

Inovação segura com IA em escala

Segurança para IA com o Cisco AI Defense

A adoção de IA está acelerando rapidamente — e os riscos também. Da shadow AI aos ataques adversariais, as empresas enfrentam uma nova fronteira de ameaças. Por meio de nossa parceria estratégica com a Cisco, a NTT DATA desenvolveu uma abordagem integrada para a segurança da IA. Ao combinar nossos serviços de segurança para todo o ciclo de vida da IA com a plataforma Cisco AI Defense, oferecemos visibilidade, proteção e validação de ponta a ponta.

Juntas, ajudamos as empresas a avançar com segurança e confiança na inovação com IA.

Sua empresa está adotando IA, mas preocupações com vieses, vazamento de dados e ataques estão desacelerando o processo de adoção. Comprovar a conformidade e estabelecer confiança continuam sendo os principais desafios.

A NTT DATA e a Cisco ajudam a superar essas barreiras ao combinar frameworks de riscos e conformidade em IA com as defesas AI-native da

Cisco, reduzindo riscos regulatórios e reputacionais. Fazemos da confiança um elemento dos sistemas de IA desde o início, integrando governança, validação e proteção em tempo de execução para que sua empresa possa inovar com segurança e em escala.

Proteção de ponta a ponta

A NTT DATA protege todo o ciclo de vida da IA — desde o design e desenvolvimento até a implantação e o monitoramento — enquanto o Cisco AI Defense protege, em tempo real, aplicações com IA integrada e o uso de shadow AI.

Validação abrangente

Com os mecanismos técnicos de proteção integrados da Cisco — incluindo defesa contra injeção de prompt, firewalls de IA e prevenção de vazamento de dados — e a governança conduzida por especialistas por meio dos serviços da NTT DATA, sua empresa estará em conformidade com a ISO/IEC 42001, o framework de gestão de riscos de IA (AI RMF) do Instituto Nacional de Padrões e Tecnologia (NIST) e a Lei de IA da União Europeia.

“Ajudamos sua empresa a avançar com mais velocidade, ampliar a inovação com IA de forma segura e evitar riscos reputacionais, financeiros e jurídicos.”

Nossa abordagem integrada

Serviços de segurança para IA da NTT DATA

- **Serviço de risco e conformidade em IA**
Avaliações e governança de todo o ciclo de vida da IA alinhadas à ISO/IEC 42001, ao NIST AI RMF e às regulamentações globais.
- **Serviço de proteção para IA**
Proteção de modelos de IA, dados, aplicações, APIs e ambientes de GenAI.
- **Serviço de segurança para IA**
Red teaming contínuo, testes estruturados de grandes modelos de linguagem (LLM) e simulações adversariais.
- **Secure AI Lab**
Ambiente completo de inovação e testes, pronto para uso e com integrações de parceiros já incorporadas.
- **Modelos de atuação**
Avaliações de prontidão, adoção, serviços gerenciados e red teaming sob demanda.

Recursos do Cisco AI Defense

- **Visibilidade da IA em ambientes cloud**
Identifica e inventaria workloads, modelos e fluxos de dados de IA em diferentes ambientes cloud.
- **Acesso à IA**
Controla o uso de IA pelos colaboradores para evitar vazamentos de dados.
- **Validação de modelos e aplicações de IA**
Identifica vulnerabilidades em modelos e aplicações de IA ainda nas etapas iniciais de desenvolvimento.
- **Gestão de riscos da cadeia de suprimentos com IA**
Protege modelos, conjuntos de dados e dependências provenientes de fontes externas contra comprometimentos.
- **Proteção da IA em tempo de execução**
Bloqueia ameaças a workloads de IA em tempo real.





Proteja a IA e seus negócios

Inovação segura em escala

Avalie casos de uso de IA e realize provas de conceito (POCs) seguras com mais rapidez no Secure AI Lab da NTT DATA, pré-configurado com os recursos do Cisco AI Defense. Isso reduz o tempo necessário para gerar valor ao acelerar a implantação, que passa de meses para semanas.

Ambiente experimental de IA

O Secure AI Lab Center of Excellence (CoE) Service da NTT DATA oferece às empresas um ambiente experimental completo de segurança para IA, pronto para uso e desenvolvido para acelerar o aprendizado, a experimentação e a definição de abordagens de segurança para casos de uso de IA empresarial.

Conformidade e governança que inspiram confiança

Os serviços de validação da NTT DATA alinham os programas de IA a padrões globais, como a ISO/IEC 42001 e o NIST AI RMF. Com o suporte das atualizações contínuas dos modelos de ameaças da Cisco, essa abordagem reduz os riscos jurídicos e ajuda a evitar multas elevadas e danos à reputação.

Identifique riscos ocultos de IA

O serviço de Red Teaming de IA da NTT DATA combina ferramentas de referência no mercado, um framework proprietário e uma ampla biblioteca de casos de uso adversariais previamente validados para identificar proativamente riscos ocultos de IA e manter um processo contínuo de validação da IA.

Gestão de riscos de shadow AI

Identificamos proativamente o uso não autorizado de ferramentas de IA e aplicamos políticas para evitar vazamentos de dados. Isso reduz os riscos ocultos e, ao mesmo tempo, contribui para a adoção segura de novas ferramentas de IA.

Defesa em tempo real para IA em produção

Protegemos workloads de IA em produção com mecanismos de segurança em múltiplas camadas, firewalls de IA e aplicação inteligente de políticas.

[Entre em contato](#) para saber mais.

“ Juntas, viabilizamos uma adoção de IA segura, escalável e resiliente, que impulsiona a inovação e o crescimento.”

Para mais informações, acesse br.nttdata.com.

A NTT DATA é uma inovadora global em serviços digitais e de tecnologia, ajudando empresas a inovar, otimizar e se transformar para alcançar o sucesso. Como Global Top Employer, temos diversos especialistas em mais de 70 países e um robusto ecossistema de parceiros. A NTT DATA faz parte do NTT Group.

