McAfee Enterprise Security Manager

Priorizar. Investigar. Responder.

A segurança mais eficaz começa com visibilidade sobre toda atividade em sistemas, redes, bancos de dados e aplicativos. O gerenciamento de eventos e informações de segurança (SIEM) é a base de uma estrutura de segurança eficaz. O McAfee® Enterprise Security Manager, núcleo da solução de SIEM da McAfee, oferece desempenho, inteligência decisiva e integração de soluções na velocidade e na escala necessárias para as organizações de segurança. Ele permite priorizar, investigar e responder a ameaças ocultas com rapidez e cumprir requisitos de conformidade.

O McAfee Enterprise Security Manager oferece uma compreensão em tempo real do mundo exterior (dados sobre ameaças e informações de reputação), bem como uma visão dos sistemas, dados, riscos e atividades dentro da sua empresa. Ele oferece à sua equipe de segurança acesso correlacionado e total ao conteúdo e ao contexto necessários para decisões rápidas com base em risco, para que você possa investir recursos da maneira mais eficaz em um cenário de ameaças e operacional dinâmico. Isso é fundamental na investigação de ataques sub-reptícios e graduais, na busca por indicadores de comprometimento ou na correção de problemas revelados por auditorias. Para que o gerenciamento de ameaças e de conformidade seja parte das operações de segurança, o McAfee Enterprise Security Manager também oferece ferramentas integradas para gerenciamento de alterações e configurações, gerenciamento de casos e gerenciamento centralizado de políticas — tudo o que você precisa para aprimorar o fluxo de trabalho e a eficiência da equipe de operações de segurança. Além disso, pacotes de conteúdo disponíveis para o McAfee Enterprise Security Manager oferecem configurações predefinidas para casos de uso avançados que ajudam a simplificar as operações de segurança.

Dimensionado para nível corporativo

As equipes de operações de segurança exigem, cada vez mais, uma eficiência maior ao coletar e explorar rapidamente volumes crescentes de dados brutos e analisados das arquiteturas corporativas dinâmicas e distribuídas de hoje em dia. Para superar esse desafio, o McAfee Enterprise Security Manager utiliza um sistema de gerenciamento de dados (reconhecido por clientes e analistas do setor como a força motriz das soluções de SIEM da McAfee) criado especificamente para processamento de grandes

Principais vantagens

- **Inteligente:** análises avançadas e contextos detalhados ajudam você a detectar e priorizar ameaças
- **Decisivo:** os dados de que você precisa são apresentados em visualizações dinâmicas que incluem a opção de realizar ações para investigação, contenção, correção e adaptação a importantes alertas e padrões
- **Integrado:** monitora e analisa dados de uma infraestrutura de segurança ampla e heterogênea e oferece integração de mão dupla por meio de interfaces abertas. Ele também possibilita que muitas ações de resposta emergencial sejam automatizadas

volumes de dados. Além disso, uma arquitetura de dados altamente expansível viabiliza o consumo, o gerenciamento e a análise de dados para prevenir comprometimentos em coleta, pesquisa e retenção de dados. Tais comprometimentos podem prejudicar as investigações quando dados críticos não estão disponíveis posteriormente, quando a resposta às consultas retarda a análise ou quando, por questão de desempenho, somente pesquisas parciais são possíveis.

Fatos críticos em minutos, em vez de horas

O acesso rápido a armazenamento de longo prazo de dados de eventos é fundamental para investigar incidentes, buscar indícios de ataques avançados ou tentar remediar uma auditoria de conformidade falha — situações que exigem visibilidade sobre dados históricos e acesso total a todos os detalhes de cada evento específico.

Appliances meticulosamente ajustados podem coletar, processar e correlacionar eventos de logs de vários anos com outros fluxos de dados, incluindo canais com informações sobre ameaças baseados em STIX, na velocidade que você precisar. O McAfee Enterprise Security Manager é capaz de armazenar bilhões de eventos e fluxos, mantendo todas as informações disponíveis para conformidade, validação de regras, análise forense e consultas pontuais imediatas.

Conscientização quanto a contexto e conteúdo

Quando informações contextuais estão disponíveis — incluindo dados sobre ameaças e informações de reputação, sistemas de gerenciamento de acesso e identidade, soluções de privacidade ou outros sistemas compatíveis — cada evento é enriquecido com esse contexto. Esse enriquecimento proporciona uma compreensão melhor e uma triagem mais precisa com base em como eventos de rede e segurança se correlacionam com políticas e processos corporativos reais e atributos de ativos.

A expansibilidade e o desempenho do McAfee Enterprise Security Manager permitem a coleta de mais informações de mais fontes, incluindo conteúdo de aplicativos, como documentos, transações e comunicações, agregando profundo valor forense. Essas informações são altamente indexadas, normalizadas e correlacionadas para detectar uma gama mais ampla de riscos e ameaças.

Interpretação de ameaças avançadas

Seja tráfego de rede, atividade de usuários ou utilização de aplicativos, qualquer variação em relação à atividade normal pode indicar que uma ameaça é iminente e que os seus dados ou a sua infraestrutura estão em risco. O McAfee Enterprise Security Manager calcula uma linha de base do nível de atividade para todas as informações coletadas e produz alertas priorizados com o objetivo de revelar ameaças potenciais antes que elas ocorram, enquanto analisa esses dados quanto a padrões que possam indicar uma ameaça maior. Além disso, o McAfee Enterprise Security Manager aproveita informações contextuais para enriquecer cada evento com contexto, permitindo um melhor entendimento de como os eventos de segurança podem afetar processos corporativos reais.

Os dashboards Cyber Threat Manager do McAfee Enterprise Security Manager oferecem monitoramento avançado em tempo real e compreensão de ameaças emergentes. Informações sobre ameaças suspeitas ou confirmadas, reportadas via STIX/TAXII, McAfee Advanced Threat Defense e/ou URLs de terceiros na

Web, podem ser agregadas e correlacionadas quase em tempo real ou retroativamente (utilizando o recurso de rastreamento retroativo) em relação a dados de eventos, proporcionando às equipes de segurança uma compreensão mais profunda da propagação das ameaças dentro de um ambiente. Essa inteligência permite que as organizações correlacionem os dados certos com as pessoas certas, executem ações quase em tempo real e tomem decisões mais acertadas.

Otimizar as operações de segurança

A experiência de usuário centrada na análise, proporcionada pelo McAfee Enterprise Security Manager, oferece mais flexibilidade, facilidade de personalização e tempos de resposta menores para investigações. Fluxos de trabalho simplificados permitem um gerenciamento de incidentes mais eficaz e imediato. Com acesso rápido e inteligente a informações sobre ameaças, analistas com qualquer nível de experiência — novatos ou especialistas — terão mais facilidade para priorizar, investigar e responder à evolução das ameaças.

A utilidade do McAfee Enterprise Security Manager comprova-se instantaneamente, com centenas de relatórios, visualizações, regras e alertas para uso imediato — tudo isso facilmente personalizável. Seja estabelecendo linhas de base para compreender o uso típico da rede ou simplesmente personalizando alertas, o dashboard do McAfee Enterprise Security Manager permite fácil visualização, investigação e geração de relatórios sobre as informações de segurança mais relevantes. Agora as organizações podem ter acesso abrangente e correlacionado aos dados e ao contexto necessários para tomar decisões inteligentes e rápidas.

Além disso, o McAfee Enterprise Security Manager oferece pacotes de conteúdo para simplificar as operações de segurança com casos de uso de segurança preconfigurados, "prontos para usar" e que oferecem acesso rápido a capacidades avançadas de gerenciamento de conformidade ou de ameaças. Os pacotes de conteúdo são configurações predefinidas para casos de uso de segurança comuns que proporcionam conjuntos de regras, alarmes, visualizações, relatórios, variáveis e listas de observação. Muitos pacotes de conteúdo contêm gatilhos predefinidos para comportamentos que podem demandar investigação adicional e correção automática.

Simplificar a conformidade

Ao centralizar e automatizar o monitoramento e a geração de relatórios de conformidade, o McAfee Enterprise Security Manager elimina processos manuais demorados. Além disso, a integração com a estrutura de conformidade unificada UCF (Unified Compliance Framework) possibilita uma metodologia de "coletar uma vez e cumprir muitas vezes" para satisfazer requisitos de conformidade e minimizar o trabalho e a despesa com auditoria. O suporte para UCF traz eficiências para a conformidade ao normalizar as especificidades de cada regulamento, possibilitando que o conjunto único de eventos coletados seja facilmente mapeado para regulamentos individuais.

O McAfee Enterprise Security Manager facilita e acelera o gerenciamento de conformidade com centenas de dashboards predefinidos, trilhas de auditoria abrangentes e relatórios para mais de 240 regulamentos e estruturas de controle globais, incluindo PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX e SOX.

Além de amplo suporte para uso imediato, todos os relatórios de conformidade, regras e dashboards do McAfee Enterprise Security Manager são totalmente personalizáveis.

Conexão da sua infraestrutura de TI

A integração pela sua infraestrutura de segurança proporciona um grau inigualável de visibilidade em tempo real sobre a postura de segurança de uma organização. O McAfee Enterprise Security Manager pode coletar dados valiosos de centenas de dispositivos de outros fornecedores de segurança, além de canais de informações sobre ameaças. A integração com o McAfee Global Threat Intelligence (McAfee GTI) agrega dados de mais de 100 milhões de sensores globais de ameaças do McAfee Labs, oferecendo um canal constantemente atualizado de endereços IP maliciosos conhecidos. O McAfee Enterprise Security Manager também pode assimilar informações sobre ameaças reportadas via STIX/TAXII e/ou URLs de terceiros na Web e realizar ações com base em análises.

O McAfee Enterprise Security Manager também oferece integrações ativas com dezenas de soluções complementares de análise e gerenciamento de incidentes, incluindo soluções de parceiros do McAfee Security Innovation Alliance e da McAfee.

Por exemplo, o McAfee Threat Intelligence Exchange, com base em monitoramento de endpoints, agrega ataques pouco predominantes, aproveitando inteligência global, local e de terceiros sobre ameaças.

O McAfee Threat Intelligence Exchange também pode utilizar outros produtos integrados, como o McAfee Advanced Threat Defense, para analisar e condenar ainda mais os arquivos.

Equipes de resposta a incidentes e administradores podem usar o McAfee Active Response para procurar arquivos maliciosos de dia zero em hibernação nos sistemas, bem como processos ativos na memória. O McAfee Active Response também utiliza coletores persistentes para monitorar continuamente seus endpoints quanto à presença de indicadores de comprometimento (IoCs) específicos, alertando automaticamente caso um IoC apareça em algum lugar do seu ambiente. Diferentemente de abordagens tradicionais de segurança, essa combinação oferece às organizações um fluxo de trabalho de ciclo fechado detalhado, da descoberta à contenção e à correção.

A McAfee fornece um sistema de segurança integrado que capacita você a impedir e responder a ameaças emergentes. Nós ajudamos você a neutralizar mais ameaças com mais rapidez e menos recursos. Nossa arquitetura conectada e nosso gerenciamento centralizado reduzem a complexidade e aumentam a eficiência operacional em toda a sua infraestrutura de segurança. A McAfee assumiu o compromisso de ser sua parceira de segurança número um, oferecendo um conjunto completo de recursos integrados de segurança.

Saiba mais

Para obter mais informações sobre o McAfee Enterprise Security Manager, visite **www.mcafee.com/br/products/siem/index.aspx**.

Para obter mais informações sobre soluções integradas, visite **www.mcafee.com/br/solutions/intelligent-security-operations.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