EQUIFAX®

Relatório Anual de Segurança

2025

Índice

Acreditamos que mais comunicação, mais colaboração e mais transparência resultam em maior segurança.

Uma mensagem do CEO da Equifax

Mark W. Begor

Diretor Executivo
Equifax

2025 foi um ano empolgante de crescimento e inovação. Com a nossa transformação global de segurança e tecnologia de US$ 3 bilhões – e a criação da Equifax Cloud™ – praticamente concluída, a EFX.AI está impulsionando o futuro da Nova Equifax. Estamos acelerando a implantação da tecnologia patenteada da EFX.AI em nossos produtos, aproveitando os dados exclusivos e proprietários que destacam a Equifax no setor. Isso impulsionou um número recorde de Inovações de Novos Produtos (NPIs), que entregam a inteligência de decisão que nossos clientes globais precisam para criar novas oportunidades mais rápido do que nunca. Além disso, estamos ganhando eficiência ao aproveitar a IA internamente, gastando menos tempo em atividades de rotina e dedicando mais tempo para desafios complexos, criativos e colaborativos, que impulsionam nossa empresa para o futuro.

Nosso compromisso inabalável com a segurança estabelece uma base sólida para esta inovação.

Quando entrei na Equifax em 2018, assumi o compromisso pessoal de estabelecer a Equifax como líder do setor em segurança de dados e de construir uma cultura em que todos na Equifax sejam responsáveis pela segurança. Transformamos todos os aspectos de nossa organização para cumprir essa promessa, tornando a segurança parte do DNA da nossa equipe global. Com o lançamento do nosso sexto Relatório Anual de Segurança, nosso foco implacável na liderança de segurança é claro: nosso nível de maturidade em segurança superou todos os principais benchmarks do setor por seis anos consecutivos, enquanto nossa pontuação de postura de segurança excedeu as médias dos setores de Tecnologia e Serviços Financeiros pelo quinto ano consecutivo.

Ao mesmo tempo, reconhecemos que nosso trabalho na segurança nunca termina.

O ano de 2025 viu uma série de novas ameaças à infraestrutura global de cibersegurança, definidas por uma convergência de volume, velocidade e sofisticação impulsionada por IA. Vimos agentes autônomos e IA industrializada amplificarem ataques tradicionais, expandindo o que devemos defender. A Equifax estava pronta. Guiados pelo nosso foco em otimização implacável e maximizando nossa infraestrutura nativa da nuvem, nos defendemos contra mais de 19,8 milhões de ameaças de segurança cibernética todos os dias, enquanto conduzíamos mais de 240.000 simulações para testar nossa força de trabalho global e nos preparar para o que vem pela frente.

Embora se espere que muitas empresas sejam impactadas ou desintermediadas pela IA, a Equifax está aproveitando a IA para revolucionar o setor e acelerar nossa liderança de segurança. Temos orgulho de que a IA mudou fundamentalmente a forma como operamos, com quase 90% da nossa equipe global aproveitando ferramentas de IA em 2025. À medida que capacitamos nossos negócios para inovar com a IA, construímos proteções rigorosas, desde filtros automatizados de segurança de conteúdo até estruturas seguras de codificação, garantindo que nossos modelos sejam explicáveis, seguros e que nossos dados proprietários permaneçam protegidos.

Continuaremos a aproveitar a IA para aprimorar nossas defesas, proteger o uso da IA pelos negócios para inovação e nos defender contra ameaças de IA. Importante ressaltar que não apenas manteremos nosso foco na segurança, mas também continuaremos a ajudar nossos clientes, parceiros e consumidores a fortalecer suas próprias posturas de segurança cibernética para o benefício do setor como um todo.

Uma mensagem do CISO da Equifax

Jeremy Koppen

Diretor de Segurança
da Informação (CISO)
Equifax

Cheguei a esta função com uma perspectiva clara sobre a jornada de segurança da Equifax. Antes de ingressar na empresa como CISO, em maio de 2025, eu era Diretor Administrativo na Mandiant, onde tive o privilégio de trabalhar ao lado desta equipe durante os estágios iniciais e fundamentais de sua transformação. E, por anos depois, admirei seu progresso contínuo de fora.

Eu sabia que a Equifax havia sido reconhecida como líder do setor em segurança. Mas quando entrei, não encontrei uma equipe dando uma volta olímpica. Encontrei uma equipe com um impulso e foco que imediatamente se destacaram.

Essa intensidade é crucial porque o cenário de ameaças de 2025 foi definido por uma convergência de volume, velocidade e sofisticação. Vimos agentes autônomos e IA industrializada ampliarem os ataques tradicionais, expandindo radicalmente o escopo do que devemos defender. Neste ambiente, simplesmente fazer mais não é uma estratégia. Devemos evoluir proativamente para nos mantermos à frente.

Então, neste ano, focamos na **otimização implacável.**

A IA mudou fundamentalmente a maneira como operamos. Aproveitando nossa infraestrutura nativa da nuvem, usamos IA para otimizar nosso Centro de Operações de Segurança e acelerar as r tarefas de rotina, para que nossos especialistas pudessem focar nas ameaças que mais importam. Também mitigamos a IA adversária, implantando controles personalizados para bloquear injeções de prompt invisíveis e deepfakes. E protegemos o uso de IA na operação dos negócios, projetando nossos sistemas para remover atritos enquanto construímos as proteções que permitiram que nossos colaboradores aproveitassem rápida e responsavelmente as capacidades de IA em cada área da Equifax. Essa disciplina ajudou a garantir que a **segurança permaneça uma verdadeira aceleradora operacional.**

A prova está em nossa produção. Em 2025, a Equifax lançou com segurança mais de 180 Inovações de Novos Produtos (NPIs na sigla em inglês), nosso sexto ano consecutivo acima de 100. Isso demonstra que a segurança rigorosa não é um interesse concorrente, mas um facilitador vital para rápida inovação e crescimento.

Talvez o mais importante, é que a segurança na Equifax é uma disciplina compartilhada. Vemos isso em ação à medida que nossas equipes de Tecnologia constroem uma arquitetura segura desde a concepção e à medida que nossos parceiros das equipes de Finanças e Jurídica fazem as perguntas difíceis sobre o risco de terceiros. Também vemos isso em nossos colaboradores em todo o mundo, que agem como sensores humanos, sinalizando novas tentativas de phishing e reforçando nossas defesas automatizadas com intuição humana.

Estamos satisfeitos? Absolutamente não. Aumentamos nossa maturidade de segurança novamente em 2025, mas as ameaças que enfrentamos continuam evoluindo. Continuaremos adotando novas tecnologias, otimizando nossas defesas e priorizando nossos esforços com base no impacto, não na facilidade.

Tenho orgulho de liderar uma equipe com ambição implacável de superar o status quo. Nossa busca pela liderança em segurança não tem limites.

Nosso impacto:

Equipe de Segurança da Equifax em 2025

Mais de 19,8 milhões
de Ameaças cibernéticas bloqueadas por dia, quase 230 tentativas hostis a cada segundo, um aumento de 30% em relação ao ano anterior.

Mais de 240.000
Simulações lançadas para testar nossa força de trabalho global em diversos cenários de segurança.

Aproximadamente 22.000
Colaboradores e prestadores de serviço treinados com módulos de segurança personalizados, aumentando a dificuldade das simulações para espelhar a evolução das ameaças.

Mais de 4.000
Questionários de clientes e solicitações de evidências concluídos para reforçar a confiança em nossa postura de segurança.

Mais de 3.700
Questionários de clientes e solicitações de evidências concluídos para reforçar a confiança em nossa postura de segurança.

Mais de 2.280
Análises de risco aprofundadas em fornecedores terceirizados cruciais e de alto risco, identificando potenciais falhas de segurança antes que possam ser exploradas.

Mais de 400
Profissionais de segurança cibernética dedicados protegendo dados do consumidor 24 horas por dia.

Mais de 330
Verificações automatizadas de segurança na nuvem monitoradas em tempo real, impulsionando uma resposta a ameaças mais rápida e consciência de postura quase instantânea.

Mais de 180
Inovações de Novos Produtos trazidas ao mercado com segurança, nosso sexto ano consecutivo acima de 100, provando que velocidade e segurança não são opostas.

52
Certificações e autorizações obtidas de auditorias externas, validando nossa profundidade e rigor.

43
Avaliações de segurança física concluídas para proteger nossas pessoas, dados e ativos.

Mais de 35
Fóruns com participação global para compartilhar inteligência e fortalecer defesas colaborativas.

18
Exercícios de mesa simulando cenários de crise nos níveis executivo e regional.

6
Anos consecutivos alcançando uma pontuação de Maturidade de Segurança que supera todos os principais benchmarks do setor.

2
Integrações de aquisição concluídas sob um novo playbook de segurança simplificado.

1
Minuto de tempo médio para detectar ameaças cibernéticas.

Cenário atual:
Segurança cibernética em 2025

Pivô de Priorização

Em 2025, as empresas continuaram a ver um aumento no volume, frequência e velocidade dos ataques cibernéticos. Neste cenário, equipes avançadas adotaram a IA para expandir o que poderia ser neutralizado automaticamente, para que menos ameaças exigissem intervenção humana. Simultaneamente, o setor refinou sua definição de "risco." Enquanto pontuações genéricas de risco sempre careceram de nuance e contexto, o cenário de ameaças de 2025 as tornou especialmente enganosas.

Para dar conta disso, as lideranças de segurança mudaram para pontuações personalizadas que eram mais específicas para os ambientes únicos de suas empresas, considerando variáveis como: se um sistema estava voltado para a internet, estritamente controlado por acesso ou mantendo dados sensíveis. Isso permitiu que as equipes filtrassem falhas com altas pontuações de risco, mas baixo risco prático para aquela empresa específica e, em vez disso, pudessem priorizar as vulnerabilidades que realmente ameaçavam o negócio.

A Evolução do Risco de Terceiros

Vulnerabilidades da cadeia de suprimentos desafiaram o setor por mais de uma década, mas em 2025, a tática mudou. Os invasores foram além da exploração de falhas de software para o sequestro de acesso legítimo. Ao comprometer fornecedores e roubar suas credenciais, os criminosos efetivamente "se tornaram" o parceiro, usando conexões autorizadas para contornar as defesas sem serem percebidos.

Essa evolução transformou um problema da cadeia de suprimentos em uma crise de identidade, exigindo que as empresas verifiquem parceiros de confiança tão rigorosamente quanto fazem com ameaças externas.

Lacuna de Governança de Agentes de IA

À medida que a IA evoluiu de chatbots simples para agentes poderosos, capazes de se conectar a sistemas internos para fazer trabalho real, ficou claro que, embora essas ferramentas pudessem acessar dados sensíveis, elas potencialmente careciam dos controles para mantê-los seguros.

Isso criou uma divisão no setor. Algumas empresas correram, aceitando o risco de usar ferramentas que talvez não conseguissem monitorar totalmente ou parar durante uma emergência. Outras pausaram a adoção inteiramente, por medo de voar às cegas. Mas as equipes mais eficazes encontraram um terceiro caminho. Elas construíram suas próprias verificações de segurança personalizadas para proteger seus dados, usando seus controles de segurança fundamentais existentes, e trabalharam simultaneamente com fornecedores para fechar lacunas de arquitetura.

Superfície de Ataque em Expansão das Credenciais

A superfície de ataque de identidade se ampliou drasticamente em 2025, expondo tanto pessoas quanto máquinas. Os invasores armaram a IA para lançar deepfakes hiper-realistas e campanhas de phishing que rotineiramente enganavam até mesmo colaboradores experientes, e o ecossistema de identidade de máquina cresceu sem controle.

À medida que as empresas correram para automatizar, elas geraram milhares de credenciais não humanas (como chaves de API), que careciam da supervisão rigorosa aplicada aos humanos. Os invasores aproveitaram esses alvos silenciosos e de alto acesso, provando que proteger a identidade agora exige governar cada entidade que se conecta à rede, humana ou não.

Nossas ações:

Iniciativas e resultados da equipe de Segurança da Equifax em 2025

Modernizamos Nossa Abordagem à Cultura de Segurança

Todo colaborador e prestador de serviço reconhece que a segurança é uma parte crítica do seu trabalho. Reforçamos isso introduzindo uma plataforma alimentada por IA que oferece treinamento personalizado e gamificado para toda a nossa força de trabalho.

Validamos o treinamento deles por meio de mais de **240.000 simulações globais de phishing em 2025**, 15% a mais que em 2024, aumentando a dificuldade para corresponder ao cenário de ameaças. E expandimos os as pontuações de avaliação para incluir seis novos comportamentos baseados em função, impulsionando uma melhoria de 10% em relação a um determinado comportamento em apenas quatro meses, mostrando que o feedback claro faz a diferença.

Demonstrando que a segurança é uma prioridade pessoal, os colaboradores usaram nossas novas ferramentas de denúncia de phishing para sinalizar 20.000 ameaças potenciais em apenas seis meses, revelando quase 1.500 indicadores maliciosos confirmados.

Reforçar a Segurança como um Diferencial de Mercado

A segurança é um diferencial competitivo que permite o sucesso comercial. Escalamos nossas defesas para permitir o lançamento seguro de um número recorde de NPIs em 2025, enquanto obtivemos 52 certificações, incluindo autorizações cruciais do governo dos EUA.

Também implantamos uma base de conhecimento de IA especializada que gera respostas a questionários de segurança com base apenas em nossa documentação oficial de políticas internas. As métricas iniciais mostram uma taxa de sucesso de 67% nas respostas de primeira tentativa, superando em muito as soluções legadas e nos permitindo **atender às necessidades dos clientes com velocidade sem precedentes**.

Em 2025, uma empresa líder em telecomunicações da Fortune 50 **destacou publicamente a Equifax como modelo do setor** por “fazer segurança da maneira certa”, citando nossa transparência como um fator fundamental para a confiança que depositam em nós. Nosso compromisso com a transparência é global, com mais de 40.000 usuários, em 70 países, acessando nossa estrutura de controles de segurança pública para fortalecer suas próprias defesas no ano passado.

Segurança e Engenharia Unificadas

Em 2025, **combinamos nossas funções de arquitetura de segurança e arquitetura de tecnologia**, unindo construtores e defensores para impulsionar soluções consistentes e automatizadas em todo o mundo.

Por meio dessa base compartilhada, nós projetamos nossos sistemas para eliminar o atrito. Ao fornecer às equipes de engenharia uma **plataforma de desenvolvimento simplificada e automatizada**, que oferece implantações com um clique e integração perfeita, nós os capacitamos para **enviar com segurança 50% mais alterações**, provando que podemos acelerar a tecnologia e a inovação de produtos sem comprometer a segurança.

Essa velocidade operacional se estendeu às nossas defesas. Com melhor visibilidade, identificamos, avaliamos e garantimos a remediação de mais de 3.700 componentes cruciais de infraestrutura, **um aumento de 164% na cobertura** na comparação anual. Apesar desse volume maior, mantivemos um **tempo médio de resolução de problemas inferior a 24 horas**, demonstrando que quando a segurança é coletiva, corrigimos problemas tão rápido quanto os encontramos.

Co-inovamos com Fornecedores e Parceiros

A Equifax continua guiando os padrões do setor por meio da co-inovação, uma estratégia na qual **fazemos parceria diretamente com nossos fornecedores de segurança para moldar melhorias de produtos e serviços** que protegem não apenas nosso ambiente, mas também o de outras empresas.

Ajudamos o nosso parceiro de proteção de terminais a **fechar lacunas de visibilidade** na infraestrutura de servidor Linux, desafiamos nosso provedor de nuvem a **desenvolver controles de acesso mais granulares** para IA generativa, pressionamos por **correções cruciais de hardware** e trabalhamos com nosso provedor de gestão de identidade e acesso para **otimizar a infraestrutura, reduzindo a latência** para melhorar a produtividade.

Essa colaboração também se estendeu além dos fornecedores de tecnologia para o setor público. Por exemplo, nos juntamos a 25 parceiros e à polícia canadense para ajudar a **executar mais de 3.000 ações contra redes de fraude.** Também expandimos nossa parceria na América Latina, **trabalhando com órgãos governamentais em El Salvador e Costa Rica** para promover a educação em segurança de IA e moldar estruturas nacionais de padronização.

Usando IA para aprimorar a segurança

Aplicamos nova tecnologia para fazer o que sempre fizemos, só que mais rápido e com maior precisão. Ao implantar a IA como um multiplicador de força estratégico, atualizamos nossa capacidade de triar e remediar ameaças e acelerar as decisões críticas de segurança que impulsionam a entrega de operacional.

Começamos a usar IA agêntica para lidar com alertas de rotina, liberando analistas para ameaças complexas.

Centros de Operações de Segurança (SOCs na sigla em inglês) enfrentam um desafio universal: a fadiga de alertas, onde analistas devem passar por milhares de notificações de baixo risco.

Então, projetamos e pilotamos um agente de triagem especializado com um mandato estrito: analisar alertas de baixa fidelidade e fechá-los apenas se atenderem a uma rigorosa "definição de pronto."

Com a adoção total em nosso SOC global programada para 2026, essa ferramenta adicionou uma nova camada ao conjunto de automação que acelera o fechamento de problemas, enquanto ajuda especialistas a gastar menos tempo fechando tickets e mais tempo caçando adversários sofisticados.

Impacto | Resolução automática de quase **50%** de todos os tickets de incidentes do SOC por meio de defesas automatizadas.

Reduzimos drasticamente o tempo necessário para testar nossas defesas contra novas ameaças.

No passado, testar nossas defesas contra as táticas criminosas mais recentes era um processo manual. Quando um teste era projetado, o adversário muitas vezes já havia seguido em frente.

Para reduzir essa janela, construímos um mecanismo alimentado por IA que lê relatórios de ameaças cibernéticas não estruturados e os converte instantaneamente em cenários de ataque acionáveis. Isso nos permite simular esses ataques e validar nossas defesas contra as táticas adversárias mais recentes, dias após sua descoberta, garantindo que nossa barreira esteja sempre calibrada para a ameaça atual.

Impacto | Passando da **divulgação da ameaça** para a **validação da defesa** em dias, não meses.

Incorporamos assistentes de IA personalizados para reduzir o atrito para o negócio.

Para garantir que nossos processos de segurança apoiem a inovação rápida e o diálogo perfeito com o cliente, usamos IA para otimizar dois fluxos de trabalho cruciais.

Primeiro, um assistente consultivo de IA agora ajuda arquitetos a analisar conceitos instantaneamente, reduzindo o tempo de resolução de consultas de segurança de 46 para 18 dias.

Segundo, uma base de conhecimento de IA acelera os questionários de segurança do cliente baseando as respostas em políticas validadas. Essa ferramenta alcançou uma taxa de sucesso de 67% na primeira tentativa, permitindo que nossas equipes respondessem aos clientes com maior velocidade e precisão.

Impacto | Reduzindo os tempos de consulta de segurança em **61%** e acelerando as respostas de vendas.

Fomos além de encontrar falhas para corrigi-las automaticamente.

Ferramentas de segurança tradicionais param na detecção, alertando desenvolvedores sobre uma vulnerabilidade e adicionando-a ao seu backlog. Demos um passo adiante implantando agentes de IA para encontrar problemas e resolvê-los.

Usando uma arquitetura de IA personalizada, nosso sistema analisa vulnerabilidades em contêineres e escreve automaticamente a correção do código. Ele então envia um "pull request" para o desenvolvedor revisar e mesclar. Isso muda a segurança de um guardião que atrasa as coisas para um parceiro que limpa o código.

Impacto | Lidando **com mais de 213.000 descobertas** anualmente sem desacelerar a entrega do produto.

Protegendo o uso de IA na operação dos negócios

À medida que nossa força de trabalho e desenvolvedores adotavam a IA para impulsionar a inovação, nossa prioridade era garantir que pudessem fazê-lo com segurança. Focamos na construção das proteções necessárias, de filtros automatizados de segurança de conteúdo a estruturas de codificação segura, que permitiram que nossas equipes adotassem novas ferramentas poderosas sem expor a empresa a potencial vazamento de dados ou risco não gerenciado.

Tornamos os modelos de IA mais seguros para uso de dados operacionais.

Projetamos nossa arquitetura para nunca depender apenas de um provedor de modelo para proteger nossos dados. Em vez disso, implementamos uma camada de controle agnóstica que fica entre nossos colaboradores e a IA.

Essa camada sanitiza prompts e respostas, verificando vazamento de dados sensíveis ou ataques de injeção maliciosa antes que toquem um modelo de IA. Isso garante que, mesmo se um modelo externo for comprometido, nossos dados permaneçam protegidos.

Impacto | Fornecendo uma **camada de controle unificada** para injeção de prompt e proteção de dados pessoais.

Projetamos os protocolos que permitem que cada colaborador seja um construtor de IA.

Para escalar a IA com segurança dentro da Equifax, nos afastamos do controle manual para a "Política como Código." Nossos portões de avaliação testam automaticamente cada novo agente antes da produção e o monitoramento contínuo detecta se um modelo começa a desviar ou se comportar de forma imprevisível.

Isso nos posiciona para atender às regulamentações de IA em evolução, garantindo que, para casos de uso de alto risco, imponhamos aprovações com intervenção humana e interruptores automáticos com recursos de reversão instantânea. Essa estrutura nos permite democratizar ferramentas de IA com a confiança de que as redes de segurança estão sempre ativas.

Impacto | Implantando com segurança ferramentas de IA Generativa para **mais de 22.000 colaboradores e prestadores de serviço** globalmente.

Substituímos a "shadow AI" por controle de precisão e acesso controlado.

Rejeitamos a abordagem "ativado por padrão" dos principais fornecedores. Quando novos recursos introduziram riscos potenciais de dados, nós os pausamos seletivamente até que pudessem atender aos padrões e controles de segurança da Equifax.

Simultaneamente, deixamos de bloquear a inovação para guiá-la. Impusemos uma lista de negação rigorosa para modelos externos de alto risco, enquanto fornecemos acesso instantâneo a uma lista de permissão pré-aprovada de ferramentas prontas para a empresa. Isso garante que nossos desenvolvedores construam sobre uma base de confiança.

Impacto | Reduzindo o risco por meio da **habilitação de recursos seletiva e compatível**.

Implementamos conexões de código seguras para agentes de IA.

À medida que a IA passa de chatbots simples para agentes autônomos que podem editar código, o risco de um agente com "privilégios excessivos" cresce. Para resolver isso, definimos uma estrutura de segurança rígida para o Protocolo de Contexto de Modelo (MCP na sigla em inglês).

Ao permitir que desenvolvedores usem servidores de MCP remotos para acessar o código ativo com segurança, garantimos que possam aproveitar a assistência de IA mais recente sem dar à máquina acesso não verificado a toda a base de código.

Impacto | Operacionalização da **conectividade segura de IA para Código**.

Defendendo contra ameaças de IA

Reconhecemos que os criminosos também estavam adotando ferramentas habilitadas por IA para criar representações altamente realistas e lançar ataques mais rápidos e complexos. Então, recalibramos nossas defesas para detectar e proteger contra essas ameaças, garantindo que nossos controles permanecessem eficazes contra uma nova geração de fraudes e ataques cibernéticos habilitados por IA.

Interceptamos com sucesso um ataque de deepfake visando nossa liderança.

Em 2025, a ameaça teórica da clonagem de voz por IA tornou-se realidade. Nossas equipes cibernéticas detectaram um ataque sofisticado de engenharia social apresentando um memorando de voz utilizando deepfake para personificar o nosso CEO.

Não apenas paramos o ataque; nós o usamos para fortalecer a nossa imunidade. Analisamos instantaneamente os padrões linguísticos do adversário e implantamos regras de detecção personalizadas em nossos gateways de e-mail, protegendo efetivamente a organização contra futuras tentativas de fraude geradas por IA.

Impacto | Transformando uma **tentativa de deepfake ao vivo** em uma atualização de defesa permanente.

Descobrimos e bloqueamos ataques invisíveis projetados para enganar modelos de IA.

À medida que integrávamos a IA, nossa equipe de simulação de ataques descobriu uma vulnerabilidade nova: adversários podiam incorporar prompts de texto invisíveis, indetectáveis ao olho humano, que enganam modelos de IA para entregar malware.

Transicionamos com sucesso essa descoberta de um caso de teste para um controle de prevenção ao vivo. Implementamos lógica para remover esses comandos ocultos antes que cheguem ao nosso ecossistema, fechando uma brecha que muitas organizações ainda não detectaram.

Impacto | Passando da **descoberta da equipe de simulação de ataque** para o **controle de prevenção** em tempo recorde.

Implantamos defesas adaptativas para capturar ataques evasivos impulsionados por IA.

Os invasores estão usando IA para escrever código que se reescreve constantemente para contornar filtros tradicionais. Esses ataques "polimórficos" são projetados para parecer diferentes a cada ataque.

Em resposta, implantamos lógica de evasão personalizada em nossas defesas de endpoint. Em vez de procurar uma assinatura de arquivo específica, nossas ferramentas agora analisam o comportamento do código, nos permitindo detectar e bloquear malware gerado por IA, independentemente de como ele se disfarça.

Impacto | Bloqueando **malware de IA evasivo** que contorna filtros tradicionais.

Fortalecemos nossos portais de consumidores contra enxames de bots impulsionados por IA.

A automação permite que criminosos ataquem em uma escala que humanos não conseguem igualar, usando "enxames" de bots para raspar dados ou testar credenciais roubadas contra nossos portais de consumidores. Para proteger alvos de alto valor, implantamos perfis de modo de bloqueio avançado.

Essas defesas identificam e neutralizam táticas impulsionadas por IA como "email tumbling" (modificar rapidamente um único endereço para contornar filtros), garantindo que nossos dados permaneçam acessíveis a pessoas, mas não a bots.

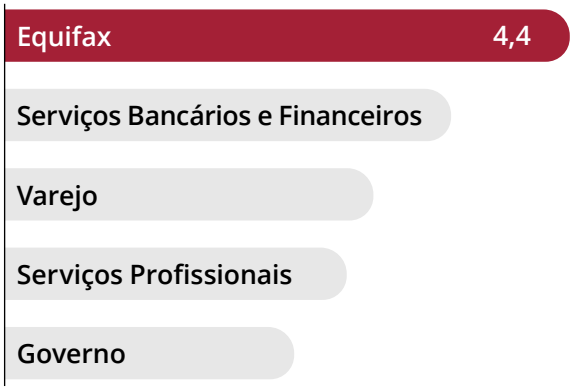
Impacto | Neutralizando **campanhas sofisticadas de raspagem de credenciais** em tempo real.

Benchmarking independente

Maturidade de Segurança

A maturidade do nosso programa de segurança cibernética, com pontuação 4,4 no Modelo de Cibersegurança de 2025 do Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST), melhorou em 2025, superando todos os principais benchmarks do setor pelo sexto ano consecutivo.

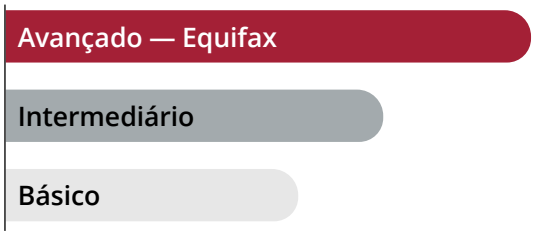
Pontuação de Maturidade de Segurança



Postura de Segurança

Nossa pontuação de postura de segurança excedeu as médias do setor de Tecnologia e Serviços Financeiros pelo quinto ano consecutivo.

Classificação de Postura de Segurança



Estas são as categorias de classificação atribuídas pelo serviço de relatórios que monitora nossa postura. A Equifax mantém uma classificação que nos coloca na categoria mais alta.

O que é Maturidade de Segurança?

A maturidade de segurança de uma organização representa quão bem ela pode se adaptar a ameaças cibernéticas e gerenciar riscos ao longo do tempo.

Temos uma parceria com uma empresa líder global de pesquisa e consultoria para conduzir uma análise aprofundada da maturidade de todo o nosso programa de segurança.

O que é Postura de Segurança?

A postura de segurança de uma organização é sua prontidão e capacidade de identificar, responder e se recuperar de ameaças e riscos de segurança.

Um serviço líder de relatórios de segurança cibernética monitora continuamente a postura do nosso programa de segurança e avalia o risco do nosso ecossistema de cadeia de abastecimento.

Resumo dos resultados:

Segurança da Equifax em 2025

Maturidade e Postura de Segurança

- Obtivemos a classificação recorde de maturidade em segurança, com uma pontuação de 4,4 no Modelo de Cibersegurança de 2025 do Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST), superando todos os principais benchmarks do setor pelo sexto ano consecutivo.
- Alcançamos uma classificação de Postura de Segurança que excedeu os benchmarks do setor de tecnologia pelo quinto ano consecutivo, demonstrando uma postura de segurança consistentemente forte para clientes e reguladores.

Conformidade

- Conquistamos com sucesso 52 certificações em 2025 com uma redução de 2% no custo por certificação ano após ano, e uma diminuição de 66% em relação a 2018.
- Otimizamos a conformidade lançando um portal de evidências automatizado e um novo painel para mapear descobertas diretamente para controles específicos, reduzindo os esforços manuais de conformidade.

Fusões e Aquisições (M&A)

- Alcançamos a integração de duas aquisições anteriores usando nossa estrutura de M&A repetível baseada no NIST, garantindo uma transição mais segura.
- Aceleramos o ciclo de vida de M&A combinando avaliações de API sem agente com IA generativa, reduzindo os prazos de due diligence de semanas para dias, enquanto automatizamos a análise de dados para integrações mais rápidas e inteligentes.

Segurança Cibernética

- Identificamos, avaliamos e garantimos a remediação de mais de 3.700 componentes de infraestrutura crítica, um aumento de 164% na comparação anual, mantendo um tempo médio de fechamento de menos de 24 horas, reduzindo significativamente a superfície de ataque da organização.
- Construímos e pilotamos um novo agente de triagem de IA, que agora está ajudando a resolver automaticamente quase 50% de todos os tickets de incidentes do SOC.
- Mantivemos logins sem senha para nossos quase 22.000 colaboradores e prestadores de serviço globalmente.
- Concluímos a migração para gerenciamento de acesso nativo da nuvem para aproximadamente 2.000 aplicativos, melhorando o controle de acesso e a visibilidade.
- Implantamos IA para traduzir relatórios de inteligência de ameaças não estruturados em cenários de ataque simulados acionáveis, nos permitindo testar nossas defesas contra novas táticas adversárias dias após sua descoberta, não meses.
- Aplicamos Autenticação Multifator (MFA) para 100% do acesso remoto, reduzindo riscos de entrada não autorizada.

Segurança Física e Investigações

- Concluímos 29 testes de acesso físico, identificando áreas de melhoria contínua.
- Conduzimos 43 avaliações de segurança física para proteger colaboradores, dados e ativos.

Gestão de Risco

- Estabelecemos um mecanismo de risco quantitativo como a fonte confiável de verdade para métricas de segurança, permitindo a ingestão diária e priorização de tarefas de remediação de vulnerabilidades.
- Realizamos análises de risco aprofundadas em 100% das empresas terceirizadas e de alto risco da nossa empresa (2.289), impulsionando planos de remediação acionáveis onde necessário.
- Concluímos avaliações de risco em 100% dos aplicativos de negócios (4.022) para estabelecer uma compreensão abrangente do risco de ativos.
- Continuamos a integrar contas estratégicas chave, incluindo algumas das maiores instituições financeiras do mundo, no CloudControl, fornecendo visibilidade em tempo real sobre a segurança dos seus produtos e serviços Equifax.

Gestão de Crises

- Conduzimos 18 exercícios de simulação com stakeholders da empresa, incluindo:
  - CEO e Equipe Executiva
  - Equipes de Crise Regionais e de Unidade de Negócios
- Introduzimos novos exercícios de mesa focados em cenários de ameaça interna, modelagem de IA, ransomware e engenharia social, capacitando as lideranças a responder a ameaças avançadas.
- Implementamos planos de crise personalizados e facilitamos exercícios de simulação regionais em espanhol e português, para garantir a prontidão da equipe local.
- Integramos a Gestão de Crises com Continuidade de Negócios e Recuperação de Desastres, formando uma organização única e unificada de Resiliência de Negócios.

Treinamento de Segurança

- Conduzimos mais de 240.000 simulações de phishing (aumento de 15% ano após ano), aumentando continuamente a dificuldade à medida que o cenário de ameaças evolui.
- Redirecionamos colaboradores que demonstraram suscetibilidade ao phishing para educar ainda mais sobre técnicas comuns de agentes de ameaças.
- Introduzimos uma nova ferramenta de denúncia de ameaças, gerando mais de 20.000 denúncias de potencial phishing de colaboradores e contratados temporariamente em apenas 6 meses, dos quais quase 1.500 foram confirmados como contendo indicadores maliciosos.
- Incorporamos 6 novos fatores aos Relatórios de Segurança mensais dos colaboradores, incluindo comportamentos relacionados a:
  - Certificação de Acesso, avaliando a recertificação oportuna do acesso do usuário, uso da conta e propriedade de direitos.
  - Utilização de Golden Image, medindo se os engenheiros estão usando golden images padronizadas para ambientes.
  - Governança de Problemas, medindo a pontualidade no fechamento de problemas de segurança abertos.

Engajamento do Cliente

- Concluímos 2.599 questionários de clientes, com um tempo médio de conclusão de 1,86 dias, fornecendo garantia de segurança rápida para partes externas.
- Concluímos 1.149 solicitações de evidências a pedido de clientes da Equifax para garantir a conformidade.
- Trouxemos com segurança mais de 180 NPIs ao mercado, nosso sexto ano consecutivo acima de 100.

Privacidade

- Implementamos uma nova ferramenta para prevenção de perda de dados (DLP na sigla em inglês) de e-mail, fornecendo maior compatibilidade com nosso conjunto de ferramentas existente, análises mais robustas e conformidade global aprimorada.
- Obtivemos recertificação para a Data Privacy Framework (DPF na sigla em inglês) pelo 2º ano, permitindo transferências seguras de dados da União Europeia/Reino Unido para os EUA.
- Lançamos uma nova plataforma de gestão de consentimento globalmente para respeitar as escolhas dos visitantes do site.

Fraude

- Finalizamos a Estratégia Global de Monitoramento de Fraudes e padronizamos o bloqueio de contas fraudulentas em uma única plataforma em nuvem, unificando processos entre unidades de negócios.
- Bloqueamos mais de 3.700 dispositivos suspeitos e 2.900 IPs suspeitos por meio de investigações de fraude.
- Incidentes de fraude envolvendo exposição de dados sensíveis caíram 18% ano após ano, destacando nossa capacidade de parar atividades suspeitas antes que aumentem.
- Estabelecemos uma nova equipe de fraude na Índia, fornecendo cobertura e capacidade de fraude global expandidas em vários fusos horários.

Desenvolvimento de Software Seguro

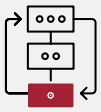
- Melhoramos a adoção de Infraestrutura como Código (IaC na sigla em inglês) em 52%, aproveitando blocos de código padronizados para garantir o alinhamento com os padrões de configuração da Equifax e eliminar configurações manuais incorretas.
- Lançamos um Assistente Pessoal alimentado por IA para fluxos de trabalho de Serviços de Consultoria em Segurança (SAS na sigla em inglês) que reduziu o tempo médio de resolução para consultas em 61% e cortou solicitações iniciais de escalonamento em 56%.
- Desenvolvemos uma arquitetura de IA personalizada para analisar vulnerabilidades de contêineres e gerar automaticamente o código de correção, simplificando o fluxo de trabalho para resolver mais de 213.000 descobertas anualmente.
- Lançamos o Kit de Ferramentas de Gerenciamento Automatizado de Certificados para automatizar a renovação dos certificados TLS das aplicações (as credenciais digitais que criptografam os dados em trânsito). Essa ferramenta controla as datas de vencimento, atualiza e testa os certificados sem intervenção manual.

Nossas prioridades em 2026

Protegendo Cada Identidade: Humana e Máquina

Ao eliminar credenciais para toda a nossa força de trabalho, provamos que o método de logins sem senha é possível. Em 2026, vamos ampliar essa revolução. Começaremos a lançar uma opção para logins sem senha para nossos clientes B2B, neutralizando ataques de preenchimento de credenciais enquanto removemos o atrito para os nossos parceiros.

Simultaneamente, estamos visando a maioria silenciosa das identidades: contas não humanas. À medida que os nossos agentes de IA e APIs se multiplicam, as mesmas verificações rigorosas que fazemos às pessoas estão sendo aplicadas às máquinas,, garantindo que um bot não possa ser usado como backdoor.



Ampliando Nossa Governança Agêntica

Em 2025, construímos os protocolos para proteger nossa primeira geração de agentes de IA. Em 2026, estamos industrializando essa rede de segurança. Estamos expandindo nossa estrutura de “Política como Código” para cobrir cada área da empresa, automatizando os testes de milhares de agentes para segurança, desvio e privacidade de dados estrita. Essa abordagem de governança desde o design garante que nos mantenhamos à frente do complexo cenário regulatório de IA.

Ao escalar essas proteções automatizadas, permitiremos que a Equifax deixe de testar fluxos de trabalho agênticos para executá-los como um motor de negócios padrão de alto volume, sem nunca comprometer nossa segurança e controle.

Evoluindo o Risco Contextual

Quando se trata de analisar o risco de segurança, somos adeptos de filtrar o ruído e considerar o contexto, incluindo valor do recurso, exposição à internet e controles compensatórios. Agora, estamos mudando como vemos o sinal.

Em 2026, estamos reformulando como o risco de segurança é visualizado, transformando cálculos complexos em um mapa de alta fidelidade da exposição do negócio. Também estamos padronizando avaliações para casos extremos e validando nosso inventário de ativos para garantir que a nossa imagem esteja completa. Essa evolução converte dados de risco abstratos em sinais de negócios claros e inegáveis, tornando o próximo movimento certo mais óbvio para cada tomador de decisão.