

# McAfee Data Loss Prevention Discover

**Localize, classifique e proteja seus dados confidenciais, onde quer que eles estejam**

Informações confidenciais que residem em laptops, servidores de arquivos compartilhados e em armazenamento na nuvem podem colocar a sua organização em risco. Há um volume imenso de informações – terabytes e até petabytes – que precisam ser protegidas. Isso é especialmente difícil porque as informações confidenciais nem sempre são rotuladas corretamente. Além disso, na maioria das organizações, não há uma maneira de determinar ou verificar se os dados confidenciais podem estar em risco ou de descobrir para onde eles se propagaram — mesmo com controles de acesso em vigor. Para complicar ainda mais, os dados confidenciais geralmente consistem em tipos de dados não estruturados, como ativos de propriedade intelectual (PI), que são mais difíceis de definir do que dados estruturados, como números de cartão de crédito ou de CPF. O McAfee® Data Loss Prevention Discover (McAfee DLP Discover) ajuda você a localizar e a classificar seus dados confidenciais, descobrir como eles estão sendo usados e protegê-los contra roubo ou vazamento.

## Recursos em destaque

O McAfee DLP Discover ajuda você a identificar e a gerenciar o risco de perda de dados, tanto no local quanto na nuvem. Utilizando técnicas avançadas, o McAfee DLP Discover permite localizar, classificar e proteger todos os tipos de dados corporativos vitais:

- EDM é um novo critério de classificação criado fazendo-se o upload de um arquivo CSV com

informações confidenciais, no qual as células de cada linha são relacionadas. Correspondências de dados exatas são possíveis, para varreduras de repositórios CIFS, SharePoint e Box.

- O McAfee DLP Discover apenas em software proporciona uma economia adicional — appliances com base em máquina virtual ou hardware não são mais necessários.

## Principais vantagens

### Identificação dos riscos de vazamento de dados

- Examine informações armazenadas no local ou na nuvem (Box)
- Identifique onde os dados confidenciais estão armazenados e quem é o proprietário do conteúdo
- Pesquise e visualize todos os dados incluídos na varredura a partir de uma interface intuitiva

### Políticas e relatórios personalizados

- Use políticas predefinidas de conformidade, governança corporativa e propriedade intelectual
- Registre informações confidenciais em sistemas de segurança de informações adjacentes

Conecte-se conosco



## DATA SHEET

- Totalmente distribuído e gerenciado pelo software McAfee® ePolicy Orchestrator® (McAfee ePO™), ele compartilha a mesma política de prevenção de perda de dados (DLP) e extensão de gerenciamento do McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint).
- A correspondência exata de dados proporciona capacidades de impressão digital para dados estruturados em bancos de dados e planilhas do Microsoft Excel. Ela oferece a flexibilidade da definição de múltiplos critérios para disparar uma política de DLP para maior precisão.
- Completamente alinhado com as capacidades de classificação do McAfee DLP Endpoint.
- Compatível com servidores Microsoft Windows Server 2008, Windows Server 2012 e Windows Server 2016.
- Suporte para implementações distribuídas que aproveitem a capacidade ociosa dos servidores existentes e possibilidade de distribuição por uma ampla área geográfica.
- O reconhecimento óptico de caracteres (OCR) identifica e protege os textos existentes em imagens e formulários digitalizados. Ele permite aos usuários inspecionar arquivos gráficos incorporados quanto à presença de conteúdo sigiloso em recursos de rede, incluindo compartilhamentos de arquivos, SharePoint e bancos de dados.<sup>1</sup>

### Prevenção de perda de dados confidenciais

De código-fonte a segredos comerciais, de planos de negócios estratégicos a propriedade intelectual, os ativos de informações são cruciais para sua marca, sua reputação pública e sua vantagem competitiva. Proteger os dados durante a transmissão é vital, mas sua primeira linha de defesa deve ser resguardar os dados confidenciais antes que sejam acessados ou movidos inadequadamente e compreender onde eles residem.

O McAfee DLP Discover ajuda a proteger sua organização contra a perda de dados. Diferentemente de soluções legadas que esperam que você saiba exatamente qual conteúdo deseja proteger, o McAfee DLP Discover proporciona uma cobertura abrangente das informações óbvias e o ajuda a descobrir outras não tão óbvias.

### Determinação de quais informações serão protegidas

Para identificar as informações e os riscos de proliferação, o McAfee DLP Discover pode ser configurado de modo a fazer uma varredura de repositórios específicos e a identificar dados para proteção explícita. Adicionalmente, todos os dados inspecionados pelo McAfee DLP Discover são indexados e disponibilizados por meio de uma interface intuitiva, permitindo que você localize rapidamente dados possivelmente confidenciais a fim de compreender quem é proprietário do conteúdo e onde ele está armazenado.

### Classificação, análise e correção de vazamentos de dados

- Filtre e controle informações confidenciais com classificação multivetorial
- Indexe todo o conteúdo e depois consulte-o e explore-o para compreender os dados confidenciais
- Registre e gere assinaturas para proteger documentos e as informações que eles contêm, mesmo quando plagiadas ou transpostas
- Envie uma notificação de alerta quando o conteúdo infringir as políticas de proteção

### Especificações

---

#### Tipos de conteúdo

Oferece suporte à classificação de arquivos com mais de 300 tipos de conteúdo, incluindo:

- Armazenamento seguro na nuvem (Box)
- Documentos do Microsoft Office
- Arquivos Adobe
- Arquivos de multimídia
- Código-fonte
- Arquivos de projeto
- Arquivos compactados
- Arquivos criptografados
- Políticas integradas
- Propriedade intelectual

## DATA SHEET

### Definição de políticas de proteção

Quando você sabe quais informações devem ser protegidas, o McAfee DLP Discover pode ajudá-lo a protegê-las com precisão. O McAfee DLP Discover oferece recursos intuitivos e unificados de criação de políticas, geração de relatórios e gerenciamento para lhe proporcionar mais controle sobre sua estratégia de proteção de informações para dados estacionários. Os principais benefícios das políticas, regras e classificações do McAfee DLP Discover incluem:

- Numerosas políticas integradas para proporcionar uma experiência simples e imediata.
- Poderoso mecanismo de construção de regras abrangendo desde dados estruturados simples (cartões de crédito, números de CPF) até informações complexas (propriedade intelectual).
- Criação e validação de regras simplificadas, com a transferência da análise dos resultados de pesquisa para uma regra de proteção.
- Integração com vetores de segurança de informações adjacentes para garantir uma proteção consistente.
- Exclusão de documentos públicos e texto comum para impedir que essas informações benignas gerem incidentes.

### Faça uma varredura de sua rede para detectar violações

Depois que as políticas são definidas, o McAfee DLP Discover pode ser instruído a fazer varreduras de rotina dos recursos da rede para detectar violações

de políticas. Opções de programação flexíveis estão disponíveis para a realização de varreduras contínuas, diárias, semanais ou mensais.

O McAfee DLP Discover inspeciona automaticamente todos os recursos acessíveis, inclusive laptops, desktops, servidores, repositórios de documentos, portais e locais de transferência de arquivos, em busca de violações de políticas. Você pode definir grupos de varredura com base em endereços IP, sub-redes, intervalos ou caminhos de rede. Também é possível restringir as operações de varredura com base em parâmetros específicos, como aplicar a varredura apenas à pasta “Meus Documentos” de todos os usuários e não às pastas do sistema, ou procurar por arquivos pertencentes a usuários específicos ou de um certo tipo ou tamanho.

### Revise e corrija as violações

O McAfee DLP Discover elimina ou minimiza a proliferação de material confidencial por meio de um sistema integrado de fluxo de trabalho de incidente e gerenciamento de caso. Quando descobre algum conteúdo que infringe as políticas de proteção, o McAfee DLP Discover gera incidentes e envia notificações. Os incidentes criados pelo McAfee DLP Discover podem ser adicionados à estrutura de gerenciamento de caso, que permite envolver especialistas de numerosas organizações dentro da empresa para adotar ações relacionadas à violação. Além disso, dashboards de riscos proporcionam ao pessoal de segurança maneiras fáceis de visualizar o perfil das violações de políticas e gerar relatórios baseados em qualquer parâmetro relevante dos dados estacionários.

### Repositórios compatíveis

- Common Internet File System/ Server Message Block (CIFS/SMB)
- Microsoft SharePoint
- Bancos de dados: Microsoft SQL, Oracle, DB2, MySQL Enterprise

### Registro de documentos

---

Os documentos podem ser registrados a partir de qualquer repositório. As assinaturas dos documentos registrados podem ser usadas localmente para detectar a proliferação de material confidencial ou disponibilizadas para outros appliances McAfee DLP.

### Geração de relatórios

---

O poderoso mecanismo de análise de incidentes e a visualização do resultado de pesquisas permitem personalizar as exibições com base em dois pontos de articulação contextuais. Estão disponíveis exibições de lista e de detalhes, bem como visualizações resumidas com análise de tendências. Múltiplos relatórios predefinidos e personalizáveis são fornecidos com o sistema.

## DATA SHEET

### Capture e analise os dados armazenados

Além de fazer uma varredura nos recursos de rede para detectar violações de políticas, o McAfee DLP Discover também indexa todo o conteúdo estacionário encontrado na rede e lhe proporciona a capacidade de consultar e explorar essas informações para compreender seus dados confidenciais. O McAfee DLP Discover permite que você compreenda rapidamente seus dados confidenciais, como são usados, a quem pertencem, onde são armazenados e onde proliferaram.

### Classifique dados complexos

O McAfee DLP Discover capacita sua organização para proteger todos os tipos de dados confidenciais — de dados comuns em formato fixo a dados complexos e altamente variáveis de propriedade intelectual. Combinando as informações fornecidas por esses mecanismos de classificação de objetos, o McAfee DLP Discover consegue gerar uma classificação multivetorial altamente precisa, que é usada para filtrar e controlar informações confidenciais e executar pesquisas que identificam riscos ocultos ou desconhecidos. Os mecanismos de classificação de objetos incluem:

- **Classificação em várias camadas:** abrange conteúdo e informações contextuais em formato hierárquico.
- **Registro de documentos:** gera assinaturas das informações conforme estas mudam.
- **Análise gramatical:** detecta a gramática ou a sintaxe de qualquer item, de documentos de texto e planilhas a código-fonte.
- **Análise estatística:** controla quantas vezes uma assinatura, padrão ou palavra-chave ocorreu em um determinado documento ou arquivo.
- **Classificação de arquivos:** identifica os tipos de conteúdo independentemente da extensão ou da compactação aplicadas ao arquivo.
- **Classificação de documentos:** as regras de descoberta para CIFS, Box e SharePoint agora suportam a reação “Classificar arquivo como”. Essa reação inclui a identificação de classificação nos formatos de arquivos compatíveis com classificações incorporadas.

1. Integrado com o DLP Discover — não é necessário um servidor separado. Um recurso complementar à sku do McAfee Total Protection for DLP.

### Especificações de software

O McAfee DLP Discover está disponível em uma versão apenas em software. Seguem abaixo os requisitos mínimos de sistema.

#### Requisitos de hardware

- CPU: Intel Core 2 de 64 bits
- RAM: mínimo de 4 GB
- Espaço em disco: mínimo de 100 GB

#### Plataformas compatíveis

- Microsoft Windows Server 2008 R2 Standard de 64 bits
- Microsoft Windows Server 2012 Standard de 64 bits
- Microsoft Windows Server 2012 R2 Standard de 64 bits
- Microsoft Windows Server 2016 Standard de 64 bits

#### Sistemas de virtualização compatíveis

- VMware vSphere utilizando servidor vCenter, versões 6.0, 6.5 ou 6.7
- vCenter Server 5.0 atualização 2

#### Software McAfee ePO e agentes

- McAfee ePO 5.3.3, 5.9.1 e 5.10
- McAfee Agent 5.0.6, 5.5, 5.5.1



Av. Nações Unidas, 8.501 – 16º andar  
Pinheiros – São Paulo – SP  
CEP 05425-070 Brasil  
+(11) 3711-8200  
[www.mcafee.com/br](http://www.mcafee.com/br)

McAfee e o logotipo da McAfee, ePolicy Orchestrator e McAfee ePO são marcas comerciais ou marcas registradas da McAfee, LLC ou de suas afiliadas nos EUA e em outros países. Outros nomes e marcas podem ser propriedade de terceiros. Copyright © 2019 McAfee, LLC. 4182\_0219 FEVEREIRO DE 2019