Forcepoint Data Visibility

powered by Getvisibility

Aprimore a segurança de dados com uma visão panorâmica dos seus dados

Forcepoint

Brochure

forcepoint.com/pt-br

Seus dados estão em todos os lugares e isso é apenas o começo dos problemas. É muito provável que estejam também distribuídos em data centers, várias nuvens e muitos notebooks, o que aumenta ainda mais o seu problema de controle. Você sabe exatamente quais dados possui, onde estão localizados e, mais importante ainda, quais são os riscos que todos esses dados estão trazendo para sua empresa neste momento? O IDC estimou que 80% dos dados globalmente não são estruturados e 90% desses dados não são analisados[1] — em outras palavras, são dados que não fazem parte do trabalho diário de uma organização e não são conhecidos. Esses dados são literalmente invisíveis. À medida que as organizações enfrentam crescentes demandas de conformidade e mais violações de dados[2], é fundamental obter visibilidade sobre todos os dados para minimizar o risco e os custos resultantes. Essa questão requer atenção contínua de organizações de todos os tipos e tamanhos.

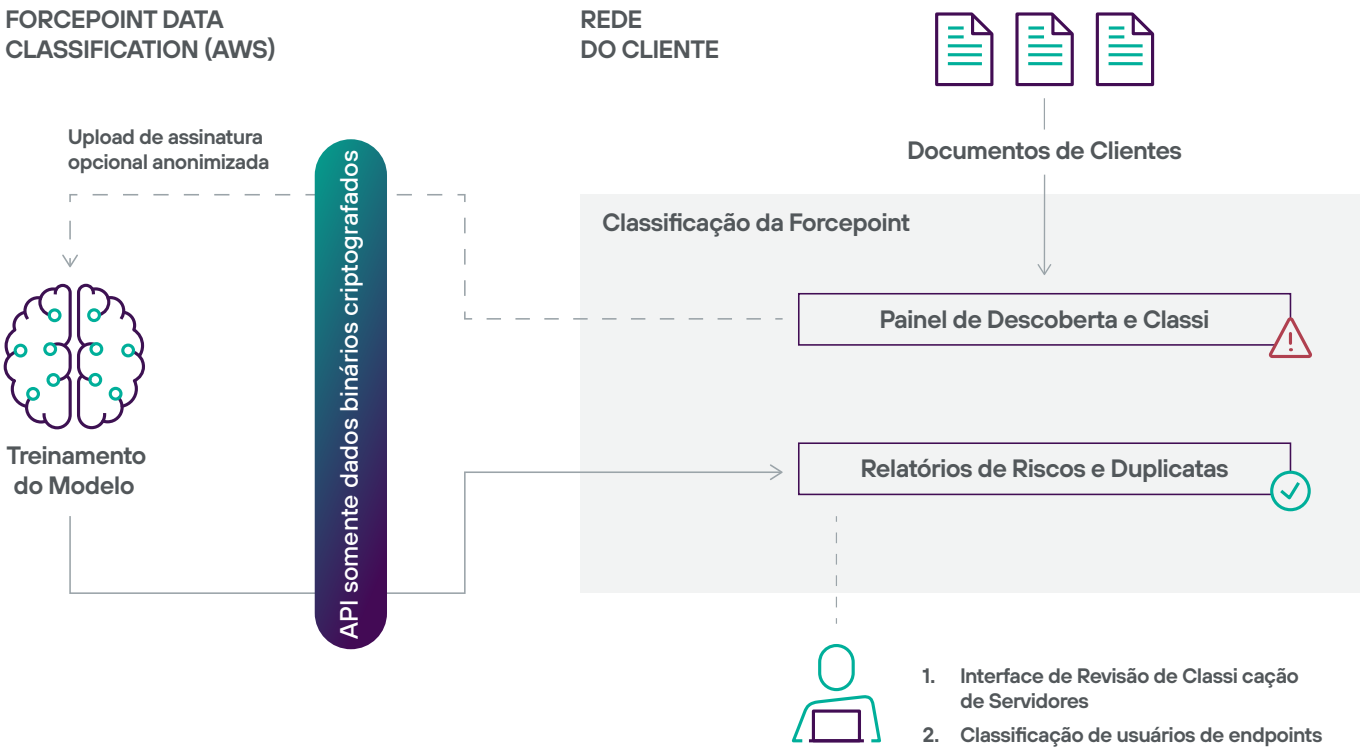
Minimizar o risco começa com a visualização dos dados onde quer que estejam — no local ou na nuvem. O Forcepoint Data Visibility fornece uma visão panorâmica dos dados da sua organização. A visibilidade de dados é uma parte essencial da abordagem da Forcepoint para segurança de dados, que permite que os clientes descubram, classifiquem, monitorem e protejam continuamente todos os dados. A visão em 360° fornecida pelo Forcepoint Data Visibility pode reduzir drasticamente a perda de dados, remover o risco de conformidade e, consequentemente, economizar os enormes custos decorrentes de violações de dados e não conformidade.

De acordo com o IDC, 80% dos dados globalmente não são estruturados e 90% desses dados não são analisados, também chamados de "dark data". [3]

94% das organizações estão armazenando dados em vários ambientes de nuvem.[4]

A Equifax fez um acordo US$ 1,4 bilhão por violação de dados5 exacerbada por hackers que acessaram uma unidade compartilhada com várias cópias de nomes de usuário e senhas de funcionários. A empresa carecia de ferramentas para detectar e identificar arquivos redundantes e desatualizados.

1 The Unseen Data Conundrum, Forbes, fevereiro de 2022
2 2022 Data Breach Investigations Report, Verizon, maio de 2022
3 The Unseen Data Conundrum, Forbes, fevereiro de 2022
4 Dark Data: The Cloud's Unknown Security and Privacy Risk, Forbes,Junho de 2023
5 Equifax agrees $1.38bn data breach lawsuit settlement, Finextra, janeiro de 2020


FORCEPOINT DATA CLASSIFICATION (AWS)
REDE DO CLIENTE
Upload de assinatura opcional anonimizada
API somente dados binários criptografados
Documentos de Clientes
Classificação da Forcepoint
Painel de Descoberta e Classi
Relatórios de Riscos e Duplicatas
Treinamento do Modelo
1. Interface de Revisão de Classi cação de Servidores
2. Classificação de usuários de endpoints

Visibilidade rápida alavancando a potência da Inteligência Artificial (IA)

Com organizações que armazenam dados em vários ambientes de nuvem, incluindo no local, depender de um provedor de nuvem que só pode fornecer visibilidade para os dados em seu próprio serviço de nuvem limita severamente a eficácia da segurança de dados. Em segundo lugar, as ferramentas típicas de descoberta e classificação requerem intervenção manual do administrador para fornecer resultados; mesmo aqueles que fazem uso limitado do Machine Learning (ML) precisam de alguém para tomar decisões de treinamento.

O Forcepoint Data Visibility supera esses desafios aplicando IA com autoaprendizagem e Modelos de linguagem de grande porte (LLMs) para automatizar o processo de encontrar, categorizar e classificar dados, independentemente de estarem armazenados na nuvem ou no local. O poderoso modelo de descoberta e classificação pré-treinado da solução baseia-se em um modelo de 50 dimensões treinado por centenas de milhões de arquivos de dados do mundo real de muitas organizações em todos os principais setores. Essa abordagem inovadora gera dados sintéticos de alta qualidade para precisão de classificação incomparável e melhoria contínua, sem comprometer a privacidade de dados associada a dados reais. À medida que o mecanismo da Forcepoint absorve os dados, seu aprendizado contínuo com IA faz sugestões de classificação de dados em linguagem natural, com categorização de dados altamente precisa, upload de assinatura anônima opcional Classificação da Forcepoint FORCEPOINT DATA CLASSIFICATION (AWS) PARA REDE DE CLIENTES Painel de descoberta e classificação Relatório de riscos e duplicatas Treinamento de modelos Documentos de clientes 1. Avaliação de usuários de endpoints 2. Classificação de usuários de endpoints Detecção de PII de API e pontuação de riscos de conformidade de dados.

O Forcepoint Data Visibility fornece essas informações em painéis e relatórios de alta fidelidade. Esses painéis também revelam o endereço IP, o caminho e as permissões detalhadas de cada arquivo descoberto. Nossa precisão de classificação melhora com o uso ao longo do tempo e, quando combinada com o Forcepoint Data Loss Prevention (DLP), traz maior visibilidade para o mais alto nível de segurança de dados.

- **Precisão com IA:** abandone a busca manual e lenta de dados. A IA de autoaprendizagem da Forcepoint localiza, categoriza e classifica automaticamente todos os seus dados, mesmo em nuvens e no local, economizando tempo e aumentando a precisão.
- **Fim dos pontos cegos de dados:** obtenha painéis claros com detalhes profundos de arquivos, incluindo localização, permissões e pontuações de riscos. Tome decisões informadas mais rapidamente com visualizações de dados intuitivas.
- **Segurança mais inteligente:** a IA da Forcepoint aprende e se adapta continuamente, sugerindo classificações de dados em linguagem simples e detectando PII confidenciais — tudo para evitar proativamente violações de dados e não conformidades.

Visibility into who can see your most sensitive information.

Você realmente deseja que os prestadores de serviços vejam PII de clientes ou informações confidenciais de vendas? Muitas organizações experimentam "acúmulo de privilégios", com permissões de acesso muito superiores ao que é necessário para os funcionários trabalharem. O controle do acesso às informações mais confidenciais costuma ser negligenciado e mal administrado, mesmo entre empresas que estão tentando estabelecer princípios de segurança Zero Trust. Usuários com excesso de privilégios podem, como consequência, custar às empresas muito dinheiro em violações e não conformidades.

O Forcepoint Data Visibility permite que você inspecione permissões para todos os arquivos e usuários. Os administradores de dados podem ver quais pessoas têm acesso a um arquivo ou às unidades de compartilhamentos de arquivos em toda a organização. Por meio de varredura regular, o excesso de privilégios pode ser interrompido, reduzindo drasticamente a oportunidade para violações de dados. Com um único clique, você pode visualizar imediatamente as permissões de todos os arquivos verificados. Então, pode aplicar o nível adequado de permissões necessárias para que os usuários façam seu trabalho.

- **Impeça o "acúmulo de privilégios":** garanta que os usuários acessem apenas os dados de que precisam, evitando ameaças internas e vazamentos acidentais. Um clique revela permissões para todos os arquivos verificados, permitindo que você aplique o nível certo de acesso à velocidade da luz.
- **Cumpra as exigências regulatórias:** evite litígios e penalidades dispendiosas ganhando visibilidade sobre as permissões para todos os arquivos e usuários.
- **Reduza o risco de violação de dados:** elimine usuários com excesso de privilégios, um alvo preferencial dos invasores. As varreduras regulares detectam e impedem o aumento de privilégios em seu caminho, reduzindo drasticamente o potencial de violações de dados.

Limpando o ROT para reduzir a responsabilidade pelos dados

Sua empresa é uma acumuladora na forma de administrar dados? Programas de TV populares apresentam pessoas que não conseguem jogar nada fora, mostrando como elas acabam vivendo em uma montanha de lixo que se torna completamente incontrolável. Muitas organizações acumulam dados, de alguma forma acreditando que a manutenção dos dados é boa e até mesmo reduz o risco. O oposto é verdadeiro. Os dados podem ser um ativo, mas também podem ser um passivo. O resultado para as organizações que se apegam aos dados é que acumulam uma grande quantidade de dados ROT (redundantes, obsoletos ou triviais). Em vez de colocar as empresas em conformidade, isso pode deixá-las extremamente vulneráveis a violações de dados e causar não conformidades ainda maiores em relação ao crescente número de regulamentações de dados. Um detalhamento do que é ROT:

- **Dados redundantes** são um grande número de cópias ou versões de arquivos armazenados em vários locais na nuvem ou no local. As organizações podem evitar erroneamente a exclusão caso os usuários dependam dessa cópia específica ou receiem que a exclusão possa criar risco de não conformidade.
- **Dados desatualizados** são informações que não são mais corretas ou não estão mais em uso. Em geral, os dados obsoletos já foram substituídos por dados atuais e úteis.
- **Dados triviais** são informações cujo armazenamento simplesmente não é necessário. Os dados triviais não fornecem nenhum benefício atual para a organização.

6 Worldwide Digital Loss Technologies Market Shares, 2020: DLP is Dead, Long Live DLP, IDC, October 2021
7 Worldwide Digital Loss Technologies Market Shares, 2020: DLP is Dead, Long Live DLP, IDC, October 2021

Os dados ROT são um passivo porque geralmente contêm informações confidenciais. Sem visibilidade sobre os dados que devem excluir, as empresas se expõem a possíveis violações de dados e penalidades regulatórias. Um exemplo caro de ROT é a violação da Equifax, que resultou em um acordo judicial de US$ 1,38 bilhão.8 No centro da violação estava uma unidade compartilhada na qual cópias de nomes de usuários e senhas eram salvas pelos funcionários, que acreditavam estar tornando os negócios mais eficientes ao fazer várias cópias de nomes de usuários e senhas. Quando os hackers conseguiram invadir o compartilhamento, as várias cópias de nomes de usuários e senhas facilitaram seu trabalho. A Equifax carecia de ferramentas para detectar e identificar cópias redundantes e desatualizadas dos arquivos.

"Até um terço dos dados corporativos pode ser considerado ROT (e outros 52% são dados obscuros com valor desconhecido)"

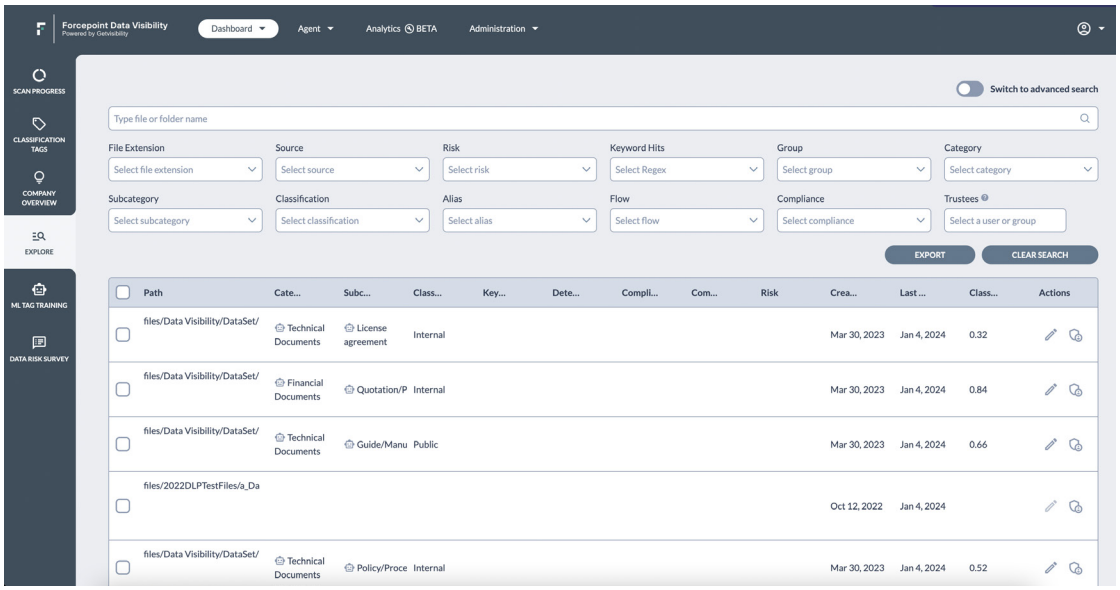
Como evitar que seus dados se deteriorem na nuvem, Forbes, janeiro de 2023

Eliminar o risco de ROT requer automação e insights granulares. O Forcepoint Data Visibility começa fornecendo recursos de descoberta e classificação que podem verificar rapidamente todos os seus dados em qualquer lugar. A precisão com uso de IA oferece clareza absoluta sobre a duplicação de arquivos, datas de criação e última utilização de cada arquivo, e classificação e risco de conformidade de cada arquivo. O painel do Forcepoint Data Visibility permite que os usuários se aprofundem nessas diferentes áreas, vejam detalhes sobre cada arquivo e obtenham relatórios sobre duplicatas. Munido dessas informações, você pode eliminar os dados ROT com sucesso. As organizações que utilizam o Forcepoint Data Visibility podem realizar verificações completas de dados e relatórios de riscos quantas vezes forem necessários, sem despesas adicionais, permitindo que elas resolvam proativamente seus problemas relacionados a dados ROT.

8 Equifax agrees $1.38bn data breach lawsuit settlement, Finextra, January 2020

O primeiro passo numa estratégia de segurança de dados Zero Trust é descobrir e classificar todas as informações existentes e determinar rapidamente o que tem valor e é necessário para a conformidade regulamentar. Todo o resto é ROT e pode ser excluído de forma defensável.

Painel amigável para uma visão panorâmica dos seus dados



O Forcepoint Data Visibility oferece aos administradores um painel amigável com pesquisa, filtros e classificação de forma fácil conforme as necessidades do administrador. Há opções para verificar os resultados do modelo de IA, alterar a categoria e subcategoria e ajustar a presença de PII dentro de um documento, que podem ser atualizadas no modelo de IA de forma automática e manual. Simplificando ainda mais as operações de segurança, esses resultados podem ser exportados em um formato acionável para correção ou uso em outras tarefas para lidar com áreas de riscos.

A utilização desse modelo de IA de treinamento orientado pelo usuário proporciona autoaprendizagem contínua para maior personalização e precisão para a organização.

Modelo de autoaprendizagem contínuo para maior personalização e precisão

O Forcepoint Data Visibility utiliza o poder da IA generativa e vários modelos de linguagem de grande porte (LLMs) líderes para aprimorar a segurança de dados de várias maneiras:

- → **Precisão aprimorada:** nossos modelos de IA avançada são pré-treinados e aprendem com um extenso repositório de centenas de milhões de arquivos de diversas empresas e setores. Essa abordagem abrangente garante a classificação precisa dos dados entendendo as nuances de vários cenários organizacionais, tornando as classificações significativas e acionáveis.
- → **Dados sintéticos de alta qualidade:** isso representa uma abordagem inovadora na qual geramos dados sintéticos precisos a partir do nosso modelo de IA, garantindo precisão de classificação incomparável e melhoria contínua sem comprometer a privacidade ou a segurança associadas a dados reais.
- → **Modelo de IA personalizada:** nosso modelo de IA é orientado pelo usuário e otimizado continuamente, oferecendo uma solução moldada às suas necessidades organizacionais e específicas do setor para seu cenário de dados, fornecendo melhor personalização e precisão.

Todos esses elementos trabalham juntos e de forma integrada para oferecer uma precisão de classificação de mais de 98% em 70 campos de classificação, proporcionando melhor visibilidade dos dados em toda a organização. Isso se traduz em um número menor de falsos positivos de DLP, além de uma defesa mais robusta contra violações e exfiltração de dados.

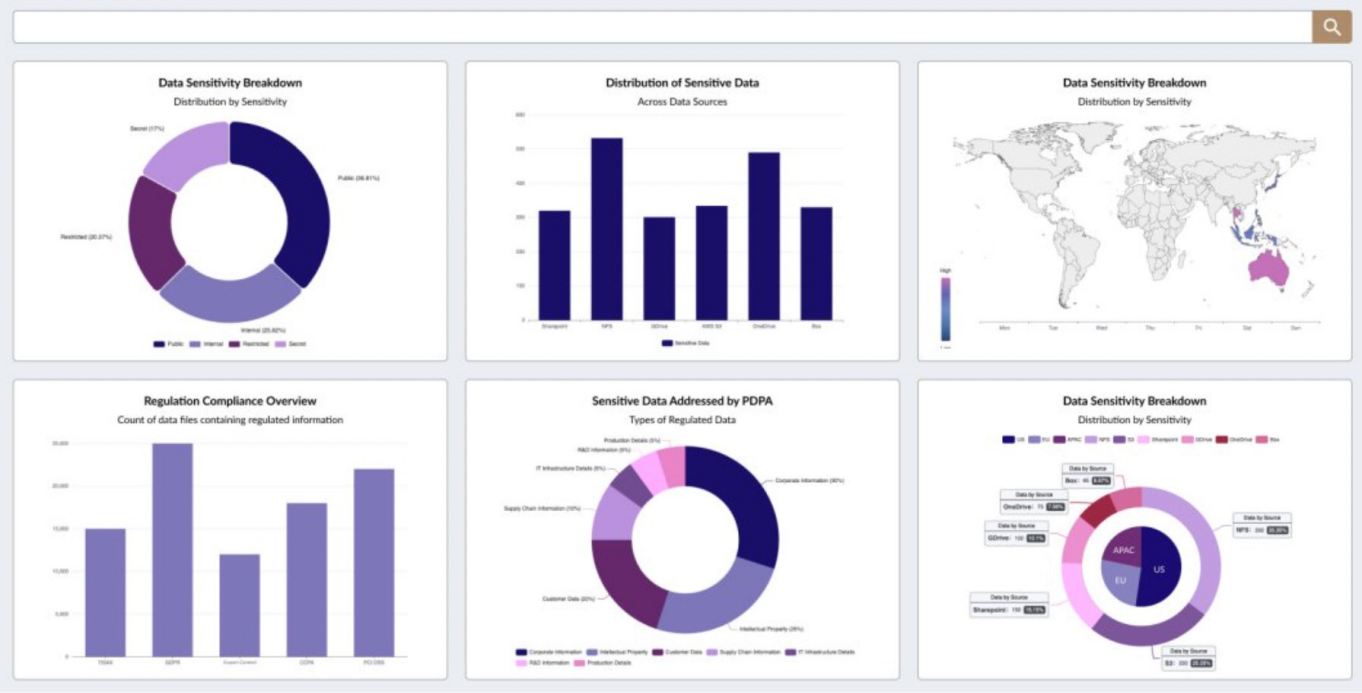
Menos privilégios de acesso fortalece sua estratégia Zero Trust

Um elemento-chave que fortalece sua estratégia Zero Trust é o princípio do acesso com menos privilégios. Ao limitar estritamente o acesso apenas aos requisitos essenciais, criamos um ambiente de dados mais seguro. Essa abordagem não apenas aprimora a visibilidade geral dos dados, mas também contribui para uma defesa robusta contra possíveis ameaças, ajudando a acelerar suas iniciativas de segurança Zero Trust

O pacote de relatórios do Forcepoint Data Visibility fica dentro do painel do administrador e permite a geração de relatórios específicos de casos de uso com um clique. Isso fornece informações sobre as principais áreas de risco relacionadas a usuários, grupos e senhas, além de garantir as permissões de acesso corretas.

Os relatórios disponíveis incluem, mas não estão limitados a: Sensitive Files

- → Arquivos confidenciais
- → Permissões de acesso
- → Arquivos duplicados
- → Redundante, obsoleto ou trivial (ROT)
- → Avaliações de riscos de dados



Usando modelos de IA e automação avançada, o Forcepoint Data Visibility oferece visibilidade, classificação e monitoramento contínuo de dados com mais rapidez e precisão do que os métodos tradicionais. Você pode facilmente identificar e diferenciar entre propriedade intelectual confidencial, PII e pilhas de arquivos sem sentido. Pode garantir o acesso com menos privilégios para evitar a exfiltração enquanto seus usuários finais permanecem produtivos com facilidade. Ao fornecer uma visão panorâmica dos dados em uma ampla gama de fontes (servidores de arquivos, Microsoft OneDrive, SharePoint, Google Drive, Box, Confluence, Azure e muito mais), o Forcepoint Data Visibility é um componente essencial de uma abordagem completa de segurança de dados.

Que tal migrar para visibilidade de dados baseada em IA?

Saiba Mais

Forcepoint

forcepoint.com/pt-br/contact

Sobre a Forcepoint

A Forcepoint simplifica a segurança para empresas e governos globais. A plataforma all-in-one verdadeiramente nativa da nuvem da Forcepoint facilita a adoção de Zero Trust e evita roubo ou perda de dados confidenciais e propriedade intelectual, não importa onde as pessoas estejam trabalhando. Com sede em Austin, Texas, a Forcepoint cria ambientes seguros e confiáveis para clientes e seus funcionários em mais de 150 países. Entre em contato com a Forcepoint em www.forcepoint.com/pt-br, Twitter e LinkedIn.

[FP-Forcepoint Data Visibility Powered By Getvisibility-Brochure-PT-BR] 24Jan2024