**Fortinet reforça o FortiRecon para estar alinhado com a Framework de Gestão Contínua de Exposição a Ameaças (CTEM)**

*Novas funcionalidades integram gestão da superfície de ataque, inteligência sob ameaças e orquestração de segurança para permitir que as equipas de segurança reduzam o risco de forma mais rápida e proativa*

**Lisboa, 29 de setembro de 2025**

**RESUMO**

A [Fortinet](https://www.fortinet.com/?utm_source=website&utm_medium=pr&utm_campaign=fortinet), líder mundial de cibersegurança que fomenta a convergência entre segurança e redes, anunciou hoje melhorias significativas na plataforma [FortiRecon](https://www.fortinet.com/products/fortirecon?utm_source=pr&utm_medium=pr&utm_campaign=fortirecon), transformando-a numa das soluções mais abrangentes do setor alinhada com o framework de Gestão Contínua de Exposição a Ameaças (CTEM). A versão mais recente introduz capacidades alargadas de monitorização da superfície de ataque, inteligência sobre ciberadversários e exposição de ativos internos na dark web e orquestração de segurança, tudo numa única plataforma unificada. Estas melhorias permitem às organizações identificar e priorizar de forma proativa exposições reais, validar riscos como o faria um atacante e acelerar a resposta, reduzindo, em última análise, a probabilidade e o impacto de incidentes de segurança.

*“Os CISOs e as equipas de segurança estão sobrecarregados com o aumento das superfícies de ataque e com um fluxo interminável de alertas sem priorização*”, afirma **Nirav Shah, Senior Vice President of Products and Solutions da Fortinet.** *“Com as recentes melhorias no FortiRecon, estamos a oferecer às organizações uma visão, sob a perspetiva de um agente de ameaça, das suas exposições internas e externas, suportada por inteligência de ameaças potenciada por IA do FortiGuard Labs, validação baseada em cenários reais e resposta automatizada. Isto permite que as organizações filtrem o ruído, se concentrem no que realmente importa e reduzam de forma mensurável riscos e vulnerabilidades antes que os atacantes consigam explorá-los.”*

O anúncio surge num contexto de crescente procura por estratégias de segurança orientadas para a exposição, à medida que as organizações enfrentam dificuldades em gerir a expansão das superfícies de ataque, a fadiga provocada por alertas e operações de segurança fragmentadas. De acordo com a Gartner®, “até 2026, as organizações que priorizarem os seus investimentos em segurança com base num programa de gestão contínua de exposição terão três vezes menos probabilidade de sofrer uma violação”.[[1]](#footnote-1)

**Uma Plataforma Unificada para a Gestão Contínua de Exposição a Ameaças**

O FortiRecon, em combinação com a sua forte integração na plataforma de Security Operations Center (SOC) da Fortinet, potenciada por IA, oferece agora capacidades que abrangem os cinco pilares do framework CTEM da Gartner — definição do âmbito, pesquisa, priorização, validação e mobilização — permitindo que as organizações operacionalizem estes pilares numa única plataforma, totalmente integrada, e promovam esforços de remediação coordenados entre as equipas de segurança e de TI. As mais recentes melhorias incluem:

* **Gestão da superfície de ataque**: monitoriza continuamente e fornece uma visão, sob a perspetiva de um adversário, da superfície de ataque digital interna e externa da organização. A nova versão adiciona classificações de severidade da National Vulnerability Database (NVD), para além das classificações de severidade de Exploração Ativa do FortiRecon, permitindo uma aplicação de patches mais rápida e inteligente.
* **Inteligência centrada no adversário**: fornece informações acionáveis sobre ameaças provenientes da atividade na dark web, inteligência sobre ransomware, credenciais comprometidas, vulnerabilidades exploradas ativamente e fornecedores em risco. As melhorias incluem downloads em lote de indicadores de compromisso (IOC) e detalhes sobre infeções por stealer, acelerando os fluxos de trabalho do SOC e melhorando a deteção de incidentes.
* **Proteção de marca**: monitoriza situações de usurpação de domínios, aplicações móveis falsas, campanhas de phishing e ataques direcionados a executivos. O FortiRecon Brand Protection recorre a algoritmos proprietários para detetar e eliminar domínios de phishing falsos, usurpações de marca e de executivos, aplicações móveis fraudulentas em várias apps stores, fugas de dados em repositórios de código, exposições de buckets abertos e campanhas de phishing, ajudando a proteger a presença online de executivos.
* **Orquestração de segurança**: utiliza orquestração de segurança e playbooks automatizados para investigar e responder a deteções de ameaças. O FortiRecon Security Orchestration reduz o tempo necessário para que as equipas de resposta priorizem e executem ações adequadas, automatizando e otimizando os fluxos de trabalho de segurança.

Os clientes FortiFlex existentes podem utilizar os seus créditos FortiFlex para implementar o FortiRecon Cloud. O FortiFlex oferece licenciamento baseado na utilização, com o portefólio mais abrangente da indústria de segurança, pensado para clientes com ambientes híbridos e multicloud dinâmicos, bem como para MSSPs. Quando adquirido através dos principais marketplaces de cloud, o FortiFlex pode também ajudar os clientes a cumprir os compromissos de consumo contratual com os fornecedores de cloud.

**Reconhecimento da Indústria e Resultados de Clientes**

A Fortinet foi recentemente nomeada **Líder Global**, bem como **Líder de Mercado** e **Líder em Inovação**, no relatório [*KuppingerCole Leadership Compass for Attack Surface Management 2025*](https://global.fortinet.com/lp-en-ap-kuppingercole-fortirecon?utm_source=Blog&utm_medium=Other&utm_campaign=AI-DrivenSecOps-GLOBAL-Global&utm_content=AR-ap-kuppingercole-fortirecon-G&utm_term=SOC&lsci=701Hr000002Rx86IAC). O documento destaca a prontidão operacional do FortiRecon, com suporte abrangente para ambientes CIS, ICS, IoT e OT, bem como as suas integrações com outras ferramentas do [Fortinet Security Fabric](https://www.fortinet.com/solutions/enterprise-midsize-business/security-fabric?utm_source=pr&utm_medium=pr&utm_campaign=security-fabric), como o [FortiGate NGFW](https://www.fortinet.com/products/next-generation-firewall?utm_source=pr&utm_medium=pr&utm_campaign=fortigate), [FortiSOAR](https://www.fortinet.com/products/fortisoar?utm_source=pr&utm_medium=pr&utm_campaign=fortisoar), [FortiSIEM](https://www.fortinet.com/products/siem/fortisiem?utm_source=pr&utm_medium=pr&utm_campaign=fortisiem) e [FortiDAST](https://www.fortinet.com/products/dynamic-application-security-testing).

*“O FortiRecon elevou a forma como prestamos serviços de segurança gerida. Permite que as nossas equipas forneçam aos clientes informações contínuas e contextualizadas sobre o risco, e não apenas alertas. Passámos a conseguir priorizar a remediação com base no impacto para o negócio, ajudando os nossos clientes a reduzir o risco de forma mais rápida e a demonstrar resultados de segurança mensuráveis. É um fator diferenciador fundamental na forma como construímos relações de confiança e valor a longo prazo*”, refere **Paul Cragg, CTO at Norm Cyber**

**Recursos Adicionais**

* Saiba mais sobre [FortiRecon](https://www.fortinet.com/products/fortirecon?utm_source=pr&utm_medium=pr&utm_campaign=fortirecon)
* Saiba mais sobre o [compromisso da Fortinet](https://trust.fortinet.com/?itemName=infrastructure&source=click) com a segurança e integridade do produto,e leia este [post recente no blog](https://www.fortinet.com/blog/psirt-blogs/proactive-responsible-disclosure-is-one-cucial-way-fortinet-strengthens-customer-security) sobre este compromisso de longa data com o desenvolvimento responsável do produto e abordagem de divulgação de vulnerabilidades e políticas.

**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).

1. Gartner. *How to Manage Cybersecurity Threats, Not Episodes*, by Jeremy D’Hoinne. Gartner, 11 Oct. 2023 [↑](#footnote-ref-1)