**Fortinet przedstawia pakiet FortiMail Workspace Security**

***Wprowadzony do oferty pakiet FortiMail Workspace Security oraz znaczące ulepszenia w rozwiązaniu FortiDLP redefiniują sposób ochrony poczty elektronicznej, przeglądarek i narzędzi do współpracy, a jednocześnie zabezpieczają poufne dane przed wewnętrznymi zagrożeniami***

**[Warszawa, 25.06.2025]** [**Fortinet**](https://www.fortinet.com/content/fortinet-com/en_us)**, światowy lider w dziedzinie cyberbezpieczeństwa, który dąży do zapewnienia konwergencji sieci i rozwiązań ochronnych, rozszerzył swoją rodzinę produktów** [**FortiMail**](https://www.fortinet.com/products/email-security?utm_source=pr&utm_medium=pr&utm_campaign=fortimail-main-page) **o pakiet** [**FortiMail Workspace Security**](https://www.fortinet.com/products/fortimail-workspace-security)**. Dzięki rozbudowanej w ten sposób funkcjonalności FortiMail stał się największą i najbardziej konfigurowalną platformą bezpieczeństwa nie tylko poczty elektronicznej, ale także przeglądarek i narzędzi umożliwiających cyfrową współpracę. Te nowe możliwości, w połączeniu z rozbudowanymi funkcjami** [**FortiDLP**](https://www.fortinet.com/products/fortidlp) **– rozwiązania Fortinet nowej generacji do zapobiegania wyciekom danych (DLP) i zarządzania ryzykiem wewnętrznym – zapewniają ujednolicone, bazujące na sztucznej inteligencji podejście do ochrony użytkowników i wrażliwych danych w funkcjonujących obecnie dynamicznych środowiskach pracy.**

– *We współczesnym zmieniającym się środowisku zagrożeń zapewnienie produktywności użytkowników, a jednocześnie zabezpieczenie wrażliwych danych wymaga ujednoliconej strategii, która uwzględnia zarówno zagrożenia zewnętrzne, jak i ryzyko wewnętrzne* – powiedział Nirav Shah, starszy wiceprezes ds. produktów i rozwiązań w firmie Fortinet. – *Cyberprzestępcy kierują swoje działania bezpośrednio przeciwko użytkownikom i coraz częściej wykorzystują takie narzędzia, jak FraudGPT, BlackmailerV3 czy ElevenLabs do automatycznego tworzenia złośliwego oprogramowania, filmów deepfake, stron phishingowych i syntetycznego głosu, dzięki czemu ataki są bardziej skalowalne, przekonujące i trudne do wykrycia. Dzięki bazującemu na sztucznej inteligencji rozszerzonemu pakietowi FortiMail Workspace Security oraz rozwiązaniom FortiDLP firma Fortinet umożliwia przedsiębiorstwom zapobieganie zewnętrznym i wewnętrznym zagrożeniom, zapewniając jednocześnie bezpieczeństwo użytkowników, danych i utrzymanie wydajności.*

**Bazująca na sztucznej inteligencji ochrona dla komunikacji, współpracy i bezpieczeństwa danych**

Pracownicy, działający obecnie coraz częściej w modelu hybrydowym, w dużym stopniu bazują na narzędziach SaaS i rozwiązaniach do współpracy, co przyczynia się do zwiększenia produktywności, ale też możliwego do zaatakowania obszaru. Ponieważ użytkownicy mają dostęp do poufnych informacji znajdujących się w tych platformach, przedsiębiorstwa muszą jednocześnie przeciwdziałać zagrożeniom zarówno wobec pracowników, jak też przetwarzanych przez nich danych. W dokumencie [2025 Fortinet Global Threat Landscape Report](https://www.fortinet.com/resources/reports/threat-landscape-report) podkreślony został wzrost cyberprzestępczości bazującej na sztucznej inteligencji, która pozwala atakującym wykorzystywać automatyzację do przeprowadzania bardziej przekonujących kampanii phishingowych, podszywających się pod inne osoby i doprowadzających do przejmowania ich kont.

Rozbudowane rozwiązania Fortinet, służące do [zabezpieczania przestrzeni roboczej](https://www.fortinet.com/solutions/workspace-security), w bezpośredni sposób odpowiadają na to wyzwanie. Zapewniają bazujące na sztucznej inteligencji mechanizmy ochronne w poczcie elektronicznej, przeglądarkach i środowiskach współpracy, chroniąc przed zagrożeniami zewnętrznymi i wewnętrznymi – niezależnie od miejsca pracy. Obejmują pełen zakres interakcji użytkowników i przepływu danych w cyfrowej przestrzeni roboczej:

**Rozbudowana ochrona poczty elektronicznej** – Dzięki przejęciu firmy [Perception Point](https://www.fortinet.com/blog/business-and-technology/fortinet-acquires-perception-point) – uznanej za wizjonera w raporcie Gartner Magic Quadrant 2024 dotyczącym zabezpieczeń poczty elektronicznej1 – a następnie integracji jej rozwiązań z portfolio Fortinet, możliwe było znaczne rozszerzenie funkcjonalności platformy ochronnej dla poczty elektronicznej FortiMail, czyniąc ją najbardziej wszechstronnym i konfigurowalnym rozwiązaniem w branży. FortiMail może zaspokoić wszelkie potrzeby w zakresie bezpieczeństwa poczty elektronicznej, w tym ochronę wiadomości przychodzących, wychodzących i wewnętrznych. Zapewnione zostały także różnorodne opcje wdrażania na urządzeniach, maszynach wirtualnych, usługach hostowanych i SaaS. FortiMail może pracować w wielu trybach – jako brama, serwer, zintegrowane chmurowe rozwiązanie do ochrony poczty elektronicznej (ICES) oraz w modelu hybrydowym – a także oferuje zarówno wysoce konfigurowalny interfejs użytkownika, jak i usprawnione środowisko SaaS.

**Rozszerzenie mechanizmów ochronnych na narzędzia do współpracy** – W pakiecie [FortiMail Workspace Security](https://www.fortinet.com/products/email-security) ochrona została rozszerzona poza pocztę elektroniczną i obejmuje teraz także przeglądarki internetowe oraz narzędzia do współpracy. Dzięki temu przedsiębiorstwa są w stanie powstrzymywać zaawansowane zagrożenia na platformach, takich jak Microsoft 365 i Teams, Google Workspace oraz Slack. Blokowane są trudne do wykrycia ataki internetowe, szkodliwy kod ukryty we współużytkowanych plikach oraz złośliwe linki wysyłane za pośrednictwem komunikatorów i aplikacji do współpracy. Platforma zwiększa również widzialność aktywności użytkowników w środowiskach chmurowych, pomagając zespołom ds. bezpieczeństwa wykrywać i zapobiegać przejęciom kont, zanim dojdzie do eskalacji ataku. Zintegrowana, zarządzana przez całą dobę usługa reagowania na incydenty wspiera szybkie analizowanie i powstrzymywanie zagrożeń, zmniejszając obciążenie operacyjne zespołów SOC.

**Bardziej inteligentna ochrona krytycznych danych** – W rozwiązaniu [FortiDLP](https://www.fortinet.com/products/fortidlp?utm_source=Paid-Search&utm_medium=Google&utm_campaign=SecOps-AMER-US&utm_content=SL-FortiDLP_Webpage-U&utm_term=fortidlp&lsci=701Hr000002RlrNIAS&UID=ftnt-9228-937519&s_kwcid=AL!11440!3!719194995017!p!!g!!fortidlp&gad_source=1&gad_campaignid=21848578728&gbraid=0AAAAACeCt-nADtqmGRJV43BJK5_n9TkA1&gclid=CjwKCAjw6NrBBhB6EiwAvnT_rpmGprnPVNEzR2Ijhf1k730arb1FGjkBBsrADXqm3xd9USRl7AqLkRoC9j8QAvD_BwE) wprowadzone zostały zaawansowane funkcje z mechanizmami wykrywania ich pochodzenia i sekwencjonowania które zapewniają bezpieczny przepływ danych,. Dzięki temu zespoły ds. bezpieczeństwa i przeciwdziałania wewnętrznemu ryzyku zyskują dostęp do mechanizmów szczegółowego śledzenia wrażliwych danych już od źródła ich pochodzenia, rejestrując sposób, w jaki są one wykorzystywane i przetwarzane przez użytkowników. Jednocześnie w automatyczny sposób korelowane są działania użytkowników w celu wykrywania zachowania wysokiego ryzyka, które wymagają dalszego zbadania. Niezależnie od tego, czy chodzi o monitorowanie nieautoryzowanego udostępniania poufnych informacji za pośrednictwem repozytoriów chmurowych, czy zapobieganie ujawnianiu wrażliwych danych nieautoryzowanym platformom SaaS i GenAI, FortiDLP zapewnia kontekst i kontrolę niezbędne do ochrony wrażliwych danych, w tym własności intelektualnej.

**Zunifikowana ochrona dla hybrydowego świata**

Dzięki rozbudowanej ofercie firma Fortinet na nowo definiuje sposób, w jaki przedsiębiorstwa chronią użytkowników i ich dane we współczesnym środowisku pracy. Łącząc możliwości sztucznej inteligencji ze zintegrowaną ochroną poczty elektronicznej, przeglądarek, danych i mechanizmów współpracy, Fortinet zapewnia zespołom ds. bezpieczeństwa widzialność, możliwość sprawowania kontroli i szybkość reagowania, przekształcając złożoność w przejrzystość, a przeciwdziałanie zagrożeniom w po prostu kolejne zadanie do wykonania.

**Dodatkowe zasoby**

* Więcej informacji o [FortiMail Workspace Security](https://www.fortinet.com/products/fortimail-workspace-security).
* Więcej informacji o platformie [Fortinet Security Fabric](https://www.fortinet.com/blog/business-and-technology/step-into-the-platform-era).
* Na stronie [fortinet.com/trust](https://www.fortinet.com/trust) dostępne są informacje o innowacjach Fortinet, współpracy z partnerami, procesach zabezpieczania produktów oraz rozwiązaniach klasy korporacyjnej.
* Więcej informacji o tym, jak [klienci firmy Fortinet](https://www.fortinet.com/customers) zabezpieczają swoje przedsiębiorstwa.
* Więcej informacji o [zaangażowaniu firmy Fortinet w bezpieczeństwo i integralność produktów](https://www.fortinet.com/content/dam/fortinet/assets/flyer/flyer-fortinet-commitment-to-product-security-and-integrity.pdf), w tym o odpowiedzialnym rozwoju produktów oraz podejściu i zasadach ujawniania podatności.
* Profile firmy Fortinet w mediach społecznościowych: [X](https://www.x.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).

GARTNER jest zarejestrowanym znakiem towarowym i znakiem usługowym firmy Gartner, Inc. i/lub jej podmiotów powiązanych w Stanach Zjednoczonych i na całym świecie, a Magic Quadrant jest zarejestrowanym znakiem towarowym firmy Gartner, Inc. i/lub jej podmiotów powiązanych i jest używany w niniejszym dokumencie za zgodą. Wszelkie prawa zastrzeżone.

Firma Gartner nie promuje żadnego dostawcy, produktu ani usługi przedstawionych w swoich publikacjach badawczych i nie doradza użytkownikom technologii, aby wybierali wyłącznie dostawców z najwyższymi ocenami lub innymi oznaczeniami. Publikacje badawcze firmy Gartner zawierają opinie organizacji badawczej Gartner i nie powinny być traktowane jako stwierdzenia faktów. Firma Gartner zrzeka się wszelkich gwarancji, wyraźnych lub dorozumianych, dotyczących niniejszych badań, w tym wszelkich gwarancji przydatności handlowej lub przydatności do określonego celu.

*1Gartner, Magic Quadrant for Email Security Platforms, Max Taggett, Nikul Patel, Franz Hinner, Deepak Mishra, 16 grudnia 2024*

**O firmie Fortinet (www.fortinet.com)**

[Fortinet](https://www.globenewswire.com/Tracker?data=3ZN1f9xQbo_Vcl9FC7lRUziylTnQD_H8Wgw0LgiNABG18h6YofSmzWyF83iQxjzGr0YOzRbtH7GvWm8mhWkB1w==) jest jednym z liderów ewolucji branży cyberbezpieczeństwa oraz konwergencji sieci i zabezpieczeń. Naszą misją jest ochrona ludzi, urządzeń i danych, niezależnie od ich lokalizacji. Dzięki największemu zintegrowanemu portfolio ponad 50 produktów klasy korporacyjnej jesteśmy w stanie zapewnić cyfrowe bezpieczeństwo wszędzie tam, gdzie potrzebują go nasi klienci. Ponad pół miliona firm zaufało opatentowanym rozwiązaniom Fortinet, które są jednymi z najczęściej wdrażanych i sprawdzonych w branży. [Fortinet Training Institute](https://www.globenewswire.com/Tracker?data=3ZN1f9xQbo_Vcl9FC7lRU427bkyusLB6LHWVez1DZI-opYsFAM_-s0wno4pnWzab0djHfLUQhnXZAVo9BzogcyNk6Zaxu_xiPipTwf8Gy64lorLnM8OiN7Q0HNI7WSn2_XNgBXM6aPYr2xsJF6FhiVwXT4qZiZOohumWLMyfVcNSL-DaFkPXHjMtP__P9629), jeden z największych i najszerszych programów szkoleniowych w branży, ma na celu udostępnienie wszystkim szkoleń z zakresu cyberbezpieczeństwa oraz nowych możliwości kariery. Współpraca z [cenionymi organizacjami](https://www.globenewswire.com/Tracker?data=FJddTxnnUs2MbUKktjnoWNiJ8pVJ3rrefMbCSN0a2wPcU3dkIq-8gtDYKEGBfuWDp7I3mpFEHKUl2_JP9UxZ06Lpi98tsUD4B9FTkEhfTdmz8EUzHp41Q757Qs4SlTG40BZObNvmtkmAAQvxF9JWFg==) zarówno z sektora publicznego, jak i prywatnego, w tym zespołami reagowania na incydenty komputerowe (Computer Emergency Response Teams, CERT), podmiotami rządowymi i środowiskiem akademickim, jest podstawowym aspektem zaangażowania firmy Fortinet w zwiększanie cyfrowej odporności na całym świecie. [FortiGuard Labs](https://www.globenewswire.com/Tracker?data=3ZN1f9xQbo_Vcl9FC7lRU7sP63Y1u7ANxMD0vN3k070iDOkurg41r7RCkKZ05g_-MU37_BxWB2D7A8oOSL4LFCj76ONcCWKDfrPqCgOU7IH9QZVmwWh5KFJ4OVPUtaQRkrRV8Ii_bqlzSOPMSXWlEreRA7JwN-ZTlLzaeMLjbs0=), elitarna jednostka Fortinet zajmująca się analizą zagrożeń i badaniami, opracowuje i wykorzystuje najnowocześniejsze techniki uczenia maszynowego oraz sztucznej inteligencji, aby zapewnić klientom terminową, konsekwentnie najwyżej ocenianą ochronę i analizę zagrożeń. Więcej informacji dostępnych jest na stronie [www.fortinet.com](http://www.fortinet.com), [blogu Fortinet](https://www.globenewswire.com/Tracker?data=3ZN1f9xQbo_Vcl9FC7lRU8UWh33yvVmOpZUoo2Rsm97Ks9X8ujEEGJ0QRz3Y9IaMjOue_vJ9g8c1YSrQhCN89ehZsIJK1nc8MSyUz16G4WIqBpHmEnBF5Jej1XsujCNH4PZgzf5Mm_56MjzpFkFFZY3oj46ZC3a62HV7dMAo74U=) oraz stronie [FortiGuard Labs](https://www.globenewswire.com/Tracker?data=3ZN1f9xQbo_Vcl9FC7lRU4aoptLCvUUmdyfmiJXtPtoXYFRdjfSVbjfxsrda2hpiXCexke6oUsCtDWqTItuCoOUYW0exXhF-_wPj9Pv6De4lYtNZkcir3gvsLghF_FgwNXW_hiakGhDWoWydEQoERqGjh59ZRCJEg51g6W6EKsMC2EVrF0lSrR_RDiHVxchn).

*Copyright © 2024 Fortinet, Inc. Wszelkie prawa zastrzeżone. Symbole ® i ™ 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 między innymi: Fortinet, logo Fortinet, FortiGate, FortiOS, FortiGuard, FortiCare, FortiAnalyzer, FortiManager, FortiASIC, FortiClient, FortiCloud, FortiMail, FortiSandbox, FortiADC, FortiAI, FortiAIOps, FortiAgent, FortiAntenna, FortiAP, FortiAPCam, FortiAuthenticator, FortiCache, FortiCall, FortiCam, FortiCamera, FortiCarrier, FortiCASB, FortiCentral, FortiCNP, FortiConnect, FortiController, FortiConverter, FortiCSPM, FortiCWP, FortiDAST, FortiDB, FortiDDoS, FortiDeceptor, FortiDeploy, FortiDevSec, FortiDLP, FortiEdge, FortiEDR, FortiExplorer, FortiExtender, FortiFirewall, FortiFlex, FortiFone, FortiGSLB, FortiGuest, FortiHypervisor, FortiInsight, FortiIsolator, FortiLAN, FortiLink, FortiMonitor, FortiNAC, FortiNDR, FortiPAM, FortiPenTest, FortiPhish, FortiPoint, FortiPolicy, FortiPortal, FortiPresence, FortiProxy, FortiRecon, FortiRecorder, FortiSASE, FortiScanner, FortiSDNConnector, FortiSIEM, FortiSMS, FortiSOAR, FortiSRA, FortiStack, FortiSwitch, FortiTester, FortiToken, FortiTrust, FortiVoice, FortiWAN, FortiWeb, FortiWiFi, FortiWLC, FortiWLM, FortiXDR oraz Lacework FortiCNAPP. Inne znaki towarowe należą do odpowiednich właścicieli. Firma Fortinet nie zweryfikowała niezależnie oświadczeń lub certyfikatów przypisanych stronom trzecim i nie promuje niezależnie takich oświadczeń. Niezależnie od jakichkolwiek przeciwnych stwierdzeń zawartych w niniejszym dokumencie, żadne z nich nie stanowi gwarancji, rękojmi, umowy, wiążącej specyfikacji ani innego wiążącego zobowiązania ze strony firmy Fortinet lub jakiegokolwiek wskazania zamiaru związanego z wiążącym zobowiązaniem, a informacje dotyczące wydajności i innych specyfikacji zawarte w niniejszym dokumencie mogą być unikalne dla niektórych środowisk.*