



Zabezpieczenie rozwiązań do zunifikowanej komunikacji i współpracy

Co oznacza w dzisiejszym zmieniającym się świecie

Opracowanie techniczne

Alcatel•Lucent 
Enterprise

Spis treści

- | Większy nacisk na cyberbezpieczeństwo
- | Sześć kluczowych obszarów kompleksowego bezpieczeństwa cybernetycznego
- | Osiągaj cele biznesowe przy mniejszym ryzyku
- | Cyberbezpieczeństwo: nieodłączna część sposobu myślenia dostawcy technologii

Większy nacisk na cyberbezpieczeństwo

W ciągu ostatnich kilku lat prawie każde przedsiębiorstwo i organ administracji zmieniły sposób, w jaki jego pracownicy komunikują się, współpracują i udostępniają informacje. Chociaż szybkie przejście na wspieranie pracowników pracujących z domu było kluczowe dla utrzymania ciągłości biznesowej podczas pandemii, miało to swoją cenę: obwód sieci wykracza teraz daleko poza granice tradycyjnego biura, znacznie zwiększając obszar, na którym organizacja jest podatna na atak.

Ryzyko związane z rozszerzeniem granic sieci nie zniknie w najbliższym czasie. Według firmy Gartner do końca 2023 roku 39 procent pracowników umysłowych na całym świecie będzie pracować w ramach hybrydowych modeli zdalnych i stacjonarnych. W Stanach Zjednoczonych liczba ta wzrasta do 51 procent¹.

Zakłócenia geopolityczne dodatkowo zwiększyły zagrożenia dla cyberbezpieczeństwa. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa nazwała rosyjską inwazję na Ukrainę czynnikiem „zmieniającym zasady gry” w globalnej domenie cybernetycznej.² Według Stowarzyszenia Ukraińskich Firm Outsourcingowych IT, w 2022 roku jedna na pięć firm z listy Fortune 500 korzystała z usług programistów z tego kraju.³

Jednocześnie rośnie wpływ cyberataków na społeczeństwo. W 2022 roku byliśmy świadkami poważnych cyberataków na krytyczną infrastrukturę obywatelską, które spowodowały stan wyjątkowy w Kostaryce⁴, a także kolejnych ataków na organizacje opieki zdrowotnej.⁵

Organizacje nie mogą sobie pozwolić na odkładanie ulepszeń cyberbezpieczeństwa na później

Szacuje się, że cyberprzestępczość kosztowała światową gospodarkę 5,5 biliona euro w 2021 roku, a szkody mają przekroczyć 10 bilionów euro do 2025 roku.⁶ Problem jest na tyle poważny, że Unia Europejska tworzy ustawę o odporności cybernetycznej i wydała znacznie udoskonaloną drugą wersję swojej dyrektywy w sprawie bezpieczeństwa sieci i informacji (NIS), aby chronić konsumentów i firmy, którzy kupują lub używają produktów albo oprogramowania z komponentem cyfrowym.⁷ Także Stany Zjednoczone wdrażają środki mające na celu wzmocnienie cyberbezpieczeństwa, w tym dekret 14028, co zachęca agencje do przyjęcia zasady zerowego zaufania i odpowiedniego dostosowywania architektur sieci.⁸

Ponieważ przedsiębiorstwa i rządy dążą do cyfrowej transformacji i bardziej trwałego wspierania elastycznych modeli pracy, nie mają innego wyjścia, jak tylko wzmocnić cyberbezpieczeństwo. Rozwiązania używane przez ich zespoły do komunikacji, współpracy i udostępniania informacji muszą uwzględniać najlepsze praktyki w zakresie cyberbezpieczeństwa na każdym poziomie i we wszystkich aspektach funkcjonalności.

¹ [Gartner Forecasts 39% of Global Knowledge Workers Will Work Hybrid by the End of 2023](#), Gartner, marzec 2023 r.

² [Zmiana geopolityki wstrząsa trendami krajobrazu zagrożeń dla cyberbezpieczeństwa w 2022 r.](#) Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, listopad 2022 r.

³ [Jedna na pięć firm z listy Fortune 500 polega na Ukrainie w zakresie rozwoju oprogramowania w 2022 r.](#) Ukrainian Hi-Tech Initiative, październik 2022 r.

⁴ [13 najbardziej kosztownych cyberataków 2022 roku: spojrzenie wstecz. Analiza bezpieczeństwa](#), grudzień 2022 r.

⁵ [Podsumowanie 2022: pełen wydarzeń rok cyberbezpieczeństwa](#), Forbes, grudzień 2022 r.

⁶ [New European Union cybersecurity proposal takes aim at cybercrime](#), Światowe Forum Ekonomiczne, wrzesień 2022 r.

⁷ [Europejska Ustawa w sprawie odporności cybernetycznej](#), Komisja Europejska, wrzesień 2022 r.

⁸ [Dekret w sprawie poprawy bezpieczeństwa cybernetycznego kraju](#), Agencja Bezpieczeństwa Cyberbezpieczeństwa i Infrastruktury.

Opracowanie techniczne

Zabezpieczenie rozwiązań do zunifikowanej komunikacji i współpracy





Sześć kluczowych obszarów kompleksowego bezpieczeństwa cybernetycznego

W rozwiązaniach do ujednoliconej komunikacji i współpracy należy wdrażać kompleksowe zabezpieczenia cybernetyczne, ponieważ tylko w ten sposób można zapewnić pełne stosowanie zabezpieczeń. Kompleksowe podejście do cyberbezpieczeństwa pomaga przedsiębiorstwom i rządcom:

- **Zapobiegaj cyberatakam**, wdrażając zabezpieczenia cybernetyczne w każdym aspekcie konstrukcji produktu, aby zmniejszyć obszar podatny na atak
- **Zapewnij ochronę przed cyberatakami**, wdrażając we wszystkich składnikach rozwiązania najnowsze standardy bezpieczeństwa i najlepsze praktyki w celu zwiększenia odporności
- **Reaguj na cyberataki**, podejmując w przypadku wystąpienia ataku szybkie i adekwatne działania w celu ograniczenia skutków i zwiększenia odporności

Aby stwierdzić, czy rozwiązania do zunifikowanej komunikacji i współpracy realizują kompleksowe cyberbezpieczeństwo, należy przeprowadzać oceny rozwiązań w obszarach opisanych poniżej. Skoncentrowanie się na tych obszarach pomoże uzyskać kompleksową ocenę rozwiązań przy jednoczesnym ukierunkowaniu na kluczowe luki w całym krajobrazie cyberzagrożeń.

1 Bezpieczeństwo z założenia

W przeszłości większość projektów rozwiązań wynikała z potrzeby wprowadzenia nowych funkcji, a bezpieczeństwo było kwestią ważną, ale drugorzędną. Wobec zmian krajobrazu tradycyjne priorytety projektowania uległy odwróceniu, a projekty rozwiązań muszą teraz opierać się na wymaganiach dotyczących bezpieczeństwa cybernetycznego.

Rozwiązania sprzętowe i programowe, które z założenia są bezpieczne, uwzględniają bezpieczeństwo na każdym etapie definiowania, opracowywania i dostarczania produktu. Cały sprzęt i systemy operacyjne są wzmacniane, zabezpieczenia typu „odmowa usługi” (DoS) są zintegrowane, a w rozwiązaniach wdrażane są najlepsze praktyki w zakresie cyberbezpieczeństwa, które są dla branży najważniejsze. Na przykład rozwiązanie do zunifikowanej komunikacji i współpracy dla organizacji zajmujących się bezpieczeństwem wewnętrznym ma spełniać bardzo wysokie standardy odporności i poufności, których wymagają te organizacje.

2 Bezpieczeństwo dostępu do sieci dzięki zasadzie zerowego zaufania

Strategie bezpieczeństwa zapewniające zaufanie na podstawie lokalizacji użytkownika w firmowej zaporze ogniowej, wprowadzanych przez niego danych uwierzytliwiających lub używanej aplikacji lub urządzenia już nie wystarczają – nawet w przypadku połączenia wielu mechanizmów bezpieczeństwa. Obecnie żaden użytkownik, urządzenie ani aplikacja nie powinny być darzone zaufaniem dorozumianym.

Rozwiązania do zunifikowanej komunikacji i współpracy, które wdrażają model bezpieczeństwa dostępu do sieci dzięki zasadzie zerowego zaufania (ZTNA), pomagają organizacjom skutecznie przeciwdziałać stale ewoluującym zagrożeniom. Zgodnie z ZTNA, nie udziela się zaufania żadnemu użytkownikowi, urządzeniu ani aplikacji, bez względu na to, gdzie się znajduje. Podejście to opiera się na pięciu kluczowych twierdzeniach:

- Sieć jest wroga
- Zagrożenia zewnętrzne i wewnętrzne są zawsze obecne
- Lokalizacja i tożsamość nie wystarczą, by obdarzyć zaufaniem
- Każde urządzenie, użytkownik i przepływ w sieci muszą zostać uwierzytelnione oraz autoryzowane
- Sieć i zasady bezpieczeństwa muszą być dynamiczne i wykorzystywać jak najwięcej źródeł danych



3 Makro- i mikrosegmentacja

Makro- i mikrosegmentacja umożliwia szczegółowe i wysoce kontrolowane podejście do cyberbezpieczeństwa wszystkich zróżnicowanych użytkowników, urządzeń i aplikacji uzyskujących dostęp do sieci.

Makrosegmentacja polega na segregowaniu użytkowników, urządzeń i aplikacji zgodnie z ich domeną funkcjonalną, aby nie mogli komunikować się z elementami w innych makrosegmentach. Na przykład aplikacje do zunifikowanej komunikacji i współpracy w jednym makrosegmencie nie mogą komunikować się z technologiami bezpieczeństwa, takimi jak kamery CCTV i systemy zamków do drzwi, w drugim makrosegmencie lub z czujnikami i elementami sterującymi oświetleniem, ogrzewaniem i klimatyzacją w trzecim makrosegmencie.

Mikrosegmentacja określa, w jaki sposób użytkownicy, urządzenia i aplikacje w ramach makrosegmentu mogą wchodzić ze sobą w interakcje i zwykle podlega bardzo szczegółowym zasadom bezpieczeństwa. Na przykład kamera monitorująca nie powinna łączyć się z blokadą w drzwiach, mimo że znajdują się one w tym samym makrosegmencie związanym z bezpieczeństwem.

4 Szyfrowanie na całej drodze przesyłu danych

W nowoczesnych organizacjach pracownicy, klienci, partnerzy i dostawcy mogą znajdować się w dowolnym miejscu na świecie. Z kolei rozwiązania, których używają do komunikacji i współpracy, mogą być zainstalowane w budynku, w którym pracują, po drugiej stronie miasta lub w centrum danych na drugiej półkuli. W każdym przypadku ludzie muszą mieć możliwość bezpiecznej i poufnej wymiany informacji za pomocą głosu, wideo i tekstu.

Aby mieć pewność, że tylko uczestnicy rozmowy mają dostęp do wymienianych informacji, każda rozmowa musi być w pełni zaszyfrowana od źródła do miejsca docelowego. Oznacza to, że każdy element sprzętu i oprogramowania biorący udział w komunikacji typu „end to end” musi mieć wbudowane mechanizmy szyfrowania zatwierdzone przez agencje bezpieczeństwa.

5 Certyfikaty i akredytacje dotyczące bezpieczeństwa i prywatności

Zaledwie kilka lat temu najbardziej rygorystyczne certyfikaty i akredytacje bezpieczeństwa były wymagane tylko w przypadku produktów zabezpieczających, takich jak zapory ogniowe, lub w określonych branżach, takich jak wojskowość. Obecnie standardy bezpieczeństwa muszą być stosowane do wszystkich produktów technologicznych we wszystkich branżach.

Niezwykle ważne jest sprawdzanie, czy deklaracje dotyczące bezpieczeństwa cybernetycznego są poparte uznanymi certyfikatami i akredytacjami. Oto kilka przykładów zgodności, których należy szukać:

- **Globalne standardy bezpieczeństwa i prywatności**, takie jak norma ISO 27001 dotycząca bezpieczeństwa informacji, norma ISO 27017 dotycząca bezpieczeństwa środowisk opartych na chmurze, norma ISO 27018 dotycząca ochrony danych osobowych w środowiskach opartych na chmurze oraz Wspólne kryteria oceny poziomu zabezpieczeń (EAL) 2 i nowsze dotyczące bezpieczeństwa systemu komputerowego
- **Specyficzne dla branży standardy bezpieczeństwa i prywatności**, takie jak ustawa Health Insurance Portability and Accountability Act (HIPAA) w Stanach Zjednoczonych oraz HÉbergeurs de Données de Santé (HDS) dotycząca hostingu danych zdrowotnych we Francji
- **Regionalne standardy bezpieczeństwa i prywatności**, takie jak rozporządzenie o ochronie danych osobowych (RODO) w Unii Europejskiej

6 Prowadzone w sposób ciągły specjalistyczne testy bezpieczeństwa

Podobnie jak standardy bezpieczeństwa, wyspecjalizowane procesy testowania zabezpieczeń, które kiedyś były zarezerwowane dla produktów zabezpieczających, są teraz obowiązkowe w rozwiązaniach do zunifikowanej komunikacji i współpracy.

Doskonałym przykładem są testy penetracyjne. Testy te symulują cyberataki w celu ujawnienia luk w zabezpieczeniach, dzięki czemu można je proaktywnie usunąć, zanim pojawią się problemy. Aby być o krok przed cyberzagrożeniami w ciągle zmieniającym się środowisku, testy penetracyjne, które są oparte wyłącznie na wymaganiach bezpieczeństwa cybernetycznego, muszą być przeprowadzane na bieżąco.

Dostawcy technologii, którzy pomagają swoim klientom w utrzymaniu maksymalnego bezpieczeństwa cybernetycznego, muszą zapewnić zasoby, narzędzia i wiedzę niezbędną do przeprowadzania ciągłych testów penetracyjnych.



Osiągaj cele biznesowe przy mniejszym ryzyku

Rozwiązania do zunifikowanej komunikacji współpracy, które wdrażają pełny zakres środków bezpieczeństwa cybernetycznego opisanych w poprzedniej sekcji, zapewniają przedsiębiorstwom i organizacjom rządowym swobodę i elastyczność w prowadzeniu działań przy jednoczesnym minimalizowaniu ryzyka i zapewnianiu zgodności. Stwarza to następujące możliwości:

- **Umożliwienie pracownikom** bezpiecznej i poufnej współpracy oraz udostępniania informacji przy użyciu dowolnych mediów i urządzeń w dowolnej lokalizacji
- **Poprawa jakości obsługi klienta** dzięki wzbogaconej, bogatej w informacje i atrakcyjnej komunikacji, szybszemu podejmowaniu decyzji, zautomatyzowanym procesom biznesowym oraz możliwości proaktywnego wykrywania problemów, zanim wpłyną one na klienta
- **Większa doskonałość i sprawność operacyjna** dzięki infrastrukturze cyfrowej, która jest wdrażana tam, gdzie ma to największy sens dla organizacji – lokalnie lub w chmurze hybrydowej, prywatnej lub publicznej – przy jednoczesnym przestrzeganiu surowych zasad ochrony danych i zapewnieniu zgodności z przepisami dotyczącymi prywatności

Poniższe przykłady przedstawiają tylko kilka pojawiających się możliwości, które można je łatwo dostosować do innych wymagań i branż.

Stwórz elastyczne, cyfrowe miejsce pracy, aby upodmiotowić pracowników

Dzięki odpowiedniemu połączeniu bezpiecznych rozwiązań do komunikacji i współpracy pracownicy mogą pracować szybciej i bardziej elastycznie, zachowując pełną zgodność z przepisami branżowymi.

- **W opiece zdrowotnej** bardzo mobilni pracownicy mogą współpracować i udostępniać informacje, zachowując pełną zgodność ze standardami bezpieczeństwa danych. Pracownicy mogą łatwo wymieniać się aktualizacjami i szybko uzyskiwać potrzebną pomoc. Personel medyczny może korzystać z bezpiecznej komunikacji w czasie rzeczywistym w celu poprawy wyników leczenia pacjentów i wydajności pracy. Personel niemedyczny może przyspieszyć procesy i reakcje na problemy konserwacyjne, które mogą mieć wpływ na bezpieczeństwo pacjentów i personelu.
- **W dziedzinie edukacji** nauczyciele mogą oferować bogatsze i ciekawsze metody nauki zdalnej, dając uczniom więcej możliwości uczestniczenia w zajęciach, współpracy przy projektach i interakcji przy użyciu preferowanego medium. Kompleksowa kontrola dostępu i zautomatyzowane zasady zapewniają integralność danych, a funkcje analityczne nadają priorytet komunikacji i zasobom sieciowym o krytycznym znaczeniu.
- **W organizacjach rządowych** pracownicy mogą bezpiecznie wymieniać informacje w zespołach rozproszonych. Mogą udostępniać ekrany, zdalnie sterować pulpitem innej osoby i wymieniać duże pliki, aby usprawnić współpracę. Mogą też bezpiecznie wchodzić w interakcje z obywatelami za pośrednictwem aplikacji internetowych lub mobilnych za pomocą głosu, wideo, czatu lub komunikatorów.
- **W transporcie** cyfrowe miejsce pracy umożliwia pracownikom korzystanie z własnych urządzeń podczas pracy, wprowadzanie wydajniejszych procesów i zapewnianie pasażerom ulepszonych usług, takich jak możliwość do pracy podczas podróży. Bezpieczne protokoły komunikacyjne, wzmocnione instalacje i zróżnicowany kod chronią dane w całej sieci.

Opracowanie techniczne

Zabezpieczenie rozwiązań do zunifikowanej komunikacji i współpracy

Połącz wszystko, aby poprawić jakość obsługi klienta

Bezpieczne łączenie ludzi, obiektów i aplikacji za pomocą komunikacji w czasie rzeczywistym umożliwia przedsiębiorstwom i organizacjom rządowym:

- Dostarczenie pracownikom urządzeń, technologii i danych, których potrzebują, aby lepiej obsługiwać klientów, jednocześnie minimalizując ryzyko, że błąd ludzki lub brak świadomości zagrazi bezpieczeństwu
- Korzystanie ze zintegrowanych, bezpiecznych urządzeń do komunikowania się i współpracy z klientami w ruchu dzięki pełnemu dostępowi do rozwiązań do zarządzania relacjami z klientami (CRM)
- Podniesienie poziomu ochrony, kontroli i widoczności szybko rozwijającej się i zróżnicowanej gamy urządzeń Internetu przedmiotów (IoT).
- Aktualizowanie systemów komunikacji i współpracy w celu uniknięcia ryzyka, że przestarzałe aplikacje zwiększą powierzchnię ataku i ujawnią luki w zabezpieczeniach
- Wdrożenie skutecznej kontroli dostępu i kompleksowe szyfrowanie na wszystkich platformach

Ujednolicone zarządzanie siecią umożliwia całościowe zarządzanie wszystkimi platformami komunikacyjnymi, aplikacjami i urządzeniami IoT. Ujednolicone zarządzanie siecią:

- Upraszcza zarządzanie sieciami przewodowymi i bezprzewodowymi oraz urządzeniami IoT w celu obniżenia kosztów zarządzania siecią, optymalizacji wydajności sieci i zwiększenia wydajności operacyjnej
- Przyspiesza rozwiązywanie problemów w coraz bardziej zróżnicowanych środowiskach technologicznych, aby zmniejszyć ryzyko przerw w świadczeniu usług i przestojów

Ujednolicone zarządzanie siecią w różnych branżach zapewnia cały szereg korzyści. Na przykład:

W opiece zdrowotnej rozwiązania IoT mogą śledzić lokalizację sprzętu o znaczeniu krytycznym, takiego jak butle z tlenem, wózki ratunkowe, monitory pacjenta, stojaki do kroplówek i wózki inwalidzkie, aby poprawić bezpieczeństwo i wydajność. Połączenia między ludźmi, przedmiotami i aplikacjami mogą być również wykorzystywane do wyzwalania alarmów, które informują personel medyczny o potrzebach pacjentów lub awariach sprzętu i mogą ostrzegać wszystkich w placówce o niebezpiecznych sytuacjach.

W edukacji powstaje nowy potencjał łączenia inteligentnych urządzeń kampusowych i aplikacji z wieloma warstwami zabezpieczeń w celu ochrony zasobów instytucji przed niedostatecznie zabezpieczonymi urządzeniami uzyskującymi dostęp do sieci. Instytucje edukacyjne mogą również korzystać z odcisków palców urządzeń IoT do identyfikowania ich cech, takich jak typ, producent, model i system operacyjny, aby uprościć przyspieszyć konfigurację sieci IoT i wdrażanie urządzeń.



Zwiększ doskonałość i sprawność operacyjną

Dzięki elastyczności umożliwiającej bezpieczne wdrażanie ujednoliconej komunikacji i rozwiązań do współpracy lokalnie lub w chmurze hybrydowej, prywatnej lub publicznej, przedsiębiorstwa i organizacje rządowe mogą korzystać z technologii cyfrowych w sposób najbardziej zgodny z ich celami i zadaniami. Każda organizacja może osiągnąć nowy poziom doskonałości operacyjnej i jednocześnie spełnić specyficzne wymagania branżowe, przyjmując modele chmurowe zwiększające doskonałość operacyjną i sprawność, np. w następujących dziedzinach:

- **Opieka zdrowotna:** dane cyfrowe można wykorzystać do poprawy opieki nad pacjentem i zwiększenia wydajności przy zachowaniu całkowitej pewności, że dane osobowe są przechowywane w bezpiecznym i certyfikowanym centrum danych w chmurze
- **Edukacja:** wykładowcy, pracownicy i studenci mają bezpieczny, szanujący prywatność dostęp do aplikacji i usług w chmurze z dowolnego miejsca. Zarazem działy IT mogą skrócić czas i obniżyć koszty związane z wdrażaniem, obsługą i aktualizacją szerokiej gamy aplikacji.
- **Instytucje rządowe:** poufną komunikację można obsługiwać z wysoką dostępnością i chronić za pomocą wbudowanych mechanizmów DoS oraz sprzętu i systemów operacyjnych o zwiększonych zabezpieczeniach
- **Transport:** zmiana możliwości komunikacji może prowadzić do niebezpiecznych sytuacji, dlatego niezbędne są odporne i niezależne od danych rozwiązania

Opracowanie techniczne

Zabezpieczenie rozwiązań do zunifikowanej komunikacji i współpracy

Cyberbezpieczeństwo: nieodłączna część sposobu myślenia dostawcy technologii

Chociaż wielu dostawców technologii kładzie nacisk na bezpieczeństwo cybernetyczne, nie wszyscy mają wszechstronną wiedzę specjalistyczną w zakresie wdrażania kompleksowych zabezpieczeń.

Alcatel-Lucent Enterprise znacznie wyprzedza innych dostawców, wdrażając wszystkie najlepsze praktyki wymagane dla kompleksowego bezpieczeństwa cybernetycznego. Oto zasady, którymi się kierujemy:

- Postępujemy zgodnie z najlepszymi praktykami i zaleceniami Narodowego Instytutu Nauki i Technologii (NIST) podczas przeprowadzania w naszych rozwiązaniach oceny ryzyka nowych funkcji i wdrażania funkcji cyberbezpieczeństwa, takich jak natywne szyfrowanie
- Posiadamy certyfikat Common Criteria EAL2
- Stosujemy normy ISO 27001 do wszystkich naszych rozwiązań opartych na chmurze
- Stosujemy ZTNA, szczegółową segmentację sieci i bardzo szczegółowe zasady bezpieczeństwa, aby zmniejszyć ryzyko nieautoryzowanych działań
- Przeprowadzamy wysoce specjalistyczne testy bezpieczeństwa, takie jak testy penetracyjne, na wszystkich naszych produktach
- Dbamy o to, by nasze produkty posiadały kluczowe certyfikaty branżowe, takie jak HDS, HIPAA oraz ustawa Family Educational Rights and Privacy Act (FERPA), jako Rainbow by Alcatel-Lucent Enterprise

Jako uznani eksperci ds. cyberbezpieczeństwa mamy wkład w propozycje Unii Europejskiej dotyczące dyrektyw w sprawie cyberbezpieczeństwa. Wykorzystujemy również naszą wiedzę, aby pomóc naszym klientom wybrać i wdrożyć odpowiednią kombinację bezpiecznych rozwiązań do zunifikowanej komunikacji i współpracy, a także szkolić ich pracowników w zakresie najlepszych praktyk w dziedzinie bezpieczeństwa cybernetycznego.

Dowiedz się więcej

Aby dowiedzieć się, jak możemy pomóc Twojej organizacji w pełnym wykorzystaniu bezpiecznych rozwiązań komunikacyjnych ery cyfrowej, [odwiedź naszą witrynę internetową](#) lub [skontaktuj się z nami już dziś](#).

Alcatel-Lucent Enterprise cieszy się zaufaniem na całym świecie

Wiodące organizacje w różnych branżach stosują nasze bezpieczne rozwiązania komunikacyjne ery cyfrowej, aby osiągnąć swoje cele. Są wśród nich:

- [Metropolis i miasto Perpignan](#) we Francji, gdzie urzędnicy rządowi wdrażają strategiczny plan transformacji cyfrowej, obejmujący wideokonferencje i komunikację głosową dla pracowników, obsługę aplikacji IoT oraz nowe treści i usługi dla mieszkańców Perpignan, turystów i pracowników organów miejskich.
- [Uniwersytet Newmana](#) w Stanach Zjednoczonych to katolicka uczelnia, która dostarczyła pracownikom funkcje telefonów komórkowych niewymagające używania bezpośrednich numerów telefonów, a zespołowi IT – jedną, intuicyjną platformę opartą na chmurze przeznaczoną do zarządzania, udostępniania i monitorowania całej infrastruktury sieciowej.
- [Szpital Kingsway Hospitals](#) w Indiach wdrożył rozwiązania w zakresie infrastruktury komunikacyjnej w czasie rzeczywistym, które zapewniają łączność personelowi klinicznemu i administracyjnemu, dzięki czemu można optymalizować opiekę nad pacjentami i zwiększać ich komfort.
- [Grupa J. Malucelli](#) w Brazylii zmodernizowała swoją sieć za pomocą konwergentnego rozwiązania głosowego i do transmisji danych, które obejmuje telefonię w chmurze, a także sieci LAN i Wi-Fi zarządzane w chmurze, aby uprościć i obniżyć koszty komunikacji dla kilku firm należących do grupy.

