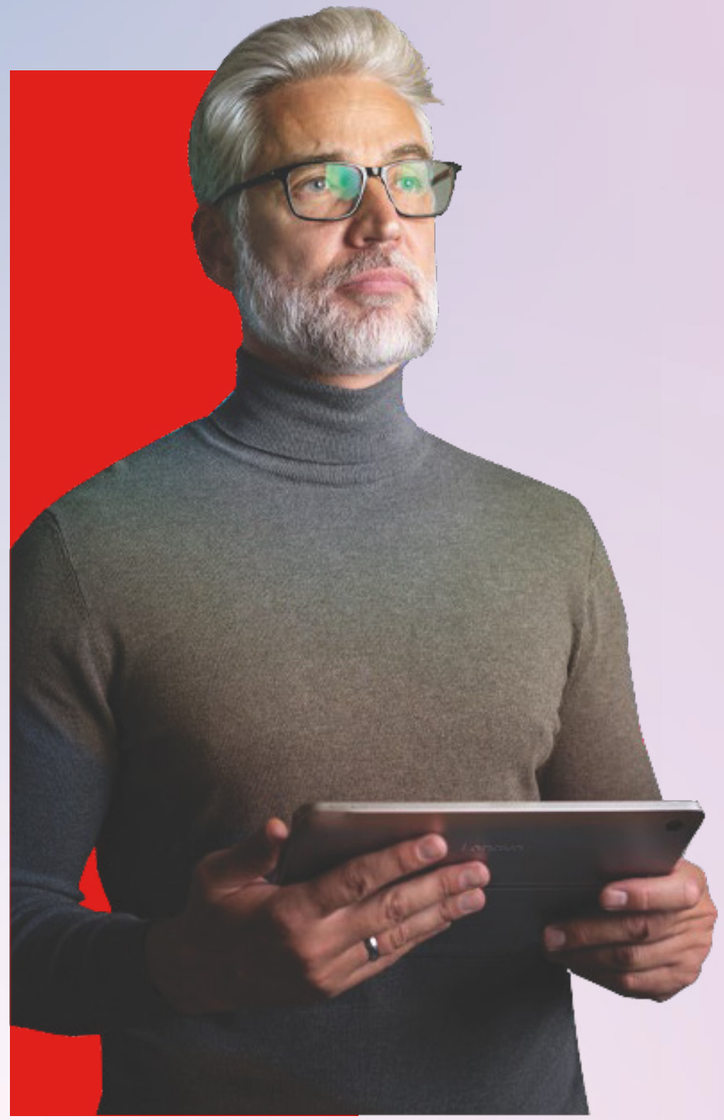


Série de Pesquisas Lenovo Work Reborn 2025

Reforçando o ambiente de trabalho moderno.

Como avaliar e combater com confiança as ameaças de IA enquanto você transforma o ambiente de trabalho digital.

Leia mais

Smarter technology for all

Lenovo

Prepare seu ambiente de trabalho para tudo.

Para turbinar a produtividade dos colaboradores com IA, os líderes de TI precisam transformar o ambiente de trabalho digital. Mas, à medida que as ameaças de segurança evoluem, também é necessário transformar as defesas para garantir que nada interrompa esse avanço.

No primeiro relatório da série Work Reborn, mostramos como a produtividade e engajamento dos colaboradores estão entre as prioridades mais urgentes dos líderes de TI. Ao criar um ambiente de trabalho mais dinâmico, aprimorado por IA e personalizado, as lideranças permitem que as pessoas se concentrem no que fazem de melhor: resolver problemas de forma criativa e colaborar com outros humanos.

Também revelamos que os líderes de TI entendem a necessidade de uma transformação profunda do ambiente de trabalho digital para aproveitar a promessa de produtividade da IA. Os ambientes de trabalho precisam ser reinventados para que a IA dê suporte às necessidades individuais e o suporte de TI deve ser repensado para oferecer experiências contínuas e sem interrupções aos colaboradores.

Agora, investigamos outro pilar vital da transformação do ambiente de trabalho digital na era da IA: a cibersegurança.

O avanço da IA deu origem a novas ameaças, tanto de agentes externos quanto de fontes internas. Nossa pesquisa mais recente, com 600 líderes de TI de grandes empresas, mostra quais preocupações de segurança em IA mais tiram o sono dessas lideranças — e quais riscos podem estar sendo subestimados.

Acreditamos que é necessária uma resposta em duas frentes para reforçar o ambiente de trabalho moderno. Primeiro, as empresas devem intensificar seus esforços para detectar novas ameaças alimentadas por IA, cada vez mais adaptativas. Segundo, precisam fortalecer suas operações de segurança utilizando a própria IA para proteger seus ativos mais valiosos.

Este relatório apresenta o caminho para que líderes de TI evoluam suas defesas e incorporem a IA no coração da arquitetura de cibersegurança, permitindo uma transformação geradora de valor no ambiente de trabalho impulsionado por IA.

Esperamos que você aproveite a leitura.

Rakshit

Rakshit Ghura

Vice President & General Manager
Lenovo Digital Workplace Solutions

Transforme seu ambiente de trabalho sem interromper a segurança.

Nossa pesquisa mostra como as organizações precisam evoluir suas defesas de cibersegurança para a era da IA.

Clique para ir para a seção:

AVALIAR

Identificando novas ameaças de IA.

Os líderes de TI têm razão em se preocupar com os riscos trazidos pela IA — mas nem todos estão confiantes de que conseguem se defender deles.

Entendendo os riscos de ameaças externas.

Os líderes de TI estão atentos aos riscos de cibersegurança que surgem com a IA. Eles se mostram especialmente preocupados com a ameaça representada por cibercriminosos que usam IA, e mais de 6 em cada 10 reconhecem isso como uma fonte crescente de risco de segurança.

90% dos líderes de TI não se sentem “muito confiantes” em sua capacidade de lidar com os riscos decorrentes de cibercriminosos que utilizam IA.

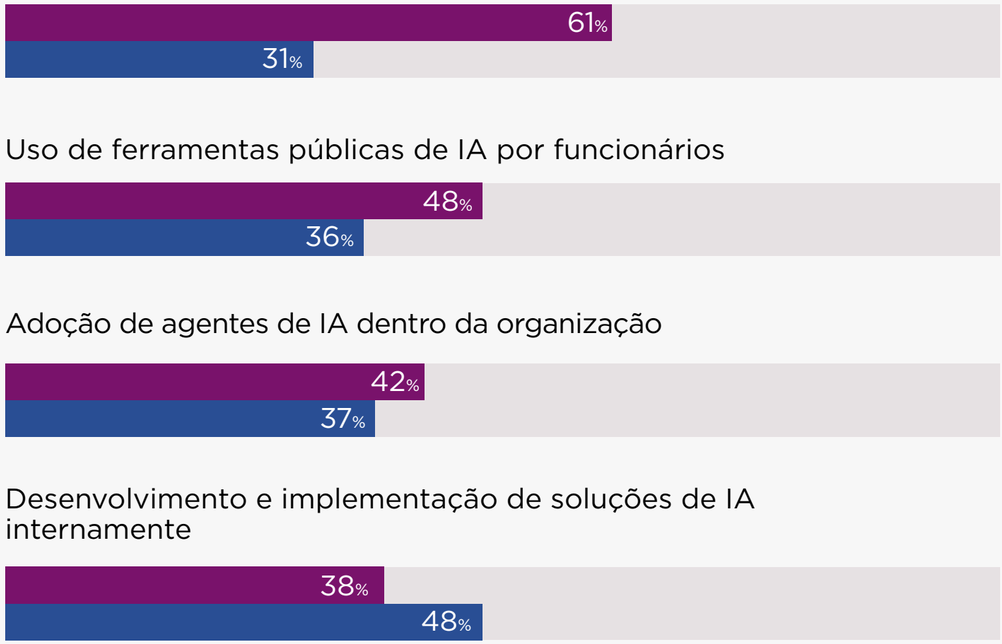
Os líderes de TI têm razão em se preocupar com o uso de IA por cibercriminosos. Em vez de substituir táticas tradicionais, a IA as potencializa — ajudando atacantes a driblar sistemas de detecção com métodos mais rápidos e dinâmicos.

Ataques modernos gerados por IA conseguem evoluir em resposta aos mecanismos de defesa que encontram. Podem imitar comportamentos aparentemente benignos e se propagar por múltiplos domínios: nuvem, dispositivos, aplicações e muito mais.

Onde os riscos estão crescendo x confiança para lidar com eles:

% que relatam aumento “significativo” ou “moderado” no risco de cibersegurança

% que se dizem “muito” ou “razoavelmente” confiantes em sua capacidade de gerir esses riscos



AVALIAR

Lidando com ameaças internas de IA.

Identificar ataques baseados em IA vindos de fontes externas é apenas uma dimensão do desafio de segurança em IA.

Mais de 6 em cada 10

líderes de TI concordam que agentes de IA representam um novo tipo de ameaça interna para a qual eles não estão totalmente preparados.

Sete em cada 10

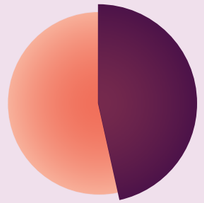
concordam que o uso indevido de IA por funcionários é um risco que precisa ser endereçado.

Menos de 4 em cada 10

se sentem confiantes em sua capacidade de gerenciar qualquer um desses riscos.

A IA está evoluindo rapidamente e as implicações de cibersegurança associadas a ela só agora começam a ficar claras. Isso se estende à proteção da própria IA — incluindo modelos, dados de treinamento e prompts — que se tornou outro objetivo central das equipes de segurança.

Embora a confiança seja baixa quando o assunto é se defender de ataques externos habilitados por IA, os líderes de TI se sentem mais seguros em relação à gestão dos riscos que surgem de iniciativas internas de IA.



Quase metade (48%)

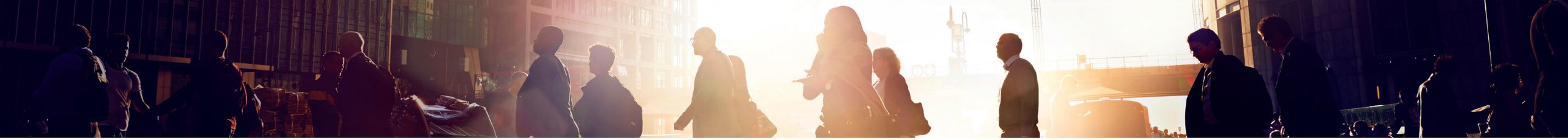
dos líderes de TI se dizem “muito” ou “razoavelmente” confiantes em sua capacidade de gerenciar riscos decorrentes do desenvolvimento e implementação de soluções de IA dentro da organização.

Se as organizações já adotaram medidas de cibersegurança adequadas para proteger sistemas internos de IA, essa confiança pode estar bem fundamentada. Mas também é possível que alguns estejam subestimando os riscos.

“Os líderes de TI estão focados na corrida para implementar múltiplas iniciativas de IA — mas isso pode fazê-los ignorar vetores de ameaça que surgem exatamente dessas implementações.”

Tiago Da Costa Silva

Security Services Director
Lenovo Digital Workplace Solutions



AVALIAR

Novos riscos pedem novas abordagens.

As capacidades tradicionais de cibersegurança não são suficientes para lidar com os riscos relacionados à IA.

Os líderes de TI precisam garantir que suas capacidades de cibersegurança acompanhem os riscos relacionados à IA. Em muitos casos, esses riscos exigem abordagens fundamentalmente novas.

Por exemplo, medidas tradicionais de proteção de dados — como limitar o acesso com base na função do usuário — já não são suficientes quando um sistema de IA varre dezenas de documentos para encontrar a resposta a uma pergunta de um colaborador.

Da mesma forma, abordagens tradicionais de segurança de endpoint — como antivírus — só identificam ameaças depois que elas foram descobertas e catalogadas. A IA permite criar código malicioso muito mais rápido do que antes e facilita a geração de malware polimórfico, que se modifica para evitar detecção e se mistura às atividades normais.

Diante desses novos riscos, as empresas precisam atualizar suas capacidades e reforçar a proteção dos ativos mais valiosos.

"A capacidade da IA generativa de criar ataques polimórficos deu aos adversários uma vantagem assimétrica, permitindo ataques mais rápidos, evasivos e que se misturam à atividade normal, escapando dos mecanismos tradicionais de detecção. Mesmo com Zero Trust, os defensores precisam assumir e se preparar para falhas de detecção."

David Majernik

Senior Offering Design Technologist
Lenovo

Fatores de risco em cibersegurança de IA

Ameaças emergentes a serem observadas:

- Envenenamento de modelo/dados
- Manipulação de modelos de IA
- Vazamento de privacidade de dados de IA
- Acesso excessivo ou permissões acima do necessário
- Entradas adversariais em IA
- Malware impulsionado por IA
- Ataques de negação de serviço por exaustão de cargas de IA
- Alucinações e desinformação geradas por IA
- Vazamento de dados via aplicações de IA
- Uso de shadow AI
- Riscos na cadeia de suprimentos de IA
- Viés e riscos éticos que levam à não conformidade regulatória
- Ataques de força bruta potencializados por IA

AVALIAR

Avaliando suas capacidades de defesa.

Os líderes de TI entendem a importância da proteção de dados e da gestão de vulnerabilidades, apontando essas áreas como as duas capacidades mais importantes para se defender de ameaças relacionadas à IA. Mas nem todos têm certeza de que suas capacidades dão conta do recado.

Falta confiança

Mais da metade (54%) dos líderes de TI acredita que suas ferramentas, processos e equipes de proteção de dados não são totalmente suficientes para lidar com ameaças de cibersegurança relacionadas à IA.

A confiança é ainda menor em relação às capacidades de análise de vulnerabilidades e ameaças

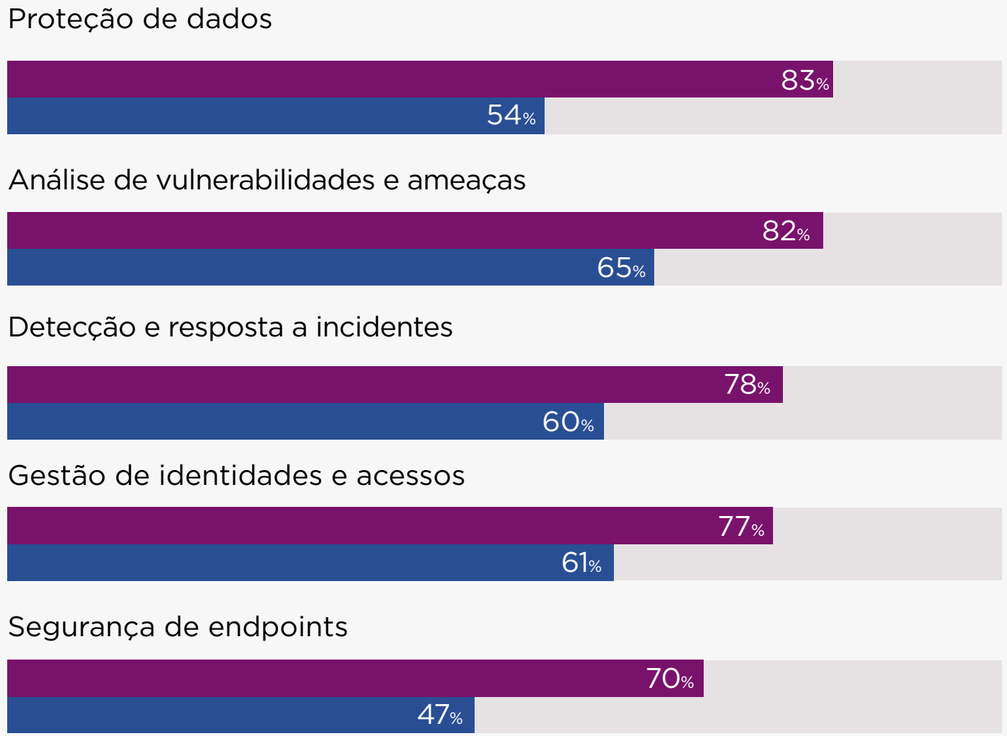
65% acreditam que suas capacidades atuais não são plenamente suficientes para enfrentar ameaças de IA.

A maioria também tem dúvidas sobre suas capacidades de detecção e resposta a incidentes e de gestão de identidades e acessos.

Capacidades que os líderes consideram importantes x confiança nelas

% que consideram "crítica" ou de "alta importância" para enfrentar os riscos de IA

% dizem que as capacidades atuais não são totalmente suficientes para lidar com os riscos de IA



AVALIAR

Como entender e mitigar riscos de IA.

Recomendações para identificar e mitigar riscos impulsionados por IA, tanto de fontes internas quanto externas.

Para ameaças externas.

Reconheça as novas ameaças de IA externas e tome medidas proativas para proteger seus sistemas.

Reavalie seus sistemas de segurança.

Com a baixa confiança dos líderes de TI em suas capacidades de cibersegurança, é fundamental que as empresas tenham clareza sobre suas habilidades defensivas atuais diante das ameaças de IA. Isso começa com avaliações dinâmicas da postura de segurança cibernética e da tecnologia da organização, para garantir que o nível de risco esteja alinhado ao que o negócio considera aceitável.

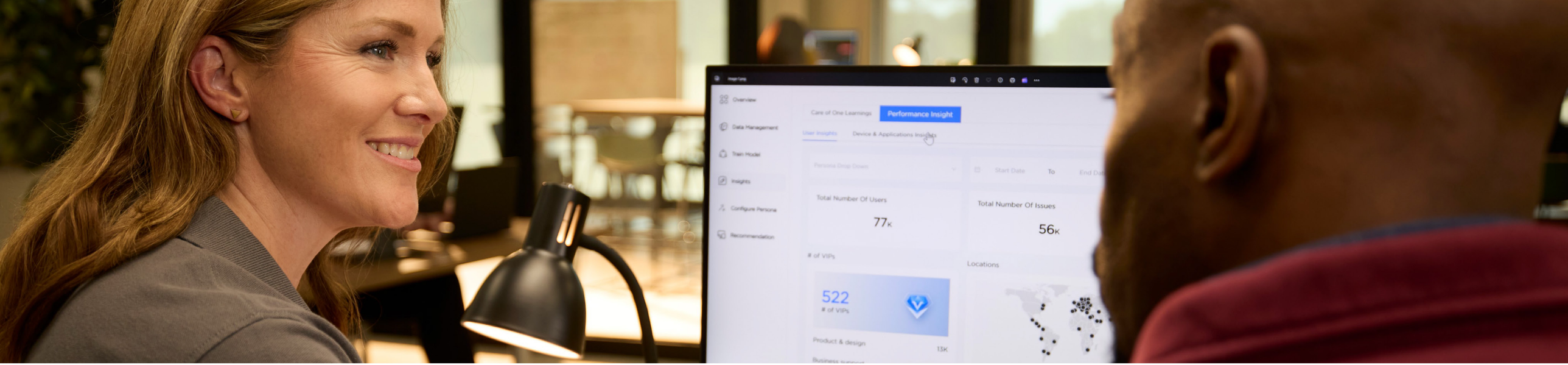
Fique à frente das ameaças.

Quem ataca agora opera em velocidade de máquina, levando apenas alguns instantes para ganharem vantagem e causarem danos irreversíveis antes que as defesas tradicionais possam responder. As organizações precisam ir além do monitoramento isolado e adotar uma capacidade de interpretação nativa em IA: a habilidade de traduzir sinais em tempo real, vindos de múltiplos domínios, em respostas inteligentes e coordenadas. Ao unificar a arquitetura de telemetria e consolidar análises contextuais em todas as camadas, as organizações conseguem detectar, compreender e agir antes que as ameaças se estabeleçam.

Reduza vulnerabilidades humanas.

Identificar ameaças de IA exige ir além de programas estáticos de conscientização. Atacantes avançados podem usar engenharia social com IA, como deepfakes de voz e vídeo, para induzir colaboradores a compartilhar informações sensíveis ou credenciais. Assim como os funcionários precisam reconhecer um e-mail de phishing, também devem ser treinados para identificar e mitigar ameaças sofisticadas baseadas em IA.

Supere as ameaças em velocidade



Para ameaças internas.

Identifique pontos frágeis que surgem com sistemas e práticas internas de IA — muitas vezes ignorados pelas abordagens tradicionais de cibersegurança.

Estabeleça políticas claras de uso de IA.

Colaboradores podem não perceber que inserir informações sensíveis em sistemas públicos de IA pode tornar esses dados acessíveis a outros usuários fora da organização. É essencial definir políticas explícitas e mecanismos de controle para orientar os funcionários e afastá-los de comportamentos de risco.

Audite direitos de acesso.

Se os privilégios de acesso a dados por agentes de IA não forem controlados com rigor, esses agentes podem comprometer as medidas internas de proteção de dados ou ser utilizados por atacantes para extrair rapidamente informações sensíveis. O risco de vazamento de dados exige que as empresas reforcem o monitoramento e garantam que sistemas de IA e colaboradores só acessem o que realmente precisam.

Proteja o ciclo de desenvolvimento de IA.

Criar e implementar sistemas de IA dentro da organização traz novos tipos de risco. Por exemplo, se cibercriminosos alterarem os dados de treinamento de uma solução de IA voltada ao cliente, isso pode causar grande dano reputacional e regulatório. As organizações devem estabelecer controles internos e verificações que impeçam a manipulação desses sistemas.

EVOLUIR

Combatendo IA com IA.

Para enfrentar os riscos de cibersegurança da IA, os líderes de TI precisam desbloquear todo o potencial da própria IA.

Aumentando a capacidade de reação.

Em um ambiente onde a velocidade dos ataques supera a capacidade de resposta humana, utilizar IA para apoiar e ampliar a tomada de decisão das equipes de segurança é fundamental.

Soluções de cibersegurança integradas à IA também permitem que as equipes interajam com suas ferramentas por meio de linguagem natural, em vez de navegar por diversas telas para encontrar rapidamente as informações necessárias em uma situação crítica.

"Do ponto de vista da segurança, quanto mais holística é a visão do que está acontecendo, mais rápido você consegue perceber que algo está errado."

Mikkel Seiero

Global Security Services Offering Lead
Lenovo

A conquista de uma visibilidade unificada.

Em arquiteturas tradicionais de cibersegurança corporativa, capacidades como proteção de dados e análise de vulnerabilidades costumam ser responsabilidade de equipes separadas, com ferramentas especializadas. Adversários que usam IA generativa exploram os pontos cegos entre essas funções, reduzindo a capacidade de observação dos ataques.

Para enfrentar esse cenário, as equipes de segurança precisam de uma visão holística da postura de segurança da empresa — cruzando domínios e utilizando múltiplos conjuntos de ferramentas. Extrair inteligência, pontuações dinâmicas de postura de segurança e ações automatizadas a partir dessa visão agregada só é possível com apoio de IA.

"A visibilidade é o primeiro passo para a segurança em IA — ao obter visão completa de todos os módulos e aplicações de IA, suas funcionalidades e o uso contínuo, conseguimos proteger dados sensíveis, garantir conformidade e defender a organização contra ameaças emergentes baseadas em IA."

Kamrul Hasan

Cybersecurity Architect
Lenovo

EVOLUIR

Os obstáculos para integrar IA à cibersegurança.

Para se defender das ameaças do futuro, as equipes de TI precisam usar IA em toda a defesa do ambiente de trabalho digital. Mas chegar lá não é simples.

Nossa pesquisa mostra que as empresas já avançaram na adoção de IA em cibersegurança. Quase metade, por exemplo, usa IA e automação extensivamente em segurança de endpoints e gestão de identidades e acessos (IAM).

Mas, com menos da metade dos líderes se dizendo plenamente confiantes em suas capacidades de segurança para lidar com riscos de IA, ainda há muito espaço para melhoria.

E reforçar medidas de cibersegurança com IA não é apenas uma questão de instalar a ferramenta certa. Para muitas organizações, existem barreiras significativas a superar.

Barreira 1: Ambientes de TI complexos.

dos líderes de TI dizem que a “complexidade do ambiente de TI” é uma das principais barreiras para a segurança impulsionada por IA.

Nossa pesquisa revela que a barreira mais comum é a complexidade do ambiente de TI.

A maioria das grandes empresas possui um parque de TI — incluindo o conjunto de ferramentas de cibersegurança — que se desenvolveu ao longo de décadas. Isso geralmente inclui soluções legadas que não são suportadas por novas plataformas de segurança com IA.

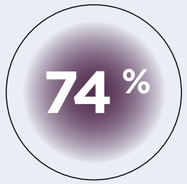
Barreira 2: Falta de profissionais especializados em cibersegurança.

dos líderes de TI afirmam que “custo das soluções / orçamento limitado” é uma das principais barreiras à segurança com IA.

A segunda barreira mais comum é a escassez de profissionais qualificados na área de cibersegurança. Isso não surpreende: habilidades em IA e em cibersegurança são ambas muito demandadas e difíceis de encontrar. Ter pessoas experientes nas duas áreas é ainda mais desafiador.

Essa falta de talentos é agravada pela carga crescente sobre analistas de segurança, que trabalham em um ambiente de alta pressão cognitiva, lidando com adversários cada vez mais sofisticados.

Barreira 3: Custo das soluções/orçamentos limitados.



dos líderes de TI apontam a “falta de profissionais qualificados na função de cibersegurança” como uma barreira importante para a segurança baseada em IA.

Ferramentas avançadas, profissionais especializados e investimentos contínuos em prontidão para IA exigem recursos significativos. Para muitas organizações já sob pressão orçamentária, direcionar fundos para tecnologias emergentes é um desafio — especialmente quando ferramentas existentes ainda funcionam, mesmo que estejam desatualizadas.

EVOLUIR

Como transformar suas defesas.

Recomendações práticas que as organizações podem adotar para se defender de ameaças impulsionadas por IA.

Construa uma visão holística.

Com ambientes de TI complexos e equipes de segurança sobrecarregadas, conjuntos fragmentados de ferramentas geram ineficiências, custos ocultos e visibilidade limitada de ameaças. Consolidar a telemetria de usuários, endpoints, aplicações e infraestrutura em nuvem ajuda a reduzir a proliferação de ferramentas e o custo de treinamento — ao mesmo tempo em que cria a visão unificada necessária para detectar e responder mais rápido a ameaças com IA.

Adote ferramentas versáteis.

Grandes empresas frequentemente mantêm sistemas essenciais ao negócio em plataformas legadas que não podem ser facilmente migradas. Para aproveitar recursos de cibersegurança baseados em IA, é preciso adotar soluções de segurança que compatibilizem uma ampla variedade de sistemas operacionais, inclusive aqueles que, de outra forma, estariam fora de suporte.

Reforce sua equipe com parceiros experientes.

As ameaças baseadas em IA avançam rapidamente, enquanto treinar equipes internas leva tempo e exige investimento. Ampliar capacidades por meio de parceiros especializados oferece acesso imediato às habilidades necessárias, na escala que o desafio exige.

Bem-vindo ao Work Reborn, reforçado.

Proteger o ambiente de trabalho digital na era da IA em evolução exige reinventar completamente a forma como as empresas monitoram, compreendem e respondem a ameaças de cibersegurança, e como defendem seus ativos digitais.

Para virar o jogo contra ameaças com IA generativa, as empresas precisam:

- **Aprimorar as capacidades de detecção.**

  Dado que ameaças alimentadas por IA conseguem escapar da detecção, as organizações devem redobrar esforços para proteger seus ativos de alto valor. Isso inclui os próprios sistemas de IA — agentes, modelos, dados de treinamento e prompts são alvos cada vez mais valiosos para agentes maliciosos.

- **Aproveitar as capacidades da própria IA.**

  As organizações também precisam adotar uma postura de segurança mais adaptativa, enfrentando ameaças em tempo real sempre que possível. Isso só é viável ao utilizar as mesmas capacidades de IA usadas pelos atacantes, oferecendo às equipes de segurança os insights, o contexto e as recomendações rápidas de que precisam.

Essa abordagem em duas frentes gera melhores resultados de negócio:

Mais produtividade.

Incorporar IA às operações de segurança pode fortalecer a produtividade das equipes de cibersegurança. O Microsoft Security Copilot, assistente de IA para equipes de segurança, pode aumentar a produtividade de equipes de SecOps entre 23% e 47%, segundo avaliação da Forrester Research[1]. De acordo com análises da própria Microsoft, conflitos de políticas em dispositivos podem ser resolvidos 54% mais rapidamente[2], e incidentes podem ser encerrados 30% mais rápido[3] com o uso do Security Copilot.

Redução de custos.

Transformar suas defesas com IA traz diversos benefícios financeiros. Ao criar uma visão holística das operações de segurança com o apoio de IA, você reduz custos de treinamento necessários para usar as ferramentas subjacentes. Também é possível minimizar custos de manutenção otimizando o número de ferramentas utilizadas — e abrir espaço para terceirizar funções não estratégicas para parceiros que tenham escala para entregar com eficiência de custo.

Transformação sem atritos.

Talvez o mais importante seja que modernizar a cibersegurança para a era da IA em alta velocidade dá a confiança necessária para abraçar totalmente a transformação do ambiente de trabalho digital. Nossos estudos anteriores mostraram que preocupações de segurança são uma das barreiras mais comuns para a adoção de IA por líderes de negócio — e, como vimos, tais preocupações são justificadas. Por isso, qualquer transformação do ambiente de trabalho liderada por IA precisa vir acompanhada de uma atualização de cibersegurança.

1 New Technology: The Projected Total Economic Impact™ Of Microsoft Security Copilot, Forrester Research, November 2024
2 Security Copilot: Evidence of Productivity Gains in Live Operations, Microsoft Corporation, March 2025
3 Generative AI and Security Operations Center Productivity: Evidence from Live Operations, Microsoft Corporation, November 2024

Pronto para transformar com segurança o seu ambiente de trabalho?

Avalie com confiança as ameaças de IA e garanta que sua organização esteja segura enquanto moderniza o ambiente de trabalho digital.

Comece aqui.

A visão é sua. Chegue lá com a Lenovo.

Metodologia

Para este estudo, a Lenovo entrevistou 600 líderes de TI entre abril e maio de 2025. A amostra incluiu respondentes dos Estados Unidos (17%), Canadá, Reino Unido, França, Alemanha, Índia, Japão, Cingapura, Brasil e México (8% cada), Austrália (4%) e Nova Zelândia (4%). Os participantes eram líderes de TI de empresas com pelo menos 1.000 funcionários, atuando em diversos setores.

Smarter technology for all

Lenovo