**Fortinet lança nova oferta de proteção contra riscos digitais para capacitar equipas de segurança e executivas na perspetiva do atacante**

*FortiRecon combina machine learning, automatização e inteligência humana para monitorizar continuamente a superfície de ataque externa de uma organização, determinar o risco da marca e fornecer informações personalizadas para agir mais rapidamente contra as ameaças.*

**Lisboa, 30 de junho de 2022**

**John Maddison, EVP of Products and CMO da Fortinet**

"Quanto mais cedo, no ciclo de ataque, se conseguir identificar e deter um adversário, menos dispendiosa e prejudicial será a sua tentativa. Utilizando uma poderosa combinação de inteligência humana e artificial, o FortiRecon fornece às organizações uma visão do que os adversários estão a ver, fazer e planear. O modelo de entrega SaaS agnóstico do FortiRecon, combinado com uma interface intuitiva e relatórios facilmente percetíveis, permite aos executivos de toda a organização compreender rapidamente os riscos colocados à sua empresa, dados e reputação da marca, enquanto a nossa equipa de especialistas em cibersegurança, da FortiGuard Labs, melhora a oferta com serviços de takedown, orientação sobre a priorização dos esforços de remediação, e investigação e inteligência de ameaças direcionadas".

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 [FortiRecon](https://www.fortinet.com/products/fortirecon), uma oferta completa de Digital Risk Protection Service (DRPS) que utiliza uma poderosa combinação de machine learning, capacidades de automação e especialistas em cibersegurança, da [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=pr&utm_campaign=fortiguard-labs-consulting#fortiguard-labs-consulting), para gerir a postura de risco de uma empresa e aconselhar ações significativas para proteger a reputação da marca, bens e dados empresariais. O FortiRecon oferece, de forma única, uma solução tripla de cobertura externa de External Attack Surface Management (EASM), Brand Protection (BP) e Adversary-Centric Intelligence (ACI) para combater ataques na fase de reconhecimento - a primeira fase de um ciberataque - para reduzir significativamente o risco, o tempo e o custo da mitigação de ameaças em fases posteriores.

**As organizações estão sobrecarregadas na defesa da sua rede, dados, reputação e na mitigação dos riscos de forma antecipada**

Antes de atacar uma organização, o principal objetivo de um cibercriminoso é reunir o máximo de informação sobre o seu alvo. Esta fase de reconhecimento inicial, mune o adversário com tudo o que precisa para determinar se, e como, irá explorar uma organização. Testará as táticas de defesa e resposta de uma empresa, procurará sistemas não corrigidos, utilizará as redes sociais para aprender mais sobre os seus colaboradores e seu comportamento normal, e irá chegar ao ponto de investigar parceiros de negócios, aquisições recentes e qualquer outra afiliação de terceiros que possa conduzir a um ataque bem-sucedido. À medida que as organizações aceleram digitalmente os seus negócios e implementam [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), que expandem a superfície de ataque, a identificação e a mitigação destas ameaças tem vindo a tornar-se cada vez mais difícil. Em resposta à velocidade das ameaças, as melhores práticas de cibersegurança evoluíram de avaliações pontuais para uma monitorização contínua, bem como revisões e melhorias contínuas na postura de segurança de uma organização.

**Extrair uma página do Playbook do adversário para Mitigar o Risco**

Com a introdução do FortiRecon, a Fortinet fornece às organizações empresariais uma ferramenta poderosa para compreender como o adversário vê uma organização a partir do exterior para ajudar a informar as equipas de cibersegurança, o nível C e a gestão de risco e conformidade sobre como dar prioridade ao risco e melhorar a postura global de segurança da empresa. O FortiRecon oferece às empresas uma cobertura consistente e abrangente em três áreas:

* **Monitorização externa da superfície de ataque:** Capacita as organizações para compreenderem o seu perfil de risco e mitigarem os riscos antecipadamente. Proporciona uma visão externa de uma organização e das suas filiais para identificar os ativos empresariais conhecidos e desconhecidos expostos e as vulnerabilidades associadas, e dar prioridade à remediação de questões críticas. O EASM identifica servidores, credenciais, configurações erradas de serviços públicos na cloud, e mesmo vulnerabilidades de código de software de parceiros terceiros que poderiam ser exploradas por atores maliciosos.
* **Proteção da marca:** Permite às organizações proteger a sua marca e identificar os riscos para os seus clientes. Algoritmos proprietários detetam erros de digitalização baseados na internet, desfigurações, e personificações de phishing, bem como aplicações móveis desonestas, divulgação de credenciais, e personificação da marca nas redes sociais, todas técnicas comuns utilizadas pelos atores da ameaça cibernética. A deteção precoce de atividade maliciosa permite que as equipas tomem rapidamente medidas (tais como a retirada de websites ou aplicações) para parar e prevenir danos.
* **Inteligência Centrada no Adversário:** Aumenta a consciencialização de segurança da equipa de SOC de uma organização, com cobertura específica do sector, e da geografia para entender melhor os seus invasores e proteger os ativos. Os especialistas em segurança cibernética da FortiGuard Labs avaliam os riscos de ameaças underground e iminente, apresentados por cibercriminosos ativos a uma empresa individual, monitorizando proativamente fóruns públicos e privados, código aberto, dark web e outros domínios dos cibercriminosos. Juntamente com a inteligência humana, os especialistas da FortiGuard Labs avaliam e selecionam inteligência de ameaças personalizada, fornecendo recomendações específicas para a empresa, sector e localização.

Para os parceiros, o FortiRecon pode ser vendida adicionando ao [Fortinet Security Fabric](https://www.fortinet.com/solutions/enterprise-midsize-business/security-fabric?utm_source=pr&utm_medium=pr&utm_campaign=fabric) ou como uma solução autónoma e agnóstica de fornecedor que entrega relatórios facilmente percetiveis e permite aos seus clientes compreenderem, rapidamente os riscos colocados à sua empresa, dados e reputação da marca. O FortiRecon também alarga as categorias de risco para as quais os parceiros podem fornecer informações aos clientes e aumenta a oportunidade de conseguir novos clientes que apenas investiram em soluções de segurança mais tradicionais.

**Melhoria do Portfólio de Deteção, Resposta antecipada da Fortinet, e Serviços de Segurança líderes na indústria**

O FortiRecon complementa o robusto portfólio da Fortinet de produtos de deteção antecipada e resposta avançada, incluindo [FortiNDR](https://www.fortinet.com/products/network-detection-and-response?utm_source=pr&utm_campaign=fortindr), [FortiXDR](https://www.fortinet.com/products/fortixdr?utm_source=pr&utm_campaign=fortixdr), [FortiDeceptor](https://www.fortinet.com/products/fortideceptor.html?utm_source=blog&utm_campaign=deception), [in-line sandboxing](https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/inline-sandboxing?utm_source=pr&utm_campaign=fortiguard-security-subscriptions%2Finline-sandboxing), bem como automação avançada com [FortiAnalyzer](https://www.fortinet.com/products/management/fortianalyzer.html?utm_source=pr&utm_campaign=fortianalyzer), [FortiSIEM](https://www.fortinet.com/products/siem/fortisiem.html?utm_source=pr&utm_campaign=fortisiem) e [FortiSOAR](https://www.fortinet.com/products/fortisoar.html?utm_source=pr&utm_campaign=fortisoar)

A Fortinet está empenhada no sucesso das equipas SOC e na proteção das organizações e oferece um extenso portfólio de serviços externos, que vão desde avaliações de cibersegurança, desenvolvimento de playbooks, tabletop training, [resposta a incidentes](https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/incident-response?utm_source=pr&utm_campaign=incident-response), [MDR](https://www.fortinet.com/products/endpoint-security/fortiedr?utm_source=pr&utm_campaign=endpoint-security/fortiedr%23services#services) e [SOC-as-a-Service](https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/forticloud-socaas?utm_source=pr&utm_campaign=fortiguard-security-subscriptions%2Fforticloud-socaas). Esta oferta combinada juntamente com os vários aperfeiçoamentos em todo o Fortinet Security Fabric, e o ecossistema alargado proporcionam simplificação e automatização para ajudar as equipas SOC a recuperarem o foco, o controlo e a rapidez, reforçando o SOC de uma organização com ferramentas e especialistas em cibersegurança da FortiGuard Labs.

**Recursos adicionais**

* Leia o nosso [blog](https://www.fortinet.com/blog/business-and-technology/strengthening-human-elements-in-your-cybersecurity-stack?utm_source=pr&utm_medium=pr&utm_campaign=fortirecon) para saber mais sobre o valor que os serviços de segurança podem trazer a qualquer organização e descubra mais sobre o robusto portfólio de Serviços de Segurança alimentados por IA da Fortinet.
* Saiba mais sobre as ofertas de deteção avançada da Fortinet para o SOC: [FortiNDR](https://www.fortinet.com/products/network-detection-and-response?utm_source=pr&utm_campaign=fortindr), [FortiDeceptor](https://www.fortinet.com/products/fortideceptor.html?utm_source=blog&utm_campaign=deception), [FortiXDR](https://www.fortinet.com/products/fortixdr?utm_source=pr&utm_campaign=fortixdr), e [FortiGuard In-line Sandbox Service](https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/inline-sandboxing?utm_source=pr&utm_campaign=fortiguard-security-subscriptions%2Finline-sandboxing)
* Saiba mais sobre Fortinet [SOC-as-a-Service](https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/forticloud-socaas).
* Saiba mais sobre como o [Fortinet Security Fabric](https://www.fortinet.com/solutions/enterprise-midsize-business/security-fabric?utm_source=pr&utm_medium=pr&utm_campaign=fabric)  oferece uma proteção ampla, integrada e automatizada em toda a infraestrutura digital de uma organização.
* Saiba mais sobre os [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=pr&utm_medium=pr&utm_campaign=FGLabs) de Inteligência e [Investigação](https://www.fortinet.com/blog/threat-research?utm_source=pr&utm_medium=pr&utm_campaign=threatresearch) de Ameaças ou sobre o [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.
* 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.

***FTNT-O***

*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, o logótipo Fortinet, FortiGate, FortiOS, FortiGuard, FortiCare, FortiAnalyzer, FortiManager, FortiASIC, FortiClient, FortiCloud, FortiCore, FortiMail, FortiSandbox, FortiADC, FortiAP, FortiAppEngine, FortiAppMonitor, FortiAuthenticator, FortiBalancer, FortiBIOS, FortiBridge, FortiCache, FortiCall, FortiCam, FortiCamera, FortiCarrier, FortiCASB, FortiCenter, FortiCentral, FortiConnect, FortiController, FortiConverter, FortiCWP, FortiDB, FortiDDoS, FortiDeceptor, FortiDirector, FortiDNS, FortiEDR, FortiExplorer, FortiExtender, FortiFirewall, FortiFone, FortiGSLB, FortiHypervisor, FortiInsight, FortiIsolator, FortiLocator, FortiLog, FortiMeter, FortiMoM, FortiMonitor, FortiNDR, FortiNAC, FortiPartner, FortiPenTest, FortiPhish, FortiPortal, FortiPresence , FortiProtect, FortiProxy, FortiRecorder, FortiReporter, FortiSASE, FortiScan, FortiSDNConnector, FortiSIEM, FortiSDWAN, FortiSMS, FortiSOAR, FortiSwitch, FortiTester, FortiToken, FortiTrust, FortiVoice, FortiVoIP, 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 de 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.