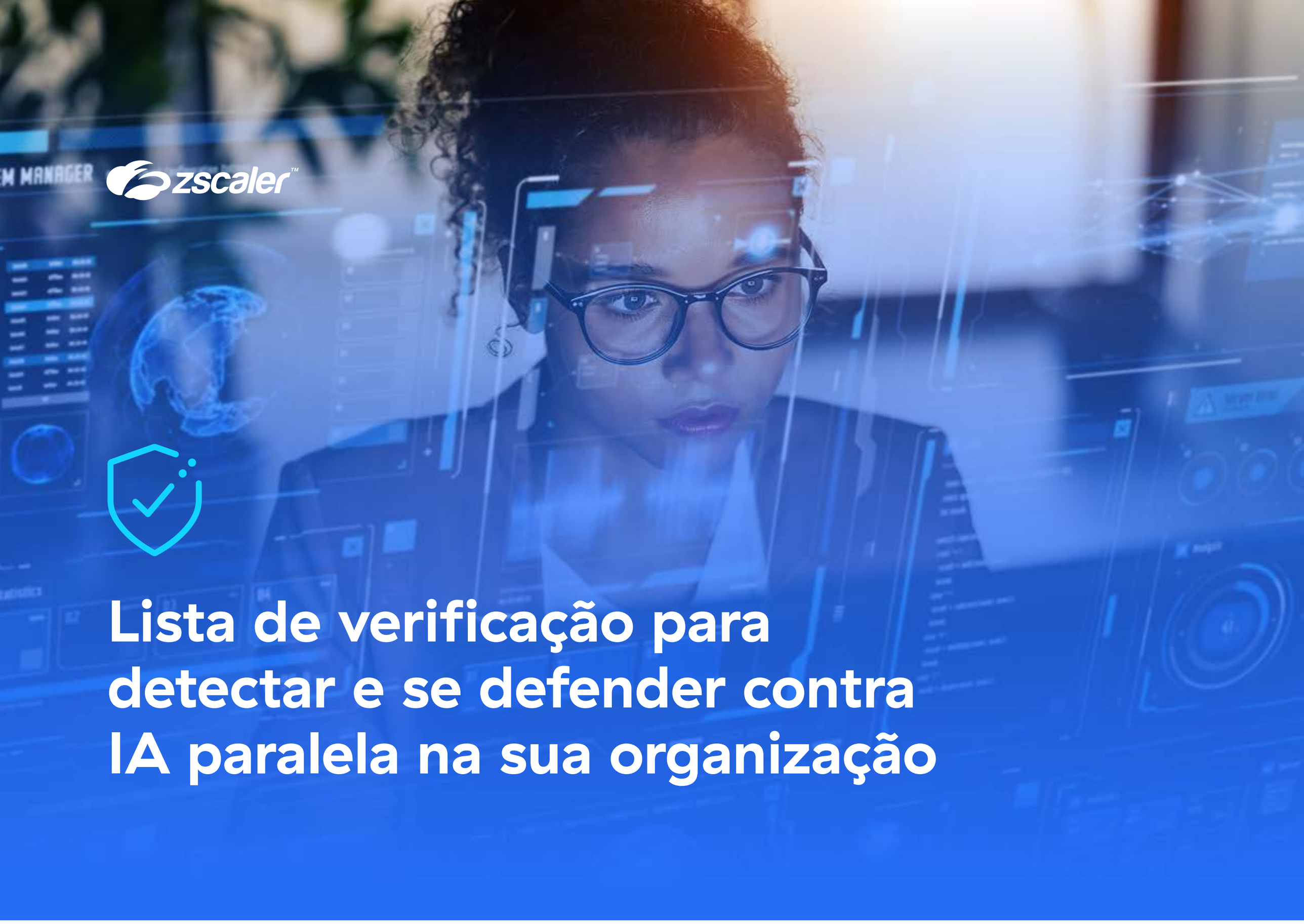


Lista de verificação para detectar e se defender contra IA paralela na sua organização

A inteligência artificial generativa (GenAI) está remodelando a forma como os funcionários trabalham e expandindo a superfície de ataque das empresas. Embora ferramentas como ChatGPT, Gemini e Claude ofereçam ganhos de produtividade significativos, seu uso não autorizado (conhecido como IA paralela) pode introduzir silenciosamente sérios riscos à segurança de dados e à conformidade.

Os funcionários estão recorrendo cada vez mais a esses sistemas de GenAI para gerar e-mails, resumir documentos ou escrever código. Mas, sem a supervisão do setor de TI, eles podem acidentalmente enviar dados sigilosos, como informações de identificação pessoal (PII), registros financeiros ou propriedade intelectual, para modelos externos de inteligência artificial (IA) que não podem ser controlados ou auditados. Isso torna a perda de dados não apenas possível, mas provável.

Em vez de bloquear completamente as ferramentas de GenAI, o que prejudicaria a produtividade das equipes, muitos líderes de TI estão buscando maneiras eficazes de viabilizar a adoção segura da IA, protegendo os dados sem criar atritos. Siga estes seis passos proativos abaixo para identificar atividades de IA paralela no seu ambiente, avaliar os riscos e implementar políticas e controles técnicos; tudo isso mantendo os benefícios que esses aplicativos oferecem.

01

Audite sua exposição à IA paralela

- [ ] Antes de poder proteger as atividades da GenAI, você precisa entender o que está acontecendo em seu ambiente. Comece realizando uma auditoria em toda a empresa dos aplicativos de IA de terceiros usados por seus funcionários e, em seguida, identifique aqueles que não foram aprovados pelo departamento de TI. Certifique-se de monitorar o tráfego para as ferramentas de GenAI, acompanhar o acesso de dispositivos não gerenciados a essas ferramentas e avaliar o volume e os tipos de dados que suas equipes de trabalho estão compartilhando.

02

Avalie o seu nível de risco de dados

- [ ] Em muitos casos, os funcionários recorrem à GenAI em busca de rapidez e conveniência, sem se darem conta das implicações. Compreender os tipos de dados que seus funcionários compartilham com ferramentas de IA, e os motivos pelos quais o fazem, é essencial para priorizar seus esforços de resposta. Avalie se sua equipe está compartilhando dados sigilosos, como informações de identificação pessoal (PII), propriedade intelectual ou registros financeiros, e mapeie os fluxos de trabalho por onde os dados entram nessas ferramentas. Você também deve determinar se suas equipes de TI conseguem controlar ou recuperar os dados compartilhados e identificar se algum risco de conformidade está sendo acionado como resultado.

03

Crie diretrizes para o uso de GenAI

- [ ] Estabelecer políticas claras de utilização de IA cria a base para uma adoção responsável em toda a sua organização. Defina quais aplicativos de GenAI são permitidos e forneça orientações sobre o que fazer e o que não fazer para garantir um comportamento seguro no compartilhamento de dados corporativos com ferramentas de IA. Defina as expectativas desde o início, incorporando regras para o tratamento de dados específicos de IA nos treinamentos de integração e segurança, e exija que todos os funcionários reconheçam e sigam essas diretrizes. Mecanismos de proteção como esses ajudam a proteger os dados sem comprometer a produtividade.

04

Reforce a segurança na borda

- Políticas robustas precisam ser respaldadas por controles eficazes. Monitore e controle os fluxos de dados para ferramentas de GenAI implementando uma arquitetura de segurança moderna, como o zero trust. As plataformas de zero trust incorporam diversas ferramentas para ajudar a reduzir a exposição de dados, como um agente de segurança de acesso à nuvem (CASB) para detectar o acesso a aplicativos de IA não autorizados, prevenção contra perda de dados (DLP) em linha para impedir que os funcionários insiram dados sigilososem campos de prompt, isolamento de navegador para bloquear o uso de IA paralela sem interromper o acesso à web e análise de comportamento de usuários e entidades (UEBA) para detectar anomalias no uso de ferramentas de IA.

05

Crie uma cultura de IA responsável

- Tecnologia e políticas públicas são apenas parte da equação. É igualmente importante criar uma cultura de conscientização em toda a sua organização. Instrua suas equipes sobre os riscos de compartilhar informações sigilosas com a GenAI e ofereça exemplos de uso seguro e apropriado de IA. Explique como usar os aplicativos aprovados para aumentar a produtividade com auxílio da IA e incentive os funcionários a relatarem ferramentas não aprovadas ou comportamentos questionáveis. Criar uma cultura de responsabilidade ajuda a transformar suas equipes de trabalho em uma extensão da sua equipe de segurança.

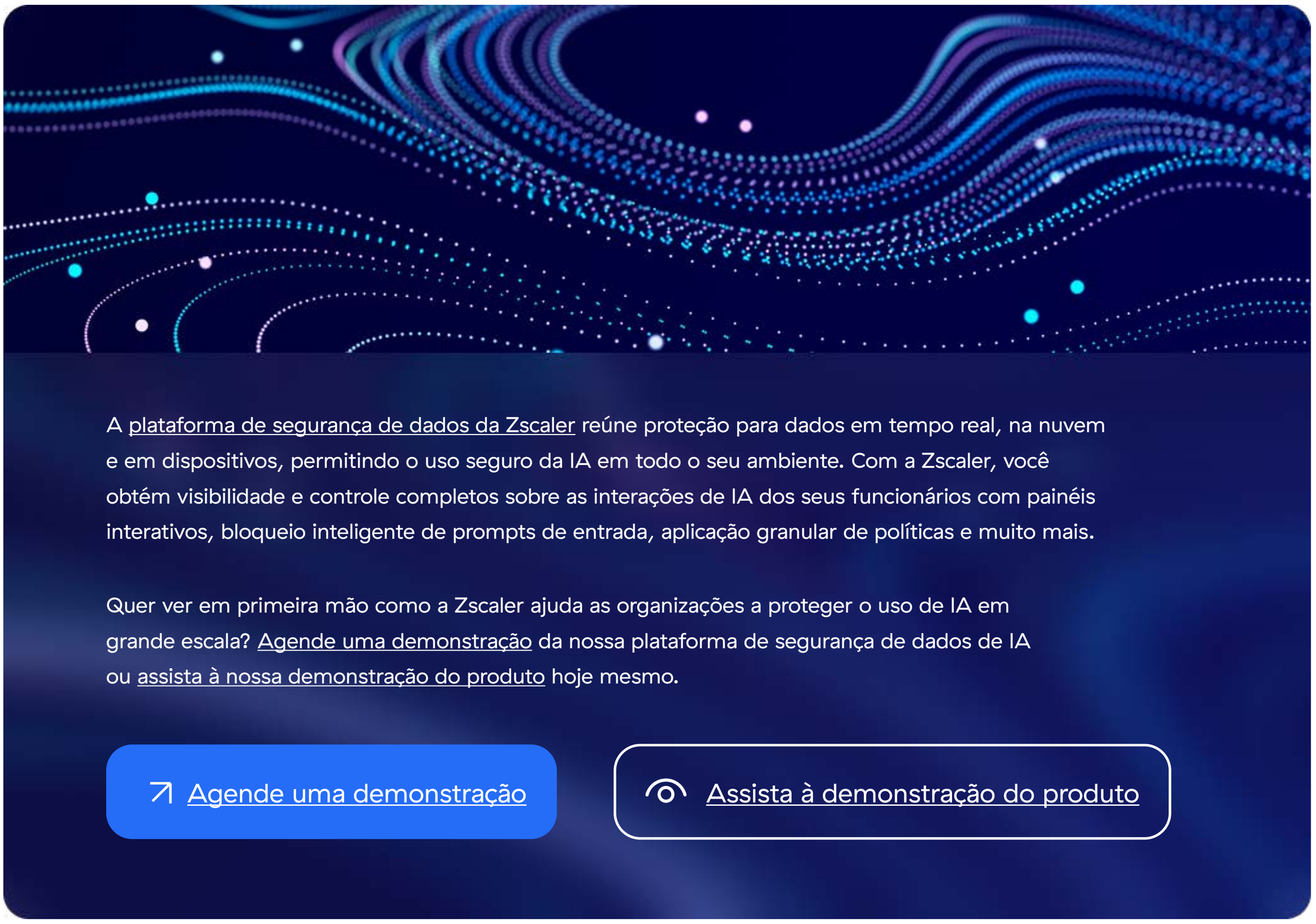
06

Torne o gerenciamento da IA paralela um processo contínuo

- Garantir a segurança do uso de IA por suas equipes de trabalho não é um algo pontual, mas um programa contínuo que deve evoluir com o cenário de ameaças. Mantenha suas defesas atualizadas, realizando buscas contínuas por novas ferramentas de GenAI, monitorando tendências de uso e atualizando o conteúdo e as políticas de treinamento para lidar com ameaças emergentes. Alinhar seus esforços de gerenciamento de IA oculta com a abordagem zero trust e a estratégia de DLP (prevenção contra perda de dados) mais amplas da sua organização garante que isso se torne um esforço contínuo, em vez de uma solução paliativa.

Zscaler: segurança de GenAI que atende a todos os requisitos

Ao implementar as medidas de segurança descritas nesta lista de verificação, você estabelecerá uma base que permitirá à sua organização adotar a GenAI com confiança, sem sacrificar a segurança. Essa abordagem passo a passo oferece às suas equipes de TI controle sobre todos os aspectos do uso da GenAI, desde a solicitação de informações até os aplicativos permitidos, para que suas equipes possam aproveitar com segurança a produtividade baseada em IA.



A plataforma de segurança de dados da Zscaler reúne proteção para dados em tempo real, na nuvem e em dispositivos, permitindo o uso seguro da IA em todo o seu ambiente. Com a Zscaler, você obtém visibilidade e controle completos sobre as interações de IA dos seus funcionários com painéis interativos, bloqueio inteligente de prompts de entrada, aplicação granular de políticas e muito mais.

Quer ver em primeira mão como a Zscaler ajuda as organizações a proteger o uso de IA em grande escala? Agende uma demonstração da nossa plataforma de segurança de dados de IA ou assista à nossa demonstração do produto hoje mesmo.

Agende uma demonstração

Assista à demonstração do produto

zscaler™ | Experience your world, secured.™

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 150 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 zscaler.com/br.

+1 408.533.0288 Zscaler, Inc. (Sede) • 120 Holger Way • San Jose, CA 95134

zscaler.com/br