McAfee Enterprise Log Manager

Reduza os custos da conformidade com gerenciamento, armazenamento e coleta de logs de forma automatizada

Com a coleta e armazenamento adequados de logs, você reduzirá o custo da conformidade proporcionando uma trilha de auditoria clara para atividades que não podem ser repudiadas. O McAfee® Enterprise Log Manager coleta, compacta e armazena com eficiência todos os arquivos de log. Sua integração com o McAfee Enterprise Security Manager proporciona pesquisas avançadas, análise, correlação, envio de alertas e geração de relatórios. Todos os eventos e alertas proporcionam acesso fácil, com um único clique, ao registro de log original, para que o seu trabalho de perícia também seja beneficiado.

Caso se trate de um arquivo de log, o McAfee Enterprise Log Manager o coleta, assina e armazena. A McAfee automatiza o gerenciamento e a análise de logs de todos os tipos, inclusive logs de eventos, logs de banco de dados, logs de aplicativos e logs de sistema do Microsoft Windows. Os logs são assinados e validados, garantindo sua autenticidade e integridade: o que é fundamental para a conformidade regulatória. Os conjuntos de regras de conformidade e relatórios prontos para uso facilitam a comprovação de que sua empresa está em conformidade e que as políticas estão sendo cumpridas.

Com o uso desse ambiente bem integrado de coleta, gerenciamento e análise de logs, seu perfil de segurança será fortalecido e sua capacidade de cumprir normas, como PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, e SOX, será consideravelmente melhorada.

Gerenciamento inteligente de logs

O McAfee Enterprise Log Manager coleta logs de forma inteligente, armazenando os logs corretos para conformidade e avaliando e analisando os logs certos para segurança. É possível manter os logs no formato original por quanto tempo for necessário, a fim de atender às suas necessidades específicas de conformidade. Como a McAfee não altera os arquivos de log originais, ela apoia as iniciativas de cadeia de custódia e não repúdio.

As necessidades de retenção de informações variam de acordo com a origem do log e as diversas exigências de conformidade que devem ser atendidas. O McAfee Enterprise Log Manager utiliza pools de armazenamento que podem ser personalizados facilmente, para garantir que seus logs sejam armazenados de forma

Principais vantagens

- Coleta e retenção universais de logs para atender exigências de conformidade
- Armazenamento e retenção flexíveis, adequados para cada origem de log
- Compatível com cadeia de custódia e perícia
- Análise e pesquisa de logs
- Armazenamento de logs local ou por meio de uma rede de área de armazenamento gerenciada
- Integração total com o McAfee® Enterprise Security Manager
- Opções de entrega híbridas e flexíveis incluem appliances físicos e virtuais

correta e pelo tempo certo. Escolha a melhor opção de armazenamento para as suas necessidades: armazenamento em disco rígido nos appliances e placas FC (Fiber Channel) opcionais para redes de área de armazenamento de alta velocidade (SANs).

Os arquivos de log, por si sós, não nos dão todas as informações necessárias. Eles contêm indícios essenciais e são um elo fundamental para estabelecer a cadeia de custódia, mas também levantam importantes questões de segurança. Por exemplo, vamos supor que possamos ver o nome de usuário no log de acesso, mas não haja informações sobre a função ou os privilégios daquele usuário. Também podemos saber qual sistema foi acessado, mas talvez não tenhamos conhecimento sobre os tipos de informações utilizadas por esse sistema ou sobre quem deveria acessá-las.

Integração com o McAfee Enterprise Security Manager

O McAfee Enterprise Log Manager é um componente integrado e opcional do McAfee Enterprise Security Manager. Enquanto o McAfee Enterprise Log Manager armazena os logs, o McAfee Enterprise Security Manager pode avaliar, normalizar e analisar a fundo as informações dos logs, disponibilizando-as imediatamente para as investigações de segurança e respostas a incidentes em tempo real.

Quando um evento de segurança é gerado, os arquivos de evento analisados são vinculados diretamente ao arquivo de log de origem e ao registro de log específico, possibilitando acesso com um único clique durante os processos de gerenciamento de eventos e perícia. Não há necessidade de realizar outras etapas, iniciar aplicativos adicionais ou perder tempo pesquisando os logs manualmente.

Amplo contexto para análise

Juntos, o McAfee Enterprise Security Manager e o McAfee Enterprise Log Manager oferecem contexto sobre todo e qualquer log, aumentando o valor de cada log analisado. Algumas dessas informações são:

- O endereço IP de origem ou destino
- Contexto de identidade
- O nome do host ou serviço que está sendo usado
- Informações sobre vulnerabilidades de um mecanismo de varredura de avaliação de vulnerabilidade
- Informações sobre a topologia da rede
- Informações sobre políticas e privacidade

Pools de armazenamento flexíveis

Os pools de armazenamento do McAfee Enterprise Log Manager conferem mais flexibilidade ao modo como os logs são mantidos a longo prazo. Pools de armazenamento são grupos virtuais de armazenamento utilizável que podem ser distribuídos em diversos grupos de dispositivos de armazenamento físico (armazenamento local, NFS, SAN, CIF e outros) para atender diversas necessidades de gerenciamento de logs.

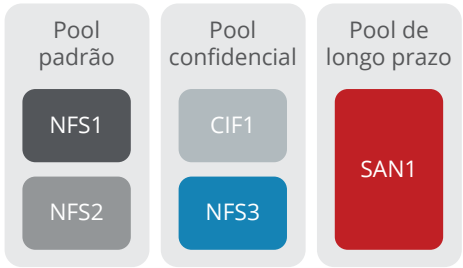

Figura 1. Pools de armazenamento flexíveis oferecem retenção de logs personalizada.

Um pool de armazenamento pode ser composto por uma série de dispositivos e os dados podem ser atribuídos a um pool específico com base no dispositivo de origem, para que os logs sejam armazenados em locais separados de acordo com sua relevância em termos de segurança, conformidade, confidencialidade ou outros critérios. Por exemplo, é possível armazenar os logs importantes para a conformidade em um pool composto por diversos dispositivos de armazenamento em rede redundantes. Os logs menos importantes podem ser armazenados em sistemas menos redundantes; e os logs mais úteis para a perícia podem ser armazenados localmente para uma análise mais rápida.

Distribuição rápida

O McAfee Enterprise Log Manager e o McAfee Enterprise Security Manager podem ser distribuídos conjuntamente utilizando-se um único appliance combinado ou podem ser distribuídos horizontal e hierarquicamente para serem compatíveis até mesmo com as maiores redes corporativas. Opções de distribuição flexíveis e híbridas, incluindo appliances físicos e virtuais.

Integração com sua infraestrutura

Embora a maioria das soluções de gerenciamento de logs funcionem isoladamente, o McAfee Enterprise Log Manager trabalha em conjunto com outros sistemas de segurança da informação. Ele se liga ao restante da infraestrutura de segurança por meio do McAfee Enterprise Security Manager para simplificar as operações de segurança, melhorar a eficiência geral e reduzir custos. Você pode integrar o gerenciamento inteligente de logs com análise eficiente, inspeção de rede, monitoramento de eventos do banco de dados e muito mais.

Saiba mais

Para obter mais informações, visite **www.mcafee.com/br/products/siem/index.aspx**.

McAfee
Together is power.

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