Wymagania minimalne dla zadania:

Wdrożenie systemu służącego do wykrywaniu i reagowaniu na podejrzane aktywności na urządzeniach końcowych klasy EDR (Endpoint Detection and Response) wraz ze szkoleniem

Cel Zamówienia:

Zakup system klasy EDR na potrzeby Urzędu Miejskiego w Strzegomiu wraz ze szkoleniem.

Informacje wstępne:

W związku z rozszerzeniem procesów bezpieczeństwa systemów informatycznych przedmiotem zamówienia jest rozszerzenie istniejącego sytemu antywirusowego o funkcjonalności EDR (Endpoint Detection and Response), służącemu wykrywaniu i reagowaniu na podejrzane aktywności na urządzeniach końcowych.

Zamawiający obecnie posiada wdrożone oprogramowania firmy ESET o identyfikatorze publicznym 33B-TJ3-PB7 z licencją ESET PROTECT Essential Plus ON-PREM, obejmującą 160 stanowisk, ważną do dnia 10-03-2025. Zamawiający planuje rozszerzenie istniejącej licencji o funkcje EDR tj. do licencji ESET PROTECT Enterprise, obejmującą 120 stanowisk. Licencja na 24 miesiące od dnia dostawy przez wykonawcę.

Wykonawca zobowiązany jest do przeszkolenia dwóch osób zgodnie z poniższą specyfikacją.

Wykonawca zobowiązuję się do wdrożenia zakupionego systemu – minimum 2 godziny, zdalnie.

Zamawiający dopuszcza rozwiązanie równoważne pod warunkiem spełniania wymagań poniższej specyfikacji oraz będące kompatybilne lub spełniające tożsame funkcjonalności obecnie wdrożone wynikające z licencji ESET PROTECT Essential Plus ON-PREM. Koszt rozwiązania równoważnego musi zawierać koszty wdrożenia rozwiązania, przeniesienia funkcjonalności obecnego rozwiązania oraz przynajmniej dwudniowego szkolenia dwóch administratorów w siedzibie zamawiającego z zarządzania i konfiguracji rozwiązania wraz z minimum półrocznym wsparciem powdrożeniowym.

Wymagania minimalne	
Administracja	1. Wsparcie instalacji na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD. 2. Zapewnienie instalacji z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL. 3. Pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta. 4. Dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL. 5. Zabezpieczona komunikacja pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów. 6. Utworzenie własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi. 7. Centralna konfiguracja i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci. 8. Weryfikacja podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe). 9. Instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT. 10. Wymuszenie dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 11. Możliwość tworzenia grup statycznych i dynamicznych komputerów. 12. Tworzenie grup dynamicznych na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 13. Korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz tworzenie własnych raportów przez administratora. 14. Wysłanie powiadomienia przynajmniej za pośrednictwem

	wiadomości email, komunikatu SNMP oraz do dziennika syslog. 15. Podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
Ochrona stacji roboczych	1. Wsparcie systemów operacyjnych Windows (Windows 10/Windows 11). 2. Wsparcie architektury ARM64. 3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Wbudowana technologia do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Opcja umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP w czasie rzeczywistym, zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od klienta pocztowego). 11. Skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 12. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 13. Blokowanie zewnętrznych nośników danych na stacji, w tym przynajmniej: pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 14. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, umożliwiająca tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 15. Moduł HIPS z możliwością pracy w jednym z pięciu trybów: • reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to rozwiązanie pyta

	użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program automatycznie przełącza się w tryb pracy oparty na regułach, • tryb inteligentny, w którym rozwiązanie powiadamia wyłącznie o szczególnie podejrzanych zdarzeniach. 16. Wbudowana funkcja generująca pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 17. Funkcja generująca logi, posiadająca przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane i mogą stanowić zagrożenie bezpieczeństwa. 18. Automatyczna, inkrementacyjna aktualizacja silnika detekcji. 19. Jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 20. Funkcjonalność skanera UEFI, chroniąca użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 21. Ochrona antyspamowa dla programu pocztowego MS Outlook. 22. Zapora osobista pracująca w jednym z czterech trybów: • tryb automatyczny – blokowanie całego ruchu przychodzącego i zezwalanie tylko na połączenia wychodzące, • tryb interaktywny – pytanie o każde nowo nawiązywane połączenie, • tryb oparty na regułach – blokowanie całego ruchu przychodzącego i wychodzącego, zezwalanie tylko na połączenia skonfigurowane przez administratora, • tryb uczenia się – automatyczne tworzenie nowych reguł zezwalających na połączenia przychodzące i wychodzące. Możliwość konfigurowania czasu działania trybu przez administratora. 23. Moduł bezpiecznej przeglądarki. 24. Automatyczne szyfrowanie wszelkich danych wprowadzanych przez użytkownika w bezpiecznej przeglądarce. 25. Praca w bezpiecznej przeglądarce wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. 26. Zintegrowany moduł kontroli dostępu do stron internetowych. 27. Możliwość filtrowania adresów URL w oparciu o co najmniej

	140 kategorii i podkategorii. 28. Ochrona przed zagrożeniami 0-day. 29. Możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum na stacjach roboczych.
Ochrona serwera	1. Wsparcie systemów Microsoft Windows Server 2012 i nowszych oraz Linux, w tym co najmniej: RedHat Enterprise Linux (RHEL), CentOS, Ubuntu Server, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux. 2. Ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Możliwość skanowania dysków sieciowych typu NAS. 5. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie - z użyciem jednej lub obu metod jednocześnie. 6. Automatyczna, inkrementacyjna aktualizacja silnika detekcji. 7. Możliwość wykluczania procesów ze skanowania. 8. Możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
Dodatkowe wymagania dla ochrony serwerów Windows:	1. Możliwość skanowania plików i folderów znajdujących się w usłudze chmurowej OneDrive. 2. System zapobiegania włamaniom działający na hoście (HIPS). 3. Wsparcie skanowania magazynu Hyper-V. 4. Funkcjonalność skanera UEFI, chroniącego użytkownika poprzez wykrywanie i blokowanie zagrożeń przed uruchomieniem systemu operacyjnego. 5. Blokowanie zewnętrznych nośników danych na stacji, w tym: pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 6. Automatyczne wykrywanie usług zainstalowanych na serwerze i tworzenie dla nich odpowiednich wyjątków. 7. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 8. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 9. Ochrona przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
Dodatkowe wymagania dla	1. Możliwość uruchomienia lokalnej konsoli administracyjnej

ochrony serwerów Linux:	działającej z poziomu przeglądarki internetowej. 2. Lokalna konsola administracyjna bez konieczności instalacji i uruchomienia dodatkowego rozwiązania w postaci usługi serwera Web. 3. Działanie w architekturze bazującej na technologii mikro-serwisów, co zapewnia podwyższony poziom stabilności; awaria jednego z komponentów nie przerywa pracy całego procesu, a jedynie wymusza restart zawieszonego mikro-serwisu.
Szyfrowanie	1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10/11 32/64-bit. 2. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. 3. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
Ochrona urządzeń mobilnych opartych o system Android	1. Zapewnienie skanowania wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 2. Zapewnienie co najmniej 2 poziomów skanowania: inteligentnego i dokładnego. 3. Automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Możliwość podejrzenia listy zainstalowanych aplikacji przez administratora. 5. Blokowanie aplikacji w oparciu o: • nazwę aplikacji, • nazwę pakietu, • kategorię sklepu Google Play, • uprawnienia aplikacji, • pochodzenie aplikacji z nieznanego źródła
Sandbox w chmurze	1. Zapewnienie ochrony przed zagrożeniami 0-day. 2. Wykorzystywanie chmury producenta do działania. 3. Możliwość określenia, które pliki mają być automatycznie przesyłane do chmury, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. 4. Definiowanie przez administratora czasu, po którym przesłane pliki muszą zostać usunięte z serwerów producenta. 5. Definiowanie maksymalnego rozmiaru przesyłanych próbek przez administratora. 6. Tworzenie listy wykluczeń określonych plików lub folderów z przesyłania. 7. Przesyłanie wyników analizy do wszystkich wspieranych produktów po zakończonej analizie pliku. 8. Możliwość podejrzenia listy plików przesłanych do analizy przez

	administratora. 9. Analizowanie plików niezależnie od lokalizacji stacji roboczej; w przypadku wykrycia zagrożenia, natychmiastowa ochrona całego środowiska. 10. Brak konieczności instalacji dodatkowego agenta na stacjach roboczych. 11. Możliwość wysłania dowolnej próbki do analizy przez użytkownika lub administratora za pomocą wspieranego produktu; administrator może podejrzeć, jakie pliki zostały wysłane do analizy oraz przez kogo. 12. Odpowiednie oznaczenie przeanalizowanych plików. 13. Wstrzymywanie uruchamiania pobieranych plików na stacjach roboczych za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. 14. Wstrzymywanie dostarczania wiadomości do momentu zakończenia analizy próbki w przypadku serwerów pocztowych. 15. Przenoszenie wykrytych zagrożeń do bezpiecznego obszaru kwarantanny, z którego administrator może przywrócić dowolne pliki oraz utworzyć dla nich wyłączenia.
Moduł XDR	1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. 2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. 3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. 4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. 5. Wykluczenia muszą dotyczyć procesu lub procesu nadrzędnego. 6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. 7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. 8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta. 9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. 10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu

	przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. 11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. 12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny. 13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. 14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych. 15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich. 16. Konsola administracyjna musi mieć możliwość tagowania obiektów. 17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

Szkolenie dla administratorów systemu EDR

Wymagania minimalne	
Informacje podstawowe	• Szkolenie dla dwóch osób • Szkolenie w trybie stacjonarnym lub zdalnym • Czas trwania szkolenia: minimum 1 dzień (7 godzin) • Szkolenie musi być przeprowadzone przez autoryzowane centrum szkoleniowe producenta zakupionego systemu EDR • Prowadzący szkolnie muszą posiadać certyfikaty do

	przeprowadzania autoryzowanych szkoleń wystawione przez producenta zakupionego systemu EDR • Oferta powinna zawierać wspomniane certyfikaty, jak również szczegółowy program szkolenia.
Program szkolenia powinien zawierać minimum takie zagadnienia	• Omówienie pojęcia Extended Detection & Respond (EDR/XDR), • Omówienie architektury systemu, • Wdrożenie systemu, • Wdrożenie i konfiguracja agentów ESET Inspect, • Omówienie funkcji systemu, • Generowanie detekcji i ich analiza, • Reguły i automatyzacja, • Raportowanie, powiadomienia i zarządzanie uprawnieniami, • Rozwiązywanie problemów.

Szkolenie dla administratorów systemu ESET PROTECT

Szkolenia dotyczą posiadanych obecnie rozwiązań firmy ESET, które zamawiający planuje rozszerzyć o funkcjonalność EDR. W przypadku złożenia oferty na równoważny system EDR, nie będący rozwinięciem posiadanego rozwiązania firmy ESET, wykonawca zobowiązany jest zaoferować szkolenia zgodnie poniższą specyfikacją.

1. **ESET Client & Network Security Administrator**

Wymagania minimalne	
Informacje podstawowe	• Szkolenie dla dwóch osób • Szkolenie w trybie stacjonarnym lub zdalnym • Czas trwania szkolenia: minimum 2 dni (14 godzin) • Szkolenie musi być przeprowadzone przez autoryzowane centrum szkoleniowe producenta posiadanego systemu ESET PROTECT • Prowadzący szkolnie muszą posiadać certyfikaty do przeprowadzania autoryzowanych szkoleń wystawione przez producenta systemu ESET PROTECT • Oferta powinna zawierać wspomniane certyfikaty, jak również szczegółowy program szkolenia.
Program szkolenia powinien zawierać minimum takie zagadnienia	• Omówienie dostępnych produktów, • Różnice pomiędzy ESET PROTECT i ESET PROTECT CLOUD, • Różnice pomiędzy EEA i EES, • Przydatne strony WWW, • ESET Business Account – licencjonowanie, • ESET PROTECT - architektura i omówienie komponentów, • Instalacja i aktualizacja serwera ESET PROTECT, • ESET PROTECT - omówienie funkcji serwera, • Zarządzanie administratorami i ich uprawnieniami, • ESET Management Agent - zdalna instalacja i omówienie

	możliwości, • Grupy statyczne i dynamiczne, • Zadania klienta, serwera oraz wyzwalacze, • Zdalna instalacja klienta ESET, • Typowe scenariusze, • Omówienie funkcji podstawowych i zaawansowanych klienta EES, • Ochrona antywirusowa, • Zarządzanie aktualizacją, • Polityki i dziedziczenie, • ESET Bridge, • Zapora osobista, • Typowe scenariusze, • Moduł antyspamowy, • Powiadomienia, • Raportowanie, • Kontrola dostępu do stron internetowych, • Kontrola dostępu do urządzeń, • Migracja ESET PROTECT do ESET PROTECT CLOUD, • Wdrożenie klienta ESET Endpoint Security for Android, • Rozwiązywanie problemów.

2. ESET Advanced Administration - warsztat praktyczny

Wymagania minimalne	
Informacje podstawowe	• Szkolenie dla dwóch osób • Szkolenie w trybie stacjonarnym lub zdalnym • Czas trwania szkolenia: minimum 1 dzień (7 godzin) • Szkolenie musi być przeprowadzone przez autoryzowane centrum szkoleniowe producenta posiadanego systemu ESET PROTECT • Prowadzący szkolnie muszą posiadać certyfikaty do przeprowadzania autoryzowanych szkoleń wystawione przez producenta systemu ESET PROTECT • Oferta powinna zawierać wspomniane certyfikaty, jak również szczegółowy program szkolenia.
Program szkolenia powinien zawierać minimum takie zagadnienia	• Utworzenie konta ESET Business Account i dodanie kluczy licencyjnych. • Wdrożenie i konfiguracja serwera centralnego zarządzania ESET PROTECT w postaci maszyny wirtualnej. • Migracja agentów ESET Management Agent pomiędzy serwerami. • Wdrożenie i konfiguracja usługi ESET Bridge w celu replikacji agentów przy pracy zdalnej oraz w środowiskach rozproszonych. • Zaawansowane zarządzanie politykami.

	• ESET Full Disk Encryption – szyfrowanie. • ESET LiveGuard Advanced – sandboxing chmurowy. • Rozwiązywanie problemów.