**Fortinet revela nova suite de segurança de espaço de trabalho alimentado por IA**

***A FortiMail Workspace Security e as poderosas atualizações do FortiDLP permitem redefinir a proteção para e-mail, browsers e ferramentas de colaboração, ao mesmo tempo que protegem dados confidenciais contra ameaças internas.***

**Lisboa, Portugal, 03 de julho de 2025**

**Resumo**

A [Fortinet](https://www.fortinet.com/content/fortinet-com/en_us), líder global em cibersegurança que promove a convergência entre redes e segurança, revelou recentemente um conjunto de melhorias no seu portefólio de segurança de dados e produtividade, com a expansão do [FortiMail](https://www.fortinet.com/products/email-security?utm_source=pr&utm_medium=pr&utm_campaign=fortimail-main-page) que passa a incluir a nova suite [FortiMail Workspace Security](https://www.fortinet.com/products/fortimail-workspace-security). Estas novas capacidades estabelecem o FortiMail como a plataforma de segurança de e-mail mais ampla e personalizável do setor e aumentam a segurança para além do e-mail, incluindo a proteção do browser e das ferramentas de colaboração. Estas melhorias, alinhadas com os novos recursos do [FortiDLP](https://www.fortinet.com/products/fortidlp), a solução de prevenção de perda de dados (DLP) e gestão de risco interno de última geração da Fortinet, oferecem uma abordagem unificada e alimentada por IA para proteger os utilizadores e dados confidenciais nos atuais ambientes de trabalho mais dinâmicos.

*“No atual cenário de ameaças em evolução, a segurança da produtividade dos utilizadores e dos dados sensíveis requer uma estratégia unificada que considere tanto as ameaças externas como os riscos internos”,* afirmou **Nirav Shah, Senior Vice President, Products and Solutions at Fortinet.** *“Os cibercriminosos estão a direcionar os seus esforços para os utilizadores e a utilizar cada vez mais ferramentas como FraudGPT, BlackmailerV3 e ElevenLabs para automatizar a criação de malware, vídeos deepfake, sites de phishing e vozes sintéticas - tornando os ataques mais escaláveis, convincentes e difíceis de detetar. Com a suite FortiMail Workspace Security* *alimentada por IA e as soluções FortiDLP, a Fortinet tem como objetivo capacitar as organizações a ficarem à frente dos agentes de ameaças e riscos internos, garantindo que os utilizadores, dados e produtividade permaneçam seguros.”*

**Defesa potenciada por IA para comunicação, colaboração e segurança de dados**

A atual força de trabalho híbrida depende fortemente de SaaS e de ferramentas de colaboração, aumentando a produtividade e a superfície de ataque. À medida que os utilizadores interagem com dados sensíveis através destas plataformas, as organizações devem abordar as ameaças aos utilizadores e aos dados em simultâneo. O [Fortinet Global Threat Landscape Report 2025](https://www.fortinet.com/resources/reports/threat-landscape-report) destaca o aumento do cibercrime potenciado pela IA, com os atacantes usando a automação para lançar campanhas mais convincentes de phishing, personificação e aquisição de contas.

As [soluções melhoradas de segurança do espaço de trabalho](https://www.fortinet.com/solutions/workspace-security) da Fortinet enfrentam este desafio de frente com proteção alimentada por IA em ambientes de e-mail, browsers e ferramentas de colaboração, criando uma defesa contra ameaças externas e internas onde quer que o trabalho aconteça. Isto abrange todo o espetro de interações do utilizador e movimentação de dados no espaço de trabalho digital:

**Segurança de e-mail, evoluída**: Com a aquisição e integração do [Perception Point](https://www.fortinet.com/blog/business-and-technology/fortinet-acquires-perception-point) - reconhecido como *Visionary in the 2024 Gartner® Magic Quadrant™ for Email Security*1 - a Fortinet expandiu significativamente os recursos da plataforma de segurança de e-mail FortiMail, estabelecendo-a como a solução mais ampla e personalizável do setor. O FortiMail pode responder a qualquer necessidade de segurança de e-mail, incluindo entrada, saída (incluindo relays) e proteção interna de e-mail, com opções flexíveis de implementação em dispositivos, máquinas virtuais, serviços hospedados e SaaS. Esta solução oferece vários modos operacionais - gateway, servidor, ICES e híbrido - e apresenta uma interface de utilizador altamente configurável e uma experiência SaaS simplificada.

**Expansão da segurança às ferramentas de colaboração**: A suite [FortiMail Workspace Security](https://www.fortinet.com/products/email-security?utm_source=pr&utm_medium=pr&utm_campaign=fortimail-main-page) expande a proteção para além do e-mail, para browsers e ferramentas de colaboração, permitindo às organizações travar ameaças sofisticadas em plataformas como o Microsoft 365 e Teams, Google Workspace e Slack. Bloqueia ataques evasivos baseados na Web, malware oculto em ficheiros partilhados e ligações maliciosas enviadas através de aplicações de chat e de colaboração. A plataforma também melhora a visibilidade da atividade dos utilizadores em ambientes cloud, ajudando as equipas de segurança a detetar e a evitar a apropriação de contas antes que estas se agravem. Um serviço integrado de resposta a incidentes gerido 24 horas por dia, 7 dias por semana, suporta a rápida análise e contenção de ameaças para reduzir a carga operacional das equipas SOC.

**Defesa mais inteligente para dados críticos**: O [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) reforça esta oferta adicionando caracteristicas avançadas como o fluxo de dados seguro com deteção de linhagem e sequência de dados, fornecendo às equipas de segurança e de risco interno um rastreio detalhado dos dados sensíveis desde a sua origem, capturando a forma como esses dados são utilizados e manipulados pelos utilizadores e correlacionando automaticamente as actividades dos utilizadores para detetar comportamentos de alto risco que justifiquem uma investigação mais aprofundada. Seja monitorizando a partilha não autorizada de informações confidenciais através de unidades na nuvem ou impedindo a exposição de dados sensíveis a plataformas SaaS e GenAI não sancionadas, o FortiDLP fornece o contexto e o controlo necessários para proteger dados sensíveis, incluindo a propriedade intelectual.

**Proteção unificada para um mundo híbrido** - Com as recentes melhorias, a Fortinet redefine a forma como as organizações protegem os utilizadores e os dados no espaço de trabalho moderno. Ao combinar o poder da IA com a segurança integrada de e-mail, browser, ferramentas de colaboração e dados, a Fortinet oferece a visibilidade, o controlo e a velocidade de resposta que as equipas de segurança precisam, transformando a complexidade em clareza e as ameaças em apenas mais uma tarefa resolvida.

**Recursos Adicionais**

* Saiba mais sobre a [FortiMail Workspace Security](https://www.fortinet.com/products/fortimail-workspace-security).
* Saiba mais sobre o [Fortinet Security Fabric](https://www.fortinet.com/blog/business-and-technology/step-into-the-platform-era).
* Visite [fortinet.com/trust](https://www.fortinet.com/trust) para conhecer as inovações da Fortinet.
* Descubra como é que os [**Clientes Fortinet**](https://www.fortinet.com/customers) estão a proteger as suas organizações.
* Siga a Fortinet no [X](https://twitter.com/Fortinet), [LinkedIn](https://www.linkedin.com/company/fortinet/), [Facebook](https://www.facebook.com/Fortinet/), e [Instagram](https://www.instagram.com/fortinet/). Subscreva o [blog](https://www.fortinet.com/blog?utm_source=website&utm_medium=pr&utm_campaign=blog) ou [YouTube](https://www.youtube.com/channel/UCJHo4AuVomwMRzgkA5DQEOA) da Fortinet

**Sobre a Fortinet**

A [Fortinet](https://www.fortinet.com/blog?utm_source=pr&utm_medium=pr&utm_campaign=boiler%22%20\t%20%22_blank) é uma força motriz na evolução da cibersegurança e na convergência da rede com a segurança. A sua missão é proteger pessoas, dispositivos e dados em qualquer lugar, sendo que hoje oferece cibersegurança onde for necessário, com um portfólio com mais de 50 produtos de nível empresarial. Mais de meio milhão de clientes confiam nas soluções Fortinet, que se encontram entre as mais adotadas, mais patenteadas e mais validadas na indústria. O [Fortinet Training Institute](https://www.fortinet.com/nse-training?utm_source=pr&utm_campaign=nse-training%22%20\t%20%22_blank), um dos maiores e mais amplos programas de formação da indústria, dedica-se a tornar a formação em cibersegurança e novas oportunidades de carreira disponíveis a todos. A colaboração com organizações de alto nível e respeitadas dos sectores público e privado, incluindo CERTs, entidades governamentais e académicas, é um aspeto fundamental do compromisso da Fortinet para melhorar a ciber resiliência a nível global. A [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=pr&utm_campaign=fortiguardlabs%22%20\t%20%22_blank), a organização de elite de investigação e inteligência sobre ameaças da Fortinet, desenvolve e utiliza tecnologias inovadoras como *Machine Learning* e *AI* para fornecer atempadamente aos clientes a melhor proteção de forma consistente e medidas de ação inteligentes na contenção de ameaças. Saiba mais em  [https://www.fortinet.com](https://www.fortinet.com/%22%20/t%20%22_blank), no [Blog da Fortinet](https://www.fortinet.com/blog?utm_source=blog&utm_medium=blog&utm_campaign=blog%22%20\t%20%22_blank), e na [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=pr&utm_medium=pr&utm_campaign=fglabs%22%20\t%20%22_blank).

**Para mais informação contacte:**

**Lift Consulting**

Erica Macieira | erica.macieira@lift.com.pt  | 910549515

Hugo Costa | hugo.costa@lift.com.pt

GARTNER é uma marca registada e uma marca de serviço da Gartner, Inc. e/ou das suas afiliadas nos EUA e internacionalmente, Magic Quadrant é uma marca registada da Gartner, Inc. e/ou das suas afiliadas e é utilizada aqui com permissão. Todos os direitos reservados.

A Gartner não apoia qualquer fornecedor, produto ou serviço descrito nas suas publicações de investigação e não aconselha os utilizadores de tecnologia a selecionar apenas os fornecedores com as classificações mais elevadas ou outra designação. As publicações de pesquisa da Gartner consistem nas opiniões da organização de pesquisa da Gartner e não devem ser interpretadas como declarações de factos. A Gartner renuncia a todas as garantias, expressas ou implícitas, relativamente a esta investigação, incluindo quaisquer garantias de comercialização ou adequação a um determinado fim.

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