Test: ESET PROTECT to więcej niż antywirus i firewall s. 63

Obrona przed atakami DDoS s. 46

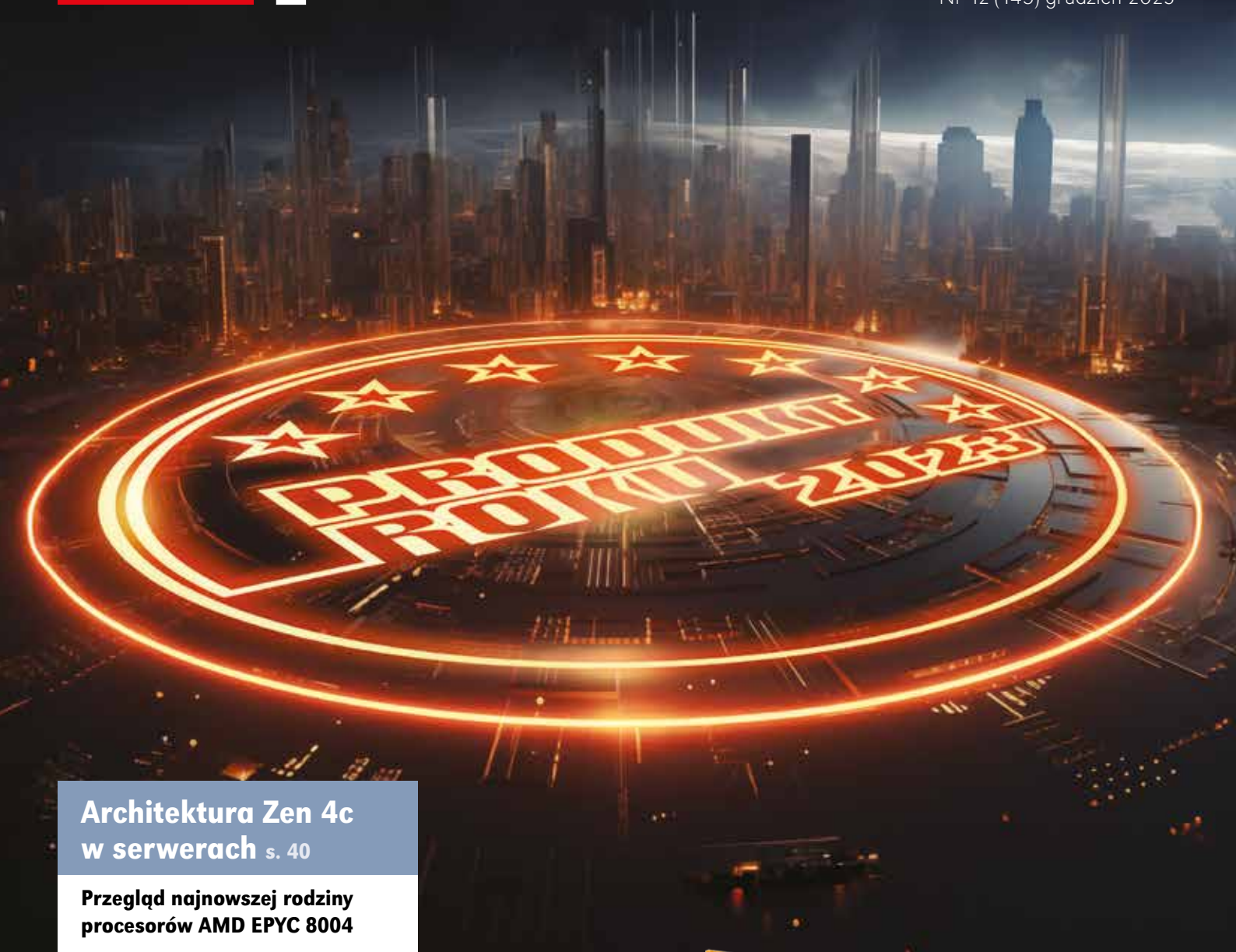
12
2023

Miesięcznik informatyków i menedżerów IT

itprofessional.pl

IT professional

Nr 12 (145) grudzień 2023



Architektura Zen 4c w serwerach s. 40

Przegląd najnowszej rodziny procesorów AMD EPYC 8004

Scenariusze ataków chmurowych na przykładzie AWS s. 51

Techniki i narzędzia etycznego hakowania środowisk cloudowych oraz ich ochrony

KSIĄŻKA GRATIS

Standardy zarządzania cyberbezpieczeństwem

Cena 41,00 zł (w tym 8% VAT)
ISSN 2083-9588
9 772083 958004

DOSTĘPNE E-WYDANIE

Od ponad 30 lat ESET oferuje rozwiązania dotyczące bezpieczeństwa przedsiębiorcom i klientom indywidualnym. Wydaje się, że w tym czasie do firmy przylgnęła łatka dostawcy antywirusa, jednak jest to tylko jeden z elementów w gamie narzędzi oferowanych przez ESET.

12/2023 REKOMENDACJA REDAKCJI IT professional

ANALIZA INFRASTRUKTURY IT

ESET PROTECT to więcej niż antywirus i firewall

Piotr Maziakowski

Rozwiązania ESET obejmują wiele narzędzi bezpieczeństwa, w tym wielowarstwową ochronę punktów końcowych i serwerów przed zagrożeniami takimi jak ransomware, phishing, botnety czy ataki zero-day, wykrywanie i reagowanie na punktach końcowych (XDR) oraz narzędzia do zarządzania szyfrowaniem czy dwuskładnikowym uwierzytelnieniem. W artykule skupimy się na funkcjonalnościach biznesowego pakietu ESET PROTECT Elite opartego na konsoli ESET PROTECT Cloud.

ESET PROTECT Cloud to rozwiązanie chmurowe do zarządzania bezpieczeństwem stacji roboczych i serwerów. Konsola umożliwia sprawne wdrażanie, monitorowanie i aktualizowanie narzędzi zabezpieczających ESET. PROTECT Cloud zapewnia również zaawansowaną ochronę oraz pozwala na tworzenie polityk bezpieczeństwa i zarządzanie nimi, generowanie raportów i alertów, a także zdalne zarządzanie urządzeniami mobilnymi i stacjami roboczymi.

Podstawowe funkcje ESET PROTECT Cloud to:

- wdrażanie, monitorowanie i aktualizowanie oprogramowania antywirusowego oraz zabezpieczającego na wszystkich urządzeniach w sieci;
- ochrona przed zagrożeniami, takimi jak ransomware, phishing, botnety czy ataki zero-day, dzięki inteligentnym mechanizmom wykrywania i blokowania;
- tworzenie dostosowanych polityk i zarządzanie nimi;
- raportowanie i alertowanie o zagrożeniach oraz kondycji urządzeń;
- zdalne zarządzanie urządzeniami mobilnymi i stacjami roboczymi umożliwiające blokowanie urządzeń, usuwanie danych, lokalizowanie czy instalowanie aplikacji.

Różnorodność licencji pozwala dopasować produkt do potrzeb organizacji.

Rys. 1. Konsola administracyjna ESET PROTECT.

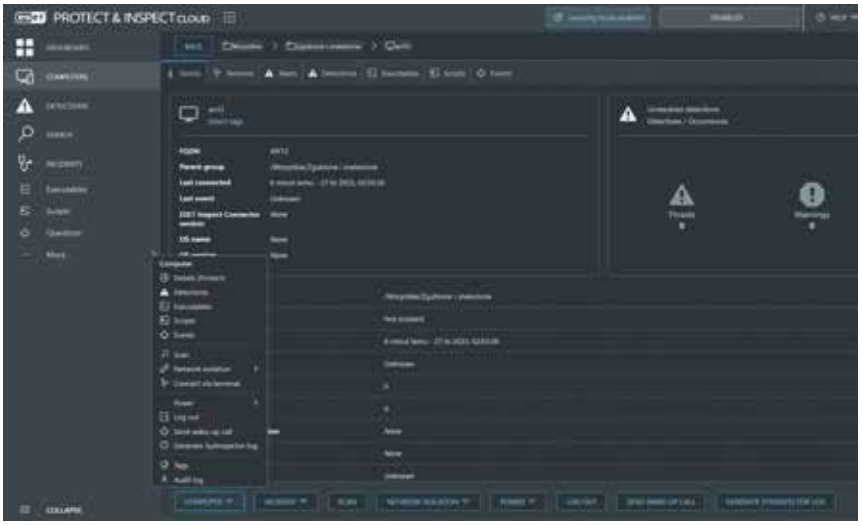
> PIERWSZE KROKI

Aktywowanie konsoli ESET PROTECT wymaga wygenerowania dostępu, poprzez przypisanie licencji, w portalu ESET Business Account (EBA). EBA to platforma internetowa, która umożliwia zarządzanie licencjami, produktami i usługami oferowanymi przez ESET. Pozwala na centralne monitorowanie i kontrolowanie, ile urządzeń jest chronionych i które licencje zostały do nich przypisane. Z poziomu EBA możemy m.in. udostępnić licencje w oddziałach firmy (lokacje w EBA), np. poprzez zwalnianie licencji z nieaktywnych urządzeń, które po określonym czasie mogą zostać przypisane do innego urządzenia, przypisywać użytkowników do określonych lokacji, włączać 2FA dla użytkowników EBA oraz konfigurować powiadomienia e-mail informujące o stanie licencji (w tym

zbliżającym się wygaśnięciu, możliwym nadużyciu licencji czy zbyt wielu jej aktywacjach). Ze względu na techniczne informacje, które po podłączeniu urządzeń zawiera EBA (m.in. dane o licencjach aktywowanych na stacjach i serwerach czy lokacjach firmy), warto skorzystać z włączenia uwierzytelniania dwuskładnikowego. Uruchomienie 2FA jest proste i polega na użyciu jednorazowych haseł generowanych w aplikacji mobilnej ESET Secure Authentication (ESA), a na wypadek braku dostępu do urządzenia z ESA prześlemy na adres e-mail kody zapasowe umożliwiające zalogowanie.

Po zarejestrowaniu licencji w portalu EBA przechodzimy do głównej konsoli administracyjnej ESET PROTECT Cloud (**rys. 1**). Nie jest wymagane każdorazowe logowanie do EBA. Docelowo możemy logować się bezpośrednio w konsoli Protect tymi samymi poświadczeniami co w przypadku logowania do konsoli EBA.

Nawigacja jest bardzo intuicyjna. Panel kontrolny podzielono na zakładki, co pozwala na dostęp do praktycznie wszystkich najważniejszych informacji. Na pierwszym ekranie otrzymujemy podstawowe dane o statusie urządzeń oraz zidentyfikowanych najnowszych zagrożeniach. Z tego miejsca możemy przechodzić do podglądu informacji o incydentach z ostatnich siedmiu dni, szczegółów urządzeń, wykryć system antywirusowy, zapory i stan aplikacji ESET. Skonfigurujemy również własny widok panelu, dodając widoki z predefiniowanych szablonów, które także dostosowujemy do własnych potrzeb. Po lewej stronie ekranu znajdują się od góry główne pozycje menu, takie jak: Pulpit nawigacyjny, Komputery, Wykrycia i Luki w zabezpieczeniach, a pozostałe sekcje, przede wszystkim konfiguracyjne, są poniżej. Taki rozkład funkcji ułatwia w pierwszej kolejności dotarcie do tego, co najważniejsze. Ogromna ilość danych prezentowanych w panelu kontrolnym, możliwości konfiguracyjne oraz intuicyjna nawigacja pozwalają na sprawny przegląd stanu bezpieczeństwa oraz łatwe i szybkie podjęcie działań w przypadku zagrożeń. Każdy wykres pierścieniowy można kliknąć, aby wyświetlić widok szczegółowy. Zagrożenia da się np. przeanalizować na poziomie systemu, sprawdzić każde zagrożenie pod kątem podjętych działań i oznaczyć je jako rozwiązane.



Rys. 2. Konsola ESET Inspect.

ESET PROTECT Cloud to rozwiązanie chmurowe do zarządzania bezpieczeństwem stacji roboczych i serwerów. Konsola umożliwia sprawne wdrażanie, monitorowanie i aktualizowanie narzędzi zabezpieczających ESET.

> DODAWANIE URZĄDZEŃ

Po zapoznaniu się z pulpitem nawigacyjnym przechodzimy do dodawania urządzeń. Istnieje kilka sposobów wdrożenia narzędzi ESET na końcówkach. ESET PROTECT Cloud umożliwia utworzenie własnego, niestandardowego instalatora z jednoczesnym wskazaniem domyślnej polityki do zastosowania oraz komponentów, które domyślnie zostaną uruchomione.

Po utworzeniu instalatora wdrożymy go na końcówkach na kilka sposobów. Można wygenerować obiekt zasad grupy (GPO) lub skrypt Menedżera konfiguracji programu System Center (SCCM). W przypadku instalacji systemu Linux konieczne będzie wygenerowanie skryptu instalatora agenta lub wykonanie czynności ręcznych. Ewentualnie skorzystajmy z narzędzia ESET Remote Deployment Tool, które umożliwia dystrybucję pakietów instalatora za pośrednictwem sieci dzięki wybranej opcji:

- Active Directory – poprzez wyeksportowanie struktury usługi Active Directory w celu jej późniejszego zaimportowania do programu ESET PROTECT Cloud;
- skanowanie sieci zgodnie ze wskazanym zakresem adresów;
- importowanie listy stacji końcowych na podstawie nazw hostów lub adresów IP;
- ręczne dodawanie komputerów poprzez podanie nazw hostów lub adresów IP ręcznie.

Po zarejestrowaniu urządzeń w ESET PROTECT dostosowujemy ich ustawienia, przypisując właściwe polityki bezpieczeństwa, np. możemy skonfigurować program antywirusowy, ustawienia aktualizacji oprogramowania, zaporę ogniową, skanowanie sieci i poczty e-mail, kontrolę urządzeń. Wdrożenie rozszerzymy na smartfony i tablety, instalując moduł zarządzania urządzeniami mobilnymi – MDM.

Zarządzanie politykami w ESET PROTECT bywa uciążliwe. Co prawda większość istotnych funkcji jest prosta i oczywista, ale niektóre polityki wyjaśniono w taki sposób, że ich zrozumienie wymaga czasu, a nawet zajrzenia do dokumentacji. Wyświetlając szczegóły jednej z polityk, otrzymujemy informacje: „Ta polityka włącza lub wyłącza wiele ustawień dla wszystkich odpowiednich urządzeń w sieci. Wyświetl szczegóły polityk, aby uzyskać więcej informacji o określonych ustawieniach. Tę politykę można edytować za pomocą akcji konfiguracji ochrony w menu kontekstowym lub szybkich łączy”.

> SZCZEGÓŁOWE RAPORTOWANIE

Moduł raportowania to jedna z mocniejszych stron ESET PROTECT. Zawiera bardzo dużo wystarczająco szczegółowych raportów, aby zadowolić najbardziej wymagające osoby. Każdy raport ma również szybki podgląd.

Wszystkie najważniejsze zdarzenia (rodzaj zagrożeń, wykorzystywane moduły, podjęte działania, pełny dziennik audytu zmian wprowadzonych w konsoli z informacją, kto i kiedy wprowadził zmiany w politykach) są raportowane w łatwy do śledzenia sposób. Moduł raportowania podzielono na sekcje dostępne z lewej strony, a dostęp do szczegółowych raportów widzimy w głównej części ekranu. Każdy raport możemy wygenerować na żądanie lub zaplanować wysyłkę na wskazany adres e-mail. Dodatkowo stworzymy własne szablony raportów, definiując ich zawartość z niezwykle bogatej listy informacji. Platforma ESET PROTECT udostępnia ponad 170 wbudowanych raportów i pozwala na tworzenie niestandardowych raportów z ponad 1000 punktów danych.

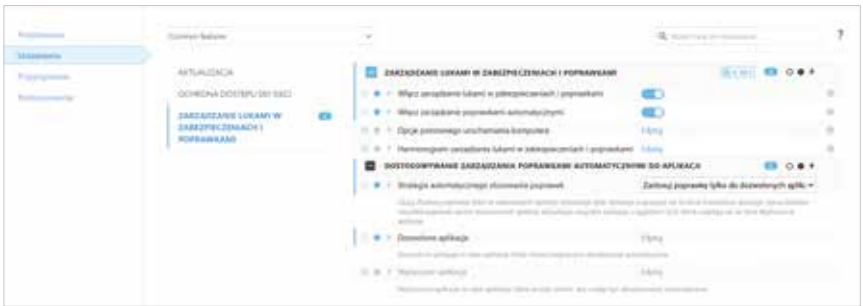
Rys. 3. Cloud Office Security – ochrona przed phishingiem.

> ROZSZERZONE WYKRYWANIE I REAGOWANIE (EDR)

W programie ESET PROTECT nie brakuje również funkcji EDR. Choć funkcjonalność jest dostępna w pakiecie Elite, warto zaznaczyć, że tego rodzaju technologia może znacząco pomóc administratorom w przestawieniu się z reaktywnych zabezpieczeń na bardziej proaktywną ochronę dzięki możliwości identyfikacji punktów wejścia dla zagrożeń. Za funkcjonalność EDR odpowiada konsola ESET Inspect, jako element dla platformy ESET PROTECT. Umożliwia identyfikację nietypowych zachowań i naruszeń, ocenę ryzyka, reakcję na incydenty, dochodzenie i naprawę. Konsola ESET Inspect zawiera kilka pulpitów nawigacyjnych (**rys. 2**).

Pulpit Detections pokazuje nierozwiązane wykrycia, ich wagę i częstotliwość oraz umożliwia łatwy dostęp do szczegółów poprzez kliknięcie nazwy wykrycia. Każde wykrycie zawiera szczegółowe wyjaśnienie wraz z prawdopodobnymi przyczynami, a także zalecane działania, które należy podjąć, aby ocenić wykrycie i mu zaradzić. Jeśli wykrycie zostanie uznane za złośliwe, za pomocą kilku kliknięć da się wdrożyć działanie, pomimo iż wiele reguł wykrywania ma wbudowane automatyczne reagowanie. Możemy też wybrać, jakie działania mają zostać podjęte automatycznie w przypadku wykrycia zagrożenia, np. automatyczne zablokowanie plików wykonywalnych i odizolowanie stacji od sieci. Niektórymi elementami ESET Inspect, jak komputery lub prawa dostępu, można zarządzać z poziomu konsoli ESET PROTECT.

Sekcje Executables i Scripts przedstawiają odpowiednio wszystkie pliki wykonywalne zidentyfikowane na urządzeniach w sieci i skrypty uruchomione w sieci. Pliki wykonywalne można



Rys. 4. Funkcje zarządzania poprawkami.

szczegółowo przeglądać, aby określić ich przeznaczenie i potencjalne zagrożenie, jakie mogą stwarzać. Jednocześnie dla ułatwienia oceny wyświetlane są w tym miejscu informacje o reputacji zebrane z ESET LiveGrid. Niestety konsola ESET Inspect obsługuje tylko język angielski.

> SZYFROWANIE DYSKÓW

Z poziomu konsoli ESET PROTECT możemy wdrożyć szyfrowanie dysków na zarządzanych endpointach. Warto zwrócić uwagę, że narzędzie ESET Full Disk Encryption – choć bardzo upraszcza wdrożenie szyfrowania, gdyż jego włączenie i monitorowanie jest dostępne z poziomu jednego narzędzia – to zaledwie część ESET Endpoint Encryption. Endpoint Encryption to kompleksowe rozwiązanie do szyfrowania z szeroką gamą opcji. Pozwala szyfrować dane na dyskach twardych, przenośnych nośnikach danych, w wiadomościach e-mail czy zasobach sieciowych.

> OCHRONA USŁUG CHMUROWYCH

Kolejną nowością w palecie narzędzi ESET jest ESET Cloud Office Security (**rys. 3**). Narzędzie pozwala na integrację ze środowiskami chmurowymi Microsoft 365 oraz Google Workspace i ich ochronę (w tym poczty elektronicznej) przed zagrożeniami. To ochrona przed malware'em i wirusami na poziomie plików np. zlokalizowanych na OneDrive czy w plikach poczty elektronicznej. Filtracja poczty elektronicznej oferuje ochronę poczty Exchange Online lub Gmail poprzez filtrowanie wiadomości spam, blokowanie potencjalnie niebezpiecznych załączników lub linków wyłudzających oraz stanowi wsparcie ochrony przed atakami phishingowymi. Pozwala na kontrolę dostępu do zawartości w poczcie elektronicznej, blokowanie niebezpiecznych treści i monitorowanie aktywności użytkowników. Umożliwia administratorom definiowanie polityk dotyczących skanowania, blokowania czy filtrowania i zarządzanie nimi. W prosty sposób integruje się z najpopularniejszymi usługami chmurowymi, jak Microsoft 365 czy Google Workspace, i pozwala na równoległe zarządzanie nimi.

> ZARZĄDZANIE LUKAMI I POPRAWKAMI

To kolejna niezwykle przydatna funkcja (**rys. 4**). Aby wdrożyć zarządzanie poprawkami, należy zdefiniować politykę common features. Dzięki niej będą usuwane luki wykryte w zabezpieczeniach poprzez zautomatyzowane aktualizacje oprogramowania. Funkcja umożliwia wdrożenie zasad instalacji poprawek dla wielu popularnych aplikacji, których lista jest ciągle aktualizowana. Poprawki mogą być instalowane domyślnie zgodnie z listą dozwolonych aplikacji lub ręcznie po zatwierdzeniu. Zarządzanie lukami w zabezpieczeniach i poprawkami można uruchomić tylko na komputerach z systemem Windows, a funkcjonalność dostępna jest jedynie w pakiecie ESET PROTECT Elite.

Autor od 2004 r. związany z branżą IT i nowych technologii w obszarze administrowania systemami klasy ERP. Specjalizuje się w realizacji wdrożeń i audytów bezpieczeństwa informacji.

PODSUMOWANIE

ESET PROTECT w ostatnich latach stale ewoluuje, i to w bardzo dobrym kierunku. Bezsprzecznie jest to solidna platforma ochrony, a usprawnienia interfejsu sprawiają, że jest łatwiejsza i bardziej intuicyjna w obsłudze. W porównaniu z wcześniejszymi wersjami technologii firmy ESET interfejs konsoli PROTECT Cloud jest dużo bardziej przyjemny w obsłudze. Minimalny zakup dla PROTECT Elite to 26 sztuk, a cena rocznej subskrypcji wynosi 385,23 zł netto (26–49 stanowisk). Cena jednostkowa wraz ze zwiększaniem chronionego środowiska się zmniejsza, od niej naliczane są promocje, np. GOV dla instytucji publicznych czy EDU dla organizacji edukacyjnych. W tej cenie otrzymujemy kompletne narzędzie, łatwe we wdrożeniu i konfiguracji, z gotowymi zasadami bezpieczeństwa, z których wybieramy te najbardziej dopasowane do potrzeb organizacji, z przyjaznym dashboardem prezentującym na bieżąco stan każdego urządzenia, możliwością instalacji agentów w zróżnicowanym środowisku (Windows, MAC, Linux, iOS, Android) oraz z zaawansowanymi funkcjami bezpieczeństwa poczty Exchange i Gmail.

Werdykt

ESET PROTECT Elite

Zalety

- duże możliwości dostosowania panelu sterowania
- intuicyjny interfejs
- obsługa wielu systemów
- zarządzanie poprawkami i aktualizacjami
- ochrona usług chmurowych
- rozbudowane raportowanie
- automatyzacja zadań

Wady

- wysoka cena wersji Elite

Ocena **9**/10