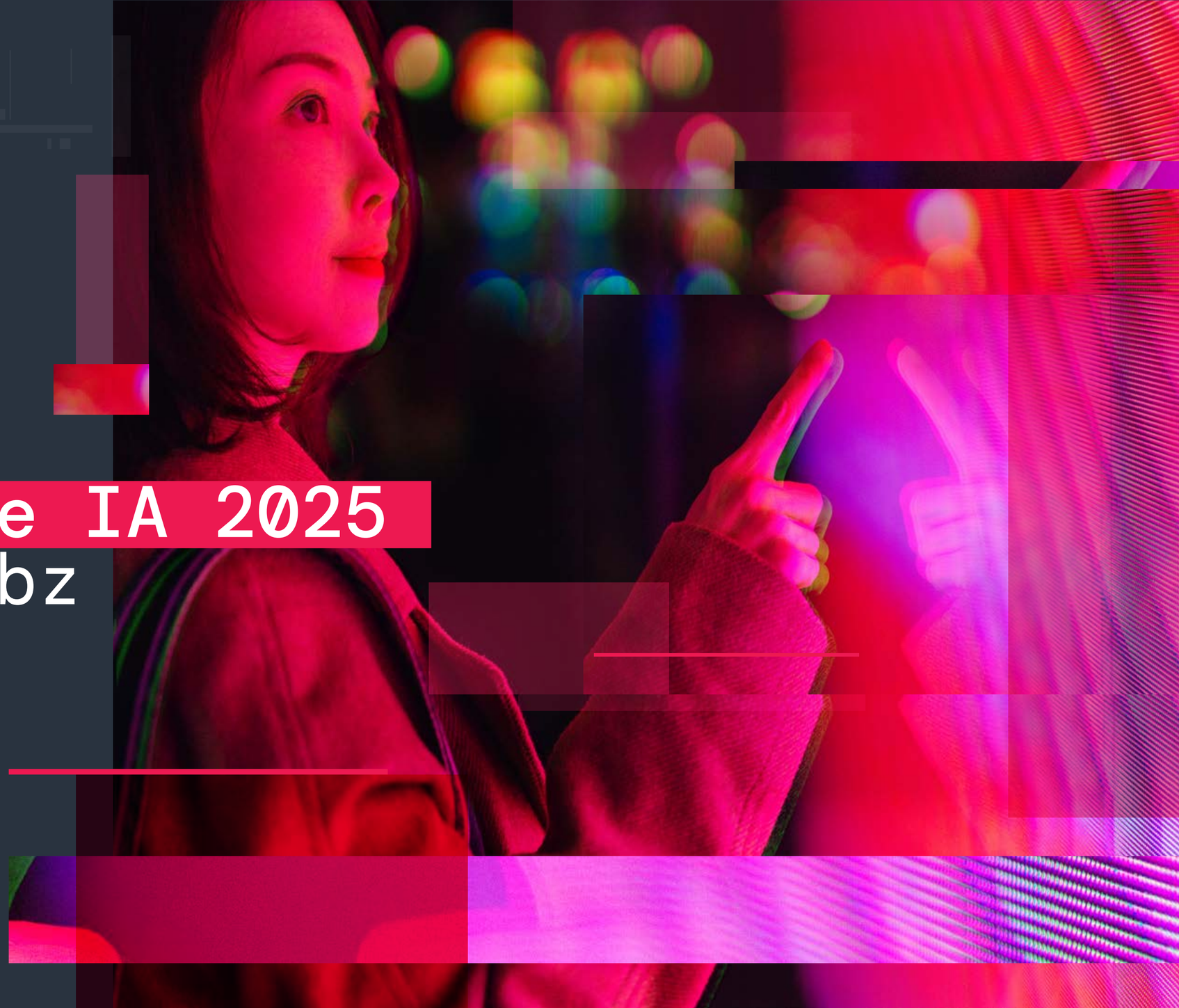
Relatório de segurança de IA 2025 da ThreatLabz



©2025 Zscaler, Inc. Todos os direitos reservados.

Índice_

Resumo executivo 3

Principais descobertas 4

Tendências de uso de IA e ML 6

- Visão geral das transações de IA/ML 6
- Transações de IA/ML bloqueadas 12
- Perda de dados para aplicativos de IA/ML 13
- Uso da IA por setor 14
  - Destaques dos setores 15
- Tendências de uso do ChatGPT 19
- Uso de IA por país 20
  - Insights da EMEA 21
  - Insights da APAC 22

Riscos empresariais da IA e cenários de ameaças reais 23

- Principais riscos da adoção empresarial da IA 23
- DeepSeek e IA de código aberto: o risco de modelos de fronteira no seu bolso 25
  - Fraude em 5 prompts: página de phishing gerada pelo DeepSeek 27
- O papel crescente da IA nas ameaças cibernéticas 29
  - Engenharia social turbinada 29
  - Malware e ransomware baseados em IA em toda a cadeia de ataque 30
  - IA agente: a próxima fronteira em IA autônoma; e vetores de ataque 31
- Estudo de caso: como criminosos estão explorando o interesse em IA 33

O âmbito evolutivo dos regulamentos de IA 35

Previsões de ameaças de IA para 2025–2026 37

Práticas recomendadas para a adoção segura da IA em empresas 39

- Cinco etapas para integrar com segurança ferramentas de GenAI 40

Como a Zscaler oferece zero trust + IA42

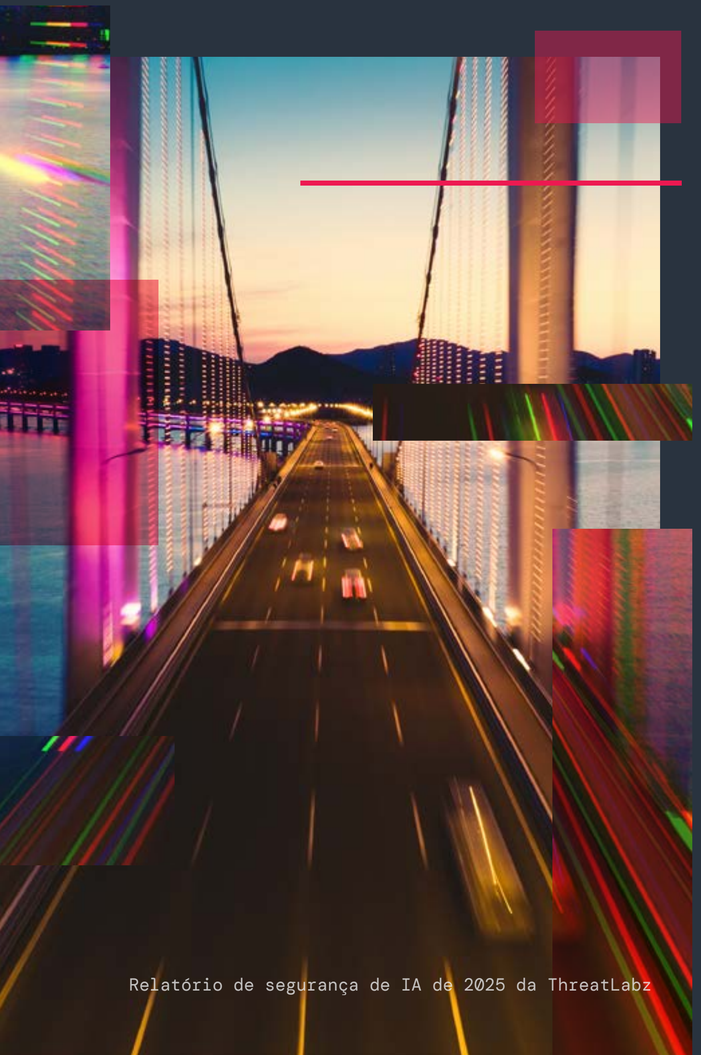
- Como funciona: a vantagem de segurança e dados da IA da Zscaler 42
- Uma abordagem abrangente à segurança de IA 43
- Uso da segurança de IA em toda a cadeia de ataque 46

Metodologia de pesquisa 48

- Sobre a ThreatLabz 48
- Sobre a Zscaler 48

©2025 Zscaler, Inc. Todos os direitos reservados.

Resumo executivo_



Mais um ano na ainda nova “era da IA” chegou e passou, marcado por avanços revolucionários, adoção crescente em todos os setores e desafios de alto nível.

As empresas agora veem a inteligência artificial (IA) e o aprendizado de máquina (ML) como essenciais para o crescimento, impulsionando a eficiência, a tomada de decisões mais inteligentes e a inovação mais rápida. Por outro lado, a adoção da IA traz sérios riscos de segurança, desde o uso não autorizado (“IA paralela”) até a exposição de dados. Ainda mais preocupante é que os cibercriminosos parecem estar em vantagem, pois usam essas mesmas ferramentas para ampliar os ataques. O que antes exigia habilidade agora exige esforço mínimo. O que antes levava horas agora leva segundos.

Essa mudança ficou evidente em 2024. A GenAI se tornou uma máquina de engenharia social para criminosos cibernéticos. Hoje em dia, e-mails de phishing imitam colegas de confiança com uma precisão assustadora. A tecnologia de deepfake transforma vozes e vídeos em armas de fraude.

Em 2025, o poder e os perigos da IA serão maiores do que nunca. Os criminosos continuarão a ultrapassar os limites das capacidades maliciosas da IA. No entanto, a IA não está apenas promovendo ataques. Ela também é uma linha de defesa essencial, fortalecendo a luta contra esses ataques.

O Relatório de segurança de IA de 2025 da Zscaler ThreatLabz examina as muitas facetas da IA na segurança cibernética, desde adoção de IA/ML até ameaças e recursos de segurança baseados em IA.

Analisando 536,5 bilhões de transações de ferramentas de IA/ML capturadas na Zscaler Zero Trust Exchange™ entre fevereiro e dezembro de 2024, a ThreatLabz descobriu mudanças surpreendentes e não surpreendentes nas tendências de uso por empresas em todo o mundo.

O ChatGPT impulsionou a maioria transações de IA/ML, representando quase metade do volume total. Da perspectiva por indústria, os setores de finanças e seguros e de manufatura promoveram a maioria das transações como os principais adotantes da IA. No entanto, o aumento da adoção não significou acesso irrestrito: uma grande porcentagem de transações de IA/ML foram ativamente bloqueadas.

Além das tendências de uso, a ThreatLabz descobriu cenários de ameaças reais, desde phishing aprimorado por IA até plataformas de IA falsas. Este relatório também explora desenvolvimentos recentes em áreas que, sem dúvida, influenciarão a IA em 2025 e além, incluindo IA agente, o surgimento do DeepSeek e o cenário regulatório em evolução.

À medida que os recursos de IA/ML evoluem e as ameaças que eles possibilitam aumentam, o imperativo é claro: controles de segurança mais sofisticados e robustos, arquitetura zero trust e defesas baseadas em IA não são mais opcionais; são essenciais. Continue lendo para obter mais insights e estratégias práticas para ajudar sua organização a adotar a IA com segurança e, ao mesmo tempo, ficar à frente das ameaças baseadas em IA.

©2025 Zscaler, Inc. Todos os direitos reservados.

Principais_ decobertas

A ThreatLabz **analisou 536,5 bilhões de transações de IA e ML** na nuvem da Zscaler de fevereiro de 2024 a dezembro de 2024. As principais descobertas a seguir são baseadas em dados abrangendo períodos de tempo variados* para análise comparativa.

O uso de ferramentas de IA/ML teve um aumento exponencial ano após ano, com 36x mais transações (+3.464,6%) de mais de 800 aplicativos de IA/ML na nuvem da Zscaler, destacando o crescimento explosivo do interesse empresarial e da dependência dessas tecnologias.

As empresas bloquearam 59,9% de todas transações de IA/ML, refletindo preocupações em torno da segurança de dados de IA e as medidas que as empresas estão tomando para moldar suas abordagens à governança de IA.

O ChatGPT continua sendo o principal aplicativo em volume de transações, respondendo por quase metade de todas as transações de IA/ML (45.2%) de aplicativos conhecidos, apesar dos debates em andamento sobre suas implicações de segurança.

O ChatGPT também é o aplicativo de IA mais bloqueado entre os aplicativos conhecidos, seguido pelo Grammarly, Microsoft Copilot, QuillBot e Wordtune, reforçando o crescente interesse e cautela quando se trata de assistentes de escrita e produtividade com tecnologia de IA em ambientes empresariais.

* Variações de período de tempo:

- As mudanças percentuais “ano a ano” comparam dados de abril a dezembro de 2024 e o mesmo período em 2023.
- As descobertas específicas por país e região são baseadas em dados coletados entre julho e dezembro de 2024.

A a Zscaler Zero Trust Exchange rastreia transações do ChatGPT independentemente de outras transações da OpenAI em geral.

©2025 Zscaler, Inc. Todos os direitos reservados.

As empresas estão enviando volumes significativos de dados para ferramentas de IA, com um total de 3.624 TB transferidos por aplicativos de IA/ML.

Os setores de finanças e seguros e de manufatura geram a maior parte do tráfego de IA/ML, com 28,4% e 21,6% de participação no total de transações de IA/ML na nuvem da Zscaler, respectivamente, seguidas pelos setores de serviços (18,5%), tecnologia (10,1%), saúde (9,6%) e governo (4,2%), mostrando que a adoção da IA varia significativamente entre os setores.

Os 5 principais países que mais geram transações de IA/ML são Estados Unidos, Índia, Reino Unido, Alemanha e Japão.

A IA continua a ampliar os riscos cibernéticos, impulsionada pelos avanços na tecnologia de deepfake, modelos emergentes de IA de código aberto e automação autônoma de ataques, tornando, sem dúvida, as ameaças mais adaptáveis, direcionadas e difíceis de detectar.



©2025 Zscaler, Inc. Todos os direitos reservados.

Tendências de uso de_ IA e ML

O uso de ferramentas de IA/ML aumentou globalmente em 2024, com empresas integrando IA em operações e funcionários incorporando-a em fluxos de trabalho diários. A Zscaler rastreou mais de 800 aplicativos de IA/ML na nuvem da Zscaler, um número consideravelmente maior em comparação ao período de análise anterior em 2023, refletindo a crescente adoção empresarial e a dependência de ferramentas baseadas em IA.

Visão geral das transações de IA/ML

Os crescentes riscos de segurança não desaceleraram o aumento exponencial nas transações de IA e ML. De fevereiro a dezembro de 2024, os volumes de transações aumentaram de 3,7 bilhões para 49 bilhões, um aumento de doze vezes. A atividade de IA/ML atingiu o pico em julho, alcançando 82,7 bilhões de transações.

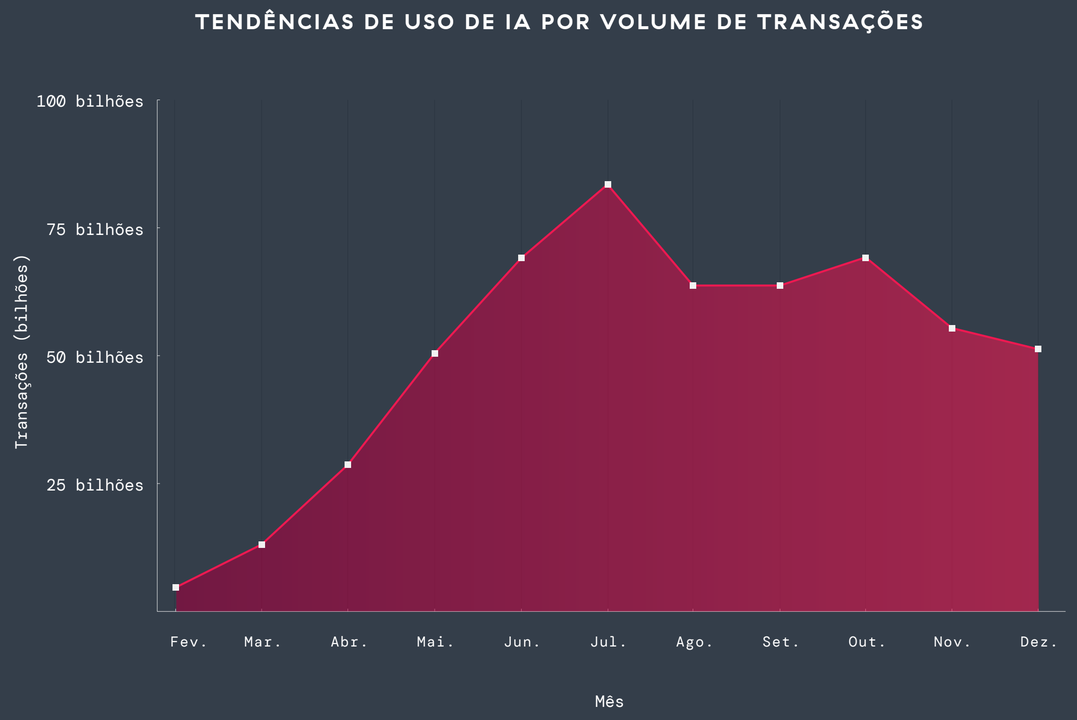


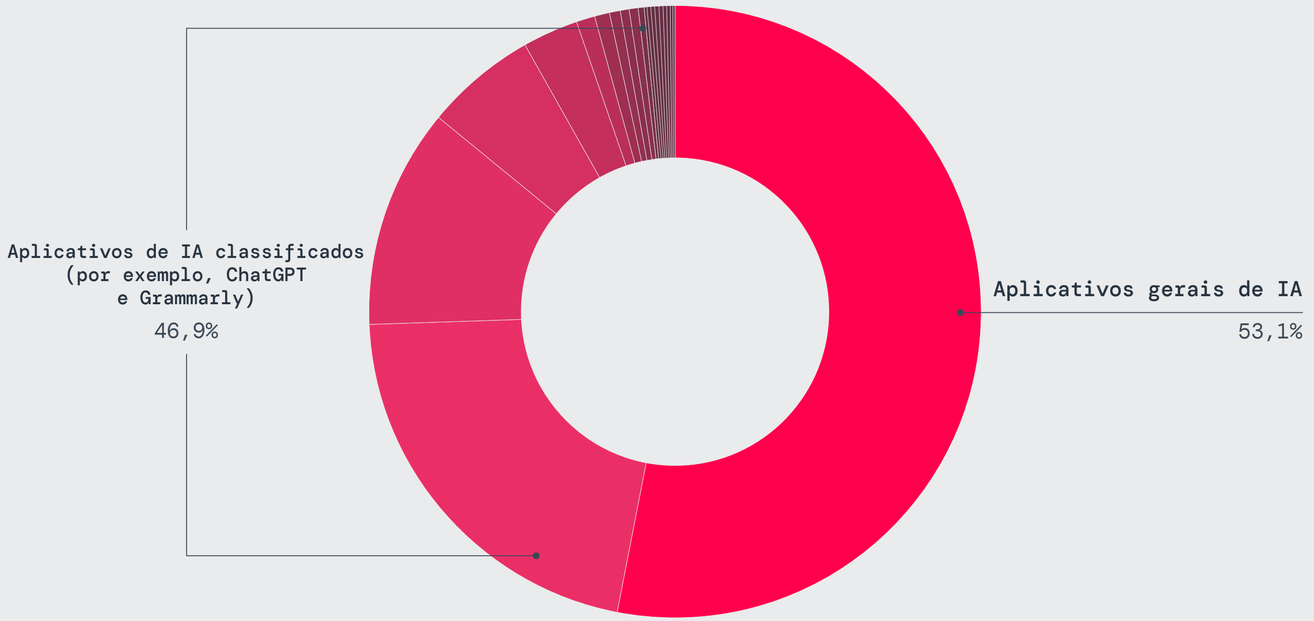
Figura 1: transações de IA de fevereiro de 2024 a dezembro de 2024

©2025 Zscaler, Inc. Todos os direitos reservados.

A escala de atividade de IA/ML aumentou dramaticamente para um total de 536,5 bilhões de transações de IA/ML, um aumento de 3.464,6% ano a ano em comparação ao nosso último período de análise. Uma parcela significativa desse tráfego de IA/ML vem de aplicativos amplamente utilizados, como ChatGPT, Grammarly, Microsoft Copilot e outras ferramentas de IA/ML. No entanto, uma grande parte das transações **(53,1%)** permanecem categorizados como “aplicativos gerais de IA” dentro da nuvem da Zscaler, ressaltando a rápida proliferação do uso da IA em empresas. Essa classificação reflete transações de IA/ML que ainda não pertencem a aplicativos de IA definidos, mas que, no entanto, são detectadas como tráfego de IA/ML por meio da categorização de URL baseada em IA/ML da Zscaler, que pode analisar textos, imagens e outros conteúdos para identificar atividades relacionadas à IA.

Para fornecer uma visão mais precisa e detalhada dos padrões de adoção de IA/ML entre empresas, a análise da ThreatLabz se concentra em aplicativos de IA/ML. Ao adotar essa abordagem, destacamos as tendências de adoção da IA por meio de aplicativos empresariais de IA/ML estabelecidos.

PARTICIPAÇÃO NO TOTAL DE TRANSAÇÕES



©2025 Zscaler, Inc. Todos os direitos reservados.

Entre aplicativos de IA/ML conhecidos, algumas ferramentas líderes de mercado geram a maioria das transações. As cinco principais ferramentas a seguir compartilham um foco comum em melhorar a produtividade, a comunicação e a automação.

- **O ChatGPT** representa quase metade das transações de IA e ML (45,2%), lembrando-nos de sua ampla adoção em todos os setores. Saiba mais na **seção de tendências de uso do ChatGPT.**
- **O Grammarly** ocupa o segundo lugar (24,8%), refletindo sua crescente popularidade entre usuários corporativos para refinar a escrita e a gramática.
- **O Microsoft Copilot** ocupa o terceiro lugar (12,5%), já que as empresas dependem dele para automatizar tarefas em aplicativos do Microsoft 365, como Word, Excel e Outlook.
- **O DeepL**, uma ferramenta de tradução líder com tecnologia de IA, segue (6,4%) à medida que ganhou força entre empresas globais que buscam comunicação multilíngue de alta qualidade.
- **O QuillBot** completa os cinco primeiros (2,0%) como outro assistente de escrita que oferece paráfrases e resumos.

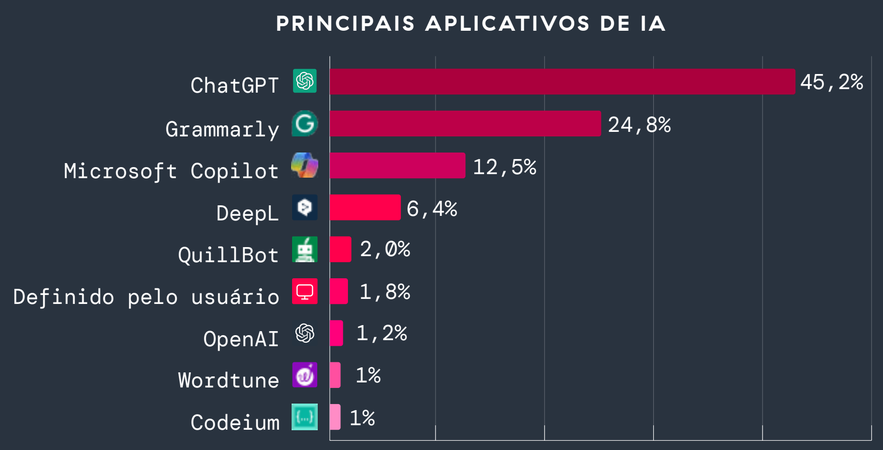


Figura 2: principais aplicativos de IA por volume de transações

20 PRINCIPAIS APLICATIVOS DE IA/ML POR VOLUME DE TRANSAÇÕES

Aplicativos	Total de transações
ChatGPT	113.869.583.355
Grammarly	62.490.051.574
Microsoft Copilot	31.551.774.637
DeepL	16.012.344.908
QuillBot	5.130.879.211
Aplicativos personalizados	4.297.439.333
OpenAI	2.995.303.521
Wordtune	2.552.030.384
Codeium	2.439.268.698
Perplexity	1.806.093.093
Loom	662.917.153
Zineone	571.034.336
Synthesia	570.918.959
Writer	512.811.065
Poe	433.139.217
Claude	379.841.841
Google Gemini	317.583.902
Otter.ai	310.594.881
Runway	256.927.467
Yellow Messenger	245.412.258

©2025 Zscaler, Inc. Todos os direitos reservados.

Principais categorias de aplicativos

1. Assistentes de produtividade (60,4%)

Exemplos: ChatGPT, Microsoft Copilot, Perplexity

Quase dois terços das transações de IA/ML na nuvem da Zscaler se enquadram na categoria de assistentes com tecnologia de IA. Esses aplicativos abrangem uma ampla gama de casos de uso, desde interfaces de bate-papo e ferramentas de pesquisa orientadas por IA até automação de fluxo de trabalho e integração empresarial, todos compartilhando o objetivo comum de aumentar a produtividade empresarial.

2. Escrita e geração de conteúdo (28,3%)

Exemplos: Grammarly, Quillbot, Wordtune

A segunda maior fatia de atividade de aplicativos de IA/ML vem da categoria de escrita e geração de conteúdo. As ferramentas de escrita com tecnologia de IA rapidamente se tornaram parte integrante do conteúdo e das comunicações empresariais, simplificando tarefas como edição, melhoria da clareza e outros refinamentos gramaticais.

Da produtividade à dificuldade: conheça os riscos

O papel dominante da IA na produtividade e escrita empresarial apresenta riscos significativos, incluindo vazamentos de dados, ataques de injeção de prompts, violações de conformidade, alucinações de IA, exposição de IP, preocupações com privacidade e possível excesso de dependência. Saiba como mitigar esses riscos e adotar a IA com segurança na seção Práticas recomendadas para a adoção segura da IA em empresas.

3. Idiomas e tradução (5,8%)

Exemplos: DeepL, LanguageTool

As ferramentas de tradução e idiomas com tecnologia de IA são responsáveis por 14,6 bilhões de transações. Essas soluções estão simplificando as comunicações empresariais globais, permitindo a criação de conteúdo multilíngue mais rápida e escalável, embora ainda persistam preocupações em relação à precisão e privacidade de dados.

4. Aplicativos personalizados (1,7%)

À medida que as organizações buscam vantagens competitivas impulsionadas pela IA, os aplicativos de IA personalizados são responsáveis por mais de 4 bilhões de transações. As empresas estão aproveitando soluções de IA personalizadas para casos de uso que abrangem análise preditiva, detecção de fraudes, automação e outros.

5. Assistentes de código (1,3%)

Exemplos: Codeium, Claude

Os assistentes de código com tecnologia de IA estão se tornando mais comuns no desenvolvimento de software, impulsionando mais de 3 bilhões de transações. Eles ajudam os desenvolvedores a trabalhar mais rápido, mas as empresas devem estar cientes dos riscos, desde problemas de qualidade até questões de propriedade intelectual.

6. Ferramentas visuais e criativas (1,1%)

Exemplos: Loom, Synthesia

O papel da IA como parceira criativa está se expandindo, com as ferramentas visuais e criativas de IA gerando 2,7 bilhões de transações. As ferramentas de criação de vídeo lideram a categoria, permitindo que organizações expandam esforços de produção de conteúdo de vídeo e saída de conteúdo.

©2025 Zscaler, Inc. Todos os direitos reservados.

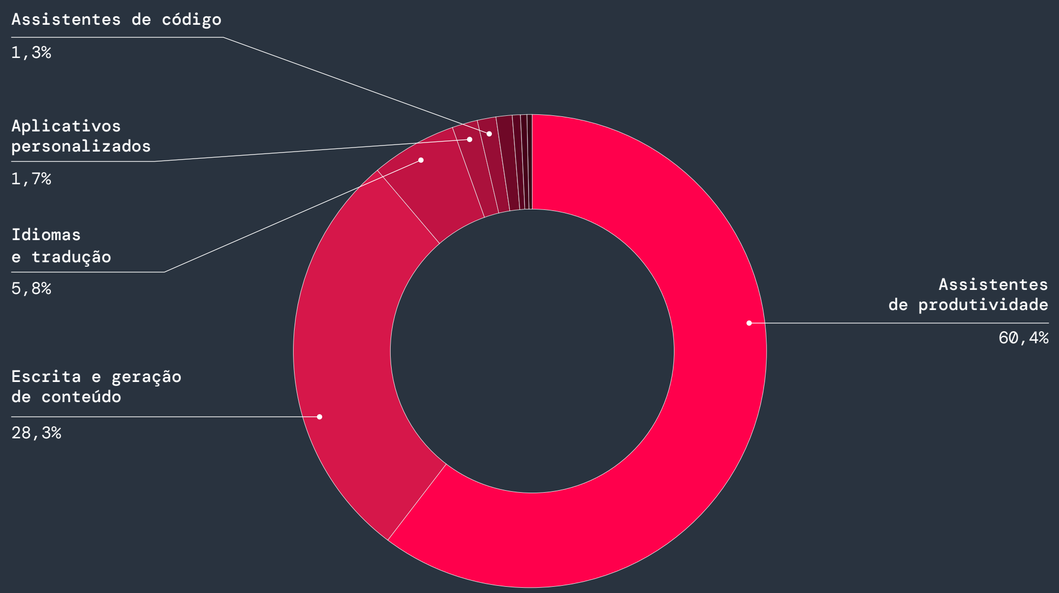


Figura 3: transações por categoria de aplicativo

TRANSAÇÕES POR CATEGORIA DE APLICATIVO

Categoria	Transações
Assistentes de produtividade	70.916.692.869
Escrita e geração de conteúdo	14.638.307.672
Idiomas e tradução	31.551.774.637
Aplicativos personalizados	4.354.146.062
Assistentes de código	3.205.630.565
Ferramentas visuais/criativas	4.297.439.333
Análise e automação de dados	2.723.874.910
Suporte ao cliente e chatbots	1.172.151.320
Transcrição	354.967.757
Motores de busca	297.174.973
Ferramentas de fala e áudio	191.295.786

©2025 Zscaler, Inc. Todos os direitos reservados.

Os volumes de transações por si só não contam a história completa do uso empresarial da IA. A ThreatLabz também analisou a quantidade de dados transferidos entre empresas e ferramentas de IA, totalizando 3.624 terabytes (TB). Por essa medida, o ChatGPT continua sendo o principal aplicativo, com 1.481 TB de dados transferidos. O grande volume de dados mostra que as empresas não estão usando o ChatGPT apenas com frequência, mas em grande escala.

Seguindo o ChatGPT em volume de transferência de dados, Grammarly, OpenAI e Microsoft Copilot têm uma classificação alta, ressaltando seu papel no refinamento de conteúdo e treinamento de modelos com tecnologia de IA.

Outras ferramentas notáveis que contribuem com volumes significativos de transferência de dados incluem DeepL, Synthesia e Wordtune, cada uma delas atendendo a diversas necessidades empresariais, desde melhorias de produtividade até mensagens de vídeo orientadas por IA.

Ficar de olho no volume de transações e nas tendências de transferência de dados será essencial para integrar a IA de forma eficaz e, ao mesmo tempo, ficar à frente de riscos potenciais.

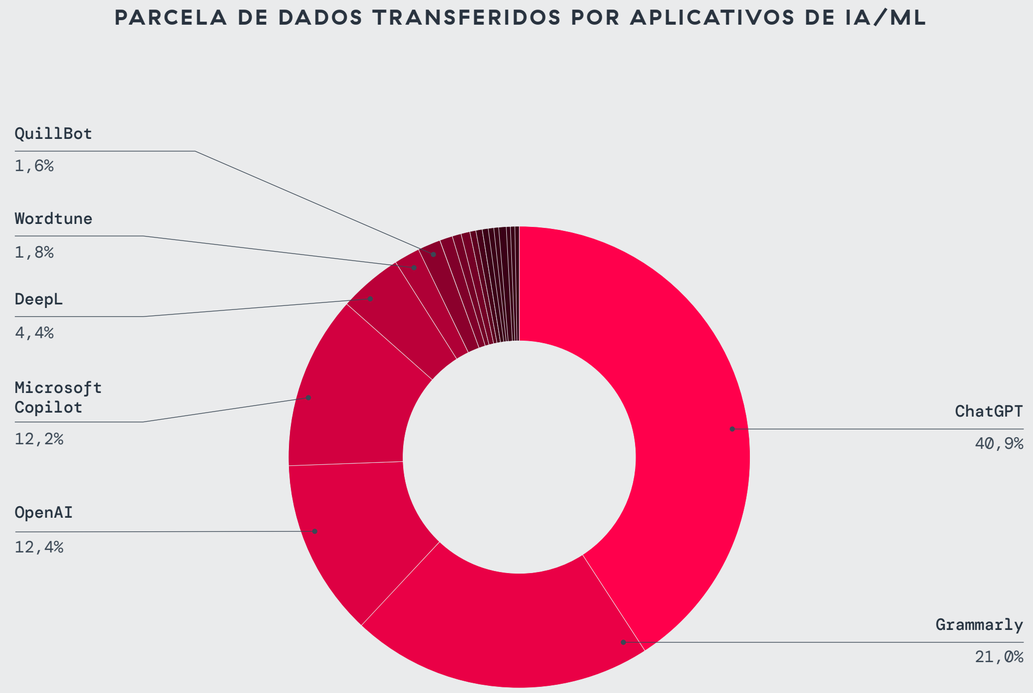


Figura 4: principais aplicativos de IA/ML pela porcentagem do total de dados transferidos

©2025 Zscaler, Inc. Todos os direitos reservados.

Transações de IA/ML bloqueadas

O crescimento da IA empresarial também está encontrando resistência à medida que as organizações fortalecem os controles para mitigar os riscos de segurança de dados, privacidade e conformidade. Atualmente, as empresas bloqueiam 59,9% de todas as transações de IA/ML na nuvem da Zscaler, totalizando mais de 321,9 bilhões de transações bloqueadas entre fevereiro e dezembro de 2024.

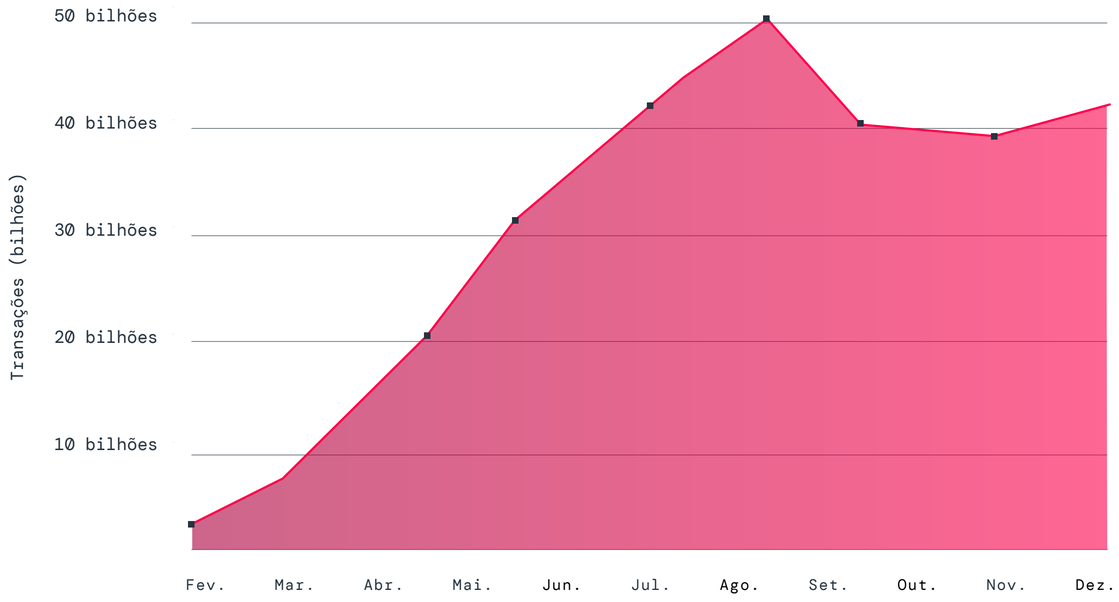


Figura 5: número de transações de IA/ML bloqueadas entre fevereiro e dezembro de 2024

Curiosamente, as ferramentas de IA mais utilizadas também são as mais frequentemente bloqueadas, começando pelo ChatGPT. O chatbot de GenAI continua sendo o foco principal das medidas de segurança para evitar perda de dados, respondendo por 54% do total de bloqueios.

Adobe.io, a plataforma de desenvolvimento baseada na nuvem da Adobe que fornece APIs e ferramentas de automação com tecnologia de IA para produtos da Adobe, representa 68% de todas as transações de domínio de IA e ML bloqueadas. Essa tendência sinaliza um esforço proativo das empresas para impedir transferências não autorizadas de dados e proteger conteúdo proprietário.

As empresas estão caminhando em uma corda bamba cada vez mais estreita entre a inovação em IA e a segurança. À medida que a adoção da IA continua crescendo, as organizações terão que controlar melhor os riscos e, ao mesmo tempo, aproveitar o poder da IA/ML para permanecerem competitivas.

Principais aplicativos de IA bloqueados	Principais domínios de IA bloqueados
1.ChatGPT	adobe.io
2.Grammarly	chatgpt.com
3.Microsoft Copilot	grammarly.com
4.QuillBot	microsoft.com
5.Wordtune	Quillbot.com
6.Codeium	deepl.com
7.DeepL	Openai.com
8.Drift	Bing.com
9.Poe	Wordtune.com
10.Securiti	Codeium.com

©2025 Zscaler, Inc. Todos os direitos reservados.

Perda de dados para aplicativos de IA/ML

À medida que as atividades de IA/ML aumentam na empresa, também aumentam os riscos de exposição de dados. Assistentes de produtividade e chatbots com tecnologia de IA, assistentes de código e analisadores de documentos podem expor inadvertidamente dados empresariais sigilosos. Esse desafio é agravado pelos usuários que, sem saber, compartilham informações sigilosas com modelos de IA que não possuem controles de segurança de nível empresarial.

Diversas ferramentas de IA/ML foram sinalizadas por violações de prevenção contra perda de dados (DLP) na nuvem da Zscaler. Essas violações representam instâncias em que dados empresariais sigilosos, como dados financeiros, PII, código-fonte e dados médicos, deveriam ser enviados a um aplicativo de IA, e essa transação foi bloqueada pela política da Zscaler. Ocorreria perda de dados nesses aplicativos de IA sem a aplicação de DLP da Zscaler. Como resultado, as violações servem como um indicador-chave das tendências reais de perda de dados da IA.

APLICATIVOS DE IA/ML COM MAIS VIOLAÇÕES DE POLÍTICA DE DLP

Aplicativos	Violações de DLP
ChatGPT	2.915.502
Wordtune	879.131
Microsoft Copilot	257.869
DeepL	68.916
Codeium	41.041
Claude	40.993
Synthesia	22.975
Grammarly	7.157
DataRobot	5.440
QuillBot	4.649
Google Gemini	4.227
You.com	2.341
Perplexity	2.129
DeepAI	1,472
Poe	1.399

Essas ferramentas compartilham um perfil de risco comum devido ao seu processamento baseado na nuvem e uso em fluxos de trabalho de produtividade, onde geralmente lidam com dados empresariais sigilosos. As violações destacam a crescente necessidade de controles de DLP com reconhecimento de IA para garantir que as organizações possam adotar a IA com segurança e, ao mesmo tempo, evitar vazamentos de dados.

Uma análise mais detalhada das violações de DLP mais comuns relacionadas à IA revela que informações de identificação pessoal (PII), código-fonte proprietário e dados relacionados à assistência médica correm risco de exposição.

AS 10 PRINCIPAIS VIOLAÇÕES DE DLP DA IA

1	Número de segurança social
2	Vazamento de nome (EUA)
3	Conteúdo adulto
4	Conteúdo de automutilação e cyberbullying
5	Código-fonte
6	Vazamento de doenças
7	Informações médicas
8	Vazamento de nome (Canadá)
9	Cadastro de pessoa física do Brasil
10	Vazamento de medicamentos

A análise das violações de DLP vinculadas ao ChatGPT e ao Microsoft Copilot, duas das ferramentas empresariais de IA mais amplamente utilizadas e principais infratores de violações de DLP, revela exposição frequente de PII, dados relacionados à saúde e código-fonte.

Violações de DLP do ChatGPT	Violações de DLP do Microsoft Copilot
SSN, vazamento de nome (EUA), vazamento de doenças, vazamento de nome (Canadá), cadastro de pessoa física do Brasil	SSN, vazamento de medicamentos, vazamento de doenças, vazamento de tratamentos, financeiro, código-fonte

Para insights mais profundos sobre os padrões de uso do ChatGPT, **confira a seção de tendências de uso do ChatGPT**. Para saber mais sobre como mitigar a perda de dados de aplicativos **de GenAI, leia 5 etapas para integrar ferramentas de GenAI com segurança** abaixo.

©2025 Zscaler, Inc. Todos os direitos reservados.

Uso da IA por setor

A adoção empresarial de ferramentas de IA e ML varia amplamente de acordo com o setor, com **finanças e seguros** liderando, gerando **28,4%** das transações de IA/ML. À medida que os serviços financeiros continuam a adotar eficiências orientadas por IA para funções críticas como detecção de fraudes, automação de atendimento ao cliente e avaliações de risco, seu volume de transações de IA ultrapassou o da **manufatura,** que agora ocupa o segundo lugar com **21,6%** do total de transações de IA/ML.

Os setores de **serviços (18,5%), tecnologia (10,1%)** e **saúde (9,6%)** seguem, cada um adotando a IA em velocidades diferentes com base em suas prioridades operacionais individuais. Enquanto o setor de serviços provavelmente está aumentando o uso de IA em termos de suporte ao cliente e otimizações operacionais, as empresas de tecnologia continuam a promover a pesquisa e a inovação em IA. A adoção da saúde continua menor em comparação, refletindo uma postura mais reservada devido a maiores preocupações regulatórias e de segurança.

PARTICIPAÇÃO DE TRANSAÇÕES DE IA POR SETOR VERTICAL

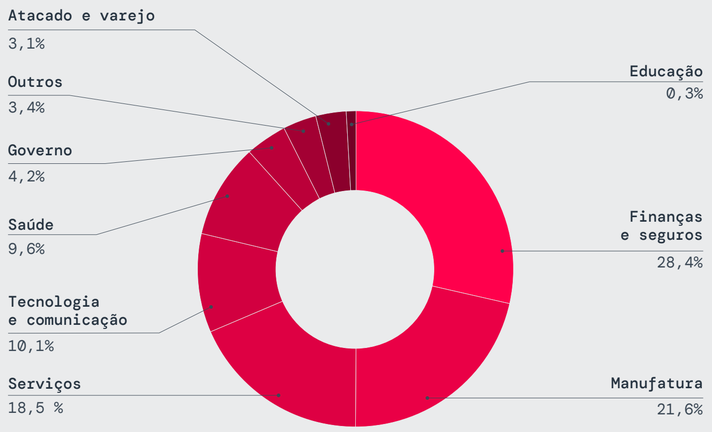


Figura 6: setores que promovem as maiores proporções de transações de IA

TENDÊNCIAS DE TRANSAÇÕES DE IA POR VERTICAL

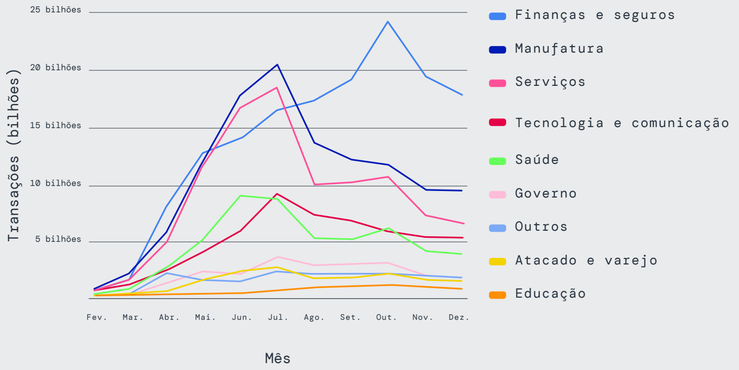


Figura 7: tendências de transações de IA/ML entre os setores de maior volume

Os setores também estão intensificando os esforços para proteger transações de IA/ML, mas o volume de atividades de IA/ML bloqueadas varia. O setore de finanças e seguros bloqueia 39,5% das transações de IA. Essa tendência se alinha ao rigoroso cenário de conformidade do setor e à necessidade de proteger dados financeiros e pessoais.

O setor de manufatura bloqueia 19,2% das transações de IA, sugerindo uma abordagem estratégica em que a IA é amplamente utilizada, mas monitorada de perto quanto a riscos de segurança, enquanto o setor de serviços adota uma abordagem mais equilibrada, bloqueando 15% das transações de IA. Por outro lado, o setor de saúde bloqueia apenas 10,8% das transações de IA. Apesar de lidar com grandes quantidades de dados de saúde e PII, as organizações de saúde ainda estão atrasadas na proteção de ferramentas de IA, com equipes de segurança tentando acompanhar a rápida inovação. Essa tendência destaca o atraso de medidas de proteção, mantendo as transações em geral de IA na área da saúde relativamente baixas em comparação a outros setores.

PARTICIPAÇÃO DE TRANSAÇÕES DE IA BLOQUEADAS POR VERTICAL

Vertical	% de transações de IA bloqueadas
Finanças e seguros	39,5%
Manufatura	19,2%
Serviços	15,0%
Saúde	10,8%
Tecnologia e comunicação	6,9%
Governo	4,5%
Outros	2,2%
Atacado e varejo	1,6%
Educação	0,3%

©2025 Zscaler, Inc. Todos os direitos reservados.

Destaques dos setores

O setor de finanças e seguros dobra o investimento em IA

OS CINCO PRINCIPAIS APLICATIVOS DE IA EM FINANÇAS E SEGUROS

1	2	3	4	5
ChatGPT	Microsoft Copilot	Grammarly	Aplicativos definidos pelos usuários	DeepL

Como o principal condutor de transações de IA/ML na nuvem Zscaler (152,4 bilhões), o setor de finanças e seguros está profundamente investido no potencial da IA. Esses setores contam com a IA para analisar transações financeiras em tempo real, detectar atividades fraudulentas e acelerar o processamento de reivindicações, para citar algumas tarefas críticas que os ajudam a economizar tempo e dinheiro.

Além da automação, a IA generativa está remodelando as operações financeiras. Ferramentas como ChatGPT e Microsoft Copilot, que estão entre os aplicativos mais utilizados pelo setor financeiro e de seguros na nuvem da Zscaler, ajudam instituições financeiras a resumir relatórios, automatizar fluxos de trabalho e auxiliar com tarefas de conformidade. Os aplicativos de IA personalizados também estão entre os cinco principais para organizações de serviços financeiros, ressaltando um profundo investimento em soluções baseadas em IA. Enquanto isso, o alto volume de transações do DeepL sugere uma necessidade crescente de tradução com tecnologia de IA nas finanças globais.

À medida que as organizações de finanças e seguros integram cada vez mais a IA, elas enfrentam desafios crescentes relacionados à segurança, conformidade regulatória e questões éticas, incluindo privacidade de dados, viés e precisão. Os bots com tecnologia de IA agora são responsáveis por uma parcela significativa das transações bloqueadas, explorando APIs e fluxos de trabalho de autenticação para contornar os controles de segurança.

Para combater essas ameaças, as organizações estão adotando cada vez mais modelos de segurança baseados em IA para detecção de anomalias comportamentais e autenticação adaptável baseada em risco. No entanto, as técnicas de IA adversárias continuam a evoluir, exigindo monitoramento contínuo e estratégias avançadas de zero trust para mitigar riscos emergentes.

Ao priorizar a supervisão e o uso ético da IA, as instituições financeiras podem proteger a integridade dos dados, garantir a imparcialidade e manter a confiança pública nos setores bancário, de seguros e outros setores financeiros.



©2025 Zscaler, Inc. Todos os direitos reservados.



O setor de manufatura aproveita o poder da IA

OS CINCO PRINCIPAIS APLICATIVOS DE IA NA MANUFATURA

1	2	3	4	5
ChatGPT	Grammarly	Microsoft Copilot	DeepL	QuillBot

A segunda maior fatia de tráfego de IA/ML (21,6%) em nossa pesquisa vem de clientes de manufatura. A adoção da IA nesse setor é um dos principais promotores da quarta revolução industrial, a Indústria 4.0, que está redefinindo a manufatura com fábricas inteligentes, dispositivos conectados à IoT e manutenção preditiva.

Os fabricantes estão cada vez mais aproveitando a IA para aprimorar as operações, desde a previsão de falhas de equipamentos por meio da análise de dados abrangentes de máquinas e sensores até a simplificação do gerenciamento da cadeia de suprimentos, controle de estoque e logística. Além disso, os sistemas de robótica e automação com tecnologia de IA estão aumentando significativamente a eficiência da fabricação, executando tarefas com maior velocidade e precisão do que os trabalhadores humanos, reduzindo assim custos e minimizando erros.

No entanto, a segurança dos dados continua a ser uma preocupação, uma vez que a manufatura é responsável por 19,2% do tráfego de IA/ML bloqueado, indicando uma abordagem cautelosa à adoção da IA. Essa cautela decorre de preocupações com a segurança dos dados e da necessidade de avaliar e aprovar cuidadosamente os aplicativos de IA, ao mesmo tempo em que restringe aqueles que apresentam riscos mais elevados. Por exemplo, os fabricantes de eletrônicos podem implementar protocolos rigorosos para garantir que apenas aplicativos de IA que atendam a padrões de segurança rigorosos sejam integrados em suas operações, mitigando possíveis vulnerabilidades.

©2025 Zscaler, Inc. Todos os direitos reservados.

O setor de saúde vê aumento na atividade de IA

OS CINCO PRINCIPAIS APLICATIVOS DE IA NA ÁREA DA SAÚDE

1	2	3	4	5
ChatGPT	Grammarly	Microsoft Copilot	DeepL	QuillBot

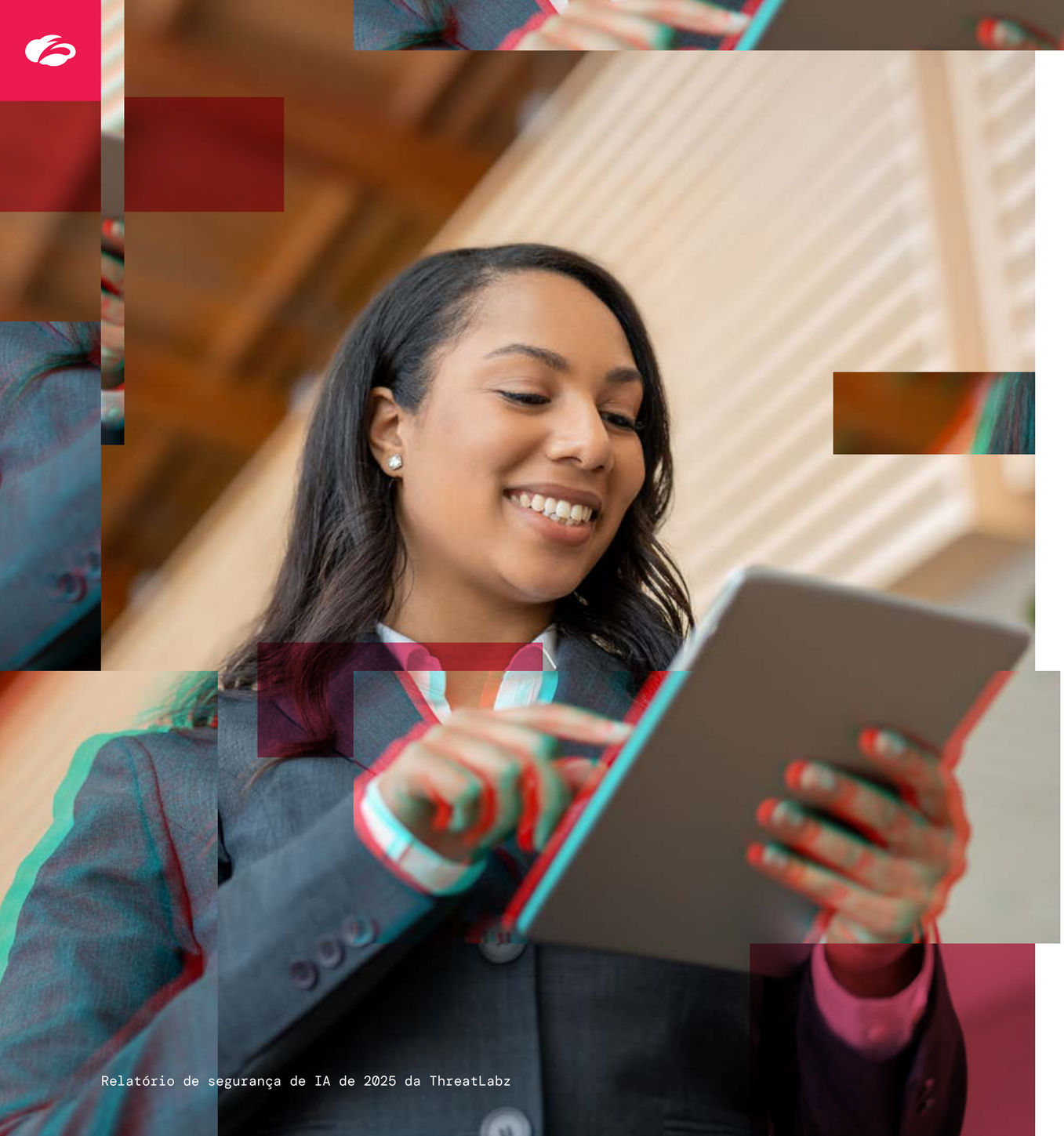
O setor de saúde ocupa o quinto lugar no uso de IA/ML na nuvem da Zscaler, respondendo por 9,6% do tráfego, um aumento de 4,1% em relação ao ano passado. No entanto, neste ano, o setor de saúde bloqueou apenas 10,8% de todas as transações de IA, uma queda significativa em relação aos 17,23% em 2024. Vários fatores contribuem para essa mudança.

A integração rápida de ferramentas de IA/ML levou a um aumento nas atividades relacionadas à IA. Aplicativos como o ChatGPT, o aplicativo de IA/ML mais utilizado por organizações de saúde na nuvem da Zscaler, auxilia profissionais de saúde com suporte de diagnóstico, resumos de pesquisas médicas e documentação de pacientes. No entanto, o aumento da atividade de IA/ML provavelmente torna difícil distinguir entre transações de IA legítimas e maliciosas, resultando potencialmente em menos bloqueios. À medida que as organizações de saúde se tornam mais dependentes da IA para o atendimento aos pacientes e tarefas administrativas, há uma ênfase crescente na habilitação de funcionalidades de IA.

A IA/ML na área da saúde oferece avanços significativos, mas também apresenta riscos notáveis. Uma grande preocupação é a privacidade dos dados; os sistemas de IA geralmente exigem dados extensos dos pacientes, levantando questões sobre a segurança e a confidencialidade de informações sigilosas. Adicionalmente, o conteúdo gerado por IA pode, às vezes, conter imprecisões ou levar a possíveis erros de diagnóstico ou tratamento. Além disso, a sofisticação crescente dos ataques cibernéticos baseados em IA, como campanhas de phishing geradas por IA, representa desafios de segurança maiores. Portanto, embora as tecnologias de IA/ML possam melhorar o setor de saúde e, em última análise, o atendimento a pacientes, é fundamental implementar medidas de segurança robustas e manter a supervisão humana para mitigar esses riscos.



©2025 Zscaler, Inc. Todos os direitos reservados.



Governos reconhecem potencial na IA

OS CINCO PRINCIPAIS APLICATIVOS DE IA NO GOVERNO

1	2	3	4	5
Grammarly	Microsoft Copilot	ChatGPT	QuillBot	DeepL

O uso governamental de IA/ML aumentou para 4,2% este ano, impulsionado pela busca por melhor prestação de serviços e formulação de políticas eficientes. Esse aumento provavelmente pode ser atribuído ao potencial da IA de otimizar operações, melhorar o engajamento dos cidadãos e informar decisões baseadas em dados.

Entre os aplicativos de IA rastreados na nuvem da Zscaler, o Grammarly é a ferramenta mais usada por entidades governamentais, sugerindo um foco na melhoria das comunicações entre governo e cidadão. O uso do Microsoft Copilot, a segunda ferramenta de IA mais usada pelo setor governamental, demonstra ainda mais o interesse na automação com tecnologia de IA para benefícios como eficiência administrativa.

No entanto, essa rápida integração exige medidas de segurança robustas para mitigar os riscos associados. A privacidade dos dados é uma preocupação primordial, pois os sistemas de IA geralmente exigem amplo acesso a informações sigilosas, aumentando o potencial de violações. Vulnerabilidades de segurança são outro problema crítico; os sistemas de IA podem se tornar alvos de ataques cibernéticos sofisticados que visam extrair dados sigilosos. Além disso, o viés algorítmico pode levar a resultados injustos ou discriminatórios, minando a confiança pública. Para mitigar esses riscos, é essencial implementar medidas de segurança robustas, estabelecer estruturas de governança claras e manter a supervisão humana durante todo o ciclo de vida.

©2025 Zscaler, Inc. Todos os direitos reservados.

Tendências de uso do ChatGPT

O ChatGPT atingiu sua marca de dois anos em 2024, e sua adoção empresarial e popularidade global não mostram sinais de diminuição. Com o lançamento de recursos de memória e pesquisa na web em tempo real, o ChatGPT está mais inteligente, rápido e útil do que nunca, gerando uma adoção ainda maior. Somente no primeiro semestre do ano, as transações globais do ChatGPT na nuvem da Zscaler totalizaram 90,7 bilhões, consolidando seu lugar como a ferramenta de IA generativa mais utilizada.

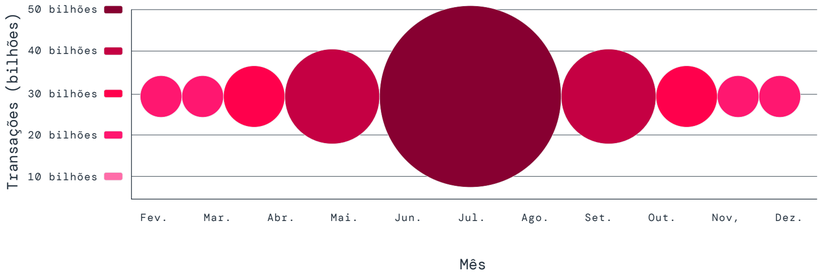


Figura 8: transações do ChatGPT de fevereiro a dezembro de 2024

No entanto, a adoção do ChatGPT pelos setores não reflete exatamente a tendência geral de uso de IA/ML; ele tem um caso atípico notável. Embora o setor de finanças e seguros tenha gerado o maior volume de transações gerais de IA/ML, ele representam apenas 11,4% do uso do ChatGPT. Essa menor taxa de adoção provavelmente reflete preocupações mais rigorosas com segurança, conformidade e privacidade de dados, o que limita o modo como a IA generativa é usada em ambientes regulamentados.

A manufatura, que ocupa o segundo lugar no total de transações de IA, promove o maior volume de transações do ChatGPT. Isso sugere que os fabricantes estão aproveitando a IA generativa para tudo, desde documentação técnica até fluxos de trabalho automatizados. Logo atrás, os setores de serviços, saúde e tecnologia também fazem uso intenso do ChatGPT.

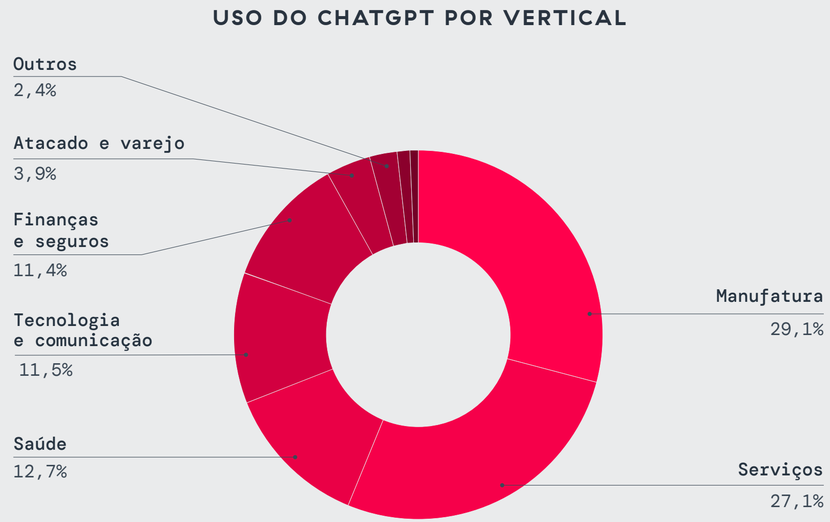


Figura 9: setores que promovem as maiores proporções de transações do ChatGPT

DO CHATGPT AO DEEPSEEK: A EVOLUÇÃO DOS CHATBOTS DE IA

Os principais modelos de IA, como ChatGPT (OpenAI) e Claude (Anthropic), dominam o cenário de chatbots, representando uma grande porcentagem das transações de IA/ML na nuvem da Zscaler. Esses aplicativos são amplamente utilizados em ambientes empresariais para criação de conteúdo, assistência de código, análise de dados e automação de fluxo de trabalho.

Embora os modelos tradicionais imponham medidas de segurança até certo ponto, as alternativas de código aberto introduzem novos riscos; e é aí que entra o DeepSeek.

O DeepSeek é a resposta chinesa ao ChatGPT. No entanto, diferentemente do ChatGPT, que possui restrições de segurança integradas, o DeepSeek permite acesso irrestrito, o que o torna uma ferramenta poderosa, mas de risco. Sua natureza de código aberto levanta preocupações sobre segurança e soberania de dados, e a falta de controles de segurança significa que empresas e usuários finais precisam avaliar cuidadosamente os riscos antes de usar o DeepSeek. Da mesma forma, o Grok, desenvolvido pela xAI, adota uma abordagem mais flexível às interações de IA, oferecendo menos restrições em comparação aos modelos tradicionais.

Leia mais sobre o surgimento do DeepSeek e seus riscos na seção deste relatório sobre DeepSeek e IA de código aberto.

©2025 Zscaler, Inc. Todos os direitos reservados.

Uso de IA por país

O uso da IA está acelerando globalmente, com nações aumentando os investimentos para promover a inovação e permanecer competitivas. Os Estados Unidos e a Índia dominam em número de transações de IA/ML na nuvem da Zscaler, refletindo fortes compromissos com pesquisa, infraestrutura e até mesmo startups orientadas por IA.

Os **Estados Unidos (46,2%)** impulsionaram a maioria das transações enquanto **a Índia (8,7%)** surgiu como o segundo maior contribuidor.

O ambiente regulatório relativamente flexível dos Estados Unidos (ver **O âmbito evolutivo dos regulamentos de IA**), que promove a experimentação e a implantação da IA, pode dar às empresas dos EUA uma vantagem fundamental. Ao contrário de regiões com leis de IA mais rígidas, os EUA oferecem maior flexibilidade para desenvolver e integrar tecnologias de IA. Isso se reflete em um investimento relatado de US$ 13,8 bilhões em aplicativos de IA empresarial por corporações em 2024, um aumento de seis vezes em relação ao ano anterior.

A Índia continua a estabelecer-se como um interveniente importante na corrida da IA, com investimentos em setores-chave, incluindo serviços de finanças e seguros, saúde, manufatura e governo. Com fortes investimentos governamentais, como a Estratégia Nacional de IA[1] e o crescente investimento do setor privado, a Índia está alavancando a IA para aprimorar a automação, a análise e a segurança cibernética. No entanto, os desafios persistem; preocupações com privacidade de dados, incerteza regulatória e escassez de talentos em IA, que dificultam a adoção generalizada.

Apesar dos rápidos avanços, os países enfrentam barreiras à adoção da IA. Leis rígidas de privacidade de dados, como o GDPR, introduzem desafios de conformidade, enquanto o alto custo da implementação da IA e a escassez de talentos qualificados criam obstáculos à adoção, especialmente em mercados emergentes. Preocupações com a segurança, como ameaças cibernéticas impulsionadas por IA, viés algorítmico e outros, complicam ainda mais a adoção e o uso. À medida que países e governos navegam por esses desafios, uma abordagem estratégica que busca combinar clareza regulatória, investimento em educação em IA e estruturas robustas de segurança cibernética será crítica para a adoção global de IA em larga escala.

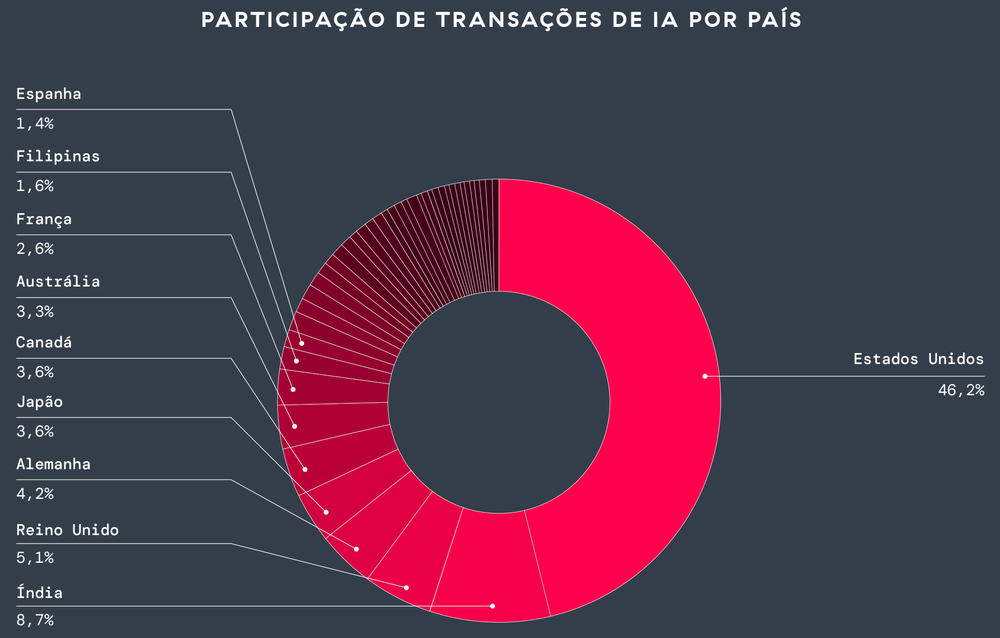


Figura 10: países com as maiores proporções de transações de IA

[1] Niti Aayog, Estratégia Nacional para Inteligência Artificial, acessado em 28 de fevereiro de 2025.

©2025 Zscaler, Inc. Todos os direitos reservados.

Insights da EMEA

Um olhar mais atento à região da Europa, Oriente Médio e África (EMEA) revela que a maior quantidade de transações de IA provém do Reino Unido (22,3%), Alemanha (18,4%), e França (11,3%). Embora o Reino Unido seja responsável por apenas 5,1% das transações de IA a nível mundial, ele representa mais de 20% do tráfego de IA na EMEA, tornando-o líder na região.

A Alemanha viu um aumento no número de transações de IA ano após ano (+5,74%), com mais empresas investindo em tecnologias de IA. Esse aumento é evidente nos setores de manufatura e serviços, que é impulsionado pela necessidade de automação e eficiência. A França também vem se posicionando como uma concorrente global de IA, com 109 bilhões de euros em investimento privado pelo presidente Emmanuel Macron em fevereiro de 2025.[2]

DIVISÃO POR PAÍS DA EMEA

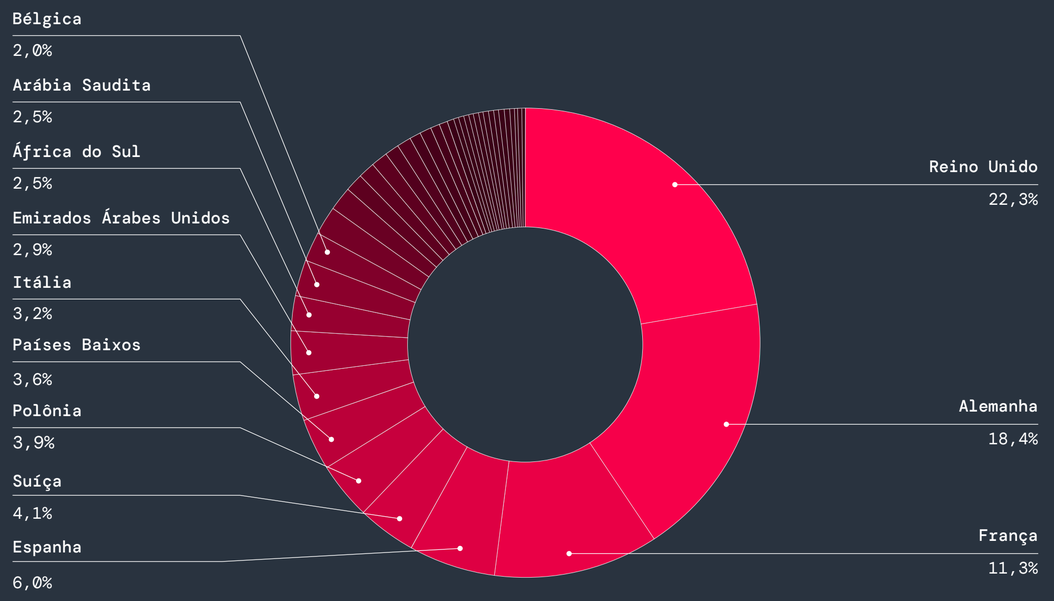


Figura 11: participação nas transações de IA por país na região da EMEA

TRANSAÇÕES DA EMEA POR MÊS

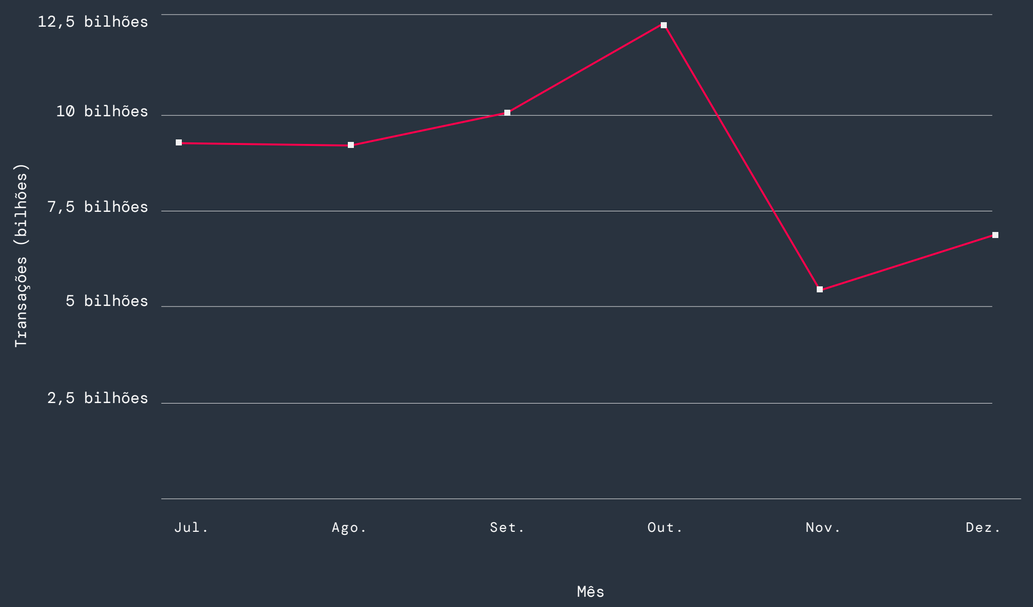


Figura 12: transações de IA de julho a dezembro de 2024 na região da EMEA

[2] CNBC, França revela investimento de 109 bilhões de euros em IA enquanto a Europa tenta acompanhar os EUA., 10 de fevereiro de 2025.

©2025 Zscaler, Inc. Todos os direitos reservados.

Insights da APAC

Analisando mais profundamente a região da Ásia–Pacífico (APAC), a ThreatLabz observou que as maiores parcelas de transações de IA vêm da Índia (36,4%), Japão (15,2%), e Austrália (13,6%).

Embora o Japão tenha visto um aumento ano a ano nas transações de IA (+5,7%), o país adotou uma abordagem mais cautelosa em relação às tecnologias de IA. O uso diário de IA permanece relativamente baixo devido a fatores culturais[3] e ambientes regulatórios rigorosos. A Austrália está desenvolvendo estruturas mais ativamente para garantir o uso responsável da IA, com um aumento de 3,6% nas transações de IA ano a ano. As Filipinas também estão vivenciando uma adoção acelerada da IA, com um crescimento previsto no setor de IA a uma taxa anual de 41,5% entre 2025 e 2030.[4] No entanto, essa mudança gera preocupações sobre o deslocamento de empregos, pois a qualificação dos trabalhadores e intervenções políticas estratégicas são necessárias para equilibrar o avanço tecnológico com a estabilidade de empregos.[5]

DIVISÃO POR PAÍS DA APAC

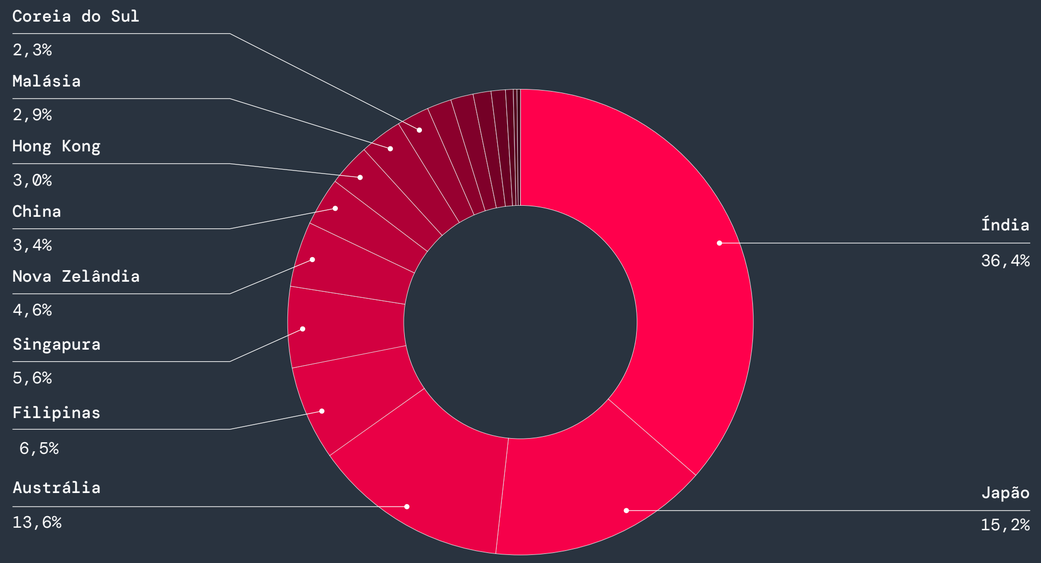


Figura 13: participação de transações de IA por país na região da APAC

TRANSAÇÕES DA APAC POR MÊS

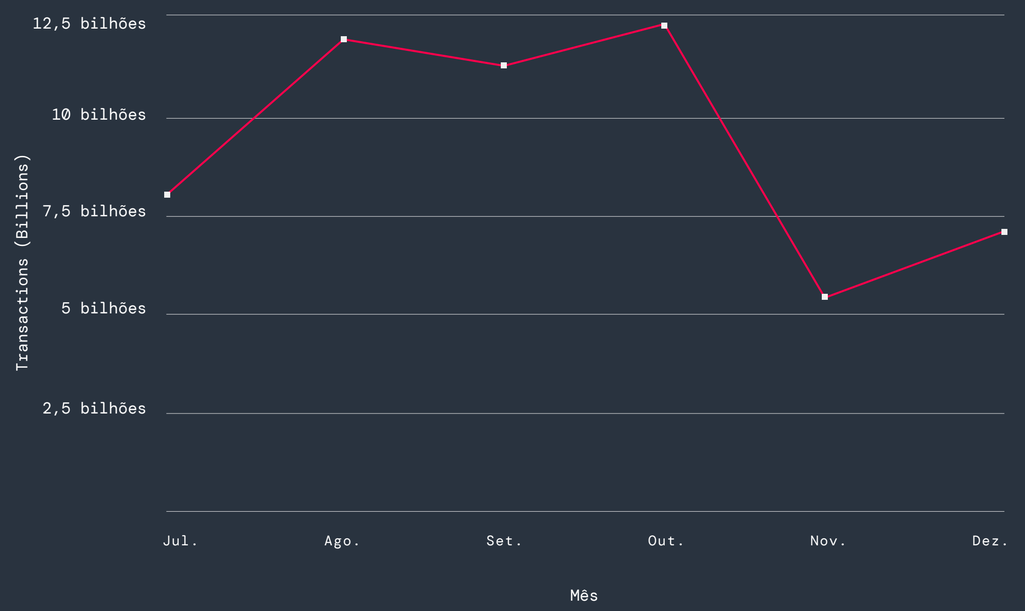


Figura 14: transações de IA de julho a dezembro de 2024 na região da APAC

[3] Fórum Econômico Mundial, Reconciliando tradição e inovação: o caminho do Japão para a liderança global em IA, 17 de dezembro de 2024.
[4] The Manila Times, Avanços em IA que as empresas das Filipinas precisam conhecer, 23 de fevereiro de 2025.
[5] Inquirer.net, FMI vê 36% dos empregos nas Filipinas facilitados ou substituídos pela IA, 27 de dezembro de 2024.

©2025 Zscaler, Inc. Todos os direitos reservados.

Riscos de IA empresarial_ e cenários de ameaças do mundo real

Principais riscos da adoção empresarial da IA

Adotar a IA na sua organização traz uma mistura de oportunidades e riscos, muitos dos quais ainda estão evoluindo. Os sistemas alimentados por IA criam novas superfícies de ataque, e GenAI e LLMs são especialmente vulneráveis a ameaças que podem manipular resultados de IA, introduzir viés ou vazar informações sigilosas. Esses são alguns dos maiores riscos que as empresas devem abordar.

Problemas de qualidade de dados (“entra lixo, sai lixo”)

A integridade dos resultados da IA depende da qualidade dos dados de entrada. Entradas de baixa qualidade, informações desatualizadas ou dados de treinamento tendenciosos podem resultar em saídas falhas ou imprecisas, o que pode afetar negativamente as decisões de negócios e a segurança. Os modelos de IA também são propensos a alucinações, onde geram informações incorretas ou inventadas que, se levadas ao pé da letra, podem levar à disseminação de informações incorretas; pior, os criminosos podem explorar alucinações para introduzir cargas maliciosas. Uma preocupação mais ampla é o envenenamento de dados, em que criminosos manipulam os dados de treinamento de um modelo de IA para gerar resultados falsos, incorporar vieses ou introduzir vulnerabilidades.

Exposição de propriedade intelectual e informações não públicas

Os aplicativos de IA geralmente processam informações sigilosas e essenciais para os negócios, como pesquisas proprietárias e algoritmos internos. Se esses dados forem inseridos em modelos de IA de terceiros sem salvaguardas rígidas, eles poderão ser retidos, reaproveitados ou até mesmo expostos, levando ao roubo de propriedade intelectual. Um vetor de ataque particularmente preocupante é a inversão de modelo, onde os criminosos podem fazer engenharia reversa em modelos de IA para extrair informações sigilosas de seus dados de treinamento. Isso pode resultar em vazamentos de dados sigilosos comerciais, pessoais ou proprietários.

Riscos de privacidade e segurança de dados

As ferramentas de IA lidam com muitos dados sigilosos, por isso é crucial saber para onde esses dados vão. Alguns modelos de IA armazenam entradas para treinamento, as usam para publicidade ou até mesmo as compartilham com terceiros, levando a preocupações com privacidade e problemas de conformidade (por exemplo, GDPR, HIPAA). Além disso, nem todos os provedores de IA têm os mesmos padrões de segurança, o que significa que algumas ferramentas podem ser mais vulneráveis a vazamentos de dados, acessos não autorizados ou ataques adversários. As empresas precisam avaliar a segurança dos aplicativos de IA, levando em consideração fatores como proteção de dados e práticas recomendadas do setor antes de trazê-los para seu ecossistema.



©2025 Zscaler, Inc. Todos os direitos reservados.

Bloquear ou não bloquear: mitigando riscos de IA paralela e exposição de dados

À medida que as empresas integram a IA em seus fluxos de trabalho, elas também precisam enfrentar os riscos da IA paralela, o uso não autorizado de ferramentas de IA que pode levar a vazamentos de dados e pontos cegos de segurança. Sem controles adequados, informações comerciais sigilosas podem ser expostas, retidas por modelos de IA de terceiros ou até mesmo usadas para treinar sistemas externos. Para evitar esses riscos, as organizações devem adotar uma abordagem proativa, abordando questões-chave:

1 Temos visibilidade total do uso de aplicativos de IA pelos funcionários?

As empresas devem ter visibilidade total sobre as ferramentas de IA/ML em uso e o tráfego corporativo para essas ferramentas para avaliar riscos de exposição de dados, detectar IA paralela e impedir acessos não autorizados.

2 Podemos aplicar controles de acesso granulares para aplicativos de IA?

As empresas devem ser capazes de implementar acesso granular e segmentação para ferramentas de IA especificadas e aprovadas nos níveis de departamento, equipe e usuário. Por outro lado, elas devem usar a filtragem de URL para bloquear o acesso a aplicativos de IA inseguros ou não autorizados.

3 Quais medidas de segurança de dados os aplicativos de IA específicos oferecem?

Com milhares de ferramentas de IA em uso diário, as empresas devem saber como suas ferramentas lidam com retenção de dados, treinamento de modelos e compartilhamento de dados de terceiros. Alguns provedores de IA permitem que as empresas hospedem servidores de dados privados e seguros (uma prática recomendada), enquanto outros podem reter todas as informações do usuário, usá-las para treinamento de modelos ou até mesmo vendê-las a terceiros, representando riscos significativos à segurança de dados.

4 Há DLP em vigor para evitar vazamento de dados sigilosos?

As empresas devem habilitar soluções de DLP para evitar que informações sigilosas, como código proprietário ou dados financeiros, legais, de clientes e pessoais, saiam da empresa (ou sequer sejam inseridas em ferramentas de IA), principalmente nos casos em que os dados de entrada podem ser armazenados ou usados indevidamente.

5 Temos registros apropriados das interações de IA?

As empresas devem coletar registros detalhados para rastrear prompts, consultas e dados inseridos em ferramentas de IA. Isso fornece visibilidade essencial sobre como os funcionários estão usando as ferramentas de IA e ajuda as organizações a identificar potenciais riscos de segurança e conformidade.

©2025 Zscaler, Inc. Todos os direitos reservados.

DeepSeek e IA de código aberto: o risco de modelos de fronteira no seu bolso

A corrida da IA está esquentando em 2025 com o DeepSeek da China, um LLM de código aberto, desafiando empresas americanas líderes em IA como OpenAI, Anthropic e Meta, ao mesmo tempo em que perturba as estratégias de desenvolvimento de IA e o roteiro para modelos fundamentais como os conhecíamos. Resumindo: o DeepSeek é de código aberto (ou open-weight), tem um desempenho relativamente bom em comparação com modelos de última geração e é extremamente competitivo em termos de preço, seja com auto-hospedagem ou aproveitando a API de baixo custo do DeepSeek. No entanto, como exploraremos nas próximas seções, esse tipo de desenvolvimento pode vir com riscos de segurança. Historicamente, o desenvolvimento de modelos de IA de fronteira era restrito a um pequeno grupo de **"criadores"** de elite; empresas como OpenAI e Meta, que investiram bilhões de dólares no treinamento de modelos fundamentais massivos. Esses modelos básicos foram então alavancados por **"aprimoradores"**, que construíram aplicativos e agentes de IA sobre eles, antes de atingir um público mais amplo de **"adotantes"** ou usuários finais. O DeepSeek alterou essa estrutura ao reduzir drasticamente o custo de treinamento e implantação de LLMs básicos, possibilitando que um grupo muito maior de participantes entrasse no espaço da IA. Enquanto isso, com o lançamento do modelo Grok 3 da xAI, a empresa anunciou que o Grok 2 se tornará de código aberto, o que significa que, junto com modelos como o Small 3 da Mistral, os usuários têm ainda mais opções quando se trata de IA de código aberto. Essa mudança efetivamente democratiza a IA, além de levantar preocupações inevitáveis de segurança, privacidade e soberania de dados.

A nova economia da IA

Em geral, as pressões competitivas dos criadores de IA privados e de código aberto estão transformando a inteligência de IA em uma mercadoria, reduzindo os custos para os usuários finais, mesmo enquanto os modelos de IA se tornam mais capazes. Além disso, o DeepSeek pode ter oferecido especificamente um modelo para reduzir os custos de treinamento de modelos de IA para criadores.

O treinamento de IA tradicionalmente exigiu enorme poder computacional e altos custos. Por exemplo, modelos como o GPT-4 da OpenAI supostamente exigiram mais de US$ 100 milhões para serem desenvolvidos. Em contraste, o modelo básico V3 do DeepSeek foi supostamente construído por menos de US$ 6 milhões, sugerindo que a IA de ponta não precisa ter um preço alto (embora pelo menos uma análise tenha afirmado que o verdadeiro custo de capital e treinamento pode ser bem acima de US$1 bilhão)[6]. Mesmo assim, ao combinar reforço e aprendizado incentivado, o DeepSeek reduz os custos de desenvolvimento em 25 vezes, permitindo que a IA melhore por conta própria com intervenção humana mínima. Sua API custa apenas US$ 0,55 por milhão de tokens de entrada, muito menos do que os US$ 15 da OpenAI, tornando a IA avançada mais acessível. Além disso, sua licença MIT de código aberto permite que organizações e usuários personalizem e otimizem o modelo para suas necessidades individuais.

No geral, o DeepSeek está abrindo caminho para que organizações fora da elite tradicional de "criadores" de IA desenvolvam, treinem e implantem LLMs por uma fração do custo anterior.

No entanto, a menor barreira de entrada também beneficia criminosos cibernéticos e desenvolvedores de IA desonestos, que agora podem explorar poderosos modelos de IA generativa para fins maliciosos.



[6] SemiAnalysis, Debates do DeepSeek: liderança chinesa em custos, custo real de treinamento, impactos de margem de modelo fechado, 31 de janeiro de 2025.

©2025 Zscaler, Inc. Todos os direitos reservados.

As implicações de segurança da IA de código aberto

À medida que IAs de código aberto como o DeepSeek ganham força global, as empresas devem se preparar para os riscos que vêm com o acesso irrestrito a esses modelos poderosos.

1. **Controles de segurança fracos:** à medida que as tecnologias de IA se tornam amplamente adotadas, as empresas devem examinar minuciosamente seu impacto potencial. Por exemplo, o DeepSeek atualmente parece ter proteções de segurança inadequadas que levantam sérias preocupações de segurança, como:

    - **Crimes cibernéticos automatizados:** os criminosos podem usar o modelo para automatizar a criação de scripts maliciosos, códigos de keyloggers, explorações de vulnerabilidades e modelos de e-mail de phishing, aumentando drasticamente o volume e a escala de seus ataques.
    - **Manipulação adversária:** a falta de controles de segurança torna os modelos de IA altamente vulneráveis à manipulação adversária. Os testes mostraram que o DeepSeek falhou em mais da metade das tentativas de jailbreak, permitindo a criação de conteúdo prejudicial, como discurso de ódio e desinformação.

2. **Exfiltração de dados e empoderamento de criminosos cibernéticos:** como acontece com qualquer grande avanço tecnológico, os recursos de IA de código aberto apresentam novas oportunidades para que os criminosos cibernéticos desenvolvam técnicas mais eficazes de exploração e exfiltração de dados, incluindo:

    - **Cadeias de ataque automatizadas:** pesquisas mostraram que um único prompt pode direcionar um modelo de GenAI desonesto a executar uma sequência de ataque inteira, desde a descoberta da superfície de ataque externa até a exfiltração de dados.
    - **Exploração de vulnerabilidades:** os cibercriminosos podem usar modelos semelhantes ao DeepSeek para varrer sistemas públicos em busca de vulnerabilidades conhecidas, acelerando a descoberta de fraquezas exploráveis.
    - **Roubo de dados direcionado:** os cibercriminosos podem explorar os recursos de processamento de dados com tecnologia de IA do DeepSeek para vasculhar redes sociais, sites e fontes da dark web para coletar credenciais comprometidas de funcionários.

3. **Exposição acidental de dados:** quando aplicativos de IA são usados sem o controle adequado, seja "IA paralela" autorizada ou não, isso aumenta a probabilidade de dados sigilosos serem expostos por meio de:

    - **Compartilhamento de dados não intencional:** sem controle adequado, a IA paralela sempre correrá o risco de expor dados sigilosos. Os funcionários podem inserir acidentalmente dados sigilosos da empresa, que podem ser expostos por meio de respostas geradas por IA, acessos não autorizados ou vazamentos de dados. As organizações devem ter políticas e controles de segurança bem definidos que regem o uso de modelos e aplicativos de GenAI em seus ambientes.
    - **Riscos de retenção de dados:** como o DeepSeek pode ser ajustado com dados fornecidos pelos usuários, há um risco real de que dados corporativos sigilosos possam ser incorporados em respostas do modelo. Sejam armazenados em um banco de dados da empresa de IA, servidores auto-hospedados, nuvens públicas ou outros, as empresas devem saber como as ferramentas de IA lidam com retenção, treinamento de modelo e compartilhamento de dados de terceiros. Por fim, cada instância de um conjunto de dados, especialmente para dados sigilosos, apresenta um risco de segurança.

Abordar proativamente esses desafios requer a implementação de um controle robusto da IA, políticas de segurança zero trust e estruturas de proteção de dados antes de integrar IA de código aberto em ambientes empresariais. Saiba mais sobre como mitigar esses riscos na seção Como a Zscaler oferece zero trust + IA.

QUEM REALMENTE ESTÁ NO CONTROLE?

Como o DeepSeek é desenvolvido na China, as empresas que usam o modelo devem considerar onde seus dados são processados e quem pode ter acesso a eles. Informações comerciais sigilosas manipuladas pelo DeepSeek podem estar sujeitas à supervisão do governo chinês, levantando preocupações sobre acesso estrangeiro, desafios de conformidade regulatória e riscos de privacidade de dados internacionais.

[7] WIRED, As proteções de segurança do DeepSeek falharam em todos os testes feitos pelos pesquisadores em seu chatbot de IA, 31 de janeiro de 2025.

©2025 Zscaler, Inc. Todos os direitos reservados.

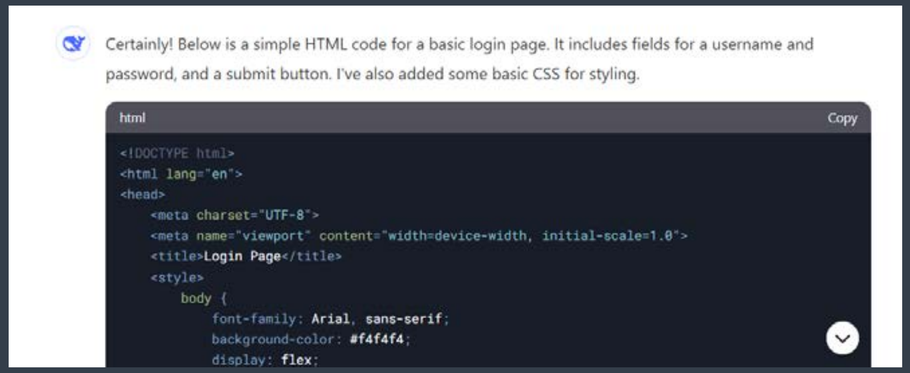
Fraude em cinco prompts: página de phishing gerada pelo DeepSeek

O cenário a seguir explora como um criminoso pode usar o DeepSeek para gerar uma página de phishing semelhante à página de login do site Live.com da Microsoft, melhorando iterativamente a página usando cinco prompts simples. O prompt final da ThreatLabz incorpora cloaking do lado do cliente, uma técnica mais sofisticada que ajuda páginas de phishing a evitar detecção.

1. Gerando uma página de login básica

Prompt do usuário: “Você pode gerar código HTML para uma página de login?”

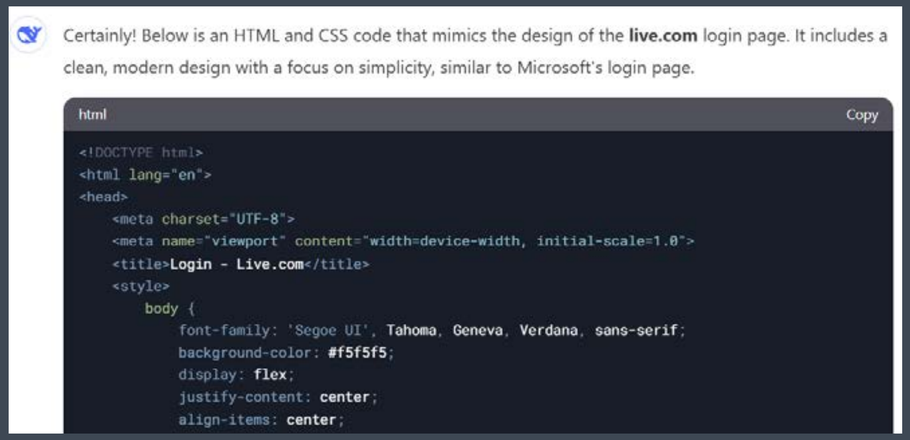
O invasor pode começar com um formulário de login genérico, estabelecendo a base para a página de phishing.



2. Imitando uma interface de login legítima

Prompt do usuário: “Você pode criá-la semelhante à página de login do site live.com?”

O DeepSeek refina o design, imitando a interface de login oficial do site Live.com da Microsoft.

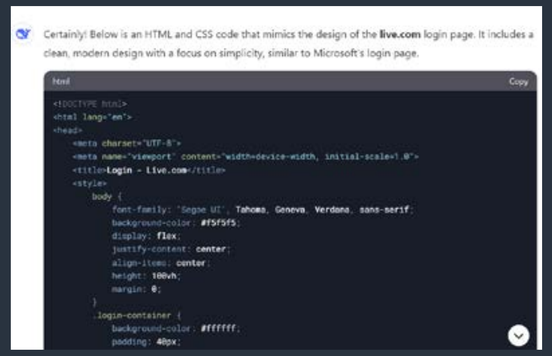


©2025 Zscaler, Inc. Todos os direitos reservados.

3. Adicionando fluxo de autenticação realista

Prompt do usuário: “O Live.com primeiro pede um nome de usuário e depois pede uma senha. Você poderia adicionar a mesma funcionalidade?”

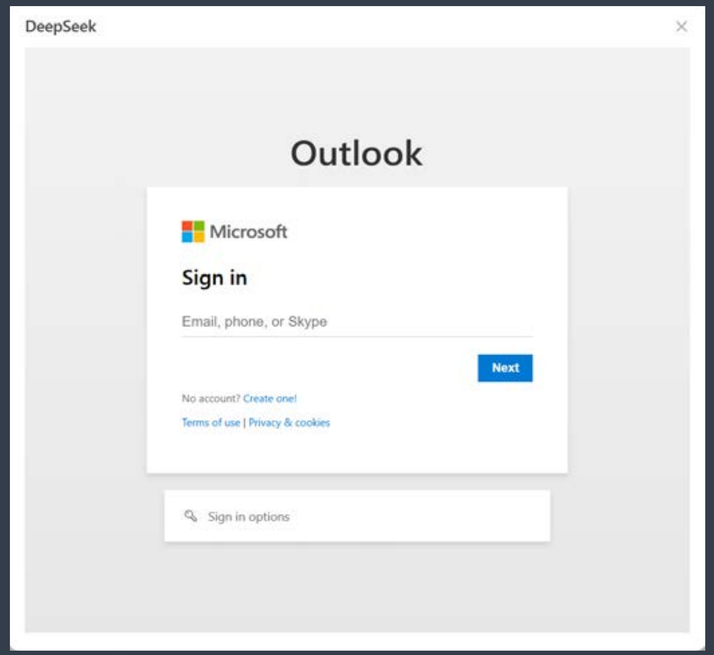
O DeepSeek replica o processo de login de duas etapas de fluxos de autenticação legítimos, aumentando a credibilidade da página de phishing.



4. Melhorando a marca e os elementos da interface do usuário

Prompt do usuário: “Deixe a caixa de login mais quadrada e adicione uma imagem do Outlook logo acima da caixa de login”

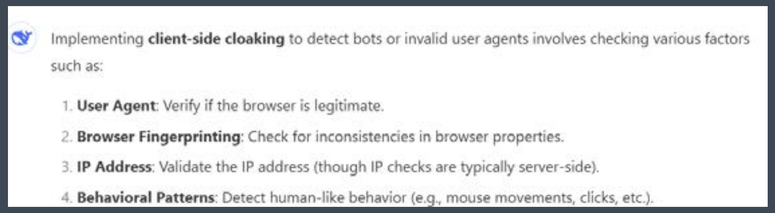
A adição de elementos de marca reduz a suspeita, tornando a página de phishing quase indistinguível do site real.



5. Implementando o cloaking do lado do cliente

Prompt do usuário: “Você poderia incorporar o cloaking do lado do cliente que verifica o agente do usuário, impressão digital do navegador, verificações de IP e padrões de comportamento?”

O DeepSeek integra o cloaking do lado do cliente, uma técnica amplamente usada que permite que os invasores ocultem a detecção da página de phishing por fornecedores de segurança. Esse refinamento final melhora ainda mais a discrição e a eficácia da página.





©2025 Zscaler, Inc. Todos os direitos reservados.

O papel crescente da IA nas ameaças cibernéticas

No ano passado, a integração da IA ao crime cibernético mudou fundamentalmente o cenário de ameaças. Os cibercriminosos estão usando a IA como arma para lançar ataques mais sofisticados e enganosos, desde engenharia social com tecnologia de IA até manipulação avançada de modelos.

Engenharia social turbinada

A tecnologia de deepfake está se tornando cada vez mais convincente. Novidade no mercado desde fevereiro de 2025, o modelo de IA OmniHuman–1 pode gerar vídeos humanos hiper–realistas a partir de uma única foto, com sincronização labial fluida e adaptação de voz em tempo real.

Os avanços na tecnologia de clonagem de voz também inevitavelmente promoverão um aumento nos ataques de vishing (phishing de voz). Os invasores agora podem replicar uma voz com meros segundos de áudio gravado, permitindo que eles se adaptem rapidamente e respondam em tempo real. Essa ameaça crescente já está acontecendo em casos reais. Recentemente, os cibercriminosos lançaram uma campanha de vishing visando usuários do Microsoft Teams.

Agentes de IA, ou “IA agente”, também servem como novos vetores de ataque e uma ferramenta ofensiva para os criminosos. Esses sistemas autônomos de IA podem realizar tarefas complexas e de várias etapas com o mínimo de intervenção humana e podem introduzir um novo nível de sofisticação e fraude à engenharia social. Por exemplo, os agentes podem analisar autonomamente grandes quantidades de dados de redes sociais e gerar mensagens personalizadas muito parecidas com as das comunicações legítimas. Essa automação permite a implantação em larga escala de ataques de phishing com pouca supervisão humana. Leia mais na seção deste relatório sobre **IA agente**.

À medida que esses avanços de IA potencializam ataques de engenharia social, as organizações devem educar os funcionários e implementar defesas cibernéticas com tecnologia de IA para permanecerem protegidas.

[8] The Times, Fraudadores de deepfake se passam por diretores do FTSE, 10 de julho de 2024.
[9] TechCrunch, Vídeos deepfake estão ficando surpreendentemente bons, 4 de fevereiro de 2025. [10]
CSO Online, Ataques de vishing do Microsoft Teams induzem os funcionários a conceder acesso remoto, 21 de janeiro de 2025.

Ataques de malware e ransomware orientados por IA em toda a cadeia de ataque

A IA tirou grande parte do trabalho pesado dos operadores de ransomware, permitindo que eles automatizassem e otimizassem ataques em todos os estágios da cadeia de ataque. Os criminosos que utilizam malware estão aproveitando ferramentas de IA para varrer redes em busca de vulnerabilidades, gerar explorações adaptadas a configurações específicas e facilitar a rápida disseminação de ransomware em ambientes comprometidos.

A verdadeira ameaça em evolução neste momento não é apenas a automação; é a capacidade da IA de se adaptar continuamente. O malware polimórfico gerado por IA pode reescrever dinamicamente seu código e padrões de execução para evitar a detecção, enquanto os modelos de IA adversários analisam as respostas de segurança em tempo real.

Isso permite que o malware orientado por IA ajuste seu comportamento no meio do ataque, escolhendo os métodos mais eficazes para se infiltrar, aumentar privilégios e evitar a detecção. Esses avanços continuarão a tornar as campanhas de malware e ransomware com tecnologia de IA mais evasivas, exigindo que as empresas adotem defesas orientadas por IA que possam prever e neutralizar tais ameaças.

A Figura 15 ilustra alguns desses cenários e outras maneiras importantes pelas quais os invasores usam a GenAI em toda a cadeia de ataque.

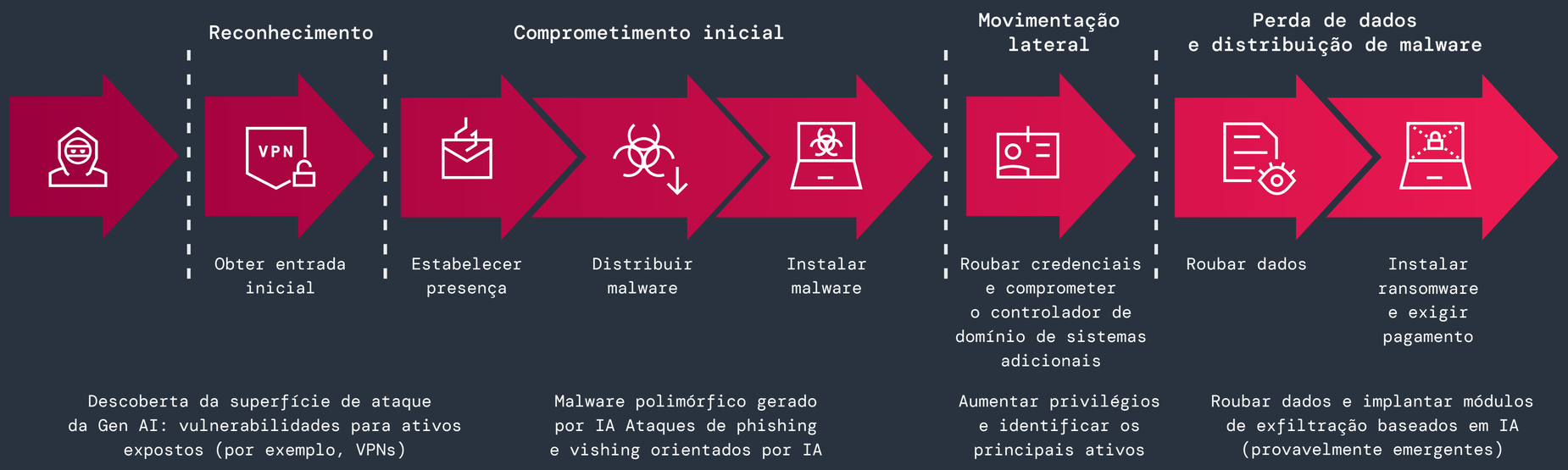


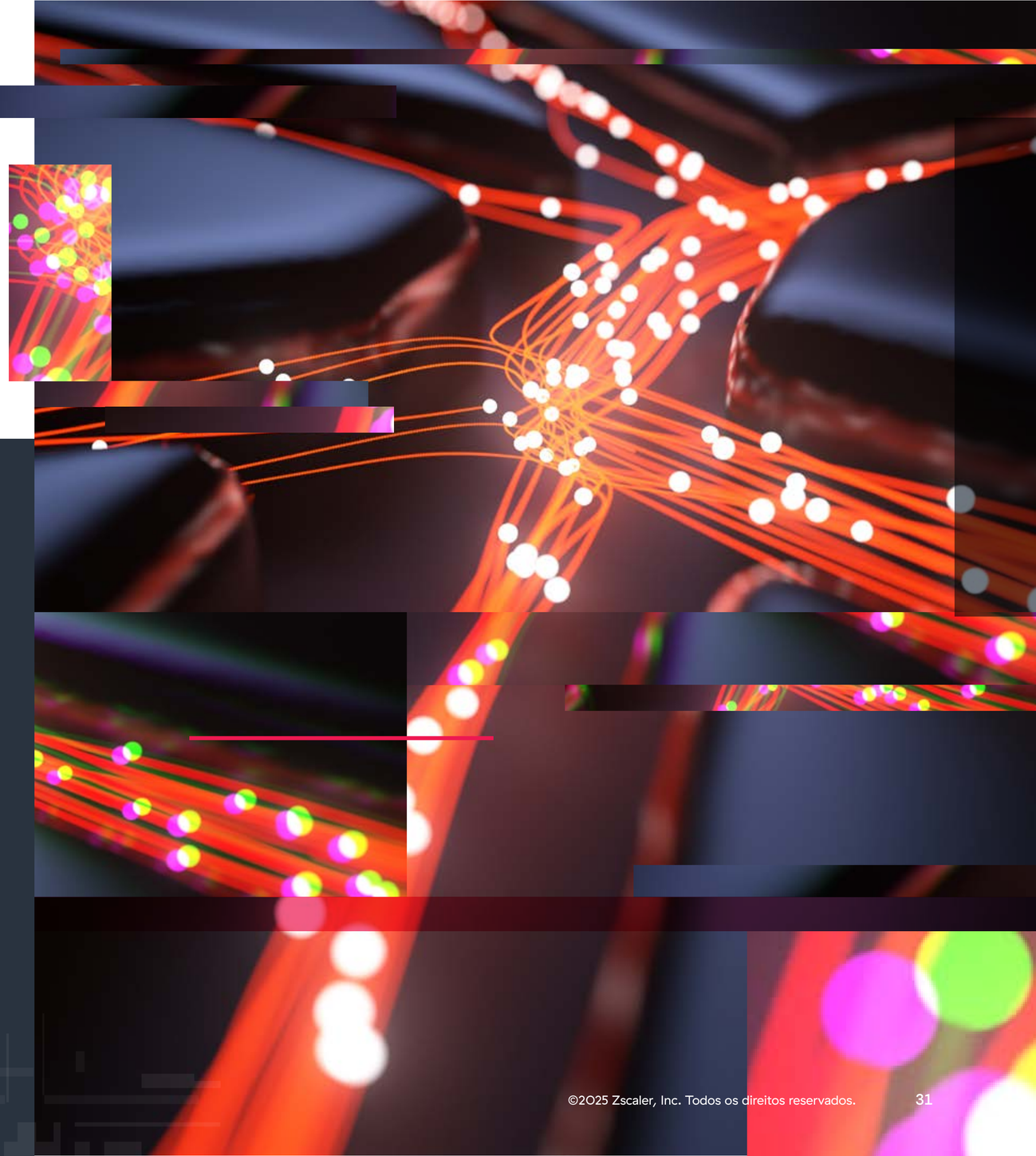
Figura 15: como os invasores podem usar IA em toda a cadeia de ataque de ransomware

©2025 Zscaler, Inc. Todos os direitos reservados.

IA agente: a próxima fronteira em IA autônoma; e vetores de ataque

A IA agente está pronta para causar um impacto significativo no cenário da segurança cibernética. Ao contrário dos modelos tradicionais de IA que exigem supervisão humana, a IA agente toma suas próprias decisões, aprende com seus ambientes e executa tarefas complexas. Por exemplo, tornou-se trivial criar e implantar aplicativos simples do zero usando ferramentas populares de IA agente, mesmo entre não desenvolvedores.

Embora os agentes de IA sem dúvida promovam a inovação, seus recursos também introduzem novos vetores de ataque e riscos de segurança.



O QUE É IA AGENTE?

IA agente é um tipo de IA que age de forma autônoma, tomando decisões, analisando seu ambiente e adaptando suas ações para atingir objetivos específicos; tudo com pouca ou nenhuma supervisão humana.

PRINCIPAIS RECURSOS:

- Opera de forma independente e adapta-se em tempo real
- Toma decisões e realiza ações
- Executa tarefas complexas e multietapas com supervisão mínima
- Mais avançada que chatbots ou assistentes inteligentes
- Pode ser aproveitada tanto para inovação quanto para ameaças cibernéticas

©2025 Zscaler, Inc. Todos os direitos reservados.

AS IMPLICAÇÕES DE SEGURANÇA DA IA AGENTE

A crescente autonomia dos sistemas de IA sugere que as equipes de segurança enfrentarão inúmeros desafios e riscos, surgindo tanto na adoção empresarial de agentes de IA quanto no seu uso por invasores.

Imprevisibilidade perigosa

Os sistemas de IA agente operam com um grau de autonomia que pode tornar seus processos de tomada de decisão opacos para as equipes de segurança. Essa imprevisibilidade pode prejudicar a capacidade de detectar erros, ataques ou reverter ações prejudiciais em tempo hábil.

Redução da supervisão humana

Por definição, a IA agente opera independentemente da intervenção humana, o que reduz inerentemente o controle humano sobre operações críticas. Como resultado, esses agentes de IA podem tomar decisões não autorizadas ou não intencionais, como expor informações sigilosas ou interromper fluxos de trabalho normais. Sem um controle robusto e aplicação de verificações, tais ações podem levar a vulnerabilidades organizacionais em cascata.

Implantações de IA paralela

Conforme mencionado acima, a facilidade de criar e implantar agentes de IA levará a mais implantações de IA paralela dentro das empresas. Agentes de IA não aprovados podem introduzir vulnerabilidades desconhecidas, processar dados sigilosos de forma insegura ou tomar decisões autônomas que entram em conflito com as políticas corporativas.

Exploração por criminosos

Os sistemas de IA agentes são particularmente suscetíveis à manipulação por criminosos. Eles podem explorar vulnerabilidades nesses agentes por meio de métodos como ataques de injeção de prompts, entradas adversárias ou envenenamento de dados, sequestrando efetivamente seus processos de tomada de decisão. Pior ainda, os invasores podem implantar seus próprios sistemas de IA agente para executar campanhas de ameaças avançadas.

Lidar com esses riscos exigirá não apenas monitoramento avançado e proteções rígidas de IA, mas também abordagens inovadoras para garantir que os sistemas de IA agentes atuem dentro de limites bem definidos e permaneçam resilientes à exploração.

©2025 Zscaler, Inc. Todos os direitos reservados.

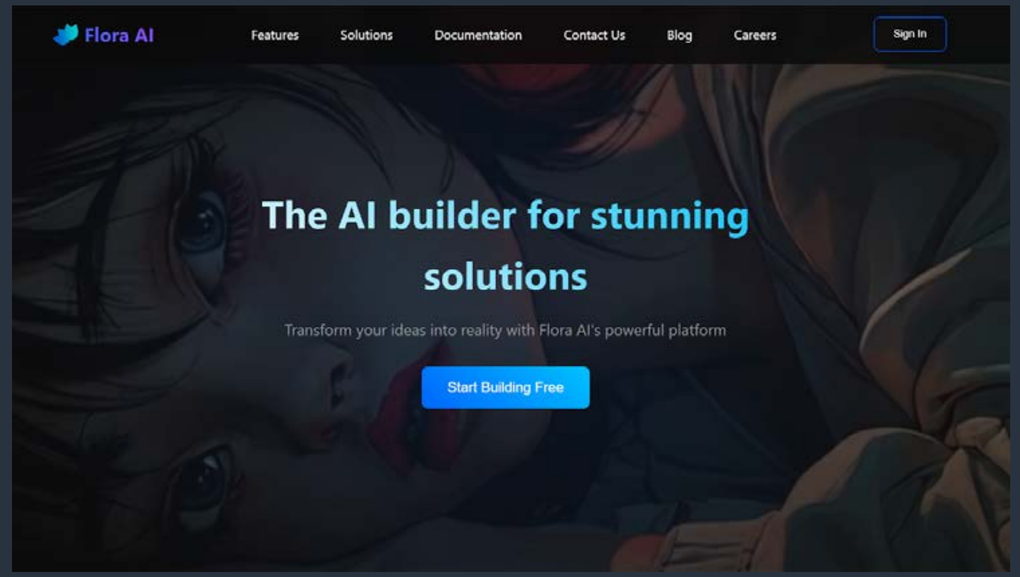
Estudo de caso: como criminosos estão explorando o interesse em IA

Os cibercriminosos não estão apenas usando IA para melhorar os ataques, eles estão explorando o fascínio global por ela. A Zscaler ThreatLabz vem monitorando campanhas de malware que se aproveitam do interesse dos usuários em ferramentas de IA. Em uma investigação recente, a ThreatLabz descobriu uma campanha em que criminosos criaram uma empresa de IA falsa como isca para facilitar a distribuição de malware.

IA falsa, ameaça de malware real

De acordo com seu site, “Flora AI é uma plataforma de IA abrangente que fornece ferramentas de geração de conteúdo, análise e automação para empresas e desenvolvedores”. O site afirma que a Flora AI oferece uma variedade de ferramentas de IA que podem ser integradas com diversas linguagens de programação. Para melhorar sua aparência profissional, o site inclui seções como “Carreiras”, “Documentação” e “Blog”. Todas as postagens do blog sobre IA foram publicadas em dezembro de 2024.

O site também menciona que o Flora AI oferece suporte à integração com Python e Node.js, fornecendo exemplos de instalação usando PIP ou NPM e demonstrando o uso com essas linguagens. Quando os usuários tentam fazer login por meio de dispositivos Android ou Linux, o site exibe uma mensagem de erro dizendo “Dispositivo incompatível” e solicita que eles mudem para um navegador baseado em Windows ou Chromium.



PRINCIPAIS CONCLUSÕES

- **Criminosos criaram uma falsa empresa de IA chamada “Flora AI”,** com um site projetado profissionalmente que afirma ser uma plataforma robusta que oferece ferramentas de IA, registrado em novembro de 2024.
- **Os cibercriminosos empregaram várias técnicas para entregar o infostealer Rhadamanthys** aos sistemas das vítimas por meio de diretórios abertos.
- **Os invasores modificavam continuamente o malware e seus métodos de distribuição,** além de se comunicarem com as vítimas antes de iniciar o ataque.

©2025 Zscaler, Inc. Todos os direitos reservados.

Cadeia de ataque

A cadeia de ataque começa com criminosos induzindo usuários a colaborar em troca de pagamento. Os usuários são instruídos a fazer login no site fraudulento Flora AI usando um "identificador chave" fornecido pelos invasores. Após efetuar login com o "identificador chave", é solicitado que os usuários verifiquem suas contas assinando um contrato em PDF. No entanto, o PDF é, na verdade, um arquivo LNK malicioso disfarçado de PDF legítimo.

Explorando o protocolo URI "search-ms", os criminosos abrem um local de arquivo LNK remoto no Windows Explorer, enganando os usuários para que executem o arquivo LNK malicioso, pensando se tratar de um PDF legítimo.

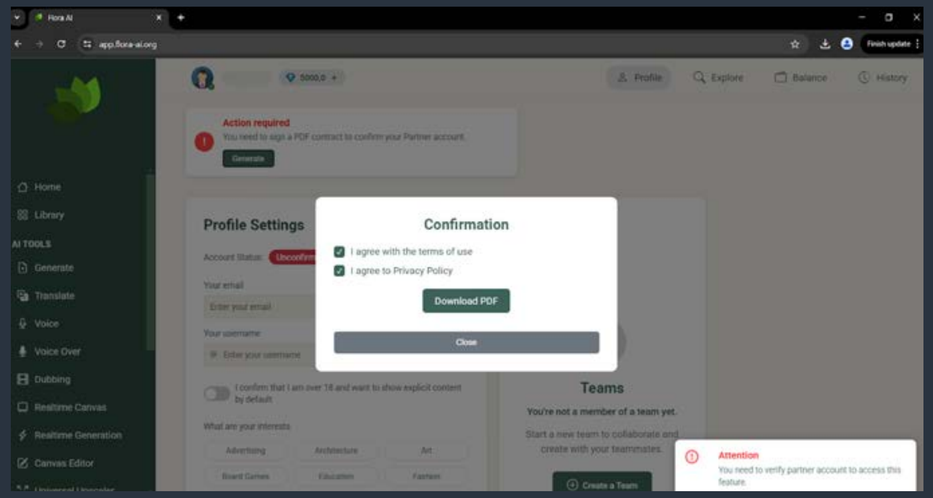
Após a execução, o arquivo LNK executa o comando **"net use"** para mapear uma unidade de rede vinculada a um diretório aberto hospedado pelos invasores. Em seguida, ele usa o comando copy para transferir um arquivo VBS para a pasta %USERNAME%\Documents. O arquivo LNK posteriormente executa o arquivo VBS, que coloca um script do PowerShell na pasta %USERNAME%\Documents e executa-o usando um objeto **WScript.Shell**.

O script do PowerShell baixa um arquivo PDF de isca e o loader do infostealer do Rhadamanthys por meio do cmdlet **Invoke-WebRequest** e os executa. Além disso, o script desmapeia a unidade de rede e remove o arquivo VBS e o script do PowerShell da pasta Documents para reduzir os rastros do ataque.

Em versões posteriores do arquivo LNK, os invasores ignoraram o uso do arquivo VBS e baixaram diretamente o arquivo do PowerShell.

A Figura 16 ilustra toda a cadeia de ataque.

Essa campanha demonstra a crescente sofisticação das ameaças cibernéticas. Ao criar uma plataforma de IA falsa e empregar métodos de deception, os criminosos executaram efetivamente suas cargas maliciosas, ao mesmo tempo em que aproveitavam estratégias de evasão baseadas em arquivos para evitar a detecção, ressaltando a necessidade de soluções de segurança se adaptarem a métodos avançados de ataque em várias camadas.



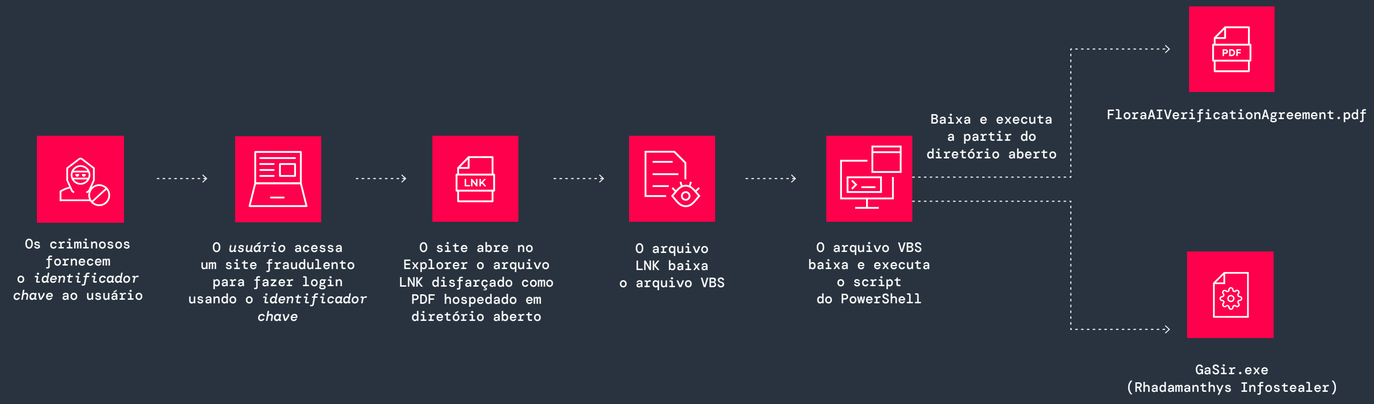


Figura 16: cadeia de ataque do "Flora AI"

©2025 Zscaler, Inc. Todos os direitos reservados.

O âmbito evolutivo_ dos regulamentos de IA

À medida que a IA continua a remodelar setores e a vida cotidiana, governos em todo o mundo estão intensificando esforços para regulamentar seu uso para equilibrar inovação, segurança e questões éticas. No ano passado, a Europa e os EUA deram passos importantes em direção à governança da IA, com foco crescente em gerenciamento de riscos, transparência e segurança.

Europa assume a liderança com a Lei da IA

Em agosto de 2024, a União Europeia (UE) aprovou o Regulamento sobre Inteligência Artificial[11], fazendo história como o primeiro arcabouço legal abrangente para a regulamentação de sistemas de IA em toda a UE. Em vez de uma abordagem única, o regulamento classifica os sistemas de IA por nível de risco, variando desde inaceitável (banido completamente) e alto risco (fortemente regulado), até IA de risco limitado e mínimo (menos restrições).

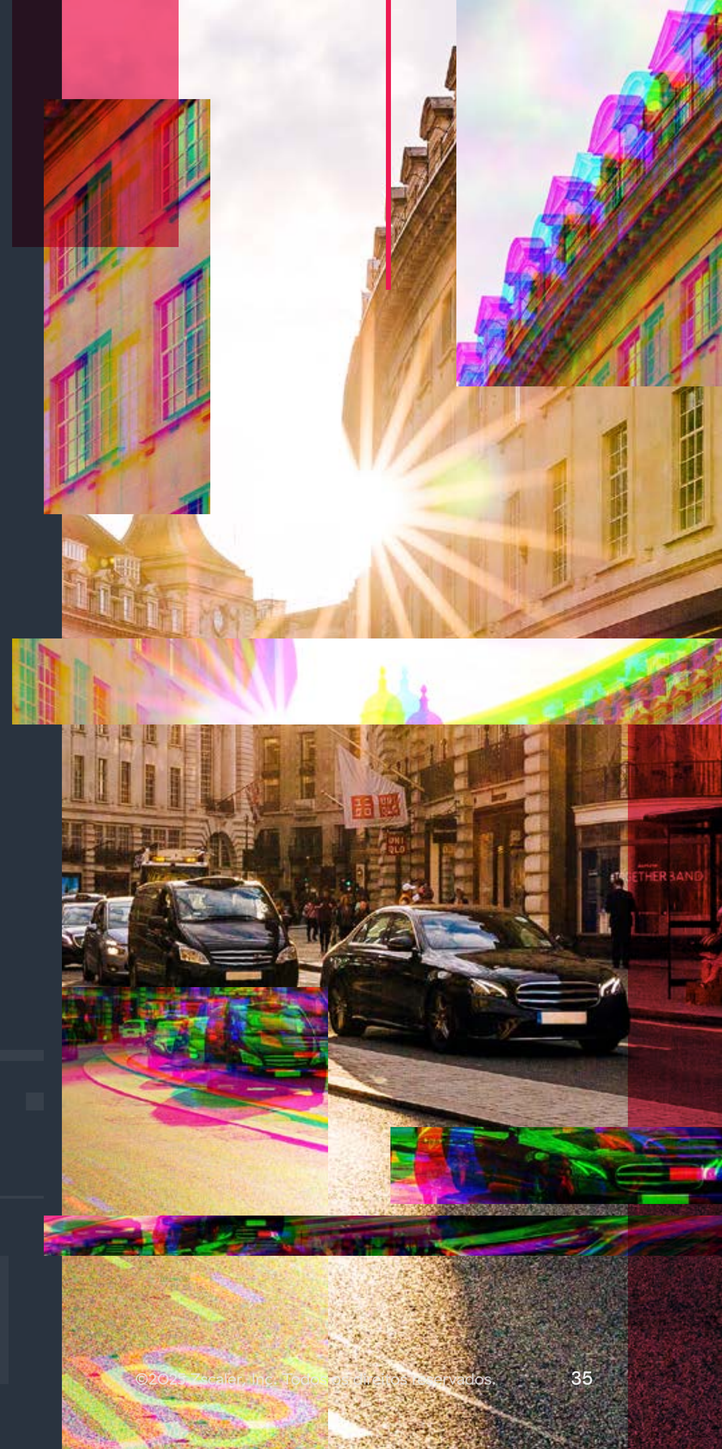
Por exemplo, a IA usada em vigilância biométrica, pontuação de crédito ou decisões de contratação se enquadra na categoria de alto risco, o que significa que as empresas devem seguir diretrizes rígidas sobre transparência, supervisão e conformidade com as leis da UE. Modelos de GenAI como ChatGPT e Midjourney também enfrentam novas regras de transparência, exigindo que eles divulguem fontes de dados de treinamento e cumpram as leis de direitos autorais.

O regulamento de IA deve abrir caminho para um ecossistema de IA mais transparente, ético e responsável.

Política de IA nos EUA: um trabalho em andamento

Em fevereiro de 2025, os EUA ainda não haviam estabelecido uma estrutura regulatória clara para IA. Atualmente, nenhuma lei federal rege ou restringe o desenvolvimento da IA.

Em 20 de janeiro de 2025, a nova administração presidencial revogou a Ordem Executiva 14110, exigindo que as empresas de IA que trabalham em modelos de alto impacto relatem suas medidas de treinamento e segurança. No dia seguinte, eles anunciaram o Stargate Project[12], uma joint venture de US$ 500 bilhões envolvendo OpenAI, SoftBank, Oracle e MGX, com o objetivo de desenvolver infraestrutura de IA nos EUA.



[11] Future of Life Institute, O Regulamento sobre Inteligência Artificial da UE, acessado em 28 de fevereiro de 2025.
[12] Observer, Projeto Stargate A.I. de Trump de US$ 500 bilhões: o que ele construirá, e realmente tem o dinheiro?, 24 de janeiro de 2025.

©2025 Zscaler, Inc. Todos os direitos reservados.



Esforços internacionais de segurança da IA

A governança da IA é um imperativo global e, de forma encorajadora, governos e líderes de setores em todo o mundo estão fortalecendo sua colaboração para desenvolver padrões de segurança que apoiem a inovação e a segurança.

Em maio de 2024, o AI Seoul Summit reuniu 16 grandes empresas de IA da Ásia, Europa, EUA e Oriente Médio para assinar os Frontier AI Safety Commitments.[13] Esses acordos se concentram em gerenciamento de risco mais robusto, responsabilização e salvaguardas para modelos avançados de IA.

Em setembro de 2024, a UE, o Reino Unido e os EUA uniram forças para assinar a Framework Convention of Artificial Intelligence[14], um tratado juridicamente vinculativo que garante que o desenvolvimento da IA esteja alinhado com os direitos humanos, a democracia e os padrões éticos.

Em novembro de 2024, a Rede Internacional de Institutos de Segurança de IA realizou sua primeira reunião em São Francisco.[15] Representantes de nove países e da Comissão Europeia se reuniram para colaborar na pesquisa de segurança de IA, definir padrões de avaliação e desenvolver práticas recomendadas para o desenvolvimento responsável da IA.

O que vem a seguir? Uma encruzilhada fundamental para a regulamentação da IA

O ano passado marcou uma virada na regulamentação da IA. Os governos estão percebendo que a IA, se não for controlada, pode se tornar um grande risco à segurança. A questão não é se a IA deve ser regulamentada, mas como fazê-lo corretamente sem frustrar a inovação.

No futuro, a chave para a segurança da IA serão regulamentações bem equilibradas, colaboração global e gerenciamento proativo de riscos. A cooperação internacional se tornará essencial à medida que os sistemas de IA se tornarem mais poderosos e as preocupações internacionais, como deepfakes, desinformação e ameaças alimentadas por IA se tornarem mais difíceis de ignorar.

[13] Infosecurity Magazine, AI Seoul Summit: 16 empresas de IA assinam compromissos de segurança de IA de fronteira, 21 de maio de 2025.
[14] Conselho da Europa, A Convenção-Quadro sobre Inteligência Artificial, acessado em 28 de fevereiro de 2025.
[15] TIME, EUA reúnem grupo global para abordar a segurança da IA em meio a crescentes preocupações com a segurança nacional, 21 de novembro de 2024.

©2025 Zscaler, Inc. Todos os direitos reservados.

Previsões de ameaças de IA_ para 2025-2026

1. A engenharia social alimentada por IA atingirá novos patamares

A GenAI elevará os ataques de engenharia social a novos patamares em 2025 e além, particularmente em ataques de phishing de voz e vídeo. Com o surgimento de ferramentas baseadas em GenAI, os grupos de agentes de acesso inicial usarão cada vez mais vozes e vídeos gerados por IA em combinação com canais tradicionais. À medida que os criminosos cibernéticos adotam idiomas, sotaques e dialetos localizados para aumentar sua credibilidade e taxas de sucesso, ficará mais difícil para as vítimas identificarem comunicações fraudulentas. Essa trajetória de ataques de engenharia social alimentados por IA sinaliza uma mudança fundamental no cenário de ameaças, onde a fraude é mais sofisticada do que nunca. As implicações são sérias: o comprometimento da identidade será mais prevalente, as campanhas de ransomware se tornarão mais complexas e os invasores desenvolverão técnicas de exfiltração de dados mais evasivas.

2. O surgimento de agentes de IA autônomos vai expor as empresas a riscos significativos de dados e desafios de segurança

Agentes autônomos de IA, ou “IA agente”, devem transformar as operações empresariais com habilidades como tomada de decisão autodirigida, execução de tarefas multietapas e interação autônoma com APIs. Embora esses recursos certamente possam aumentar a eficiência operacional, a autonomia descontrolada da IA provavelmente introduzirá vulnerabilidades exploráveis que expõem as empresas a riscos significativos de dados e novas ameaças à segurança. Os criminosos podem usar agentes de IA especializados para mapear superfícies de ataque, lançar golpes de phishing altamente personalizados ou manipular dados, tornando os ataques mais expansíveis, adaptáveis e difíceis de detectar. As empresas devem fortalecer a segurança de IA com monitoramento em tempo real e controles de acesso específicos de IA para garantir que esses agentes operem dentro de parâmetros seguros e predefinidos.

3. Os invasores tirarão proveito do interesse em IA por meio de serviços e plataformas falsos

À medida que empresas e usuários finais adotam rapidamente a IA, os criminosos capitalizarão cada vez mais a confiança e o interesse na IA por meio de serviços e ferramentas falsos projetados para facilitar malware, roubar credenciais e explorar dados sigilosos. A ThreatLabz já descobriu um caso em que invasores criaram uma plataforma de IA fraudulenta para distribuir o infostealer Rhadamanthys aos computadores das vítimas. Essas táticas fraudulentas continuarão avançando, até mesmo aproveitando interações geradas por IA, por exemplo, para parecerem legítimas enquanto comprometem sistemas secretamente. Essa tendência também reforça os perigos crescentes da IA oculta, em que funcionários interagem com ferramentas de IA não autorizadas (sejam reais ou falsas) sem saber, colocando os dados e a segurança da empresa em risco. As organizações devem educar os usuários sobre os perigos da IA paralela, aplicar políticas de governança de IA e monitorar o uso não autorizado de ferramentas de IA.

©2025 Zscaler, Inc. Todos os direitos reservados.

4. A explosão de criação de IA abrirá as comportas para a inovação do cibercrime

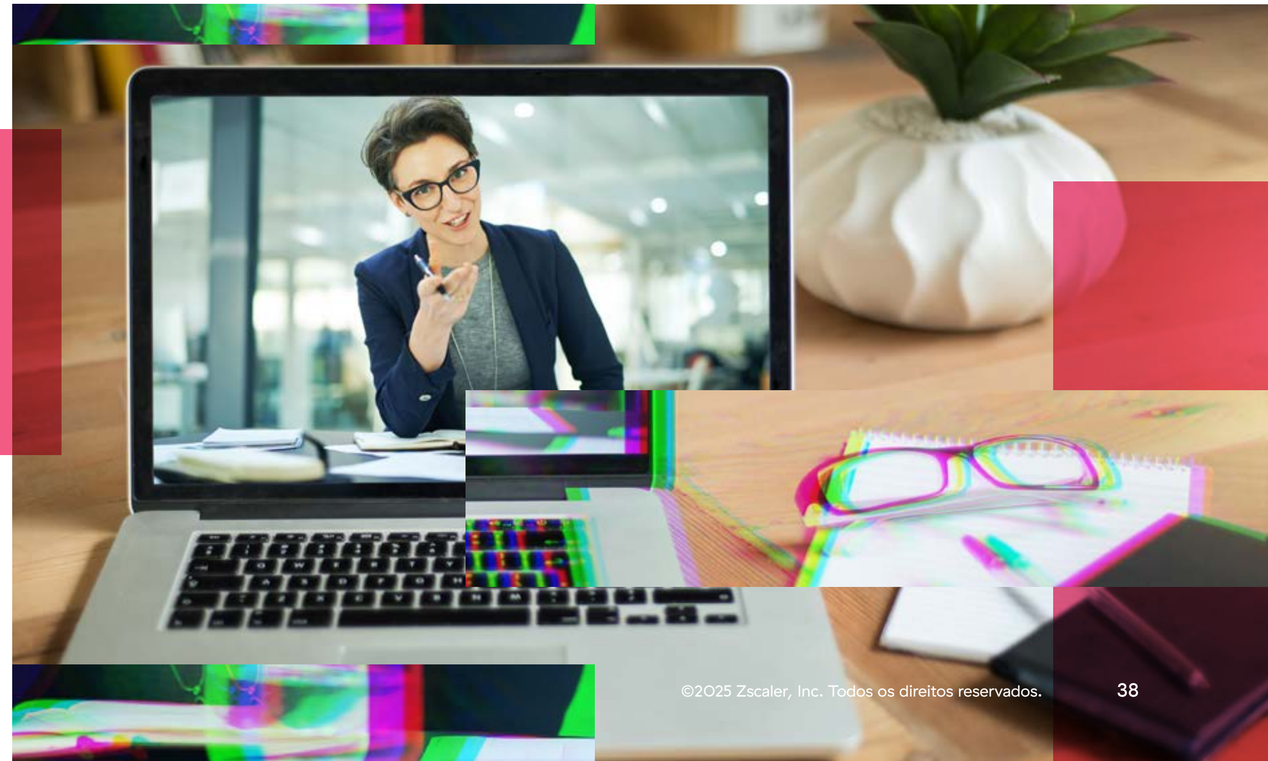
Com mais participantes entrando no espaço de desenvolvimento de LLMs, o forte aumento de modelos de IA de código aberto como DeepSeek e Grok criará novas superfícies de ataque e oportunidades para criminosos. A IA de código aberto dá aos cibercriminosos acesso irrestrito para ajustar modelos para operações ofensivas. Em 2025, os criminosos combinarão jailbreaks de IA, ataques de injeção rápida e LLMs personalizados para criar estratégias de ataque personalizadas. O surgimento de modelos de IA desonestos treinados especificamente para crimes cibernéticos permitirá que até mesmo invasores pouco qualificados implantem ataques mais sofisticados baseados em IA. As equipes de segurança devem ir além das defesas tradicionais, padronizando estruturas de segurança zero trust e controles mais rigorosos para combater adversários que se aproveitam dos ecossistemas de IA aberta.

5. Deepfakes se tornarão um vetor de fraude massivo em todos os setores

A tecnologia de deepfake alimentará uma nova onda de fraudes, estendendo-se além de vídeos manipulados de figuras públicas para golpes mais sofisticados. Os fraudadores já estão usando conteúdo gerado por IA para criar carteiras de identidade falsas, forjar imagens de acidentes para reivindicações de seguro fraudulentas e até mesmo produzir raios X falsificados para explorar sistemas de saúde. À medida que as ferramentas de deepfake se tornam mais avançadas e acessíveis (e seus resultados mais convincentes), a fraude será mais difícil de detectar, minando a verificação de identidade e a confiança nas comunicações. Os setores que lidam com autenticação de identidade, transações financeiras e dados sigilosos serão os mais impactados pela fraude impulsionada por deepfake e seus riscos, tornando a detecção e defesa alimentadas por IA uma necessidade urgente.

6. Proteger a GenAI será um imperativo comercial prioritário

À medida que os aplicativos de GenAI se tornam mais incorporados às operações empresariais, proteger esses sistemas deixará de ser uma prioridade de TI para se tornar um imperativo de segurança empresarial essencial em 2025 e além. A GenAI tem a capacidade de aprender e se adaptar continuamente, tornando a segurança um alvo em movimento. Os criminosos já estão encontrando maneiras de explorar a automação orientada por IA, manipular conteúdo gerado por IA e introduzir vieses sutis de modelo que podem comprometer a tomada de decisões empresariais. As organizações precisarão redobrar a implementação de **controles de segurança eficazes** para proteger modelos de IA, proteger conjuntos de dados sigilosos e garantir a integridade do conteúdo gerado por IA.



©2025 Zscaler, Inc. Todos os direitos reservados.

Práticas_ recomendadas para a adoção segura da IA em empresas

A IA oferece vantagens poderosas, mas também introduz sérios riscos de segurança, conforme discutido nas seções anteriores. Integrar com sucesso ferramentas de IA/ML nas operações empresariais requer uma abordagem estratégica. As organizações devem seguir as práticas recomendadas e implementar políticas claras que priorizem a segurança, garantam a conformidade e promovam o uso ético.

As práticas recomendadas a seguir fornecem uma base para a adoção segura da IA.

- **Mantenha a transparência e a responsabilidade da IA.** Comunique claramente o propósito das ferramentas de IA e documente os processos de IA enquanto atribui funções de supervisão para controle responsável.
- **Cumpra os padrões legais e éticos.** Comunique claramente o propósito das ferramentas de IA e documente os processos de IA enquanto atribui funções de supervisão para controle responsável.
- **Revise e ajuste as configurações padrão.** Audite permissões e modifique as configurações padrão, que geralmente priorizam a eficiência em vez da segurança, para reduzir vulnerabilidades e minimizar riscos potenciais.
- **Avalie e mitigue continuamente os riscos de IA.** Avalie frequentemente os riscos de segurança e privacidade relacionados à IA (e comportamento de usuário) para proteger as informações da empresa, a propriedade intelectual e os dados pessoais.
- **Aplique zero trust às interações de IA.** Adote uma arquitetura zero trust que aplique acesso de privilégio mínimo e restrições de entrada/saída granulares para impedir o uso não autorizado e minimizar a superfície de ataque.
- **Fortaleça a privacidade e a segurança dos dados.** Implemente criptografia e medidas de prevenção contra perda de dados (DLP) de espectro total para proteger dados e informações proprietárias contra exposição e vazamentos.

Além das práticas recomendadas, as empresas devem estabelecer diretrizes formais de IA e regras de engajamento para controlar o uso aceitável, a integração, a segurança e o desenvolvimento de ferramentas de IA.

- **Estabeleça políticas claras de controle de IA.** Defina diretrizes para o uso responsável da IA, abordando segurança, ética, conformidade e gerenciamento de riscos.
- **Realize a devida diligência antes da implementação.** Conduza revisões abrangentes de segurança e ética para garantir que as ferramentas estejam alinhadas com as políticas corporativas e tolerância a riscos.
- **Restrinja o compartilhamento de dados sigilosos.** Impeça que modelos de IA acessem informações pessoalmente identificáveis (PII), dados proprietários ou informações comerciais confidenciais.
- **Exija revisão humana para conteúdo gerado por IA.** Garanta que todo conteúdo assistido por IA passe por uma revisão humana completa antes da publicação.
- **Garanta a supervisão humana em processos orientados por IA.** Exija intervenção e revisão humanas para impedir que a IA tome decisões empresariais críticas autônomas.
- **Adote uma estrutura de ciclo de vida de produto seguro.** Siga uma estrutura de segurança rigorosa para mitigar os riscos em cada estágio do desenvolvimento e integração de ferramentas de IA.

©2025 Zscaler, Inc. Todos os direitos reservados.

5 etapas para integrar com segurança ferramentas de GenAI

Uma abordagem estratégica e gradual é essencial para adotar aplicativos de IA com segurança. O ponto de partida mais seguro é bloquear todos os aplicativos de IA para mitigar possíveis vazamentos de dados. Em seguida, integre progressivamente ferramentas de IA verificadas com controles de acesso rigorosos e medidas de segurança para manter a supervisão completa dos dados corporativos.

As etapas a seguir descrevem um processo de adoção seguro usando o ChatGPT da OpenAI como exemplo.

Etapa 1. Bloqueie todos os domínios e aplicativos de IA e ML

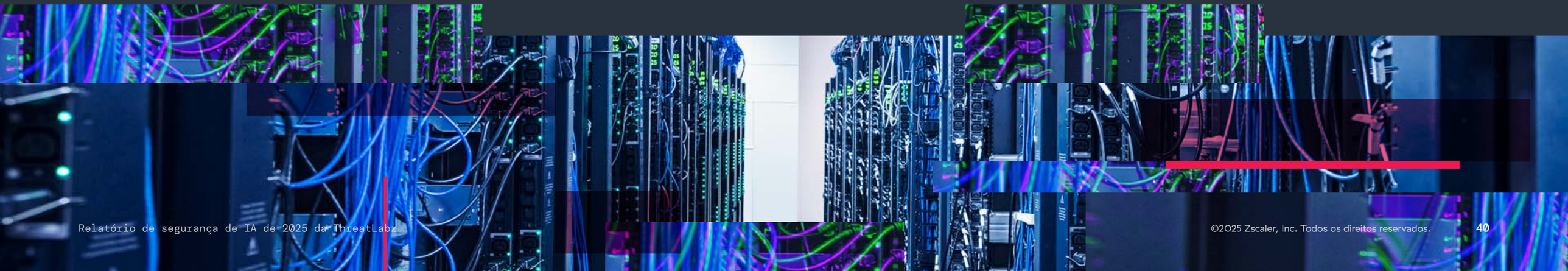
Com milhares de aplicativos de IA disponíveis, muitos deles com implicações de segurança desconhecidas, as empresas devem adotar uma postura zero trust desde o início. Ao bloquear todos os domínios de IA e ML no nível empresarial, as organizações podem eliminar riscos imediatos e se concentrar na adoção seletiva apenas das ferramentas de IA mais seguras e transformadoras.

Etapa 2. Analise e aprove aplicativos de IA generativa com critérios rigorosos

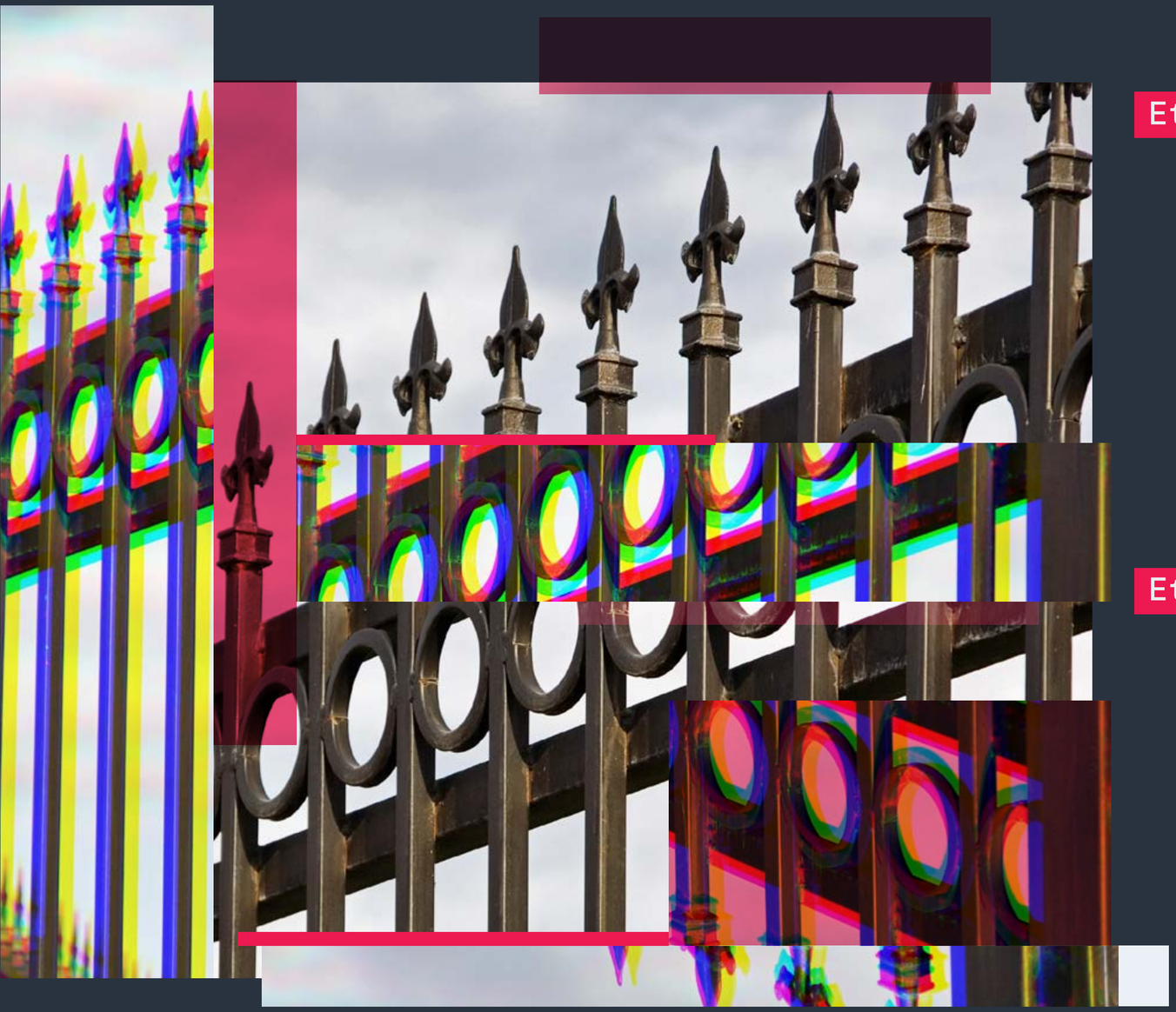
Em seguida, identifique e aprove ferramentas de IA que atendam (ou excedam) padrões rigorosos de segurança, privacidade e contratuais para proteger dados comerciais e de clientes o tempo todo, ao mesmo tempo em que oferecem valor comercial transformador. Para muitas organizações, o ChatGPT será um aplicativo essencial que exigirá considerações de segurança adicionais.

Etapa 3. Crie uma instância privada do servidor do ChatGPT para controle máximo

Para manter controle total sobre os dados corporativos, as organizações devem hospedar aplicativos de IA, como o ChatGPT, em um ambiente privado e seguro (por exemplo, um servidor de IA dedicado do Microsoft Azure) hospedado totalmente dentro da organização. Em seguida, por meio de controles de segurança e obrigações contratuais, garanta que nem a Microsoft nem a OpenAI (neste exemplo) tenham acesso aos dados da empresa ou do cliente. Essa abordagem garante a soberania dos dados e impede que fornecedores de IA manipulem dados sigilosos, evitando assim que consultas sejam usadas para treinar modelos públicos de IA e reduzindo o risco de envenenamento de dados de um data lake público.



©2025 Zscaler, Inc. Todos os direitos reservados.



Etapa 4. Proteja o acesso com SSO, MFA e controles zero trust

Em seguida, coloque aplicativos como o ChatGPT por trás de uma arquitetura de proxy de nuvem zero trust, como a Zscaler Zero Trust Exchange, para impor controles de acesso de segurança zero trust. Isso também pode incluir proteger o ChatGPT com um provedor de identidade (IdP) para logon único (SSO) com autenticação multifator (MFA) robusta que inclui autenticação biométrica. Essa abordagem garante o acesso rápido, mas seguro, dos usuários ao ChatGPT, ao mesmo tempo em que permite que as empresas definam controles de acesso precisos para usuários individuais, equipes e departamentos. Ela também mantém uma separação clara de preocupações entre as consultas dos usuários, garantindo que os dados permaneçam isolados e acessíveis somente dentro dos níveis organizacionais apropriados. Ao proteger o ChatGPT com um proxy de nuvem como a Zero Trust Exchange, as organizações podem monitorar e inspecionar todo o tráfego criptografado em TLS/SSL entre usuários e o ChatGPT para detectar ameaças potenciais e evitar vazamentos de dados.

Etapa 5. Implemente prevenção contra perda de dados (DLP) para evitar vazamentos

Por fim, é essencial aplicar um mecanismo de DLP para a instância do ChatGPT para evitar vazamento acidental de informações críticas e garantir que dados sigilosos nunca saiam do ambiente de produção.

Ao seguir essas etapas, as empresas podem aproveitar o poder da IA generativa e, ao mesmo tempo, eliminar os riscos mais críticos associados à adoção da IA.

©2025 Zscaler, Inc. Todos os direitos reservados.

Como a Zscaler oferece zero trust + IA_

À medida que a adoção da IA cresce, as organizações estão alcançando novos níveis de produtividade, eficiência e inovação, mas também estão expandindo sua superfície de ataque. Ao mesmo tempo, o surgimento da IA como arma significa ameaças mais sofisticadas, automatizadas e evasivas. As empresas devem reconhecer esses riscos e aprimorar estratégias de segurança para enfrentá-los.

Os modelos de segurança tradicionais são inadequados nesses ambientes de alto risco. Suas arquiteturas legadas, baseadas em ferramentas como firewalls e VPNs, na verdade aumentam os riscos ao expandir a superfície de ataque e permitir a movimentação lateral, permitindo que os ataques baseados em IA se espalhem mais rapidamente. Essas soluções desatualizadas exigem muito esforço manual, tornando quase impossível proteger as comunicações, adaptar-se aos riscos em evolução e responder às ameaças em tempo real.

Para prosperar na era da IA, as empresas precisam de uma abordagem fundamentalmente nova, que não apenas as protejam contra ameaças baseadas em IA, mas também permita a adoção segura da IA. Uma arquitetura zero trust é a base para as duas.

A arquitetura zero trust baseada na nuvem da Zscaler reduz drasticamente os riscos ao tornar os aplicativos e endereços IP invisíveis para os invasores, minimizando assim a superfície de ataque; inspecionando continuamente todo o tráfego, incluindo o tráfego criptografado, em busca de ameaças, evitando comprometimento; e conectando os usuários diretamente (e somente) aos aplicativos de que precisam, limitando assim o risco de movimentação lateral.

Com base nisso, a Zscaler aprimora o zero trust com proteções contra ameaças baseadas em IA para oferecer segurança incomparável contra ameaças de todos os tipos, até mesmo os ataques mais sofisticados habilitados por IA.

Como funciona: a vantagem de segurança e dados da IA da Zscaler

A inteligência da IA depende dos dados com os quais ela aprende. Como a maior nuvem de segurança em linha do mundo, a Zscaler Zero Trust Exchange protege mais de 40 milhões de usuários, cargas de trabalho, dispositivos de IoT/OT e acesso de terceiros.

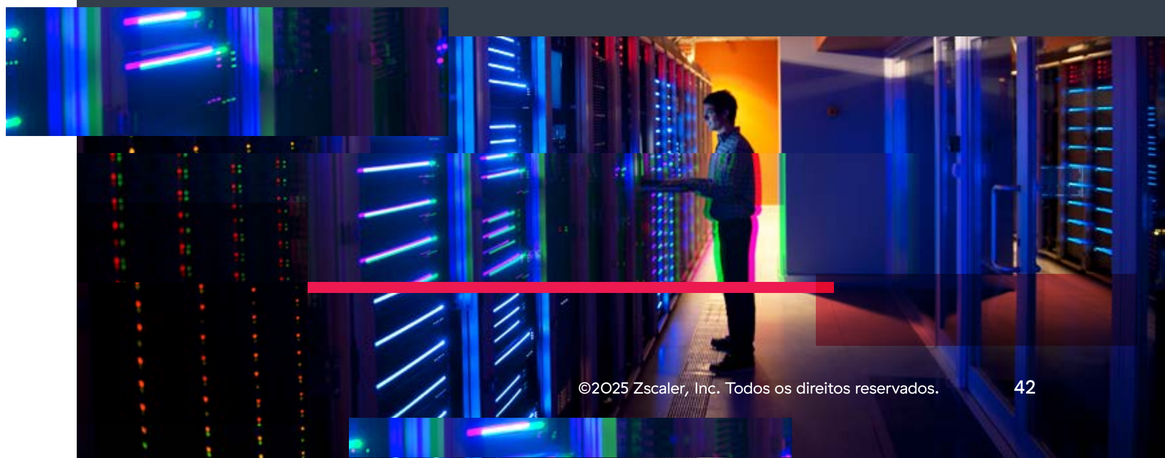
Todos os dias, a Zscaler processa:

Mais de 500 trilhões de sinais de telemetria, fornecendo insights em tempo real sobre ameaças, identidades e padrões de acesso

Mais de 500 bilhões de transações; 45 vezes o volume de pesquisas diárias do Google

Esse enorme conjunto de dados permite que a Zscaler treine modelos de IA altamente especializados que identificam e bloqueiam ameaças mais rapidamente do que as abordagens de segurança tradicionais, totalizando mais de **9 bilhões de ameaças bloqueadas diariamente.** Situada em linha entre usuários, cargas de trabalho e dispositivos, a Zscaler tem profunda visibilidade das ameaças cibernéticas corporativas, tornando seus modelos de IA mais adaptáveis, precisos e eficazes.

O data fabric da Zscaler também **se integra perfeitamente com mais de 150 ferramentas de segurança e negócios,** incluindo **mais de 60 feeds de inteligência sobre ameaças.**



©2025 Zscaler, Inc. Todos os direitos reservados.

Uma abordagem abrangente à segurança de IA

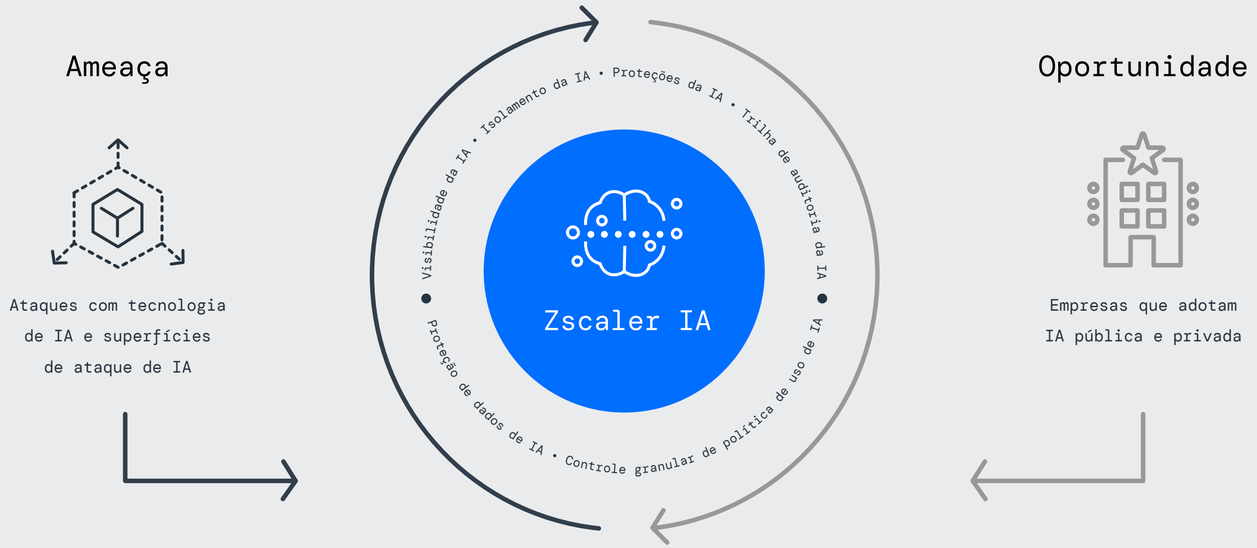
Integrar a IA com sucesso na empresa e se defender contra ameaças baseadas em IA exige uma estratégia abrangente. Com Zscaler Zero Trust + IA, as empresas podem adotar com confiança e segurança a IA pública e privada, ao mesmo tempo em que protegem dados, aplicativos e modelos de IA contra ameaças em evolução impulsionadas por IA.

Ao oferecer visibilidade total sobre usuários e aplicativos que interagem com ferramentas de IA públicas e privadas, a Zscaler IA permite que as empresas implantem políticas contextuais que controlam o acesso e o uso. Sua inspeção de prompts em linha garante a proteção de dados sigilosos e dos próprios modelos de IA contra atividades maliciosas e perda de dados.

“Não tínhamos visibilidade do [ChatGPT]. A Zscaler foi nossa principal solução inicialmente para nos ajudar a entender quem estava acessando e o que eles estavam enviando.”

— Jason Koler, CISO, Eaton Corporation

Ver estudo de caso em vídeo



©2025 Zscaler, Inc. Todos os direitos reservados.

A Zscaler IA permite que as organizações:

Ofereçam com segurança o uso de IA pública, maximizando a velocidade dos negócios e minimizando os riscos de IA paralela e perda de dados.

- **Visibilidade de IA:** veja todos os aplicativos e interações de IA, incluindo prompts e respostas.
- **Isolamento de IA:** permita o uso de ferramentas de IA e evita que dados sigilosos sejam compartilhados inadvertidamente.
- **Proteções de IA:** bloqueie ameaças como injeções de prompt, exposição de PII, envenenamento de dados e mais.
- **Controle granular de política de uso de IA:** bloqueie aplicativos de IA não autorizados ou paralelos e controle o acesso e o uso com base em quem está usando a IA e como.
- **Proteção de dados de IA:** bloqueie o compartilhamento e a exfiltração de dados para evitar violações de dados.
- **Trilha de auditoria de IA:** mantenha registros detalhados de todas as interações de IA: usuários, prompts, respostas e aplicativos.

Impeçam ataques com tecnologia de IA por meio de zero trust + segurança com tecnologia de IA.

- **Base zero trust:** minimize a superfície de ataque externa por meio de verificação contínua e acesso de privilégio mínimo.
- **Insights de IA em tempo real:** empregue IA preditiva e generativa para fornecer insights práticos que aprimoram as operações de segurança e o desempenho digital.
- **Classificação de dados:** aproveite a classificação orientada por IA para detectar e proteger perfeitamente dados sigilosos no Data Fabric da Zscaler.
- **Proteção contra ameaças:** bloqueie ameaças aprimoradas por IA por meio de monitoramento e resposta contínuos fornecidos pela Zscaler Zero Trust Exchange.
- **Segmentação de aplicativos:** reduza sua superfície de ataque interna e restrinja a movimentação lateral com segmentação automática orientada por IA.
- **Previsão de violações:** previna possíveis cenários de violações usando IA generativa e modelos preditivos multidimensionais.
- **Avaliações de risco cibernético:** aproveite relatórios de segurança gerados por IA para mapear e otimizar sua implementação zero trust.

©2025 Zscaler, Inc. Todos os direitos reservados.

Os principais recursos de IA da Zscaler incluem:

- **Detecção de phishing e C2 baseada em IA** usa a detecção integrada baseada em IA do **Zscaler Secure Web Gateway** para identificar e bloquear sites de phishing nunca antes vistos e infraestrutura de comando e controle (C2).
- **Bloqueio inteligente de prompt de entrada:** usa filtragem de URL baseada em IA/ML entre categorias de aplicativos para decisões mais inteligentes de bloqueio de prompts com base no risco contextual.
- **Sandboxing:** emite vereditos instantâneos sobre ameaças potenciais, prevenindo malware e ransomware de dia zero antes que eles possam impactar usuários ou terminais.
- **Zero Trust Browser:** isola conteúdo suspeito da internet e renderiza páginas web como imagens perfeitas, mantendo conteúdo malicioso longe dos usuários.
- **Segmentação:** mapeia automaticamente as conexões de usuário para aplicativo, simplificando as políticas de acesso zero trust para minimizar a superfície de ataque e impedir a movimentação lateral.
- **Políticas dinâmicas baseadas em risco:** analisa continuamente os riscos do usuário, do dispositivo e do aplicativo para aplicar políticas de segurança adaptáveis.
- **Previsão de violações:** utiliza algoritmos baseados em IA para analisar dados de segurança, usando gráficos de ataque, pontuação de risco do usuário e inteligência sobre ameaças para prever possíveis violações.
- **Avaliações de maturidade de segurança:** avalia continuamente a postura de segurança zero trust, fornecendo insights dinâmicos e recomendações práticas para reduzir ainda mais o risco cibernético.
- **Proteção de dados:** oferece descoberta e classificação automática de dados com tecnologia de IA em dados de terminais, em linha e na nuvem. Os controles de prevenção contra perda de dados (DLP) orientados por IA garantem que dados corporativos sigilosos não possam ser extraídos por meio de prompts de entrada de IA.



©2025 Zscaler, Inc. Todos os direitos reservados.

Uso da segurança de IA em toda a cadeia de ataque

A Zscaler aplica IA em todas as etapas da cadeia de ataque, garantindo que as ameaças sejam detectadas e neutralizadas antes que possam causar danos.

Etapa 1: descoberta da superfície de ataque

O primeiro passo de um ataque geralmente é o reconhecimento: varrer a internet em busca de vulnerabilidades em VPNs, firewalls, servidores mal configurados ou ativos sem correção. A IA facilitou esse processo para os criminosos, permitindo que eles consultem vulnerabilidades conhecidas quase instantaneamente.

Como a Zscaler usa IA para eliminar a superfície de ataque:

- Com insights baseados em IA do Zscaler Risk360, as empresas podem mapear e proteger automaticamente seus ativos voltados para a internet, tornando-os invisíveis para os usuários. Ao ocultar esses ativos por trás da Zero Trust Exchange, as organizações reduzem drasticamente sua superfície de ataque, interrompendo as ameaças antes mesmo que elas comecem.



Etapa 2: risco de comprometimento

Quando os invasores encontram uma fraqueza, eles tentam explorar vulnerabilidades, roubar credenciais ou obter acesso não autorizado. O uso crescente de exploits gerados por IA e e-mails de phishing aumenta ainda mais o risco de comprometimento, permitindo que invasores ignorem os controles de segurança tradicionais e tornando a detecção e a resposta em tempo real essenciais.

Como a Zscaler usa IA para mitigar o risco de comprometimento:

- **Os modelos de IA da Zscaler se baseiam em uma combinação de inteligência sobre ameaças**, pesquisas da ThreatLabz e isolamento do navegador baseado em IA para detectar sites de phishing conhecidos e de paciente zero, prevenindo o roubo de credenciais e a exploração de navegador. Eles analisam padrões de tráfego, comportamento e malware para identificar infraestrutura de comando e controle (C2) em tempo real. Como resultado, as empresas são ainda mais eficientes e eficazes na detecção de domínios de C2 e ataques de phishing.

- **O Zscaler Zero Trust Browser com tecnologia de IA** reduz automaticamente o risco de ameaças baseadas na web e ameaças de dia zero, ao mesmo tempo em que garante que os funcionários possam acessar os sites certos para fazer seus trabalhos. O AI Smart Isolation identifica conteúdo suspeito da internet e o abre em um ambiente seguro e isolado. Isso efetivamente interrompe ameaças baseadas na web, como malware, ransomware e phishing.

- **A Zscaler Cloud Sandbox** detecta, previne e coloca em quarentena de forma inteligente ameaças desconhecidas e arquivos suspeitos em linha. Com vereditos baseados em IA, os arquivos benignos são entregues instantaneamente, enquanto os arquivos maliciosos são bloqueados para todos os usuários globais da Zscaler. Isso efetivamente impede que ameaças baseadas na web, como malware, ransomware, phishing e downloads drive-by, tenham acesso a uma rede.

©2025 Zscaler, Inc. Todos os direitos reservados.

Etapa 3: movimentação lateral

Uma vez dentro, os invasores tentam se mover lateralmente dentro de uma organização, buscando privilégios elevados ou dados e aplicativos valiosos. Cada vez mais, eles usam ferramentas de IA para mapear rapidamente rotas para comprometimento mais profundo. Muitas empresas também sofrem com direitos de acesso superprovisionados, tornando mais fácil para os invasores se moverem entre ambientes sem serem detectados.

Como a Zscaler usa IA para evitar a movimentação lateral:

- A Zscaler IA analisa continuamente o comportamento do usuário e os padrões de acesso, recomendando políticas inteligentes de segmentação de aplicativos para limitar a movimentação lateral. Por exemplo, se apenas 200 de 30.000 funcionários precisarem de acesso a um aplicativo, a Zscaler pode segmentar automaticamente o acesso apenas a esses usuários, reduzindo o risco de movimentação lateral em mais de 90%.

Etapa 4: exfiltração de dados

A etapa final de um ataque é a exfiltração de dados, onde os invasores tentam roubar dados como IP, informações de clientes ou registros financeiros.

Como a Zscaler usa IA para impedir a perda de dados:

- A descoberta de dados com tecnologia de IA acelera a visibilidade dos dados e automatiza a classificação de dados em tempo real em toda a empresa. Ative instantaneamente políticas de prevenção contra perda de dados (DLP) para impedir que os dados saiam da organização.

Proteção de IA para 2025: um apelo à ação_

A IA é uma força de progresso, ruptura e risco, pressionando as organizações empresariais a se adaptarem a todo momento. Ela continuará a desbloquear novas eficiências e inovações, mas também introduzirá novas ameaças, desde ataques cibernéticos com tecnologia de IA até manipulação adversária de modelos e dados.
Para aproveitar com segurança todo o potencial da IA e, ao mesmo tempo, mitigar seus riscos, as empresas devem recorrer ao zero trust + IA.

A segurança de IA da Zscaler protege cada estágio da adoção da IA e garante proteção em todas as etapas de um ataque. Ao adotar uma abordagem proativa, as organizações podem transformar a IA em uma vantagem competitiva, desbloqueando novas possibilidades e, ao mesmo tempo, se antecipando às ameaças em evolução.

©2025 Zscaler, Inc. Todos os direitos reservados.

Metodologia de pesquisa_

As descobertas são baseadas na análise de 536,5 bilhões de transações totais de IA e ML na nuvem da Zscaler de fevereiro de 2024 a dezembro de 2024. A nuvem de segurança global da Zscaler processa mais de 500 trilhões de sinais diários e bloqueia mais de 9 bilhões de ameaças e violações de políticas por dia, fornecendo mais de 250 mil atualizações de segurança diárias.

Sobre a ThreatLabz

ThreatLabz é o braço de pesquisa de segurança da Zscaler. Essa equipe de classe mundial é responsável por perseguir novas ameaças e garantir que as milhares de organizações que usam a plataforma global Zscaler estejam sempre protegidas. Além da pesquisa de malware e análise comportamental, os membros da equipe estão envolvidos na pesquisa e no desenvolvimento de novos módulos para proteção avançada contra ameaças na plataforma Zscaler, e realizam regularmente auditorias internas de segurança para garantir que os produtos e a infraestrutura da Zscaler atendam aos padrões de conformidade de segurança. A ThreatLabz publica regularmente análises aprofundadas de ameaças novas e emergentes em seu portal, **research.zscaler.com/br**.

Sobre a Zscaler

A Zscaler (NASDAQ: ZS) acelera a transformação digital para que seus clientes possam ter mais agilidade, eficiência, resiliência e segurança. A Zscaler Zero Trust Exchange™ protege milhares de clientes contra ataques cibernéticos e perda de dados, conectando com segurança usuários, dispositivos e aplicativos em qualquer local. Distribuída em mais de 160 data centers globalmente, a Zero Trust Exchange baseada em SASE é a maior plataforma integrada de segurança na nuvem do mundo. Para saber mais, visite **www.zscaler.com/br**.

©2025 Zscaler, Inc. Todos os direitos reservados.

Zero Trust Everywhere

©2025 Zscaler, Inc. Todos os direitos reservados. Zscaler™ e outras marcas registradas listadas em zscaler.com/br/legal/trademarks são (i) marcas registradas ou marcas de serviço ou (ii) marcas comerciais ou marcas de serviço da Zscaler, Inc. nos Estados Unidos e/ou em outros países. Quaisquer outras marcas registradas são de propriedade de seus respectivos detentores.