



Agent 00nV w służbie administratora sieci






Jakub Kralka,
Product Manager Axence

Licencja na zarządzanie (infrastrukturą IT)

Ian Fleming napisał w swoim życiu kilkanaście powieści o najbardziej znanym agencie na świecie. Co kilka lat śledzimy również szalone akcje i działania Ethana Hunta, Jasona Bourne'a. Niegdyś pasjonowaliśmy się przygodami naszego słynnego J23. Dziś jednak opowiemy o Agencie, który nie posługuje się Berettą 418 czy Waltherem PPK, a jego postać nie kojarzy się ze spektakularnymi pościgami i wi-

dowiskowymi eksplozjami. Przybliżymy profil Agenta Axence nVision i zaprezentujemy korzyści z jego działania w sieci teleinformatycznej.

Na początek podstawy. Axence nVision® to oprogramowanie wspierające codzienną pracę administratorów sieci. Narzędzie to składa się z 5 modułów funkcjonalnych:

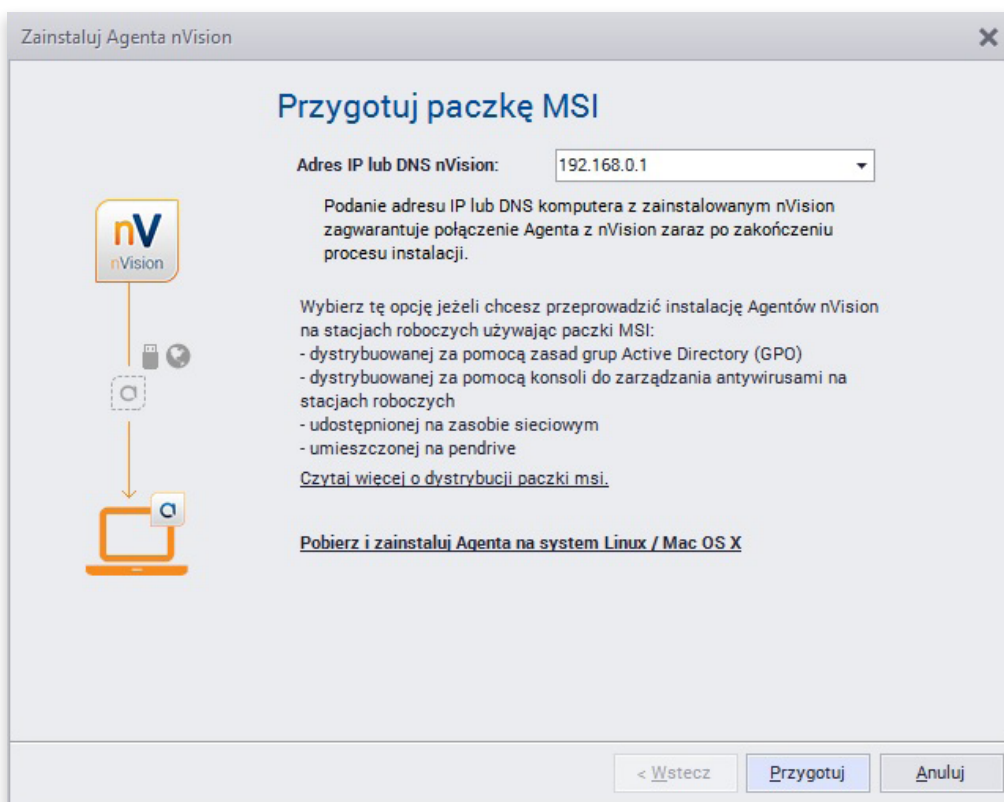
 Network	wizualizacja oraz monitorowanie urządzeń sieciowych,
 Inventory	zarządzanie zasobami IT, inwentaryzacja oprogramowania i sprzętu oraz audyt stacji roboczych,
 Users	monitorowanie aktywności użytkowników oraz budowanie polityki bezpieczeństwa wykorzystania stacji roboczych,
 HelpDesk	tworzenie i zarządzanie zgłoszeniami serwisowymi, baza wiedzy oraz narzędzie bezpośredniego wsparcia użytkownika (np. poprzez zdalne przejęcie aktywnej sesji na stacji roboczej),
 DataGuard	tworzenie polityki wykorzystania urządzeń przenośnych oraz zabezpieczenie przed wyciekiem danych.

Cztery z nich (Inventory, Users, HelpDesk oraz DataGuard), aby w pełni wykorzystać swoje możliwości, potrzebują do pracy małego programu zainstalowanego na stacjach roboczych – właśnie naszego Agenta.

Metryka Agenta

Agent nVision to lekki program zbierający dane ze stacji roboczej i przesyłający je do serwera nVision. Podczas tworzenia paczki instalacyjnej Agenta musimy podać adres IP stacji, na której zainstalowany jest Serwer nVision. Sam Agent nie posiada predefiniowanych ustawień, „wgranych” i ustawianych podczas procesu instalacji, ponieważ po zainstalowaniu łączy się z serwerem nVision i pobiera zestaw reguł przypisany do stacji roboczej lub mapy na której stacja się znajduje.

Program startuje w sesji usługi Windows, a więc użytkownik nie musi być zalogowany, aby nastąpiła komunikacja między Agentem a serwerem nVision. Pierwsza komunikacja ma na celu ustalenie czy nie zmieniły się ustawienia profili dla danej stacji roboczej. Sam profil może być zmieniany dynamicznie tzn. w przypadku konieczności zmian uprawnień dostępowych dla danej stacji roboczej może być zmieniony przez Administratora na żądanie we właściwościach urządzenia w programie.



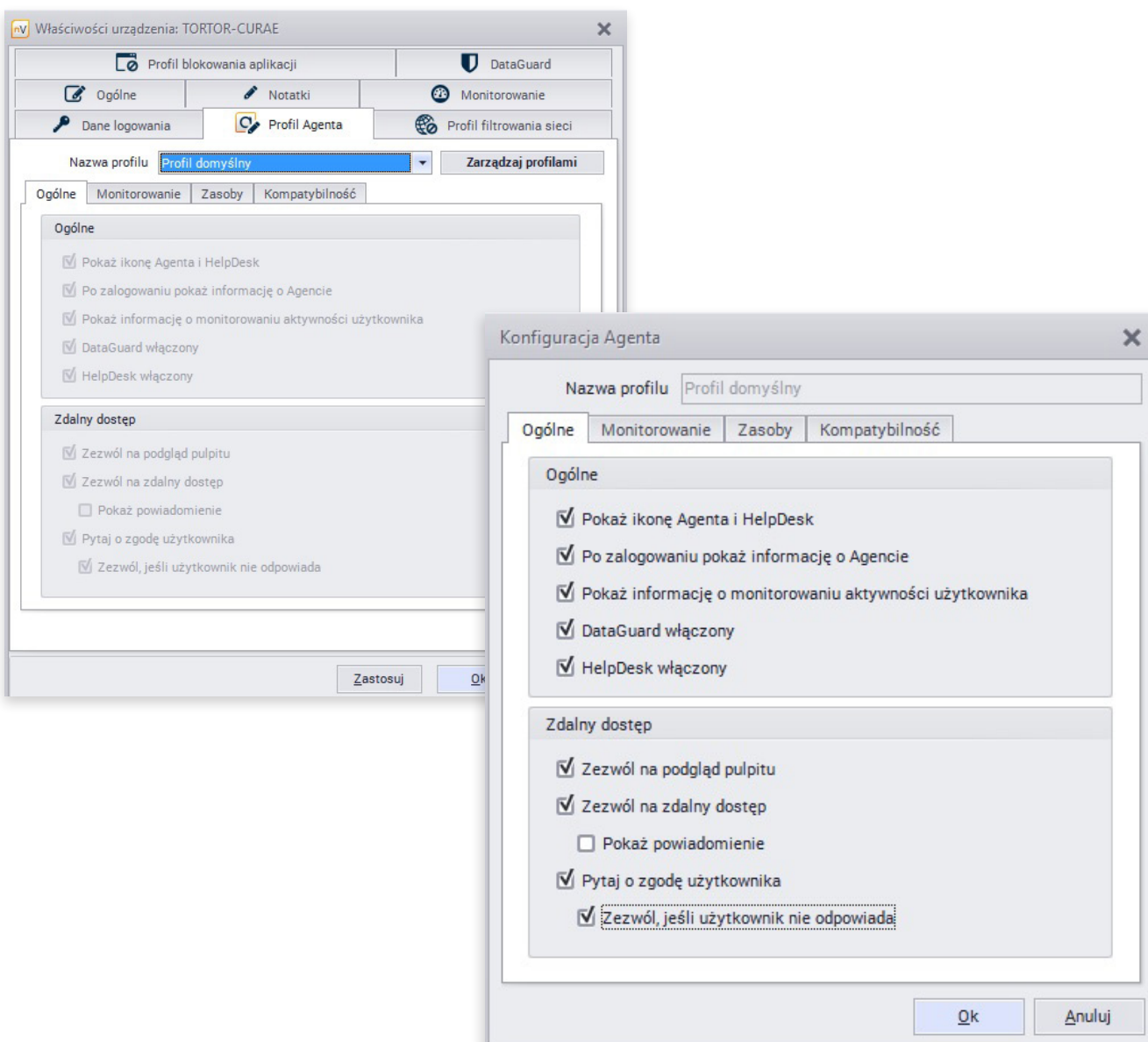
Arsenał możliwości rekomendowany przez Q

Skupmy się na możliwościach konfiguracyjnych Agenta i omówmy profile, którymi możemy zarządzać oraz informacje, jakie Agent może nam dostarczyć ze stacji roboczej.

Możemy zarządzać:

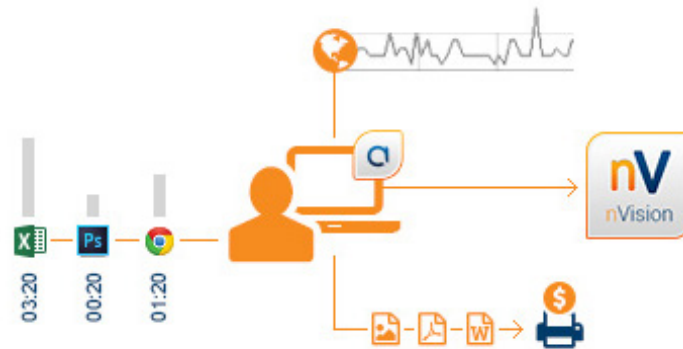
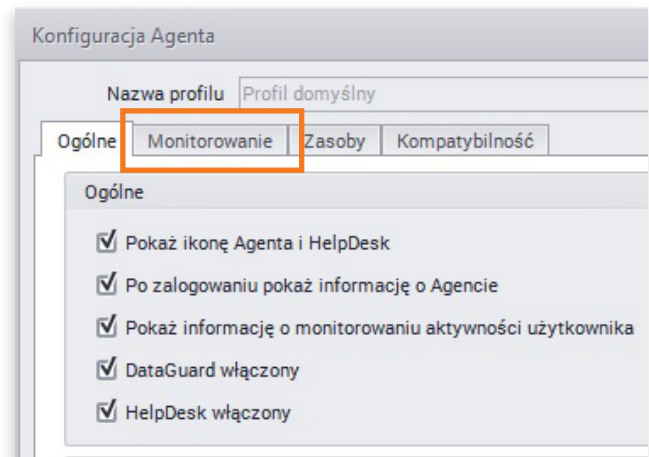
- profilem Agenta,
- profilem filtrowania sieci,
- profilem blokowania aplikacji.

Profil Agenta umożliwia nam ustawienie podstawowych funkcji pracy Agenta na stacji roboczej, które ściśle związane są z funkcjonalnościami modułów nVision. Możemy dzięki temu umożliwić użytkownikowi dostęp do HelpDesku z poziomu ikony Agenta (znajdującej się w zasobniku systemowym), ustawić możliwość dostępu zdalnego dla administratora lub włączyć politykę wykorzystania zewnętrznych nośników danych z modułu DataGuard.

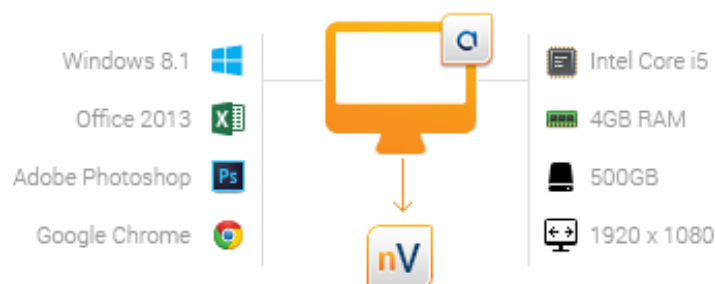
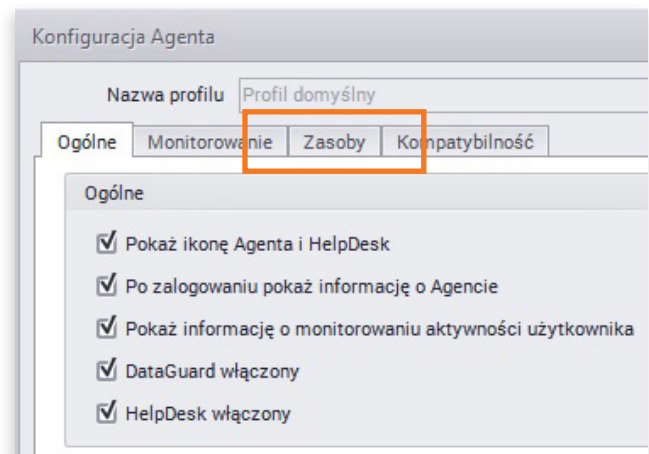


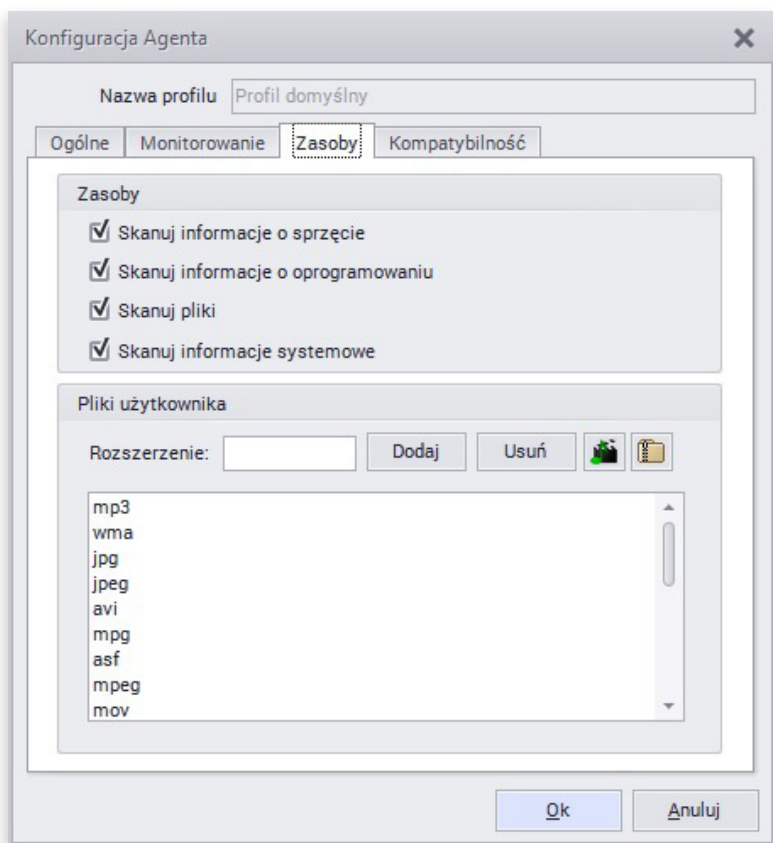
W zakładce Monitorowanie, możemy zaznaczyć jaką aktywność, lub użycie aplikacji na stacji roboczej użytkownika mają być monitorowane. Opcje monitorowania aktywności można ograniczyć do konkretnych godzin i dni aby nie zaburzać statystyk pracy i nie monitorować aktywności użytkownika po godzinach jego pracy.

W tej zakładce konfiguracyjnej możemy również zdefiniować jaki okres bezczynności na stacji roboczej będzie rejestrowany i przesyłany do Serwera nVision jako przerwa w aktywności użytkownika.



Zakładka Zasoby odwołuje się bezpośrednio do modułu Inventory. Dzięki temu możemy zdefiniować możliwość skanowania stanu oprogramowania w celu porządkowania i zarządzania licencjami w naszym środowisku sieciowym i potencjalnym ograniczeniu niepotrzebnych kosztów związanych z zakupem oprogramowania, którego nie potrzebujemy.

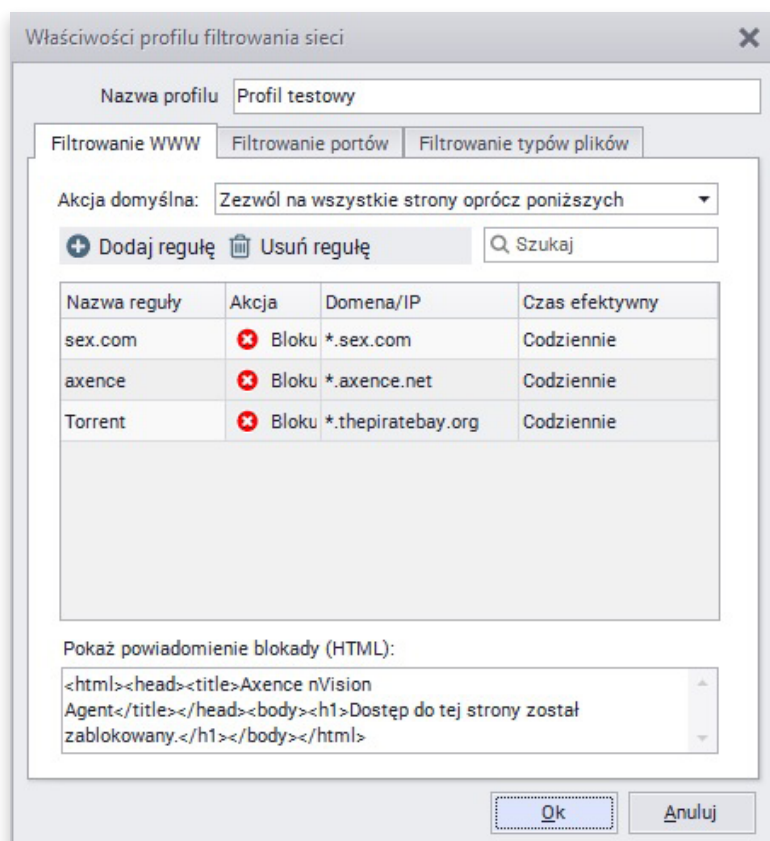


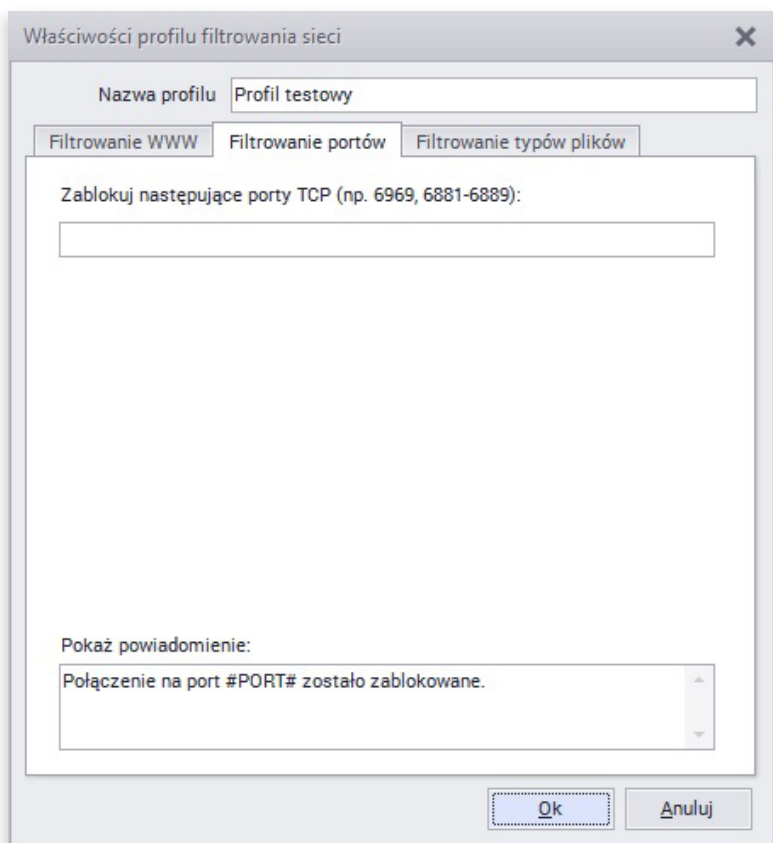


Oprogramowanie to jednak nie jedyne informacje jakie możemy uzyskać o stacji roboczej dzięki pracy Agenta. Sprzęt, jego numer seryjny oraz podłączone peryferia to informacje, które administrator może otrzymać poprzez skanowanie monitorowanego komputera. Wartością dodaną jest m.in. możliwość sprawdzenia zawartości dysków fizycznych użytkowników pod kątem przechowywania na nich plików, których przechowywanie mogłoby wiązać się z naruszeniem praw autorskich (filmy, muzyka, dokumenty).

W walce z niebezpieczeństwami

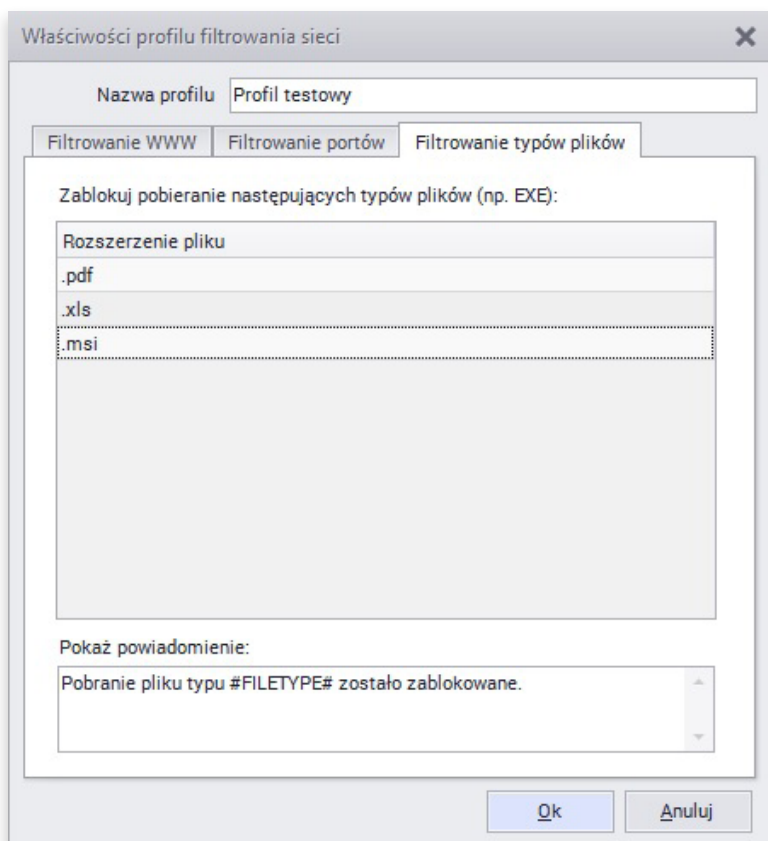
A co z zagrożeniami czyhającymi na naszych użytkowników na bezkresnych przestrzeniach Internetu? Czy jesteśmy w stanie pomóc tym, którzy cierpią na prokrastynację lub często są rozpraszeni przez np. media społecznościowe? Czy chcemy umożliwić korzystanie z prywatnej poczty opartej o serwisy webowe w godzinach pracy? Agent pozwala nam na ustawienie odpowiedniego profilu filtrowania sieci. Dzięki temu jesteśmy w stanie blokować domeny lub adresy IP, które bezpośrednio nie pomagają naszym użytkownikom w wykonywaniu ich obowiązków lub narażają naszą organizację na potencjalne problemy wynikające z pobierania nielegalnych treści z serwisów P2P.





Jako administrator mamy również możliwość blokowania portów by bez zgody przełożonego nikt nie utworzył dysku FTP służącego do wymiany plików na swojej stacji roboczej lub nie używał nieautoryzowanych klientów VPN

Częstym problemem z jakim muszą borykać się w codziennej pracy administratorzy jest pobieranie przez użytkowników sieci plików niebezpiecznych dla infrastruktury. Niekoniecznie musi być to działanie umyślne, ale jako opiekunowie infrastruktury, to admini odpowiadają za dostarczenie dobrych praktyk wykorzystania zasobów sprzętowych oraz za edukację użytkowników. Jeżeli jednak polityka bezpieczeństwa nie nakazuje tego lub nie mamy wystarczających zasobów lub czasu – możemy posłużyć się polityką blokowania rozszerzeń plików, które zezwolimy lub zabronimy pobierać na stację roboczą podczas korzystania z sieci WWW.

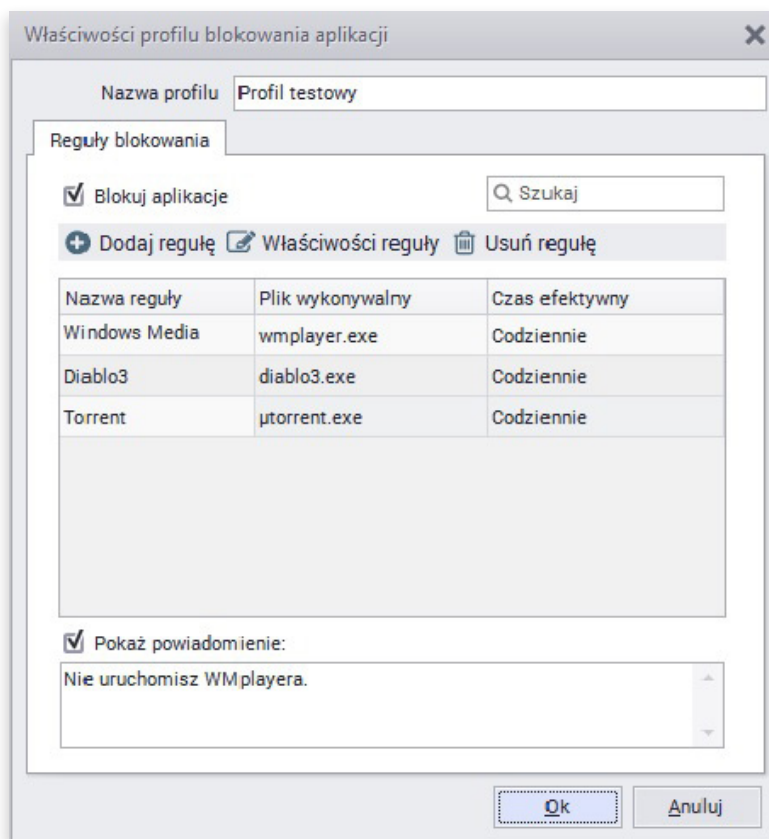


Czy Agent jest w stanie zapobiegać nieefektywnemu wykorzystywaniu czasu pracy tzw. „cyberslackingu”?

Dzięki możliwości blokowania aplikacji, jesteśmy w stanie uniemożliwić uruchomienie pliku wykonywalnego na stacji roboczej użytkownika, nawet jeżeli została zmieniona oryginalna nazwa pliku źródłowego (np. zmiana z Diablo3.exe na firefox.exe). Agent sprawdza metadane pliku wykonywalnego i jest w stanie przeciwdziałać próbom obejścia reguły blokowania.

 <http://biznesyrobie.pl/praca/123-pracodawca-patry-koniec-ery-cyberslackingu/>

To nie jedyne zalety i zdolności Agenta nVision. Lekki program posiadający szerokie możliwości konfiguracji to idealne wsparcie w codziennej pracy administratora sieci. Współpraca z nim może przynieść wiele korzyści dla całej infrastruktury i nie obciąża jej zasobów (dzienna paczka danych wysyłana z Agenta do serwera nVision nie przekracza 200 KB).



Dowiedz się więcej

Więcej informacji o możliwościach Agentów nVision, wraz z przejrzystą tabelą korzyści, można znaleźć w artykule [Jak zdobyć 100% wiedzy o swojej sieci](#), opublikowanym na stronie Axence.