**Fortinet lança nova solução de deteção e resposta de rede com recursos de IA de autoaprendizagem**

* *FortiNDR recorre ao machine learning e às redes neurais profundas - a próxima geração de IA - para identificar ciberataques com base na atividade anómala da rede e limitar a exposição a ameaças*

**Lisboa, Portugal – 20 de junho 2022**

**John Maddison, EVP de Products e CMO da Fortinet**

"Com a introdução do FortiNDR, estamos a acrescentar uma solução robusta de deteção e resposta de rede ao Fortinet Security Fabric. Alimentado por machine learning, deep learning, análise pragmática e capacidades avançadas de IA, o FortiNDR deteta e responde automaticamente a atividades anormais da rede para impedir incidentes de segurança. O conjunto completo de ofertas de deteção e resposta da Fortinet apresenta uma integração nativa para uma resposta coordenada e para capacitar as equipas de segurança a passar de uma postura de segurança reativa para uma postura de segurança proativa".

A [Fortinet](https://www.fortinet.com/?utm_source=pr&utm_campaign=fortinet)®, líder mundial em soluções amplas, integradas e automatizadas de cibersegurança, acaba de anunciar o FortiNDR, uma nova oferta de deteção e resposta de rede que utiliza inteligência artificial poderosa e análises pragmáticas para permitir uma deteção mais rápida de incidentes e uma resposta mais eficiente às ameaças.

**Equipas de SecOps devem aproveitar a IA para se manterem à frente das ameaças**

As equipas de operações de segurança enfrentam cibercrimes avançados e persistentes, que são [mais destrutivos e menos previsíveis do que nunca](https://www.fortinet.com/blog/industry-trends/fortiguard-labs-ransomware-not-slowing?utm_source=blog&amp;utm_campaign=threatreport), numa superfície de ataque que continua a expandir-se com [arquiteturas de TI híbridas](https://www.fortinet.com/blog/business-and-technology/securing-hybrid-it-with-fortigate-ngfw?utm_source=pr&utm_campaign=securing-hybrid-it-with-fortigate-ngfw) e uma contínua escassez de especialistas devido à [falta de competências em cibersegurança](https://www.fortinet.com/training/taa?utm_source=pr&utm_campaign=taa). Aqueles que utilizam soluções de segurança legacy são também desafiados com uma avassaladora e desgastante triagem manual de alerta que afasta recursos importantes de tarefas altamente prioritárias, tais como a atenuação de ameaças. À medida que os cibercriminosos se tornam mais sofisticados, também as ferramentas de segurança de uma organização devem ser mais sofisticadas.

**FortiNDR Acelera a Deteção de Ameaças com Inteligência Artificial**

Com a introdução do [FortiNDR](https://www.fortinet.com/products/network-detection-and-response), a Fortinet está a fornecer proteção, deteção e resposta de rede de ciclo de vida completo com tecnologia de IA para:

* **Detetar sinais de ciberataques sofisticados**: Com recursos de autoaprendizagem de IA, machine learning e análises avançadas, o FortiNDR estabelece linhas de base sofisticadas de atividade normal de rede para uma maior organização e identifica alterações que podem indicar possíveis ciberataques em curso. O perfil pode ser baseado em IP/Porta, protocolo/comportamento, destino, dimensão, geografia, tipo de dispositivo e muito mais. No seu conjunto, isto significa que uma deteção mais precoce, uma vez que as organizações já não precisam de recorrer a feeds genéricos de ameaças, que dependem de ameaças ou componentes para se tornarem globalmente conhecidas, com o objetivo de identificar indícios de comprometimento.
* **Atenuar as funções intensivas dos investigadores humanos através de um Virtual Security Analyst (VSATM):** o FortiNDR inclui um Virtual Security Analyst (VSATM), que incorpora redes neurais profundas – a próxima geração de IA –, e foi concebido para atenuar o trabalho dos investigadores humanos através da análise do código produzido pelo tráfego malicioso e determinar a sua propagação. VSATM vem pré-treinado com mais de 6 milhões de características maliciosas e seguras que podem identificar malware baseado em TI e OT e classificá-lo por categorias de ameaça. Estas características podem identificar com precisão o ‘paciente zero’ e a propagação lateral de malware multivariante, analisando todo o seu movimento. O VSATM é também capaz de identificar ataques encriptados, campanhas web maliciosas, criptografias/protocolos fracos e classificação de malware.
* **Identificar utilizadores comprometidos e dispositivos agentless:** Nem todos os dispositivos de uma organização (por exemplo, dispositivos pessoais, de terceiros, IoT ou OT) podem ter um agente de deteção e resposta de última geração instalado para detetar um comprometimento. O FortiNDR responde a esta questão através da implementação de um sensor de rede especializado para analisar o tráfego proveniente de todos os dispositivos.

**Resposta Coordenada com a Integração do Security Fabric**

O FortiNDR também apresenta integrações nativas com o [Fortinet Security Fabric](https://www.fortinet.com/solutions/enterprise-midsize-business/security-fabric?utm_source=pr&utm_campaign=security-fabric), bem como integrações API com soluções de terceiros para uma resposta coordenada a ameaças que são descobertas para minimizar o seu impacto. As automatizações comuns para acelerar a resposta, incluem dispositivos em quarentena, que geram tráfego anómalo, aplicação com dispositivos de terceiros através de uma estrutura API, desencadeando um processo orquestrado guiado por SOAR, e muito mais.

Sendo a plataforma mesh de segurança cibernética de maior desempenho da indústria, alimentada por FortiOS e uma estrutura de gestão comum, o Fortinet Security Fabric permite uma ampla visibilidade, integração e interoperabilidade sem falhas entre elementos críticos de segurança e controlo e automatização granular.

**O Portfólio Robusto de Soluções de Deteção e Resposta da Fortinet**

O FortiNDR completa o portfolio existente da Fortinet de soluções de deteção e resposta, incluindo managed detection and response (MDR), endpoint detection and response (EDR), e extended detection and response (XDR).

As organizações que procuram acrescentar recursos de deteção e resposta aos seus tradicionais controlos de segurança orientados para a prevenção podem escolher entre eles:

* [**FortiGuard MDR Service**](https://www.fortinet.com/products/endpoint-security/fortiedr?utm_source=pr&utm_campaign=endpoint-security/fortiedr%23services#services): Para organizações mais pequenas com uma única equipa de TI/Segurança (ou organizações maiores que procuram atenuar a monitorização e a triagem de alerta de primeira linha), a managed detection and response (MDR) é uma boa opção para acrescentar capacidades de monitorização de segurança sem precisar da perícia especializada para a executar eficazmente.
* [**FortiEDR**](https://www.fortinet.com/products/endpoint-security/fortiedr?utm_source=pr&utm_campaign=fortiedr): Para organizações de média a grande dimensão com equipas de segurança especializadas (mas pequenas), a endpoint detection and response (EDR) é uma boa opção para acrescentar uma análise profunda, ao nível do anfitrião, necessária para identificar os sinais de atividade de ransomware no endpoint.
* [**FortiNDR**](https://www.fortinet.com/products/network-detection-and-response?utm_source=pr&utm_campaign=network-detection-and-response): Para organizações maiores ou equipas de segurança robustas que já implementaram EDR, a network detection and response acrescenta uma análise mais ampla e deteção de anomalias em segmentos de rede ou mesmo em toda a organização, uma visão da atividade a partir de dispositivos sem agentes (quer sejam IoT ou dispositivos não geridos), e uma implementação mais rápida com zero impacto nos sistemas de produção.
* [**FortiXDR**](https://www.fortinet.com/products/fortixdr?utm_source=pr&utm_campaign=fortixdr): Para organizações com múltiplos controlos de segurança Fortinet, a extended detection and response acrescenta análise de curated detection, investigação de alerta alimentada por IA e resposta automática a incidentes.

**Citações de suporte**

"Como nosso fornecedor de segurança de confiança, estamos satisfeitos por ver que a Fortinet continua a fornecer tecnologia de ponta como uma extensão integrada do que já implementámos na nossa rede. A adição de inteligência artificial para análise de malware na FortiNDR dar-nos-á uma enorme vantagem na defesa contra o cibercrime, e estamos entusiasmados por expandir esta capacidade à nossa atividade de rede. Este é o mais recente exemplo da nossa capacidade de ganhar ainda mais valor com o nosso investimento inicial no Fortinet Security Fabric".

- Carolina Masso S., CEO, Gamma Ingenieros SAS

"À medida que as empresas lutam para coordenar a deteção e resposta a ameaças através de produtos pontuais individuais, a sua capacidade de aproveitar um conjunto completo de capacidades SOC integradas como parte de uma plataforma de cibersegurança promete uma melhoria significativa na eficácia e eficiência da descoberta e atenuação de ameaças. O portfólio de produtos de deteção e resposta da Fortinet, tais como FortiNDR, FortiEDR, FortiXDR, e outros, todos integrados como parte de uma plataforma, deve ser considerado para qualquer organização que procure melhorar a sua função de operações de segurança".

- John Grady, Analista Sénior, Cybersecurity na ESG

**Recursos adicionais**

* Consulte o nosso [blog](https://www.fortinet.com/blog/business-and-technology/introducing-fortindr) para mais informações sobre deteção e resposta em rede com FortiNDR.
* Consulte o nosso [blog](https://www.fortinet.com/blog/business-and-technology/battle-ai-ml-cybersecurity-world) para mais informações sobre como a Fortinet utiliza a inteligência artificial e o machine learning nas suas soluções de cibersegurança.
* Saiba mais sobre como a plataforma [Fortinet Security Fabric](https://www.fortinet.com/solutions/enterprise-midsize-business/security-fabric.html?utm_source=pr&utm_campaign=security-fabric) oferece proteção ampla, integrada e automatizada em toda a infraestrutura digital de uma organização.
* Saiba mais sobre as Inteligência de Ameaças e [investigação](https://www.fortinet.com/blog/threat-research?utm_source=pr&utm_medium=pr&utm_campaign=threatresearch) do [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=pr&utm_medium=pr&utm_campaign=FGLabs) ou sobre a [portfólio](https://www.fortinet.com/solutions/enterprise-midsize-business/security-as-a-service/fortiguard-subscriptions?utm_source=pr&utm_medium=pr&utm_campaign=services) de Serviços de Segurança FortiGuard da Fortinet alimentados por IA. Os serviços FortiNDR da FortiGuard podem ser encontrados [aqui](https://www.fortiguard.com/services/fortindr).
* Saiba mais sobre a [formação gratuita de cibersegurança da Fortinet](https://www.fortinet.com/training/cybersecurity-professionals?utm_source=blog&utm_campaign=freetraining), que inclui uma ampla consciencialização cibernética e formação de produtos. Como parte da Training Advancement Agenda (TAA), da Fortinet, o Fortinet Training Institute também oferece formação e certificação através dos programas [Network Security Expert (NSE)](https://www.fortinet.com/training-certification?utm_source=blog&utm_campaign=cert), [Academic Partner](https://www.fortinet.com/training/security-academy-program?utm_source=blog&utm_campaign=academy) e [Education Outreach](https://www.fortinet.com/training/education-outreach-program?utm_source=blog&utm_campaign=education).
* Leia mais sobre como os [clientes da Fortinet](https://www.fortinet.com/customers.html?utm_source=pr&utm_campaign=customers) estão a proteger as suas organizações.
* Participe na [Fortinet User Community (Fuse)](https://fusecommunity.fortinet.com/home?utm_source=pr&utm_campaign=fuse-community). Partilhe ideias e comentários, saiba mais sobre os nossos produtos e tecnologia e conecte-se com colegas.
* Siga a Fortinet no [Twitter](https://twitter.com/Fortinet), [LinkedIn](https://www.linkedin.com/company/fortinet), [Facebook](https://www.facebook.com/fortinet/) e [Instagram](https://www.instagram.com/behindthefirewall/). Subscreva a Fortinet no [YouTube](https://www.youtube.com/channel/UCJHo4AuVomwMRzgkA5DQEOA?sub_confirmation=1).

**Sobre a Fortinet**

A Fortinet (NASDAQ: FTNT) torna possível a existência de um mundo digital em que podemos sempre confiar através da sua missão de proteger pessoas, dispositivos, e dados em todo o lado. É por isso que as maiores empresas, fornecedores de serviços, e organizações governamentais a nível mundial escolhem a Fortinet para acelerar, com segurança, a sua jornada digital. A plataforma Fortinet Security Fabric oferece proteções amplas, integradas e automatizadas em toda a superfície de ataque digital, protegendo dispositivos, dados, aplicações e ligações críticas desde o data center até à cloud e ao escritório em casa. Classificada como #1 na maioria dos dispositivos de segurança enviados em todo o mundo, mais de 580.000 clientes confiam na Fortinet para proteger os seus negócios. E o Fortinet NSE Training Institute, uma iniciativa da Fortinet Training Advancement Agenda (TAA), fornece um dos maiores e mais amplos programas de formação na indústria para tornar a formação cibernética e novas oportunidades de carreira disponíveis a todos. Saiba mais em https://www.fortinet.com, no Blog Fortinet, ou nos Laboratórios FortiGuard.

*Copyright © 2022 Fortinet, Inc. Todos os direitos reservados. Os símbolos ® e ™ denotam respetivamente marcas comerciais registadas a nível federal e marcas comerciais de direito comum da Fortinet, Inc., suas subsidiárias e afiliadas. As marcas comerciais da Fortinet incluem, mas não estão limitadas ao seguinte: Fortinet, FortiGate, FortiGuard, FortiCare, FortiManager, FortiAnalyzer, FortiOS, FortiADC, FortiAP, FortiAppMonitor, FortiASIC, FortiAuthenticator, FortiBridge, FortiCache, FortiCamera, FortiCASB, FortiClient, FortiCloud, FortiConnect, FortiController, FortiConverter, FortiDB, FortiDDoS, FortiExplorer, FortiExtender, FortiFone, FortiCarrier, FortiHypervisor, FortiIsolator, FortiMail, FortiMonitor, FortiNAC, FortiPlanner, FortiPortal, FortiPresence , FortiProxy, FortiRecorder, FortiSandbox, FortiSIEM, FortiSwitch, FortiTester, FortiToken, FortiVoice, FortiWAN, FortiWeb, FortiWiFi, FortiWLC, FortiWLCOS e FortiWLM.*

Outras marcas pertencem aos seus respetivos proprietários. A Fortinet não verificou independentemente declarações ou certificações aqui atribuídas a terceiros e a Fortinet não endossa independentemente tais declarações. Não obstante qualquer disposição em contrário aqui contida, nada aqui constitui uma garantia, contrato, especificação vinculativa ou outro compromisso vinculativo da Fortinet ou qualquer indicação de intenção relacionada com um compromisso vinculativo, e as informações sobre desempenho e outras especificações aqui contidas podem ser exclusivas para determinados ambientes. Este comunicado à imprensa pode conter declarações prospetivas que envolvam incertezas e suposições, tais como declarações relativas a divulgações de tecnologia, entre outras. Alterações de circunstâncias, atrasos na divulgação de produtos, ou outros riscos, tal como indicado nos nossos arquivos na Comissão de Títulos e Câmbios, localizada em www.sec.gov, podem fazer com que os resultados sejam materialmente diferentes dos expressos ou implícitos neste comunicado de imprensa. Se as incertezas se materializarem ou os pressupostos se revelarem incorretos, os resultados podem diferir materialmente daqueles expressos ou implícitos por tais declarações e pressupostos prospetivos. Todas as declarações que não sejam declarações de factos históricos são declarações que podem ser consideradas declarações relativas ao futuro. A Fortinet não assume qualquer obrigação de atualizar quaisquer declarações relativas ao futuro, e renuncia expressamente a qualquer obrigação de atualizar estas declarações relativas ao futuro.

**Para mais informação contacte:**

**Lift Consulting**

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

Inês Filipe | ines.filipe@lift.com.pt | 910 283 054