Test: Axence nVision Pro – zarządzanie siecią s. 33

Nutanix – systemy hiperkonwergentne s. 26

8
2016

Miesięcznik informatyków i menedżerów IT

www.it-professional.pl

IT professional

Nr 8 (57) sierpień 2016

Cena 33,00 zł (w tym 5% VAT)

SPOSOBY UWIERZYTELNIANIA s. 10

Zapobieganie próbom nieautoryzowanego dostępu do sieci bezprzewodowych i wirtualnych sieci prywatnych. Wykorzystanie biometrycznych systemów kontroli użytkowników i protokołów wspierających uwierzytelnianie na podstawie certyfikatów. Ochrona danych osobowych i prywatności, regulacje prawne

ISSN 2083-9588

Serwery ▪ Stacje robocze ▪ Bezpieczeństwo ▪ Infrastruktura i sieci ▪ Zarządzanie i prawo IT ▪ Techn

DOSTĘPNE E-WYDANIE

Zarządzanie infrastrukturą i monitoring wszystkich urządzeń podpiętych do sieci to chleb powszedni każdego administratora. Odpowiednie narzędzie może znacznie ułatwić wykonywanie rutynowych zadań. Z kolei wszechstronność i łatwość zarządzania to pożądane atuty charakteryzujące tego typu oprogramowanie.

8/2016 REKOMENDACJA REDAKCJI IT professional

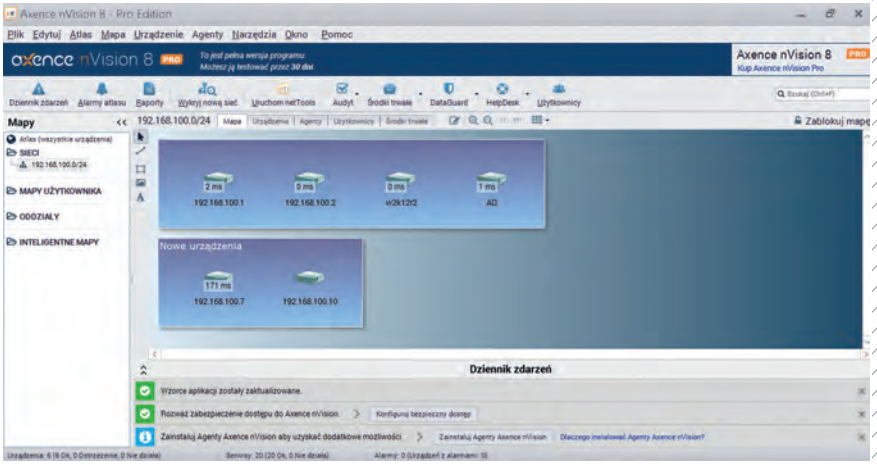
Monitorowanie i audyt

Axence nVision Pro – zarządzanie siecią

Marcin Jurczyk

Oprogramowanie nVision krakowskiej firmy Axence przez cztery lata z rzędu było wybierane przez czytelników magazynu „IT Professional" jako najlepsze w kategorii Oprogramowanie – Monitoring i zarządzanie. Hegemonia poparta zaufaniem klientów to chyba najcenniejsze trofeum dla twórców wspomnianej aplikacji. Jedyne, co ulega zmianie z roku na rok, to coraz większe możliwości pakietu zwiększające się wraz z kolejnymi numerami wersji oprogramowania Axence. Zdobyte zaufanie użytkowników zazwyczaj potwierdza wysoką jakość produktu. Przy okazji udostępnienia kolejnego uaktualnienia sprawdźmy, co takiego sprawia, że nVision niezmiennie triumfuje w corocznych zestawieniach.

Nowości wprowadzone w ósmej edycji nVision to między innymi baza wiedzy, kategoryzacja zgłoszeń, integracja poczty w module HelpDesk oraz możliwość inwentaryzacji urządzeń mobilnych działających pod kontrolą systemu Android. Aktualnie mamy już do czynienia z szóstą odsłoną dostępną w ramach wersji 8.x oznaczoną odpowiednio numerem 8.5.3. W stosunku do wersji 8.0.2 pojawiło się sporo usprawnień i funkcji, takich jak np. blokowanie typów plików pobieranych z WWW, możliwość importu licencji z pliku, nowy interfejs modułu HelpDesk czy opcja automatycznej aktualizacji serwera nVision. Nie zmienił się za to podział na moduły funkcjonalne – Network, Inventory, Users, HelpDesk i DataGuard to sekcje, w ramach których pogrupowano takie funkcje jak: wykrywanie i wizualizacja sieci z pełnym monitoringiem routerów, przełączników, serwerów, systemów i aplikacji, kontrola parametrów środowiskowych w serwerowni (SNMP), inwentaryzacja sprzętu



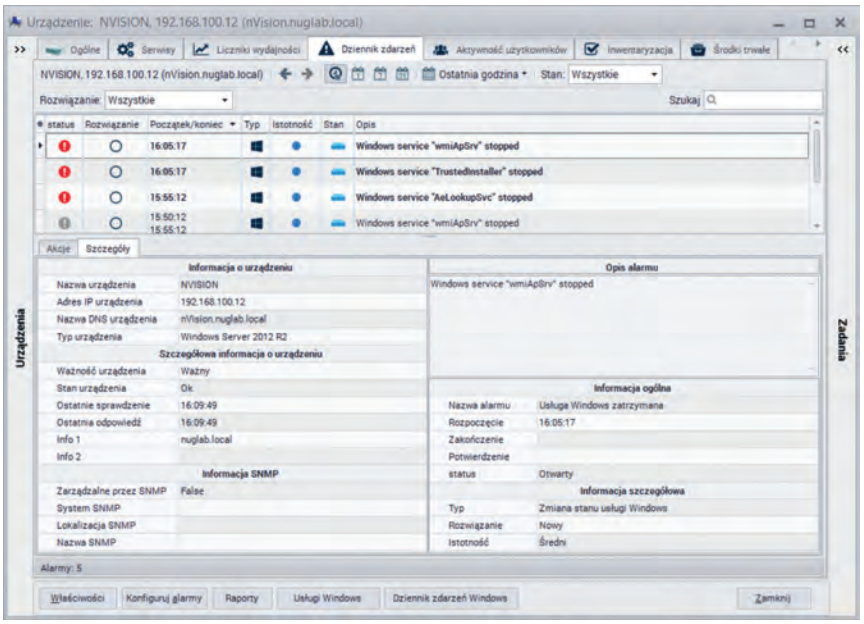
Mapa sieci może również odzwierciedlać schemat połączeń.

nVision Pro to szwajcarski scyzoryk dla administratora sieci, w której pracuje sporo serwerów Windows w środowisku domenowym. Za pomocą jednego produktu można uzyskać szczegółowe informacje nt. infrastruktury, włączając w to audyt sprzętu i oprogramowania, oraz korzystać z funkcji kontroli użytkowników.

i oprogramowania, kontrola stanowiska pracy użytkowników z rozbiciem na czas pracy, nieaktywności, wykorzystanie poszczególnych aplikacji, lista odwiedzanych stron wraz z generowanym ruchem sieciowym, a także w pełni funkcjonalne moduły HelpDesk i ochrony wrażliwych danych.

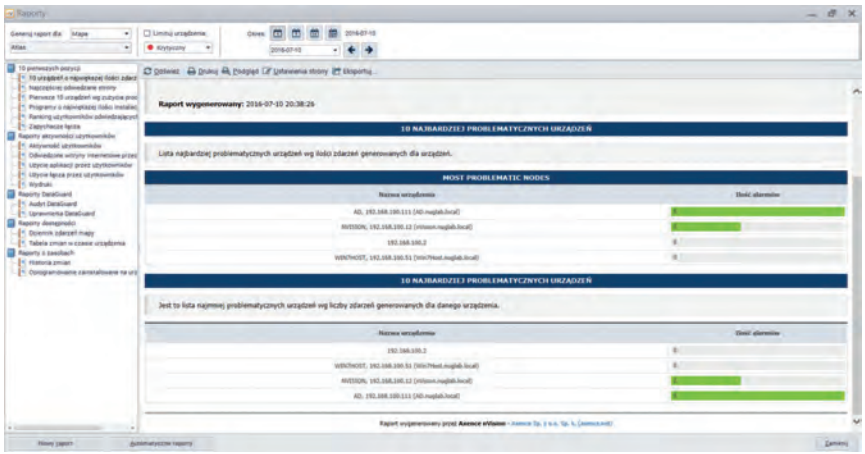
> FUNKCJONALNOŚĆ

Oprogramowanie nVision to całkiem potężne narzędzie umożliwiające szczegółowy monitoring infrastruktury sieciowej. Pięć modułów funkcjonalnych sprzężonych za pomocą pojedynczej, intuicyjnej konsoli zarządzania pozwala na monitoring i kontrolę wszystkich kluczowych elementów pracujących w sieci. Podstawowym modułem oprogramowania jest moduł Network, odpowiadający za proaktywne monitorowanie i wizualizację sieci. Elementarną częścią tego modułu jest skaner sieciowy umożliwiający wykrywanie aktywnych urządzeń. Na podstawie wyniku skanowania tworzone są mapy sieci, uwzględniające strukturę logiczną. Skaner potrafi ponadto wykryć sąsiednie sieci, znajdujące się za routerami. W tym celu konieczne jest wykorzystanie protokołu SNMP, za pośrednictwem którego pobierana jest tablica routingu, w celu identyfikacji sieci do przeskanowania. SNMP jest również wykorzystywane w celu bardziej szczegółowego monitoringu urządzeń wspierających ten protokół. Wbudowany kompilator plików MIB ułatwia współpracę ze zróżnicowanym sprzętem sieciowym. Nie zabrakło również obsługi pułapek SNMP.



Podgląd dziennika zdarzeń to jeden z elementów systemu monitoringu.

Moduł Network podaje także informacje o dostępności usług TCP/IP wraz z czasami odpowiedzi i ilością utraconych pakietów. Lista predefiniowanych usług ułatwia monitoring najbardziej popularnych serwisów sieciowych. Można również definiować własne usługi, odpowiadające indywidualnym wymaganiom użytkownika.



Predefiniowane raporty ułatwiają analizę newralgicznych danych.

Monitorowanie nie sprowadza się tylko do sprawdzenia, czy dany port jest otwarty, ale również do weryfikacji odpowiedzi na odpowiednio spreparowane żądanie. W ten sposób można wykluczyć błędną klasyfikację usług sieciowych jedynie na podstawie otwartego portu. Ponadto możliwy jest także monitoring stanu portów na przełącznikach i routerach wraz z analizą ilości ruchu sieciowego (RMON). Liczniki wydajności mogą być używane dla różnorodnych usług sieciowych, m.in. takich jak monitorowanie czasu zalogowania do serwera POP3. Usługi działające na systemach rodziny Windows można monitorować również za pośrednictwem WMI oraz poprzez aplikację agenta. W pierwszym przypadku konieczne jest odpowiednie uwierzytelnienie na stacji docelowej. Za pośrednictwem WMI odbywać się może również monitorowanie dziennika zdarzeń Windows oraz dystrybucja plików w sieci. Zaburzenie działania monitorowanej w ten sposób usługi może wiązać się z odpowiednią akcją, np. ponownym uruchomieniem serwisu, który przestał działać.

Moduł Network ma także wbudowany serwer Syslog, który można z powodzeniem wykorzystać jako centralne

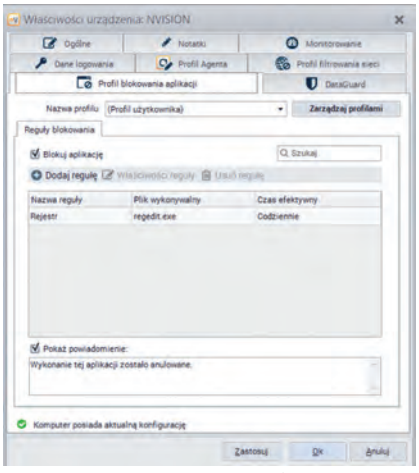
repozytorium logów wraz z generowaniem zdarzeń odpowiadających wystąpieniu określonych słów kluczowych. Wygenerowanie wiadomości Syslog może być również zdefiniowaną przez użytkownika akcją.

Moduł Inventory z kolei wykorzystuje aplikację agenta w celu gromadzenia informacji o konfiguracji sprzętowej każdego komputera oraz zainstalowanych aplikacjach. Największe możliwości oferuje agent dla systemów Windows. Dostępne są również wersje dla Linuksa, Androida oraz OS X. Komunikacja pomiędzy programem agenta a serwerem jest szyfrowana (256 bitów), a przesyłane dane pakowane. Usunięcie aplikacji agenta jest naturalnie zabezpieczone hasłem, co okazuje się skuteczne szczególnie w środowisku domenowym. Moduł Inventory umożliwia również wykonanie skanowania inwentaryzacyjnego w trybie offline – odpowiednio przygotowana wersja skanera offline (plik .exe) uruchamiana jest na komputerach, które z pewnych względów nie są podłączone do sieci, a zebrane w ten sposób dane importowane są do serwera nVision. Inwentaryzacja oprogramowania pozwala kontrolować zainstalowane aplikacje, a także pliki magazynowane na dyskach twardych monitorowanych komputerów. Identyfikacja oprogramowania odbywa się w oparciu o wzorce (około 600 ręcznie przygotowanych wzorców dostępnych wraz z nVision), które umożliwiają identyfikację typu licencji, co pozwala na późniejszą kontrolę legalności. Poza tym wzorce mogą być tworzone automatycznie w trakcie skanowania rejestru. Oprócz informacji dostępnych w rejestrze Windows wykorzystywane są również pliki na dyskach, które mogą jednoznacznie identyfikować daną aplikację. Funkcja audytu inwentaryzacji oprogramowania pozwala porównać stan zainstalowanych kopii oprogramowania z liczbą zakupionych licencji (należy najpierw wprowadzić takie informacje do systemu). Dostępna jest także historia zmian oprogramowania, dzięki czemu można łatwo prześledzić cykl życia aplikacji dla danego komputera. Podobnie sytuacja wygląda w przypadku inwentaryzacji sprzętu. Wszystkie

Automatyzacja procesowania zgłoszeń HelpDesk to jedno z dostępnych ułatwień.

komponenty sprzętowe wraz z historią zmian dostępne są w jednym miejscu. Moduł inwentaryzacyjno-rozliczeniowy w ramach modułu Inventory to tak zwane środki trwałe, czyli zbiór danych na temat komponentów infrastruktury, łącznie z informacjami na temat gwarancji, czasu życia czy fizycznej lokalizacji. Informacje inwentaryzacyjne mogą zostać uzupełnione o załączniki, takie jak skany faktur zakupowych czy kart gwarancyjnych. Stan środków stałych można również audytować, porównując stan z różnych punktów w czasie życia urządzenia.

Kolejne dwa moduły Users oraz DataGuard to elementy bezpośrednio związane z monitoringiem i kontrolą



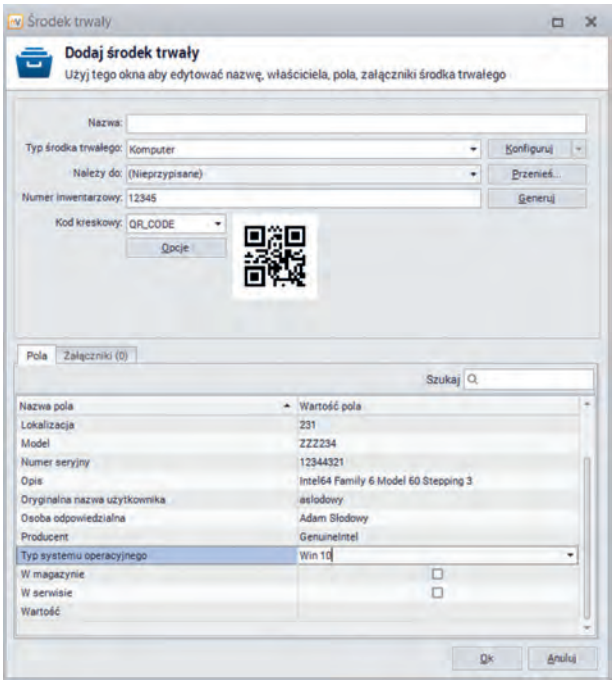
Blokowanie aplikacji za pośrednictwem indywidualnie definiowanych profili to jedna z funkcji nVision.

użytkowników. Monitoring aktywności użytkowników pozwala gromadzić informacje na temat faktycznego czasu pracy i czasu użytkowania programów. Raportowana jest również aktywność i czas spędzony na przeglądanie stron WWW czy utylizacja łącza z rozbiciem na transfer lokalny oraz do sieci globalnej. Administrator może również podejrzeć zrzut ekranu z konkretnej stacji lub zdefiniować cykliczne zapisywanie takich screenshotów. Ponadto możliwe jest monitorowanie wiadomości e-mail z ograniczeniem do informacji o nadawcy, odbiorcy, tematu i rozmiaru wiadomości. Nie mogło tu również zabraknąć monitorowania wydruków wraz z oszacowaniem kosztów, po uprzednim zdefiniowaniu parametrów wejściowych dla takiej kalkulacji.

Uzupełnieniem funkcji monitorowania użytkowników jest wspomniany moduł DataGuard, który pozwala chronić dostęp do danych przedsiębiorstwa. Ochrona przed wyciekiem informacji realizowana jest na poziomie kontroli dostępu do wszystkich urządzeń peryferyjnych mogących służyć do skopiowania informacji, takich jak pamięci flash, dyski przenośne, gniazda kart SD czy interfejsy komunikacyjne, takie jak Bluetooth. Monitorować można zarówno operacje zapisu, jak i odczytu. Możliwe jest także kontrolowanie wykonywania programów uruchamianych z tego typu nośników, dzięki czemu można ustrzec się przed

automatycznym wykonaniem kodu złośliwego oprogramowania. Uprawnienia są zależne od organizacji struktury użytkowników i grup oraz mogą być dziedziczone. DataGuard umożliwia również przeprowadzenie audytu bezpieczeństwa plików, dostarczając informacji na temat tego, jakie pliki zostały zapisane na urządzeniu przenośnym, kiedy miało miejsce takie zdarzenie i którego komputera dotyczyło. Jest to zatem sporo więcej, niż proponuje większość dostawców oprogramowania oferującego tylko proste blokowanie na podstawie białych i czarnych list. Z podłączeniem oraz wykonywaniem operacji na pamięciach zewnętrznych mogą również być kojarzone odpowiednie alerty informujące administratora o wystąpieniu podejrzanej czynności. Zarządzanie alarmami, akcjami i zdarzeniami dotyczy większości sytuacji, które można łatwo zdefiniować w programie nVision.

Ostatni z modułów – HelpDesk, to jak łatwo się domyślić, system zgłoszeń dla użytkowników sieci, za pośrednictwem którego można zgłaszać i rozwiązywać problemy występujące w środowisku IT. Dostęp do tego modułu realizowany jest za pośrednictwem dedykowanego portalu dostępnego z poziomu przeglądarki, choć zgłoszenia można również zgłaszać mailowo lub za pośrednictwem aplikacji agenta. Jest to tradycyjny moduł ułatwiający obsługę i śledzenie postępu rozwiązywania problemów wraz z możliwością częściowej automatyzacji obsługi requestów. W opisywanym pakiecie nie zabrakło integracji z zarządzalną bazą wiedzy, w której opisane zostały sposoby rozwiązania poszczególnych problemów. W zależności od rodzaju zgłoszenia możliwe jest oddelegowanie odpowiednio wykwalifikowanych pracowników do rozwiązywania określonych zgłoszeń. Kategoryzacja i priorytetyzacja to kolejne elementy, których nie mogło zabraknąć w module tego typu. Wbudowana funkcja komunikatora ułatwia wymianę informacji pomiędzy użytkownikiem zgłaszającym problem a osobą przypisaną do jego rozwiązania. Zintegrowany jest również dostęp zdalny do maszyny użytkownika w celu szybszego zdiagnozowania usterki. Administrator może również wysyłać komunikaty do użytkowników, informując np. o planowanych oknach serwisowych.



Dodawanie środków trwałych na potrzeby księgowo-inwentaryzacyjne wraz z obsługą kodów kreskowych i załączników.

Jak łatwo się domyślić na podstawie przedstawionej charakterystyki funkcjonalnej nVision Pro, naturalnym środowiskiem pracy jest sieć działająca w oparciu o domenę Active Directory. Scentralizowane zarządzanie użytkownikami oraz kontrola uprawnień to atrybuty znacznie ułatwiające monitoring za pośrednictwem oprogramowania firmy Axence. Zdalna dystrybucja oprogramowania i kontrola współdzielonych zasobów dyskowych to tylko niektóre operacje, które wykonuje się zdecydowanie łatwiej, mając pełną kontrolę nad zarządzanym środowiskiem.

> WYMAGANIA I INSTALACJA

Oprogramowanie Axence nVision dedykowane jest dla systemów operacyjnych z rodziny Microsoft Windows. Aplikację serwera zainstalować można na maszynach działających pod kontrolą co najmniej systemu Windows Vista, jednakże ze względów licencyjnych powinna być to serwerowa wersja systemu operacyjnego. Konsola nVision, jak również aplikacja agenta w minimalnej konfiguracji będą działały także na wersji XP oraz Windows Server 2003 z zastrzeżeniem, że w przypadku problemów technicznych użytkownik nie będzie miał możliwości korzystania z odpowiedniego wsparcia. Funkcja serwera nVision nie ma wygórowanych wymagań sprzętowych – wystarczą dwurdzeniowy procesor, 4 GB pamięci RAM i 10 GB przestrzeni dyskowej. W przypadku gdy mamy do czynienia ze środowiskiem, w którym monitorowanych jest ponad 1000 agentów, producent zaleca dedykowaną maszynę fizyczną, czterordzeniowy CPU, 8 GB RAM na każdy 1000 agentów, 64-bitową wersję systemu operacyjnego i szybki podsystem dyskowy. Konsolę oraz agenta nVision można za to uruchomić na dowolnym współczesnym komputerze pracującym przynajmniej pod kontrolą Windowsa XP. Co ważne – poprawne generowanie raportów z konsoli nVision wymaga przeglądarki Internet Explorer w wersji 8 lub nowszej. Sam nVision z kolei monitoruje przeglądarki: Internet Explorer, Mozilla Firefox i Google Chrome.

Konieczne jest również odpowiednie przygotowanie środowiska sieciowego, które będzie monitorowane. Odpowiednia konfiguracja SNMP czy odblokowanie portów firewalla, aby umożliwić transfer danych, to te najbardziej oczywiste kroki konfiguracyjne. Sam serwer nVision wykorzystuje porty TCP 4434 i 4436 w celu wymiany informacji diagnostycznych i komunikacji z agentami. Ponadto domyślny dostęp do nVision poprzez przeglądarkę realizowany jest na porcie 8080. Od strony agenta komunikacja odbywa się z wykorzystaniem portu TCP 4433. Z kolei monitorowanie za pośrednictwem WMI wymaga użycia dodatkowych portów 135, 139, 445 oraz 593. Starsze wersje systemów, tj. Windows XP Professional, Vista i 7, wymagają również dodatkowego odblokowania funkcjonalności WMI. Sama instalacja oprogramowania nVision sprowadza się do uruchomienia pliku instalatora i postępowania zgodnie z komunikatami kreatora instalacji. Na tym etapie można wybrać pomiędzy instalacją zarówno serwera i konsoli, jak również tylko jednego z tych elementów.

> LICENCJONOWANIE I CENY

Axence nVision Pro jest produktem licencjonowanym na jedno stanowisko robocze i wymaga jednej licencji na sieć. Zakup licencji pozwala na instalację jednego serwera nVision oraz nieograniczonej liczby konsoli zarządzających. Moduły Inventory, Users, HelpDesk oraz DataGuard wymagają instalacji aplikacji agenta na stacjach roboczych, a liczba monitorowanych końcówek jest bezpośrednio powiązana z liczbą posiadanych licencji na dany moduł. Moduł Network umożliwia monitorowanie nielimitowanej liczby urządzeń sieciowych. Wszystkie zakupione licencje dają dożywotnie prawo korzystania z aplikacji. Przy pierwszym zakupie w cenie licencji zawarta jest 12-miesięczna umowa serwisowa, zapewniająca wsparcie techniczne i dostęp do aktualizacji. Przedłużenie umowy wiąże się z kosztem na poziomie 20% licencji bazowej za każdy kolejny rok.

Ceny Axence nVision zaczynają się od 1500 zł netto za serwer zarządzający z modułem Network dla nielimitowanej liczby urządzeń. Przy zakupie większej liczby modułów ceny zależą od liczby stacji roboczych w sieci i mogą być indywidualnie negocjowane.

Warto w tym miejscu wspomnieć, że poza wersją Pro dostępna jest także wersja darmowa, która obsługuje maksymalnie 25 agentów i nielimitowaną liczbę urządzeń sieciowych dla modułu Network. Lista ograniczeń dla wszystkich modułów jest jednak spora – nie skorzystamy chociażby z funkcji audytu sprzętu i oprogramowania, zarządzania licencjami, blokowania aplikacji i stron WWW i zarządzania prawami dostępu dla urządzeń, komputerów oraz użytkowników. Szczegółową listę ograniczeń można znaleźć pod adresem: axence.net/pl/porownanie-axence-nvision/.

Duża funkcjonalność, intuicyjny interfejs, stosunkowo niewielkie wymagania sprzętowe i programowe oraz możliwość współpracy z różnymi systemami operacyjnymi to atuty, które sprawiają, że trudno znaleźć jakąkolwiek istotną wadę tego pakietu. Wygląda na to, iż uczestnicy dotychczasowych plebiscytów na produkt roku w tej kategorii nie mylili się... IT

Autor jest architektem w międzynarodowej firmie z branży IT. Zajmuje się infrastrukturą sieciowo-serwerową, wirtualizacją infrastruktury i pamięcią masową.

PODSUMOWANIE

Oprogramowanie nVision w wersji Pro to szwajcarski scyzoryk dla administratora sieci, szczególnie tej, w której pracuje sporo serwerów Windows w środowisku domenowym. Za pomocą jednego produktu można uzyskać szczegółowy wgląd w urządzenie podpięte do sieci firmowej wraz z informacjami na temat majątku IT w przedsiębiorstwie, włączając w to audyt sprzętu i oprogramowania. Funkcje kontroli i monitoringu użytkowników pozwalają reagować na incydenty związane z nadużywaniem służbowego sprzętu komputerowego w celach innych niż zakontraktowane. Blokowanie niepożądanych stron internetowych i aplikacji, a także kontrola dokumentów kopiowanych na zewnętrzne nośniki danych to świetne uzupełnienie funkcji oferowanych przez oprogramowanie antywirusowe. Uzupełnieniem jest dopracowany moduł HelpDesk umożliwiający rozbudowaną interakcję z użytkownikami, chociażby w formie funkcji chatu czy dostępu zdalnego. Całość jest przy tym łatwa w zarządzaniu, a nawigacja i odnajdywanie odpowiednich funkcji proste i intuicyjne, pomimo naprawdę bogatej funkcjonalności.

Werdykt

Axence nVision Pro

Zalety

- ⊕ Łatwa instalacja
- ⊕ Duża funkcjonalność
- ⊕ Przejrzyste GUI
- ⊕ Niewielkie wymagania
- ⊕ Wyczerpująca dokumentacja

Wady

- ⊖ brak

Ocena **10**/10