



Como criar uma base segura para a adoção e o crescimento da IA

Proteção da infraestrutura preparada para IA com a NTT DATA e a Cisco

Outubro 2025



Índice

03 Proteja sua infraestrutura para aproveitar todo o potencial da IA

04 NTT DATA e Cisco: uma parceria estratégica

06 Cibersegurança abrangente e adaptada às suas necessidades

09 Serviços de cibersegurança da NTT DATA para todo o ciclo de vida

Proteja sua infraestrutura para aproveitar todo o potencial da IA

Para aproveitar todo o potencial da IA, a infraestrutura digital e a cibersegurança não podem ser tratadas como aspectos secundários. A IA se beneficia de grandes volumes de dados que circulam com rapidez e segurança pela infraestrutura de rede e pelo ecossistema digital.

Por isso, redes e infraestruturas digitais desatualizadas ou com proteção inadequada representam riscos claros.

Ao modernizar a infraestrutura digital, sua empresa cria uma base sólida e segura para que a IA gere resultados relevantes sem ser limitada por obstáculos ou vulnerabilidades.

A IA utiliza dados e também aprende com eles. Quando a integridade desses dados é comprometida, não é possível confiar nos resultados dos modelos de IA. Uma violação de segurança pode comprometer a própria inteligência que está sendo desenvolvida. Ao implementar medidas robustas de governança e conformidade que protejam os

dados durante todo o ciclo de vida — tanto em repouso quanto em trânsito —, sua empresa mantém as informações que alimentam a IA precisas, confiáveis e protegidas contra adulterações.

Essa base também permite que a organização cresça sem enfrentar continuamente obstáculos relacionados à segurança. À medida que surgem novas formas de aplicar a IA — seja para automatizar tarefas, personalizar experiências dos clientes ou apoiar decisões em tempo real —, a infraestrutura digital também precisa ganhar escala. Uma infraestrutura flexível e preparada para IA oferece espaço para experimentar, adaptar e expandir sem reconstruções onerosas ou atualizações intermináveis.

Em resumo, uma infraestrutura digital moderna e segura, do edge à cloud, cria uma base para acelerar a inovação com IA e ganhar escala de acordo com a visão da sua empresa.



O equilíbrio da segurança em IA: do risco à inovação apresenta a visão da NTT DATA sobre os riscos de IA enfrentados pelas organizações e como gerenciá-los sem limitar a inovação.



NTT DATA e Cisco: uma parceria estratégica

Diante do impacto que o uso de tecnologias de IA pode ter no desempenho dos negócios — da estratégia às operações e às experiências digitais —, faz sentido contar com soluções integradas que reúnam tecnologias de referência, recursos full stack e serviços para todo o ciclo de vida. Assim, sua empresa mantém o controle sobre a segurança ao longo da jornada de IA.

A NTT DATA e a Cisco — líderes em suas respectivas áreas — trabalham juntas há mais de três décadas para ajudar organizações de diversos setores a alcançar seus objetivos de negócio por meio de inovação tecnológica ágil, segura e confiável.

Por meio de nossos serviços de segurança de infraestrutura e redes, prestamos consultoria, implementamos e operamos controles, tecnologias e protocolos desenvolvidos para proteger recursos críticos de rede. Criamos uma infraestrutura de rede resiliente com uma abordagem de segurança desde a concepção, Secure Access Service Edge (SASE), autenticação adaptativa e soluções de rede privada virtual (VPN).

Adaptamos o roadmap de segurança da infraestrutura à estratégia geral de segurança e TI da sua empresa para criar defesas escaláveis e garantir uma proteção proativa da rede contra ameaças cibernéticas.

Como a NTT DATA e a Cisco se alinham em torno de uma visão de segurança do edge à cloud?

A visão de segurança do edge à cloud da NTT DATA destaca a importância de uma cibersegurança integrada de ponta a ponta em toda a topologia de rede — dos endpoints e aplicações aos dados, data centers híbridos e ambientes cloud. A arquitetura da Cisco dá suporte a essa visão ao integrar a segurança a todas as camadas do ecossistema digital.

Juntas, vamos além da cibersegurança tradicional. Ajudamos sua empresa a antecipar e gerenciar riscos, avançar com segurança na transformação digital e desenvolver uma resiliência cibernética permanente diante de ameaças em constante evolução.

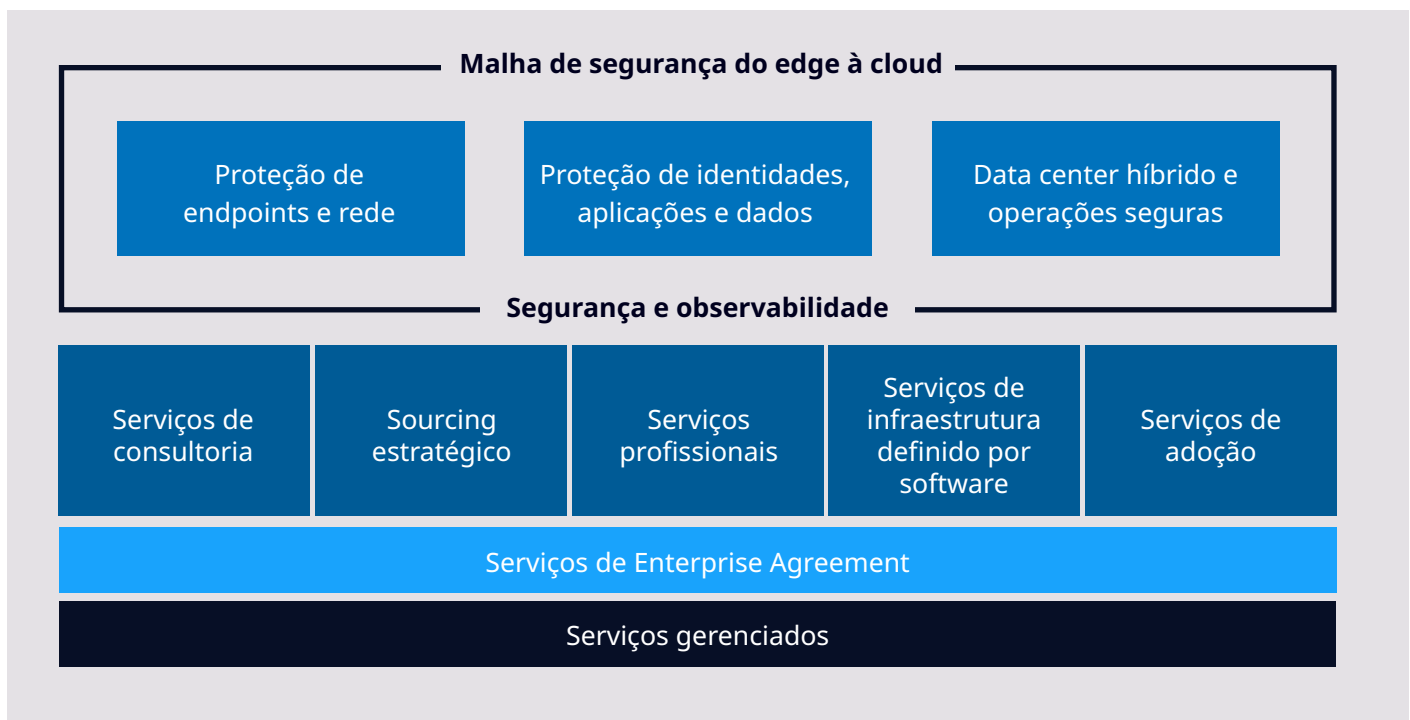
Ao combinar as avançadas plataformas de inteligência de ameaças e defesa com IA da Cisco com a Cybersecurity Assurance Platform e a Cybersecurity Insights Platform da NTT DATA, as organizações passam a contar com visibilidade e controle unificados em ambientes complexos de cloud e IA. Essa abordagem simplifica e fortalece as defesas, permitindo respostas rápidas e coordenadas, da proteção à recuperação.

Com a presença global e a expertise local da NTT DATA em mais de 50 países, além de uma parceria de mais de três décadas com a Cisco que abrange 11 especializações Cisco Powered Services, essa colaboração faz com que a cibersegurança deixe de ser um custo para o negócio e se torne uma base para inovar com segurança e confiança.



Cibersegurança abrangente e adaptada às suas necessidades

Cada organização tem necessidades específicas de segurança. Por isso, a NTT DATA, em parceria com a Cisco, oferece um portfólio abrangente de soluções e serviços de cibersegurança desenvolvido para enfrentar diferentes desafios. Nossa malha de segurança do edge à cloud se estende desde suas instalações, filiais e demais unidades da sua empresa até o ambiente cloud. E abrange três áreas principais:



1. Proteção de endpoints e rede

O que sua empresa precisa: proteger os endpoints e a infraestrutura de rede contra acessos mal-intencionados e ataques cibernéticos.

A segurança de endpoints protege dispositivos — como laptops, impressoras, servidores, máquinas industriais e dispositivos móveis — contra ameaças cibernéticas. Para isso, os serviços de segurança de endpoints utilizam diferentes controles, como software antimalware, whitelisting, blacklisting e criptografia, para manter os endpoints de TI protegidos.

Como ajudamos: soluções avançadas de proteção de endpoints e segurança de rede adaptadas a ambientes de TI, OT e IoT.

Além da segurança de endpoints, do gerenciamento de vulnerabilidades e da conformidade, protegemos ativos e redes de TI, OT e IoT industrial. Isso é feito por meio de análise de ameaças, acesso remoto seguro, convergência entre TI e OT, detecção e resposta gerenciadas para OT e segurança Zero Trust para OT.

Ao mesmo tempo, nossos serviços de segurança de infraestrutura e redes — que incluem proteção do perímetro, SASE gerenciado, Zero Trust Network Access e segurança para edge e 5G — protegem a infraestrutura de rede da sua empresa contra ameaças cibernéticas. Fornecemos consultoria e implementamos e mantemos os controles, as práticas e as tecnologias necessárias para detectar ameaças, responder a incidentes e acelerar a recuperação.

2. Proteção de identidades, aplicações e dados

O que sua empresa precisa: garantir o acesso seguro aos recursos digitais e proteger dados sensíveis contra acessos não autorizados, violações de segurança e ameaças internas.

O gerenciamento de identidades e acessos — incluindo serviços de autorização e autenticação, detecção de ameaças à identidade, gerenciamento de identidades de máquina e governança de identidades — é a porta de entrada para o ecossistema digital da sua empresa. Por isso, é fundamental proteger identidades digitais, aplicações e dados.

Como ajudamos: soluções de identidade digital e proteção de aplicações e dados que estabelecem controles de acesso robustos para proteger informações sensíveis em conformidade com as regulamentações de privacidade de dados.

Nossos serviços de segurança de aplicações protegem o software e a infraestrutura de aplicações, onde quer que estejam. Além de modelagem de ameaças, segurança de sistemas de planejamento de recursos empresariais (ERP), gerenciamento contínuo da exposição a ameaças e segurança de APIs, entre outros recursos, também incorporamos princípios de segurança desde a fase inicial dos processos de DevSecOps.

Protegemos os dados durante todo o ciclo de vida — em repouso ou em trânsito — com medidas robustas de governança e segurança alinhadas às exigências regulatórias do setor ou da região em que sua empresa atua. Isso inclui as práticas mais adequadas para classificar, tratar e proteger dados sensíveis e informações privadas, além de serviços criptográficos e proteção contra ransomware. Também realizamos avaliações aprofundadas de privacidade de dados para adaptar a jornada às necessidades da sua empresa.

Além disso, para preservar a confiança digital, protegemos as identidades digitais com mecanismos robustos de autorização e autenticação, detecção e resposta a ameaças e princípios de Zero Trust. Isso inclui a proteção contra ameaças emergentes, como deepfakes e desinformação.

3. Proteção da IA, data center híbrido, cloud e operações

O que sua empresa precisa: proteger ambientes de cloud, híbridos e de IA e contar com operações de segurança eficientes.

A segurança em cloud protege dados, aplicações e workloads hospedados em cloud, além da infraestrutura híbrida da empresa, por meio de políticas de segurança consistentes. Isso permite avançar com confiança e segurança na transformação da cloud, na adoção de IA e na inovação, com a certeza de que os ativos digitais permanecem protegidos.

Como ajudamos: segurança abrangente e adaptada a ambientes híbridos e multicloud para que sua empresa use tecnologias cloud com segurança, mantendo o controle sobre a jornada de inovação com IA e a mitigação contínua de ameaças potencializadas por IA.

Nosso modelo de segurança em cloud com IA integrada protege ambientes de infraestrutura como serviço (IaaS), plataforma como serviço (PaaS) e software como serviço (SaaS), unificando controles de identidade e acesso, proteção de dados, detecção avançada de ameaças e conformidade contínua. Com recursos de inteligência baseados em IA, esse modelo viabiliza operações preditivas, escaláveis e resilientes em todo o stack de segurança em cloud, permitindo que sua empresa avance com confiança na inovação cloud-native com IA.



Nosso Centro Global de Operações de Segurança (GSOC) oferece detecção e resposta gerenciadas, com inteligência de ameaças baseada em IA e automação avançada, para monitorar continuamente, detectar e responder a ameaças cibernéticas e ataques com uso de IA. Integramos pessoas, processos e sistemas para agir de forma rápida e coordenada — da proteção à detecção, resposta e recuperação.

Também integramos nossas análises com IA aos recursos avançados da Splunk, plataforma especializada em análise de segurança, para aumentar ainda mais o desempenho dos centros de operações de segurança, automatizar a detecção proativa de ameaças e reduzir os tempos de resposta a incidentes.

Nossa oferta de segurança para IA protege seu ambiente em evolução de IA, machine learning e grandes modelos de linguagem (LLM), protegendo os dados, preservando a

integridade e a disponibilidade dos sistemas de IA e promovendo confiança e conformidade.

Da identificação de shadow AI à implementação de red teaming em sistemas de IA, oferecemos proteção para todo o ciclo de vida da IA na sua organização.

Nosso centro de excelência dedicado oferece acesso a especialistas de referência em riscos de IA, conformidade e gestão de ameaças adversariais. Ao mesmo tempo, nossa Cybersecurity Assurance Platform ajuda sua empresa a manter o alinhamento com padrões de referência, como 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.

A combinação de nossos serviços de segurança para todo o ciclo de vida da IA com a plataforma Cisco AI Defense garante visibilidade, proteção e assurance de ponta a ponta.



Serviços de cibersegurança da NTT DATA para todo o ciclo de vida

1. Serviços de consultoria

Nossos especialistas realizam avaliações abrangentes de cibersegurança e prestam serviços de consultoria para identificar vulnerabilidades e desenvolver um roadmap personalizado para a implementação de arquiteturas de TI seguras, alinhadas às melhores práticas do setor e às necessidades do seu negócio.

2. Sourcing estratégico

Ajudamos sua empresa a identificar e selecionar as soluções de cibersegurança mais adequadas por meio de nossas parcerias estratégicas com fornecedores líderes de tecnologia, como a Cisco.

3. Serviços profissionais

Mais de 7.500 especialistas em cibersegurança, distribuídos por mais de 50 países, implementam e gerenciam soluções de cibersegurança de referência que simplificam, modernizam e integram a infraestrutura de segurança dos clientes.

4. Serviços de infraestrutura definido por software

Oferecemos suporte técnico multilíngue 24x7 — incluindo serviços em campo — para monitorar e manter a postura de segurança da sua empresa e gerenciar incidentes. Também otimizamos as licenças de software de segurança de acordo com suas necessidades e ajudamos a controlar custos com a adoção de automação e agentes de IA.

5. Serviços de adoção

Oferecemos avaliações de segurança e análises da infraestrutura instalada, além de treinamentos de conscientização em cibersegurança para os colaboradores. Nossos gerentes de sucesso do cliente ajudam sua empresa a extrair o máximo valor dos investimentos em segurança.

Todas essas ofertas contam com o suporte de nossos serviços de Enterprise Agreement, que geram valor ao simplificar a aquisição e o consumo de tecnologia.



Conheça nossos serviços de cibersegurança e veja como transformar a segurança em uma vantagem estratégica para ajudar sua organização a prosperar na era da IA.

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.



