# Kaspersky Security Network

Kaspersky Security Network to technologia proaktywna, zaimplementowana w najnowszych wersjach produktów firmy Kaspersky Lab dla biznesu i użytkowników domowych. W przypadku nowego szkodliwego oprogramowania technologia ta zapewnia szybką reakcję oraz niespotykany poziom wykrywania, co stanowi znakomitą ochronę. Kaspersky Security Network umożliwia nie tylko wykrywanie i blokowanie wcześniej nieznanych zagrożeń, ale także zlokalizowanie zasobów sieciowych i umieszczenie ich na czarnej liście, chroniąc w ten sposób użytkowników przed kolejnymi zagrożeniami pochodzącymi z tego samego źródła.

Kaspersky Security Network oferuje użytkownikom korporacyjnym dodatkowe korzyści w postaci udoskonalonej kontroli aplikacji i umieszczania ich na białej liście znanych, legalnych programów. Kaspersky Security Network łączy w sobie możliwości ciągłego, globalnego rozproszonego monitorowania rzeczywistych zagrożeń, scentralizowaną analizę przy użyciu zasobów technologicznych i eksperckich firmy Kaspersky Lab oraz natychmiastowe generowanie i dostarczanie ochronnych środków zaradczych. Tworzy to silny efekt synergii, zapewniając użytkownikom produktów firmy Kaspersky Lab kompleksową ochronę w czasie rzeczywistym przed nowym szkodliwym oprogramowaniem.

## Szybka i kompleksowa ochrona przed cyberatakami

Szkodliwe programy, takie jak wirusy, robaki i trojany, stały się głównymi zagrożeniami dla normalnie funkcjonujących komputerów oraz przechowywanych na nich informacji. Obszar i zakres działania szkodliwego oprogramowania stale się powiększa, stanowiąc ciągle rosnące wyzwanie dla bezpieczeństwa komputerów. Według wewnętrznych danych Kaspersky Lab, codziennie pojawia się około 200 000 nowych próbek szkodliwego oprogramowania. Szkodniki wykorzystują nowe metody wnikania do systemów komputerów, ukrywając swoje działania i unikając wykrycia przez oprogramowanie antywirusowe. Obecnie żadne konwencjonalne metody wykrywania szkodliwych programów nie zapewniają kompletnej ochrony, jeśli są używane jako autonomiczne narzędzia.

Dzisiejszy cyberświat wymaga zastosowania nowego, zintegrowanego sposobu ochrony komputerów. Sposób ten powinien łączyć w sobie korzyści i minimalizować braki tradycyjnych metod walki ze szkodliwymi programami, a także oswajać możliwości globalnego monitorowania i automatycznego aktualizowania bazy danych nowych, rzeczywistych zagrożeń. Takie właśnie podejście zostało zastosowane w Kaspersky Security Network.

## Podstawowe zasady działania Kaspersky Security Network

Kaspersky Security Network zawiera kilka podsystemów: ciągłe, geograficznie rozproszone, globalne monitorowanie rzeczywistych zagrożeń na komputerach użytkowników, natychmiastowe dostarczenie zgromadzonych danych na serwery firmy Kaspersky Lab, analiza zebranych danych i tworzenie środków chroniących przed nowymi zagrożeniami oraz szybkie dostarczenie tych środków do użytkowników.

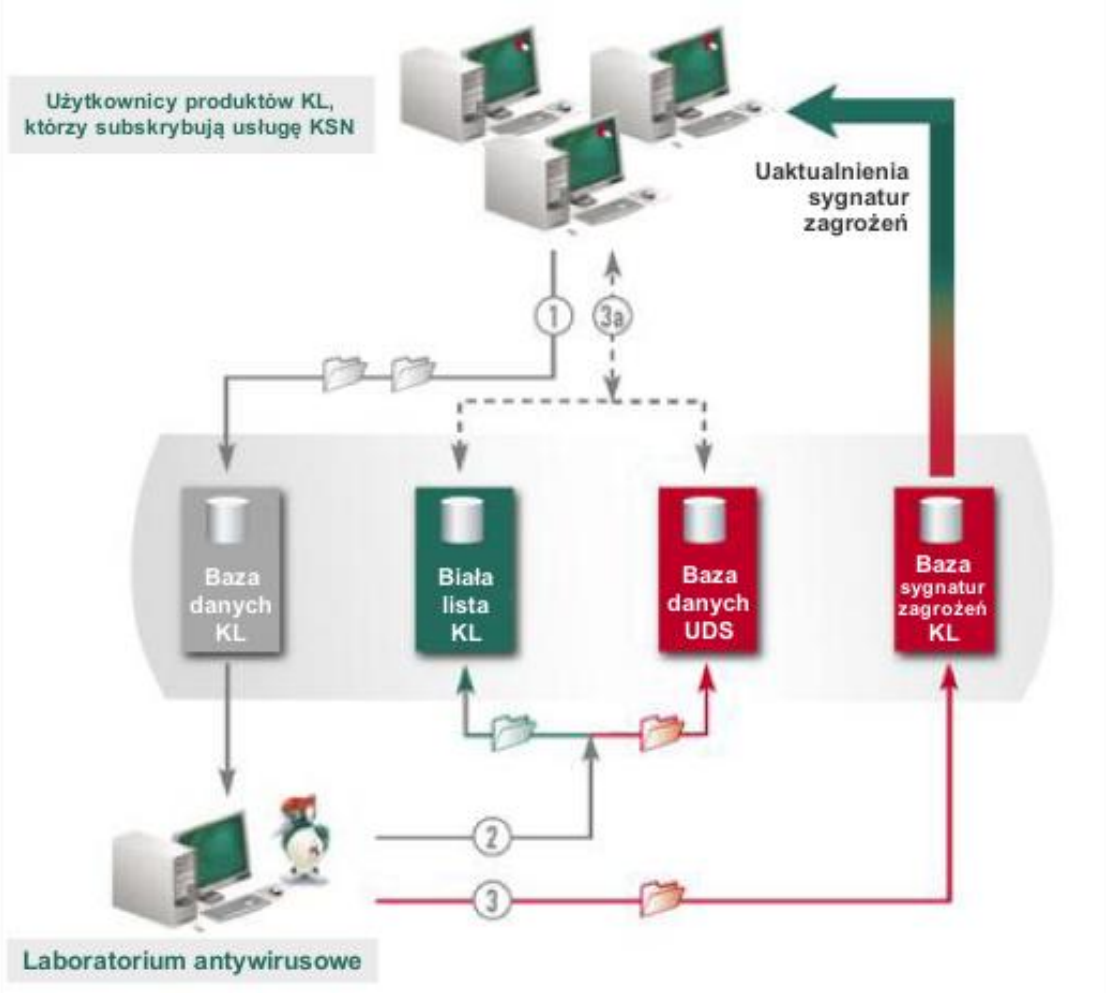
Kaspersky Security Network automatycznie zbiera informacje o podjętych próbach zainfekowania komputera i wysyła te dane do Kaspersky Lab. Gromadzone są również informacje o podejrzanych plikach, pobranych i uruchomionych na komputerach, bez względu na ich źródło (strony internetowe, załączniki

wiadomości e-mail, sieci peer-to-peer itd.). Odbywa się to dobrowolnie i świadomie – użytkownik produktu Kaspersky Lab dla użytkowników domowych musi wyrazić zgodę na uczestnictwo w systemie. Użytkownicy rozwiązań Kaspersky Lab dla biznesu nie biorą udziału w procesie tworzenia bazy danych Kaspersky Security Network. Należy zaznaczyć, że nie są gromadzone żadne dane użytkowników, takie jak informacje osobowe, hasła i inne informacje poufne.

Informacje zebrane podczas próby infekcji są wysyłane na centralne serwery Kaspersky Lab i analizowane przy użyciu silnej wewnętrznej technologii i zasobów eksperckich firmy. Zapewnia to niezwykle szybkie i dokładne wykrywanie nowych szkodliwych programów oraz bezpiecznego oprogramowania. Decyzja dotycząca bezpieczeństwa programu jest podejmowana w oparciu o dostępność podpisu cyfrowego poprzez weryfikację źródła i integralności programu, a także kilka innych czynników. Program, który zostanie uznany za bezpieczny, zostaje dodany do listy zaufanych aplikacji.

Program jest rozpoznawany jako szkodliwy po zakończeniu wykonywania wymaganych procedur wykrywania. Jak tylko program zostanie uznany za szkodliwy, zostaje wprowadzony do systemu UDS (ang. Urgent Detection System – System Natychmiastowego Wykrywania) firmy Kaspersky Lab. W rezultacie informacje stają się dostępne dla użytkowników produktów firmy Kaspersky Lab, zanim sygnatura tego szkodliwego programu zostanie utworzona i zaktualizowana na ich komputerach. W ten sposób klienci Kaspersky Lab otrzymują informacje o nowych i nieznanych zagrożeniach w kilka minut po rozpoczęciu cyberataku. W przypadku tradycyjnej aktualizacji baz danych sygnatur trwa to kilka godzin.

Jeśli program zostanie uruchomiony przez użytkownika, zostanie on sprawdzony w oparciu o białą listę i listę systemu Urgent Detection System, a następnie uzyska prawa dostępu do zasobów komputera lub zostanie zablokowany. Technologia Kaspersky Security Network odgrywa ważną rolę w aktualizowaniu tych list, zapewniając skuteczną kontrolę nad aplikacjami.




*Schemat działania Kaspersky Security Network*

Schemat przedstawia interakcję użytkowników produktów Kaspersky Lab z systemem KSN. Interakcja ta obejmuje 4 różne etapy:

1. Informacje o nowouruchomionych lub pobranych aplikacjach i odwiedzonych stronach internetowych (adresy internetowe) są wysyłane przez użytkowników najnowszych produktów Kaspersky Lab dla biznesu i klientów indywidualnych.
2. Pliki i adresy internetowe są sprawdzane i, jeśli okażą się szkodliwe, zostają dodane do bazy danych systemu Urgent Detection System. Legalne pliki zostają dodane do bazy danych „Whitelisting".
3. Eksperci z Kaspersky Lab kończą analizę szkodliwych plików, określają ich stopień zagrożenia i dodają ich opisy do bazy danych sygnatur.
4. Informacje o nowoodkrytych szkodliwych i legalnych plikach oraz adresach internetowych stają się dostępne dla wszystkich użytkowników odpowiednich produktów Kaspersky Lab (nie tylko dla subskrybentów Kaspersky Security Network) w kilka minut po ich pierwszym wykryciu.

Po zakończeniu analizy nowego szkodliwego programu generowana jest również sygnatura, która jest następnie umieszczana w antywirusowych bazach danych, regularnie aktualizowanych na komputerach użytkowników produktów Kaspersky Lab.

„Whitelisting" to nie tylko technologia umożliwiająca użytkownikom podjęcie decyzji o programie przy użyciu zasobów KSN. System ten zawiera technologię reputacji zwaną „mądrością tłumu" („Wisdom of the Crowd" - WoC), która udostępnia informacje o popularności danego programu oraz jego reputacji wśród innych użytkowników – uczestników KSN.

Co więcej, najnowsze wersje produktów Kaspersky Lab oferują możliwość uzyskania globalnego klasyfikatora bezpieczeństwa (Global Security Rating - GSR) bezpośrednio z chmury. Każdy klasyfikator jest obliczany przy użyciu elastycznego, adaptowalnego algorytmu oraz różnych danych reputacji. Dlatego też, Kaspersky Security Network wykorzystuje połączenie sygnatur i metod heurystycznego wykrywania szkodliwych programów, a także technologii kontroli aplikacji przy użyciu białej i czarnej listy, WoC i GSR.

## Udoskonalona ochrona w chmurze w produktach dla biznesu

Od chwili wydania programu Kaspersky Endpoint Security 8 for Windows klienci korporacyjni programów Kaspersky Lab mogą czerpać korzyści z Kaspersky Security Network. Wraz z tradycyjnymi technikami ochrony i zaawansowanymi narzędziami dla wdrożenia firmowej polityki bezpieczeństwa IT, Kaspersky Security Network zapewnia natychmiastową reakcję na nowe i nieznane zagrożenia oraz pomaga chronić poufne dane przed atakami ukierunkowanymi.

Ogólne zasady korzystania z Kaspersky Security Network w środowisku biznesowym są takie same, jak w przypadku produktów Kaspersky Lab dla użytkowników domowych. Firmowe punkty końcowe oparte na systemie Windows używają danych z Kaspersky Security Network do oszacowania reputacji plików i adresów stron internetowych. W oparciu o te dane blokują one dostęp do szkodliwej zawartości lub stosują określone ograniczenia na podejrzanym programie.

W funkcjonalności Kaspersky Security Network dla produktów korporacyjnych zaimplementowano kilka udoskonaleń. Technologia ochrony wspomagana przez chmurę jest używana do umieszczania aplikacji na białej liście przy wykorzystaniu danych z Kaspersky Security Network. Znane legalne pliki są automatycznie dzielone na kategorie, takie jak gry, oprogramowanie komercyjne itd. Korzystając z tych kategorii, administrator systemu może szybko zainstalować i zastosować pewne reguły dla określonych typów oprogramowania, zgodnie z profilem bezpieczeństwa. Dane dla funkcji białych list aplikacji są również dostarczane przez ponad 200 czołowych producentów oprogramowania i są używane wraz z informacjami „nadsyłanymi z tłumu" (ang. „crowd-sourced").

Rozwiązanie zarządzania poprzez Kaspersky Security Center umożliwia firmom szczegółową kontrolę wykorzystania Kaspersky Security Network do ochrony korporacyjnych punktów końcowych. Administrator może zdecydować, czy ochrona oparta o chmurę ma być włączona w określonych modułach Kaspersky Endpoint Security 8 for Windows. W celu dostosowania się do określonej polityki bezpieczeństwa, można również wyłączyć wysyłanie danych do Kaspersky Security Network. Aby zmniejszyć przepustowość, wewnętrzne proxy Kaspersky Security Network może zostać zainstalowane w sieci lokalnej.

## Ochrona dla klientów indywidualnych z wykorzystaniem chmury

Najnowsze wersje produktów Kaspersky Lab dla użytkowników domowych, a mianowicie Kaspersky Internet Security 2013 i Kaspersky Anti-Virus 2013, mogą się poszczycić całkowitym wsparciem ze strony opartej o chmurę technologii Kaspersky Security Network. Poza ogólnymi korzyściami płynącymi z korzystania z ochrony wspomaganej przez chmurę, nowe wersje produktów dla klientów indywidualnych oferują otrzymywanie ogólnych statystyk dotyczących Kaspersky Security Network: liczby chronionych użytkowników, zablokowanych szkodliwych obiektów i przetworzonych legalnych danych.


Inna, nowa funkcja zaprezentowana w najnowszych wersjach Kaspersky Internet Security 2013 i Kaspersky Anti-Virus 2013 to możliwość sprawdzenia reputacji dowolnego pliku wykonywalnego, która jest oparta o dane z Kaspersky Security Network. Takie zapytanie zwraca werdykt dotyczący danego pliku (czy program jest legalny), a także wyświetla informacje o dacie pierwszego pojawienia się pliku, jego popularności według kraju oraz inne dane. Funkcja ta umożliwia użytkownikom sprawdzenie podstawowych informacji o nieznanych programach przed ich uruchomieniem, chociaż te same informacje są otrzymywane automatycznie, gdy użytkownik próbuje uruchomić plik.

Jedną z wyróżniających się funkcji programu Kaspersky Internet Security 2013 jest wspomagana przez chmurę technologia antyspamowa. Wykorzystuje ona informacje z Kaspersky Security Network do wykrywania i blokowania niechcianych wiadomości i nie wymaga przeprowadzenia uczenia filtru antyspamowego, jak to miało miejsce w poprzednich wersjach tego produktu. Oparta o chmurę funkcja antyspamowa zależy od regionu i języka, i w niektórych krajach może być niedostępna.

## Zalety Kaspersky Security Network

Nieprzerwane globalne monitorowanie nowych zagrożeń i źródeł zagrożeń oraz natychmiastowa dostępność nowych ochronnych środków zaradczych zapewnia naszym klientom niespotykanie szybką reakcję Kaspersky Lab na nowe zagrożenia oraz bezkonkurencyjną solidność ochrony.

Obecnie technologia Kaspersky Security Network jest używana na milionach komputerów na świecie, przedstawiając globalny, ale szczegółowy obraz ewolucji i rozprzestrzeniania się szkodliwych programów, pochodzenia nowych zagrożeń oraz liczby prób infekcji pojawiających się w określonym przedziale czasu. Globalne rozproszone monitorowanie szkodliwych programów wykonywane przez Kaspersky Security Network zapewnia skuteczną reakcję na nowe zagrożenia, bez względu na lokalizację źródła i celu.

Monitorowanie szkodników na maszynach użytkowników w czasie rzeczywistym pomaga śledzić aktualne zagrożenia i blokować je w ich naturalnych środowiskach natychmiast po wykryciu próby infekcji.

Ciągłe monitorowanie szkodliwych programów i natychmiastowe zgłaszanie podejrzanych plików do Kaspersky Lab sprawia, że bazy danych szkodliwych programów i środki ochrony, służące do walki z tymi zagrożeniami, są zawsze aktualne. Automatyzacja zapewnia szybszą, dokładniejszą i kompletniejszą reakcję niż konwencjonalne, ręczne zgłaszanie podejrzanego pliku do producenta programu antywirusowego za pośrednictwem poczty elektronicznej.

Zagwarantowana jest ścisła poufność: żadne informacje osobiste, takie jak nazwy użytkowników, hasła, dane osobiste i zawartości dokumentów, nie są gromadzone i przesyłane na serwery Kaspersky Lab.

Najnowsze produkty Kaspersky Lab wykorzystują Kaspersky Security Network także do skuteczniejszego blokowania odsyłaczy internetowych, prowadzących do oszukańczych i szkodliwych stron internetowych. Odnośniki są najpierw sprawdzane w oparciu o lokalną bazę phishingowych i szkodliwych stron internetowych, a gdy nie zostanie znaleziony ich odpowiednik, są one sprawdzane w oparciu o internetowe czarne listy KSN. Jeśli odnośniki pozostaną nieznane, wówczas są skanowane z użyciem analizy heurystycznej na obecność atrybutów charakterystycznych dla szkodliwych odnośników. Wykrywanie niebezpiecznych odnośników stało się bardziej dokładne, ponieważ od chwili opublikowania produktów dla klientów indywidualnych w wersji 2011, internetowe bazy danych KSN zgromadziły ogromną ilość dodatkowych informacji o różnych stronach internetowych.

Podsumowując: użytkownicy produktów Kaspersky Lab z obsługą Kaspersky Security Network mają zapewnioną całkowitą ochronę przed kradzieżą poufnych danych. Nowe szkodliwe programy, zaprojektowane do kradzieży danych osobistych i firmowych, są blokowane na komputerach użytkowników, bez względu na to, czy są to programy szpiegujące pliki przechowywane na dysku twardym, które następnie wysyłają te pliki do hakerów, keyloggery, szkodniki wysyłające zrzuty ekranu, programy szpiegujące aktywność sieciową itd.

Kaspersky Security Network zapewnia ochronę proaktywną, tzn. identyfikuje nowe zagrożenia i blokuje ich rozprzestrzenianie, zapobiegając w ten sposób znaczącym szkodom wyrządzonym przez te zagrożenia na maszynach użytkowników. System ochrony proaktywnej jest konieczny dla stabilnego i nieprzerwanego działania sprzętu IT oraz procesów biznesowych przez niego obsługiwanych.