McAfee DLP Prevent

Imponha o cumprimento de políticas para proteger suas informações confidenciais

Quanto mais pessoas compartilham informações eletronicamente, maior é a probabilidade de que alguém, acidental ou intencionalmente, envie dados confidenciais para um indivíduo não autorizado, colocando em risco a confidencialidade dos dados corporativos. As informações podem sair da empresa por muitos canais diferentes: e-mail, Web, mensagens instantâneas ou FTP. Algumas mensagens ou transações são permissíveis, mas devem ser criptografadas para garantir a privacidade dos dados. Outros tipos de comunicação são simplesmente inaceitáveis a qualquer momento e devem ser bloqueados. A imposição das políticas corretas no momento adequado é essencial para garantir a segurança dos dados, a conformidade regulatória e a proteção da propriedade intelectual.

Principais vantagens

Aproveite a infraestrutura existente

- Proteja o e-mail corporativo por meio da integração com gateways MTA usando SMTP com cabeçalhos X-Header para bloqueio, devolução, criptografia, quarentena e redirecionamento
- Garanta a imposição das políticas de tráfego por meio da integração com proxies da Web compatíveis com ICAP para bloquear violações de conteúdo em HTTP, HTTPS, mensagens instantâneas, FTP e webmail

Imponha proativamente o cumprimento das políticas para todos os tipos de informações

- Proteja mais de 300 tipos específicos de conteúdo
- Imponha políticas para informações reconhecidamente confidenciais e também para informações não tão óbvias que você talvez desconheça
- Dimensione o sistema para oferecer suporte a centenas de milhares de conexões simultâneas

Classifique, analise e corrija vazamentos de dados

- Filtre e controle as informações confidenciais para protegê-las contra riscos conhecidos e desconhecidos
- Indexe e imponha políticas de segurança detalhadas para todos os tipos de conteúdo
- Aplique políticas relativas ao acesso a compartilhamentos de arquivos internos para impedir o acesso não autorizado dos usuários a informações ou repositórios

Imposição de políticas de segurança para dados em trânsito

Em todos os departamentos de qualquer empresa, os funcionários compartilham dados usando vários aplicativos e uma ampla variedade de protocolos. Proteja-se contra a perda de dados acidental ou intencional, impedindo proativamente que os dados confidenciais saiam da rede e impondo processos corretos de negócios.

O McAfee® Data Loss Prevention (DLP) Prevent ajuda você a impor políticas aplicáveis às informações que saem da rede por e-mail, webmail, mensagens instantâneas, wikis, blogs, portais, HTTP/HTTPS e transferências via FTP, por meio da integração com gateways de agentes de transferência de mensagens (MTA) usando o Simple Mail Transfer Protocol (SMTP) ou proxies da Web compatíveis com ICAP. Quando encontra uma violação de política, o McAfee DLP Prevent permite que você adote uma ampla variedade de ações, que incluem, entre outras, criptografia, bloqueio, redirecionamento e colocação em quarentena, de modo a garantir a conformidade com as normas que governam a privacidade das informações confidenciais e reduzir o risco das ameaças à segurança.

Integração com proxies da Web e MTAs para maior proteção

O McAfee DLP Prevent integra-se a proxies da Web (usando ICAP) e a MTAs (usando cabeçalhos X-Header) para a ação exigida. Ao encerrar as transações não autorizadas na camada do aplicativo em vez de simplesmente descartar a sessão TCP, o que não teria qualquer efeito sobre o comportamento do aplicativo, o McAfee DLP Prevent alerta o aplicativo iniciador de que a transmissão foi negada devido a uma violação de política. Isso reforça a proteção dos dados da sua organização, porque o McAfee DLP Prevent aprende o que deve ser protegido e impede que o aplicativo tente novamente o mesmo comportamento.

Proteção para informações confidenciais conhecidas e desconhecidas

Com a capacidade de classificar mais de 300 tipos de conteúdo diferentes, o McAfee DLP Prevent ajuda você a garantir a segurança das informações confidenciais conhecidas — números de CPF e de cartão de crédito, dados financeiros — e aprende quais informações ou documentos requerem proteção, como dados altamente complexos de propriedade intelectual. O McAfee DLP Prevent inclui uma ampla gama de políticas integradas,

intel Security

Especificações

Taxa de transferência do sistema
Até 150 Mbps de taxa de transferência para análise de conteúdo integral, indexação e armazenamento

Integração à rede
Integra-se à rede como um appliance fora do caminho que permanece ativo no caminho de dados usando MTAs e proxies da Web compatíveis com ICAP

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

- Documentos do Microsoft Office
- Arquivos de multimídia
- P2P
- Código-fonte
- Arquivos de projeto
- Arquivos compactados
- Arquivos criptografados

Compatibilidade com protocolos
Compatível com os protocolos HTTP, HTTPS, FTP e de mensagens instantâneas por meio do protocolo ICAP para um proxy compatível com ICAP. Consulte o fornecedor do seu proxy para determinar com quais protocolos ele é compatível. Compatível com SMTP por meio da integração com MTAs.

Políticas integradas

- Fornece uma ampla gama de políticas e regras integradas para requisitos comuns, incluindo conformidade regulatória, propriedade intelectual e uso aceitável
- Permite total personalização das regras para atender às necessidades específicas da empresa, aproveitando o banco de dados de captura da McAfee

variando de conformidade e uso aceitável a propriedade intelectual, o que lhe permite detectar correspondências totais ou parciais de documentos com um conjunto abrangente de regras, de modo a proteger todas as suas informações confidenciais, tanto conhecidas como desconhecidas.

Relatórios de incidentes e visualizações personalizáveis

Usando o console de gerenciamento do McAfee® ePolicy Orchestrator® (McAfee ePO™), você pode personalizar visualizações resumidas de incidentes de segurança e ações subsequentes com base em dois pontos de articulação contextual quaisquer. Exibições de lista e de detalhes, bem como exibições resumidas com análise de tendências, estão disponíveis imediatamente. O McAfee DLP Prevent também inclui um grande número de relatórios predefinidos, cada um dos quais pode ser exibido, salvo para uso posterior ou programado para entrega periódica.

Classificação de dados complexos

O McAfee DLP Prevent 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 esses mecanismos de classificação de objetos, o McAfee DLP Prevent coloca em prática um sistema de classificação altamente preciso e detalhado que bloqueia informações confidenciais e identifica riscos ocultos ou desconhecidos. Os mecanismos de classificação de objetos incluem:

- **Classificação em várias camadas —** Abrange informações contextuais e conteúdo em formato hierárquico.
- **Registro de documentos —** Inclui assinaturas biométricas das informações conforme elas 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 correspondência biométrica, gramatical ou de assinatura ocorreu em um determinado documento ou arquivo.
- **Classificação de arquivos** — Identifica os tipos de conteúdo independentemente da extensão ou da compactação aplicadas ao arquivo.

Especificações: appliance McAfee DLP 5500

Componente	Requisito
Processador	2x Intel E5-2620, 6 núcleos, 15 M de cache, 2 GHz, 7,20 GT/s Intel QPI
Memória	32 GB DDR3-1333 MHz
Fonte de alimentação	2 módulos de fonte de alimentação hot-swap de 760 W
Unidades de disco rígido	8 unidades SATA de 2 TB e 7.200 rpm
Placa de rede	Módulo de E/S Ethernet Intel Dual Copper 1 Gbps
IPMI	Módulos Intel Remote Management 4 (AXXRMM4)
Dimensões do produto	2 unidades de rack (2U)

Especificações: máquina virtual

O McAfee DLP Prevent está disponível como um appliance virtual que pode ser executado em ambientes VMware. São fornecidos a seguir os requisitos mínimos de hardware para execução do appliance virtual.

Componente	Requisito
Processador	Intel x86 4x vCPU
Memória	16 GB de RAM
Unidade(s) de disco rígido	Unidade 1: tamanho mínimo de 100 GB para software de máquina virtual Unidade 2: tamanho mínimo de 512 GB para imagem virtual DLP
Portas de rede	4 interfaces de rede virtuais
BIOS	Ativar thread VT

McAfee. Part of Intel Security.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com