DELL Technologies

Serviços de segurança e resiliência da IA

Confie em seu uso da IA

Como enfrentar os desafios da adoção de IA

A inteligência artificial (IA) é um divisor de águas para as empresas, pois possibilita inovações revolucionárias e agiliza a tomada de decisões. No entanto, junto ao grande potencial, surgem também desafios significativos. A adoção da IA introduz preocupações exclusivas de segurança, confiança e conformidade, colocando novas pressões sobre as organizações. Na Dell Technologies, reimaginamos como a segurança de IA deve funcionar. Nossa abordagem integra de forma especial o gerenciamento de dados, a segurança de infraestrutura e a proteção de modelos de IA para oferecer uma solução abrangente e personalizada. Se você é um iniciante em IA ou deseja aprimorar suas soluções atuais, nossos serviços de ponta a ponta são a solução ideal para tornar a adoção da IA mais rápida, segura e confiável.

A segurança não é uma responsabilidade apenas da TI

A segurança moderna relacionada à IA exige colaboração entre as equipes. A segurança da IA é um esporte de equipe, que exige a contribuição e a tomada de decisões de toda a organização. Os modelos operacionais tradicionais de TI em silos não funcionarão nesse cenário em evolução. Nossa abordagem exclusiva incorpora dados, infraestrutura, aplicativos e modelos em uma estratégia coesa e adaptável às suas necessidades comerciais específicas, oferecendo uma solução holística que ajudará você a se manter à frente.

Como lidar com os desafios de segurança exclusivos da IA

A adoção da IA introduz considerações complexas de segurança e conformidade, que podem comprometer seus possíveis benefícios, como:

- Violações de dados e perda de propriedade intelectual (PI) devido à proteção inadequada de informações ou ao acesso não autorizado.
- Ameaças baseadas em IA, como ataques adversários, manipulação de modelos ou envenenamento de dados de treinamento.
- Desafios de disponibilidade para que as ferramentas de IA, agora essenciais, como os agentes de suporte, estejam continuamente operacionais.
- Vulnerabilidades na cadeia de suprimentos de terceiros originadas de sistemas interconectados.
- Expansão das superfícies de ataque à medida que os aplicativos de IA são dimensionados em ambientes híbridos e com várias nuvens.
- Embora não seja uma preocupação puramente de segurança, as alucinações podem induzir os usuários ao erro

Principais benefícios

Confiança e transparência aprimoradas: proteja os dados, a propriedade intelectual e a integridade da IA para manter a confiança entre as partes interessadas.

Resiliência operacional: mantenha os sistemas de IA de missão crítica operacionais e resistentes a ameaças.

Conformidade regulatória: ajude a cumprir as normas governamentais e setoriais para evitar penalidades dispendiosas e danos à reputação.

Soluções escaláveis: implemente medidas de segurança de IA adaptáveis, que crescem junto com a sua organização e a sua pilha de tecnologia.

Suporte e orientação especializados: trabalhe com especialistas em segurança comprovados para adaptar sua solução e obter resultados mensuráveis.

Serviços de ponta a ponta para oferecer uma arquitetura de segurança personalizada

Nossa arquitetura de segurança, desenvolvida pela Dell, foi projetada para atender às suas necessidades exclusivas, oferecendo uma base flexível e confiável. Ela se integra perfeitamente à Dell AI Factory, adota os princípios do Zero Trust e incorpora tecnologias de parceiros habilmente integradas, promovendo assim a inovação segura e com visão de futuro.

	Recursos
Orientar Alinhe a segurança de IA às necessidades organizacionais e aos requisitos de conformidade	• **Os serviços de consultoria em segurança e resiliência para IA** incluem workshops técnicos e de negócios para o desenvolvimento de uma estratégia abrangente de segurança e disponibilidade • **O Consultor CISO para IA** oferece um CISO virtual, especialista em IA, para auxiliar na elaboração de uma estratégia de segurança para a IA • **A Segurança de dados para IA** ajuda a reduzir as ameaças à segurança de dados e os riscos para seus dados
Implementar Projete e implemente software de segurança para aumentar a visibilidade da pilha de IA	• **Design e configuração de software de segurança** para integrar ferramentas que protegem o gerenciamento de acesso, aplicativos e redes
Gerencie Permita uma visibilidade profunda em toda a pilha para detectar e responder rapidamente às ameaças	• **Managed Detection and Response (MDR)** para detecção de ameaças 24 horas por dia, 7 dias por semana, em dados, infraestrutura, aplicativos e modelos • **O firewall de IA gerenciado** impõe um conjunto isolado de barreiras de proteção baseadas em IA e inspeciona prompts e resultados para garantir a conformidade com as políticas • **Teste de penetração de IA**, que simula ataques de adversários e identifica pontos fracos • **Serviços de resposta e recuperação de incidentes** para ajudar você a se recuperar rapidamente e voltar aos negócios com o mínimo de interrupção

Crie um futuro seguro de IA com confiança

Os serviços de segurança e resiliência de IA da Dell são projetados para lidar com os novos riscos associados à integração da IA à sua organização. Criados para trabalhar com suas equipes à medida que você integra a IA o mais rápido possível, nossos serviços oferecem a experiência para orientar no planejamento estratégico, na implementação de soluções e nos serviços de segurança gerenciados para aliviar as cargas operacionais, para que você possa inovar com segurança com a IA.

Explore os serviços de resiliência e segurança da Dell

Entre em contato com um especialista da Dell Technologies

Participe da conversa usando #DellTechnologies

DELL Technologies