

Przełączniki KVM – co to tak naprawdę jest?

Przełącznik KVM (z ang. Keyboard, Video, Mouse – czyli klawiatura, monitor i mysz) eliminuje konieczność używania przy każdym z komputerów, kolejnych kompletów tych urządzeń. Pozwala to zaoszczędzić cenne miejsce na biurku. Przełączniki KVM firmy Avocent umożliwiają profesjonalistom działów IT optymalizację wykorzystania ich zasobów. Poprzez konsolidację dostępu i kontroli do serwerów oraz urządzeń z dostępem szeregowym oferują dostęp do centrów danych z dowolnego miejsca na świecie. Z pojedynczej konsoli administrator ma zdalny dostęp do serwerów i innych urządzeń zarządzanych z zachowaniem poufności sesji.

Rozwiązania Avocent pomagają w systemowych rozwiązaniach korporacyjnych działów IT operowanie w łatwiejszy, efektywniejszy sposób. Umożliwia to w konsekwencji skupienie się działowi technicznemu IT na efektywnym zarządzaniu, oszczędzając jednocześnie miejsce i czas.

Używając rozwiązania Avocenta, pracownicy działu IT mogą w czasie rzeczywistym nadzorować krytyczne urządzenia i serwery z dowolnego miejsca w dowolnym czasie... nawet jeśli serwer uległ awarii, administrator może nadal kontrolować całość pracy serwerowni na pojedynczym ekranie.

Administrator w takiej sytuacji może reagować odpowiedzialnie, niezawodnie i ekonomicznie w zależności od potrzeb zarządzania całą infrastrukturą sieciową w firmie.

Avocent jest firmą, która wytycza kierunki rozwoju w swojej branży. Konsekwentnie prowadzi w inwestycjach

badawczych i rozwojowych technologii wprowadzając coraz to nowe produkty jak seria DS. Przełączniki KVM tej rodziny pozwalają na dostęp i kontrolę do serwerów oraz innych urządzeń krytycznych poprzez połączenia sieciowe IP.

Produkty Avocenta, włączając w to również sprzedawane pod nazwami znanych firm Apex, Cybex i Avocent, są używane od lat przez znane firmy światowe jak Compaq, Dell, IBM, Hewlett Packard, Microsoft, Nortel, Motorola, Nokia, NEC, Siemens i wiele innych.



Pięć powodów, dla których warto używać przełączników KVM Avocent

Skalowalność – Twoja sieć będzie się rozwijać. Wybierz więc przełącznik zaprojektowany tak, by rozwijał się wraz z siecią

W miarę rozwoju sieci – pojawianiem się nowych użytkowników, serwerów i innych urządzeń sieciowych – pojawia się potrzeba posiadania systemu KVM, którego rozbudowa również będzie łatwa.

Podstawowe pytania, które pojawiają się w takich sytuacjach, to: jak często występuje potrzeba powiększenia ilości serwerów bądź obsługiwanych użytkowników? Czy preferowany jest dostęp z wykorzystaniem protokołu TCP/IP? Czy istnieje wygodny dostęp do serwera, czy potrzebne jest kontrolowanie maszyn położonych w odległości nawet wielu kilometrów?

Stale rozwijający się system, z setkami lub nawet tysiącami serwerów, wymaga upewnienia się, czy w posiadane rozwiązanie KVM nie stanie się jego wąskim gardłem. Poszukaj rozwiązania opartego o protokół TCP/IP, który spowoduje, iż dodawanie kolejnych użytkowników bądź serwerów będzie równie proste, jak dodawanie kolejnego urządzenia sieciowego. W miarę rozwoju Twego centrum danych miej pewność, iż wykorzystywany system KVM będzie rozwijał się wraz z nim – a wszystko to dzięki wykorzystywaniu istniejącej infrastruktury.

Jak łatwe jest dodawanie kolejnych użytkowników? Czy zmuszony jesteś do zdefiniowania z góry ilu użytkowników będzie miało jednoczesny dostęp? Systemy oparte o protokół TCP/IP wykorzystują istniejącą sieć, wobec czego dodawanie kolejnego użytkownika jest równie proste, jak dopisanie kolejnego adresu IP. Twój system KVM

powinien rozwijać się wraz z rozwojem infrastruktury sieciowej. Pracujący system, którego rozbudowa postępuje wraz z rozbudową sieci, wymaga oprogramowania, które również można w taki sposób modyfikować. A to zapewnia możliwość uaktualnienia go do nowszych wersji.

Logicznym jest również założenie, iż wymagane będzie stosowanie graficznego interfejsu użytkownika (GUI), aby nie było potrzeby kolejnego szkolenia personelu. Standardowe aplikacje systemu Windows zapewniają znany interfejs i sposób obsługi, co jest nieocenioną pomocą dla obciążonych obowiązkami pracowników działów IT, którzy potrzebują szybkiego dostępu i możliwości kontroli ustawień jakiegokolwiek urządzenia sieciowego. Po co używać oprogramowania, które będzie wymagało dodatkowych szkoleń?

Elastyczność – wszystko się zmienia. Upewnij się, iż Twój system KVM sobie z tym poradzi.

Potrzeba rekonfiguracji sprzętu będzie się stale pojawiać, to po prostu fakt. Dlaczego nie ułatwić sobie życia wybierając system, który stworzono zwracając dużą uwagę na jego elastyczność? Sprawdź czy jest możliwe użycie standardu okablowania CAT 5 do wykorzystania w całej infrastrukturze KVM. Także przy połączeniach przejściówek KVM do serwerów

Spytaj swoich sprzedawców, czy osoby z działu IT są w stanie kontrolować każde przyłączone do sieci urządzenie. Powinieneś mieć możliwość podłączenia się za pomocą jednego kliknięcia do jakiegokolwiek serwera czy innego urządzenia sieciowego z dowolnego miejsca, w którym się znajduje administrator, nawet, jeśli aktualnie naprawia konfigurację w oddziale firmy. Czy masz możliwość połączenia się z serwerem z wykorzystaniem protokołu TCP/IP bądź bezpośredniego dostępu za pomocą przełącznika KVM? Taka kombinacja zarządzania powinna występować po prostu w jednej obudowie. Możesz mieć wszystkie te zalety w urządzeniu, które zajmuje minimalną

ilość przestrzeni w obudowach typu rack czy z serwerami na półkach.

Jeżeli wybierzesz system operujący z wykorzystaniem technologii KVM OVER IP, sprawdź czy zapewnia on administratorowi możliwości pełnej kontroli a jednocześnie bezpieczeństwa połączenia. Czy mają na niego wpływ ustawienia zabezpieczeń systemu Windows? Czy możesz indywidualnie przydzielać prawa użytkownikom? Czy istnieje możliwość upgrade'u oprogramowania i firmware?

Dając swojemu personelowi IT wybór sposobu dostępu i kontroli nad urządzeniami w sieci możesz zwiększyć ich wydajność. Używając standardowego graficznego interfejsu użytkownika systemu Windows, administratorzy będą mieli możliwość szybkiego rozpoczęcia pracy i zarządzania całą strukturą nawet kilku serwerów na jednym ekranie bez konieczności przechodzenia dodatkowego szkolenia. Dajesz im do ręki narzędzie pracy z interfejsem, który już znają. Zmniejsza się również koszt wdrożenia takiego systemu, gdyż nie ma konieczności prowadzenia dodatkowego okablowania – wykorzystujesz infrastrukturę kabli UTP - czy instalacji dodatkowych kart, na które brak miejsca rozszerzeń. Daje to również oszczędność miejsca i ułatwia rozlokowanie urządzeń w serwerowni.

Szukaj systemu KVM, który jest zaprojektowany tak, aby zapewnić Ci scentralizowany dostęp do całej sieci, a nie tylko do urządzeń opartych o komputery PC. Spytaj swego dostawcę czy masz możliwość łatwego kontrolowania z jednej konsoli każdego z urządzeń czy komputerów od momentu jego uruchomienia – niezależnie od tego, czy wykorzystujesz połączenia via port PS/2, USB czy akurat łączysz się z komputerami SUN. Innym ważnym czynnikiem jest wybór systemu KVM, który posiada certyfikaty stwierdzające jego zgodność z systemami

Windows, Windows NT, Windows 2000, Novell, Unix czy Solaris.

Zdalny dostęp - zakosztuj wolności dzięki systemom opartym o protokół TCP/IP

Systemy bazujące na rozwiązaniach KVM Over IP to rozwiązania XXI wieku. Niezależnie od tego, czy znajdujesz się w tym samym budynku czy na innym kontynencie, urządzenia wykorzystujące tę technologię likwidują ograniczenia nakładane przez tradycyjne przełączniki.

Podstawową przewagą systemów KVM Over IP, jest korzystanie z istniejącej infrastruktury sieciowej – nie zmuszają do instalacji kolejnego, nietypowego okablowania. Poza tym – umożliwienie działania kolejnego serwera powinno być równie proste, jak nadanie kolejnemu urządzeniu adresu IP. Systemy KVM Over IP ustanowiły nową jakość koncepcji elastyczności i skalowalności np. centrum danych. Przy ich wykorzystaniu, personel IT jest w stanie kontrolować każdy serwer i urządzenie sieciowe z dowolnego miejsca na świecie.

Zadaj sobie pytanie, czy zarządzanie całym systemem skoncentrowane jest w jednej aplikacji, pracującej pod kontrolą systemu Windows. Aplikacja, która upraszcza dostęp i kontrolę nad urządzeniami, to podstawa systemów działających na zasadzie „wybierz i kliknij”. Oddanie pod kontrolę kolejnego urządzenia – np. zasilacza UPS, zapory ogniowej czy routera powinno wymagać dosłownie kilku kliknięć w jednej aplikacji.

Czy jesteś w stanie przewidzieć, ile dokładnie serwerów czy innych urządzeń będziesz musiał kontrolować po upływie najbliższych 18-tu miesięcy? Jeżeli odpowiedź



brzmi „nie”, powinieneś unikać systemów wymagających od Ciebie określenia z góry tej liczby. Dokonanie takiego oszacowania jest bardzo trudne, niejednokrotnie wręcz niemożliwe, lecz dostawcy, którzy zapewniają szeroki wachlarz usług i rozwiązań, powinni być w stanie pomóc Ci zaplanować dalszy rozwój.

Systemy oparte o protokół TCP/IP zapewniają niezależność od dzisiejszych standardów. W miarę rozwoju centrum danych powinieneś mieć pewność, iż Twoja sieć korzysta z najnowszych dostępnych rozwiązań.

Bezpieczeństwo – zapewnij sobie i użytkownikom system z wielopoziomowymi prawami dostępu

Jedną z zalet systemów opartych na przełącznikach KVM jest możliwość stworzenia serwerowni, do której nikt nie będzie musiał wchodzić. Możliwość ustalenia dostępu dla personelu IT z innych stanowisk sprawia, iż najważniejsze dane i sprzęt można trzymać pod kluczem. Jeżeli Twoim celem jest bezpieczeństwo, okazuje się, iż niezwykle istotne jest zapewnienie każdemu użytkownikowi indywidualnych praw dostępu. Aby stworzyć tego typu serwerownię potrzebny jest system sprawdzony i bezpieczny. Poza tym minimalizujemy przypadkowe wypięcie kabla w serwerowi.

Zastanów się czy Twój system oferuje wielopoziomowe bezpieczeństwo. Czy wspiera zabezpieczenia systemów NT, autentykację i szyfrowanie? Czy system KVM daje możliwość przypisywania praw dla każdego użytkownika, czy poziom dostępu można ustalać jedynie na poziomie grup? Co z pakietami danych? Czy są one zabezpieczone przed „podsłuchiwaniem” i przechwytywaniem?

Niezależnie od tego, czy celem jest stworzenie zamkniętej serwerowni, system przełączników KVM musi zapewniać bezpieczny dostęp. Wraz z rozwojem takich systemów okazuje się, iż nie wszystkie są poprawnie zaprojektowane. Przykładowym pytaniem jest, czy Twój system KVM zapewnia logowanie działalności użytkowników i zdarzeń systemowych?

Jeżeli przełącznik KVM jest zintegrowany z infrastrukturą sieciową, wplata się on we wszystkie już istniejące ustawienia zabezpieczeń. W systemach opartych o protokół TCP/IP użytkownik łączy się nie bezpośrednio z docelowym serwerem, a poprzez przełącznik. Przy tego typu dostępie bardzo ważne jest, aby przełącznik KVM obsługiwał wielopoziomowy system haseł, autentykacji użytkownika oraz zapewniał najwyższy poziom bezpieczeństwa użytkownikom poufność transmisji danych. Każde kliknięcie przyciskiem myszy czy wciśnięcie przycisku na klawiaturze powinno być przekazywane do przełącznika z wykorzystaniem bezpiecznego protokołu transmisji (SSL). Sprawdź, czy okres ważności kluczy szyfrujących wygasza wraz z przerwaniem sesji SSL – powinno tak się dziać.

Kiedy integrujesz system KVM ze swoją siecią, wpływa to na wiele aspektów stosowanej już polityki bezpieczeństwa. Korzystając z systemów opartych o protokół TCP/IP, użytkownik otrzymuje dostęp do nie bezpośrednio z docelowym komputerem poprzez łącze Ethernet, a jedynie z przełącznikiem KVM. Udostępnienie serwera poprzez rozwiązanie KVM over IP jest bezpieczne także z antywirusowego aspektu dostępu do komputera przez Internet. Ani klawiaturą, ani myszką wisus nie wejdzie do tak udostępnionego przez Internet serwera. A jedynie w ten sposób możliwa staje się jego pełna i bezpieczna zdalna kontrola. Każdy system, który zapewnia tego typu dostęp,



powinien również posiadać wielopoziomowy system haseł, autentykacji i wykorzystywać najcisłejszy model bezpieczeństwa. Kolejnym pytaniem jest, czy system KVM wpływa w jakiś sposób na aktualnie wykorzystywane mechanizmy bezpieczeństwa systemu Windows.

Zapewnienie użytkownikom pełnej swobody w dostępie i kontroli serwerów lub innych urządzeń sieciowych wymaga, aby zastosowany system KVM nie był kompromisem, a wręcz zwiększał ich bezpieczeństwo. Serwerownia to najczulszy punkt infrastruktury IT w każdej firmie. Tu nie opłaca się oszczędzać na bezpieczeństwie działania firmy.

Scentralizowana kontrola – nie przegap szansy, by Twoje spojrzenie sięgało po sam horyzont

Upewnij się, iż rozwiązanie KVM, którego masz zamiar użyć umożliwi Ci w łatwy sposób na podgląd działania wszystkich serwerów na jednym monitorze. Ważnym czynnikiem jest również możliwość kontroli wielu urządzeń za pomocą jednej aplikacji pracującej np. w systemie Windows. Możliwość komunikacji z urządzeniami za pomocą oprogramowania wykorzystującego graficzny interfejs użytkownika, z użyciem szyfrowanych połączeń SSL Telnet daje rozwiązaniu odpowiedni poziom bezpieczeństwa. Taka funkcjonalność – podgląd stanu wszystkich serwerów na jednym monitorze – pozwala na szybszą reakcję na pojawiający się problem i zmniejsza czas tej reakcji.

Dzisiejsze serwery oparte na komputerach klasy PC zazwyczaj obsługuje się bezpośrednio z konsoli, bądź poprzez sesję Telnet. Jeżeli rozważa się zastosowanie systemu przełączników KVM, należy także wziąć pod uwagę rozwiązania zarządzania urządzeniami z dostępem po łączy szeregowy. W ten sposób tworzy się system zdalnego i lokalnego zarządzania wszystkimi urządzeniami z serwerowni, nie tylko zawężony do serwerów opartych na

systemach PC, ale również maszyn unixowych, serwerów Sun, Firewalli, Routerów, urządzeń typu SAN, NAS czy sterowanych listw zasilających. Szukaj również systemu, umożliwiającego skonsolidowaną kontrolę nad tymi urządzeniami za pomocą jednej aplikacji. Spytaj, czy system zapewnia jednolity interfejs użytkownika dla połączeń Telnet, wykorzystujących szyfrowaną transmisję (SSL). Czy możliwy jest dostęp do tych urządzeń z poziomu przeglądarki internetowej?

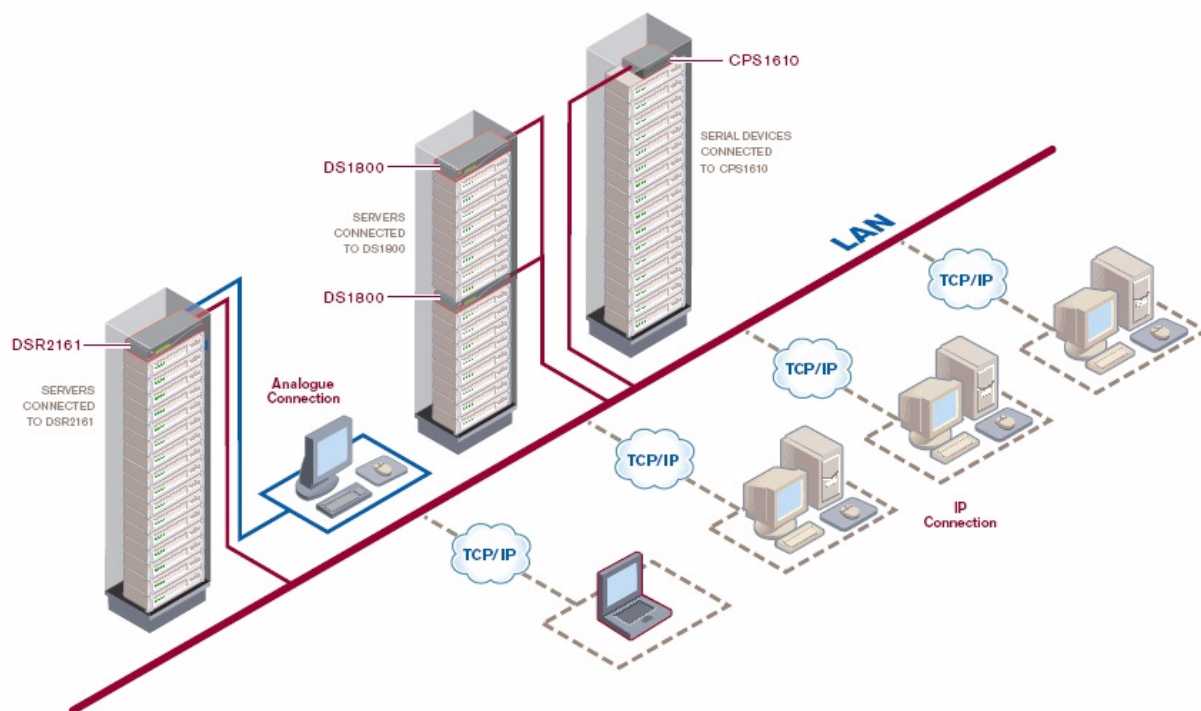
Szukaj sposobów na uproszczenie administracji Twoim systemem KVM. Sprawdź, czy przełączniki mają wbudowane oprogramowanie ułatwiające wykrywanie połączeń i nadawanie im nazw. Czy platforma administracyjna zapewnia silny system kontroli i logowania dostępu użytkowników? Częścią zabezpieczenia serwerowni jest zapewnienie bezpiecznego zdalnego dostępu poprzez przełączniki KVM. Upewnij się, czy wykorzystywane rozwiązanie daje Ci możliwość śledzenia kto i kiedy uzyskał dostęp do serwerów.

Wieloplatformowość

Dzisiejszy świat, to nie tylko urządzenia oparte o standard PC. Potrzebny jest więc system, który został zaprojektowany tak, aby w łatwy sposób łączyć różne platformy. Zasadniczą częścią centrum danych mogą być komputery PC, ale z łatwością można przewidzieć, iż wraz z jego rozbudową zaangażowane zostaną inne urządzenia i komputery pracujące pod kontrolą innych systemów operacyjnych. Czy Twój dostawca KVM ma rozwiązanie dające kontrolę nad serwerami, urządzeniami zasilającymi, Routerami lub zaporami ogniowymi w postaci jednego, centralnie zarządzanego systemu?

KVM po TCP/IP

Jeżeli interesuje Cię rozwiązanie, które nie wprowadza żadnych ograniczeń co do fizycznej odległości od kontrolowanego sprzętu, rozważ użycie systemu KVM



opartego na protokole TCP/IP, który zapewnia scentralizowaną kontrolę nad serwerami z każdego punktu Twojej sieci.

Wykorzystaj istniejącą już infrastrukturę. Z przełącznikami KVM pracującymi w oparciu o protokół TCP/IP dodawanie do systemu kolejnego użytkownika bądź serwera jest tak proste jak dopisanie kolejnego adresu IP. Rozwiązania przełączników oparte na protokole TCP/IP zmieniły znaczenie pojęć „skalowalność” i „elastyczność”. Przy ich użyciu personel IT może zarządzać każdym serwerem czy urządzeniem sieciowym np. typu Firewall, Router itp z dowolnego miejsca!

Jeżeli preferowane są rozwiązania oparte o TCP/IP, zastanów się czy system oferuje scentralizowane oprogramowanie oparte o Windows, czy też instalowane są aplikacje pisane „pod klucz”. Aplikacja pracująca w środowisku Windows upraszcza dostęp i kontrolę każdego urządzenia sieciowego. Dodawanie kolejnych urządzeń, Firewalli czy Routerów wymaga tylko kilku kliknięć myszką.

Unikaj systemów, wymagających sprecyzowania już dzisiaj docelowej ilości użytkowników i serwerów. Jest bowiem bardzo trudne do przewidzenia, jak wiele urządzeń zainstalujesz w przyszłości.

System oparty na połączeniach za pomocą protokołu TCP/IP jest na tyle uniwersalnym rozwiązaniem, iż masz pewność, że w miarę rozwoju Twojej sieci będzie on korzystał z najnowszych rozwiązań – jeżeli tylko będą one zgodne z TCP/IP.

Przełączniki systemu KVM OVER IP

Seria DS przełączników Avocent zapewnia bezpieczne połączenia z wykorzystaniem protokołu TCP/IP, dając maksymalną elastyczność i skalowalność oraz prosty w obsłudze interfejs. Seria DSR to kombinacja cyfrowej i analogowej technologii dostępowej, umożliwiającą maksymalną skalowalność i elastyczną kontrolę za pomocą jednego interfejsu pracującego w środowisku Windows.

Seria DSR również jest kombinacją cyfrowej i analogowej technologii dostępowej dedykowana do kontrolowania serwerów rack, NOC z każdej możliwej lokalizacji. Seria DS obejmuje modele: DS1800, DSR800, DSR1010, DSR2010, DSR4010 do podłączenia serwerów ze złączem PS, USB, Sun i RS232 oraz przełączniki o wejściu szeregowym CPS810 i CPS1610 do zarządzania maszynami Unixowymi, listwami zasilającymi serii SPC czy konfiguracji Firewalli, Routerów, itp urządzeń o wejściu terminalowym .

Sprawdzone rozwiązania KVM OVER IP eliminują ograniczenia co do odległości

Najbardziej zaawansowane przełączniki KVM pracujące w oparciu o protokół TCP/IP stanowią kombinację technologii cyfrowej i analogowej w jednym produkcie. Systemy te eliminują dla personelu IT ograniczenia wynikające z odległości od zarządzanej infrastruktury – dostęp można uzyskać zarówno lokalnie, jak i via Internet z dowolnego miejsca na świecie. Systemy zintegrowane z aplikacjami Windows zapewniają więcej bezpieczeństwa i pełną kontrolę. Jak działa prawdziwy system KVM OVER IP?

- * Przechwytywany jest sygnał analogowy z klawiatury, monitora i myszy.
- * Sygnały konwertowane są na cyfrowe pakiety danych.
- * Po digitalizacji dane są kompresowane i transmitowane bezpiecznym, kodowanym połączeniem z wykorzystaniem protokołu TCP/IP.

Wykorzystując kombinację przełączników KVM OVER IP oraz aplikacji Windows możliwy jest dostęp i kontrola serwera dosłownie z każdego miejsca. Co więcej – możliwe jest wręcz kontrolowanie wielu komputerów, mając podgląd ich działania na jednym monitorze.

Administratorzy mogą mieć dostęp do każdego z serwerów lub innych urządzeń sieciowych z każdego miejsca, wykorzystując ponadto interfejs Windows, który już doskonale znają. Dodatkową korzyścią jest fakt, iż można dzięki tego rodzaju aplikacjom kontrolować nie tylko komputery, ale urządzenia sieciowe wyposażone w porty szeregowo – np. routery, firewalle, zasilacze awaryjne (UPS).

Prawdziwy system KVM OVER IP jest rozwiązaniem, który pozwala na pełną kontrolę kosztów zarządzania krytycznymi węzłami sieci, niezależnie od lokalizacji serwera czy administratorów. Systemy takie pozwalają na scentralizowaną kontrolę wielu punktów bez niepożądanego marnotrawienia zasobów.

Zalety systemów KVM

- * Pozwalają na zastąpienie wielu zestawów monitorów, myszy i klawiatur za pomocą pojedynczego kompletu tych urządzeń.
- * Zapewniają łatwy dostęp i kontrolę nad każdym podłączonym komputerem.
- * Nie wymagają żadnych modyfikacji sprzętu lub oprogramowania na docelowym komputerze.
- * Zapewniają oszczędność przestrzeni, wydzielania ciepła i nadmiarowych peryferiów.
- * Dają dostęp do wielu platform wykorzystując jeden system przełączników.



Wybierz mądrze – wybierz sprawdzonego partnera

Avocent jest największym i najbardziej doświadczonym dostawcą rozwiązań KVM. Przez ponad 20 lat dostarczał menedżerom i przemysłowi urządzenia do zarządzania systemami sieciowymi. Mając na koncie tysiące wdrożeń na całym świecie, Avocent posiada doświadczenie, które pozwala dostarczyć rozwiązanie, odpowiadające potrzebom i wymaganiom użytkownika.

Avocent stale wprowadza nowe technologie i rozwiązania, które napędzają rozwój tej branży. W chwili obecnej – jak nigdy dotąd – personel IT ma wybór sposobu zarządzania stale rozrastającymi się strukturami. Sprawdzone

urządzenia Avocenta do zarządzania serwerami i sieciami, to: seria DS – DS1800, DSR800, DSR1010, DSR2010, DSR4010, CPS810/1610, SwitchView, SwitchViewIP, AutoView, AutoView Remote, LongView, OutLook.

Firma powstała w 2000 roku w wyniku fuzji Apex Inc. Oraz Cybex Computer Products Corporation. Główna siedziba mieści się w Huntsville w stanie Alabama.

Przedstawicielstwa Avocent zlokalizowane są m.in. w Redmond (stan Waszyngton), Austin (stan Teksas), Chelmsford (stan Massachusetts), Sunrise (stan Floryda), Londynie (Anglia), Shannon (Irlandia), Steinhagen, Monachium (Niemcy), Tokio (Japonia), Chinach oraz Singapurze.

