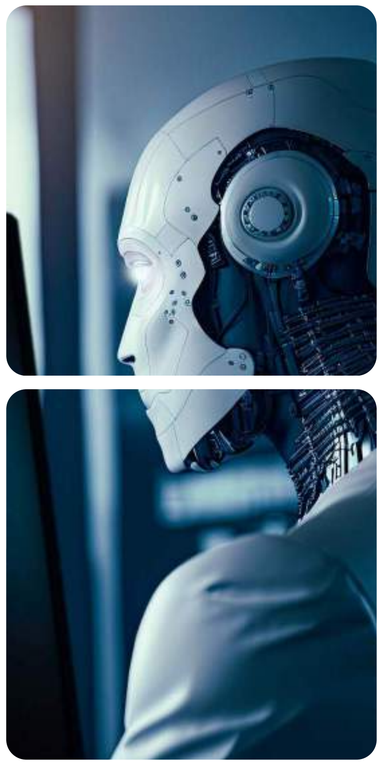
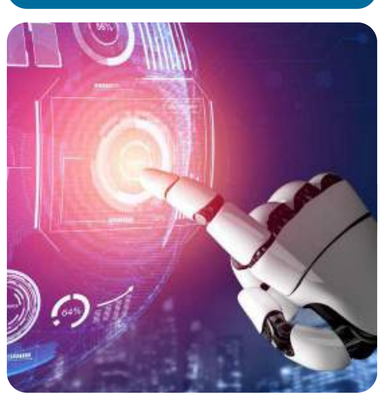
Cibersegurança
NA ERA DA
Inteligência Artificial

PRÓXIMO NÍVEL
por Embratel

Sumário





Introdução

De acordo com pesquisadores da Universidade de Stanford, não existe uma definição precisa e universalmente aceita para Inteligência Artificial (IA). No entanto, em vez de ser um problema, os estudiosos apontam o fato como uma virtude, pois essa característica tem ajudado a IA a crescer, florescer e avançar em um ritmo cada vez mais acelerado. O estudo sobre os 100 anos da IA, feito pela Universidade de Stanford, detalha que "profissionais, pesquisadores e desenvolvedores de IA são guiados por um senso de direção aproximado e por um imperativo de seguir em frente".

Sim, a IA tem um longo histórico e vem mudando de máquinas, saindo das calculadoras automáticas para migrar para smartphones, citando apenas um dos exemplos. Nesse e-book, nosso objetivo é abordar o uso da IA em cibersegurança, considerando que a adoção da Inteligência Artificial é um caminho sem volta no mercado corporativo, conforme apontado pela pesquisa da consultoria McKinsey editada em 2023. Na avaliação dos consultores, as organizações de alto desempenho investem muito mais em IA do que outras, gastando até cinco vezes mais em Inteligência Artificial do que o seu orçamento de digitalização total.

Tipos de IA

Para iniciar nossa jornada, é importante entender os tipos de IA, e começamos com o posicionamento do futurista Bernardo Marr, que identifica quatro tipos de Inteligência Artificial: Reativa, Memória Limitada, Teoria da Mente e Autoconsciente. A mesma classificação é adotada pelo site Tech Target, especializado em tecnologia.

1. IA Reativa

Nesse tipo, os algoritmos reativos operam apenas com dados atuais e têm capacidades limitadas. A IA reativa não possui nenhuma memória funcional específica, o que significa que não pode usar experiências anteriores para informar suas ações presentes e futuras. Segundo o Tech Target, os modelos de IA reativa são derivados da matemática estatística e consideram grandes quantidades de dados para produzir resultados aparentemente inteligentes. Um exemplo clássico de IA reativa foi o uso do supercomputador Deep Blue, da IBM, para derrotar o grande mestre do xadrez Garry Kasparov em 1997.

2. IA de Memória Limitada

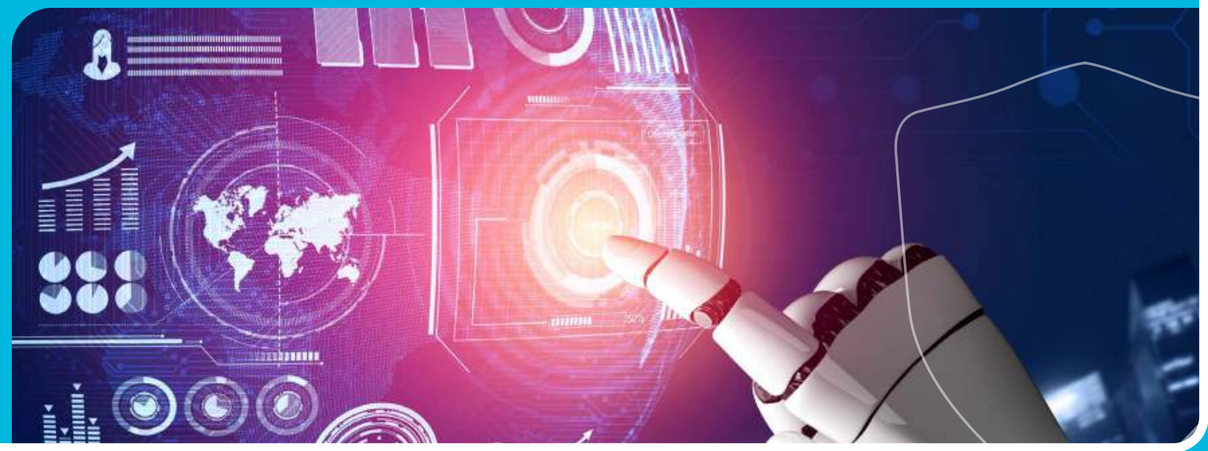
Esse tipo de Inteligência Artificial aprende com o passado e constrói conhecimento experiencial observando ações ou dados. A IA de Memória Limitada utiliza dados históricos e observacionais, combinados com informações pré-programadas, para fazer previsões e executar tarefas complexas de classificação. Segundo Bernardo Marr, esse é o tipo de IA mais utilizado atualmente.

3. IA de Teoria da Mente

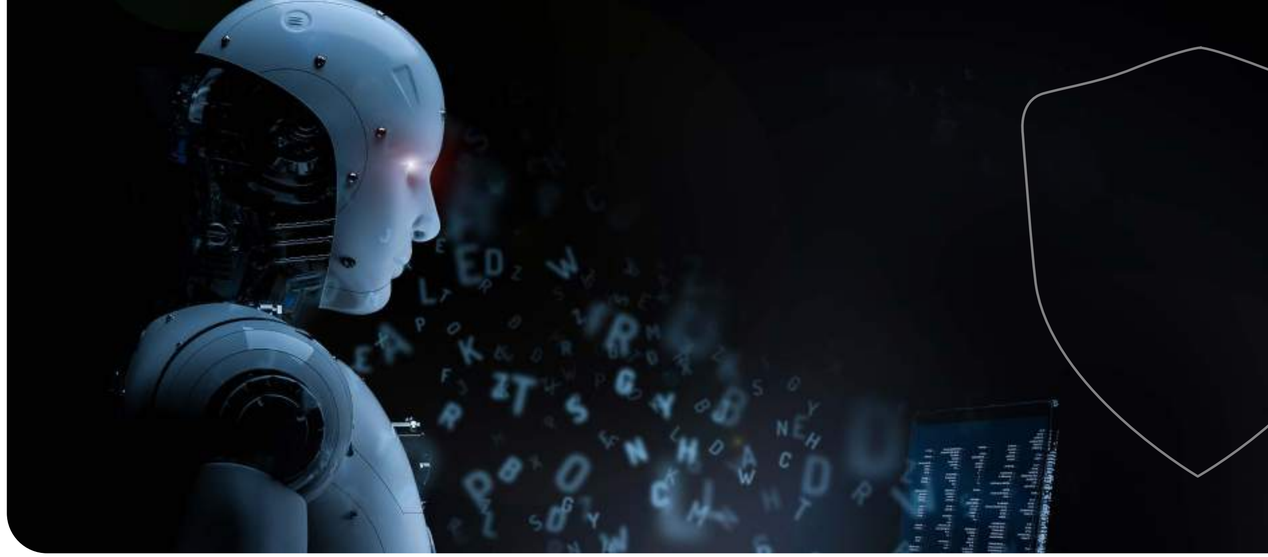
Esse tipo de IA é baseado na psicologia e considera que a IA pode inferir os motivos e intenções humanas, incluindo crenças, emoções e objetivos. Segundo a avaliação do Tech Target, a IA de Teoria da Mente ainda não foi desenvolvida. A meta desse tipo de IA é reconhecer, simular, monitorar e responder adequadamente às emoções humanas através da análise de voz, imagem e outros tipos de dados.

4. IA Autoconsciente

Esse é o tipo mais avançado. Máquinas desse tipo terão a capacidade de estar conscientes de suas próprias emoções, bem como das emoções dos outros ao seu redor, alcançando um nível de consciência e inteligência semelhante ao dos seres humanos. No entanto, ainda não desenvolvemos esse tipo de IA sofisticada e não temos hardware ou algoritmos para suportá-la, de acordo com Marr.



A relação entre **Cibersegurança e IA**



Independentemente da evolução dos tipos de IA, ela está se tornando uma ferramenta essencial na luta contra os cibercriminosos, conforme avaliação de Hari Ravichandran, especialista no assunto. Em um artigo para a revista Forbes, ele explica a relação sinérgica entre essas duas tecnologias.

A evolução do modelo de negócio dos criminosos cibernéticos inclui "ofertas" inacreditáveis, como os serviços por assinatura. Além disso, os malfeitores têm usado recursos de IA para escrever códigos maliciosos e avançar em várias frentes.

O contrário também pode acontecer, ou seja, a adoção da IA como recurso para identificar e mitigar as ameaças de cibersegurança. Uma pesquisa recente da Blackberry nos Estados Unidos indicou que 82% dos tomadores de decisão de TI planejam investir em segurança cibernética baseada em IA nos próximos dois anos, com quase metade (48%) planejando fazê-lo antes do final de 2023.

O Forbes Technology Council aponta que 76% das empresas priorizaram a IA e o aprendizado de máquina em seus orçamentos de TI. Isso ocorre devido ao crescente volume de dados que precisam ser analisados para identificar e mitigar ameaças cibernéticas, entre outros motivos.

Já o National Institute of Standards and Technology (NIST), dos Estados Unidos, destaca que a IA desempenha um duplo papel, tanto como ameaça quanto como barreira contra o cibercrime. Segundo o instituto, os riscos da IA não devem ser considerados isoladamente; o tratamento paralelo dos riscos da IA com outras ameaças críticas, como a segurança cibernética, produzirá um resultado mais integrado e eficiente.

Além disso, a IA pode ser uma grande aliada da cibersegurança, proporcionando novas ferramentas para abordar vulnerabilidades e ajudar a mitigar a escassez de mão de obra nessa área. Ao mesmo tempo, a IA pode aprimorar a capacidade dos especialistas em defesa cibernética, atuando como uma espécie de co-piloto no desenvolvimento de ferramentas de ciberdefesa.

Os ataques mais comuns usando IA

Com o avanço da Inteligência Artificial, é fundamental entender os desafios de segurança que ela traz. Em sua análise sobre o tema, o site especializado AI Infrastructure destaca vários pontos de atenção e lista os ataques cibernéticos mais comuns que utilizam a IA. São eles:

1. Evasão

Nesse tipo de ataque, um invasor modifica os dados de entrada para que o modelo de IA não consiga identificar corretamente sua entrada. O objetivo do ataque é evitar o desempenho do modelo de IA. Isso pode incluir conteúdo de spam oculto em uma imagem, para burlar medidas anti-spam, ou enganar um carro autônomo adulterando os sinais de trânsito.

2. Envenenamento

Esse tipo de ataque é baseado na capacidade da IA de aprender com os dados fornecidos a ela. Os cibercriminosos podem usar essa característica para injetar conteúdo malicioso. O invasor visa condicionar os algoritmos de acordo com suas motivações. O Instituto dos Engenheiros Eletricistas e Eletrônicos (IEEE) avalia que esse tipo de ataque é simples e prático de ser usado, não exigindo habilidades técnicas complexas dos invasores.

3. Inferência

Esse é o método preferido dos cibercriminosos, que buscam informações nos dados de treinamento para lucrar com isso. Os modelos de IA são treinados com milhares de conjuntos de dados, contendo informações confidenciais. Um ataque de inferência pode ocorrer se o invasor tiver informações parciais sobre os dados de treinamento e adivinhar os dados ausentes até que o algoritmo alcance o melhor desempenho.

4. Extração

Nesse caso, a origem do ataque pode ser interna ou de cibercriminosos. O objetivo é testar o sistema de aprendizado de máquina para reconstruir o modelo ou extrair os dados nos quais ele foi treinado. Um exemplo é a invasão do sistema de reconhecimento de pedestres em carros autônomos, onde dados de entrada elaborados são inseridos no modelo original para prever a saída.

Ciberdefesa

O outro lado da moeda

Agora que descrevemos os principais tipos de ataques, é importante ressaltar novamente o papel da IA como aliada contra os cibercriminosos. Hari Ravichandran, o especialista mencionado anteriormente, destaca cinco vantagens da IA nesse sentido:

1

Melhoria da Segurança

A capacidade da IA de fazer inferências, reconhecer padrões e realizar ações proativas, em nome do usuário, amplia a proteção contra ameaças online. Ao automatizar a resposta a incidentes, simplificar a caça por ameaças e analisar grandes quantidades de dados, a IA melhora a segurança cibernética.

2

Monitoramento Contínuo

A IA fornece acompanhamento contínuo, essencial para a segurança cibernética moderna. As ferramentas de segurança cibernética baseadas em IA identificam e detectam ataques em tempo real, automatizando o processo de resposta a incidentes. Elas também auxiliam especialistas humanos a identificar ameaças emergentes e tomar medidas preventivas.

3

Identificação de Falsos Positivos

A IA pode endereçar o desafio dos analistas humanos em identificar falsos positivos. Isso reduz a carga sobre esses profissionais e torna a detecção e análise de ameaças mais precisas e eficientes.

4

Reforço no Controle de Acesso

Algoritmos de aprendizado de máquina podem identificar padrões de comportamento anômalos e sinalizar tentativas de login suspeitas, facilitando a identificação de possíveis violações de segurança. Além disso, as soluções baseadas em IA podem melhorar o gerenciamento de senhas, identificando automaticamente senhas fracas e exigindo senhas mais fortes.

5

Mitigação de Ameaças Internas

A IA pode ser usada para mitigar ameaças internas, que representam um desafio significativo para as organizações. Ao analisar o comportamento do usuário, as soluções baseadas em IA podem identificar funcionários envolvidos em atividades maliciosas, prevenindo violações de dados e outros incidentes de segurança.

Recursos de IA
Integrados em Cibersegurança

O uso de recursos de IA como aliados da cibersegurança pode ser resumido em três áreas, conforme especialistas do site Analytics Insight:

Ferramentas de Segurança Aprimoradas por IA

Quase todas as soluções de segurança no mercado podem incorporar IA, incluindo firewalls, filtragem de conteúdo, sistemas de prevenção/detecção de intrusões e ferramentas de proteção de endpoint. A IA melhora a detecção de anomalias e a precisão da detecção, analisando padrões comportamentais e desenvolvendo inteligência preditiva por meio de coleta de dados.

Automação Alimentada por IA para Segurança e Conformidade

A IA pode ser usada para descobrir novos perigos e vulnerabilidades, e as medidas de mitigação podem ser realizadas com pouca participação humana, graças a ferramentas de automação orientadas por IA.

Casos de Uso de Segurança Baseados em IA Integrados à Infraestrutura

A IA pode ser integrada à infraestrutura de TI, como redes corporativas definidas por software (SD-WAN) e computação de borda (edge computing), protegendo novas tecnologias.

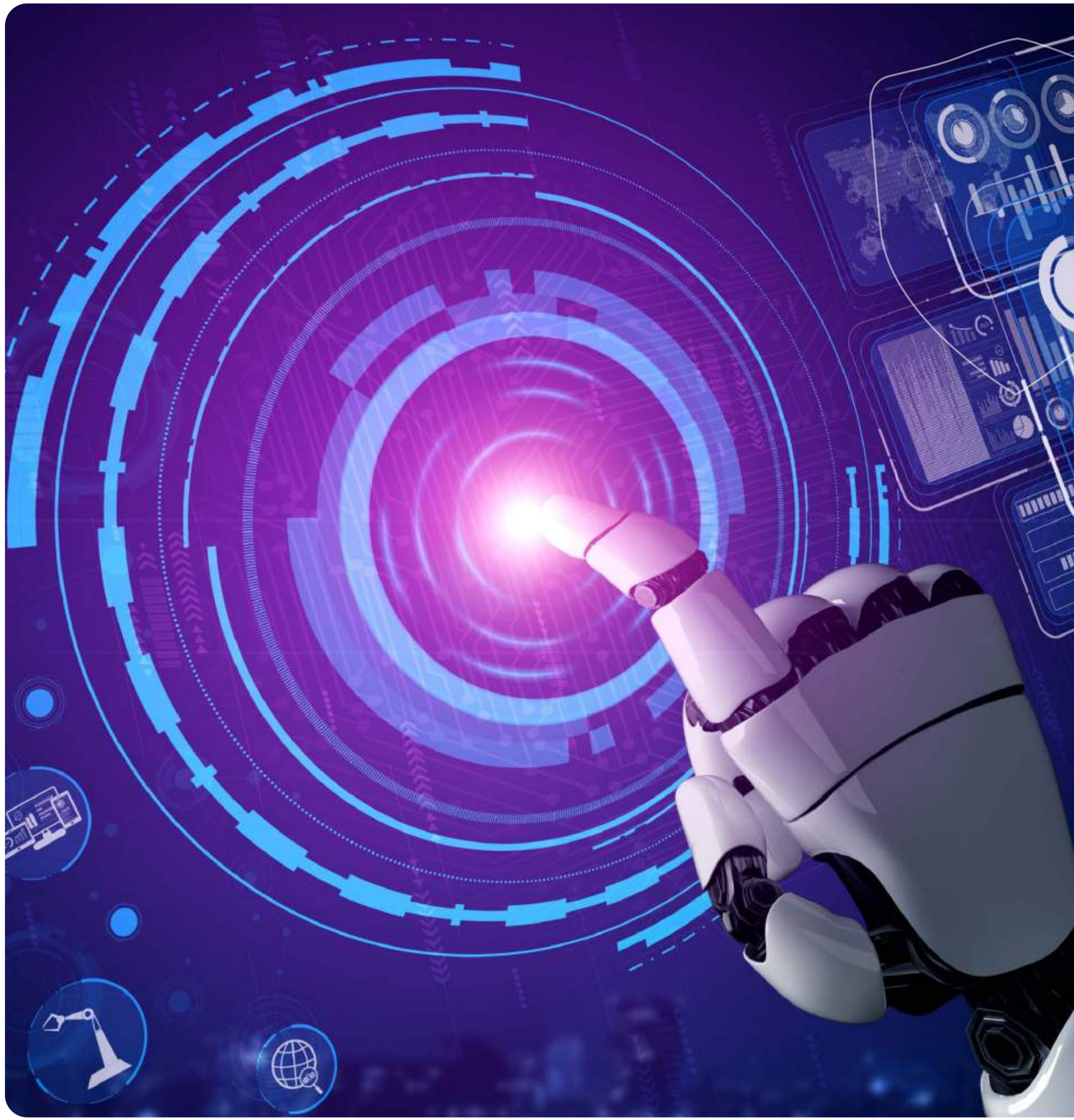
Tendências de IA em Cibersegurança

Várias subdisciplinas de IA, como visão computacional, reconhecimento de voz e processamento de linguagem natural, estão em pleno desenvolvimento. De acordo com a Huawei, o avanço da próxima geração de IA reside na inferência de conhecimento. No entanto, a garantia de segurança é crucial nesse avanço.

Nos próximos anos, com a implantação da IA em áreas como transporte e cuidados médicos, a tecnologia deve ser introduzida de forma a criar confiança e compreensão, respeitando os direitos humanos e civis.

A disseminação da IA em mercados verticais também é destacada por Bruce Schneier, que alerta que o mercado financeiro será o alvo inicial de super ataques utilizando IA. Ele ressalta que a mesma sofisticação que prejudica o mercado financeiro pode ser uma vantagem, contribuindo para a cibersegurança.

Schneier também prevê a terceirização da cibersegurança com uso intensivo de recursos de IA para lidar com o aumento de novas tecnologias e restrições orçamentárias. Ele sugere o desenvolvimento de plataformas de segurança da internet, em vez de apenas tentar mudar o comportamento do usuário.



Conclusão

Ao longo deste e-book, exploramos a relação entre a Inteligência Artificial (IA) e a cibersegurança, compreendendo como a IA está se tornando uma ferramenta indispensável na luta contra ameaças cibernéticas. Desde os diferentes tipos de IA até os ataques mais comuns que exploram suas características, ficou claro que a evolução da cibersegurança e da IA são intrinsecamente ligadas.

A IA não apenas apresenta desafios no campo da segurança, mas também oferece soluções inovadoras para proteger sistemas e dados valiosos. A capacidade da IA de identificar padrões, detectar anomalias em tempo real, automatizar processos de resposta e mitigar ameaças internas torna-se uma defesa poderosa contra-ataques cibernéticos cada vez mais sofisticados.

Enquanto enfrentamos os riscos e as complexidades trazidos pela convergência da IA e da cibersegurança, é vital que continuemos a investir em pesquisa, desenvolvimento e colaboração para garantir a evolução segura e ética dessas tecnologias. A integração inteligente da IA em ferramentas de segurança cibernética, a abordagem proativa para identificar ameaças e a compreensão de suas tendências emergentes nos guiarão na proteção de nossos sistemas, dados e, acima de tudo, da sociedade digital como um todo. Com as estratégias certas, a IA pode ser a chave para um mundo cibernético mais seguro e resiliente.

Conheça a estratégia

de segurança completa em camadas da **Embratel**

Clique aqui