FORCEPOINT
POWERED BY Raytheon

Karta produktu

Protecting the human point.

FORCEPOINT Intrusion PreventionSystem

Forcepoint oferuje najbezpieczniejsze na rynku* systemy ips do ochrony rozproszonych sieci przedsiębiorstw – centra danych, biura, oddziały i chmura.

*NSS Labs NGIPS Test 2017

Rozwiązania Forcepoint dotyczące bezpieczeństwa sieci oferują najbezpieczniejszy na rynku system wykrywania i zapobiegania włamaniom (IPS).
Najlepiej oceniany w niezależnych testach system IPS firmy Forcepoint może być wdrożony jako samodzielne urządzenie Layer 2 IPS lub jako część kompleksowej zapory nowej generacji Layer 3 (NGFW) w środowisku fizycznym, wirtualnym i w chmurze. System eliminuje próby obejścia zabezpieczeń, exploity i złośliwe oprogramowanie, które hakerzy wykorzystują do penetracji sieci przedsiębiorstw i eksfiltracji danych.

Wyjątkowa architektura zapewniająca wydajność i szybkość działania

Do przeprowadzania kontroli Forcepoint wykorzystuje dynamiczną kontrolę strumienia danych, które wykracza poza zwykłą inspekcję pakietów. Rekonstruuje i analizuje rzeczywistą zawartość, eliminując techniki obejścia zabezpieczeń, które przenoszą exploity i złośliwe oprogramowanie.

Ponadto wydajne dekodowanie ruchu szyfrowanego demaskuje ataki ukryte w transmisji SSL/TLS.
Forcepoint analizuje każdy strumień danych, dekodując różne warstwy protokołu IP w celu znalezienia nieprawidłowych lub zmienionych parametrów protokołu, metadanych i nagłówków.

Następnie Forcepoint stosuje zaawansowane techniki analizy zawartości pod kątem występowania exploitów mających na celu wykorzystanie luk w systemach.
W przeciwieństwie do rozbudowanych mechanizmów sygnatur opartych na wzorcach, podejście Forcepoint umożliwia identyfikację takich ataków za pomocą jednego fingerprintu. Fingerprinty dopasowywane są za pomocą szybkiego mechanizmu deterministycznego (ang. deterministic finite automata, DFA) dostosowanego do każdego kontekstu protokołu, umożliwiając dołączanie nowych fingerprintów bez wpływu na wydajność.

O krok przed hakerami dzięki ciągłym aktualizacjom

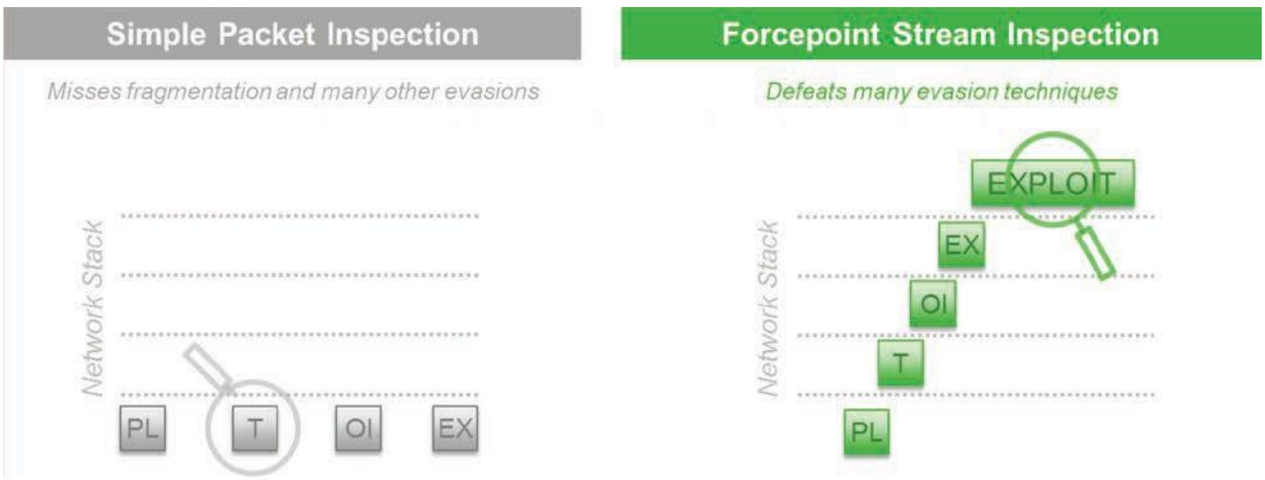
Globalny zespół badawczy Forcepoint nieustannie analizuje źródła informacji o zagrożeniach, raporty o podatnościach oraz różne systemy testowe do analizy exploitów i luk w zabezpieczeniach. Nowe aktualizacje fingerprintów publikowane są w razie potrzeby za pośrednictwem naszej usługi w chmurze i są automatycznie pobierane przez systemy bezpieczeństwa sieciowego Forcepoint. To proaktywne podejście daje zespołom IT czas na analizę nowo wprowadzonych zmian i implementację poprawek bezpieczeństwa bez obawy o narażenie na atak.

Przeciwdziałanie atakom Zero-Day i treściom niepożądanym

Produkty bezpieczeństwa sieciowego Forcepoint zapewniają także wiele warstw ochrony przed nieznanymi wcześniej atakami i treścią niepożądaną. Przesyłane pliki są poddawane rygorystycznej kontroli reputacji i złośliwego oprogramowania, a dzięki naszej zaawansowanej technologii sandboxing'u, skutecznie wykrywamy nowe zagrożenia takie jak ataki typu zero-day. Forcepoint jest jednym z pionierów w kategoryzacji i filtrowaniu stron internetowych i treści. Dzięki naszym urządzeniom IPS i NGFW organizacje mogą lepiej przestrzegać przepisów obowiązujących w miejscu pracy, ograniczyć narażenie na kradzież danych osobowych i uniemożliwić użytkownikom odwiedzanie stron internetowych zawierających niebezpieczne treści.

Funkcjonalność Fail-Open

Urządzenia Forcepoint obsługują szereg modułowych kart interfejsów sieciowych, w tym interfejsy typu fail-open, które utrzymują ruch nawet gdy IPS straci zasilanie.



FORCEPOINT ŁĄCZY REKONSTRUKCJĘ STRUMENIOWĄ Z SZYBKIM FINGERPRINTINGIEM EXPLOITÓW

Ochrona twojego biznesu

Każdego dnia hakerzy stają się coraz skuteczniejsi w penetrowaniu sieci korporacyjnych, aplikacji, centrów danych i punktów końcowych. Gdy dostaną się do środka, mogą ukraść własność intelektualną, informacje o klientach i inne wrażliwe dane, powodując nieodwracalne szkody w działaniu firmy i jej reputacji.

Ataki internetowe wykraczają poza zwykłe exploity. Złodzieje coraz częściej stosują nowe techniki, by uniknąć wykrycia przez tradycyjne urządzenia sieci bezpieczeństwa, w tym zapory ogniowe.

Takie działania prowadzone są na wielu poziomach, aby zakamuflować exploity i złośliwe oprogramowanie, sprawiając, że stają się one niewidoczne dla tradycyjnej kontroli pakietów opartej na sygnaturach. W przypadku unikania wykrycia nawet stare ataki, które były przez lata blokowane, mogą nagle zostać wykorzystane do naruszenia bezpieczeństwa systemów wewnętrznych.

Forcepoint stosuje inne podejście. Nasz wiodący w branży silnik IPS przeznaczony jest do wszystkich trzech etapów ochrony sieci: blokowania prób obejścia zabezpieczeń, wykrywania exploitów i zatrzymywania złośliwego oprogramowania. Może być wdrożony w sposób transparentny za istniejącymi zaporami ogniowymi aby zapewnić ochronę bez modyfikacji istniejącej sieci lub jako część naszego kompleksowego rozwiązania NGFW dla zachowania pełnego bezpieczeństwa.

Wszystkie produkty bezpieczeństwa sieciowego Forcepoint są stale aktualizowane oraz centralnie zarządzane a dostęp do polityk bezpieczeństwa i dashboard'ów udostępniany jest w całej sieci. Z Forcepoint możesz bezpiecznie, niezawodnie i wydajnie prowadzić swoją działalność zapewniając bezpieczenstwo centrów danych, sieci biurowych, oddziałów i środowisk w chmurze.

Zalety biznesowe

- **Mniej naruszeń bezpieczeństwa danych**
- **Większe bezpieczeństwo bez przerw w działalności**
- **Mniejsze narażenie na nowe zagrożenia, gdy zespoły IT implementują nowe poprawki bezpieczeństwa**
- **Zabezpieczenie oddziałów, chmur lub centrów danych**
- **Obniżenie TCO dotyczącego bezpieczeństwa i infrastruktury sieci**

Główne cechy

- **Wdrożenie w formie Layer 2 IPS lub jako część kompleksowego Layer 3 NGFW**
- **Inspekcja typu Stream-based**
- **Pionier w dziedzinie ochrony przed naruszeniami bezpieczeństwa**
- **Deszyfrowanie z granularną kontrolą prywatności**
- **Wykrywanie anomalii dot. użycia protokołów**
- **Wykrywanie exploitów i złośliwego oprogramowania za pomocą mechanizmu DFA**
- **Wykrywanie Denial of Service (DoS)**
- **Ochrona typu Anti-bot**
- **Zero-day Sandboxing w chmurze lub za pomocą urządzeń typu appliance**
- **Najlepsze w branży filtrowanie adresów URL**
- **Interfejsy modułowe z fail-open**
- **Jednakowa funkcjonalność i wydajność niezależnie od sposobu implementacji**
- **Scentralizowane zarządzanie politykami**
- **Szybkie aktualizacje oprogramowania bez przestojów**

Specyfikacja Forcepoint Intrusion Prevention System (IPS)

OBSŁUGIWANE PLATFORMY	
Urządzenia	Wiele wersji sprzętowych/modularnych przeznaczonych dla centrów danych, obrzeży sieci i oddziałów
Infrastruktura chmury	Amazon Web Services, Microsoft Azure
Urządzenie wirtualne	Systemy x86 64-bit; VMware ESXi, VMware NSX, Microsoft Hyper-V i środowisko wirtualizowane KVM
Tryby działania	Jako IPS (layer 2, z opcjonalnymi modułami typu fail-open) lub jako część NGFW (layer 3)
Kontekst wirtualny	Oddzielne, wirtualne konteksty logiczne; przypisanie osobnych interfejsów i polityk do każdego kontekstu wirtualnego w obrębie jednego urządzenia fizycznego typu Master

KONTROLA	
Multi-Layer Traffic Normalization / Full-Steam Deep Inspection	• Rekonstruuje i analizuje rzeczywistą zawartość, aby zapewnić integralność strumienia danych • Odrzuca zduplikowane segmenty danych, które mogą doprowadzić do nieoczekiwanych rezultatów po ponownej rekonstrukcji
Anti-Evasion Defense	Zatrzymuje: fragmenty typu out-of-order oraz overlapping, manipulowanie protokołami, techniki typu obfuscation oraz bazujące na kodowaniu zawartości
Dynamic Context Detection	Protokół, aplikacja, typ pliku
Protocol-Specific Traffic Handling / Inspection	Ethernet, H.323, GRE, IPv4, IPv6, ICMP, IP-in-IP, enkapsulacja IPv6, UDP, TCP, DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, MGCP, MSRPC, NetBIOS Datagram, OPC Classic, OPC UA, Oracle SQL Net ,POP3, POP3S, RSH, RSTP, SIP, SMTP, SSH, SunRPC, NBT, SCCP, SMB, SMB2, SIP, TCP Proxy, TFTP, zintegrowana inspekcja za pomocą proxy Sidewinder
Granular Decryption of SSL/TLS Traffic	• Wysokowydajne de-szyfrowanie SSL/TLS - dla klienta i serwera • Kontrola prywatności użytkowników i ochrona organizacji przed kradzieżą danych osobowych • Sprawdzanie ważności certyfikatu TLS i listy wyjątków na podstawie nazwy domeny certyfikatu
Vulnerability Exploit Detection	• Rozwiązanie niezależne od protokołów, dowolny protokół TCP/UDP, logowanie nieprawidłowości i prób uniknięcia wykrycia • Virual patching podatności CVE - dla serwerów i stacji roboczych • Zaawansowane fingerprint'y eliminują konieczność stosowania wielu sygnatur • Szybki silnik deterministyczny (deterministic finite automata - DFA), dopasowanie nowych fingerprintów • Ciągła aktualizacja fingerprintów ze strony Forcepoint
Custom Fingerprinting	• Dopasowywanie fingerprint'u niezależnie od protokołu • Tworzenie własnych fingerprint z użyciem regular expression • Fingerprint dla własnych, niestandardowych aplikacji
Rozpoznanie skanowania	Skan TCP/UDP/ICMP, wykrywanie metod stealth i slow scan w IPv4 i IPv6
Anti-Botnet	• Wykrywanie oparte na deszyfrowaniu transmisji • Analiza sekwencji długości komunikatów
Korelacja	Korelacja lokalna, korelacja na serwerze logów
Ochrona DoS/DDoS	• Wykrywanie SYN/UDP flood • Ograniczanie ilości jednoczesnych połączeń, kompresja logów per interfejs • Ochrona przed slow HTTP request, limit półotwartych połączeń • Rozdzielenie Control Plane i Data Plane
Metody blokowania	Bezpośrednie blokowanie, resetowanie połączenia, blacklisting (lokalny i rozproszony), HTML response, przekierowanie HTTP
Rejestracja ruchu	Automatyczna rejestracja ruchu/pcap z zapisem ataku
Automatyczne aktualizacje	• Dynamiczne aktualizacje za pomocą Centrum Zarządzania Bezpieczeństwem Forcepoint Security Management Center (SMC)

Specyfikacja systemu Forcepoint Intrusion Prevention System (IPS) c.d.

ZAAWANSOWANE WYKRYWANIE ZŁOŚLIWEGO OPROGRAMOWANIA I KONTROLA PLIKU	
Protokoły	FTP, HTTP, HTTPS, POP3, IMAP, SMTP
Filtrowanie plików	Polityka filtrowania plików. Ponad 200 obsługiwanych typów plików w 19 kategoriach
Reputacja pliku	Kontrola i blokowanie złośliwego oprogramowania na podstawie reputacji pliku (usługa w chmurze). Opcjonalne, lokalna kontrola reputacji z pomocą McAfee TIE przez DxL.
Antywirusowe skanowanie pliku	Lokalny silnik antywirusowy*
Zero-Day Sandboxing	SANDBOX - Forcepoint Advanced Malware Detection dostępny w opcji w chmurze jak i w formie appliance

FILTROWANIE ADRESÓW URL	
Kategoryzacja URL	Za pomocą Forcepoint ThreatSeeker Intelligence, ten sam mechanizm jak w przypadku Forcepoint Web Security i Forcepoint Email Security
Automatyczne aktualizacje	Nieustannie aktualizowane ze względu na analizę nowych witryn
Wdrożenie strategii dostępu wg kategorii	Forcepoint NGFW URL Filtering w formie subskrypcji add-on

ZARZĄDZANIE I MONITORING	
Interfejs zarządzania	Scentralizowany system zarządzania na poziomie przedsiębiorstwa z funkcjami analizy, monitorowania i raportowania logów (szczegółowe informacje w karcie produktu Forcepoint Security Management Center)
Monitoring SNMP	SNMPv1, SNMPv2c i SNMPv3
Rejestracja ruchu	Narzędzie tcpdump, rejestracja zdalna przez Forcepoint Security Management Center
High Security Management Communication	Szyfrowanie komunikacji pomiędzy komponentami systemu z użyciem klucza 256-bit
Certyfikaty bezpieczeństwa	Common Criteria Network Devices Protection Profile with Extended Package Stateful Traffic Filter Firewall, FIPS 140-2 crypto certificate, CSPN od ANSSI, (First Level Security Certification USGv6)

*Niedostępne dla urządzeń 110/115.

KONTAKT
www.forcepoint.com/contact
Biuro Forcepoint Polska
ul. Gintrowskiego 53
02-697 Warszawa
Tel.+48 225 480 100

Anna Zawadzka
Team Leader Territory Manager Poland
anna.zawadzka@forcepoint.com,
tel. 600 301 512

Agnieszka Mucha
Channel Account Manager,
Agnieszka.mucha@forcepoint.com,
tel. 603 990 533

[DATASHEET_FORCEPOINT_TEMPLATE_EN] XXXXXX.062817