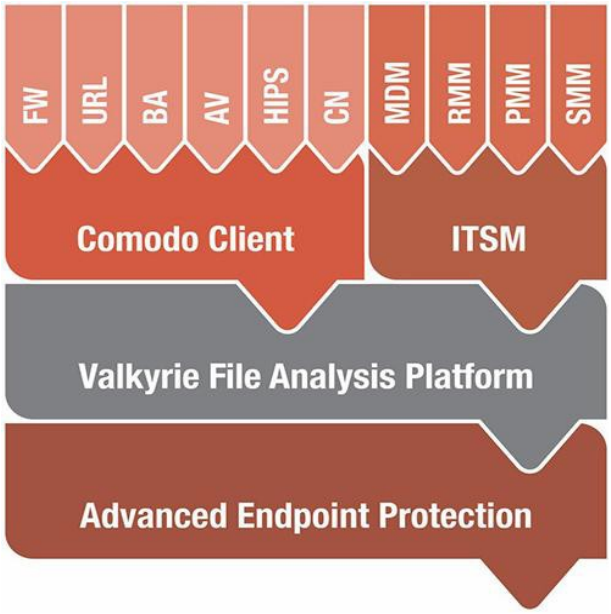
COMODO Endpoint Security & ITSM

opis siedmiu warstw ochrony

COMODO
Creating Trust Online™

Tel +48(32)745 46 12
NIP 634 280 10 31
KRS 0000403252
SĄD REJONOWY KATOWICE-WSCHÓD,
VIII WYDZIAŁ GOSPODARCZY KRAJOWEGO
BANK ZACHODNI 39 1090 2008 0000 0001 1771 9659

COMODO Polska
it partners security sp. z o.o.
wyłączny dystrybutor na Polskę
ul. Paderewskiego 35
40-282 Katowice Poland
Email: biuro@comodo-polska.pl
Web: www.comodo-polska.pl



Oprogramowanie antywirusowe Comodo zapewnia kompleksowe rozwiązanie bezpieczeństwa, które zabezpiecza stacje robocze przed wirusami, trojanami, robakami. Jednocześnie antywirus Comodo chroni przed atakami polegającymi na przepełnieniu bufora (z jęz. ang. overflow), atakami typu zero-day, aplikacjami szpiegującymi, hakerami i zagrożeniami ransomware.

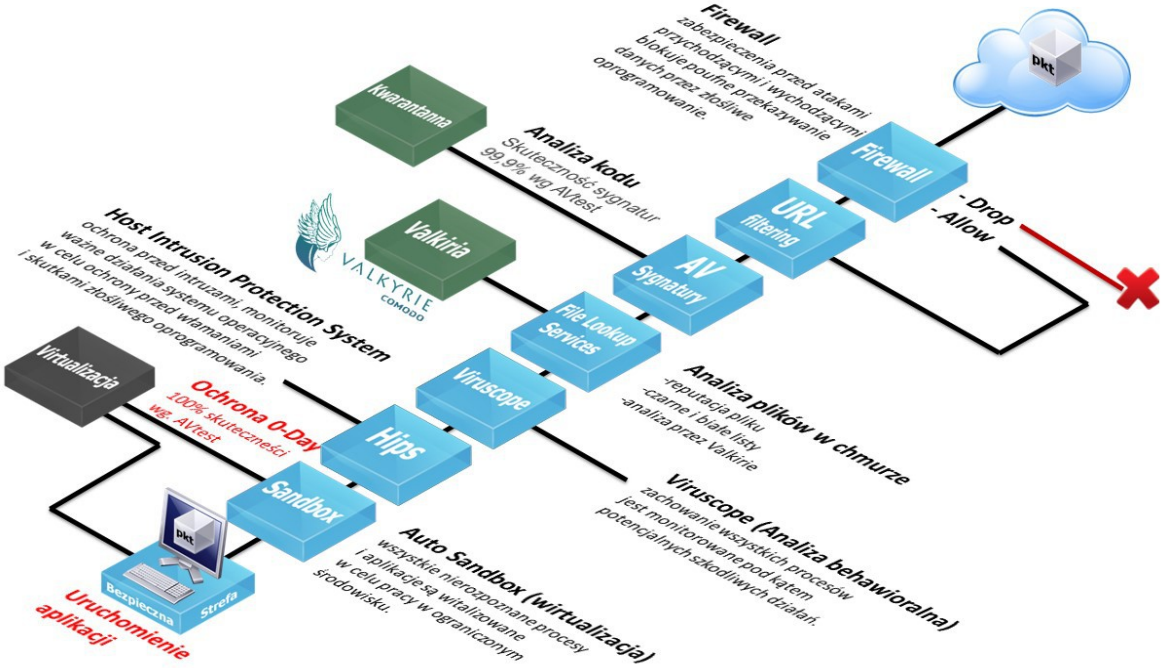
Comodo łączy w sobie skuteczną ochronę antywirusową, anty-malware, wysokiej klasy firewall korporacyjny z funkcją zapobiegania włamaniom, automatyczną piaskownicę, w której uruchamiane są nieznane i potencjalnie niebezpieczne aplikacje oraz kontrolę zasobów systemowych i sprzętowych, która daje dostęp do klawiatury, dysków i pamięci fizycznej komputera zabezpiecza przed manipulacją ze strony złośliwego oprogramowania.

Tel +48(32)745 46 12
NIP 634 280 10 31
KRS 0000403252
SĄD REJONOWY KATOWICE-WSCHÓD,
VIII WYDZIAŁ GOSPODARCZY KRAJOWEGO
BANK ZACHODNI 39 1090 2008 0000 0001 1771 9659

COMODO Polska
it partners security sp. z o.o.
wyłączny dystrybutor na Polskę
ul. Paderewskiego 35
40-282 Katowice Poland
Email: biuro@comodo-polska.pl
Web: www.comodo-polska.pl

COMODO
Creating Trust Online™

7 poziomowy system ochrony stacji roboczej



1. **Web URL Filtering -** umożliwia blokowanie dostępu do stron internetowych na podstawie kategorii „Phishing" i „Malware" oraz reguł, które mogą być tworzone dla poszczególnych użytkowników komputera, co czyni tą funkcję przydatną zarówno w domu, jak i w środowisku pracy. Firmy mogą uniemożliwić pracownikom odwiedzanie serwisów społecznościowych w godzinach pracy lub zezwolić na dzianie tylko wybranym adresom URL (białe listy).

2. **Ocena reputacji plików -** pobrane pliki na dysk komputera oceniane są w chmurze Comodo pod kątem ich reputacji sprawdzając czy znajdują się one na białych lub czarnych listach plików Comodo. Zaufane pliki są wyłączone z monitorowania przez HIPS – zmniejsza to zużycie zasobów

Tel +48(32)745 46 12
NIP 634 280 10 31
KRS 0000403252
SĄD REJONOWY KATOWICE-WSCHÓD,
VIII WYDZIAŁ GOSPODARCZY KRAJOWEGO
BANK ZACHODNI 39 1090 2008 0000 0001 1771 9659

COMODO Polska
it partners security sp. z o.o.
wyłączny dystrybutor na Polskę
ul. Paderewskiego 35
40-282 Katowice Poland
Email: biuro@comodo-polska.pl
Web: www.comodo-polska.pl

sprzętowych i systemowych. Z kolei pliki zidentyfikowane jako szkodliwe trafią na lokalną listę zablokowanych plików Comodo, gdzie będą miały zabronione prawa dostępu do innych procesów lub kont użytkowników, tym samym skutecznie odcinając je od reszty systemu operacyjnego.

3. **Antywirus -** aktywny silnik antywirusowy automatycznie wykrywa i eliminuje wirusy, robaki i inne złośliwe oprogramowanie ukrywające się na komputerze. Zaimplementowane algorytmy antyspyware wykrywają szpiegujące aplikacje i usuwają każdą infekcję. Z kolei anty-rootkit skanuje, wykrywa i eliminuje z systemu rootkity. Anty-bot nie pozwala zainfekować komputera, który mógłby się stać częścią botnetu, a znane złośliwe oprogramowanie identyfikowane jest za pomocą czarnej listy plików Comodo.

4. **HIPS -** stale monitoruje aktywność systemu i pozwala uruchamiać pliki wykonywalne (np. exe, dll, .cpl, .scr, .sys) oraz procesy, jeżeli są one podpisane cyfrowo przez dewelopera aplikacji. Dla przeciętnego użytkownika HIPS zapewnia bardzo wysoki poziom ochrony bez jego ingerencji. HIPS automatycznie chroni krytyczne pliki systemowe, foldery, klucze rejestru zapobiegając nieautoryzowanym modyfikacjom przez złośliwe aplikacje. HIPS zapewnia maksymalną ochronę przed szkodliwymi programami, które próbują uruchomić się i chroni system przed kradzieżą danych zapobiegając większości typów ataków, np. przepełnienia bufora, atakom ze strony rootkitów, wstrzykiwaniem kodu do procesów, keyloggerami i innym złośliwym oprogramowaniem.

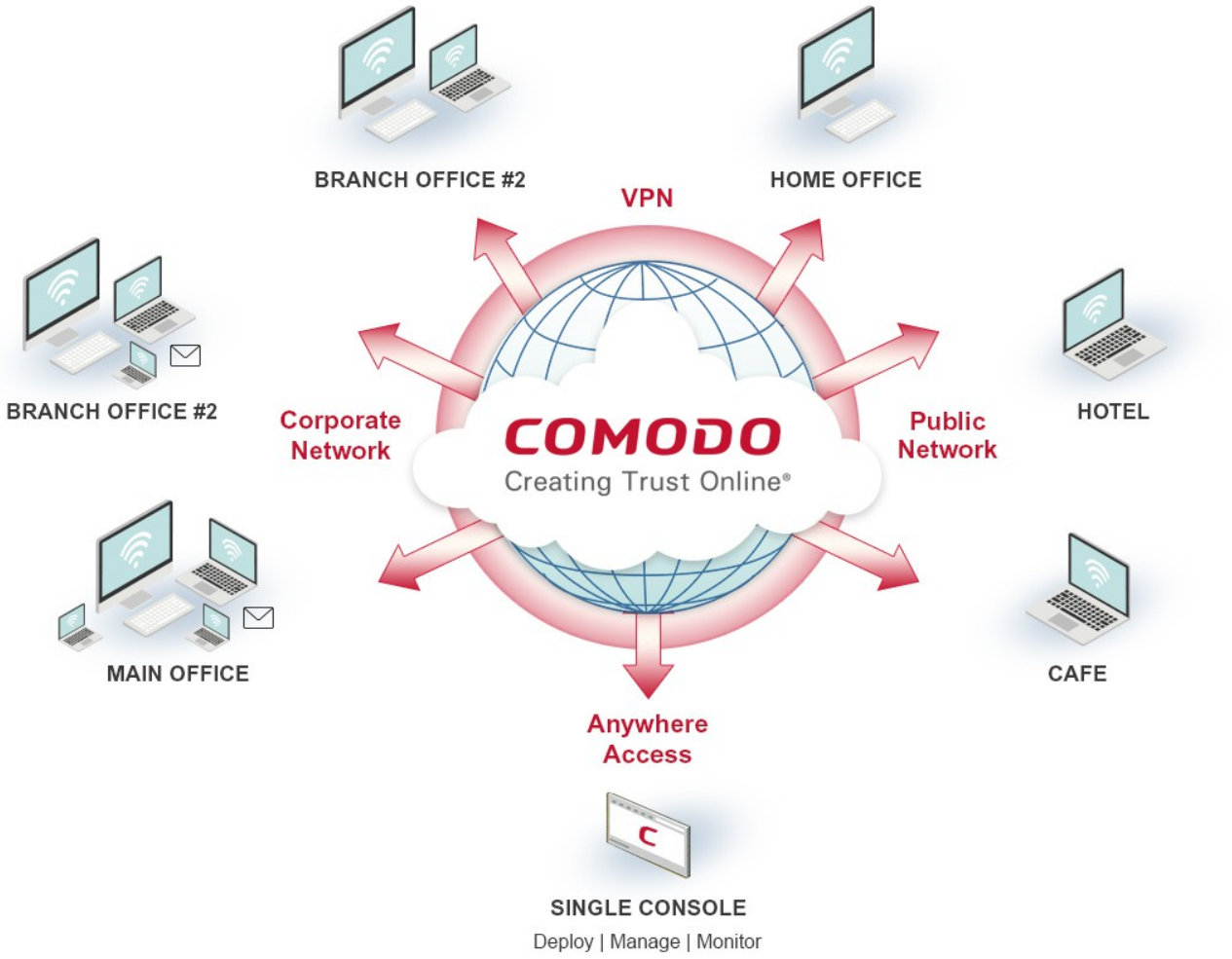
5. **Auto-sandbox -** programy wykonywalne uruchomione w automatycznej piaskownicy działają na ograniczonych uprawnieniach. Nie mogą one modyfikować plików w „prawdziwym" systemie, są odizolowane od rzeczywistego systemu i plików, więc mają znacznie mniej okazji do uszkodzenia komputera. Dla nich zasoby komputera, a więc CPU, RAM, rejestr systemowy oraz lokalizacje rzeczywistych plików są emulowane, co pozwala na automatyczne i bezpieczne uruchamianie potencjalnie niebezpiecznego oprogramowania, które mogłoby uszkodzić system lub zaszyfrować pliki.

6. **Firewall -** kontroluje ruch przychodzący i wychodzący dla protokołów IPv4 i IPv6. Blokuje podejrzane adresy IP, kontroluje protokoły HTTP, HTTPS, POP3, IMAP, SMTP oraz niestandardowe porty. Transmitowane dane za pośrednictwem pakietów są analizowane pod kątem niechcianych lub podejrzanych aktywności ze strony szkodliwego oprogramowania.

Firewall chroni przed manipulacją pamięci podręcznej protokołu ARP, który jest używany do mapowania adresów IP na adresy MAC. Hakerzy mogą wykorzystać go na wiele sposobów m.in. do ataków DoS, MiTM oraz uzyskać fizyczny dostęp do sieci. Firewall analizuje sfałszowane pakiety, które są wykorzystywane przy atakach i sprawdza, czy są zgodne z obowiązującymi standardami protokołów. Jeżeli nie są, będą blokowane.

7. **Viruscope -** monitoruje działania procesów uruchomionych na komputerze i informuje, które aplikacje wykonują podejrzane działania mogące potencjalnie zagrażać prywatności i bezpieczeństwu użytkowników. Moduł ten tworzy kolejną warstwę wykrywania szkodliwego oprogramowania wprowadzając możliwość odwrócenia potencjalnie niepożądanej modyfikacji systemu przez oprogramowanie trzecie. W efekcie Viruscope wykrywa malware zero-day poprzez analizę jego zachowania. Jeżeli wyryte zachowanie odpowiada złośliwej aplikacji, zostanie podniesiony alarm, który pozwoli przenieść program do kwarantanny i odwrócić dokonane zmiany.

Comodo ITSM zawsze tam, gdzie potrzebna jest kompleksowa ochrona.



Zapisz się na bezpłatne webinarium:

www.comodo-polska.pl/webinarium

COMODO
Creating Trust Online™

Tel +48(32)745 46 12
NIP 634 280 10 31
KRS 0000403252
SĄD REJONOWY KATOWICE-WSCHÓD,
VIII WYDZIAŁ GOSPODARCZY KRAJOWEGO
BANK ZACHODNI 39 1090 2008 0000 0001 1771 9659

COMODO Polska
it partners security sp. z o.o.
wyłączny dystrybutor na Polskę
ul. Paderewskiego 35
40-282 Katowice Poland
Email: biuro@comodo-polska.pl
Web: www.comodo-polska.pl