

Forcepoint AI Data Security

Proteja a IA. Comece pelos dados.

Desafio:

- › Agentes de IA autônomos agem sem supervisão, herdando permissões de usuário para consultar, agregar e transmitir dados sensíveis na velocidade da máquina, sem nenhuma pessoa no controle
- › A organização média tem 37 agentes de IA em uso, a maioria desconhecida pela TI e se espalhando tão rápido quanto uma extensão de navegador
- › Cada prompt enviado a um LLM público ou ao Copilot é uma possível transferência de dados, que tira PII, código-fonte e dados financeiros do controle da empresa instantaneamente

Soluções:

- › Governe agentes autônomos no ponto de ação, aplicando acesso de privilégio mínimo e controles com reconhecimento de identidade, para que cada ação seja atribuída e controlada
- › Descubra e controle a Shadow AI identificando continuamente ferramentas não autorizadas e aplicando políticas de acesso antes que elas se tornem uma exposição sem gerenciamento
- › Estenda a proteção de dados a cada prompt aplicando as políticas existentes de classificação e DLP a prompts, respostas e uploads de arquivos nas plataformas de IA autorizadas

Resultados:

- › Adote a IA com confiança, mantendo uma proteção de dados consistente
- › Estenda os investimentos existentes em segurança de dados à IA sem precisar reconstruir políticas
- › Demonstre uma governança de IA responsável com evidências claras e auditáveis

A IA transformou o cenário da segurança de dados e abriu novos caminhos de risco que as ferramentas de segurança tradicionais não conseguem bloquear. Os funcionários compartilham informações sensíveis por meio de prompts, e não de arquivos. As ferramentas de Shadow AI se espalham mais rápido do que a TI consegue rastrear. Agentes autônomos consultam e transmitem dados corporativos sem revisão humana. O que este momento exige é uma segurança que governe o que a IA pode acessar antes que ela chegue a esses dados.

Governe cada interação de IA a partir de uma única plataforma

O Forcepoint AI Data Security estende a cada interação de IA a mesma proteção já confiável em outros canais.

Aplique automaticamente a sua política de proteção de dados existente aos prompts de IA, às respostas dos agentes e ao tráfego entre agentes e aplicações, sem nenhuma reclassificação.

Veja a IA autorizada, a Shadow AI e os agentes em uma única console

Um console unificado governa todas as superfícies de IA: as plataformas autorizadas que os funcionários usam todos os dias, as ferramentas de Shadow AI que nunca passaram por revisão e os agentes autônomos que atuam sobre dados corporativos sem supervisão humana. Nada exige uma ferramenta ou política separada.

Aplique políticas em todas as superfícies de IA

O Forcepoint AI Data Security age sobre o risco, em vez de apenas relatá-lo: remedia prompts e respostas sensíveis, revoga acessos compartilhados em excesso e retém ações de agentes de alto risco até a aprovação. Uma única estrutura de políticas orienta cada resposta, de modo que a proteção permaneça consistente, não importa onde o risco surja.

Alcance uma IA governada em minutos, não em meses

O Forcepoint ARIA, o assistente de IA integrado, leva os administradores do primeiro login a um ambiente de IA governado, sem necessidade de serviços profissionais. Ele recomenda uma configuração inicial de políticas com base na região, no setor e na sensibilidade dos dados, oferecendo orientações em linguagem simples.

Obtenha provas de governança para os reguladores e para o seu conselho

Cada interação de IA e cada ação de agente é registrada em uma única trilha de auditoria imutável, que oferece suporte aos requisitos de EU AI Act, NIST AI RMF, GDPR, DORA, NIS2, LGPD e SEC. Agora você pode demonstrar governança sob demanda, em vez de depois do fato.

Como funciona: conhecer, adaptar, proteger

Conhecer

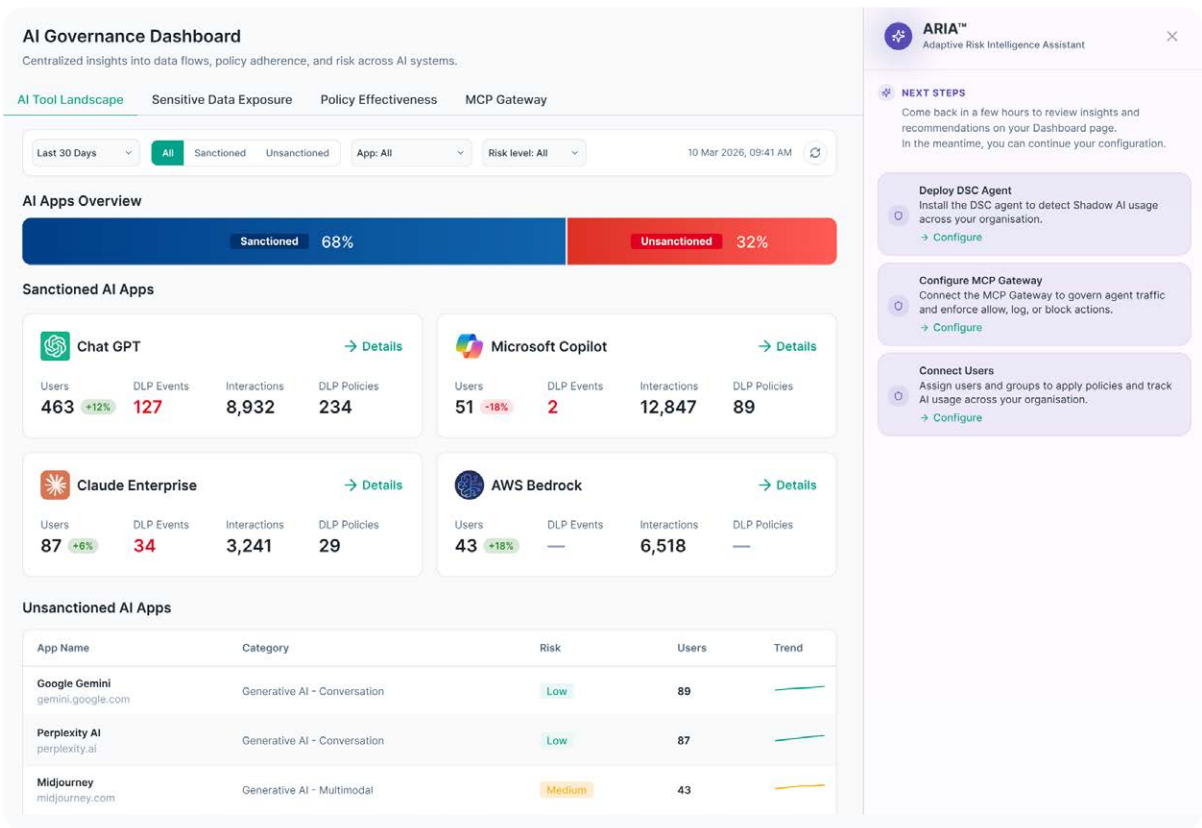
Entenda o risco da IA à medida que ele se forma

O Forcepoint AI Data Security oferece uma visão continuamente atualizada do ambiente de IA da empresa:

- Um inventário centralizado de plataformas de IA autorizadas, ferramentas de Shadow AI e agentes de IA
- Visibilidade baseada em API dos serviços de IA corporativos, incluindo a atividade histórica no momento da conexão

- Visibilidade de endpoints para detectar aplicações de IA não aprovadas e agentes executados localmente
- Classificação prévia de dados sensíveis em fontes estruturadas e não estruturadas, tornando as interações de IA cientes dos dados desde o início
- Atribuição completa de cada interação de IA ao usuário humano, ao agente de IA ou ao par agente-usuário envolvido

As equipes de segurança passam a ter uma visão operacional única de onde existe risco de IA e de quem é o responsável por ele.



Adaptar

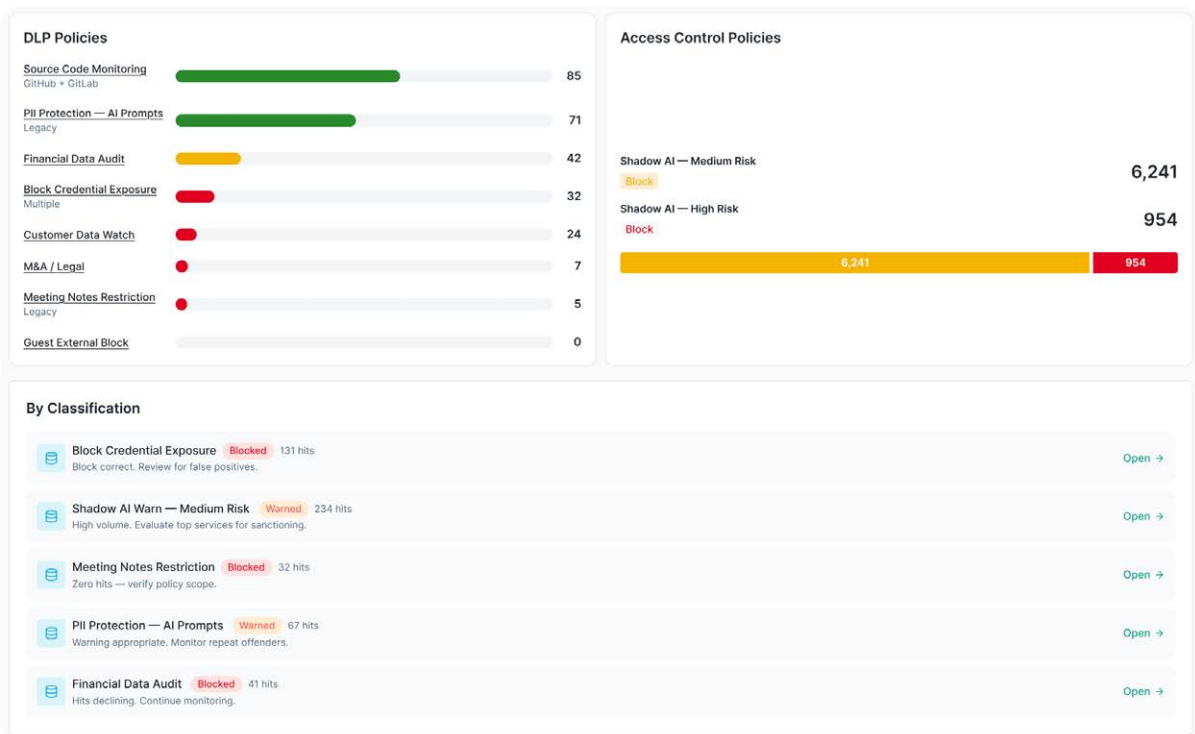
Transforme insight em ação na velocidade da IA

Visibilidade por si só não basta se a aplicação das políticas não consegue acompanhar o ritmo. O Forcepoint AI Data Security adapta a proteção automaticamente à medida que o uso de IA evolui:

- As políticas de segurança de dados existentes se estendem a prompts, respostas, uploads de arquivos e ações de agentes de IA, sem reconstrução de políticas nem reclassificação
- Uma única estrutura de políticas governa e-mail, web, endpoints, SaaS e IA, para uma proteção consistente em qualquer lugar por onde os dados fluam

- O Forcepoint ARIA orienta os administradores do primeiro login a um ambiente de IA governado, sem necessidade de serviços profissionais
- Os controles de remediação permitem que as equipes orientem usuários, restrinjam ações, exijam aprovação para a execução de agentes ou bloqueiem atividades de alto risco
- Agentes autônomos são restritos ao privilégio mínimo, impedindo excessos causados por permissões herdadas e por injeção de prompt antes mesmo que comecem

Essa abordagem permite que as organizações governem a adoção de IA sem reduzir a produtividade.



Proteger

Aplique proteção consistente onde quer que a IA interaja com dados

O Forcepoint AI Data Security aplica a proteção no ponto de interação, e não depois que a exposição ocorre:

- A aplicação baseada em API se conecta diretamente às plataformas de IA autorizadas para inspecionar prompts, respostas e ações de agentes, sem exigir proxies, extensões de navegador nem mudanças na rede
- A aplicação em endpoints estende a proteção à atividade de IA que ocorre localmente nos dispositivos, incluindo agentes executados localmente e ferramentas de IA baseadas em navegador
- O AI Agent Gateway intermedeia as credenciais de agentes autônomos que chamam aplicações corporativas, como Salesforce e Microsoft 365, inspecionando cada resposta no nível de campo e reterdo ações de alto risco até a aprovação

- Barreiras de proteção de acesso a dados impedem que assistentes de IA exponham dados compartilhados em excesso ou classificados incorretamente, remediando o acesso antes da exposição
- Quase 2.000 modelos, políticas e classificadores cobrem 80 ou mais regiões regulatórias prontos para uso, bloqueando colagens, uploads e compartilhamentos de risco sem paralisar os funcionários
- Cada ação de aplicação é registrada com atribuição completa de identidade para criar um registro auditável

Isso proporciona proteção imediata e consistente para a atividade de IA conduzida por pessoas e para a autônoma.

Policy

Access Control

Data Security

Content Inspection Policies

Inspect and control what data users share with AI tools. Define allow/block rules for sensitive data categories like PII, PHI, source code, and financial data.

Search policies...

Filters

On-prem DLP policies are managed in FSM

Name	Classifier	Action	Status
Australia PII Government-issued travel document identifiers	PII	✓ Audit	☒
Biometric Files Biometric Files	PII	✓ Audit	☒
Business and Technical Drawings Files State and national driving license identifiers	Identity	Alert	☒
Call Detail Records Fingerprints, facial recognition, retinal scans	Identity	⚠ Alert High	☒
Credit Card Magnetic Strips Personal and corporate email identifiers	PII	Alert	☒
Financial Information Bank accounts, transaction records, payment information	Financial	Alert	☒
HIPAA The Health Insurance Portability and Accountability Act	PII	✓ Audit	☒
India PHI Policy for detection of protected health information	Identity	✓ Audit	☒
Japan PII Policy for detection of Japanese private information.	Identity	✓ Audit	☐
Location coordinates Policy for detection of location coordinates.	Financial	Alert	☐

4

Principais recursos

Proteção de dados em todas as interações de IA

Inspecione prompts, respostas e uploads de IA usando as mesmas classificações de dados que já protegem e-mail, web e endpoints.

Descoberta e controle de Shadow AI

Descubra e gerencie ferramentas de IA não autorizadas em um único painel, com pontuação de risco e políticas de controle de acesso aplicadas por aplicação.

Controles de acesso a dados para IA autorizada

Identifique e remedie dados compartilhados em excesso ou classificados incorretamente antes que assistentes de IA, como o Copilot, possam expor conteúdo sensível.

Monitoramento e governança de agentes de IA personalizados

Capture logs de atividade detalhados dos agentes de IA, incluindo quem os acionou, a quais dados eles acessaram e quais ações realizaram.

AI Agent Gateway: controle e aplicação em tempo de execução

Intermedie credenciais de agentes e aplique proteção de dados no nível de campo em cada transação entre agente e aplicação, com aprovação humana para ações de alto risco.

Uma plataforma, todas as interações de IA

A plataforma Forcepoint AI Data Security protege os dados dos dois lados da IA: governando os dados para que se tornem seguros para alimentar a IA e protegendo os dados dos riscos que a IA introduz. A mesma proteção acompanha os dados em qualquer lugar: notebook gerenciado ou navegador pessoal, aplicativo autorizado ou ferramenta não autorizada, o escritório ou um celular em casa.

A Forcepoint é a única empresa que protege qualquer dado, estruturado ou não estruturado, on-premises e na nuvem, em todos os canais por onde ele circula, incluindo a IA. Outros fornecedores acrescentam a segurança de IA como uma ferramenta separada. A Forcepoint estende a segurança de dados em que as organizações já confiam à porta de entrada da IA.

