WatchGuard

6 KLUCZOWYCH CECH NOWOCZESNEGO FIREWALLA

1. WYSOKA WYDAJNOŚĆ KONTROLA SSL/TLS

Jeżeli nie używasz HTTPS i kontroli treści, prawdopodobnie 2/3 złośliwego oprogramowania przedostaje się do twojej organizacji/ firmy. Ponad **80%** ruchu biznesowego odbywa się za pośrednictwem kanałów szyfrowania i 50% witryn phishingowych używa protokołu HTTPS do ukrywania swoich ataków.

Inspekcja HTTPS umożliwia odszyfrowanie ruchu HTTPS oraz zbadanie pliku z treścią pod kątem oznak ataku. Następnie ponownie szyfruje ruch za pomocą nowego certyfikatu dla bezpieczeństwa.

BEZ ODSZYFROWANIA

Brak wglądu w typ danych, aplikacje, zgodność, typy plików lub dane eksfiltracji przez HTTPS.

WSKAZÓWKI

Szukaj firewalla z wysoką wydajnością, inspekcją HTTPS w momencie, gdy wszystkie usługi bezpieczeństwa są aktywne.

Poszukaj rozwiązania, które obsługuje inspekcję FULL TLS 1.3.

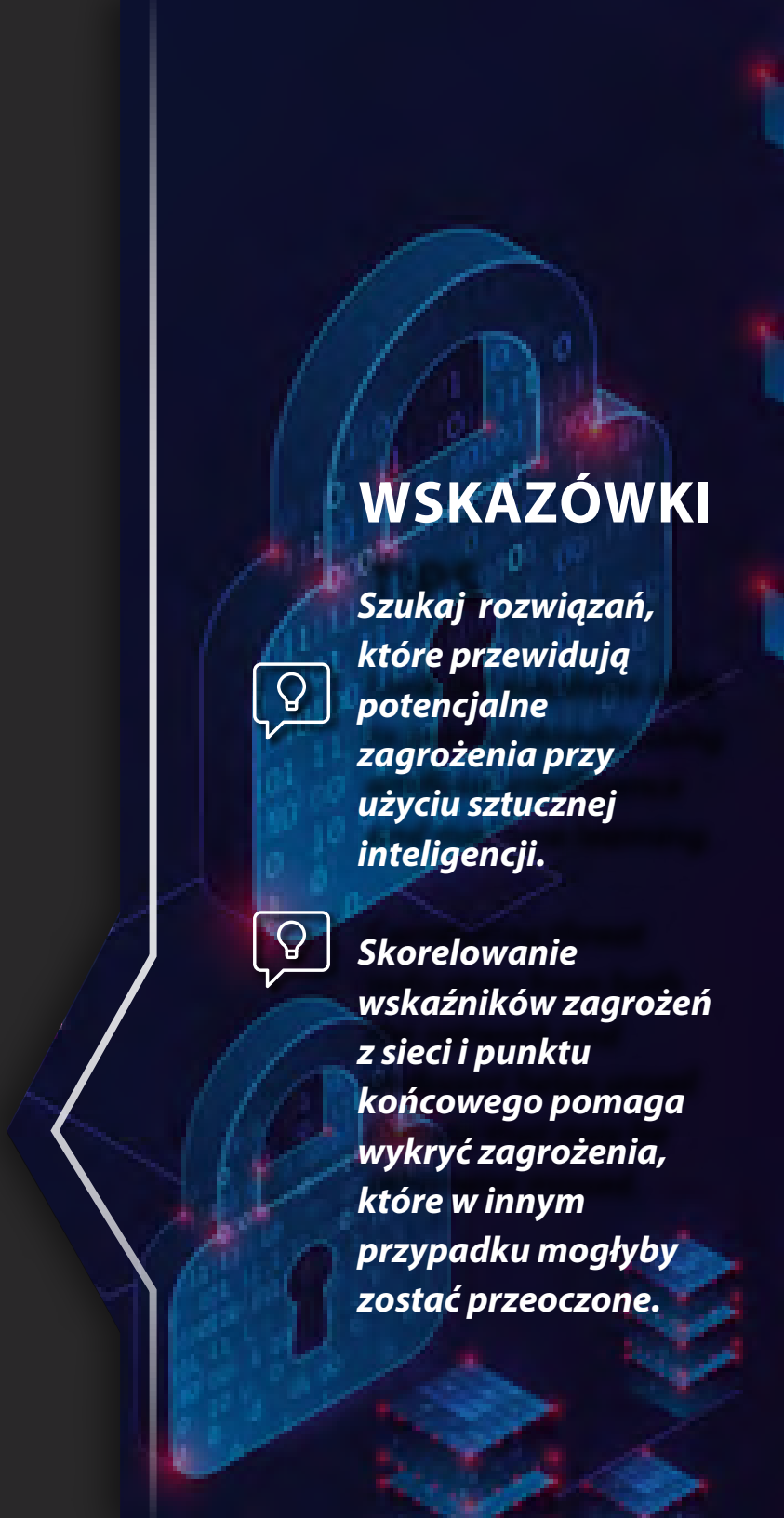
2. ATAK ZERO DAY

OBRONA PRZED ZŁOŚLIWYM OPROGRAMOWANIEM

Złośliwe oprogramowanie typu **zero-day** stanowi aż **64%** wszystkich zagrożeń napotykanych w sferze biznesowej.
Atak tego typu to próba wykorzystania luki w zabezpieczeniach oprogramowania lub sprzętu komputerowego. Istnieją oczywiście środki zapobiegawcze. Dokładane mechanizmy ataku nie są jednak znane.

WARSTWA MAKSYMALNEGO KRYCIA

Wykrywanie oparte na sztucznej inteligencji, chmurze, sandboxingu, zintegrowanym endpoincie.



WSKAZÓWKI

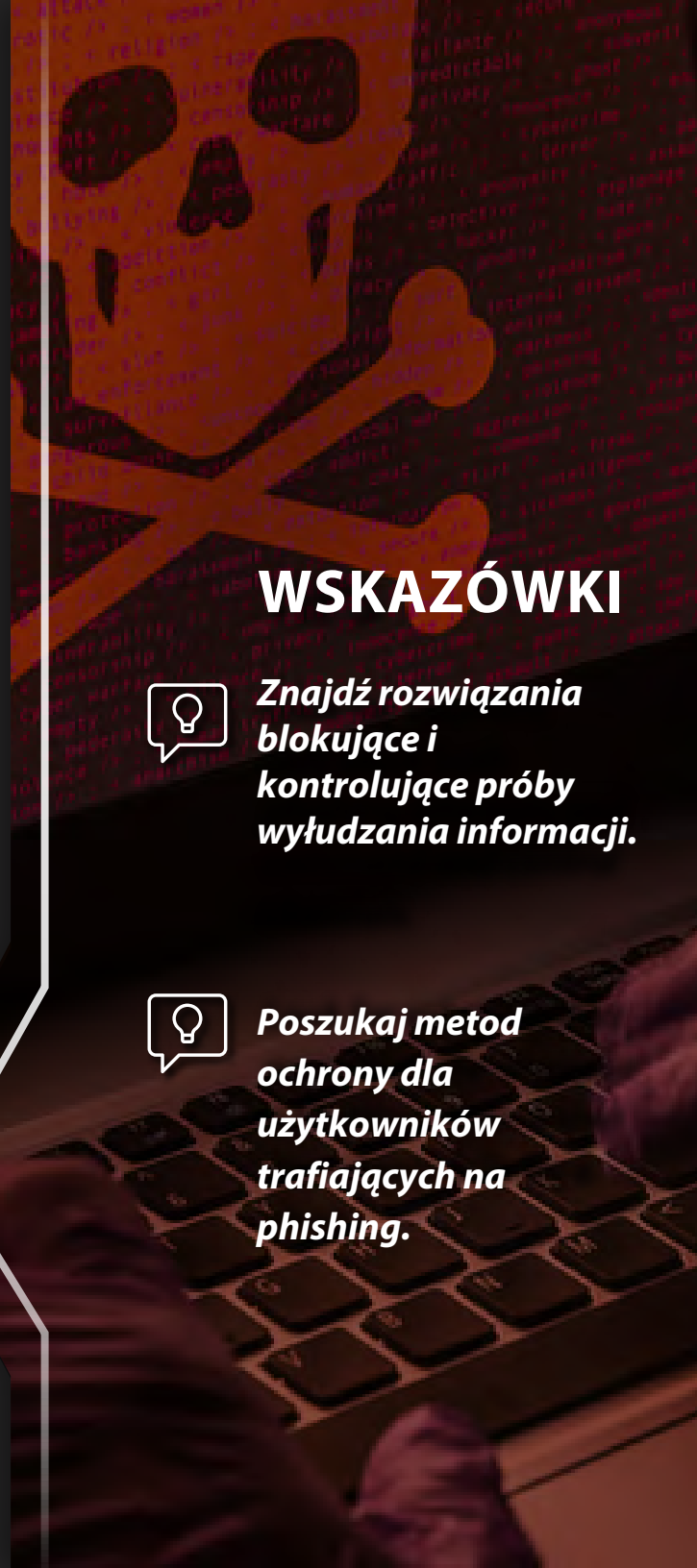
Szukaj rozwiązań, które przewidują potencjalne zagrożenia przy użyciu sztucznej inteligencji.

Skorelowanie wskaźników zagrożeń z sieci i punktu końcowego pomaga wykryć zagrożenia, które w innym przypadku mogłyby zostać przeoczone.

3. PHISHING AND HAPPY-CLICKER-OCHRONA

83% firm padło ofiarą ataku phishingowego. Hakerzy wykorzystują DNS do wyłudzania danych, dlatego warto zachować ostrożność. Badanie żądań DNS to świetny sposób na wykrycie i ostateczne przechwytywanie ataków. Nieświadome próby połączenia się ze złośliwym adresem DNS mogą być automatycznie blokowane, a użytkownik bezproblemowo przekierowany na bezpiecznie załadowaną stronę.

PIERWSZA LINIA OBRONY:
Blokuj złośliwe wyłudzenia kliknięć, phishing, podejrzane domeny niezależnie od typu połączenia i protokołów.



WSKAZÓWKI

Znajdź rozwiązania blokujące i kontrolujące próby wyłudzania informacji.

Poszukaj metod ochrony dla użytkowników trafiających na phishing.

4. PORTAL INTERNETOWY: BEZPIECZNY DOSTĘP

Przeciętny użytkownik spędza miesięcznie około **36 minut** na wprowadzaniu poświadczeń, co przekłada się na prawie cały dzień roboczy na pracownika.

Dzięki jednorazowemu logowaniu pracownicy mogą zaznaczyć zestaw poświadczeń tylko raz. Jest on dostępny dla wszystkich aplikacji, witryn internetowych. SSO poprawia ogólne bezpieczeństwo haseł, odciąża zespoły IT (prośby o resetowanie hasła).

DOBRE PRAKTYKI:
Połącz SSO z MFA, aby zabezpieczyć RDP (zdalny pulpit), SSH i dostęp do sieci.

WSKAZÓWKI

Upewnij się, że portal wspiera systemy, takie jak np. AuthPoint, Shibboleth, OneLogin, ADFS i Okta.

Poszukaj wspólnych rozwiązań dla oprogramowań: AuthPoint, Okta Mobile, Google Authenticator, OneLogin Protect, Duo Mobilny, RSA SecureID.

5. WSPIERAJ

NAJNOWSZĄ TECHNOLOGIĘ VPN

68% firm rozszerzyło korzystanie z VPN w związku z pandemią COVID-19 i przejściu na pracę zdalną.

Wirtualne sieci prywatne (VPN) służą przede wszystkim do zapewniania bezpiecznego połączenia pomiędzy centralą firmy, a oddziałem. Istnieje kilka różnych typów technologii VPN dla użytkowników mobilnych lub zdalnych. Niektórzy dostawcy zapór sprzedają dodatkowe licencje VPN wraz z rozszerzeniem Firewall. Inne usługi obejmują pełną licencję z rozszerzeniem.

TECHNOLOGIE VPN: IKEv2 najnowszy, najszybszy), IPSec (ale nie używaj kluczy wstępnych), SSL (najczęściej używany), L2TP (starsze, unikaj!).

WSKAZÓWKI

Usługa MFA powinna być stosowana podczas logowania się do aplikacji hostowanych w chmurze (SaaS), a także do dostępu VPN do sieci korporacyjnych.

Poszukaj platform obsługujących domyślną trasę tunelu ruchu do centrali zapory ogniowej, dzięki temu zachowasz pełne bezpieczeństwo.

6. RODZIMA AUTOMATYZACJA

Automatyzacja skraca czas pracy, wydatki, zarządzanie bezpieczeństwem nawet o **80%.** Aby dotrzymać kroku pojawiającym się zagrożeniom, ograniczyć marnotrawstwo czasu i pieniędzy, zadbaj o wysoki stopień technizacji.

Zunifikowane platformy zwiększą bezpieczeństwo.

4 POZIOMY AUTOMATYZACJI:
Zarządzanie, operacja, responsywność i predykcja.

WSKAZÓWKI

Integracja z RRM i narzędzia PSA odpowiadają większym wymaganiom.

Sztuczna inteligencja pomaga w blokowaniu zaawanasowanych zagrożeń, nie ma potrzeby zatrudniania aż tylu ekspertów.

Firebox®

1. Najlepsze w swojej klasie odszyfrowanie SSL/TLS.
2. 3 warstowowa ochrona przed atakami zero-day.
3. Oparte na chmurze filtrowanie DNS.
4. Portal dostępowy w standarzie.
5. 4 typy mobilnej sieci VPN, w tym IKEv2.
6. Zapewnia wszystkie 4 poziomy automatyzacji bezpieczeństwa.

Czytaj więcej na watchguard.com/wgrd-products/firewall-appliances

250
ataków sieciowych

1,300
złośliwych plików

~ średnia liczba zagrożeń zablokowanych na Firebox w 2019 roku.

WatchGuard, to wysokie bezpieczeństwo i skuteczność, przy zachowaniu jednocześnie niskich kosztów eksploatacyjnych. Jest jednym z firewalli, które blokują **100% ataków.**

- NSS Labs

PORTFOLIO WATCHGUARD

Ochrona brzegu sieci

Rozwiązania są zaprojektowane i opracowane tak, aby wdrożenie, użycie, zarządzanie nimi nie było skomplikowane. Unikalne podejście skupia się głównie na bezpieczeństwie sieci, niezależnie od rozmiaru, stanu technicznego, czy ekspertyzy.

Bezpieczne Wi-Fi

Rozwiązania WatchGuard to prawdziwy przełom na rynku. Firma odpowiednio zabezpiecza, chroni przestrzeń, jednocześnie eliminując błędy zmniejsza koszty. Ekspansywne narzędzia i duże zaangażowanie dostarcza przewagę nad konkurencją.

Uwierzytelnianie wieloskładnikowe

WatchGuard AuthPoint skutecznie rozwiązuje problem z lukami w hasłach dzięki wielu czynnikom uwierzytelniania. Platforma w chmurze posiada unikalne podejście. Dzięki dodanej funkcji "Mobile phone DNA'' do identyfikacji, odpowiednia osoba ma dostęp do sieci, chmury, czy aplikacji.

Ochrona końcówek

WatchGuard Endpoint Security to zaawansowane rozwiązanie dla Cloud-native. Portfolio chroni biznes mając na uwadze przyszłe ataki cybernetyczne. **Panda Adaptive Defense 360** napędza sztuczną inteligencję co sprawia, że natychmiast poprawia bezpieczeństwo. Połączenie Endpoint (EPP) i zdolności reagowania (EDR) chroni aplikacje - przed zero-trust.

ABOUT WATCHGUARD

WatchGuard® Technologies, Inc. is a global leader in network security, endpoint security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by more than18,000 security resellers and service providers to protect more than 250,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America.

To learn more, visit **WatchGuard.com**.

NORTH AMERICA SALES 1.800.734.9905 INTERNATIONAL SALES 1.206.613.0895 WEB www.watchguard.com