**Fortinet rozbudowuje funkcjonalność systemu FortiOS**

*Najnowsza wersja FortiOS, jedynego systemu operacyjnego, który w płynny sposób łączy funkcje sieciowe i bezpieczeństwa, a także rozbudowa platformy Security Fabric zapewniają nowe możliwości związane z generatywną sztuczną inteligencją, ochroną danych, usługami zarządzanymi i ujednoliconymi agentami*

**[Warszawa, 12.04.2024] Fortinet, globalny lider cyberbezpieczeństwa który dąży do konwergencji sieci i rozwiązań ochronnych, zaprezentował najnowszą wersję swojego** [**systemu operacyjnego FortiOS**](https://www.fortinet.com/products/fortigate/fortios.html?utm_source=pr&utm_medium=pr&utm_campaign=fortios) **oraz szereg znaczących usprawnień platformy cyberbezpieczeństwa** [**Fortinet Security Fabric**](https://www.fortinet.com/solutions/enterprise-midsize-business/security-fabric?utm_source=pr&utm_medium=pr&utm_campaign=security-fabric)**.**

FortiOS 7.6 zapewnia użytkownikom skuteczniejsze ograniczanie ryzyka, zmniejszanie złożoności środowiska bezpieczeństwa oraz poprawia ich komfort pracy w sieci dzięki nowym funkcjom obejmującym następujące obszary:

* **Setki usprawnień w FortiOS 7.6 zapewniają ulepszoną pracę całej platformy Fortinet Security Fabric** w takich obszarach jak [Secure SD-WAN](https://www.fortinet.com/products/sd-wan.html?utm_source=pr&utm_medium=pr&utm_campaign=sd-wan-web), [Secure Access Service Edge](https://www.fortinet.com/solutions/enterprise-midsize-business/unified-sase?utm_source=pr&utm_medium=pr&utm_campaign=unified-sase) (SASE), [Zero-Trust Network Access](https://www.fortinet.com/solutions/enterprise-midsize-business/network-access/application-access?utm_source=pr&utm_medium=pr&utm_campaign=ztna) (ZTNA), automatyzacja, wdrażanie i konfiguracja nowych komponentów infrastruktury, zdalna izolacja przeglądarki i [monitorowanie cyfrowych doświadczeń użytkowników](https://www.fortinet.com/products/fortimonitor?utm_source=pr&utm_medium=pr&utm_campaign=fortimonitor) (DEM), a wszystko to z elastycznymi opcjami korzystania w modelu konsumpcyjnym (SaaS lub PaaS).
* **GenAI ułatwia analizę zagrożeń i wdrażanie produktów** – W systemie FortiOS 7.6 obszernie wykorzystywane są możliwości generatywnej sztucznej inteligencji (GenAI) w celu przyspieszenia badania i usuwania zagrożeń. W FortiOS 7.6 zapewniono między innymi natywną integrację rozwiązania [FortiAI](https://www.fortinet.com/products/fortiai?utm_source=website&utm_medium=pr&utm_campaign=fortiai) (dawniej Fortinet Advisor) z centralnym jeziorem danych [FortiAnalyzer](https://www.fortinet.com/products/management/fortianalyzer?utm_source=website&utm_medium=pr&utm_campaign=pr-fortianalyzer) i jego ujednoliconą konsolą zarządzania [FortiManager](https://www.fortinet.com/products/management/fortimanager?utm_source=website&utm_medium=pr&utm_campaign=pr-fortimanager), co umożliwiło usprawnienie analizy zagrożeń i reagowania na nie, a także operacji sieciowych i bezpieczeństwa. Rozszerzenie FortiAI na całą platformę Fortinet Security Fabric ułatwia szybsze podejmowanie decyzji, pomaga szybko wykrywać i naprawiać incydenty oraz zapewnia przedsiębiorstwom możliwość łatwego wdrażania wymaganych rozwiązań.
* **Kompleksowe możliwości ochrony danych w całej sieci** – Zapewniane przez Fortinet Security Fabric scentralizowane zabezpieczanie danych w wielu punktach w całej sieci umożliwia większej liczbie przedsiębiorstw przyjęcie kompletnej strategii zapobiegania utracie danych (DLP) i zarządzanie nią. Ulepszone funkcje w FortiOS 7.6 zapewniają bezpieczeństwo poufnych informacji bez względu na to, gdzie znajdują się one w hybrydowej sieci.

Do platformy Fortinet Security Fabric wprowadzono także dodatkowe funkcje:

* **Instalowany na urządzeniach końcowych ujednolicony agent Fortinet uzupełniony o funkcje wykrywania zagrożeń i reagowania na nie** –[FortiClient](https://www.fortinet.com/products/endpoint-security/forticlient?utm_source=website&utm_medium=pr&utm_campaign=pr-forticlient), ujednolicony agent platformy Fortinet Security Fabric, został zintegrowany z rozwiązaniem EDR, które zapewnia pełne wykrywanie zagrożeń na urządzeniach końcowych i reagowanie na nie, co zapewnia ochronę przed atakami ransomware, wykrywanie zagrożeń bazujące na analizie zachowania złośliwego kodu i automatyczne reagowanie, a także głębszą widzialność środowiska IT, jego kontrolę i możliwości zdalnego dostępu w modelu ZTNA. Aby uprościć zarządzanie w złożonych środowiskach, Fortinet dostarcza ujednoliconego agenta, który integruje funkcjonalność wielu rozwiązań, w tym VPN, ZTNA, platformy ochrony urządzeń końcowych (EPP), EDR, DEM, kontroli dostępu do sieci (NAC) i SASE.
* **Więcej sposobów na walkę z niedoborem cyfrowych umiejętności** – Oprócz generatywnej sztucznej inteligencji, FortiAnalyzer umożliwia skorzystanie z opcjonalnych usług [SIEM](https://www.fortinet.com/products/siem/fortisiem?utm_source=pr&utm_medium=pr&utm_campaign=fortisiem) i [SOAR](https://www.fortinet.com/products/fortisoar?utm_source=pr&utm_medium=pr&utm_campaign=fortisoar), zapewniając szerszy zakres pozyskiwania danych i zautomatyzowane playbooki w celu usprawnienia wdrażania operacji bezpieczeństwa (SecOps). Ich rozszerzenie jest dostępne już teraz dzięki ofercie [SOC-as-a-Service](https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/socaas?utm_source=website&utm_medium=pr&utm_campaign=pr-socaas), która wspomaga działy SecOps, natomiast obecnie dodana została zarządzana usługa FortiGate, aby wspierać zespoły operacji sieciowych. Usługi te odzwierciedlają zaangażowanie firmy Fortinet we wspieranie partnerów kanałowych w rozwijaniu ich portfolio w celu dotarcia do szerszego grona odbiorców oraz promowania najlepszych praktyk wdrożeniowych na całym świecie. Usługi te w szczególności pomagają partnerom skuteczniej przezwyciężyć trwający niedobór umiejętności związanych z rozwiązaniami IT i usprawnić cyfrową transformację ich klientów końcowych.

**Siła jednego systemu operacyjnego**

Zaangażowanie firmy Fortinet w integrację swojego portfolio w ramach jednego systemu operacyjnego, w połączeniu z inwestycjami w [specjalizowane układy ASIC](https://www.fortinet.com/products/fortigate/fortiasic?utm_source=pr&utm_medium=pr&utm_campaign=fortiasic), przyniosło wymierne korzyści klientom różnej wielkości w następujących obszarach:

* **Firewall** – Zapora sieciowa była pierwszą funkcją systemu operacyjnego FortiOS od jego powstania i nadal doskonale sprawdza się on w tej roli, zapewniając o rząd wielkości wyższą wydajność i energooszczędność dzięki zastosowaniu opracowanych przez Fortinet układów ASIC. Wykorzystanie jednego systemu operacyjnego we wszystkich modelach FortiGate, w połączeniu ze specjalistycznymi układami ASIC, umożliwiło stworzenie hybrydowej zapory sieciowej przyspieszającej pracę 14 aplikacji sieciowych i ochronnych, zabezpieczającej za pomocą spójnych zasad środowiska lokalne, zdalne i chmurowe oraz ułatwiającej zarządzanie nimi.
* **Segmentacja i ZTNA** – W przypadku urządzeń zarządzanych mechanizm ZTNA kontroluje uprawnienia użytkowników łączących się z aplikacjami i danymi oraz dokonuje segmentacji dostępu do aplikacji przy użyciu bramy aplikacyjnej znajdującej się także w FortiOS. Wewnętrzne mechanizmy segmentacyjne, włączone w obsługiwanej przez FortiOS zaporze sieciowej o wysokiej przepustowości i niskich opóźnieniach, dodatkowo ograniczają ruch boczny (lateral movement) generowany przez cyberprzestępców oraz podczas ataków ransomware.
* **Bezpieczeństwo infrastruktury OT, IoT i brzegowej** – Ponieważ FortiOS może kontrolować oraz zabezpieczać sieci przewodowe i bezprzewodowe, spójną ochroną mogą być objęte również urządzenia brzegowe, IoT, infrastruktura OT oraz inny sprzęt bezagentowy.
* **Zunifikowany dostęp SASE** – System FortiOS umożliwia stworzenie globalnej, skalowanej sieci składającej się z rozwiązań Fortinet, chroniącej pracowników hybrydowych i urządzenia działające w infrastrukturze brzegowej. Taka sieć wyposażona jest również w wiodącą w branży, wbudowaną w system FortiOS funkcjonalność SD-WAN, poprawiającą komfort pracy użytkowników.
* **Operacje bezpieczeństwa bazujące na sztucznej inteligencji** – Wszystkie scenariusze wykorzystania rozwiązań Fortinet uwzględniają ochronę bazującą na sztucznej inteligencji, której zapewnienie jest możliwe dzięki ujednoliconemu pozyskiwaniu danych, telemetrii i informacji o zagrożeniach za pośrednictwem naszego jednego jeziora danych oraz zastosowania systemu FortiOS w całej platformie Fortinet Security Fabric.

**Ken Xie, Founder, Chairman of the Board, and Chief Executive Officer, Fortinet**

Zakładając firmę Fortinet przyjęliśmy cel, którym jest wzmacnianie sieci naszych klientów poprzez ich konwergencję w bezpieczną infrastrukturę. Aby to osiągnąć, przez ostatnie dwie dekady koncentrowaliśmy się na organicznym rozwoju naszych rozwiązań z wykorzystaniem wspólnego systemu operacyjnego i inwestowaniu w nasze specjalistyczne procesory obliczeniowe FortiASIC. Obecnie FortiOS jest najpotężniejszym na świecie systemem operacyjnym umożliwiającym zabezpieczanie sieci w czasie rzeczywistym, który upraszcza zarządzanie treściami, aplikacjami, użytkownikami, urządzeniami, danymi i lokalizacjami. Natomiast nasze opatentowane procesory FortiASIC zapewniają bezprecedensową wydajność, niższe koszty użytkowania i mniejsze zużycie energii. Nasze ponad 20-letnie zaangażowanie w nieustanną innowacyjność w wyjątkowy sposób umożliwia współistnienie ponad 30 funkcji sieciowych i bezpieczeństwa, a teraz z dumą prezentujemy ulepszone wydanie systemu operacyjnego FortiOS 7.6, który wyznacza branżowe standardy.

**Dodatkowe zasoby**

* Więcej informacji o [zaprezentowanych nowych funkcjach systemu FortiOS](https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-accelerate-fortios.pdf).
* Więcej informacji o [Fortinet Security Fabric](https://www.fortinet.com/blog/business-and-technology/step-into-the-platform-era).
* Więcej informacji o organizowanych przez Fortinet [darmowych szkoleniach dotyczących cyberbezpieczeństwa](https://www.fortinet.com/training/cybersecurity-professionals?utm_source=blog&utm_medium=blog&utm_campaign=freetraining), obejmujących szeroki zakres informacji produktowych oraz budujących świadomość dotyczącą cyberzagrożeń. Jako część składowa strategii Fortinet Training Advancement Agenda (TAA), Fortinet Training Institute prowadzi także szkolenia i certyfikacje w ramach programów [Network Security Expert (NSE) Certification](https://www.fortinet.com/training-certification?utm_source=pr&utm_medium=pr&utm_campaign=NSE), [Academic Partner](https://www.fortinet.com/training/security-academy-program?utm_source=pr&utm_medium=pr&utm_campaign=academy) oraz [Education Outreach](https://www.fortinet.com/training/education-outreach-program?utm_source=pr&utm_medium=pr&utm_campaign=outreach).
* Profile firmy Fortinet w mediach społecznościowych: [Twitter](https://twitter.com/Fortinet), [LinkedIn](https://www.linkedin.com/company/fortinet), [Facebook](https://www.facebook.com/fortinet/), [YouTube](https://www.youtube.com/channel/UCJHo4AuVomwMRzgkA5DQEOA?sub_confirmation=1) oraz [Instagram](https://www.instagram.com/fortinet/). Dodatkowe informacje dostępne są także na [blogu](https://www.fortinet.com/blog?utm_source=blog&utm_medium=blog&utm_campaign=blog).

**O firmie Fortinet**

[Fortinet](https://www.fortinet.com/?utm_source=website&utm_medium=pr&utm_campaign=boiler) jest czołowym producentem systemów ochronnych i innowatorem przyczyniającym się do ich ewolucji, co umożliwiło stworzenie rozwiązań zapewniających konwergencję funkcji sieciowych i zabezpieczających środowisko IT. Misją firmy jest ochrona ludzi, urządzeń i danych, niezależnie od ich miejsca. Obecnie producent zapewnia cyberbezpieczeństwo wszędzie tam, gdzie potrzebują go klienci, dzięki największemu portfolio ponad 50 zintegrowanych ze sobą produktów klasy korporacyjnej. Ponad pół miliona klientów zaufało rozwiązaniom Fortinet, które należą do najczęściej wdrażanych, posiadających najwięcej patentów i najlepiej ocenianych w branży.

Instytut szkoleniowy Fortinet ([Fortinet Training Institute](https://www.fortinet.com/nse-training?utm_source=website&utm_campaign=nse-training)), jeden z największych i najszerszych programów szkoleniowych wśród dostawców rozwiązań ochronnych, gwarantuje, że szkolenia z zakresu cyberbezpieczeństwa oraz nowe możliwości rozwoju kariery są dostępne dla każdego. Współpraca z renomowanymi i uznanymi [organizacjami](https://www.fortinet.com/trust?tab=trusted%20partners) zarówno z sektora publicznego, jak i prywatnego, w tym zespołami CERT, podmiotami rządowymi i środowiskiem akademickim, jest podstawowym aspektem zaangażowania firmy Fortinet w zwiększanie cyfrowej odporności na całym świecie. Natomiast [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=website&utm_campaign=fortiguardlabs) to elitarny oddział Fortinet, który zajmuje się badaniem i analizą zagrożeń, opracowuje i wykorzystuje wiodące mechanizmy uczenia maszynowego oraz sztucznej inteligencji, aby zapewnić klientom terminową, nieustannie najlepszą ochronę i dostęp do informacji o zagrożeniach. Więcej informacji dostępnych jest na stronie [www.fortinet.com](http://www.fortinet.com/), [blogu Fortinet](https://www.fortinet.com/blog?utm_source=website&utm_medium=blog&utm_campaign=blog) oraz stronie [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=website&utm_campaign=fortiguardlabs).

**Copyright © 2023 Fortinet, Inc**. Wszelkie prawa zastrzeżone. Symbole ® oraz ™ oznaczają odpowiednio zarejestrowane federalnie znaki towarowe i znaki towarowe prawa zwyczajowego firmy Fortinet, Inc. oraz jej podmiotów zależnych i stowarzyszonych. Znaki towarowe firmy Fortinet obejmują, ale nie ograniczają się do następujących: Fortinet, logo Fortinet, FortiGate, FortiOS, FortiGuard, FortiCare, FortiAnalyzer, FortiManager, FortiASIC, FortiClient, FortiCloud, FortiMail, FortiSandbox, FortiADC, FortiAI, FortiAIOps, FortiAntenna, FortiAP, FortiAPCam, FortiAuthenticator, FortiCache, FortiCall, FortiCam, FortiCamera, FortiCarrier, FortiCASB, FortiCentral, FortiCNP, FortiConnect, FortiController, FortiConverter, FortiCWP, FortiDAST, FortiDB, FortiDDoS, FortiDeceptor, FortiDeploy, FortiDevSec, FortiEDR, FortiExplorer, FortiExtender, FortiFirewall, FortiFone, FortiGSLB, FortiGuest, FortiHypervisor, FortiInsight, FortiIsolator, FortiLAN, FortiLink, FortiMonitor, FortiNAC, FortiNDR, FortiPAM, FortiPenTest, FortiPhish, FortiPolicy, FortiPortal, FortiPresence, FortiProxy, FortiRecon, FortiRecorder, FortiSASE, FortiSDNConnector, FortiSIEM, FortiSMS, FortiSOAR, FortiSwitch, FortiTester, FortiToken, FortiTrust, FortiVoice, FortiWAN, FortiWeb, FortiWiFi, FortiWLC, FortiWLM i FortiXDR. Inne znaki towarowe należą do ich właścicieli. Firma Fortinet nie zweryfikowała w niezależny sposób oświadczeń lub certyfikatów przypisywanych osobom trzecim w niniejszym dokumencie, a także nie udziela niezależnego poparcia takim oświadczeniom. Niezależnie od wszelkich postanowień zawartych w niniejszym dokumencie, żaden z jego zapisów nie stanowi gwarancji, rękojmi, umowy, wiążącej specyfikacji ani innego wiążącego zobowiązania firmy Fortinet, ani też nie wskazuje na intencje związane z wiążącym zobowiązaniem, a wydajność i inne informacje o specyfikacji zawarte w niniejszym dokumencie mogą być unikalne dla niektórych środowisk.