

# Advanced Data Loss Prevention (DLP)

## para o Acronis Cyber Protect Cloud

### Programa de acesso antecipado

#### Aproveite uma solução de DLP desenvolvida para MSPs com criação de políticas automática e específica para cada cliente

Considerando-se que 72% dos funcionários compartilham informações confidenciais da empresa, não surpreende que o Ponemon Institute tenha descoberto que incidentes relacionados a elementos internos representam 45% de todas as violações. Contudo, as soluções tradicionais de DLP que remediem esses riscos exigem amplos e caros conhecimentos sobre segurança em seu provisionamento e operação – as políticas de DLP não são universais, mas específicas de cada empresa, o que torna sua

configuração um processo demorado, manual e caro que envolve aprender as necessidades específicas da empresa do cliente e mapear manualmente essas necessidades com as políticas de DLP correspondentes.

O Acronis Advanced DLP capacita você com uma simplicidade inigualável no provisionamento e no gerenciamento, evitando vazamentos de dados das workloads dos clientes através de dispositivos periféricos e comunicações de rede. Com geração de políticas de DLP básicas e automáticas, você pode criar políticas específicas para a empresa de cada cliente de maneira precisa e eficiente.

### Incremente sua linha de serviços com uma prevenção de perda de dados simplificada

CONTROLES DE DLP SENSÍVEIS AO CONTEXTO E AO CONTEÚDO	GERAÇÃO AUTOMÁTICA DE POLÍTICAS DE DLP BÁSICAS E ESPECÍFICAS PARA CADA CLIENTE	IMPOSIÇÃO ADAPTÁVEL DE POLÍTICAS DE DLP
Proteja os dados confidenciais dos clientes evitando vazamentos de dados de workloads através de dispositivos periféricos e comunicações de rede analisando o conteúdo e o contexto das transferências de dados e impondo controles preventivos com base em políticas.	Pare de se aprofundar nos detalhes dos negócios dos clientes e de definir políticas manualmente. Políticas básicas de DLP específicas da empresa são criadas automaticamente por meio do monitoramento de fluxos de saída de dados confidenciais. Os clientes podem validar essas políticas antes que o sistema as imponha.	Elimine o trabalho manual normalmente necessário para gerenciar e ajustar uma política de DLP após a imposição inicial. Uma opção adaptável de imposição de política expande automaticamente a política imposta com base em fluxos de dados novos e anteriormente não utilizados detectados nas workloads dos clientes.

#### Revele novas oportunidades de lucro

- **Aumente a sua receita por cliente** com serviços altamente solicitados de DLP gerenciados pelo MSP
- **Atraia mais clientes** demonstrando o valor dos seus serviços com um modo de observação que aumenta a conscientização dos clientes quanto à DLP
- **Controle o seu custo total de propriedade (TCO) e viabilize margens melhores** com uma estratificação de serviços mais fácil utilizando uma plataforma integrada e única para backup e recuperação de desastres, antimalware de última geração, segurança de e-mail, gerenciamento de workloads e DLP

#### Aumente a sua produtividade e evite o descontrole dos custos

- **Reduza o tempo gasto em provisionamento e configuração** com criação automatizada de políticas básicas de DLP específicas para cada cliente
- **Alinhe as políticas de DLP com os requisitos da empresa e minimize erros** com justificativa opcional de transferências de dados confidenciais pelos usuários finais durante a criação da política básica e validação fácil pelo cliente, antes da imposição da política
- **Simplifique os relatórios de conformidade e aumente a visibilidade do desempenho da DLP** por meio de widgets informativos, alertas e coleta de logs configurável

#### Reduza os riscos de vazamento de dados para os clientes

- **Minimize os riscos de violações de dados relacionados a elementos internos dos clientes** evitando o vazamento de informações confidenciais em dispositivos periféricos e comunicações de rede
- **Minimize o impacto de erros humanos e imponha políticas de uso aceitável** dos dados no âmbito da empresa
- **Reforce a conformidade regulatória dos clientes** protegendo dados sujeitos a regulamentações

## Diferencie seus serviços de DLP tendo vantagens em relação à concorrência

GERAÇÃO DE POLÍTICAS DE DLP AUTOMATIZADA	POLÍTICAS DE DLP ESPECÍFICAS PARA CADA CLIENTE	MATRIZ INCOMPARÁVEL DE CANAIS CONTROLADOS	CONTROLES ABRANGENTES DE DLP	PROTEÇÃO CIBERNÉTICA CENTRALIZADA POR MEIO DE UM CONSOLE ÚNICO
Minimize o trabalho manual e o risco de erros. Simplifique o provisionamento gerando automaticamente uma política de DLP básica para cada cliente.	Monitore os fluxos de dados de confidências para fora da organização mapeando automaticamente os processos corporativos do cliente com uma política de DLP ajustada especificamente. Aproveite uma assistência opcional ao usuário final para uma precisão maior e solicite a validação do cliente antes de impor uma política.	Controle fluxos de dados por canais de rede e locais, incluindo armazenamentos removíveis, impressoras, área de transferência e unidades mapeadas redirecionadas, e-mails e webmails, mensagens instantâneas, serviços de compartilhamento de arquivos, redes sociais e protocolos de rede.	Assegure um controle independente do navegador em transferências de dados para mídias sociais, webmail e serviços de compartilhamento de arquivos. Aproveite a inspeção de conteúdo das mensagens instantâneas enviadas para fora e detecção de dados confidenciais dentro de imagens em computadores remotos e desconectados.	Controle o seu custo total de propriedade (TCO), reduza a sobrecarga de gerenciamento e aumente as margens utilizando uma única solução que integra backup, recuperação de desastres, antimalware de nova geração, segurança de e-mail, gerenciamento de workloads e DLP.

### Simplifique o provisionamento de clientes e a geração e o gerenciamento de políticas de DLP

Para ajudar os MSPs a simplificar suas tarefas de provisionamento e gerenciamento, o Advanced Data Loss Prevention (DLP) atua em dois modos diferentes:

#### Modo de observação

Provisione serviços de DLP facilmente eliminando a complexidade da criação inicial de políticas. No modo de observação, o agente monitora os fluxos de saída de dados confidenciais dos computadores de endpoint dos clientes para gerar a política de DLP básica automaticamente ou, opcionalmente, com justificativa, pelo usuário final, das transferências de dados mais arriscadas.

#### Modo de imposição

Uma vez que a política de DLP tenha sido validada pelos clientes, você pode impô-la para começar a proteger seus dados. O modo de imposição permite determinar como impor políticas de DLP:

- **Imposição rigorosa** – impõe a política de DLP conforme esta foi definida, sem complementá-la com novas regras de fluxo de dados. Qualquer transferência de dados que não corresponda a uma regra de fluxo de dados definida na política é bloqueada, a não ser que o usuário final solicite uma exceção não recorrente, relacionada a dados corporativos, para ativar uma exceção de bloqueio.
- **Imposição adaptável** – impõe a política de DLP, mas proporciona flexibilidade ao estendê-la com novas regras para permitir fluxos de dados corporativos não observados anteriormente.

