

As 10 principais
tendências
tecnológicas
estratégicas
para 2026



Estratégias para o mundo hiperconectado e impulsionado pela IA

Para os líderes de tecnologia, o ano de 2026 será decisivo, marcado pela velocidade sem precedentes de disrupção, inovação e risco. As 10 principais tendências tecnológicas estratégicas do Gartner para 2026 não são apenas mudanças: são vetores para a transformação empresarial que exigem proatividade da diretoria executiva.

As tendências deste ano refletem o mundo hiperconectado e impulsionado pela IA, em que competências isoladas não são suficientes. Elas estão classificadas em três temas que definem como as principais organizações vão inovar, competir e proteger seu valor:



O arquiteto

Construa bases digitais seguras, expansíveis e adaptáveis com plataformas de desenvolvimento nativas de IA, supercomputação de IA e computação confidencial.



O sintetizador

Orquestre diferentes tecnologias – incluindo sistemas multiagentes, modelos de linguagem específicos ao domínio e IA física – para obter acesso a novas fontes de valor.



O vanguardista

Amplie a confiança, a governança e a proteção por meio de segurança cibernética preventiva, rastreabilidade digital, plataformas de segurança de IA e geopolitização.

Ao explorar essas tendências, considere como alinhá-las às metas estratégicas de sua organização e como integrá-las ao seu planejamento para impulsionar o crescimento sustentável e a vantagem competitiva.



Gene Alvarez

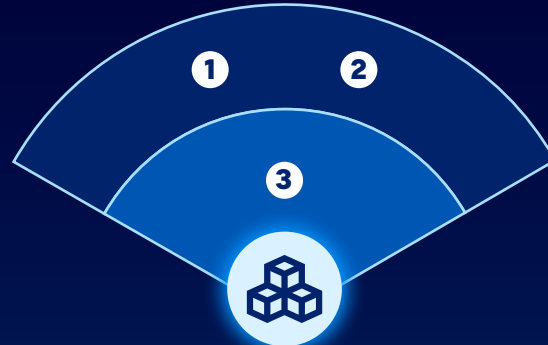
Vice-Presidente Emérito de Insights de Negócios e Tecnologia do Gartner

As principais tendências tecnológicas estratégicas do Gartner para 2026

O Gartner selecionou criteriosamente estas 10 tendências com base em seu potencial de fomentar a inovação, fortalecer a resiliência e ampliar a confiança no mundo hiperconectado e impulsionado pela IA. Elas representam imperativos estratégicos que exigem reflexão e proatividade dos líderes de tecnologia.

● **Agora**
1 a 3 anos

● **Em breve**
3 a 5 anos



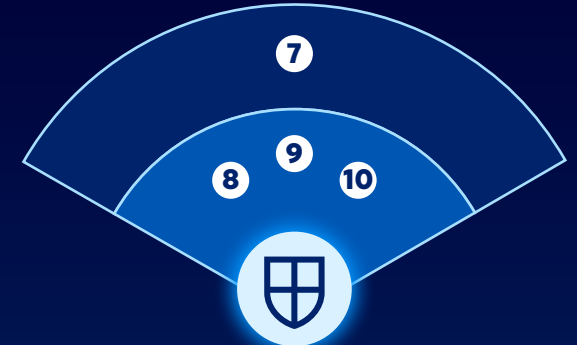
○ **arquiteto**

- 1 Plataformas de desenvolvimento nativas de IA
- 2 Plataformas de supercomputação de IA
- 3 Computação confidencial



○ **sintetizador**

- 4 Sistemas multiagentes
- 5 Modelos de linguagem específicos ao domínio
- 6 IA física



○ **vanguardista**

- 7 Segurança cibernética preventiva
- 8 Rastreabilidade digital
- 9 Plataformas de segurança de IA
- 10 Geopatriação



O arquiteto

Construa bases digitais seguras,
expansíveis e adaptáveis.

Para acelerar a inovação e a resiliência, os líderes de tecnologia precisam modernizar as plataformas e a infraestrutura. As tendências do arquiteto priorizam a criação de bases prontas para IA que viabilizem agilidade, segurança e escalabilidade, fundamentais para prosperar em um mundo hiperconectado e impulsionado pela IA.

1



das plataformas de desenvolvimento nativas de IA

O que é?

As plataformas de desenvolvimento nativas de IA usam IA generativa para criar softwares com mais rapidez e facilidade do que nunca. Elas abrangem ferramentas “one-shot”, que geram softwares a partir de um único prompt, e “vibe coding”, que dispensam conhecimento técnico aprofundado, além de agentes de IA orquestrados para criar programas.

Por que é uma tendência?

Os CIOs estão animados com a rapidez de entrega de softwares e com o aumento da produtividade. Já os CEOs e CFOs enxergam o potencial de economia de custos. As plataformas de desenvolvimento nativas de IA possibilitam que “equipes enxutas” criem mais aplicativos com os mesmos recursos. Por exemplo, cinco equipes de duas pessoas podem entregar cinco aplicativos simultaneamente. Essa tendência ajuda os CIOs a eliminarem gargalos e priorizar o desenvolvimento de soluções, em vez de comprá-las.

O que vem por aí

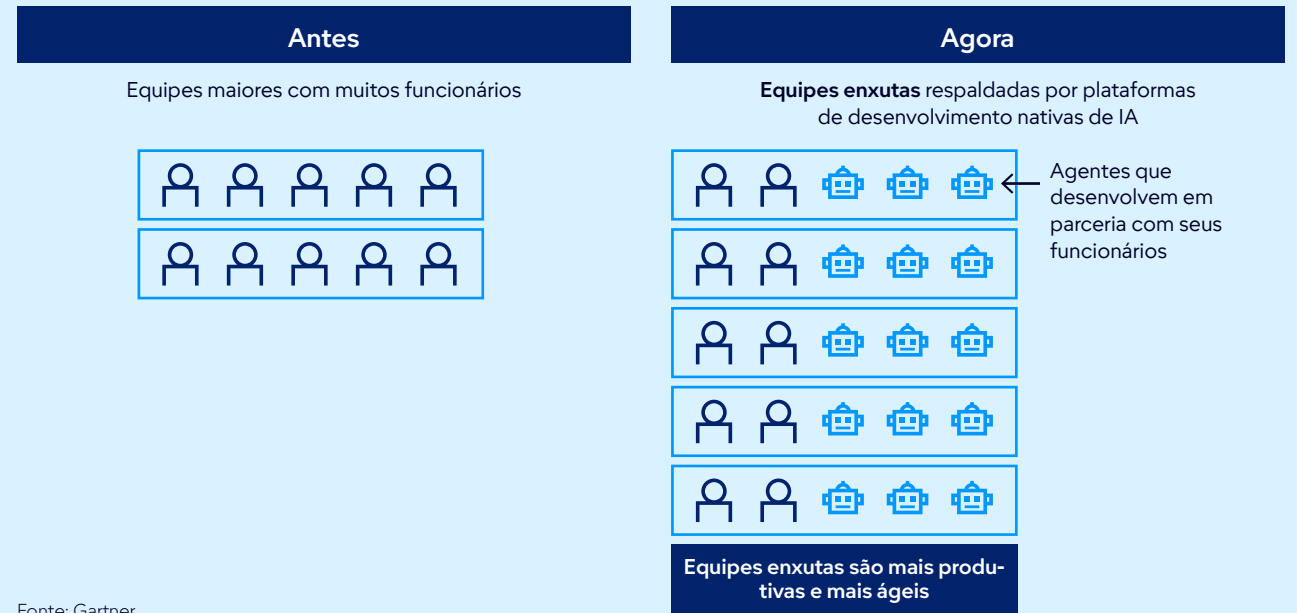
80%

das organizações reestruturarão grandes equipes de engenharia de software em equipes menores aprimoradas pela IA até 2030.

40%

dos portfólios de aplicativos empresariais incluirão versões personalizadas, desenvolvidas em plataformas nativas de IA até 2030 (em comparação com apenas 2% em 2025).

Equipes enxutas



Fonte: Gartner

1



Gere resultados com plataformas de desenvolvimento nativas de IA

Plano de ação para acelerar, economizar e fomentar a inovação

Etapas	1 Crie uma equipe de plataforma	2 Implemente mecanismos de proteção	3 Teste o desenvolvimento nativo de IA	4 Priorize o uso da IA	5 Qualifique e capacite as equipes
Resultado esperado	Supervisão centralizada para assegurar padrões uniformes e governança.	Redução do risco de códigos vulneráveis ou fora de conformidade.	Ganhos imediatos, comprovando o valor e estabelecendo a confiança.	Agilidade na entrega e otimização da capacidade de inovação.	Ampliação da adoção e eficácia na colaboração.
Ação	Crie uma equipe exclusiva para gerenciar plataformas nativas de IA e selecionar modelos de IA.	Integre plataformas de governança de IA para analisar o código e atestar a conformidade.	Comece com projetos de baixo risco para comprovar o aumento da produtividade.	Priorize ferramentas nativas de IA para novas iniciativas de desenvolvimento.	Treine desenvolvedores e parceiros de negócios em engenharia de prompt e governança.

Partes estratégicas para garantir o sucesso da implementação

CIO	Parceiros de TI	Parceiros de negócios
Parceria: define a estratégia que prioriza a IA e o modelo de governança. Colaboração: alinha recursos da plataforma com as prioridades de negócios. Governança: assegura a conformidade e estabelece mecanismos de proteção para o desenvolvimento nativo de IA.	Engenharia de plataforma: gerencia ferramentas nativas de IA, integrações e desempenho. Segurança: implementa governança de IA para análise do código e gestão de riscos. Aquisição: avalia e seleciona fornecedores e serviços de plataformas nativas de IA.	Proprietários do produto: compartilham conhecimento específico e validam soluções impulsionadas pela IA. Financeiro: alinha modelos de financiamento para apoiar iniciativas de desenvolvimento nativo de IA.

2



Plataformas de supercomputação de IA

O que é?

As plataformas de supercomputação de IA fornecem a capacidade de processamento em larga escala necessária para treinar e executar modelos avançados de IA. Esses sistemas integram computação de alto desempenho (HPC), processadores especializados e arquiteturas expansíveis para lidar com cargas de trabalho que incluem grandes volumes de dados.

Por que é uma tendência?

A demanda pela supercomputação de IA está aumentando à medida que as organizações desenvolvem modelos maiores e mais complexos que extrapolam os limites da infraestrutura tradicional.

O que vem por aí

40% das empresas adotarão arquiteturas híbridas de computação até 2028 (contra 8%).

+20 fornecedores oferecerão plataformas unificadas de desenvolvimento baseadas em ambientes de supercomputação até 2028.

Plataforma de supercomputação de IA



Fonte: Gartner

2



Gere resultados com plataformas de supercomputação de IA

Plano de ação para obter acesso à capacidade de processamento em larga escala

Etapas	1 Identifique cargas de trabalho de alto impacto	2 Invista em stacks unificados de softwares	3 Elabore uma estratégia de integração em fases	4 Agilize o desenvolvimento entre os ambientes	5 Planeje-se para governança e a conformidade
Resultado esperado	Comprovação do valor e desenvolvimento de conhecimento interno.	Simplificação da integração e flexibilidade na alocação da carga de trabalho.	Preparação da infraestrutura e da força de trabalho para o futuro.	Agilidade na entrega e diminuição do atrito.	Redução do risco e aprimoramento da supervisão.
Ação	Implante projetos-piloto usando orquestração híbrida.	Adote padrões abertos em sistemas tradicionais e de ponta.	Introduza novos paradigmas computacionais gradualmente e treine os funcionários de TI.	Incentive as equipes a adotar plataformas híbridas e arquiteturas combináveis.	Integre estratégias de segurança e de conformidade ao sistema.

Partes estratégicas para garantir o sucesso da implementação

CIO	Parceiros de TI	Parceiros de negócios
Define uma estratégia de orquestração híbrida alinhada com as prioridades de negócios. Garante a governança visando à alocação da carga de trabalho, à segurança e à conformidade. Colabora com líderes de negócios para priorizar cargas de trabalho de alto impacto.	Infraestrutura e operações: integra aceleradores de ponta a sistemas que já existem. Segurança: implementa a governança para ambientes multiarquitetônicos. DevOps: adota stacks unificados de softwares e ferramentas de orquestração.	Produto: identifica casos de uso para a computação híbrida (por ex., simulações e aplicativos habilitados por IA). Financeiro: alinha o orçamento com as fases da integração e as metas de sustentabilidade. Operações: preparam-se para fluxos de trabalho impulsionados por IA em processos-chave.

3



Computação confidencial

O que é?

A computação confidencial usa ambientes de execução confiáveis (TEEs) baseados em hardware para proteger os dados durante o processamento, impedindo o acesso não autorizado, inclusive de provedores de nuvem.

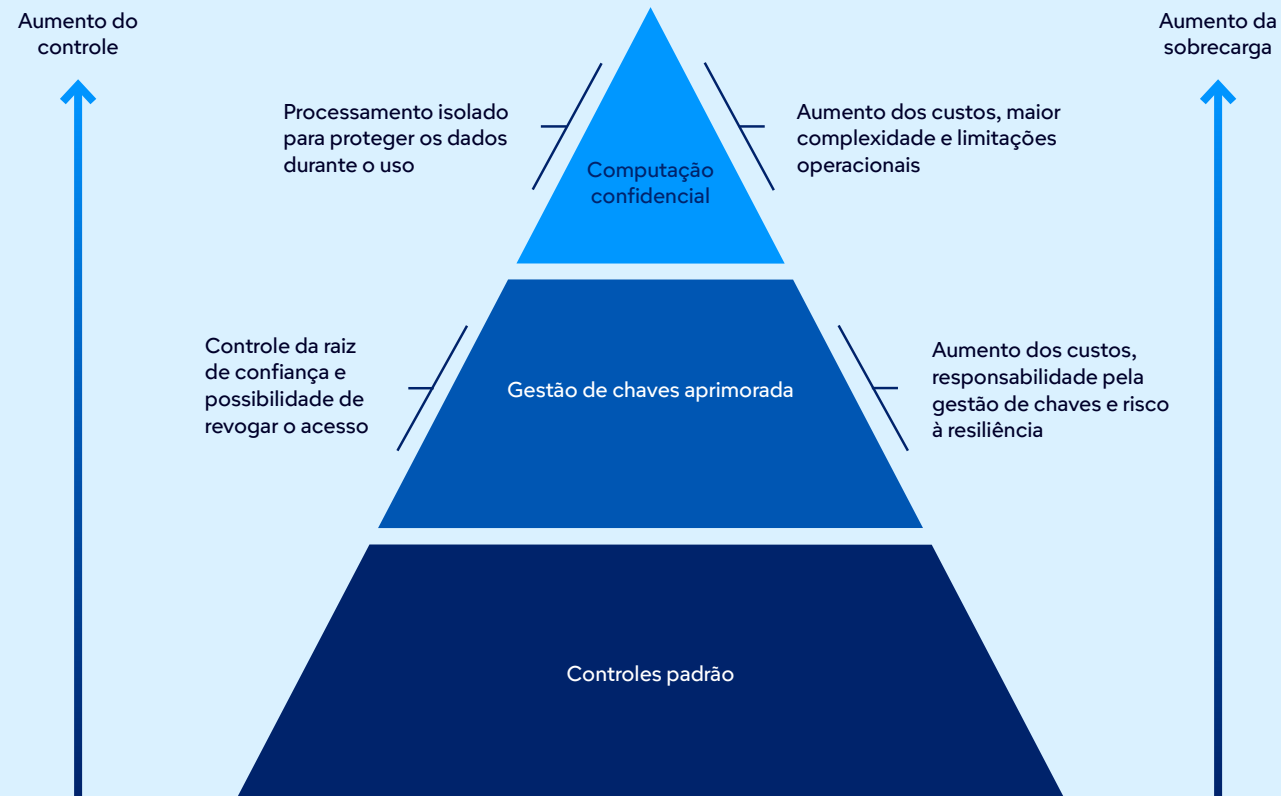
Por que é uma tendência?

Leis de privacidade mais rigorosas, normas de localização de dados e a adoção da IA tornam a proteção durante o uso imprescindível. A computação confidencial viabiliza estratégias seguras na nuvem e garante a conformidade para cargas de trabalho sigilosas.

O que vem por aí

75% do processamento em infraestrutura vulnerável serão protegidos pela computação confidencial até 2029.

Controles para limitar o acesso a dados de CSPs



Fonte: Gartner

3



Gere resultados com computação confidencial

Plano de ação para garantir o processamento de dados seguro e em conformidade em todos os ambientes

Etapas	1 Analise cargas de trabalho sigilosas.	2 Teste TEEs para modelos de IA.	3 Garanta colaboração segura.	4 Estabeleça a gestão autônoma de chaves.	5 Prepare-se para desafios de integração.
Resultado esperado	Identifique onde a proteção durante o uso é necessária.	Reforce a confidencialidade e a proteção da propriedade intelectual.	Compartilhe insights sem expor dados brutos.	Controle o acesso aos dados de ponta a ponta.	Assegure a implantação sem atritos entre os ambientes.
Ação	Mapeie as cargas de trabalho sujeitas a regras de privacidade ou localização.	Teste TEEs com modelos de IA proprietários e de código aberto.	Use computação confidencial para projetos analíticos e de inteligência comercial.	Implemente sistemas de chaves criptográficas de propriedade da organização.	Planeje a orquestração entre diversos chipsets e provedores.

Partes estratégicas para garantir o sucesso da implementação

CIO	Parceiros de TI	Parceiros de negócios
Define uma estratégia de computação confidencial alinhada às metas de privacidade, conformidade e nuvem. Colabora com as equipes jurídica e de conformidade para cumprir as exigências de localização e soberania de dados. Supervisiona a governança para TEEs e garante a integração com modelos de segurança que já existem.	Infraestrutura e operações: implanta TEEs em ambientes híbridos e multinuvm. Segurança: implementa processos de validação e gestão de chaves criptográficas. DevOps e plataforma: adaptam as cargas de trabalho para a computação confidencial e monitoram o desempenho.	Conformidade: atesta o cumprimento de exigências regulatórias e a prontidão para auditorias. Financeiro: alinha o orçamento destinado à adoção da computação confidencial e à redução de riscos. Proprietários de dados: identificam cargas de trabalho sigilosas para proteção durante o uso e priorizam projetos.



O sintetizador

Orquestre diversas tecnologias
para agregar valor inédito.

Para contar com novos diferenciais, os líderes de tecnologia devem integrar modelos especializados, sistemas multiagentes e IA física para soluções de domínios específicos. As tendências do sintetizador priorizam a orquestração de diversas tecnologias para criar ecossistemas inteligentes e adaptáveis que impulsionam a inovação entre fluxos de trabalho, produtos e experiências.

4

Sistemas multiagentes

O que é?

Os sistemas multiagentes (MAS) usam conjuntos de agentes de IA especializados que colaboram para concluir fluxos de trabalho complexos. Cada agente desempenha uma tarefa específica, aprimorando a eficiência e a escalabilidade em comparação com soluções de IA monolíticas.

Por que é uma tendência?

Enquanto a IA de agente único apresenta limitações em processos com diversas etapas, os MAS viabilizam a automação modular e a integração entre plataformas. Registramos um aumento de 1,445% nas consultas relacionadas a MAS entre o 1.º trimestre de 2024 e o 2.º trimestre de 2025, indicando que o interesse empresarial cresceu rapidamente.

O que vem por aí

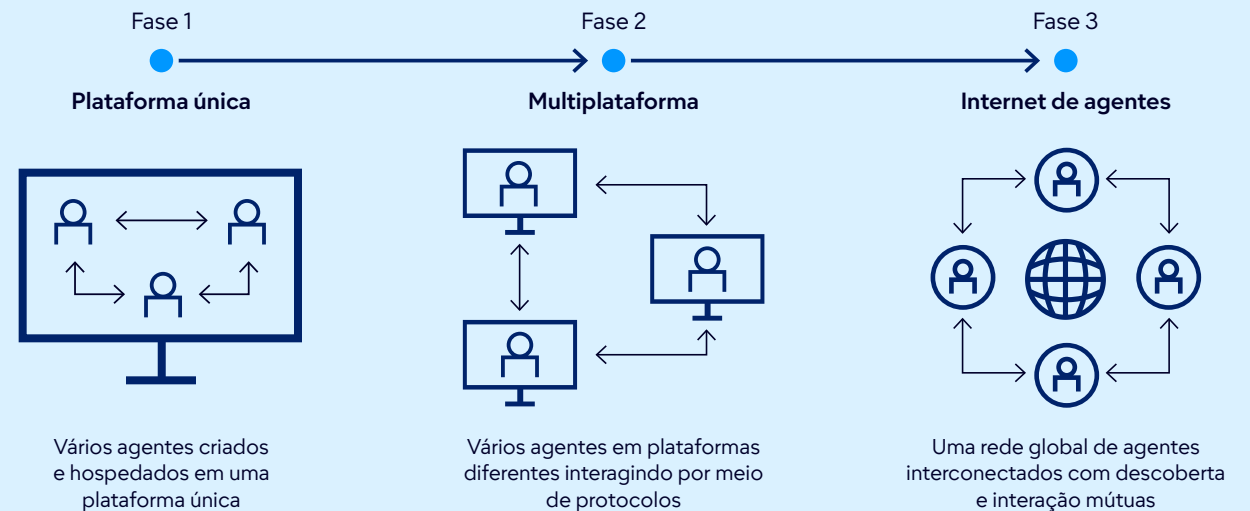
70%

de MAS usarão agentes altamente especializados até 2027, aprimorando a precisão, além de tornar a coordenação mais complexa.

60%

de MAS respaldarão a interoperabilidade multifornecedores até 2028, impulsionando inovação e flexibilidade.

A evolução dos sistemas multiagentes



Fonte: Gartner

4



Gere resultados com sistemas multiagentes

Plano de ação para impulsionar a automação modular e a plena integração

Etapas	1 Identifique casos de uso de alto valor	2 Crie agentes modulares	3 Implemente governança e observabilidade	4 Adote padrões de interoperabilidade	5 Qualifique as equipes
Resultado esperado	Impacto mensurável e adoção mais rápida.	Confiabilidade e escalabilidade aprimoradas.	Risco reduzido e controle otimizado.	Investimentos em MAS com viabilidade garantida a longo prazo.	Implantação eficaz e redução de riscos.
Ação	Comece com fluxos de trabalho bem definidos para testar os MAS.	Crie agentes especializados em vez de soluções monolíticas.	Implemente ferramentas robustas de governança e monitoramento de APIs.	Use protocolos de ponta para a colaboração de agentes de vários fornecedores.	Treine os funcionários em modelos de MAS e gestão de mudanças.

Partes estratégicas para garantir o sucesso da implementação

 CIO	 Parceiros de TI	 Parceiros de negócios
Define a estratégia de MAS para fluxos de trabalho de alto valor e alinhe com as prioridades de negócios. Estabelece a governança visando à interoperabilidade dos agentes, à segurança e à conformidade. Divulga planos de gestão de mudanças para abordar preocupações da força de trabalho.	Plataforma e DevOps: criam agentes modulares e gerencia ferramentas de orquestração. Segurança: implementa a governança de APIs e monitora as interações dos agentes. Equipes de integração: adotam padrões de interoperabilidade e observabilidade.	Proprietários de processos: identificam fluxos de trabalho para pilotos de MAS e validam os resultados. Financeiro: gerencia custos imprevisíveis e aloca orçamento para ferramentas de observabilidade. Operações: apoiam a colaboração entre humanos e agentes, bem como iniciativas de treinamento.

5



Modelos de linguagem específicos ao domínio

O que é?

Os modelos de linguagem específicos ao domínio (DSLML) são sistemas de IA treinados a partir de conjuntos de dados especializados para setores ou funções de negócios em particular, garantindo mais precisão e conformidade em comparação com grandes modelos de linguagem (LLMs) genéricos.

Por que é uma tendência?

Os CIOs precisam extrair valor comercial mensurável da IA. Os DSLMLs reduzem erros, aceleram a implantação e cortam custos de fluxos de trabalho essenciais, como finanças, saúde e RH.

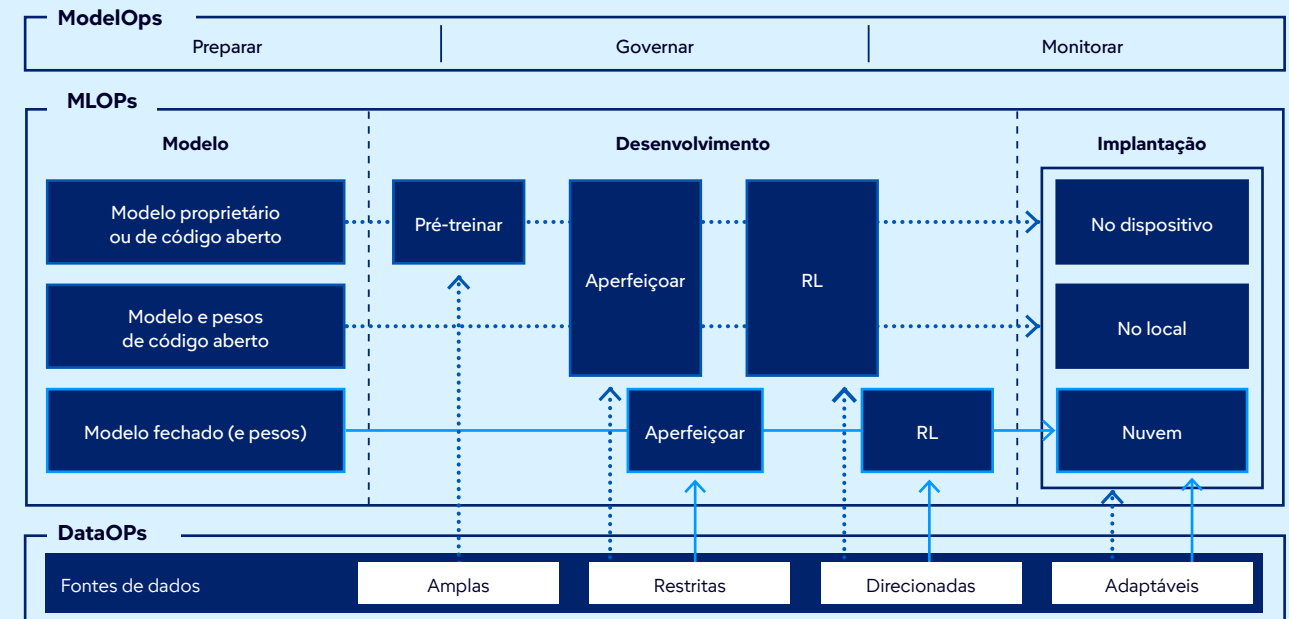
O que vem por aí

+60% dos modelos empresariais de IA generativa serão para domínios específicos até 2028.

30% das cargas de trabalho de IA generativa executarão DSLMLs no local ou no dispositivo até 2028.

Abordagens para criar DSLMLs

... Opções de hospedagem interna — Por meio de API externa



Fonte: Gartner

5



Gere resultados com DSLMs

Plano de ação para assegurar a conformidade específica de cada setor

Etapas	1 Identifique casos de uso de alto impacto	2 Aprimore a governança de dados	3 Teste DSLMs em domínios-chave	4 Forme equipes multifuncionais	5 Monitore e otimize
Resultado esperado	ROI mais rápido e precisão aprimorada.	Resultados de DSLM confiáveis e em conformidade.	Comprovação do valor comercial mensurável.	Integração e adoção facilitadas.	Desempenho sustentável e controle de custos.
Ação	Priorize fluxos de trabalho em que o desempenho de LLMs genéricos é abaixo do esperado.	Implemente controles abrangentes de privacidade e qualidade.	Comece pelos processos financeiros, de saúde ou de RH.	Inclua os departamentos de TI, SMEs e conformidade nos projetos de DSLM.	Implante modelos de explicabilidade e conformidade.

Partes estratégicas para garantir o sucesso da implementação

 CIO	 Parceiros de TI	 Parceiros de negócios
Define a estratégia de DSLM para domínios regulamentados e de alto valor. Garante a governança visando à precisão, à conformidade e à explicabilidade. Alinha a adoção de DSLM com o ROI e as metas de gestão de riscos.	Análise de dados: preparam conjuntos de dados para domínios específicos e asseguram a qualidade. ModelOps: gerenciam o aperfeiçoamento, o monitoramento e a governança do ciclo de vida útil. Segurança: garante privacidade e conformidade para as implantações de DSLM.	Especialistas em domínio: atestam a precisão e a relevância dos resultados de DSLM. Financeiro: aloca orçamento para a adoção de DSLM e a otimização de custos. Conformidade: assegura o cumprimento de padrões regulatórios.

6

IA física

O que é?

A IA física integra inteligência ao mundo real por meio de robôs, drones, veículos e dispositivos inteligentes que detectam, tomam decisões e executam ações. Esses sistemas combinam sensores, atuadores e modelos de IA para automatizar tarefas físicas.

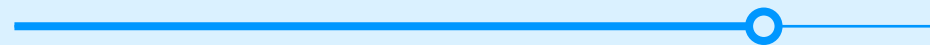
Por que é uma tendência?

As organizações querem replicar a produtividade da IA digital em ambientes físicos. Até 2028, cinco dos dez principais fornecedores de IA oferecerão produtos de IA física.



O que vem por aí

80% dos centros de distribuição usarão robótica ou automação até 2028.



Categorização da IA

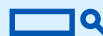
Exemplos



Estimativa de demanda



Chatbots



Mecanismos de recomendação

101100
010110

IA digital



IA



IA física

Exemplos



Robôs industriais



Robôs biônicos/
robótica geral



Dispositivos
autônomos



Tecnologia wearable

Fonte: Gartner



Gere resultados com IA física

Plano de ação para automatizar tarefas do mundo real e impulsionar a produtividade em todos os ambientes

Etapas	1 Analise os domínios operacionais	2 Teste sistemas de IA física	3 Forme equipes multifuncionais	4 Instrua os stakeholders	5 Planeje-se para a coordenação de sistemas multiagentes
Resultado esperado	Identificação de áreas para automação e economia de custos.	Validação do desempenho e do ROI.	Eficácia da governança e da integração.	Eliminação de ambiguidades e de falta de alinhamento nos investimentos.	Garantia de viabilidade das implantações a longo prazo.
Ação	Priorize os fluxos de trabalho de logística, manutenção e segurança.	Faça simulações e utilize gêmeos digitais antes da implantação no ambiente.	Inclua os departamentos de TI, operações e engenharia no planejamento.	Esclareça as diferenças entre IA física, IA embarcada e IA de borda.	Explore plataformas de orquestração para conjuntos de dispositivos.

Partes estratégicas para garantir o sucesso da implementação

CIO	Parceiros de TI	Parceiros de negócios
Define a estratégia de IA física alinhada às metas operacionais. Assegura governança visando à segurança, à confiabilidade e à explicabilidade. Colabora com os departamentos de operações e de engenharia para realizar a integração e a gestão de riscos.	Infraestrutura e operações: integra a IA física em sistemas existentes e de Internet das Coisas. Segurança: implementa mecanismos de proteção para sistemas autônomos. Análise de dados: apoia simulações e testes com gêmeos digitais.	Operações: identificam casos de uso de alto valor e atestam o desempenho. Financeiro: aloca orçamento para investimentos em robótica e automação. Conformidade: assegura o cumprimento de padrões regulatórios e de segurança.



O vanguardista

Amplie a confiança,
a governança e a proteção.

Em um cenário de riscos e fiscalização regulatória cada vez maiores, a confiança é inegociável. As tendências do vanguardista enfatizam segurança proativa, governança transparente e integridade digital. Por meio dessas estratégias, as organizações podem proteger sua reputação, assegurar a conformidade e continuar contando com a confiança dos stakeholders ao expandir a IA e a transformação digital.

7



Segurança cibernética preventiva

O que é?

A segurança cibernética preventiva (PCS) usa técnicas avançadas e impulsionadas por IA para antecipar, bloquear e neutralizar ciberataques antes que aconteçam, indo além da detecção e da resposta tradicionais.

Por que é uma tendência?

As ameaças orientadas por IA estão aumentando exponencialmente e redes, aplicativos e sistemas de IoT são seus alvos. Até 2029, os produtos tecnológicos que não incluem segurança cibernética preventiva perderão relevância no mercado, já que a defesa proativa será uma exigência padrão.

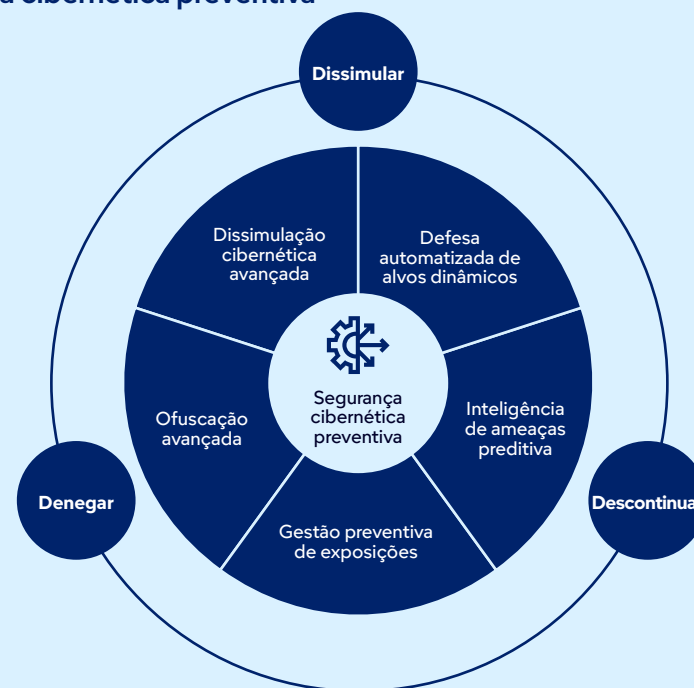
Precisa de insights direcionados para organizações de tecnologia e provedores de serviços? Leia nosso artigo sobre segurança cibernética preventiva para fornecedores: **Não adie o desenvolvimento de soluções de segurança cibernética preventiva.**

O que vem por aí

50% dos gastos com softwares de segurança serão destinados a soluções preventivas até 2030.

1 mi As vulnerabilidades documentadas deverão ultrapassar 1 milhão anualmente até 2030.

Os 3 “Ds” da segurança cibernética preventiva



Fonte: Gartner

7



Gere resultados com segurança cibernética preventiva

Plano de ação para proteger os ativos antes do surgimento de ameaças

Etapas	1 Avalie a arquitetura de segurança atual	2 Teste a PCS em áreas de alto risco	3 Defina critérios de seleção de fornecedores	4 Comunique a estratégia de PCS	5 Integre a PCS com as ferramentas existentes
Resultado esperado	Identificação de lacunas e priorização de investimentos em PCS.	Comprovação da redução mensurável dos riscos.	Adoção da PCS com viabilidade garantida a longo prazo.	Construção de suporte executivo e do conselho.	Maximização do ROI e aceleração da adoção.
Ação	Realize análises de riscos e da prontidão.	Implemente prevenção e dissimulação preditivas contra ameaças.	Exija diretrizes detalhadas das capacidades preventivas.	Comunique o impacto empresarial e o ROI da PCS.	Integre a PCS a processos vigentes de segurança e de conformidade.

Partes estratégicas para garantir o sucesso da implementação

 CIO Defende a mudança das estratégias de segurança, migrando da postura reativa para a preventiva. Define critérios de compra de recursos de PCS e instrui colegas da liderança. Supervisiona a governança visando a medidas de defesa avançada e à conformidade.	 Parceiros de TI Segurança: implanta tecnologias de prevenção e de dissimulação preditivas contra ameaças. Infraestrutura e operações: integra a PCS com sistemas ciberfísicos, de nuvem e de OT. Risco e conformidade: garante o cumprimento de normas regulatórias e de privacidade.	 Parceiros de negócios Financeiro: aloca orçamentos para pilotos de PCS e para a adoção a longo prazo. Operações: apoiam iniciativas de transformação digital segura. Produto: incorpora a segurança preventiva nas ofertas para se diferenciar no mercado.
---	---	--

Rastreabilidade digital

O que é?

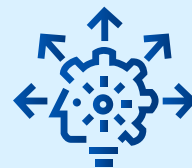
A rastreabilidade digital verifica a origem e a integridade de softwares, dados e mídias, usando ferramentas como listas de materiais (BOMs), bancos de dados de validação e marca d'água. A técnica assegura transparência e confiabilidade em sistemas desenvolvidos a partir de componentes externos e conteúdo gerado por IA.

Por que é uma tendência?

As organizações enfrentam riscos cada vez maiores relacionados à adulteração de código, descontinuação de projetos de código aberto e desinformação impulsionada por deepfake.

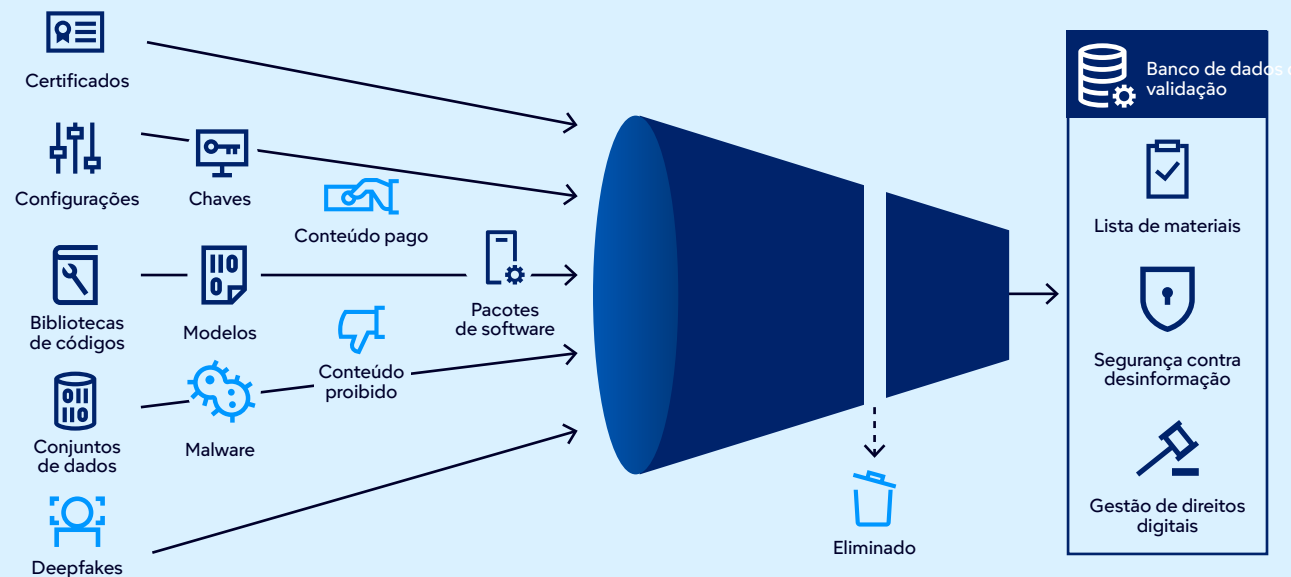


O que vem por aí



Arcabouços regulatórios crescentes – como a Lei de IA da União Europeia – impõem o uso de marca d'água em conteúdos gerados por IA, além da rastreabilidade de sua procedência.

Filtre pela rastreabilidade digital



Fonte: Gartner



Gere resultados com rastreabilidade digital

Plano de ação para assegurar confiabilidade ao verificar a autenticidade dos dados e do conteúdo

Etapas	1 Implante BOMs	2 Implemente um banco de dados de validação	3 Adote ferramentas de segurança contra desinformação	4 Use marca d'água digital	5 Aprimore a governança
Resultado esperado	Viabilização de rastreabilidade, transparência e segurança para softwares.	Centralização e confiabilidade de registros de rastreabilidade.	Proteção contra falsidade ideológica e fraude.	Conformidade com regulamentações para conteúdo de IA.	Redução dos riscos legais e à reputação.
Ação	Implemente BOMs de softwares (SBOMs) para softwares e BOMs de aprendizado de máquina (MLBOMs) para modelos de IA.	Armazene a comprovação da origem assinada criptograficamente.	Integre a detecção de identidades sintéticas aos planos de detecção e resposta de ameaças à identidade.	Identifique as mídias geradas por IA em formatos legíveis por máquina.	Promova a colaboração entre as equipes de TI, conformidade e marketing.

Partes estratégicas para garantir o sucesso da implementação

CIO	Parceiros de TI	Parceiros de negócios
Define uma estratégia de rastreabilidade digital alinhada com a conformidade e a gestão de riscos. Supervisiona a implementação de BOMs e de bancos de dados de validação. Colabora com o CISO e o CMO na resposta contra desinformação e na proteção da reputação.	DevOps: integra SBOMs e MLBOMs aos pipelines de entrega. Segurança: implementa ferramentas de segurança contra desinformação e gestão de direitos digitais (DRM). Dados: documentam a linhagem de dados de treinamento para modelos de IA.	Conformidade: garante o cumprimento de novas regulamentações. Jurídico: valida a conformidade com direitos autorais e licenciamento. Marketing: gerencia riscos à reputação relacionados a deepfakes e conteúdo sintético.



Plataformas de segurança de IA

O que é?

As plataformas de segurança de IA (AISPs) consolidam controles para proteger tanto serviços de IA externos quanto aplicativos de IA personalizados. Elas abordam riscos nativos de IA como injeção de prompts, ações de agentes não autorizados e vazamento de dados.

Por que é uma tendência?

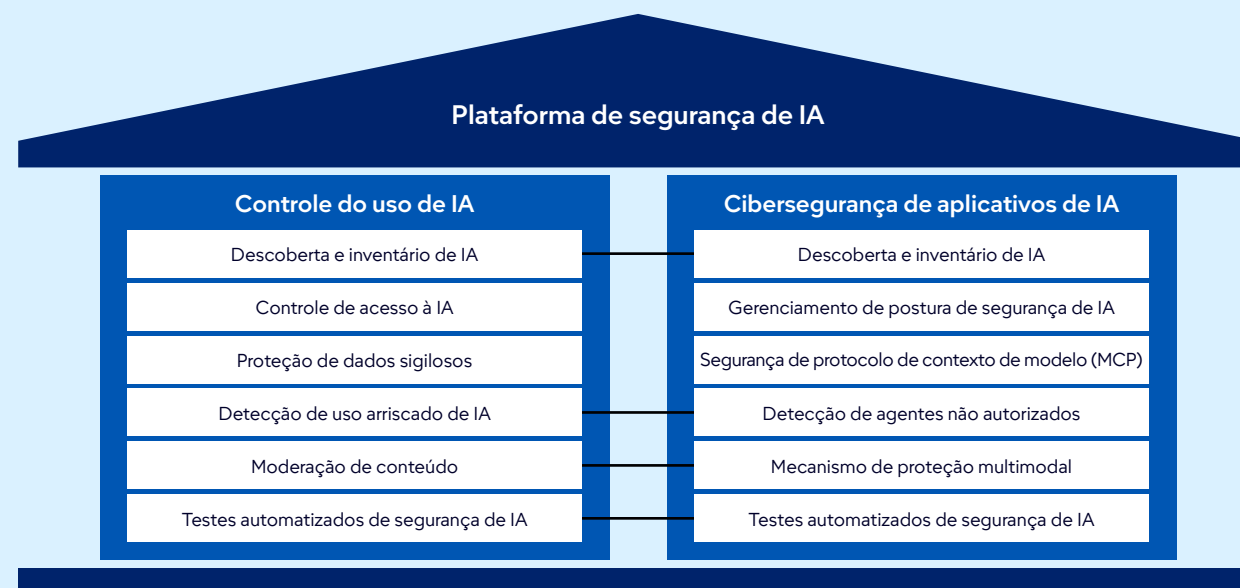
Com o avanço rápido da adoção da IA, as ferramentas tradicionais de segurança falham ao proteger os fluxos de trabalho de IA.

O que vem por aí

+50% das empresas adotarão AISPs até 2028.

80% das transações de IA não autorizadas serão decorrentes de violações de políticas internas, não de ataques externos.

Mapeamento dos recursos da plataforma de segurança de IA



Fonte: Gartner



Gere resultados com plataformas de segurança de IA

Plano de ação para proteger operações de negócios em transformação impulsionadas pela IA

Etapas	1 Avalie o cenário de riscos de IA	2 Teste soluções de AISP	3 Priorize plataformas unificadas	4 Integre testes de segurança	5 Monitore a inovação dos fornecedores
Resultado esperado	Identificação de lacunas no stack de segurança atual.	Validação da eficácia e do ROI.	Simplificação da gestão e redução da complexidade.	Aprimoramento da resiliência contra injeção de prompts.	Antecipação ao surgimento de ameaças.
Ação	Mapeie riscos nativos de IA entre os fluxos de trabalho.	Comece com serviços de IA de alto risco e aplicativos personalizados.	Escolha AISPs que integrem controle do uso de IA e segurança dos aplicativos.	Inclua testes automatizados de segurança de IA aos pipelines.	Acompanhe startups e empresas consolidadas em busca de recursos avançados.

Partes estratégicas para garantir o sucesso da implementação

CIO	Parceiros de TI	Parceiros de negócios
Define uma estratégia de segurança de IA que abrange aplicativos de IA externos e personalizados. Seleciona fornecedores que oferecem soluções unificadas de controle do uso de IA e segurança de aplicativos. Comunica a postura em relação aos riscos de IA e as exigências de conformidade ao conselho.	Segurança: implanta mecanismos de proteção para detectar injeção de prompts e agentes não autorizados. DevOps: integra testes de segurança de IA aos pipelines de desenvolvimento. Infraestrutura e operações: asseguram a compatibilidade com ambientes de nuvem e no local.	Conformidade: alinha as AISPs com modelos regulatórios, como a Lei de IA da União Europeia. Financeiro: aloca orçamento para a adoção da plataforma e a redução dos riscos. Produto: integra recursos de segurança às ofertas habilitadas por IA.

10

Geopatriação



O que é?

Geopatriação é a realocação de cargas de trabalho de nuvens globais em hiperescala para ambientes soberanos ou locais com o objetivo de reduzir o risco geopolítico. O processo inclui estratégias como reimplantação em regiões de nuvem soberana ou repatriação de cargas de trabalho no local.

Por que é uma tendência?

A instabilidade geopolítica e as exigências regulatórias estão obrigando as organizações a reavaliar a dependência da nuvem.

O que vem por aí

75%

das empresas vão utilizar o recurso de geopatriação em suas cargas de trabalho até 2030.

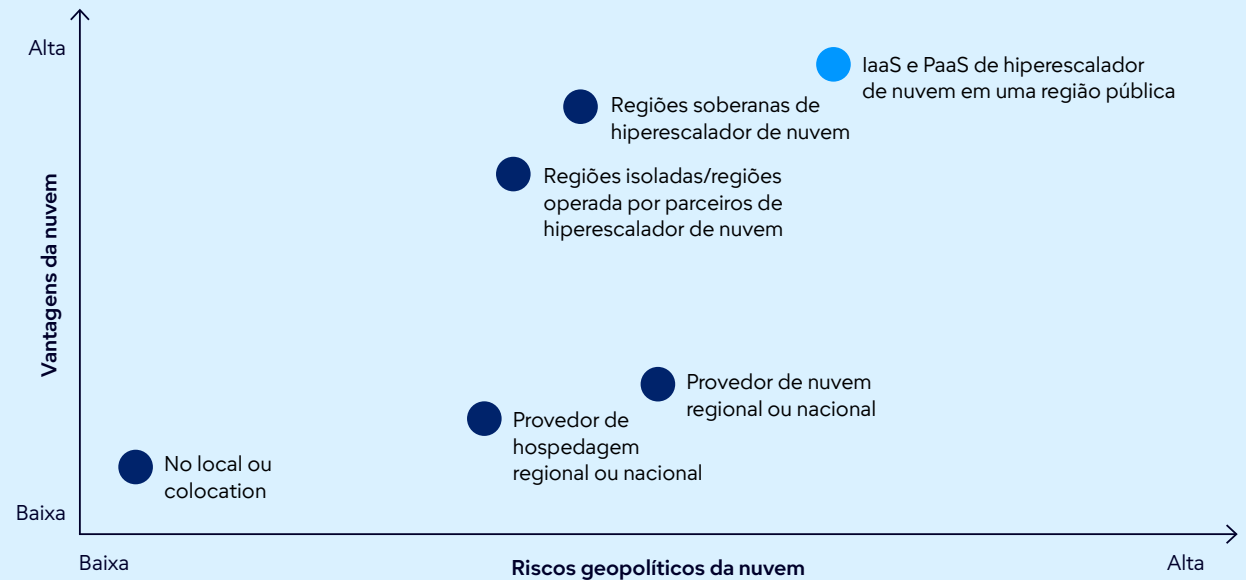


Ofertas de nuvem soberana de hiperescaladores e provedores locais estão se expandindo rapidamente.

Vantagens e riscos geopolíticos da nuvem

● Alternativas para geopatriação

● Cenário atual típico



Fonte: Gartner

10



Gere resultados com geopolitiação

Plano de ação para reduzir o risco ao localizar cargas de trabalho digitais críticas

Etapas	1 Avalie a criticidade da carga de trabalho	2 Considere opções soberanas	3 Elabore estratégias híbridas	4 Implemente controles de governança	5 Monitore tendências geopolíticas
Resultado esperado	Priorização da geopolitiação para ativos de alto risco.	Equilíbrio entre agilidade e soberania.	Manutenção de resiliência e desempenho.	Redução de riscos à conformidade e à segurança.	Adaptação proativa da estratégia.
Ação	Classifique as cargas de trabalho de acordo com a criticidade e a exposição geopolítica.	Compare ofertas soberanas de hiperescalador com provedores locais.	Combine nuvem soberana com hospedagem no local ou colocation.	Adote modelos de validação e de soberania.	Atualize a alocação da carga de trabalho à medida que os riscos evoluem.

Partes estratégicas para garantir o sucesso da implementação

CIO	Parceiros de TI	Parceiros de negócios
Define a estratégia de geopolitiação, equilibrando soberania, agilidade e resiliência. Avalia os prós e contras entre provedores locais e opções de soberania de hiperescaladores globais. Supervisiona a pontuação de risco de cargas de trabalho críticas e o alinhamento da conformidade.	Infraestrutura e operações: planeja rotas de migração e integração com os sistemas existentes. Segurança: valida controles de soberania e assegura a conformidade. Arquitetos da nuvem: otimizam a alocação da carga de trabalho visando ao desempenho e à resiliência.	Conformidade: monitora mudanças regulatórias e exigências de soberania. Financeiro: aloca orçamento para custos de migração e investimentos na redução dos riscos. Operações: asseguram a continuidade durante a realocação da carga de trabalho.

Insights práticos e objetivos

Explore as ferramentas e recursos adicionais gratuitos para líderes de TI:



Modelo

Crie um plano estratégico de TI

Coloque a estratégia em prática com este modelo de planejamento de uma página.

[Acesse o modelo](#)



Ferramenta

Gartner Benchmarking and Diagnostics

Descubra benchmarking que impulsionam decisões de TI mais inteligentes.

[Saiba mais](#)



Insights

Gartner Hype Cycle™ de 2025

O Hype Cycle para IA de 2025 vai além da IA generativa.

[Explore agora](#)



Insights

Principais dúvidas sobre IA e tecnologias emergentes

Os especialistas do Gartner compartilham respostas breves a perguntas dos clientes sobre tecnologias emergentes.

[Confira as respostas](#)

Já é um cliente?

Obtenha acesso a mais recursos no seu portal do cliente. [Faça login](#) ↗

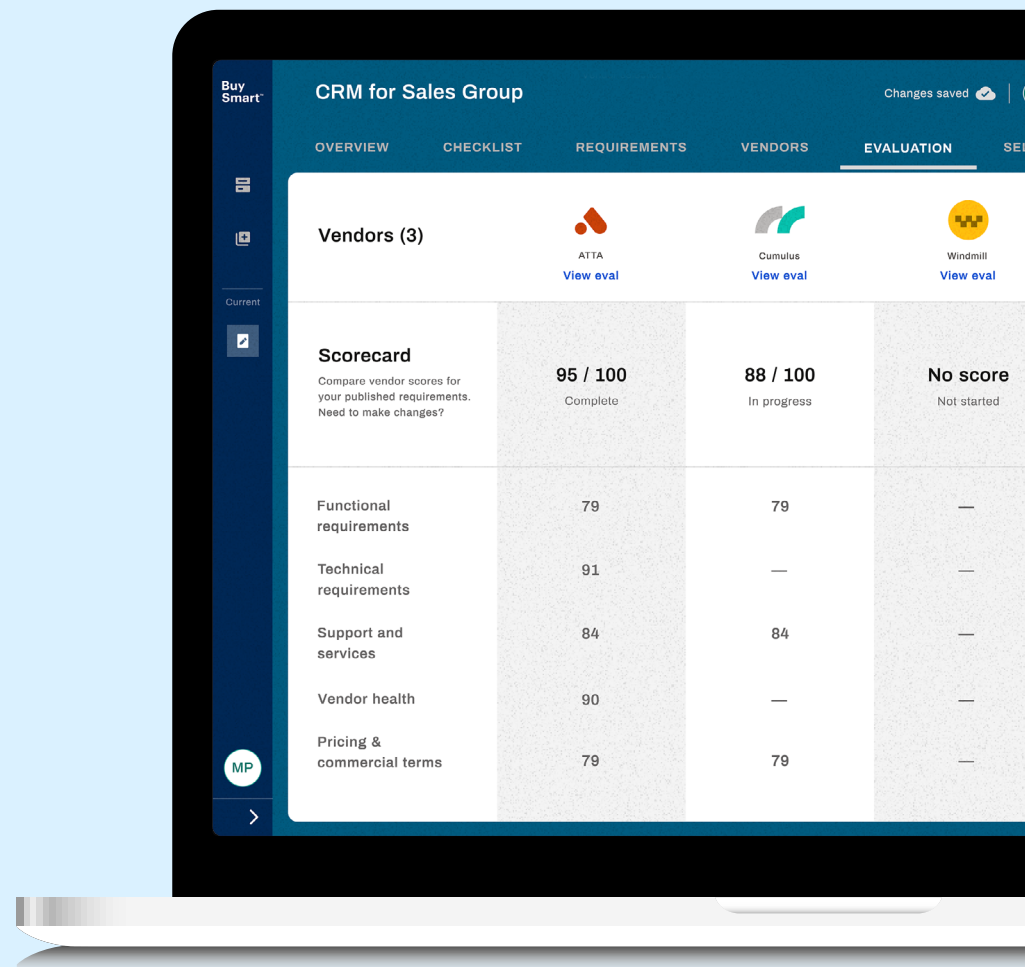


Gartner BuySmart™

Simplifique o processo para sua equipe tomar decisões de compra de tecnologia mais assertivas.

O que você vai obter:

- Acesso a mais de 100 modelos com os principais mercados de tecnologia;
- Listas de verificação e requisitos predefinidos e totalmente personalizáveis;
- Recursos de colaboração para dar suporte ao fluxo de trabalho da sua equipe, tudo em um só lugar;
- Score padronizado para desenvolver a confiança na seleção de fornecedores.



Saiba mais ↗

 Pesquisa

 Pré-selecionar

 Avaliar

 Negociar

Conecte-se conosco

Obtenha insights práticos e objetivos sobre negócios e tecnologia que impulsionam decisões mais inteligentes e otimizam o desempenho em relação às suas prioridades essenciais.

EUA: +1 855 811 7593

Internacional: +44 (0) 3330 607 044

Converse com
um especialista

Saiba mais sobre as soluções do Gartner para diretores de tecnologia da informação e executivos de TI

<https://www.gartner/en/chief-information-officer>



Mantenha-se conectado aos insights mais recentes

Participe de uma conferência do Gartner

[Veja o calendário de conferências](#)

Gartner®