



McAfee Data Loss Prevention Endpoint

Não seja a próxima estatística de perda de dados

Você está perdendo dados sem perceber? Suas informações de clientes, propriedade intelectual, dados financeiros e arquivos de pessoal podem estar deixando seus limites corporativos neste exato momento. E os perpetradores não são somente hackers — são também seus próprios funcionários. A perda de dados acidental ou intencional pode ocorrer por meio de canais comuns, como e-mail, publicações na Web, unidades USB e uploads para a nuvem, podendo acarretar custos milionários.

Todos os dias, empresas sofrem perdas de dados maciças resultantes do vazamento acidental ou malicioso de informações. Os custos das violações de dados e correções são extremamente altos. Segundo o mais recente *Cost of Data Breach Study* (Estudo do custo de uma violação de dados) do Ponemon Institute¹, o custo médio de cada registro roubado ou perdido que contém informações confidenciais ou sigilosas é de US\$ 201 e o custo médio total pago pelas organizações é de US\$ 5,9 milhões. E se você pudesse eliminar a perda de dados de maneira fácil e eficaz? E se você pudesse alcançar a conformidade normativa e do setor, protegendo a propriedade intelectual ao mesmo tempo? Agora você pode — com o abrangente McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint).

Prevenção de vazamentos em tempo real

Com o McAfee DLP Endpoint, é fácil e rápido monitorar atividades do usuário final em tempo real e aplicar políticas de segurança de gerenciamento centralizado para regular e restringir a maneira como os dados confidenciais são transferidos, sem afetar a produtividade. O McAfee DLP Endpoint, integrado com o McAfee Threat Intelligence Exchange e o McAfee Data Exchange Layer, comunica-se com este último e bloqueia os dados confidenciais nos aplicativos identificados como maliciosos ou aplica políticas de segurança mais rigorosas a endpoints não confiáveis.

Conectado à sua infraestrutura de segurança como um todo, o McAfee DLP Endpoint pode oferecer respostas instantâneas a ameaças persistentes avançadas (APTs) e impedir que os dados vazem.

Capacidades avançadas de proteção

O McAfee DLP Endpoint oferece proteção abrangente para todos os possíveis canais de vazamento, incluindo dispositivos de armazenamento removíveis, a nuvem, e-mail, mensagens instantâneas, Web, impressão, área de transferência, captura de telas, aplicativos de compartilhamento de arquivos e muito mais.

Eis alguns recursos importantes:

- **Novidade!** Classificação manual — Dá aos usuários finais o poder de classificar documentos manualmente, aumenta a conscientização dos funcionários quanto à proteção dos dados e reduz o trabalho administrativo.
- **Novidade!** Varreduras e correções iniciadas pelo usuário — Permitem que os usuários finais executem varreduras de descoberta de endpoints e realizem ações de autocorreção.
- **Novidade!** Suporte aprimorado para Mac OS — Aumenta a proteção com reconhecimento de conteúdo para Mac OS em armazenamento removível, acesso a arquivos de aplicativos e compartilhamentos de rede.

Principais vantagens

- **Prevenção de vazamentos em tempo real:** integração com o McAfee Threat Intelligence Exchange e o McAfee Data Exchange Layer para visibilidade e monitoramento em tempo real
- **Capacidades avançadas de proteção:** aproveite impressões digitais, classificação e marcação de arquivos para proteger dados confidenciais e desestruturados, como propriedade intelectual e segredos comerciais
- **Gerenciamento centralizado:** integração nativa com o software McAfee® ePolicy Orchestrator® (McAfee ePO™) para simplificar o gerenciamento de políticas e incidentes
- **Cumprimento de conformidade:** garanta conformidade lidando com ações cotidianas dos usuários finais, como envio de e-mails, postagens na nuvem, download para dispositivos de mídia removível e muito mais
- **Conscientização do usuário final:** feedback em tempo real via pop-ups educativos ajudam a promover uma conscientização e uma cultura de segurança corporativa

Plataformas compatíveis

- Windows 7 SP1 ou posterior, edições Enterprise e Business (32 e 64 bits)
- Windows 8 e 8.1 ou posterior, Enterprise e Professional, 32 e 64 bits
- Windows Server 2008 R2 e 2008 SP2 ou posterior, 32 e 64 bits
- Windows Server 2012 e 2012 R2 ou posterior, 64 bits
- Mac OS X Mountain Lion 10.8.5
- Mac OS X Mavericks 10.9.5
- Mac OS X Yosemite 10.10

Navegadores compatíveis

- Internet Explorer, versões de 8 a 11
- Mozilla Firefox 34 ou superior
- Google Chrome 31 ou superior

Software McAfee ePO e agentes

- Software McAfee ePO 4.6.9 e 5.1.1
- McAfee Agent for Windows 4.8 Patch 2 e 5.0
- McAfee Agent for Mac 4.6 Patch 3, 4.8 Patch 2 e 5.0

- **Novidade!** Sem reinicializar — Aumenta a eficiência administrativa ao não exigir reinicialização para atualizar para o McAfee DLP Endpoint 10.0 ou superior.
- Classificação flexível, incluindo dicionários, expressões regulares e algoritmos de validação, documentos registrados e suporte para soluções de terceiros para a classificação de usuários finais.
- Tecnologia exclusiva de marcação para identificar documentos de acordo com sua origem. Evite que informações confidenciais de aplicativos Web, aplicativos de rede e compartilhamentos de rede sejam duplicadas, renomeadas ou saiam dos limites da corporação.
- Suporte aprimorado à virtualização para proteger desktops remotos e soluções VDI.

Gerenciamento centralizado

Agora com integração nativa com o software McAfee® ePolicy Orchestrator® (McAfee ePO™), o McAfee DLP Endpoint pode ser distribuído de forma centralizada e administrado facilmente. A interface de gerenciamento completamente redesenhada do McAfee DLP Endpoint oferece conjuntos de regras versáteis e reutilizáveis, com granularidade aprimorada e experiência do usuário melhorada.

Eis alguns recursos importantes:

- Com a integração nativa com o software McAfee ePO, o McAfee DLP Endpoint não precisa mais que um controle ActiveX do Internet Explorer seja instalado para fins de administração.
- Múltiplas políticas e conjuntos de regras reutilizáveis oferecem a capacidade de definir múltiplas políticas de DLP por toda a organização, criar políticas conforme o escritório, departamento, regulamento e muito mais.

- Granularidades aprimoradas no gerenciamento de incidentes permitem consultar/filtrar/visualizar segundo qualquer propriedade de incidente (por exemplo, número de série do dispositivo, nome do arquivo de evidência e grupos).
- Capacidades centralizadas de auditoria e monitoramento de eventos.
- Controle de acesso com base em funções (também conhecido como separação de tarefas) aprimorado para gerenciamento de políticas, bem como análise de incidentes.
- Acesso à interface de atendimento.

Imposição de conformidade e conscientização do usuário final

Com o desaparecimento do perímetro corporativo, está ficando cada vez mais difícil para as empresas impor conformidade. O McAfee DLP Endpoint não apenas ajuda a monitorar comportamentos cotidianos dos usuários, como também pode assegurar conformidade ao promover a conscientização dos usuários. Com o clique de um botão, o software McAfee DLP Endpoint oferece relatórios detalhados para comprovar aos auditores, gerência sênior e outras partes interessadas que as medidas de conformidade regulatória e interna estão em vigor. Ele oferece políticas prontas para regulamentos e casos de uso, tornando fácil para você permanecer em conformidade. Seus usuários também obtêm feedback em tempo real via pop-ups de imposição com base na sua política corporativa e essas oportunidades educacionais de fácil assimilação ajudam a consolidar uma cultura de segurança corporativa mais forte.

Saiba mais

Para obter mais informações, visite www.mcafee.com/br/products/dlp-endpoint.aspx.



McAfee. Part of Intel Security.

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

1. 2014 Cost of Data Breach Study: United States (Estudo sobre o custo de violações de dados em 2014 nos Estados Unidos); Ponemon Institute, setembro de 2014