WatchGuard Total Security

Pełna ochrona sieci w jednym, łatwym do wdrożenia rozwiązaniu.

BEZPIECZEŃSTWO NA POZIOMIE KORPORACYJNYM

PEŁNA OCHRONA

Każda sieć potrzebuje pełnego arsenału silników skanujących, aby zapewnić ochronę przed oprogramowaniem szpiegującym i wirusami, złośliwymi aplikacjami i wyciekiem danych - aż po oprogramowanie typu ransomware, botnety, zaawansowane trwałe zagrożenia i złośliwe oprogramowanie typu zero day. Profesjonalne rozwiązanie w zakresie bezpieczeństwa sieciowego zajmie się wszystkimi aspektami zapobiegania zagrożeniom, wykrywania, korelacji i reagowania – obecnie oraz w miarę rozwoju tych zagrożeń. Rozwiazania WatchGuard nie tylko zapewniają kompletny pakiet ujednoliconych zabezpieczeń na rynku, ale oferują też ochronę w zakresie przeciwdziałania nowym i zmieniającym się zagrożeniom sieciowym, w tym zaawansowanemu złośliwemu oprogramowaniu typu malware i ransomware.

PROSTOTA

PROSTOTA

To jednak coś więcej niż tylko narzędzia do skanowania zabezpieczeń. Dla WatchGuard prostota jest kluczem do pomyślnego zaadoptowania technologii. W związku z tym, wszystkie produkty są nie tylko łatwe w początkowej konfiguracji i wdrożeniu, ale także zaprojektowane z naciskiem na scentralizowane zarządzanie, dzięki czemu bieżące zarządzanie polityką i siecią staje się proste. Bezpieczeństwo jest kwestią złożoną, ale zarządzanie nim nie musi być skomplikowane.

NAJWYŻSZA WYDAJNOŚĆ

WYDAJNOŚĆ

Każdy biznes, niezależnie od wielkości, musi zwracać uwagę na kwestię wydajności. Krótkie czasy skanowania zabezpieczeń mogą zaburzyć zdolność sieci do obsługi ruchu o dużym natężeniu. Niektóre firmy są zmuszone do redukcji poziomu ochrony, aby utrzymać wysoką wydajność, ale rozwiązania WatchGuard nigdy nie powodują konieczności wyboru między bezpieczeństwem a szybkością. Wykorzystując moc przetwarzania wielordzeniowego, platforma WatchGuard została zaprojektowana tak, aby zapewnić najszybszą przepustowość, przy włączonych wszystkich kontrolach bezpieczeństwa. Platforma może uruchamiać wszystkie silniki skanujące jednocześnie w celu zapewnienia maksymalnej ochrony, zachowując jednocześnie bardzo wysoką przepustowość.

WIDOCZNE ZAGROŻENIA

KOMPLETNA WIDOCZNOŚĆ

Zarówno w sali posiedzeń zarządu jak i w biurze oddziału, krytyczne decyzje dotyczące bezpieczeństwa często muszą być podejmowane szybko, zanim dojdzie do uszkodzenia. Ponadto warto wiedzieć, co dzieje się nie tylko w sieci, ale także na urządzeniach wewnątrz i na zewnątrz zapory sieciowej. Widoczność osiągana jest przez przekształcenie danych w informacje, które łatwo można uzyskać i wykorzystać. Dodanie czujnika hosta WatchGuard, dostępnego poprzez funkcję wykrywania i reagowania na zagrożenia, zapewnia ciągłe monitorowanie zdarzeń, wykrywanie i usuwanie zagrożeń w punkcie końcowym. Platforma widoczności sieciowej WatchGuard Dimension pobiera dane ze wszystkich urządzeń w sieci i przedstawia je w formie wizualnych informacji. Używając narzędzia Dimension można zidentyfikować trendy behawioralne, wskazać potencjalne zagrożenia sieciowe, zablokować niewłaściwe użytkowanie, monitorować stan sieci.

O WatchGuard

WatchGuard® Technologies, Inc. jest światowym liderem w dziedzinie bezpieczeństwa sieci, zabezpieczeń Wi-Fi, uwierzytelniania wieloczynnikowego i inteligencji sieciowej. Nagradzane produkty i usługi firmy cieszą się na całym świecie zaufaniem prawie 10 000 sprzedawców i dostawców usług ochrony, chroniących ponad 80 000 klientów. Misją WatchGuard jest zapewnienie bezpieczeństwa klasy korporacyjnej dostępnego dla firm wszystkich typów i wielkości poprzez prostotę, dzięki czemu WatchGuard jest idealnym rozwiązaniem dla rozproszonych przedsiębiorstw oraz tych małych i średnich. Siedziba firmy mieści się w Seattle, w stanie Waszyngton, a jej biura ulokowane są w Ameryce Północnej, Europie, Azji i Ameryce Łacińskiej. Aby dowiedzieć się więcej, odwiedź stronę internetową WatchGuard.com.

Usługi bezpieczeństwa **WatchGuard**

WatchGuard oferuje najbardziej wszechstronne portfolio usług z zakresu bezpieczeństwa sieciowego, począwszy od tradycyjnego IPS, GAV, kontroli aplikacji, blokowania spamu i filtrowania stron internetowych, a skończywszy na bardziej zaawansowanych usługach ochrony przed złośliwym oprogramowaniem, oprogramowaniem typu ransomware i utratą poufnych danych. Dostępny jest pełen pakiet usług w zakresie widoczności sieci i zarządzania.

PODSTAWOWE USŁUGI BEZPIECZEŃSTWA

ZAPOBIEGANIE WTARGNIĘCIOM (IPS)
Wykorzystuje stale aktualizowane sygnatury do skanowania ruchu we wszystkich głównych protokołach, zapewnieniając ochronę przed zagrożeniami sieciowymi w czasie rzeczywistym.

OCHRONA NA BAZIE REPUTACJI (RED)
Działająca w chmurze usługa chroni użytkowników przed złośliwymi witrynami i botnetami, jednocześnie znacząco poprawiając przetwarzanie danych w sieci.

WIDOCZNOŚĆ SIECI
Usługa oparta na subskrypcji, która generuje wizualną mapę wszystkich węzłów w sieci, abyś mógł łatwo zobaczyć, gdzie możesz spodziewać się zagrożenia.

FILTROWANIE WEBBLOCKER
Usługa automatycznie blokuje znane złośliwe witryny za pomocą narzędzi do filtrowania zawartości, aby wykluczyć nieodpowiednią zawartość i zwiększyć wydajność.

KONTROLA APLIKACJI
Zezwalanie, blokowanie, ograniczanie dostępu do aplikacji w oparciu o dział, funkcję pracy, porę dnia - monitorowanie dostępów w czasie rzeczywistym.

GATEWAY ANTIVIRUS (GAV)
Stale aktualizowane sygnatury identyfikują i blokują znane programy szpiegujące, wirusy, trojany i inne - w tym nowe warianty znanych wirusów.

SPAMBLOCKER
Wykrywanie spamu w czasie rzeczywistym (bloker sprawdza do 4 miliardów wiadomości dziennie).

Ujednolicone podejście do **bezpieczeństwa sieci**

Małe i średnie przedsiębiorstwa oraz firmy rozproszone nieustannie padają ofiarą zaawansowanych zagrożeń, które poważnie wpływają na bezpieczeństwo działalności, niezależnie od istniejących zabezpieczeń.
Dzięki pakietowi Total Security Suite organizacje każdej wielkości mogą korzystać z funkcji zapobiegania, wykrywania, korelacji i reagowania od brzegu sieci do punktu końcowego.

ThreatSync, oparty na chmurze silnik korelacji i oceny zagrożeń, gromadzi dane o zdarzeniach sieciowych z kilku usług bezpieczeństwa w Firebox, w tym APT Blocker, Reputation Enabled Defense, Gateway AntiVirus i WebBlocker. Jest on skorelowany z aktywnością zagrożeń, wykrywaną przez czujnik hosta WatchGuard Host Sensor, co zapewnia jednolite spojrzenie na środowisko i pozwala przypisać kompleksowy wynik w zależności od stopnia zagrożenia.

ZAAWANSOWANE USŁUGI BEZPIECZEŃSTWA

APT BLOCKER – ZAAWANSOWANA OCHRONA PRZED MALWARE

Wykrywa i zatrzymuje najbardziej wyrafinowane ataki, w tym ransomware i zagrożenia typu zero day.

OCHRONA PRZED UTRATĄ DANYCH (DLP)

Zapobiega przypadkowemu lub złośliwemu wyciekowi danych, poprzez skanowanie tekstu i powszechnych plików pod kątem poufnych informacji próbujących opuścić sieć.

PORTAL DOSTĘPOWY

Zapewnia centralną lokalizację dla dostępu do aplikacji hostowanych w chmurze oraz bezpieczny dostęp do zasobów wewnętrznych za pomocą protokołu RDP i SSH.

DIMENSION COMMAND

Umożliwia dostęp do wielu funkcji kontroli sieci, w tym do zmian konfiguracji za pomocą jednego kliknięcia, z dostępem do poszczególnych urządzeń poprzez interfejs webowy i narzędzia do zarządzania VPN.

WYKRYWANIE I REAGOWANIE NA ZAGROŻENIA (TDR)

Usługa koreluje zdarzenia w sieci ze zdarzeniami na punktach końcowych pod kątem bezpieczeństwa. Wykrywa zagrożenia, ustala priorytety i umożliwia natychmiastowe działanie w celu powstrzymania ataków.

DNSWATCH™

Ogranicza infekcje poprzez blokowanie złośliwych żądań DNS, przekierowując użytkowników do informacji o najlepszych praktykach w zakresie bezpieczeństwa.

INTELLIGENTAV™

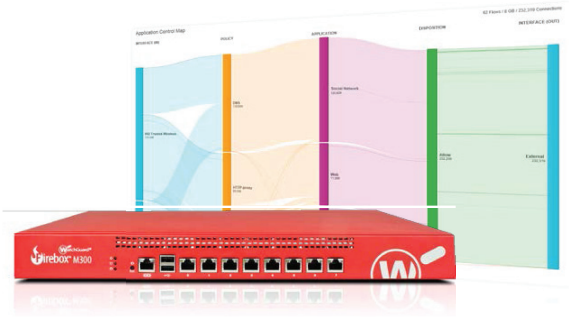
To rozwiązanie typu anty-malware, które w oparciu o sztuczną inteligencję automatyzuje wykrywanie złośliwego oprogramowania. Wykorzystując dogłębną analizę statystyczną, może sklasyfikować obecne i przyszłe ataki w zaledwie kilka sekund.

ROZWIĄZANIA FIREBOX

Produkt	Liczba użytkowników	Wydajność					Licencje VPN Licencje współdzielone		Charakterystyka				
WatchGuard Firewall	Recommended, not licensed	Firewall	AV	IPS	UTM	VPN	Site to Site Tunnels	Mobile SSL / IPSec	1 Gig Ports	Fiber Ports	#Empty Module Bays	Form Factor	Dual Power Supply
Firebox T15	5	400 Mbps	120 Mbps	160 Mbps	90 Mbps	150 Mbps	5	5	3	0	0	Tabletop	No
Firebox T35	20	940 Mbps	325 Mbps	573 Mbps	278 Mbps	560 Mbps	25	25	5 incl. 1 PoE+	0	0	Tabletop	No
Firebox T55	30	1 Gbps	636 Mbps	636 Mbps	523 Mbps	360 Mbps	40	50	5 incl. 1 PoE+	0	0	Tabletop	No
Firebox T70	60	4 Gbps	1.2 Gbps	1.5 Gbps	1.1 Gbps	750 Mbps	50	60	8 incl. 2 PoE+	0	0	Tabletop	No
Firebox M270	60	4.9 Gbps	2.1 Gbps	2.3 Gbps	1.6 Gbps	1.6 Gbps	50	75	8	0	0	1U rack	No
Firebox M370	150	8 Gbps	3.0 Gbps	4.8 Gbps	2.6 Gbps	4.6 Gbps	100	100	8	0	0	1U rack	No
Firebox M470	450	19.6 Gbps	3.5 Gbps	5.7 Gbps	3.1 Gbps	5.2 Gbps	250	250	8	Optional	1	1U rack	No
Firebox M440	450	6.7 Gbps	2.2 Gbps	2.2 Gbps	1.6 Gbps	3.2 Gbps	600	300	25 incl. 8 PoE+	2 x 10G SFP+	0	1U rack	Optional
Firebox M570	600	26.6 Gbps	5.4 Gbps	8.0 Gbps	4.4 Gbps	5.8 Gbps	500	500	8	Optional	1	1U rack	No
Firebox M670	850	34 Gbps	6.2 Gbps	10.4 Gbps	5.4 Gbps	7.6 Gbps	750	750	8	Optional	1	1U rack	No
Firebox M4600	1500	40 Gbps	9 Gbps	13 Gbps	8 Gbps	10 Gbps	5,000	10,000	8	Optional	2	1U rack	Yes
Firebox M5600	7500	60 Gbps	12 Gbps	18 Gbps	11 Gbps	10 Gbps	Unre-stricted	Unre-stricted	8 x 1Gb 4x10Gb	Optional	2	1U rack	Yes

POTĘGA WIDOCZNOŚCI

WatchGuard Dimension to darmowe rozwiązanie, które jest standardowo dostarczane z każdą platformą bezpieczeństwa WatchGuard. Zapewnia pakiet narzędzi do analizy, prezentacji i raportowania danych, które natychmiast identyfikują kluczowe zagrożenia i problemy, przyspieszając tym samym ustalanie zasad bezpieczeństwa w obrębie całej sieci. Aktywacja funkcji Dimension Command odblokowuje dostęp do różnych funkcji kontroli sieci: do zmian konfiguracji za pomocą jednego kliknięcia, możliwości powrotu do poprzednich konfiguracji, bezpośredniego dostępu do poszczególnych urządzeń poprzez interfejs sieciowy i narzędzia zarządzania VPN. Dostępne jako usługa chmurowa lub rozwiązanie do instalacji w środowiskach wirtualnych.



Jedno urządzenie - **pełne bezpieczeństwo**

Misją w WatchGuard jest prostota. Opracowaliśmy dwa pakiety, które upraszczają proces podejmowania decyzji podczas wyboru rozwiązania bezpieczeństwa. Pakiety Total i Basic Security Suite są dostępne w naszych urządzeniach Firebox serii T i M oraz w modelach Firebox Cloud i FireboxV virtual.

- Pakiet **Basic Security Suite** zawiera wszystkie tradycyjne usługi bezpieczeństwa sieciowego, typowe dla urządzeń UTM: IPS, GAV, filtrowanie adresów URL, kontrolę aplikacji, blokowanie spamu i wyszukiwanie reputacji. Obejmuje on również scentralizowane zarządzanie i funkcję widoczności sieci, jak również standardowe wsparcie 24x7.

- Pakiet **Total Security Suite** obejmuje wszystkie usługi oferowane wraz z pakietem Basic Security Suite oraz zaawansowaną ochronę przed złośliwym oprogramowaniem, ochronę przed utratą danych, zwiększonymi możliwościami widoczności sieci, bezpiecznym portalem dostępowym oraz możliwością podejmowania działań przeciwko zagrożeniom bezpośrednio z platformy Dimension - odpowiedzialnej za widoczność sieci.

FUNKCJE I USŁUGI	TOTAL SECURITY SUITE	BASIC SECURITY SUITE
Zapobieganie wtargnięciom (IPS)	✔	✔
Kontrola aplikacji	✔	✔
WebBlocker	✔	✔
SpamBlocker	✔	✔
Gateway AntiVirus	✔	✔
Ochrona w oparciu o reputacje (RED)	✔	✔
Odkrywanie sieci	✔	✔
APT Blocker	✔	
Ochrona przed utratą danych (DLP)	✔	
Threat Detection & Response	✔	
DNSWatch	✔	
Portal dostępowy	✔	
IntelligentAV*	✔	
Dimension Command	✔	
Wsparcie	**GOLD (24X7)**	Standard (24x7)

O Veracomp

Veracomp jest dystrybutorem rozwiązań teleinformatycznych realizującym model dystrybucji z wartością dodaną (VAD), dysponując wieloletnim doświadczeniem w obszarze bezpieczeństwa sieciowego. Firma oferuje szeroką gamę nowych technologii, mając w ofercie produkty ponad 130 producentów i działając obecnie w 18 krajach. Na rynku obecna jest od 1991 roku. Aby dowiedzieć się więcej, odwiedź stronę veracomp.pl

Kontakt: Michał Jurczak, Product Manager WatchGuard w Veracomp SA, tel. +48 691 480 113, e-mail: michal.jurczak@veracomp.pl