

Networld

PRZEDRUK

KWIECIEŃ 2015 (04/223) INDEKS 328820

CENA 26,90 ZŁ (W TYM 5% VAT)

www.networld.pl

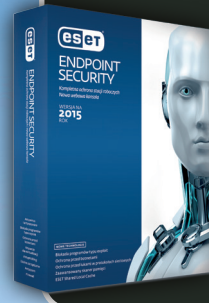
9 mitów o SSD

Obalamy przesady
o nośnikach flash

PRAWDA

FAŁSZ

TEST
Eset Endpoint
Security



INTEGRATOR CORAZ WAŻNIEJSZY

Jak nowe trendy technologiczne wpływają
na współpracę przedsiębiorstw z integratorami IT

VIRTUALBOX VS. VMWARE WORKSTATION

Porównanie możliwości wiodących
produktów do wirtualizacji stacji roboczych



Kompleksowa ochrona

Na rynku rozwiązań do kompleksowej ochrony stacji roboczych oraz serwerów ciągle pojawiają się nowe produkty. Niektóre z nich to tylko odświeżone wersje istniejących od wielu lat produktów, ale są i takie, które zmieniono uwzględniając wymagania klientów. Do tych ostatnich należy nowa wersja pakietu Eset Endpoint Security Suite.

Jarosław Kowalski

Na przestrzeni lat rozwiązania antywirusowe oraz smart security firmy Eset cieszyły się uznaniem użytkowników dzięki gwarancji skuteczności przy umiarkowanym obciążeniu systemów oraz prostocie instalacji i zarządzania. Cała gama zastosowań sprawiała, że wdrożeniem rozwiązania Eset interesowali się zarówno użytkownicy domowi, jak i firmy.

Niedawno firma Eset udoostępniła najnowsze edycje swoich produktów, gdzie najwięcej zmian wprowadzono w elementach przeznaczonych do zastosowań biznesowych. Całkowicie zmieniło się podejście producenta do kwestii licencji, a także w zakresie konfiguracji i zarządzania.

NAJWAŻNIEJSZE ZMIANY

Eset Endpoint Antivirus oraz Eset Endpoint Security, dostępne są teraz dla stacji roboczych z Windows, Linux oraz OS X. Nowe wersje chronią dodatkowo serwery plików z zainstalowanym systemem Windows Server (Eset File Security for Microsoft Windows Server). Aplikację do ochrony znajdują dla siebie również użytkownicy urządzeń mobilnych z systemem Android (Eset Endpoint Security for Android). Aplikacje dla

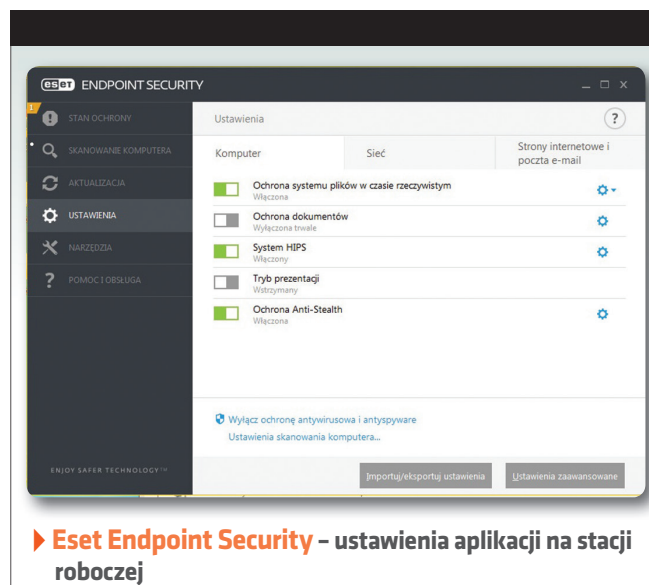
systemów końcowych wyposażone zostały w nowe skuteczne narzędzia skanujące, potrafiące zidentyfikować nawet najbardziej skomplikowane zagrożenia oraz zaawansowany system blokady programów typu exploit, który chroni przed wykorzystywaniem luk w zainstalowanych aplikacjach. Zaimplementowane mechanizmy ochrony zostały wyposażone również w algorytmy rozpoznające działanie sieci botnetowych. Dzięki rozpoznaniu ruchu sieciowego odpowiadającego zainfekowanym komputerom (zombie) blokuje on wszelkie działania, mające na

celu przeprowadzenie ataku na zewnątrz.

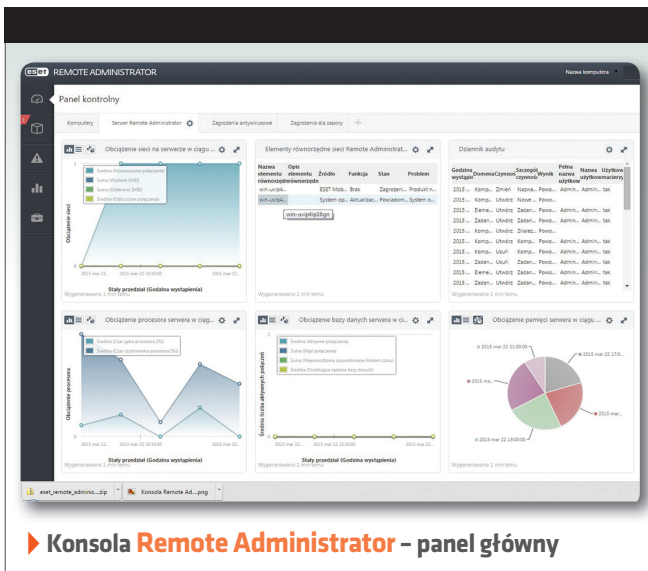
Firma Eset przebudowała silnik skanujący. Mając na uwadze odciążenie lokalnego systemu od wielokrotnego sprawdzania tych samych elementów, a tym samym znaczne przyspieszając operację skanowania, producent korzysta z chmurowego systemu reputacji Eset Live Grid. Dzięki temu pliki raz sprawdzone przez rozwiązania Eset są przy kolejnych skanowaniach porównywane z wzorcem zapisanym w chmurze. Jeśli wzorec i sprawdzany plik są identyczne, program błyskawicznie rozpoznaje, że plik jest znany i nie musi być skanowany.

Nowa wersja rozwiązań Eset zawiera także mechanizmy znacznie poprawiające wydajność pracy w środowiskach wirtualnych. Technologia Eset Shared Local Cache działa podobnie do Live Grid. Dzięki współdzielonym zasobom udostępnianym na poziomie hosta poprawne elementy raz skanowane nie muszą być ponownie sprawdzane.

Jednak dwie najbardziej charakterystyczne zmiany dotyczą modelu licencjonowania oraz konsoli centralnego zarządzania. W pierwszym przypadku utworzono centralną konsolę zarządzania licencjami, Eset License Administrator (ELA), która przede wszystkim umożliwia przejrzysty widok posiadanych licencji w podziale na już wykorzystane i wolne, możliwe do użycia. Dzięki ELA administrator w prosty sposób w ramach jednego konta synchronizuje wszystkie posiadane licencje oraz może dodawać kolejne w miarę powiększania się środowiska. Znacznie ułatwia to kontrolę nad wykorzystaniem zakupionych elementów oraz dezaktywację licencji z usuniętych urządzeń końcowych. Również dotychczasowa nazwa użytkownika i hasło do aktywacji produktów Eset zostały



▶ Eset Endpoint Security – ustawienia aplikacji na stacji roboczej



Konsola Remote Administrator - panel główny

zastąpione prostym i wygodnym kluczem licencyjnym, z którego wspólnie korzystają wszystkie zakupione rozwiązania biznesowe. Nowe licencjonowanie obejmuje również dotychczas używane produkty i dla obecnych klientów istnieje możliwość zamiany loginu i hasła na nowy format klucza licencyjnego.

Znaczącej zmianie uległa również koncepcja centralnego zarządzania produktami Eset. Konsola zarządzania (Eset Remote Administrator) została przebudowana od podstaw. Uwzględniając sugestie administratorów, którzy musieli na co dzień pracować przy konfiguracji i monitorowaniu produktów Eset oraz mając na uwadze coraz popularniejsze wykorzystywanie urządzeń mobilnych, interfejs został przebudowany w taki sposób, aby wszystko było przejrzyste i czytelne bez względu na wykorzystywaną platformę.

PRODUKTY ESET W PRAKTYCE

Mając na uwadze dotychczasowe, raczej pozytywne doświadczenia związane z używaniem produktów Eset na platformach

klienckich oraz serwerowych postanowiliśmy sprawdzić, jak działają nowe rozwiązania, przechodząc całą ścieżkę od momentu zamówienia, do instalacji i konfiguracji w symulowanym środowisku firmowym.

Rozpoczęliśmy od zalogowania się do konsoli zarządzania licencjami. Po zamówieniu odpowiedniej liczby licencji do naszego środowiska testowego otrzymaliśmy z firmy Eset email z kluczem licencyjnym do aktywacji zamówionych elementów oraz wszystkimi niezbędnymi informacjami koniecznymi do zarządzania i instalacji. Warto wspomnieć, że jeśli klient wybierze jednak do instalacji produkty w wersji 5 lub starszej, do wiadomości dołączone są również nazwa użytkownika i hasło niezbędne do aktywacji w starym modelu licencjonowania. Dodatkowo mail zawiera Identyfikator Publiczny, który służy do identyfikacji licencji przez osobę trzecią, na przykład administratora odpowiedzialnego za bezpieczeństwo oraz zarządzanie i dystrybucję środowiska Eset.

Ze względów bezpieczeństwa nie wszystkie informacje

konieczne do zalogowania się do konsoli Eset License Administrator (ELA) przesyłane są w pojedynczej wiadomości. W kolejnej klient dostaje hasło do konsoli, które w połączeniu z kluczem licencyjnym należy użyć do pierwszego zalogowania i zarejestrowania licencji. W ELA można również w razie potrzeby wskazać dodatkowo administratora licencji.

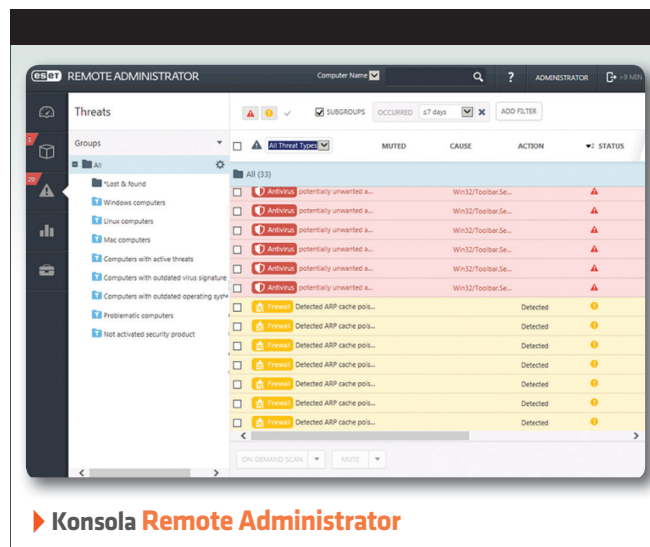
Konsola Eset License Administrator jest skonstruowana w niezwykle prosty sposób. Składa się z kilkuelementowego menu, gdzie po kliknięciu dowolnie wybranej pozycji w centralnej części ekranu wyświetlają się możliwe do określenia opcje. Każdy, kto zarządza dystrybucją licencji w firmie może tu sprawdzić, które elementy są już wykorzystane oraz ile z nich pozostaje jeszcze do dyspozycji na nowe urządzenia końcowe.

CENTRALNE ZARZĄDZANIE

Żadna firma nie obejdzie się bez centralnego zarządzania infrastrukturą, w tym aplikacjami odpowiedzialnymi za bezpieczeństwo stacji roboczych, serwerów oraz urządzeń mobilnych. Dlatego w kolejnym kro-

ku sprawdziliśmy działanie Eset Remote Administrator.

Mimo że to produkt całkowicie zmieniony, bez problemu obsługuje starsze wersje aplikacji Eset. W przypadku wątpliwości, na stronie producenta można znaleźć listę produktów, których obsługa jest wspierana przez nową konsolę administracyjną. Eset Remote Administrator to nie tylko sama konsola. Jest to cały system, który pozwala na skuteczne centralne zarządzanie systemem bezpieczeństwa opartym na produktach Eset. Składa się z kilku elementów, które wspólnie tworzą wydajne narzędzie do kontroli zainstalowanych aplikacji. Podstawą jest Remote Administrator Server, który jest silnikiem całego systemu. Do tego konsola webowa oparta na platformie Tomcat, umożliwiająca dostęp z dowolnego miejsca przy użyciu jedynie przeglądarki internetowej. Do składowania danych i statystyk wykorzystywanych przez serwer zarządzający użyty jest jeden z dwóch silników bazodanowych w zależności od systemu, pod którym pracuje Remote Administrator Server. Jest to MS SQL w wersji Express dla



Konsola Remote Administrator

Windows Server oraz MySQL, jeśli serwer zainstalowany jest pod Linuxem.

Wersje instalacyjne wszystkich produktów dostępne są do pobrania na stronie Eset, a w przypadku konsoli Remote Administrator mamy do wyboru kilka wariantów. Podstawowy z nich to instalacja *all-in-one* przeznaczona na 32- i 64-bitowe systemy Windows, zawierająca wszystkie niezbędne do działania komponenty. Zamiennie można ściągnąć instalatory samego Remote Administrator Server bez dodatkowych komponentów przeznaczonych na platformy Windows, Linuks oraz OS X.

Specjalnie dla środowisk wirtualnych utworzono obrazy maszyn dla Remote Administrator Server, Remote Administrator Proxy oraz osobno z modułem zarządzania urządzeniami mobilnymi. Należy wspomnieć, że wersja proxy jest wykorzystywana do komunikacji z głównym serwerem w przypadku, gdy firma posiada infrastrukturę rozproszoną w odległych lokalizacjach. Sama instalacja

przebiega raczej bez problemu, tym bardziej że produkty Eset dają możliwość wyboru języka polskiego już na poziomie instalacji, co znacznie ułatwia sprawę choćby w przypadku wyboru komponentów.

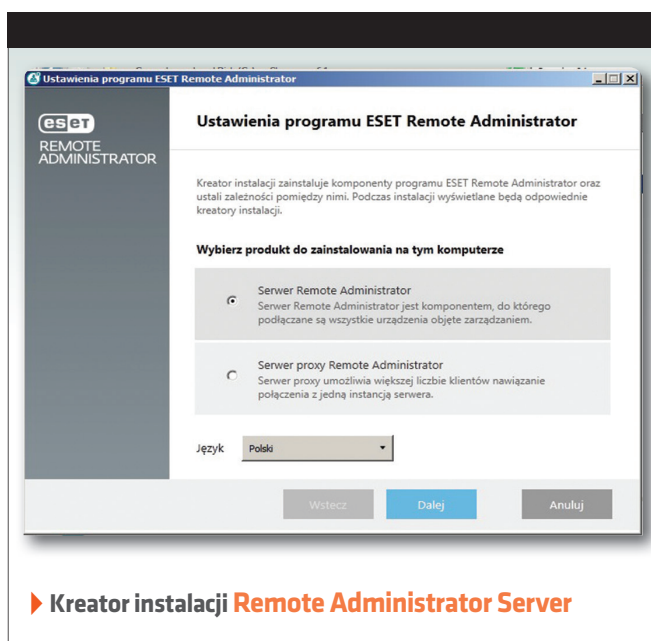
Konsola administracyjna pozwala na centralną administrację produktami zainstalowanymi zarówno na stacjach roboczych, jak i serwerach, a także na urządzeniach mobilnych. Główna zaleta polega na tym, że z poziomu jednego miejsca można zrobić te same operacje, które realizuje się w konfiguracji bezpośrednio na aplikacji zabezpieczającej, a dodatkowo Remote Administrator umożliwia wykonanie tych samych czynności dla wielu stacji lub użytkowników jednocześnie. Centralne polityki bezpieczeństwa można tworzyć na podstawie pojedynczych elementów identyfikacyjnych, jak również na podstawie grup. Dzięki możliwości integracji z wieloma domenami Active Directory w prosty sposób można utworzyć grupy dynamiczne, przez co nowy użytkownik lub komputer

spełniający wymagania zostanie przypisany do odpowiedniej polityki.

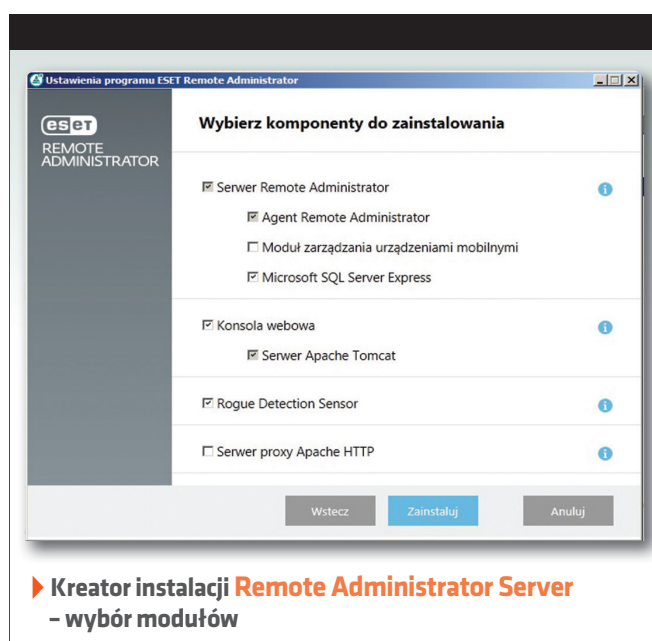
Ciekawym narzędziem, z którego może skorzystać administrator jest Rogue Detection Sensor. Jest to skaner sieciowy pomagający wykryć w infrastrukturze firmowej końcówki, które nie mają jeszcze zainstalowanej ochrony lub takie, które mimo że zawierają aplikacje Eset, nie zgłaszają się do serwera zarządzającego. Równie przydatną aplikacją jest darmowy Eset SysInspector, który generując raporty o stanie systemu pomaga diagnozować problemy z komputerem, w tym brak możliwości instalacji produktów Eset.

Sama konsola administracyjna została zorganizowana w taki sposób, aby wszystko można było łatwo w niej znaleźć bez względu na urządzenie i przeglądarkę, z której się korzysta. Elementy są rozmieszczone i opisane w prosty i przejrzysty sposób, tak że korzystając po raz pierwszy bardzo łatwo znaleźć poszukiwane opcje. Menu znajdujące

się po lewej stronie podzielone jest na kilka obszarów, z których każdy pełni inną rolę. *Panel kontroli* zawiera aktualne statystyki w postaci wykresów. Elementy wyświetlane w panelu można dowolnie dostosowywać do własnych potrzeb, dzięki czemu każdy administrator może wyświetlać jedynie najważniejsze dla siebie informacje. Kolejne obszary to *Komputery* i *Zagrożenia*. Pierwszy z nich zawiera listę wszystkich urządzeń, jakie zostały rozpoznane przez system łącznie z tymi, które nie posiadają zainstalowanych aplikacji Eset. Występuje tu podział na grupy dynamiczne (do których stacje są automatycznie przypisane z uwagi na filtry) lub statyczne utworzone na potrzeby administratora. Z poziomu tego obszaru można całkowicie zarządzać ochroną i konfiguracją zabezpieczeń wszystkich elementów końcowych zarówno komputerów, jak i urządzeń mobilnych czy serwerów. Trzeba przyznać, że konsola administracyjna oferuje bardzo dużo, jeśli chodzi o uzyskiwanie informacji o chronionych systemach



▶ Kreator instalacji Remote Administrator Server



▶ Kreator instalacji Remote Administrator Server - wybór modułów

Pakiety licencji:	Zawartość pakietów:	OCHRONA KOMPUTERÓW POZIOM ANTIWIRUS	OCHRONA KOMPUTERÓW POZIOM SECURITY	OCHRONA URZĄDZEŃ MOBILNYCH	OCHRONA SERWERÓW PLIKOWYCH	OCHRONA SERWERÓW POCZTOWYCH	OCHRONA BRAMY INTERNETOWEJ	KONSOLA CENTRALNEGO ZARZĄDZANIA
ESET Secure Enterprise		✓	✓	✓	✓	✓	✓	✓
ESET Secure Enterprise AV Level		✓	✓	✓	✓	✓	✓	✓
ESET Secure Business		✓	✓	✓	✓	✓	✓	✓
ESET Secure Business AV Level		✓	✓	✓	✓	✓	✓	✓
ESET Endpoint Security Suite		✓	✓	✓	✓	✓	✓	✓
ESET Endpoint Antivirus Suite		✓	✓	✓	✓	✓	✓	✓
ESET Endpoint Security		✓	✓	✓	✓	✓	✓	✓
ESET Endpoint Antivirus		✓	✓	✓	✓	✓	✓	✓

► **Nowy pakiet licencji produktów Eset**

oraz pozwala na zaawansowane działania na urządzeniach końcowych, włączając w to deinstalację oprogramowania, wiele poziomów blokowania dostępu do zasobów fizycznych oraz treści internetowych (w ponad 140 kategoriach). Konsola zarządzania pozwala również na pełną automatyzację podstawowych czynności administracyjnych, począwszy od wykrywania urządzeń końcowych, przez zdalną instalację agentów, po planowanie skanowania zarówno dla pojedynczych końcówek, jak i dla całych grup. Wszystkie zaawansowane funkcje wykonywane na systemach mogą również zostać spersonalizowane w zależności od rodzaju użytkownika korzystającego z danego zasobu objętego ochroną.

W części *Zagrożenia* administrator znajdzie komunikaty z problemami dotyczącymi chronionych obiektów podzielone na kategorie wskazujące, jakiego obszaru dotyczą i czy są związane z atakiem sieciowym, czy może z zagrożeniem infekcją.

Konsola Remote Administrator ma również możliwość wygenerowania kilkudziesięciu raportów o stanie chronionych zasobów oraz zdarzeniach, które

na nich nastąpiły, co pozwala administratorom znaleźć słabe punkty w obsługiwanej infrastrukturze.

URZĄDZENIA KOŃCOWE

Aplikacje Eset w wersji dla biznesu z centralnym zarządzaniem pracują w architekturze klient-serwer. Klientem jest tutaj agent zainstalowany na urządzeniu końcowym, który komunikuje się z serwerem Remote Administrator. O ile najprościej zainstalować agenta zdalnie za pomocą centralnej konsoli, to istnieje również możliwość ręcznej instalacji agenta oraz aktywowania na nim licencji z pliku, w przypadku gdy jest to system całkowicie

odizolowany od sieci z serwerem Remote Administrator.

Firma Eset w przypadku zastosowania swoich produktów w firmie oferuje ochronę nie tylko stacji roboczych oraz urządzeń mobilnych. Najwyższy poziom ochrony dostarczany jest również dla serwerów, które pełnią w infrastrukturze przedsiębiorstwa różne role. W ofercie znajdują się produkty chroniące usługi, przetwarzające duże ilości plików i informacji, skierowane w szczególności dla serwerów plików oraz serwerów pocztowych. Ochronę można zapewnić również instalując produkt przeznaczony dla bram internetowych, który skutecznie realizuje polityki bezpieczeństwa w zakresie odpierania ataków z zewnątrz oraz realizacji polityk kontroli dostępu z poziomu wewnętrznej infrastruktury.

W ramach nowej wersji swoich produktów firma Eset oferuje dla biznesu elastyczne pakiety oprogramowania w ramach licencji na konkretne rozwiązania. Należy również pamiętać, że w każdym z nich można wybrać dwa poziomy zabezpieczenia. Jeden, jako kompleksowa ochrona całego systemu na poziomie Security lub ewentualnie tylko na poziomie Antivirus.

Podstawowe pakiety licencyjne Eset Endpoint Security lub Antivirus obejmują jedynie stacje robocze, urządzenia mobilne i konsolę centralnego zarządzania, natomiast wyższe pakiety Eset Endpoint Suite i Eset Secure Business występują z dodatkową ochroną serwerów plików i poczty. Wersja z maksymalną ochroną przedsiębiorstwa Eset Secure Enterprise zawiera wszystkie komponenty pakietów niższych, a ponadto oferuje ochronę bramy internetowej.

PODSUMOWANIE

Nowe wersje produktów Eset zapewniają wysoki poziom zabezpieczeń przy niskim zużyciu zasobów systemowych. Wprowadzone zmiany podniosły funkcjonalność aplikacji oraz rozszerzyły wachlarz obsługiwanych urządzeń i systemów. Mając na uwadze zagrożenia płynące z coraz powszechniej używanych urządzeń mobilnych, pójście w tym kierunku wydaje się strzałem w dziesiątkę, a uruchomienie elementów zarządzania w postaci platformy webowej i dostosowanie jej w szczególności do urządzeń przenośnych powoduje, że kontrolę nad infrastrukturą można pełnić bez względu na miejsce. O tym, że Eset swoimi produktami może objąć infrastrukturę rozproszoną świadczy również fakt, że cały system zarządzania Remote Administrator można podzielić na poszczególne moduły, gdzie w przypadku odrębnych lokalizacji w szczególności przydaje się proxy.

Zmiana zarządzania licencjami, sposobu aktywacji produktów oraz podział na kilka pakietów o różnym poziomie ochrony według nas przysłużą się do tego, że klienci, którzy poważnie myślą o kompleksowym bezpieczeństwie swoich systemów chętniej sięgną po produkty firmy Eset. ■

