



Względy IT dotyczące projektowania systemu wideo IP

Dziewięć kluczowych problemów IT podczas projektowania systemu wideo IP

Spis treści

Wprowadzenie	3
1. Rola wiedzy IT w systemach wideo	4
2. Dopasowanie sprzętu do potrzeb nadzoru wideo	5
3. Kluczowa rola networkingu	6
4. Podkreślanie wartości ponad cenę	7
5. Zagrożenia i rozwiązania dotyczące cyberbezpieczeństwa	7
6. Ograniczenia podejścia „izolowanego”	8
7. Zapewnienie braku utraty danych wideo	9
8. Zarządzanie cyklami życia w systemach nadzoru IP	10
9. Ekosystem IT w systemach wideo	10

Firma Alcatel-Lucent Enterprise zleciła firmie SourceSecurity.com sporządzenie tego dokumentu.



Wprowadzenie

System nadzoru wideo ma specjalne potrzeby w zakresie technologii informatycznych (IT). Chociaż cyfrowy system wideo może wykorzystywać te same technologie, co inne systemy informatyczne, są one konfigurowane inaczej i uwzględniają specyficzne potrzeby nadzoru wideo.

Wideo jest bardziej wymagającym środowiskiem i powoduje większe obciążenie każdej części systemu informatycznego. Ze względu na stres, zwłaszcza w przypadku większego systemu korporacyjnego, wszystko może zacząć się psuć. Wybór odpowiedniego sprzętu do konkretnego zadania zapewnia większą niezawodność w czasie.

Firma Alcatel-Lucent Enterprise współpracowała z ekspertami branżowymi SourceSecurity.com i Stone Security, aby zidentyfikować dziewięć kluczowych problemów informatycznych występujących podczas projektowania systemów wideo IP. W niniejszym opracowaniu technicznym badamy, w jaki sposób wyspecjalizowane potrzeby systemu nadzoru wideo wpływają na wdrażanie technologii informatycznych i sposób ich wykorzystania.

Opracowanie techniczne

Względy IT dotyczące projektowania systemu wideo IP



1. Rola wiedzy informatycznej w systemach wizyjnych

Projektowanie i tworzenie systemu monitoringu wizyjnego opartego na protokole internetowym (IP) wymaga wysokiego poziomu wiedzy informatycznej w społeczności integratorów.

Niektórzy integratorzy mają wystarczające umiejętności, aby fachowo uruchomić system wideo IP, inni mogą mieć z tym trudności.

Dodatkowe szkolenia i certyfikaty znane większości osób w świecie IT mogą umożliwić integratorom świadczenie wymaganego wysokiego poziomu usług. Na początek instalatorzy muszą posiadać odpowiednie umiejętności i podstawową wiedzę na temat sieci i umiejętności rozwiązywania problemów.

Integratorzy mogą zapewnić wykwalifikowaną siłę roboczą, ograniczając wybór technologii i upewniając się, że każdy pracownik jest dobrze przeszkolony w zakresie mniejszej liczby technologii. Wybór najlepszych w swojej klasie rozwiązań i zapewnienie, że pracownicy są ekspertami w tych produktach, pozwala integratorowi dostarczać klientom system wyższej klasy.

Ograniczenie asortymentu produktów umożliwia także integratorowi lepsze zrozumienie zakresu funkcji oferowanych przez dany produkt. Zbyt często klient kupuje system oferujący szeroki zakres funkcji, a następnie wykorzystuje w codziennej pracy jedynie ograniczoną ich liczbę, podważając w ten sposób wartość systemu, za który zapłacił.

Integratorzy mogą pomóc klientom, ucząc ich, jak odblokować pełną wartość niezależnie od zakupionego systemu.

Integratorzy mogą również polegać na usługach doradztwa wstępnego producentów sprzętu. W niektórych przypadkach producenci sprzętu posiadają szczególną wiedzę na temat różnych rynków pionowych, zgromadzoną w trakcie ich obsługi.

Producenci, którzy poważnie podchodzą do konkretnego rynku pionowego, zatrudnią ekspertów branżowych, aby zapewnić wsparcie dostosowane do potrzeb każdego klienta. Ich wskazówki mogą pomóc integratorom odnieść sukces na nowych rynkach i/lub usprawnić najlepsze praktyki na rynkach, na których działają.

Producenci zapewniają również szkolenia i certyfikaty, aby zapewnić integratorom dobre wyposażenie do instalowania ich systemów. Skuteczne i merytoryczne szkolenie powinno być prezentowane w krótszych sesjach, w których szanowany jest czas każdego uczestnika.

2. Dostosowanie sprzętu do potrzeb nadzoru wideo

Kwestie takie jak wymagania dotyczące przepustowości i zasilania przez Ethernet (PoE) są ważnymi zmiennymi w systemie wideo. A serwer wideo ma większe obciążenie, szczególnie jeśli chodzi o wideo z transmisji na żywo. Każdy fragment danych łąduje na serwerze, nawet te, które nie są rejestrowane.

Obraz wideo jest buforowany, co gwarantuje, że przed faktycznym nagraniem wideo wywołującym alarm może zostać zachowane co najmniej kilka sekund materiału wideo. Dłuższe okresy buforowania mogą być konieczne w przypadku identyfikacji obrazu pochodzącego z większej odległości. Wszystkie wejścia i wyjścia przechodzą przez serwer, mimo że ograniczona ilość danych zostanie zapisana w pamięci długoterminowej.

Istnieje zasadnicza różnica pomiędzy tym, jak integratorzy systemów bezpieczeństwa postrzegają rozmiar systemu, a tym, jak postrzegają go specjaliści IT. Integratorzy systemów częściej mówią o liczbie kamer, natomiast specjaliści IT częściej mówią o zarządzaniu danymi z systemu. Obydwa zjawiska są oczywiście ze sobą nierozdzielnie powiązane, jednak zależność ta nie jest liniowa. Ogólnie rzecz biorąc, większa liczba kamer oznacza więcej danych, którymi musi zarządzać dział IT. Istnieją jednak inne czynniki wpływające na zapotrzebowanie na dane, takie jak liczba klatek, wymagania dotyczące jakości obrazu, potrzeby w zakresie przechowywania, aplikacje działające w trybie dziennym/nocnym i wykorzystanie analityki wideo.

Kluczową umiejętnością przy określaniu systemu bezpieczeństwa IP jest przełożenie wymagań sprzętowych i funkcjonalnych systemu na dane niezbędne do zaspokojenia tych potrzeb. W przypadku systemu lokalnego oznacza to konieczność określenia serwera komputerowego, który maksymalizuje wydajność systemu przy jednoczesnym obniżeniu kosztów. Kwestie takie, jak wirtualizacja i systemy chmurowe mogą zarówno skomplikować równanie, jak i zapewnić nową elastyczność.

Kolejną zmienną związaną z konstrukcją systemu jest wykorzystanie kamer na obrzeżach sieci do nagrywania wideo za pomocą kart SD. Obecnie istnieją nawet systemy „bezserwerowe”; na przykład całe nagrywanie odbywa się na obrzeżach. W efekcie takie podejście przenosi obciążenie obliczeniowe z serwera na obrzeże, co powoduje zmniejszenie zapotrzebowania na pojemność serwera. Dzisiejsze kamery dostarczają dane wykraczające poza strumień wideo, takie jak metadane i dźwięk, które również wpływają na projekt systemu.

Specjaliści IT powinni mieć dokładny ogląd całego systemu, np. tego, co będzie podłączone, liczby klatek na sekundę, rozdzielczości i kodeków wideo kamer. Dzięki tym informacjom mogą obliczyć wymagania dotyczące sieci, zasilania, serwerów, pojemności dysku, pamięci i pamięci masowej oraz określić, czy korzystać z systemów chmurowych czy lokalnych. Zapewnia to dokładne i przemyślane podejście do projektowania oraz wdrażania.

Producenci dostarczają „kalkulatory” oprogramowania, które pomagają integratorom projektować systemy poprzez przełożenie wymagań systemowych na specyfikacje konkretnego sprzętu. Należy pamiętać, że obliczenia powinny spełniać lub przekraczać oczekiwania i umożliwiać przyszły rozwój.

Wdrożenie systemów chmurowych to kolejna zmienna, jeśli chodzi o projektowanie systemów nadzoru wideo. Wyraźną tendencją jest wykorzystywanie większej liczby systemów chmurowych do nadzoru wideo. Jednak wyboru rozwiązań chmurowych czy lokalnych należy dokonywać indywidualnie do każdego przypadku. Projektanci systemów i użytkownicy końcowi powinni oprzeć się pozornej nieuchronności chmury i raczej podejmować decyzje w oparciu o potrzeby klienta.

Wielu producentów znajduje się pod presją przeniesienia swoich systemów do chmury, ale w idealnym przypadku powinni zapewnić swoim klientom wybór systemów, a nie rozwiązanie uniwersalne.

Producenci mogą doradzać klientom, czy preferowana jest konfiguracja w chmurze w porównaniu z projektem lokalnym. Integratorzy powinni także być dobrze zaznajomieni z zaletami obu podejść lub ułatwiać klientowi podjęcie decyzji w obu przypadkach. Rynek nie powinien wypychać aplikacji do chmury, chyba że jest to optymalne podejście dla każdego indywidualnego klienta.

3. Kluczowa rola networkingu

System wideo jest tak mocny, jak jego najsłabsze ogniwo. Switche sieciowe mogą nie być tak widoczne, jak kamery i systemy VMS, ale są nie mniej istotne.

Zwykle jednak zdarza się, że klienci traktują działanie sieci jako coś oczywistego, nie zwracając uwagi na to, jak ona działa i jak zmaksymalizować jej użyteczność. W rzeczywistości niektórzy klienci chcą zainstalować system wideo, korzystając z istniejącej infrastruktury sieciowej. Jest to możliwe, ale dostępność optymalizacji elementu sieciowego systemu wideo może być ograniczona.

Idealnie byłoby, gdyby klient zdecydował się na najlepsze switchy do monitoringu wideo, które zapewnią systemowi niezawodne i efektywne działanie.

Każdy system wideo jest inny, dlatego zwrócenie szczególnej uwagi na jego zindywidualizowane wymagania gwarantuje realizację jego wyjątkowej misji. Podczas uruchamiania systemu nie należy myśleć o sieci jako coś do przemyślenia później. Powinien raczej zostać starannie zmontowany przy użyciu najlepszych komponentów, aby umożliwić i usprawnić działanie w całym systemie.

Switchy działające z „prędkością okablowania”, co oznacza, że mają wystarczającą moc obliczeniową, aby obsłużyć pełną prędkość Ethernetu przy minimalnych rozmiarach pakietów, są obecnie standardem w branży. Nowym punktem różnicującym switchy jest możliwość zrozumienia i zarządzania ruchem.

Switchy niezarządzalne są dostępne na rynku, ale zazwyczaj nie są używane w zastosowaniach komercyjnych i/lub korporacyjnych. Są przeznaczone do stosowania w małych sieciach o podstawowych potrzebach; nie ma żadnych ustawień do skonfigurowania.

Z drugiej strony switchy zarządzane umożliwiają wykrywanie i diagnozowanie problemów z wydajnością oraz zapewniają niezawodne działanie systemów nadzoru wideo. Umożliwiają użytkownikom szczegółowe sprawdzenie, co może być przyczyną problemów w systemie i pozwalają zrozumieć, jak wyglądają te informacje.

Wartość zarządzanych switchów, które są w pełni konfigurowalne, dostosowywalne i dostarczają szeregu danych na temat wydajności, stanie się oczywista w trakcie eksploatacji systemu, zapewniając ważny wgląd w działanie systemu i umożliwiając łatwiejsze rozwiązywanie problemów w celu zidentyfikowania problemów.

Switchy powinny być zaprojektowane tak, aby spełniać potrzeby systemów wideo IP. Przykładem w przypadku switcha 16-portowego jest budżet mocy wystarczający do obsługi wszystkich kamer wideo podłączonych do niego. Dzisiejsze kamery PoE pobierają więcej energii niż poprzednie generacje. Integratorzy muszą wiedzieć, że switch zapewnia moc wystarczającą do obsługi liczby kamer i przyszłego rozwoju.

„Dokonując wyboru sprzętu, chcemy, aby każdy switch miał odpowiednią przepustowość, budżet mocy i był switchem zarządzanym, który oszczędza nam ogromną ilość czasu podczas rozwiązywania problemów. Oszczędzają nam pieniądze i pieniądze naszych klientów. Jest to większa inwestycja z góry, ale zwróci się na dłuższą metę, tworząc system bardziej serwisowany”.

Aaron H. Simpson, prezes i dyrektor ds. technologii w firmie Stone Security

4. Przedkładanie wartości nad cenę

Niezawodność ma kluczowe znaczenie w monitoringu wideo i zaczyna się od wyboru sprzętu.

Określanie komponentów o niższej jakości może wydawać się wówczas koniecznością ekonomiczną. Jednak na dłuższą metę działanie systemu będzie ucierpieć. Koszt wyboru mniej niż optymalnego działania może nie być oczywisty podczas projektowania systemu, ale z biegiem czasu stanie się wyraźnie widoczny.

Z drugiej strony wybór lepszego sprzętu – nawet jeśli będzie droższy – się opłaci.

Niezwykle istotne jest porównanie kosztów (takich jak cena lepszego sprzętu) z ryzykiem nieadekwatności lub awarii systemu. Najlepszą strategią jest przyjęcie podejścia opartego na całkowitym koszcie posiadania (TCO). Kolejnym elementem kosztów długoterminowych, który należy wziąć pod uwagę, jest wartość systemów otwartych, które mogą zapewnić elastyczność podczas rozbudowy lub zmiany systemu w przyszłości.

Zawsze najlepiej jest współpracować z dostawcą, który oferuje produkt, do którego ma zaufanie i który może wspierać przez długi czas.

5. Zagrożenia i poprawki cyberbezpieczeństwa

Historycznie rzecz biorąc, ironią losu w branży bezpieczeństwa fizycznego był brak uwagi na cyberbezpieczeństwo systemów IP.

Na szczęście zainteresowane strony zajmujące się bezpieczeństwem fizycznym zwracają obecnie większą uwagę na kwestie cyberbezpieczeństwa na każdym poziomie i w całym łańcuchu dostaw bezpieczeństwa fizycznego. W rzeczywistości cyberbezpieczeństwo stało się jednym z kluczowych filarów procesu decyzyjnego w przypadku większych systemów bezpieczeństwa wideo.

Minimalnym krokiem w kierunku ochrony przed cyberzagrożeniami i ograniczenia dostępu do systemu jest unikanie używania domyślnych haseł. Są one mniej bezpieczne i haker lub bot mogą je łatwiej odgadnąć. Domyślne hasła zostały w Kalifornii wręcz zakazane.

Zagrożenia cyberbezpieczeństwa zaczynają się w łańcuchu dostaw, gdzie ataki mogą zagrozić produktowi, zanim jeszcze zostanie dostarczony. Analiza produktu pod kątem możliwych ataków typu „backdoor” lub „przepełnienie bufora” przed dostawą może złagodzić zagrożenie. Klienci mogą również zdecydować się na wirtualną instalację „dobrego kodu” po dostarczeniu sprzętu, zapewniając w ten sposób cyberbezpieczeństwo i zastępując wszelki złośliwy kod, który mógł zostać zainstalowany podczas wysyłki.

Istnieje również szereg środków cyberbezpieczeństwa, które należy uwzględnić podczas instalacji i na różnych etapach wdrażania systemu. Na przykład „wyuczone bezpieczeństwo portu” gwarantuje, że dostęp do portu będzie miało jedynie autoryzowane urządzenie. Jeśli nieautoryzowane urządzenie spróbuje połączyć się z systemem — na przykład w celu podłączenia nowej kamery — zostanie wygenerowany alert i dostęp do portu zostanie zablokowany do czasu autoryzacji przez człowieka.

Technologia mostkowania najkrótszej ścieżki (SPB) może zapobiegać przeskakiwaniu szkodliwych działań z jednego systemu do drugiego. Reguły są skonfigurowane w taki sposób, że kamera może przesyłać strumieniowo tylko do rejestratora, a w sieciach multi-IoT wdrażana jest inna zaawansowana technologia segmentacji.

Systemy powinny wyłączać niepewne protokoły, takie jak FTP i Telnet, które ułatwiają komunikację w sieci, ale mogą zapewnić hakerom dodatkowe możliwości. Funkcje te powinny być „domyślnie bezpieczne”, aby nie umożliwiać połączenia z siecią, jeśli nie jest to zamierzone.

Skuteczne cyberbezpieczeństwo wymaga również ograniczenia fizycznego dostępu do systemu. Jeśli switch zostanie umieszczony w składziku z mopem, do której wszyscy mają dostęp fizyczny, oznacza to, że nie będzie on dobrze chroniony. Umożliwienie fizycznego dostępu do systemu ułatwia każdemu — w tym pracownikowi stwarzającemu zagrożenie wewnętrzne — podłączenie laptopa i uzyskanie dostępu do całego systemu.

Kamery powinny rejestrować dostęp do sprzętu sieciowego w ramach podejścia „dogłębnej ochrony”.



6. Ograniczenia podejścia „izolowanego”

Jeśli chodzi o ochronę systemów wideo przed atakami cybernetycznymi za pośrednictwem Internetu, historycznie powszechnym podejściem było tworzenie systemów izolowanych.

System izolowany polega na izolowaniu komputera lub sieci i uniemożliwianiu mu nawiązania połączenia zewnętrznego. Ponieważ komputer izolowany jest fizycznie oddzielony i nie można go połączyć bezprzewodowo ani fizycznie z innymi komputerami lub urządzeniami sieciowymi, podejście to jest postrzegane jako panaceum na zapewnienie cyberbezpieczeństwa systemu wideo.

Poleganie na izolacji jako jedynej ochronie cyberbezpieczeństwa jest ryzykowną propozycją. Istnieje wiele różnych sytuacji, w których izolowany system może być narażony na dostęp do Internetu nawet przez krótki czas. Kiedy tak się dzieje, system polega na wszelkich innych środkach cyberbezpieczeństwa – jeśli takie istnieją – aby chronić go przed katastrofą.

Założenie, że system będzie na zawsze zamknięty w izolacji, nie jest rozwiązaniem z punktu widzenia cyberbezpieczeństwa. Tu aż prosi się o katastrofę.

Systemy typu izolowanego nie są również w stanie korzystać ze sztucznej inteligencji (AI) i innych funkcji, które zależą od dostępu wielu użytkowników i analizowania wspólnych doświadczeń. Dane od jednego klienta nie są tak przydatne, jak dane od setek klientów dostępne w chmurze. Systemy izolowane nie pozwalają klientom wykorzystać dodatkowej wartości inteligentniejszych analiz. Rezygnacja z części danych (co wiąże się ze względami prywatności) to cena, jaką płać klienci, aby wykorzystać większą wartość.

Biorąc pod uwagę dzisiejsze wymagania klientów dotyczące łączenia się i ciągłego dostępu do swoich systemów, zastosowanie izolowanych systemów staje się coraz bardziej ograniczone.

Organizacje mają również tendencję do odrzucania perspektywy stworzenia całkowicie oddzielnej infrastruktury sieciowej do nadzoru wideo. Nie ma czegoś takiego jak „oddzielna, bezpieczna” sieć.

7. Zapewnienie braku utraty danych wideo

Utrata danych to problem każdego systemu informatycznego, ale w większym stopniu dotyczy to systemów informatycznych zapewniających nadzór wideo. System nadzoru wideo ma krytyczne znaczenie i musi działać 24 godziny na dobę, 7 dni w tygodniu. Nie ma przestojów, co pozwala administratorom diagnozować i rozwiązywać problemy związane z utratą danych; raczej problemy należy rozwiązywać stale i w czasie rzeczywistym.

W tym miejscu pomocne mogą być switche zarządzane. Umożliwiają one administratorom systemu szybkie diagnozowanie i rozwiązywanie wszelkich problemów związanych z utratą danych. Mogą również łatwo zidentyfikować źródła utraty danych. Nie ma możliwości wskazania palcem, który element systemu jest uszkodzony.

Pakiety mogą być odrzucane z powodu konwersji danych z transmisji światłowodowej do sieci miedzianej i Ethernet. Przekazniki elektryczne służą do translacji danych z transmisji światłowodowej na transmisję elektryczną, a urządzenia te mogą być źródłem utraconych pakietów danych.

W monitoringu wideo utracony pakiet danych jest równoznaczny z naruszeniem obrazu wideo, co w efekcie powoduje jego utratę na zawsze. Nie ma możliwości przywrócenia obrazów wideo utraconych podczas przestojów. Rozważmy na przykład aplikację kasyna, w której konsekwencją awarii systemu wideo jest utrata wizji stołu do gry, co z kolei może oznaczać również utratę przychodów.

W szerokiej gamie zastosowań nadzoru wideo wymagana jest redundancja, aby zapewnić ciągłą pracę 24 godziny na dobę, 7 dni w tygodniu.

Potrzebę niezawodności należy rozważyć w kontekście ryzyka i korzyści. System może być tańszy, mniej złożony i/lub mniej odporny na awarie, ale może nie działać zgodnie z oczekiwaniami, co ma swoje własne koszty.

Inna zmienna, która może powodować problemy z wydajnością w systemach wideo, dotyczy rozróżnienia między emisjami pojedynczymi (unicast) i wielokrotnymi (multicast), które są dwiema metodami przesyłania danych przez sieć. Unicast zapewnia model komunikacji jeden do jednego, w którym pojedynczy nadawca dostarcza dane do jednego odbiorcy. Natomiast multicast jest to model jeden do wielu, w którym jeden nadawca dostarcza dane do kilku odbiorców.

Wiele aplikacji do nadzoru wideo działa w trybie unicast. Oznacza to, że kamera jest monitorowana w czasie rzeczywistym przez jedną osobę — zaangażowany jest jeden strumień wideo.

Jednak niektóre aplikacje wymagają rozwiązania multicast, w którym pojedynczy strumień wideo jest oglądany przez wielu użytkowników. Problemy pojawiają się, gdy system przechodzi z emisji pojedynczej do wielokrotnej. Dokonanie przejścia wymaga czegoś więcej niż tylko „przestawienia switcha”, a niuanse i szczegóły przejścia mogą powodować problemy z wydajnością systemu. Problemy pojawiają się, jeśli części systemu są ustawione na transmisję pojedynczą, podczas gdy powinny być przesyłane w trybie multicast, lub na odwrót. Kluczowa jest właściwa konfiguracja tego punktu w całym systemie.

Funkcje inteligentnego doradcy sieciowego pozwalają użytkownikowi końcowemu zrozumieć, co jest normalne pod względem wydajności sieci, a następnie wykryć, kiedy coś jest nienormalne lub wykracza poza zwykłe oczekiwania. Wszelkie odchylenia są zgłaszane automatycznie, a w razie potrzeby można interweniować w celu rozwiązania problemów.



8. Zarządzanie cyklami życia w systemach monitoringu IP

W świecie IT cykl życia produktu może wynosić od trzech do dziesięciu lat, w zależności od branży i produktu. Istnieją protokoły rozwiązujące problemy, takie jak okres między awariami (MTBF), oprogramowanie sprzętowe i poprawki zabezpieczeń.

W dziedzinie nadzoru wideo cykle życia produktów były w przeszłości dłuższe – w tej dziedzinie nadal sprawdzają się kamery wideo sprzed kilkudziesięciu lat. Dostosowanie strategii zarządzania IT do systemów wideo IP może ujawnić oderwanie od rzeczywistości.

Wsparcie IT zapewniane przez producenta stanowi ogromną wartość dla integratora i użytkownika końcowego. Historycznie rzecz biorąc, dłuższe cykle życia zabezpieczeń fizycznych skutkowały tym, że systemy nadal działały dłużej niż oczekiwany okres i w środowisku nieobsługiwanym.

Dalsze korzystanie ze sprzętu, który nie jest wspierany przez producenta, wiąże się z nieodłącznym ryzykiem. Na przykład brak aktualizacji oprogramowania sprzętowego może otworzyć drzwi do zagrożeń cyberbezpieczeństwa.

Większość dzisiejszego sprzętu ma pięcioletnią gwarancję i – realistycznie rzecz biorąc – mogłaby działać kolejne pięć lat. Jednak w obliczu szybko zmieniającego się krajobrazu technologicznego większość klientów będzie chciała skorzystać z najbardziej aktualnych możliwości. W efekcie przyspieszenie technologii oznacza krótsze cykle życia zabezpieczeń, podobnie jak ma to miejsce w szerszym środowisku informatycznym i sieciowym.

9. Ekosystem IT w systemach wideo

Ujednolicony ekosystem IT to najlepsze podejście do zapewnienia skutecznego systemu wideo IP. Sukces każdej nowej technologii zależy od wspierającego ją ekosystemu IT. Kwestie takie, jak interoperacyjność sprzętu i oprogramowania zapewniają płynne działanie systemu.

Otwarte standardy zapewniają klientom maksymalną elastyczność obecnie i w przyszłości. Przydatne są także uproszczone oferty. Na przykład firma [Alcatel-Lucent Enterprise](#) ma jeden system operacyjny, który działa z każdym sprzedawanym przez nią przełącznikiem Ethernet.

Aby zapewnić sukces, utrzymuj strategię obejmującą produkty, które „dobrze współgrają” z otoczeniem i innymi produktami w ekosystemie.

Skuteczny ekosystem IT nie powstaje samoistnie. Jest raczej rozwijany przez partnerów branżowych pracujących razem, aby zapewnić sukces. Zasady takie, jak otwartość i interoperacyjność przyczyniają się do rozwoju ekosystemu IT. Sukces zwiększa wydajność każdego komponentu systemu i systemu jako całości.

Dowiedz się więcej o technologii [rozwiązań nadzoru wideo](#) firmy Alcatel-Lucent Enterprise.