DELPHIX

DESCRIÇÃO TÉCNICA

Mascaramento de Dados com a Plataforma de Dados Delphix

Histórico do Setor

O mascaramento de dados é agora mais importante do que nunca. Com as frequentes violações de dados aparecendo no noticiário e a criação de legislações rígidas sobre privacidade dos dados, é imprescindível que as empresas de todos os setores gerenciem seus dados com mais cautela e sigilo. Não proteger informações pessoais, de saúde e sensíveis em conformidade com as leis de proteção de dados, como GDPR, LGPD, e HIPAA, resulta em pesadas multas e danos permanentes à reputação.

O rápido aumento dos volumes de dados torna ainda mais difícil o desafio de proteger dados confidenciais, principalmente porque os dados estão dispersos em ambientes usados para desenvolvimento, testes, analytics e outras aplicações “não produtivas”. Uma pesquisa recente estima que, para cada cópia de dados produtivos, as empresas criam mais de dez cópias que multiplicam a exposição ao risco. Organizações com foco em segurança estão adotando o mascaramento de dados como uma solução para proteger essas cópias. Na verdade, a tecnologia de mascaramento está rapidamente se tornando uma parte da arquitetura de referência para organizações que buscam uma abordagem holística de gerenciamento e proteção de dados.

Descrição da Solução

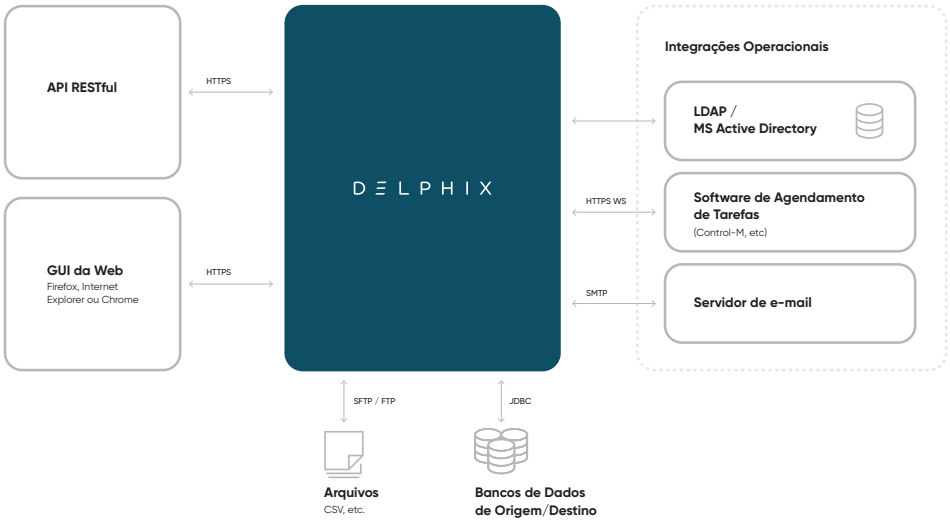
A Plataforma de Dados Delphix consiste em uma abordagem abrangente para o mascaramento de dados, atendendo aos requisitos de desempenho, escalabilidade e segurança de nível corporativo. Com a plataforma Delphix, as organizações conseguem proteger dados sensíveis de maneira eficaz executando as seguintes etapas fundamentais:

- **Identificação de dados sensíveis:** Identifique informações sensíveis como nomes, endereços de e-mail e informações de pagamento de modo a fornecer uma visão geral da organização com relação aos riscos e para indicar os dados que precisam de mascaramento.
- **Proteção de dados sensíveis:** Faça o mascaramento para transformar valores de dados sensíveis em equivalentes fictícios, mas realistas, além de preservar o valor para o negócio dos dados para aplicações que envolvem ambientes de desenvolvimento e testes. Ao contrário de abordagens que utilizam criptografia, o mascaramento não apenas garante que os dados transformados ainda possam ser usados em ambientes não produtivos, mas também implica um processo irreversível que impede que os dados originais sejam restaurados usando-se chaves de descriptografia ou outros recursos.
- **Escalonamento e integração:** Amplie a solução para atender aos requisitos corporativos de segurança e integre-a a workflows fundamentais (ex.: aplicações de SDLC ou processos de compliance).

Em conjunto, essas funcionalidades permitem que as empresas definam, gerenciem e apliquem políticas de segurança a partir de um gerenciamento centralizado de grandes e complexos conjuntos de dados. Delphix permite a realização de operações globais com suporte a endereços internacionais e conjuntos de caracteres. Além disso, o mascaramento do Delphix é rapidamente configurado e implantado utilizando workflows orientados por GUI sem a necessidade de conhecimentos específicos de programação ou contratação de serviços demorados.

Como o Mascaramento do Delphix Funciona

Um exemplo de aplicação da Plataforma de Dados Delphix – um “engine” da Delphix – se refere a um ambiente operacional independente que é fornecido como um dispositivo virtual certificado para ser executado em diversas plataformas, como VMware, AWS e Microsoft Azure. A interface gráfica da plataforma Delphix pode ser acessada por navegadores como Explorer, Firefox ou Chrome. Ela dispõe de um sistema de controles robusto baseado em funções que permitem que as organizações atribuam permissões específicas com relação aos locais que os usuários têm acesso e às tarefas que eles podem executar ou não.



Identificação de Dados Sensíveis

Após conectar-se a uma fonte de dados compatível, a plataforma Delphix identifica quais dados devem ser protegidos. A busca por dados sensíveis é realizada aplicando-se dois métodos diferentes: identificação de colunas e identificação de dados.

Identificação de Colunas

A identificação de colunas usa expressões regulares (regex) para escanear metadados (nomes de colunas) das fontes de dados selecionadas. Há diversas expressões de identificação pré-configuradas que foram desenvolvidas para identificar categorias de dados sensíveis comuns (CPF, nome, endereço etc.). Os usuários também podem criar suas próprias expressões usuais de identificação.

Exemplo: Expressão do primeiro nome <(?>(fi?rst)_?(na?me?)|f_?name)(?!\w*ID)>

Identificação de Dados

A identificação de dados usa regex, mas com o objetivo de escanear os dados reais em vez de metadados. Semelhante à identificação de colunas, existem diversas expressões pré-configuradas, e os usuários podem incluir suas próprias expressões.

Expressão do número de telefone < ((\(?\b[0-9]{3}\)?[-.]?[0-9]{3}[-.]?[0-9]{4}\b)(?<![0-9]{6}[.][0-9]{4}))>

Delphix fornece mais de 50 expressões de identificação desenvolvidas após a validação de dezenas de clientes da Fortune 500 para ajudar as empresas a encontrar mais de 25 tipos (números de conta, endereços etc.) de dados sensíveis usando a identificação por colunas ou dados.

Tipos de dados que podem ser localizados usando modelos de expressões de identificação

Números de conta	Número da habilitação	Nome da escola
Endereços	E-mail	Código de segurança
Identidade do beneficiário	Nome	Número de série
Biometria	Endereço IP	Assinatura
Passaporte	Sobrenome	RG
Cidade	Local	CPF
País	Número da placa	Número de telefone
Cartão de crédito	Caixa postal	Número de identificação do veículo
Número do cliente	Região	Endereço de internet
Data de nascimento	Número de registro	CEP

As etapas de criação de perfis de identificação podem ser executadas em diversas fontes de dados para disponibilizar às organizações uma visão geral dos riscos associados a dados sensíveis. Quando um elemento dos dados é identificado como sensível, a plataforma Delphix recomenda algoritmos de mascaramento específicos para serem usados na proteção dos dados.

Templates com Perfis Específicos de Aplicações e Regulamentações

Delphix também oferece templates com perfis para identificação de dados considerando aplicações específicas (ex.: SAP, Oracle EBS) ou dados relevantes no âmbito das leis de proteção de dados específicas (ex.: LGPD, HIPAA, PCI, entre outros). Os templates com perfis contemplam conjuntos de expressões regulares para localizar dados geralmente associados a aplicações/legislações ou um inventário pré-configurado contendo campos que a plataforma Delphix precisa mascarar.
Ao agregar inteligência adicional ao processo de identificação, as organizações podem eliminar a busca e validações manuais, o que as permite mascarar com rapidez e precisão os campos corretos com os algoritmos adequados.

Proteção de Dados Sensíveis

O principal método da plataforma Delphix para proteção dos dados é o mascaramento. Os algoritmos de mascaramento criam uma versão com estrutura semelhante, mas fictícia dos dados que pode ser usada para atividades de desenvolvimento e testes de aplicações. O mascaramento protege as informações sensíveis reais e, ao mesmo tempo, gera um substituto funcional para situações em que os dados reais não são necessários. O mascaramento do Delphix:

- **É irreversível:** os dados mascarados não podem ser submetidos à engenharia reversa para serem restaurados ao seu estado original não mascarado.
- **Cria Resultados Representativos dos Dados de Origem:** o resultado do mascaramento do Delphix é semelhante a dados produtivos para fins não produtivos. É um processo que pode incluir atribuições geográficas, atribuições de cartão de crédito (ex.: manter os primeiros 4 números inalterados e embaralhar os demais) ou manter nomes e endereços (fakes) legíveis.
- **Preserva a integridade referencial:** Delphix tem a capacidade de mascarar dados de forma consistente para manter a integridade referencial. Se o número de uma conta for uma chave principal e for embaralhado como parte do mascaramento, todas as instâncias desse número de conta vinculadas por meio de pares de chave serão mascaradas de forma idêntica. Além disso, a plataforma Delphix escala horizontalmente, de maneira que os algoritmos de mascaramento preservam a integridade referencial em fontes de dados diversas e heterogêneas (consulte “Escalonamento e Integração”).

Quando os campos de dados sensíveis são identificados, o Delphix automaticamente recomenda um algoritmo pré-definido para proteger os dados. Estes algoritmos fazem parte de alguma das seguintes estruturas:

Estrutura do Algoritmo de Mapeamento

Um algoritmo de mapeamento permite que os usuários indiquem quais valores substituirão os dados originais. O algoritmo mapeia de forma sequencial os valores de dados originais como valores mascarados que são pré-propagados em uma tabela de busca por meio da interface de usuário Delphix. Para satisfazer quaisquer requisitos de exclusividade, o algoritmo mapeia dados individualmente. O mapeamento não produz colisões nos dados mascarados e o algoritmo sempre combina a mesma entrada com a mesma saída. Por exemplo, “Davi” sempre se tornará “Rafael” e nenhum outro nome será mascarado como “Rafael”. O algoritmo confere se uma entrada já foi mapeada; em caso positivo, o algoritmo transforma o dado em sua saída designada. Os algoritmos de mapeamento lidam com dados de string arbitrários e preservam a integridade referencial.

Algoritmo “Secure Lookup”

O Secure Lookup preserva a integridade referencial: “Davi” é mascarado consistentemente como “Rafael”; ele também cria colisões: “Davi” e “João” são mascarados como “Rafael”.

Algoritmo de “Mapping”

O mapeamento preserva a integridade referencial: “Davi” é consistentemente mascarado como “Rafael”; ele satisfaz restrições de especificidade: nenhum outro valor será mascarado como “Rafael” além de “Davi”.

Secure Lookup

É o tipo de algoritmo mais usado. É fácil de gerar e funciona com diversos idiomas. Quando esse algoritmo substitui dados reais e sensíveis por dados fictícios, é possível que padrões de dados repetidos sejam criados, os quais são conhecidos como “colisões”. Por exemplo, os nomes “Tomás” e “Pedro” poderiam ser mascarados como “Mateus”. Como nomes e endereços se repetem naturalmente em dados reais, isso imita um conjunto de dados real. O Secure Lookup lida com dados de string arbitrários e preserva a integridade referencial. Entretanto, se você quiser que a Engine de Mascaramento mascare todos os dados transformando-os em saídas específicas, é preciso usar o Mapeamento de Caracteres.

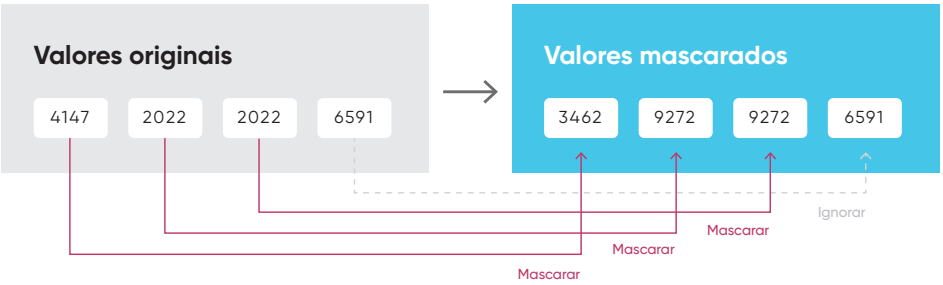
Estrutura de Mapeamento de Caracteres

Este algoritmo mapeia valores de texto, definidos por um conjunto de grupos de caracteres, para outros valores de texto gerados a partir dos mesmos grupos de caracteres. Os mapeamentos são calculados de forma algorítmica, sendo que não é necessário fornecer o conjunto de valores de mapeamento. O algoritmo preserva quaisquer caracteres não atribuídos a um grupo. Quaisquer caracteres do primeiro plano Unicode podem ser mapeados, abrangendo a maioria dos caracteres utilizados nas línguas modernas. Outros caracteres (complementares) só podem ser preservados.

Descrição: capacidade de mascarar caracteres não ASCII.

Estrutura do Algoritmo de Mapeamento de Segmento

Os algoritmos de mapeamento de segmento não produzem sobreposições ou repetições nos dados mascarados. Eles permitem que os usuários criem valores mascarados específicos dividindo um valor alvo em, no máximo, 36 segmentos e mascarando cada segmento individualmente. As organizações podem aplicar esse método para obter informações que envolvem valores específicos, como números de CPF, colunas de chave primária ou colunas de chave estrangeira. O mapeamento de segmentos lida com strings de um formato conhecido e preserva a integridade referencial.



Exemplo mascarar o número de um cartão de crédito em segmentos, preservando os últimos 4 dígitos.

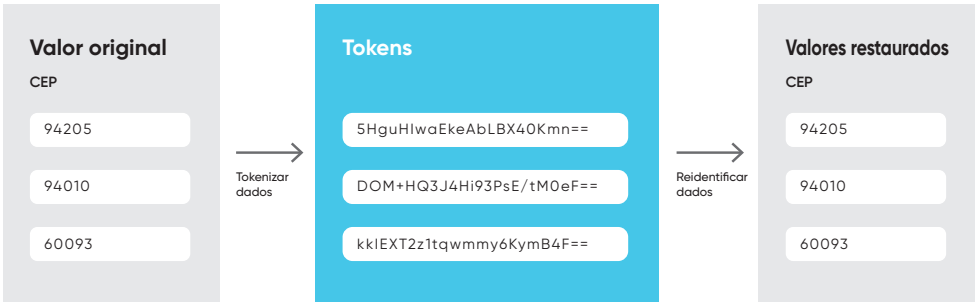
Estrutura do Algoritmo "Binary Lookup"

Um algoritmo de busca binário é semelhante ao algoritmo de busca segura, mas é usado quando todos os arquivos são armazenados em uma coluna específica. Por exemplo, se um banco tem uma coluna de objeto que armazena imagens de cheques, o Delphix pode usar um algoritmo de busca binário para mascarar essas imagens. O Delphix não pode alterar os dados dentro das imagens, como os nomes em radiografias ou carteiras de motorista. Entretanto, o algoritmo pode substituir todas essas imagens por uma nova imagem fictícia. O algoritmo mascara colunas binárias com blob, varbinary ou dados de imagem e preserva a integridade referencial.

Estrutura do Algoritmo de Tokenização

Um algoritmo de tokenização é o único tipo de algoritmo que permite reverter um valor mascarado para seu valor original. Por exemplo, o Delphix pode tokenizar um dado antes de ser enviado a um profissional externo para análise, o que permite que esse profissional identifique contas que precisam de suporte sem ter acesso aos dados sensíveis originais. Após o profissional enviar o feedback, os valores tokenizados podem ser revertidos, permitindo que o proprietário dos dados execute determinadas ações nas devidas contas.

Assim como o mapeamento, o algoritmo de tokenização cria um token exclusivo para cada entrada, como "Davi " ou "Melissa". Os valores de dados reais são convertidos em tokens que não apresentam mais nenhum significado. A tokenização lida com dados de string arbitrários e preserva a integridade referencial.



O parceiro processa dados com valores originais mascarados

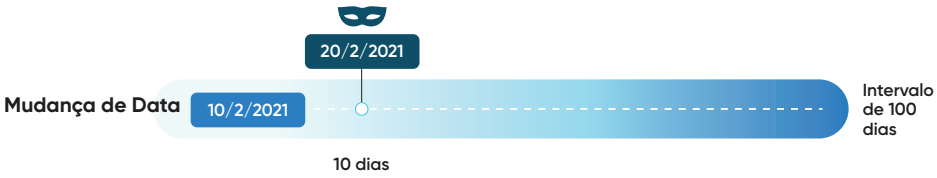
Estrutura de Substituição de Data

A Plataforma Delphix permite mascarar um valor de data com base em datas específicas de início e fim. Os valores de saída mascarados são calculados algoritmicamente usando a chave do algoritmo, por isso, o rechaveamento do algoritmo fará com que seja gerado um valor de saída diferente para cada entrada. Também é possível que uma entrada seja automaticamente mascarada.

Descrição: o algoritmo considera que é importante preservar três meses consecutivos. Também pode ser um número específico de horas, segundos, dias, semanas, ou anos.

Estrutura de Mudança de Data

Este algoritmo mascara os valores de data para datas diferentes com base em um intervalo específico próximo ao valor de entrada. Os valores mascarados são calculados algoritmicamente usando a chave do algoritmo, por isso, o rechaveamento do algoritmo fará com que diferentes valores de saída sejam gerados para cada entrada. Todos os valores de entrada válidos serão mascarados para um novo valor e o novo valor nunca corresponderá ao valor de entrada.



Descrição: neste exemplo, o intervalo do ano de nascimento precisava ficar entre 1950 e 1959.

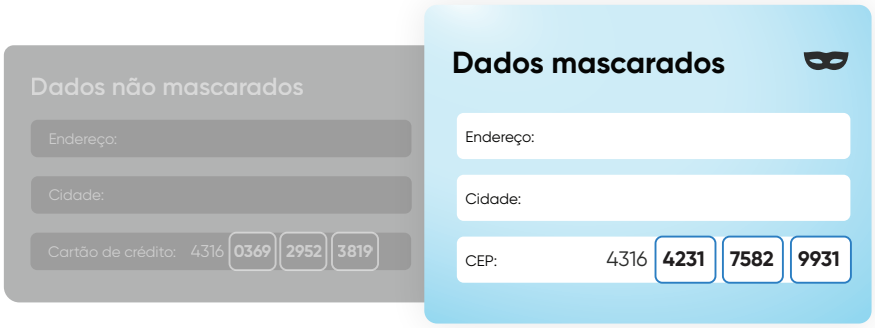
Algoritmo de Mudança de Data Dependente

Quando existe uma dependência entre duas datas que devem ser mantidas, este algoritmo disponibiliza um método que permite tratar datas conjuntas. Alguns exemplos incluem a data de internação e data de alta ou data de nascimento e data de óbito. Se tentarmos mascarar estas datas independentemente, podemos chegar a uma situação em que uma data posterior, como a data da alta, foi mascarada para ser anterior à data da internação. Se estivéssemos tratando com data de nascimento e data do óbito, podemos acabar mascarando os valores de uma forma que transforma uma criança de 80 anos em uma criança de 5 meses.

Descrição: neste exemplo, a regra era ter sempre o ano da alta quatro anos após o ano de internação.

Estrutura de Cartão de Pagamento

O algoritmo do cartão de pagamento mascara números de cartões de pagamento com base nos dígitos iniciais a serem preservados e no número mínimo de posições a serem mascaradas. A estrutura em questão é construída sobre a Estrutura de Algoritmo de Mapeamento de Caracteres com um conjunto de caracteres de [0-9]. Todos os caracteres que não pertencem a este grupo de caracteres continuam sem serem mascarados. Os valores mascarados são calculados algoritmicamente usando a chave do algoritmo, por isso, o rechaveamento do algoritmo fará com que diferentes valores de saída sejam gerados para cada entrada. O último dígito pode continuar o mesmo se o dígito de controle calculado for equivalente ao último dígito do valor de entrada. Quaisquer valores de entrada com mais do que um dígito nunca serão mascarados ao valores originais.

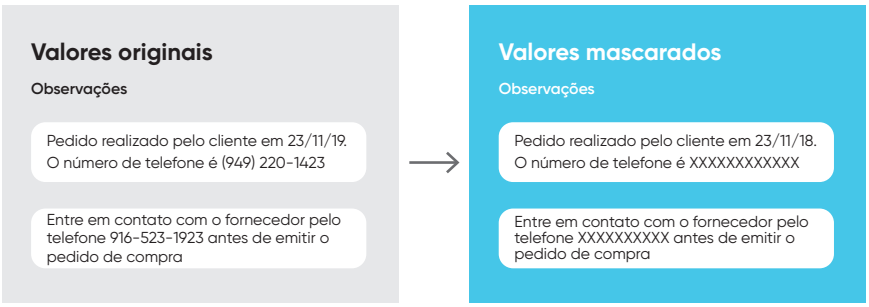


Mascarar os últimos 12 dígitos

Descrição: o mascaramento dos números de cartão de crédito pode manter os dígitos iniciais preservados ou mascarar o número inteiro.

Estrutura de Algoritmo de Texto Livre

Esse algoritmo remove dados sensíveis que aparecem em colunas de texto livre como “Observações”. Por exemplo, o algoritmo pode procurar strings pré-definidas como “R.”, “Av.”, “Al.” e outras palavras que indiquem um endereço. Ele também pode usar a correspondência de padrão para identificar possíveis informações sensíveis. Após a identificação das informações sensíveis em um texto, o algoritmo pode ocultar ou mostrar informações exibindo uma “lista de proibições” (os valores definidos serão removidos/eliminados) ou uma “lista de permissões” (apenas os itens definidos estarão visíveis e os outros itens serão removidos/eliminados). O algoritmo lida com dados de string arbitrários e não preserva a integridade referencial.

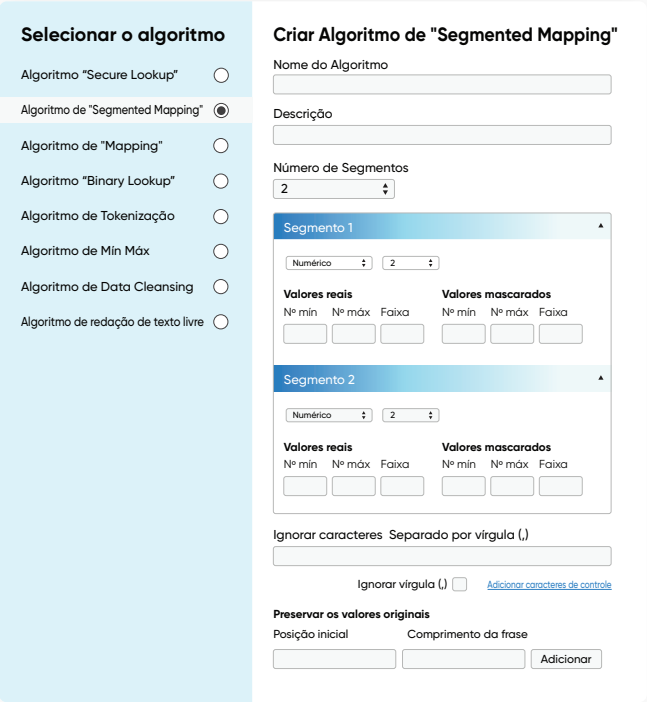


Exemplo Redefinição dos números de telefone na coluna “Observações“.

Criação de Novos Algoritmos Personalizados

A plataforma Delphix permite que as empresas definam com facilidade seus próprios modelos de mascaramento caso nenhum dos algoritmos padrão atenda aos requisitos. Primeiramente, os usuários selecionam uma estrutura de algoritmo como base de um novo algoritmo personalizado e então definem e modificam as propriedades do algoritmo utilizando um processo orientado por GUI. Por exemplo, os usuários podem especificar novas tabelas de busca para o algoritmo de busca segura, personalizar segmentos para um algoritmo de mapeamento de segmento e determinar intervalos de valor para a estrutura do algoritmo de mín máx. .

Como Criar um Algoritmo de Mapeamento de Segmentos Personalizado



Caso os requisitos da organização necessitem que os dados sejam transformados de uma forma que não é compatível com o produto básico, um algoritmo personalizado conhecido como mapplet pode ser criado com a contratação dos Serviços Profissionais da Delphix ou de um Parceiro autorizado e importado para a Plataforma Delphix. Os mapplets são aplicados como funções de JavaScript adaptadas a um formato específico e computam um valor mascarado de acordo com o valor original inserido.

Mascaramento SDK

O Mascaramento SDK permite aos clientes e parceiros desenvolver extensões de algoritmos utilizando ferramentas padrão da indústria, sem o conhecimento interno detalhado dos produtos de mascaramento Delphix que são atualmente necessários para escrever algoritmos personalizados. Trata-se de um recurso que proporciona aos clientes e parceiros um meio direto para criar novos algoritmos de mascaramento nos casos em que os algoritmos Delphix padrão não possam ser facilmente adaptados para atender às necessidades dos clientes.

Execução de Tarefas de Mascaramento

Tarefas de mascaramento são criadas por meio de um workflow orientado por GUI, no qual o usuário seleciona um banco de dados alvo, os algoritmos a serem usados com base nos resultados da identificação, os recursos a serem alocados à tarefa e, caso deseje, as declarações SQL a serem executadas antes ou depois da realização da tarefa.
A Plataforma Delphix pode processar e gerar valores de dados mascarados de duas maneiras:

Mascaramento Local: uma instância do Delphix vai ler os dados de uma fonte, proteger os dados na engine e depois atualizar a fonte de dados com os dados seguros. O mascaramento local apenas transforma as colunas assinaladas, que contêm informações sensíveis, e ignora o restante das colunas. Como para esse método talvez seja necessário copiar dados produtivos em uma zona não produtiva enquanto é feito o mascaramento, os dados sensíveis podem existir em uma zona não produtiva até que o mascaramento seja concluído.

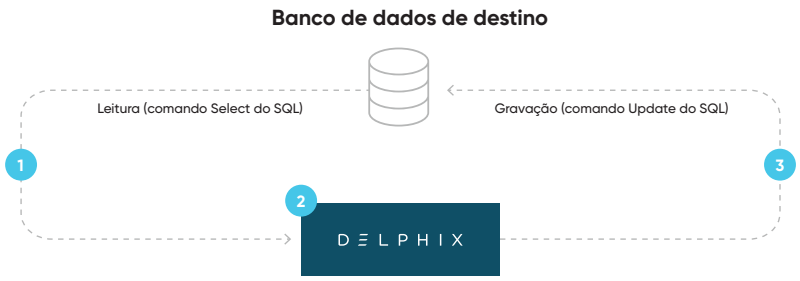


Figura 2. Mascaramento local

1. Leia sobre os dados não mascarados originais do destino.
2. Transforme os valores originais em memória.
3. Atualize os valores de dados sensíveis trocando-os por valores mascarados no destino.

Mascaramento em Trânsito: Delphix lê os dados da fonte de dados, protege os dados na engine e depois coloca os dados seguros em uma fonte de dados de destino (diferente da localização da fonte de dados inicial) em um processo Extract-Transform-Load (ETL). Delphix extrai os dados de um ambiente de origem, como uma cópia de produção, golden copy ou cópia de recuperação de desastres (apenas fazendo a leitura de um banco de dados, não de um documento arquivado). Em seguida, os dados são mascarados na memória do servidor da aplicação no qual eles estão localizados e depois os dados mascarados são carregados no ambiente de destino. Delphix não modifica os dados da origem inicial; apenas os dados de destino são alterados.

Variáveis importantes que afetam o desempenho do mascaramento são: número de tabelas a serem mascaradas, linhas por tabela, colunas por tabela, algoritmo de mascaramento de coluna, tipo de dados, tamanho médio por coluna, além de índices, restrições e acionadores na tabela mascarada.

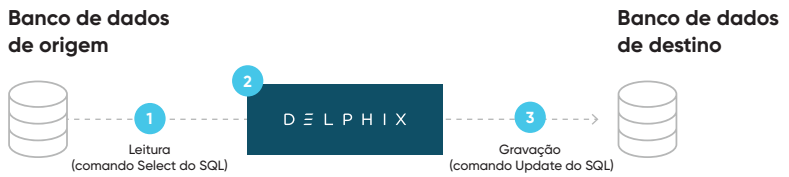


Figura 3. Mascaramento em trânsito

1. Leia sobre dados não mascarados originais.
2. Transforme os valores de dados in-memory.
3. Grave dados mascarados no destino.

Escalonamento e Integração

Delphix permite implantações com diversas engines que garantem que as organizações mascarem os dados de forma consistente em grande escala em fontes de dados diversas e heterogêneas. Nesses cenários, o Delphix facilita a sincronização de informações definindo tarefas de mascaramento em diversos engines de mascaramento. Essas informações podem incluir os algoritmos a serem executados, os conectores de fontes de dados, os inventários de metadados e o conjunto de tabelas ou arquivos em que uma engine executará a identificação, o mascaramento ou a tokenização. A sincronização de engines fornece uma maneira flexível de migrar esses "objetos" de mascaramento – os algoritmos e as informações relacionadas a uma tarefa de mascaramento – necessários para a execução de uma tarefa idêntica em outra engine.

Há dois cenários específicos em que é vantajoso para as organizações aplicarem a orquestração entre diversas engines de mascaramento. No primeiro deles, uma implementação de múltiplas engines lida com o problema de escala horizontal: conseguir um mascaramento consistente em um grande conjunto de fontes de dados implementando diversas engines de mascaramento. A segunda arquitetura lida com a intenção de criar algoritmos em uma engine, testar e validá-los em outras engines e, por fim, implantá-los em uma engine produtivo.

Execução Distribuída

Para muitas organizações, o tamanho dos workloads de identificação e mascaramento exigem mais de uma engine para mascaramento produtivo. Tais engines de mascaramento podem ser idênticas em relação à configuração ou serem parcialmente equivalentes dependendo das necessidades da organização. Objetos sincronizáveis são criados em uma engine chamada "Control Masking Engine" (Engine de Controle de Mascaramento) no diagrama abaixo. Em seguida, esses objetos são distribuídos para "Engines para Processamento de Mascaramento" usando APIs de sincronização de engines. Esses algoritmos e tarefas de mascaramento sincronizados produzirão a mesma saída mascarada em todas as engines, o que permitirá que grandes bancos de dados sejam mascarados de forma consistente.

Figura 4. Sincronização de tarefas de mascaramento em diversas engines.

Ciclo de Vida de Desenvolvimento de Software (SDLC)

Usar um processo de SDLC geralmente exige a configuração de diversas engines de mascaramento, cada uma para uma parte diferente do ciclo (Desenvolvimento, QA, Produção). Aqui, os algoritmos são criados na primeira engine chamada “Dev Engine” (Engine de Desenvolvimento) no diagrama abaixo. Quando o desenvolvedor estiver satisfeito, os algoritmos serão exportados da Engine de Desenvolvimento e importados para a Engine de QA, onde poderão ser testados e validados. Por fim, eles são exportados da Engine de QA e importados para a Engine de Produção.

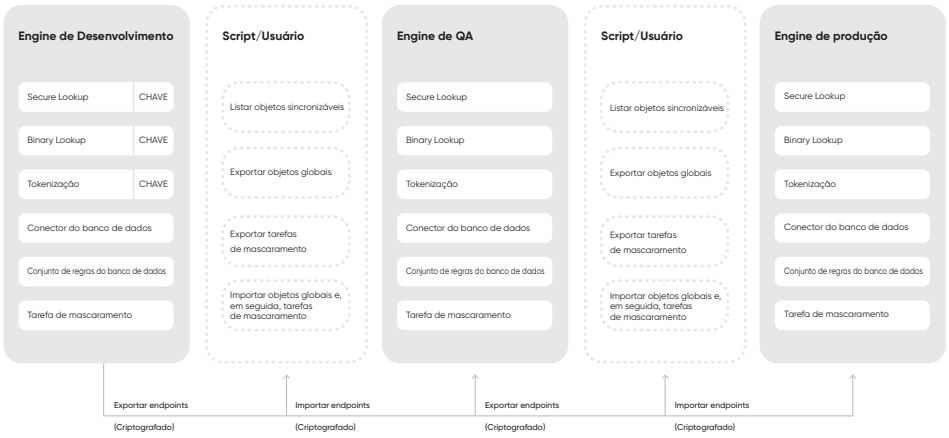


Figura 5. Relação entre as engines nos estágios do SDLC.

Integração por API

Delphix inclui um conjunto robusto de API RESTful que permite que as equipes acessem e manipulem uma representação programática de objetos de mascaramento e recursos usando um conjunto de operações pré-definido. As APIs usam JSON (JavaScript Object Notation) para ingerir e retornar representações de vários objetos usados em inúmeras operações. JSON é um formato padrão e, por isso, tem muitas ferramentas disponíveis para ajudar a criar e analisar cargas úteis de solicitação e resposta, respectivamente. As organizações podem usar as APIs para controlar, com base nos códigos de programação, as características de identificação e mascaramento do Delphix integrando-as aos workflows como:

- Acionamento de tarefas de identificação ou mascaramento conforme os dados mudam ou novos dados são inseridos em repositórios de dados.
- Criação de relatórios de compliance regulatório personalizados para registrar atividades de mascaramento.
- Conexão a sistemas de monitoramento corporativos como o Splunk.
- Sincronização de tarefas de mascaramento em diversas engines Delphix.

Compatibilidade com Fontes de Dados

O mascaramento da Plataforma Delphix é compatível com a identificação, mascaramento e tokenização de diversas fontes de dados, inclusive bancos de dados distribuídos, mainframe, bancos de dados PaaS e arquivos. A Plataforma de Dados Delphix classifica a compatibilidade com fontes de dados em duas categorias:

Conectores Delphix: eles se referem a fontes de dados às quais uma engine de mascaramento pode se conectar diretamente usando conectores integrados que foram otimizados para realizar mascaramento, identificação e tokenização. Delphix apresenta conectores de mascaramento específicos para as seguintes origens de dados:

- **Banco de dados distribuído:** DB2 LUW, Oracle, MS SQL, MySQL, SAP ASE (Sybase), PostgreSQL, MariaDB
- **Mainframe/Midrange:** DB2 Z/OS, DB2 iSeries, VSAM
- **Banco de Dados PaaS:** AWS RDS Oracle
- **Arquivos:** Excel, largura fixa, delimitado, XML

Outras fontes de dados podem ser mascaradas por meio do upload de drivers JDBC em engines Delphix.

Método File Extract Mask and Load (FEML): esse método é usado para mascarar e tokenizar fontes de dados que não têm conectores Delphix específicos. O FEML usa APIs existentes em fontes de dados com o objetivo de extrair dados para um arquivo, mascarar o arquivo e depois usa as APIs para carregar o arquivo mascarado novamente no banco de dados. Fontes de dados complementares como Informix, Azure SQL, Hadoop, Teradata e muitas outras podem ser mascaradas usando FEML.

Entrega Segura de Dados

Em conjunto, as características de mascaramento da plataforma Delphix permitem que as organizações definam, mantenham e implantem diversas políticas de segurança a partir de um gerenciamento centralizado. Delphix codifica qual tipo de informação é considerada sensível com base em vários padrões ou regulamentações, determina exatamente como essas informações são protegidas e grava ações de segurança ao registrar todas as tarefas de mascaramento.

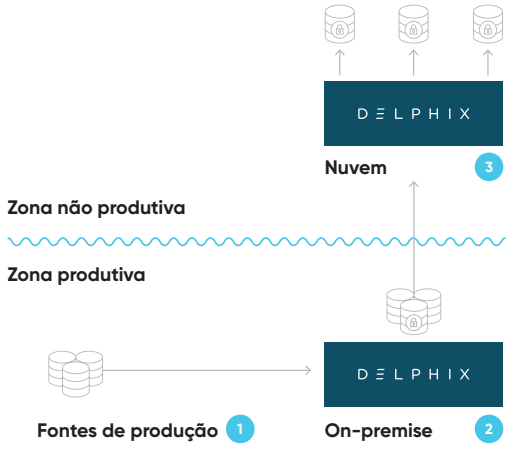


Figura 6. Entrega de cópias de dados virtuais e mascaradas para uma zona não produtiva

1. Sincronização com a zona produtiva de origem.
2. Mascaramento de dados sensíveis.
3. Entrega de dados mascarados em zonas não produtivas e provisionamento de cópias.

A Plataforma de Dados Delphix também combina o mascaramento de dados com a capacidade de virtualizá-los. A plataforma Delphix pode provisionar cópias virtuais de dados produtivos, aplicar mascaramento dentro dos limites da zona de produção e em seguida entregar automaticamente múltiplas cópias mascaradas em ambientes de downstream para tarefas de desenvolvimento, testes, analytics ou outras aplicações não produtivas. Ela é compatível com as iniciativas de aceleração de processos de negócios fundamentais, além de aumentar a governança dos dados: as equipes podem controlar facilmente quem tem acesso a quais dados, em que momento, em qual lugar e por quanto tempo.

Mascaramento de Dados com a Plataforma de Dados Delphix

DELPHIX

www.delphix.com.br

Delphix é a líder da indústria de infraestrutura de dados programáveis. Delphix automatiza o maior obstáculo dos programas de transformação digital — os dados. Com a nossa plataforma de dados em múltiplas nuvens, as empresas modernizam as aplicações legadas 20% mais rápido, migram para a nuvem 30% mais rápido e concluem os ciclos de desenvolvimento de softwares em metade do tempo, garantindo a manutenção da conformidade com as leis GDPR, LGPD, HIPAA e outras Leis de Proteção de Dados.

000199