E-book

5 mitos sobre a IA de segurança cibernética desmascarados

Um guia para equívocos gerais sobre a IA, oportunidades e o Microsoft Copilot para Segurança

Microsoft Security

Conteúdo

Introdução

Uma nova era da IA chegou, juntamente com novos equívocos

As ameaças cibernéticas estão aumentando, em número e gravidade, e as equipes de segurança estão lutando para acompanhar o ritmo das ferramentas tradicionais de segurança cibernética. É por isso que muitos líderes de segurança estão recorrendo a soluções da plataforma IA.

Essas ferramentas transformadoras oferecem uma oportunidade para enfrentar seus maiores desafios de segurança e podem ser um divisor de águas para sua equipe de segurança. Equipados com soluções de IA generativas, seus profissionais de segurança podem proteger mais, mover-se mais rapidamente e ganhar uma vantagem sobre os criminosos cibernéticos. Além disso, eles gastarão menos tempo realizando tarefas tediosas e mais tempo tomando decisões estratégicas e proativas.

Como as soluções de segurança cibernética com IA generativas são novas, talvez você hesite em adotar essas ferramentas. Como líder de segurança, é natural ter dúvidas sobre qualquer nova tecnologia. Na verdade, é um sinal de que você é bom no seu trabalho. Mas quando você trabalha com um parceiro de tecnologia confiável, descobrirá que as recompensas da IA generativa superam em muito os riscos.

Este e-book vai explorar e desmascarar os cinco mitos mais comuns sobre ferramentas de segurança cibernética de IA generativas, incluindo:

1. Acesso não autorizado aos dados
2. Privacidade e propriedade de dados
3. Vazamento e exposição de dados
4. Problemas de conformidade
5. Alucinações

Continue lendo para se aprofundar nesses mitos e descobrir como o Microsoft Copilot para Segurança aborda cada um com controles internos de segurança, conformidade e privacidade.

1

O caso da IA na segurança cibernética

Os ciberataques estão crescendo cada vez mais predominantes, coordenados e sofisticados. No ano passado, o número de ataques de senha detectados pela Microsoft disparou de 579 para mais de 4.000 por segundo.[1] Como a maioria das organizações usa dezenas de ferramentas de segurança cibernética para gerenciar seu ambiente, as equipes de segurança de hoje enfrentam um dilúvio de dados, fadiga de alerta e visibilidade limitada em várias soluções – tudo isso enquanto lidam com uma escassez global de talentos e complexidade regulatória.

As chances estão contra os analistas de segurança de hoje:

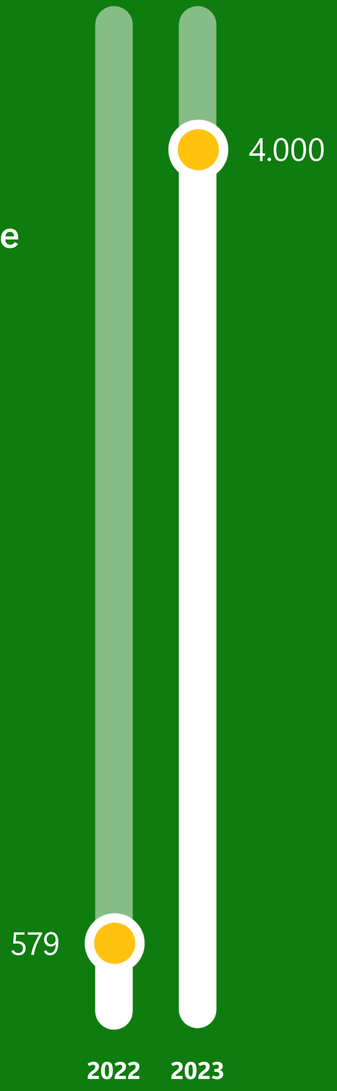
- 4.000: ataques de senha por segundo
- 72 minutos: o tempo médio necessário para um invasor acessar seus dados privados se você abrir um email de phishing
- 3,5 milhões: escassez global de profissionais qualificados em segurança cibernética

É por isso que é mais importante do que nunca fornecer às suas equipes de segurança soluções inovadoras que as ajudem a detectar, investigar e responder rapidamente à escalada de ciberameaças. Para navegar pelos desafios complexos de hoje, os líderes de segurança estão procurando:

- Mais automação e ferramentas que trabalham juntas para ajudar suas equipes de segurança a superar e superar os ciberataques.
- Maneiras de fortalecer a experiência de sua equipe e aliviar tarefas tediosas para que ela possa se concentrar na proteção de sua organização.
- Soluções que ajudam seus analistas a ver mais e mover-se mais rapidamente, para que possam detectar e responder a incidentes antes que causem danos.

A IA é a chave para tornar tudo isso possível.

Muitas equipes de segurança já estão ganhando vantagem com soluções com a IA. E o impacto é real.



[1] Relatório de Defesa Digital da Microsoft 2023.

O Microsoft Copilot para Segurança representa um avanço inovador para as equipes de Operações de Segurança no mundo todo. Por meio do nosso serviço global Microsoft MXDR [detecção e resposta estendidas gerenciadas], estamos vendo até 40% de redução no tempo de resolução de incidentes ao modelar em relação aos processos atuais.

Além disso, ela aprimora significativamente o ambiente de trabalho dos analistas do SOC (Centro de Operações de Segurança), servindo como assistente de segurança de IA para operações diárias.

Jason Revill
Líder do Centro de Excelência Global, Avanade

A inteligência artificial será um componente crítico da defesa bem-sucedida. Nos próximos anos, a inovação na defesa cibernética da plataforma IA ajudará a reverter a atual maré crescente de ciberataques.

— Tom Burt
Vice-presidente Corporativo, Segurança e Confiança do Cliente, Microsoft

Para enfrentar desafios de segurança cibernética cada vez mais complexos, muitas equipes de segurança estão adotando ferramentas de IA generativas, como o Microsoft Copilot para Segurança, que aprimoram a experiência humana com insights inteligentes e fluxos de trabalho automatizados.

O Copilot para Segurança é um assistente de IA para operações diárias em segurança e TI. Essa solução generativa com IA foi projetada para ajudar as equipes de segurança a serem mais rápidas, produtivas e precisas. Com o Copilot, as equipes de segurança obtêm insights personalizados com base na inteligência global contra ameaças, nas práticas recomendadas da indústria e nos dados de segurança de suas organizações. Esses insights acionáveis fornecem aos profissionais de segurança o conhecimento necessário para superar e superar os ciberataques.

40%

do tempo é economizado por analistas que usam o Copilot para tarefas típicas de operações de segurança

60%

do tempo é economizado por analistas que usam o Copilot para tarefas tediosas, como triagem de alertas e relatórios[2]

[2] Dados antecipados do cliente do Microsoft Copilot para Segurança, 2023.

2

5 mitos sobre soluções de segurança da plataforma IA desmascarados

Embora esteja claro que a IA generativa pode ajudar a amplificar o impacto das equipes de segurança, alguns líderes desconfiam de mergulhar imediatamente sem uma cuidadosa consideração. É razoável hesitar sobre qualquer nova tecnologia e curioso sobre seu potencial impacto em sua equipe e organização. É por isso que é importante fazer sua pesquisa.

Aqui estão as cinco principais preocupações dos líderes de segurança sobre a IA generativa – e como o Copilot para Segurança foi criado para enfrentá-los.

Mito 1:

Acesso não autorizado aos dados

Alguns líderes de segurança estão preocupados que, se um usuário não autorizado fizer uma pergunta a uma ferramenta com IA, poderá obter uma resposta que inclua informações que o usuário não está autorizado a ver. Mas esse não é o caso.

A segurança de dados é a principal preocupação para as organizações que adotam novas ferramentas de IA generativas. Quando qualquer usuário não autorizado, interno ou externo, obtém acesso aos dados, isso pode interromper os negócios e colocar a reputação de uma organização em risco. Para gerar respostas úteis para consultas, aplicações de IA generativos podem ter acesso a dados confidenciais. No entanto, o aplicativo só mostrará ao usuário aquilo ao que ele tem acesso para ver.

Pergunta frequente:
Os usuários não autorizados podem obter acesso a dados confidenciais com o Copilot?

Resposta: Não.

Isso não acontecerá com o Copilot porque ele usa direitos de "administrar em nome de" para o usuário conectado. Isso significa que os direitos são limitados somente a esse usuário específico e a esse usuário. O Copilot executa consultas como o usuário, portanto, ele nunca tem privilégios elevados além do que o usuário tem.

Mito 2:

Privacidade e propriedade de dados

Garantir a privacidade dos dados é essencial para que uma organização crie uma cultura de transparência, ganhe a confiança do cliente e atenda aos regulamentos de conformidade. Ao considerar soluções de IA generativa, os líderes de segurança estão preocupados com o fato de que os dados de seus clientes serão usados para treinar outros modelos, o que pode comprometer a reputação da organização. Isso não acontecerá quando você trabalhar com um parceiro de tecnologia confiável.

Pergunta frequente:
os dados do meu cliente serão usados para treinar modelos de linguagem no Copilot?

Resposta: Não.

Na Microsoft, estamos definindo o padrão de segurança, privacidade e conformidade quando se trata de IA. Isso não é verdade apenas para o Copilot para Segurança, mas para todas as nossas ofertas de IA.

Por padrão, a Microsoft não treina modelos de linguagem em dados do cliente. Há uma funcionalidade de aceitação dedicada no Copilot para clientes que optam por contribuir para a segurança coletiva e a inovação na IA.

Quando se trata de dados, ao contrário do ChatGPT, o Copilot é fundamentado no contexto único da sua organização. Isso significa que quando você fizer qualquer pergunta ao Copilot, a resposta se baseará no que está acontecendo em sua organização naquele momento. Seus dados não são usados para treinar os modelos de IA básicos. É um loop de aprendizado fechado que melhora continuamente com base no seu uso.

Criada com segurança, privacidade e conformidade

Esses dados são de sua propriedade.

Seus dados não são usados para treinar os modelos de IA básicos.

Seus dados são protegidos pelos controles de conformidade e segurança corporativos mais abrangentes.

Pergunta frequente:
os dados transferidos são protegidos contra acesso não autorizado?

Resposta: Sim.

Nenhum usuário humano tem acesso ao banco de dados, e o acesso é restrito à rede privada onde a aplicação Copilot para Segurança está implantada. Se for necessário acesso para que um ser humano responda a um incidente, o engenheiro de plantão precisará de acesso elevado e acesso à rede aprovados por funcionários autorizados do Microsoft. O Copilot atende a todos os requisitos de privacidade, segurança e conformidade da Microsoft.

Ao usar o Copilot para Segurança, seus dados:

- São seus dados.
- São armazenados onde você escolhe e sempre criptografados em repouso.
- Não são usados para vendas ou compartilhados com terceiros.
- Estão alojados em sistemas regidos pela Microsoft SOC e pelos processos certificados pela International Organization for Standardization.
- Não são usados para treinar modelos de IA de base.
- Nunca são compartilhados com o OpenAI.
- São protegidos pelos controles de conformidade e segurança corporativos mais abrangentes.

Habilitado por dados exclusivos para você e sua organização

Mito 3:

Vazamento e exposição de dados

No ano passado, 74% das organizações sofreram um incidente que expôs dados de negócios, como propriedade intelectual.[3] As violações de dados são extremamente dispendiosas para as organizações, e não apenas no sentido financeiro. Esses incidentes também diminuem a confiança dos clientes que podem se tornar vítimas de roubo de identidade, fraude de cartão de crédito ou outras atividades maliciosas devido à violação. Com tanto em jogo, os líderes de segurança estão compreensivelmente preocupados que novas tecnologias, como a IA generativa, possam levar ao vazamento de dados.

Pergunta frequente:
O Copilot poderia expor meus dados a outras pessoas usando a ferramenta?

Resposta: Não.

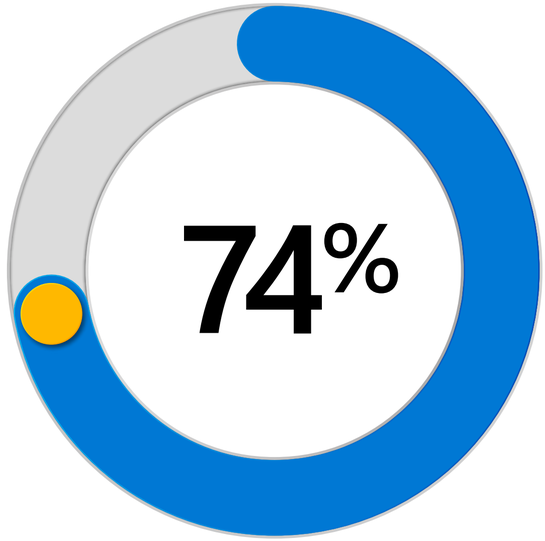
O Copilot para Segurança foi projetado com base na IA responsável. Ele inclui os mesmos controles de segurança, privacidade e conformidade que outros produtos da Microsoft confiáveis, bem como mecanismos de segurança específicos da IA. Seus dados são analisados no sistema do Copilot e não deixam o locatário de produção do Microsoft Azure. De acordo com os padrões da Microsoft, seus dados são criptografados em trânsito e em repouso.

Além disso, os dados da sessão são armazenados somente em logs e para fins de tempo de execução para operar o serviço. No banco de dados de tempo de execução, quando uma sessão é excluída usando a experiência do usuário (UX) no produto, todos os dados associados a essa sessão são marcados como excluídos e o tempo de vida (TTL) é definido como 30 dias. Depois que o TTL expirar, os dados não poderão ser acessados por consultas. Nesse momento, os dados são excluídos fisicamente por um processo em segundo plano.

Além disso, há backups periódicos de banco de dados, que ficarão mais longos. Eles têm períodos de retenção de curta duração.

Copilot:

- Executa consultas como seu usuário e, portanto, ele nunca tem privilégios elevados.
- É um serviço de produção do Azure e é protegido por controles de segurança da Microsoft.[4]
- Armazena dados limitados (contexto de investigação e logs) e criptografa todos os dados que usa em repouso.
- Está no limite de dados da UE — um limite geograficamente definido no qual a Microsoft se comprometeu a armazenar e processar dados de clientes e dados pessoais para serviços corporativos online.



das organizações tiveram um incidente que expôs dados de negócios

[3] Índice de segurança de dados, Microsoft, outubro de 2023
[4] Proteção de dados do cliente no Azure, Microsoft Learn

Mito 4:

Problemas de conformidade

Ajudar sua organização a atender aos requisitos de conformidade pode ser um dos desafios de negócios mais exigentes que você enfrenta como líder de segurança. Muitas organizações devem cumprir uma série de requisitos regulatórios e de negócios rigorosos que variam de acordo com a região e a indústria. Em alguns casos, a não conformidade pode resultar em penalidades financeiras ou fazer com que sua organização perca o acesso a um segmento inteiro do mercado. Considerando as complexidades do cenário de conformidade atual, alguns líderes de segurança estão preocupados que novas soluções de IA generativa não atendam aos requisitos. Com soluções confiáveis como o Copilot, isso não é um problema.

Pergunta frequente:
o Copilot para Segurança atende aos requisitos de conformidade regional ou da indústria?

Resposta: Sim.

O Copilot atende aos requisitos do GDPR (Regulamento Geral sobre a Proteção de Dados) para os mercados da UE implementando os requisitos da Versão Preliminar Pública do Azure. Ele armazena todos os dados de clientes da UE dentro do Limite de Dados da UE e está disponível em vários idiomas. O Copilot também fornece controles de conformidade para ajudá-lo a atender aos requisitos de negócios e regulamentações.

A IA aumenta a experiência humana, não o contrário.

Mito 5:
Alucinações

Contos de precaução sobre um fenômeno da IA chamado alucinações tornaram-se muito comuns. Uma alucinação é o conteúdo gerado por um modelo de linguagem que parece plausível, mas é factualmente incorreto ou irrelevante. Ele aparece como conhecimento qualificado e é entregue em uma resposta confiante, mas é falso.

Essas alucinações se tornam um problema ainda maior quando os humanos:

- Aceitam o conteúdo como fato sem verificação.
- Supõem que o conteúdo esteja livre de preconceitos ou desinformação.
- Confiam no conteúdo para decisões críticas sem a entrada ou supervisão humana.

Embora essa seja uma preocupação compreensível, as alucinações não são um problema quando você usa soluções transparentes de IA que capacitam os seres humanos a tomar suas próprias decisões.

Pergunta frequente:
O Copilot para Segurança ajuda a detectar alucinações?

Resposta: Sim.

A confiança é fundamental na segurança. Se você não puder confiar em dados e insights de segurança, não poderá alcançar os resultados certos. Para que os seres humanos trabalhem com confiança com ferramentas com IA, como o Copilot, é fundamental conquistar a confiança na tecnologia.

Na Microsoft, estamos comprometidos com a IA responsável, razão pela qual o Copilot foi projetado para:

- Mostrar raciocínio, fontes, depuração e runtime.
- Garantir que os dados estejam em conformidade, seguros e privados.
- Abordar danos e alucinações.
- Ser transparente e permitir um diálogo aberto.

Com ou sem alucinações, é fundamental que as pessoas sempre se sintam confiantes de que estão no controle ao usar ferramentas da plataforma IA. A IA aumenta a experiência humana, não o contrário.

Com o Copilot, a meta é ajudar as equipes de segurança a alcançar resultados de segurança positivos de forma mais eficiente sem uma dependência excessiva da IA. Os analistas de segurança recebem sugestões do Copilot para ajudá-los a agir em relação a insights, mas cabe a eles decidir se e como usar essas recomendações.

Em outras palavras, o ser humano decide o que confiar, o que compartilhar, o que é importante, o que é relevante e quando e como agir. Os usuários do Copilot não podem apenas controlar e classificar a saída da IA, mas também editar e corrigir as saídas de IA e fornecer comentários.

A criatividade e o conhecimento humanos sempre serão imperativos para a segurança cibernética. O Copilot foi projetado para complementar as habilidades e a experiência da sua equipe de segurança para que eles possam trabalhar de forma mais rápida, precisa e proativa.

3

Ofereça à sua equipe de segurança uma vantagem com a IA generativa líder da indústria

À medida que as capacidades com IA se tornam mais prevalentes em segurança cibernética, e as ameaças cibernéticas se tornam cada vez mais complexas, a IA generativa está rapidamente se tornando essencial para SOCs. O Microsoft Copilot para Segurança é uma solução abrangente e geral de segurança cibernética de IA que pode ajudar você a:

- Capacitar talentos de segurança cibernética com os insights e conhecimentos necessários para entender o que está acontecendo no ambiente e agir.
- Avançar o trabalho de membros de equipe menos experientes por meio de orientação passo a passo e aliviar tarefas tediosas para a equipe sênior para que eles possam se concentrar em prioridades mais estratégicas.
- Colocar a orientação e o contexto essenciais nas mãos de sua equipe de segurança para que possa responder a incidentes em minutos, e não em horas ou dias.
- Simplificar os relatórios e preparar relatórios personalizáveis para sua equipe de liderança executiva e conselho de administração.
- Transformar grandes quantidades de sinais de dados em insights importantes para reduzir o ruído, detectar e responder a ameaças cibernéticas em minutos e reforçar sua postura de segurança.

Aumentar a produtividade a novos níveis com o Copilot para Segurança

O Microsoft Office of the Chief Economist conduziu um estudo[5] para testar os ganhos de produtividade obtidos pelos profissionais de segurança obtidos com o Copilot para Segurança, e os resultados superaram as expectativas.

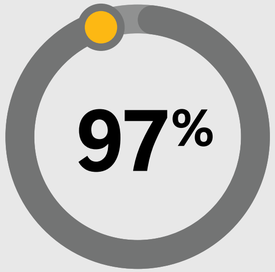
Usando o Copilot para Segurança, os profissionais de segurança foram:

- 22% mais rápidos em todas as tarefas
- 7% mais precisos em todas as tarefas
- 14% mais rápidos na análise de scripts
- 12% mais precisos na análise de script
- 39% mais rápidos ao resumir um incidente

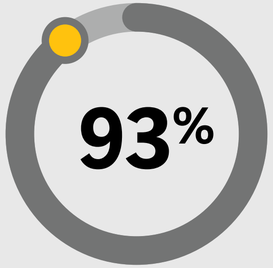
Além disso, os analistas que usam o Copilot para Segurança criaram resumos de incidentes com 49% mais fatos sobre incidentes.

[5] O RTC (trial controlado aleatório) do Microsoft Copilot para Segurança com analistas de segurança experientes conduzido pelo Escritório do economista-chefe da Microsoft, janeiro de 2024.

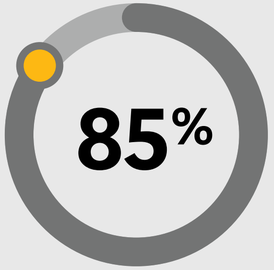
Quando perguntado sobre sua experiência:



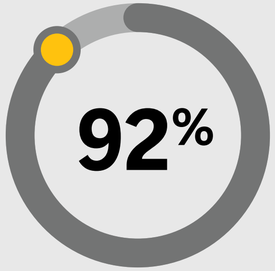
97% dos profissionais de segurança disseram que querem o Copilot na próxima vez que realizarem a mesma tarefa.



93% relataram que o Copilot ajudou a melhorar a qualidade do trabalho.



85% relataram que Copilot reduziu o esforço em tarefas.



92% relataram que o Copilot os tornou mais produtivos.

Com o Copilot, você também receberá os principais sinais de inteligência contra ameaças e ameaças de todo o mundo. A inteligência contra ameaças está em constante evolução, por isso é fundamental que as organizações se mantenham atualizadas.

Inteligência contra Ameaças da Microsoft:

- Sintetiza 65 trilhões de sinais por dia, em todos os tipos de dispositivos, aplicativos, plataformas e pontos de extremidade, usando a IA líder da indústria.
- Protege mais de 1,4 bilhão de pontos de extremidade em todo o planeta, compreendendo dispositivos móveis, servidores, dispositivos IoT e PCs.
- Cria gráficos de toda a Internet todos os dias para mapear ciberataques e sua infraestrutura.

Além disso, 8.500 engenheiros e pesquisadores de segurança da Microsoft estão trabalhando duro para investigar mais fundo em sinais desconhecidos para determinar sua verdadeira natureza.

Todos os clientes do Copilot para Segurança obtêm acesso premium de bancada o MDTI (Informações sobre Ameaças do Microsoft Defender) sem nenhum custo adicional (API não incluída). O MDTI ajuda você a acessar, ingerir e agir diretamente sobre o enorme repositório da Microsoft de inteligência contra ameaças acabada e bruta para expor e neutralizar ciberataques.

Bem-vindo(a) a uma nova era na segurança cibernética

Se você quiser superar os ciberataques na era da IA, é mais importante do que nunca equipar sua equipe com ferramentas de segurança de última geração. Capacite seus analistas a ganhar uma vantagem contra ciberameaças com controles internos de segurança, conformidade e privacidade do Microsoft Copilot para Segurança.

Saiba mais sobre o Microsoft Copilot para Segurança