su standard industriali con attuazione nativa nella soluzione, senza alcun impatto sulla qualità della voce e sulle prestazioni, per offrire l'esperienza che clienti e dipendenti si aspettano
- **Privacy e protezione dei dati** con controllo degli accessi basato sui ruoli e crittografia dei dati memorizzati. Questo assicura che tutti i dati cruciali raccolti nell'ambiente aziendale in evoluzione siano completamente protetti e sotto il controllo dell'utente.
- **Conformità ai regolamenti e alle norme** quali (ma non solo) il regolamento generale sulla protezione dei dati (GDPR), ISO27001, Common Criteria EAL2+, HDS ("Hébergeur Données Santé",certificazione dei servizi cloud ALE per la conformità alla protezione dei dati dei pazienti in Francia)
- **Sicurezza come processo** con Product Security Incident Response Team (PSIRT) per la gestione attiva delle vulnerabilità, software regolarmente aggiornato e piattaforma di policy

ANSSI (CSPN)

ENS (Esquema Nacional de Seguridad)

Certificazione istituita dal Sistema di Sicurezza Nazionale Spagnolo per avere un sistema che garantisca la corretta protezione dei sistemi d'informazione contro le minacce e gli incidenti esterni.

ISO27001 - 017/018

L'Agenzia per l'Italia Digitale sotto la Presidenza del Consiglio dei Ministri, disciplina l'uso, la conservazione e l'accesso ai dati importanti, garantendo la sicurezza.

CERTIFICAZIONI IN CORSO

Certificazione BSI

L'Ufficio federale per la sicurezza informatica (Bundesamt für Sicherheit in der Informationstechnik). Equivalente al CSPN dell'ANSSI (3° trimestre 2021)

eBook
Considerazioni e soluzioni per la digitalizzazione del luogo di lavoro del settore pubblico

Sicurezza della rete

La trasformazione digitale ha cambiato profondamente i requisiti necessari per garantire la sicurezza informatica, poiché il numero di dispositivi connessi aumenta, i confini della rete spariscono e il cambiamento continua ad accelerare. La soluzione Digital Age Networking di Alcatel-Lucent Enterprise mantiene le risorse IT e i dati al sicuro nell'attuale era di trasformazione digitale. Grazie a questa soluzione è possibile gestire da vicino l'accesso degli utenti, ridurre le vulnerabilità create dai dispositivi IoT, mobili e di rete, evitare che le inevitabili violazioni rappresentino un punto di attacco e offrire un ecosistema aziendale da una posizione sicura.

Le soluzioni ALE sono sicure per progettazione con:

- **Secure Diversified Code** che promuove la sicurezza e l'assicurazione a livello del dispositivo di rete utilizzando la verifica e la convalida di terze parti indipendenti, tra cui:
  - Analytics del codice sorgente, test white box e black box da parte di un'azienda specializzata in sicurezza informatica per eliminare le vulnerabilità tra cui:
    - ¬ Minacce back-door
    - ¬ Malware incorporato
    - ¬ Vulnerabilità strumentali
    - ¬ Esposizione di informazioni proprietarie e/o classificate
- **Diversificazione del software:** il software ALE implementa l'Address Space Layout Randomisation (ASLR). Ogni avvio dello switch genera dinamicamente un layout di memoria univoco per impedire o prevenire lo sfruttamento del software.
- **Sicurezza zero trust (micro e macrosegmentazione):** una struttura basata sull'approccio zero trust presuppone la presenza di hacker. L'impresa non è più considerata un'implicita zona di fiducia. Questo comporta azioni come l'autenticazione di tutte le connessioni. Nessuna risorsa e nessun utente è intrinsecamente affidabile.
- **Sicurezza per impostazione predefinita:** l'accesso remoto su OmniSwitch deve essere abilitato, al contrario della maggior parte degli altri switch dove tutti gli accessi agli sono attivati come impostazione predefinita e gli amministratori devono capire come proteggere il dispositivo
- **Protezione Denial of Service (DoS) integrata:** protezione del sistema operativo e del modulo di gestione da una serie di attacchi DDOS che sono di norma utilizzati per causare un utilizzo della CPU al 100%.
- **Nessun pacchetto software** da acquistare e tracciare: ogni funzionalità e capacità, anche il codice sicuro ALE, è incluso nel prezzo dello switch - nessun modulo da aggiungere, nessun aggiornamento da acquistare. Il software è tutto incluso.
- **Onboarding IoT automatizzato e sicuro:** tramite le impronte digitali dei dispositivi, la classificazione e la containerizzazione

GDPR dell'UE

US Federal

US Joint Interoperability

US MIL-STD

US Trade Agreements Act (TAA)

eBook
Considerazioni e soluzioni per la digitalizzazione del luogo di lavoro del settore pubblico

Ulteriori informazioni

Scopri di più sulle soluzioni Alcatel-Lucent Enterprise per il settore pubblico progettate per il luogo di lavoro digitale o contattataci per discutere le esigenze della tua azienda.

www.al-enterprise.com/it-it/industries/government

Alcatel·Lucent Enterprise