

Forcepoint AI Security



O que ele governa:

- › Proteção de dados em interações com IA
- › Descoberta e controle de Shadow AI
- › Controles de acesso a dados para IA autorizada
- › Monitoramento e governança de agentes de IA personalizados
- › AI Agent Gateway: controle e aplicação em tempo de execução

Principais benefícios:

- › **Painel de governança de IA:** Visão única de cada plataforma de IA autorizada, ferramenta de Shadow AI e agente.
- › **Zero reclassificação:** As políticas de DLP existentes se estendem a todos os canais de IA desde o primeiro dia. Sem reconstrução de políticas e sem novos classificadores.
- › **Cobertura completa:** Uma única plataforma governa os prompts dos funcionários, as ferramentas de Shadow AI, os agentes personalizados e os agentes hospedados na nuvem.
- › **Conformidade integrada:** Cada interação e ação de agente é registrada com atribuição completa para segurança, conformidade, auditoria e investigação forense.
- › **Valor imediato:** O Forcepoint Adaptive Risk Intelligence Assistant (ARIA) orienta os administradores desde o primeiro login até um ambiente governado.

Visão geral

A maioria dos programas de segurança corporativa foi construída com base em uma premissa simples: os dados confidenciais circulam por canais que a equipe de segurança consegue monitorar. Essa premissa não se sustenta no ambiente de IA de hoje. Quando um funcionário cola um registro de cliente no ChatGPT ou pede ao Copilot que resuma arquivos no SharePoint, nada dessa atividade passa por filtros de e-mail, proxies da web ou controles de endpoint. As ferramentas de Shadow AI agravam ainda mais o efeito: os funcionários usam aplicativos de IA que a equipe de segurança nunca revisou, e cada ferramenta não autorizada é uma exposição de dados sem visibilidade e sem trilha de auditoria.

Os agentes de IA ampliam esse risco. Um agente personalizado pode encadear dezenas de chamadas de ferramentas, consultar repositórios de dados confidenciais e gravar em sistemas externos em uma única sessão, totalmente fora da visibilidade de qualquer ferramenta de segurança em uso. Esses riscos não são teóricos. É assim que a IA está sendo usada hoje em ambientes de produção.

O Forcepoint AI Security fecha essa lacuna. Ele governa cada interação com IA em toda a empresa, desde o prompt digitado por um funcionário até a chamada de ferramenta feita por um agente autônomo à velocidade de máquina, com os mesmos controles de aplicação que já protegem todos os demais canais de dados: SaaS, web, e-mail e endpoints. São políticas unificadas, aplicadas a partir de uma plataforma centrada em dados que classifica os dados confidenciais, governa cada interação e interrompe todos os riscos automaticamente.

Detecção e resposta de IA

Monitoramento e resposta baseados em API em plataformas de IA autorizadas e agentes personalizados

Proteção de dados em interações com IA

Você sabe o que seus funcionários estão inserindo no ChatGPT?

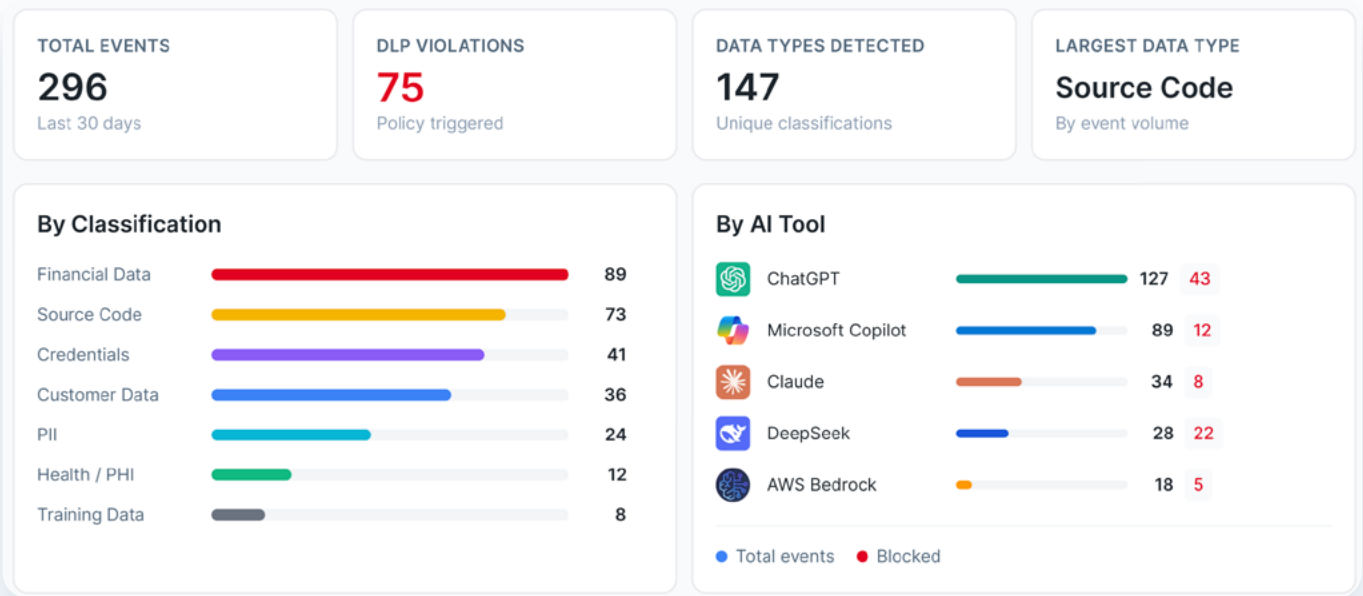
Cada prompt de IA é uma transferência de dados. Os funcionários costumam colar registros de clientes, dados financeiros e código-fonte em ferramentas de IA, movendo informações confidenciais para fora do controle da empresa, sem interceptação e sem registro. Os controles de DLP existentes não foram projetados para inspecionar as cargas de prompts e respostas de IA.

O Forcepoint AI Security traz as interações com IA para dentro da mesma estrutura de políticas que governa todos os demais canais de dados. As políticas de classificação existentes se aplicam a prompts, respostas e uploads de arquivos no ChatGPT Enterprise, no Microsoft 365 Copilot, no Claude for Enterprise e no AWS Bedrock. As violações de política acionam uma ação de remediação: auditar, colocar em quarentena, copiar ou excluir.

→ **Zero reclassificação:** Para organizações que já usam o Forcepoint DLP, as políticas existentes se

estendem aos canais de IA desde o primeiro dia. Nenhuma nova taxonomia é necessária.

- **Inspeção de prompts e respostas:** A detecção abrange texto digitado, conteúdo colado, uploads estruturados e respostas geradas por IA, não apenas anexos de arquivos.
- **Descoberta retroativa:** O preenchimento do histórico revela eventos de dados confidenciais que eram invisíveis antes da implantação do produto.
- **Sem interrupção do fluxo de trabalho:** A varredura baseada em API não exige mudanças na forma como os funcionários trabalham e não adiciona sobrecarga às ferramentas autorizadas que eles usam.



Controles de acesso a dados para IA autorizada

“O Copilot está lendo seus arquivos do SharePoint agora mesmo. Você sabe o que ele pode acessar?”

O Microsoft Copilot tem acesso direto a todos os arquivos do OneDrive e do SharePoint que um funcionário consegue alcançar. As permissões corporativas foram projetadas para pessoas, não para assistentes de IA capazes de varrer e resumir milhares de arquivos em segundos. Arquivos compartilhados em excesso ou mal configurados expõem instantaneamente registros de RH, dados financeiros, materiais do conselho e propriedade intelectual a usuários que nunca deveriam vê-los.

O Forcepoint AI Security usa a inteligência de classificação existente para entender o que os assistentes de IA autorizados podem acessar antes que qualquer prompt seja digitado. A marcação MIP impede que o Copilot resuma ou exiba arquivos confidenciais. A remediação baseada em API revoga o acesso a arquivos compartilhados em excesso antes que eles possam ser ingeridos. A mesma estrutura de conectores estende a auditoria completa de sessões ao ChatGPT Enterprise e ao Claude for Enterprise.

- **Classificação prévia ao acesso:** Os arquivos confidenciais são identificados antes do início de qualquer interação com assistentes de IA. Os controles são aplicados antes da recuperação, e não depois da exposição.
- **Marcação MIP para o Copilot:** Os arquivos confidenciais no OneDrive e no SharePoint são marcados para impedir que o Copilot os acesse, resuma ou exiba nas respostas aos prompts.
- **Remediação automática de compartilhamento excessivo:** A remediação baseada em API revoga o acesso a conteúdo compartilhado em excesso sem exigir revisão manual de permissões.
- **Auditoria completa de prompts e respostas:** Cada sessão em uma plataforma de IA conectada é registrada e atribuída, abrangendo o que foi acessado, o que foi perguntado e o que a plataforma retornou.

Monitoramento e governança de agentes de IA personalizados

“Você pode me mostrar todos os agentes de IA personalizados em execução no seu ambiente agora mesmo?”

As empresas estão implantando agentes de IA personalizados no AWS Bedrock e no Copilot Studio com acesso a fontes de dados internas. A maioria das organizações não tem um inventário dos agentes em execução, dos dados que eles conseguem acessar ou de quais deles operam fora dos limites previstos. Quando algo dá errado, não há trilha de auditoria nem atribuição.

O Forcepoint AI Security ingere e analisa os logs de invocação do AWS Bedrock por meio do CloudWatch e do S3, reconstruindo os rastros de sessão e atribuindo a atividade a identidades via IAM, Okta ou Entra ID. Cada agente recebe uma pontuação de risco com base na sensibilidade dos dados. As equipes de segurança podem correlacionar as ações dos agentes com eventos de DLP e agir antes que um incidente ocorra.

→ **Atribuição completa:** Cada ação de agente é vinculada tanto à identidade do agente quanto à

pessoa que a acionou. Esse vínculo é o que torna possível a investigação de incidentes de IA.

→ **Alerta antecipado sobre a proliferação de agentes:** Alertas automáticos são disparados quando novos agentes são publicados ou quando agentes existentes adicionam novas conexões externas.

→ **Controles de governança acionáveis:** Pause uma execução, exija aprovação humana, revogue o acesso ou coloque em quarentena arquivos gravados por agentes.

→ **Logs de auditoria prontos para conformidade:** Os registros de atividade dos agentes atendem aos requisitos do EU AI Act (artigo 12), do GDPR (artigo 30), do DORA, do NIS2, LGPD e de divulgação de IA da SEC.

Agent	Owner / Team	Profile	Scope	Token	Last Active
Sale-Copilot-Prod cl_748651dfbd...sdgd	Mary Rodriguez Revenue Ops	Read-Only	6 tools	Active	18-May-26 11:11:11
Market-Analyzer-Prod cl_853462dfbf...ghij	John Smith Marketing Lead	Editable	4 tools	Expiring	20-May-26 12:15:30
Customer-Insights-Prod cl_948273dfbe...ijkl	Emma Johnson Data Analyst	Read-Only	5 tools	Active	22-May-26 14:30:45
SalesTracker-Prod cl_748652dcba...mnop	Liam Brown Sales Manager	Editable	3 tools	Inactive	23-May-26 09:00:00
Product-Feedback-Prod cl_652348dfgh...qrst	Olivia Taylor UX Designer	Editable	2 tools	Active	24-May-26 10:05:12
Competitor-Tracker-Prod cl_763291dfgh...uvwx	Noah Wilson Research Analyst	Read-Only	6 tools	Active	25-May-26 13:45:20
Campaign-Optimizer-Prod cl_253471dfgh...yzab	Ava Lee Marketing Specialist	Editable	5 tools	Inactive	26-May-26 15:30:00
Lead-Management-Prod cl_847162dfgh...cdef	Sophia White Lead Strategist	Read-Only	7 tools	Active	27-May-26 11:20:33

Descoberta e controle de Shadow AI

Descoberta, pontuação de risco e controle de acesso para cada ferramenta de IA não autorizada na empresa

“Quantas ferramentas de IA seus funcionários estão usando sem a sua aprovação?”

As ferramentas de Shadow AI proliferam na velocidade de uma extensão de navegador. Os funcionários adotam contas pessoais de IA, assistentes de redação, ferramentas de programação e processadores de documentos sem passar por uma revisão de segurança, e as organizações agora gerenciam em média 37 agentes de IA, enquanto muitas equipes de segurança não têm visibilidade sobre o que esses agentes acessam. Cada ferramenta não autorizada é uma possível exposição de dados que os controles existentes não conseguem enxergar.

O Forcepoint AI Security oferece às equipes de segurança um inventário continuamente atualizado e com pontuação de risco de cada aplicativo de IA não autorizado em uso. As equipes de segurança veem o detalhamento completo da atividade por usuário e por ferramenta: visitas, prompts, respostas, uploads e downloads de arquivos. Quando os funcionários usam contas pessoais em vez das contas corporativas

autorizadas, o AI Security detecta a diferença e aplica a política correspondente.

- **Inventário de IA com pontuação de risco:** Cada aplicativo de IA não autorizado é categorizado e pontuado, fundamentando as decisões de acesso em riscos reais.
- **Detalhamento da atividade:** Visibilidade total do que os funcionários fazem em cada ferramenta de Shadow AI, incluindo a atividade de prompts e as transferências de arquivos.
- **Detecção de contas corporativas versus pessoais:** Identifique se os funcionários usam as ferramentas de IA por meio de contas corporativas autorizadas ou de contas pessoais e aplique a política correspondente.
- **Controle de acesso por ferramenta:** Permita, bloqueie ou restrinja uploads e downloads por aplicativo de IA, de acordo com o usuário ou o departamento.

Unsanctioned AI Apps

App Name	Category	Risk	Users	Trend
Google Gemini gemini.google.com	Generative AI - Conversation	Low	89	
Perplexity AI perplexity.ai	Generative AI - Conversation	Low	87	
Midjourney midjourney.com	Generative AI - Multimodal	Medium	43	
DeepSeek deepseek.com	Generative AI - Conversation	High	31	
Hugging Face huggingface.co	Other - AI App	Medium	29	
Poe poe.com	Generative AI - Conversation	Low	22	
Jasper AI jasper.ai	Generative AI - Text and Code	Low	18	
Cursor cursor.so	Generative AI - Text and Code	High	15	

AI Agent Gateway

Aplicação inline nativa de MCP entre agentes de IA hospedados na nuvem e os aplicativos SaaS que eles chamam

“Você consegue impedir que um agente de IA acesse dados que não deveria tocar?”

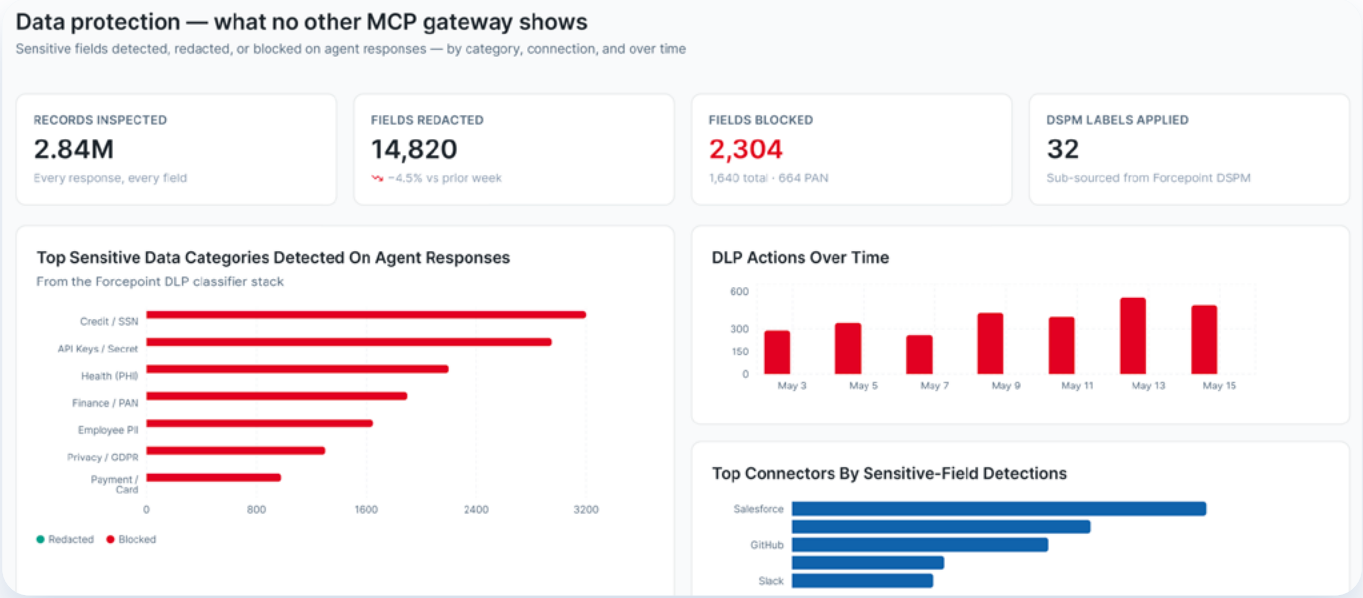
Os agentes hospedados na nuvem se conectam diretamente a aplicativos SaaS, como Microsoft 365, Salesforce e Jira, operando com todas as permissões da conta de serviço que receberam na implantação. Não há nenhum mecanismo para limitar quais dados um agente lê, bloquear campos que ele nunca deveria ver ou interromper uma operação durante a execução. Um agente comprometido é, na prática, uma credencial comprometida com acesso irrestrito a aplicativos e sem responsabilização.

O Forcepoint AI Agent Gateway é um gateway MCP desenvolvido sob medida que atua como intermediário obrigatório entre os agentes de IA hospedados na nuvem e os aplicativos SaaS que eles chamam. Nenhum agente jamais detém diretamente credenciais de qualquer aplicativo de negócios. Cada agente opera dentro de um escopo definido de ferramentas aprovadas, com tokens de curta duração sujeitos a revogação instantânea. Cada resposta é inspecionada em nível de campo antes que o agente possa lê-la: PII, código-fonte, credenciais e segredos são bloqueados ou ocultados antes da transmissão. Operações de gravação e exclusão podem ser retidas para aprovação humana por meio do Teams, do Slack ou de e-mail. Cada transação é registrada de forma imutável.

→ **Os agentes nunca detêm credenciais diretas:** O Gateway intermedia todas as credenciais de aplicativos.

Um agente comprometido não consegue se autenticar diretamente em nenhum aplicativo conectado.

- **Privilegio mínimo aplicado por design:** Cada agente é registrado com um escopo definido de ferramentas aprovadas e recebe tokens de curta duração. Os agentes não conseguem acessar dados ou operações fora do limite aprovado.
- **Proteção de dados em nível de campo:** PII, código-fonte, credenciais e segredos são bloqueados ou ocultados antes que o agente possa lê-los, agregá-los ou transmiti-los.
- **Controles com intervenção humana:** As operações de gravação e exclusão podem ser retidas para aprovação humana. O aprovador vê o nome do agente, a identidade do usuário, a ferramenta, os parâmetros e a classificação dos dados antes de decidir.
- **Deteção de comportamento anômalo:** Consultas com volume incomum de registros são detectadas e interrompidas na camada de execução antes que uma extração em massa de dados seja concluída.
- **Trilha de auditoria imutável:** Cada transação gera um registro completo: identidade do agente, identidade do usuário, ferramenta chamada, classificação dos dados, decisão da política, campos bloqueados ou ocultados, quantidade de registros e carimbo de data e hora.



Valor desde o primeiro dia

O Forcepoint AI Security foi projetado para entregar valor desde o primeiro dia. A ARIA, o assistente de integração com IA da Forcepoint, é iniciada automaticamente no primeiro login e orienta o administrador na configuração de conectores e políticas, recomendando um conjunto inicial de políticas de DLP com base na região, no setor e no perfil de sensibilidade dos dados da organização. Não são necessários serviços profissionais. Os dados históricos de interação são preenchidos automaticamente na primeira conexão, de modo que o painel de governança de IA tenha conteúdo real desde o momento em que a configuração é concluída.

AI Security Setup

✕ Exit

Complete setup to start monitoring AI usage across your organisation.

1

2

3

Connect AppsData ProtectionConfirm Setup

Connect your AI Applications

Connect **at least one app** to begin monitoring. You can add more at any time.
We will monitor user prompts sent to AI apps and any backend data access across services.



AWS Bedrock



ChatGPT



Claude



Copilot

Principais recursos

RECURSO	BENEFÍCIO
Conectores baseados em API	Visibilidade e controle profundos sobre o ChatGPT Enterprise, o Microsoft 365 Copilot, o Claude for Enterprise e o AWS Bedrock.
Herança de políticas de DLP	As classificações existentes do Forcepoint DLP se estendem automaticamente a prompts, respostas e uploads de arquivos de IA, sem exigir uma nova taxonomia.
Registro de prompts e respostas	Texto completo de cada prompt e resposta de IA, capturado, indexado e pesquisável por usuário, intervalo de datas, rótulo de classificação e ferramenta de IA.
Visibilidade de operações com arquivos	Cada arquivo enviado a uma ferramenta de IA autorizada é detectado, classificado de acordo com a taxonomia de DLP da organização e registrado com contexto de auditoria completo.
Painel de governança de IA	Visão única em tempo real de todas as plataformas de IA autorizadas, ferramentas de Shadow AI e atividade de agentes. Blocos de KPI, dados de tendência, descobertas classificadas por risco e próximas ações orientadas em uma única visão operacional.
Inventário e governança de agentes	Inventário em tempo real de agentes de IA no Copilot Studio, no ChatGPT Enterprise e no AWS Bedrock, com identidade do agente, modo de autenticação, fontes de dados conectadas e pontuação de risco exibidos por agente.
Descoberta e controle de Shadow AI	Inventário continuamente atualizado de ferramentas de IA não autorizadas, com pontuações de risco, detalhamento completo da atividade por usuário e ferramenta, detecção de contas corporativas versus pessoais e políticas de controle de acesso.
Barreiras de proteção de acesso a dados	Identificação, com base na classificação, de arquivos compartilhados em excesso ou rotulados incorretamente antes que os assistentes de IA possam acessá-los. Marcação MIP e remediação baseada em API disponíveis para Microsoft 365, SharePoint, OneDrive e Microsoft Copilot.
Ações de remediação	Permitir, permitir e monitorar, restringir a ação, excluir o histórico de conversas, revogar o acesso a arquivos, colocar em quarentena arquivos gravados por agentes, pausar a execução de um agente ou exigir aprovação humana. As ações disponíveis variam de acordo com o tipo de interação e a superfície de aplicação.
Configuração guiada pela ARIA	Assistente de integração com IA que orienta os administradores na configuração de conectores e políticas, recomendando um conjunto inicial de políticas com base na região, no setor e na sensibilidade dos dados. Não são necessários serviços profissionais.
AI Agent Gateway	Intermediário obrigatório entre os agentes de IA hospedados na nuvem e os aplicativos de negócios SaaS conectados. Os agentes nunca detêm credenciais diretas de aplicativos. Proteção de dados em nível de campo, aprovações configuráveis com intervenção humana e registro de auditoria imutável em cada transação entre agente e aplicativo.
Exportação de auditoria de conformidade	Log de auditoria exportável que abrange todas as interações de IA, ações de agentes e eventos de política. Atende aos requisitos do EU AI Act, do NIST AI RMF, do GDPR (artigo 30), do DORA, do NIS2, LGPD e de divulgação de IA da SEC. Exportável em CSV, JSON e PDF.

O Forcepoint AI Security é construído sobre a plataforma Forcepoint AI Data Security, que classifica os dados confidenciais antes que a IA os acesse e aplica políticas em cada interação em toda a empresa. Uma única estrutura de políticas governa e-mail, web, endpoint, aplicativos em nuvem e IA a partir de um único plano de controle.

A plataforma aborda os dois lados do mesmo problema: proteger os dados corporativos contra as ferramentas de IA e governar os dados para que a IA possa operar com segurança. Descoberta, aplicação e insights de risco são executados no mesmo mecanismo, oferecendo às equipes de segurança uma visão operacional única de todas as superfícies que a IA toca.

Forcepoint AI Data Security



Qualquer dispositivo, qualquer app, qualquer local