kaspersky AKTYWUJ PRZYSZŁOŚĆ

Kaspersky Sandbox

Zaawansowane możliwości wykrywania w celu ochrony przed nieznanymi i unikającymi identyfikacji zagrożeniami – bez konieczności zatrudniania specjalistów ds. bezpieczeństwa IT

Obecnie zaawansowane cyberataki potrafią sparaliżować działanie firmy, wywołać ogromne straty finansowe oraz przyczynić się do utraty reputacji. Na stabilność i prawidłowe działanie organizacji ma wpływ nie tylko kradzież aktywów finansowych i tajemnic handlowych, ale także utrata zaufania klientów z powodu niedostępności usług i wiele innych negatywnych skutków, jakie wywołują złożone cyberzagrożenia. Działające samodzielnie tradycyjne narzędzia stworzone z myślą o ochronie obwodu sieci (zapory sieciowe, bramy poczty e-mail/sieciowe, serwery proxy), a także stacji roboczych i serwerów (ochrona antywirusowa i rozwiązania klasy Endpoint Protection Platform z podstawową funkcjonalnością), nie są wystarczające do uniemożliwienia szybkiej ewolucji cyberataków. Firmy, które wolą zapobiegać incydentom, muszą rozważyć stosowanie wyspecjalizowanych narzędzi do wykrywania, analizowania i reagowania na skomplikowane cyberzagrożenia.

Rozwiązanie Kaspersky Sandbox jest odpowiednie dla:

- firm, które nie mają specjalnego zespołu bezpieczeństwa, w których rola ochrony IT jest przypisana działowi IT,
- małych firm, które nie chcą narażać się na dodatkowe koszty związane z zasobami ochrony IT,
- dużych organizacji z geograficznie rozproszoną infrastrukturą i bez lokalnych specjalistów ds. bezpieczeństwa IT,
- firm, które muszą mieć pewność, że zatrudnieni przez nie analitycy bezpieczeństwa IT są w pełni skupieni na zadaniach krytycznych.

Na przestrzeni dwudziestu lat firma Kaspersky rozwijała narzędzia zabezpieczające dla firm wszystkich rozmiarów, działających we wszystkich branżach i o różnym poziomie doświadczenia w ochronie IT. Dzięki nieustannym badaniom i rozwoju, jak również ulepszeniom, jakich dokonaliśmy w dziedzinie polowania na zagrożenia, analizy i reagowania, pozostajemy liderem w zwalczaniu cyberprzestępczości.

Portfolio produktów i usług marki Kaspersky do zwalczania skomplikowanych zagrożeń obejmuje:

- Kaspersky Anti Targeted Attack — innowacyjne rozwiązanie służące do wykrywania i analizowania zagrożeń złożonych i ataków ukierunkowanych na poziomie sieci.
- Kaspersky Endpoint Detection and Response — rozwiązanie do wykrywania, analizowania i reagowania na zagrożenia złożone wymierzone w stacje robocze i serwery.
- Kaspersky Threat Intelligence Portal — zapewnia dostęp do usługi piaskownicy w chmurze, analitycznych raportów na temat zagrożeń APT, a także innych usług.

Jednak aby skutecznie korzystać z tych rozwiązań i usług, w firmach musi funkcjonować kompleksowy dział ds. bezpieczeństwa IT posiadający stosowne doświadczenie i wiedzę. Globalny brak specjalistów potrafiących radzić sobie z zagrożeniami złożonymi, jak również koszt ich zatrudnienia, często stanowią najważniejszy czynnik powstrzymujący firmy przed nabyciem takich rozwiązań i usług.

Oparte na opatentowanej technologii (patent nr US 10339301B2) rozwiązanie Kaspersky Sandbox pomaga organizacjom w walce z coraz liczniejszymi i bardziej skomplikowanymi współczesnymi zagrożeniami, które potrafią omijać ochronę na punktach końcowych. Uzupełniając funkcjonalność rozwiązania Kaspersky Endpoint Security for Business, Kaspersky Sandbox umożliwia organizacjom znacząco zwiększyć poziom ochrony stacji roboczych i serwerów przed wcześniej nieznanymi szkodliwymi programami, nowymi wirusami i programami ransomware, exploitami dnia zerowego itp. – bez konieczności zatrudniania wysoko wyspecjalizowanych analityków bezpieczeństwa informacji.

W ten sposób małe firmy mogą oszczędzić koszt rekrutowania i zatrudniania profesjonalistów, którzy zwykle mają wygórowane wymagania finansowe. Tymczasem dużym firmom posiadającym sieci rozproszone pomaga w optymalizacji kosztów w kontekście skutecznej ochrony ich biur zdalnych, przy jednoczesnym zmniejszeniu obciążenia pracy ręcznej wykonywanej przez analityków bezpieczeństwa.

Opcje dostarczania i wdrażania:
Kaspersky Sandbox jest dostarczany w postaci obrazu ISO ze wstępnie skonfigurowanym systemem CentOS 7 i wszystkimi niezbędnymi komponentami rozwiązania. Rozwiązanie może zostać wdrożone na serwerze fizycznym lub serwerach wirtualnych opartych na VMware ESXi.

Integracja:
- Systemy SIEM mogą otrzymywać informacje na temat wykrycia incydentu przez Kaspersky Sandbox. Informacje te są wysyłane za pośrednictwem Kaspersky Security Center jako wiadomości ogólne.
- Zaimplementowany w rozwiązaniu Kaspersky Sandbox interfejs API zapewnia integrację z innymi rozwiązaniami, co umożliwia wysyłanie plików do Kaspersky Sandbox na potrzeby skanowania i sprawdzania ich reputacji.

Skalowalność
Dzięki konfiguracjom obsługującym od 250 do nawet 5 000 chronionych stacji roboczych rozwiązanie zapewnia łatwą skalowalność i nieustanną ochronę większym infrastrukturom.

Podział na klastry
Poszczególne serwery można podzielić na klastry w celu zwiększenia przestrzeni i dostępności.

Jak to działa

Kaspersky Sandbox wykorzystuje najlepsze praktyki naszych ekspertów w zwalczaniu zagrożeń złożonych i ataków APT, a także jest ściśle zintegrowany z rozwiązaniem Kaspersky Endpoint Security for Business. Do zarządzania nim służy Kaspersky Security Center, nasza ujednolicona konsola administracyjna, działająca na zasadzie stosowania profili bezpieczeństwa.

Agent Kaspersky Endpoint Security for Business pobiera dane na temat podejrzanego obiektu ze współdzielonej operacyjnej pamięci podręcznej zawierającej werdykty, zlokalizowanej na serwerze Kaspersky Sandbox. Jeśli obiekt został już przeskanowany, Kaspersky Endpoint Security for Business otrzymuje werdykt i stosuje jedną lub kilka opcji leczenia:

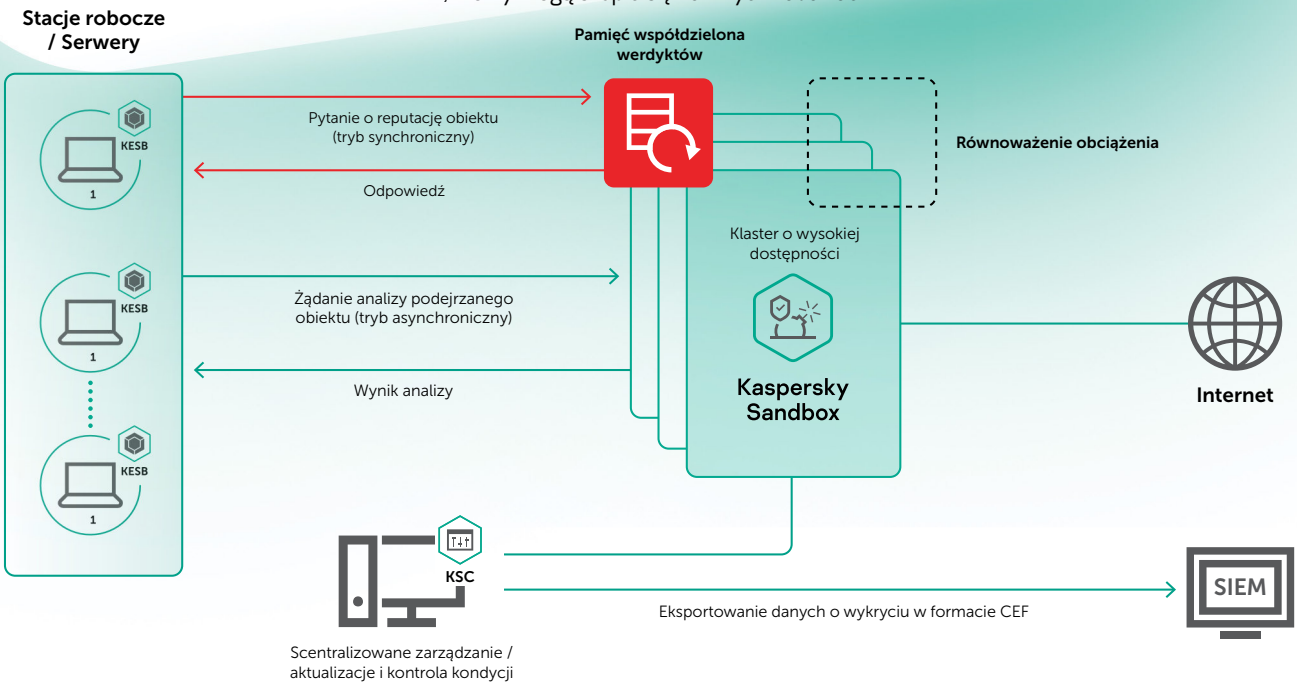
- Usuń i poddaj kwarantannie
- Poinformuj użytkownika
- Rozpocznij skanowanie obszarów krytycznych
- Wyszukaj wykryty obiekt na innych maszynach w obrębie sieci zarządzanej

Jeśli w pamięci podręcznej nie znajduje się werdykt zawierający informacje o reputacji obiektu, agent Kaspersky Endpoint Security for Business wysyła podejrzany plik do rozwiązania Sandbox i czeka na odpowiedź. Sandbox otrzymuje polecenie przeskanowania obiektu, które uruchamiane jest w środowisku odizolowanym od prawdziwej infrastruktury.

Skanowanie plików odbywa się na maszynach wirtualnych, na których znajdują się narzędzia emulujące typowe środowisko pracy (systemy operacyjne/zainstalowane aplikacje). W celu wykrycia szkodliwego zamiaru obiektu przeprowadzana jest analiza jego zachowania, a także gromadzenie i analizowanie artefaktów. Jeśli obiekt wykonuje szkodliwe działania, Sandbox uznaje go za niebezpieczny. Podczas analizy w piaskownicy do obiektu przypisywany jest werdykt.

Po zakończeniu procesu emulacji obiektu werdykt końcowy jest wysyłany w czasie rzeczywistym do współdzielonej podręcznej pamięci operacyjnej, dzięki czemu inne hosty z zainstalowanym rozwiązaniem Kaspersky Endpoint Security for Business mogą szybko uzyskać dane na temat reputacji skanowanego obiektu bez konieczności ponownego analizowania go. Podejście to zapewnia szybkie przetwarzanie podejrzanych obiektów, zmniejsza obciążenie serwerów Kaspersky Sandbox, a także przyspiesza i zwiększa skuteczność reagowania na zagrożenia.

Kaspersky Sandbox to podstawowy dodatek do rozwiązania Kaspersky Endpoint Security for Business. Automatycznie blokuje on zaawansowane, nieznane i złożone zagrożenia, bez konieczności używania dodatkowych zasobów, a także odciąża analityków bezpieczeństwa IT, którzy mogą skupić się na innych zadaniach.



Oficjalny blog Kaspersky Daily: kaspersky.pl/blog
Najnowsze informacje: kaspersky.pl/nowosci
Rozwiązania dla małych i średnich firm: kaspersky.pl/biznes
Rozwiązania dla korporacji: kaspersky.pl/dla-korporacji

www.kaspersky.pl

Jesteśmy skuteczni. Jesteśmy niezależni. Jesteśmy transparentni. Zobowiązaliśmy się do budowania bezpieczniejszego świata, w którym technologia czyni nasze życie lepszym. Dlatego go chronimy, aby każda osoba wszędzie mogła korzystać z jego nieskończonych możliwości. Aktywuj cyberbezpieczeństwo dla lepszego jutra.

Dowiedz się więcej na stronie www.kaspersky.pl/transparentnosc

Sprawdzony.
Transparentny.
Niezależny.