Datasheet

McAfee Vulnerability Manager

Monitoramento de ativos contínuo, de alto desempenho e em tempo real

Principais diferenciais

- Expansibilidade, precisão e flexibilidade incomparáveis
- Avaliação em tempo real de novos dispositivos no momento em que eles aparecem na rede, inventário completo de ativos de hardware e software, mapeamento de usuários para ativos e topologia de rede automática
- Combina monitoramento e descoberta de rede ativos e passivos para revelar dispositivos virtualizados, móveis e ocultos
- Auditorias profundas dos dispositivos orientam as varreduras e alimentam um banco de dados de ativos de referência
- A marcação dinâmica do sistema pode automatizar totalmente a avaliação de vulnerabilidade
- Atualizado com as últimas vulnerabilidades e ameaças pelo McAfee Global Threat Intelligence™
- Segurança elevada com base em credenciais com a integração com o Cyber-Ark
- Faz varredura em redes IPv4 e IPv6
- Geração de relatórios totalmente flexível — faz varredura nos ativos uma vez e gera relatórios deles a qualquer momento
- Os fluxos de trabalho de gerenciamento de risco automatizados podem incluir aplicativos desenvolvidos internamente, da McAfee e de terceiros

Proteja seus negócios com a solução mais flexível, comprovada e expansível do mercado — gerenciamento de vulnerabilidades abrangente de forma simples e realizado em tempo real. O McAfee® Vulnerability Manager com o recurso McAfee Asset Manager oferece expansibilidade e desempenho inigualáveis, examinando tudo na rede de forma ativa e passiva. Se um dispositivo ou ativo tem um endereço IP ou está usando sua rede, o McAfee Vulnerability Manager pode descobri-lo e avaliá-lo, automaticamente e em tempo real, revelando a conformidade de todos os ativos em sua rede.

O McAfee Vulnerability Manager define o padrão do mercado trabalhando com as realidades que definem o seu negócio, examinando todos os tipos de configurações de rede e ativos. Ele faz varreduras de forma passiva, ativa ou sem interrupções quando e onde você precisar, permitindo que você descubra, avalie, corrija e gere relatórios sobre todos os seus ativos. Você pode descobrir dispositivos ocultos em sua rede, assim como smartphones, tablets e laptops que vão e vêm entre varreduras programadas. O que você não estava vendo ou descobrindo vai surpreendê-lo — e poderia estar comprometendo sua conformidade. Milhares de organizações confiam no McAfee Vulnerability Manager para rapidamente encontrar e priorizar vulnerabilidades, com distribuições variando de algumas centenas de nós a uma varredura contínua em mais de quatro milhões de endereços IP.

Implementação fácil

A McAfee facilita a implementação da varredura confiável. O McAfee Vulnerability Manager é instalado com muita facilidade em seu hardware físico ou virtualizado — ou você pode usar os appliances reforçados da McAfee. Depois de alguns minutos, você pode iniciar sua primeira varredura.

Carregar e manter o seu inventário de ativos também é muito simples. Com o módulo McAfee Asset Manager, o banco de dados de ativos é atualizado imediatamente conforme os novos dispositivos aparecem on-line, garantindo que você saiba em tempo real quais dispositivos estão ali. Além disso, o McAfee Vulnerability Manager se integra diretamente com ferramentas de gerenciamento de ativos corporativos, incluindo LDAP, Microsoft Active Directory e a plataforma de gerenciamento McAfee® ePolicy Orchestrator® (McAfee ePO™); você pode manter um repositório central para os dados de ativos.

Obtenha visibilidade para todos os ativos

A opção McAfee Asset Manager aumenta a visibilidade por meio de descoberta e monitoramento passivos sempre ativados. Rapidamente distribuído em uma porta SPAN, esse sistema monitora o tráfego para descobrir e mapear tudo em sua rede, incluindo dispositivos não autorizados, hosts VMware esquecidos e dispositivos móveis. Conforme ele observa, ele enumera os dispositivos, os padrões e as comunicações — detalhes que ajudam a avaliar e mitigar riscos. Os detalhes dos dispositivos são automaticamente enviados ao McAfee Vulnerability Manager para avaliação imediata. Além disso, o McAfee Asset Manager pode executar um inventário completo de software e hardware em cada ativo descoberto.

Personalize varreduras conforme seus requisitos

O McAfee Vulnerability Manager oferece várias opções para ajudar você a comparar e documentar a conformidade com as regulamentações do setor. Para uma definição rápida de políticas, faça uma varredura em um sistema "padrão ouro" para estabelecer uma linha de base, aproveite modelos de conformidade fornecidos ou carregue políticas que utilizem o protocolo de automação de conteúdo de segurança (SCAP).

O McAfee Vulnerability Manager faz varredura em todos os ativos em rede, até mesmo ativos complicados, localizados em ambientes de infraestrutura crítica e isolados. Por exemplo, se você tiver redes sem uma ligação externa, pode distribuir um mecanismo de varredura virtual ou com base em laptop para descobrir e fazer varredura nesses ativos. Você tem então a opção de manter os resultados no ambiente restrito ou, se necessário, passá-los para um sistema centralizado.

Cobertura da varredura

- Faz varredura em mais de 450 variedades de sistemas operacionais, incluindo plataformas Microsoft Windows, UNIX, Cisco, Android, Linux, Apple Macintosh, Apple iOS e VMware
- Faz varredura profunda em aplicativos Web (o top 10 da OWASP e o top 25 da CWE)
- Procura vulnerabilidades e malware em software Adobe, AOL, Apple, Microsoft (Office, IIS, Exchange), Blue Coat, CA, Cisco, Citrix, Facebook, Google, HP, IBM (Lotus Notes e WebSphere), Novell, Oracle, Real Networks, RIM (BlackBerry Enterprise Server), SAP, Oracle Java, Symantec e VMware
- Faz varredura nos principais bancos de dados, incluindo DB2, MySQL, Oracle, Microsoft SQL Server e Sybase

Normas e certificações

- Inclui modelos para ASCI 33, BASEL II, BILL 198 (CSOX), BSI IT (GR), COBIT, FDCC, FISMA, GLBA, HIPAA, ISO 27002, JSOX, MITS, PCI, SOX, NIST SP 800-68, top 20 da SANS, SCAP, OVAL e muito mais
- Compatível com normas, incluindo auditorias de certificação CIS, COBIT, CPE, CVE, CVSS, DISA STIG, FDCC/SCAP, ISO17799/ISO 27002/FINRA, ITIL, NIST-SP800, NSA, OVAL e o top 20 da SANS
- Critérios comuns certificados
- Criptografia validada segundo FIPS-140-2

Especificações técnicas

Visite www.mcafee.com/br para obter os requisitos e as especificações atuais de hardware e software.

A maioria dos sistemas operacionais exige credenciais de ativos antes de revelar informações de configuração confidenciais, mas algumas equipes de segurança consideram um desafio conseguir acesso a essas credenciais. Com a integração do pacote Privileged Identity Management da Cyber-Ark, a descoberta e a varredura altamente seguras e com base em credenciais acontece de forma fácil e segura e com um excelente desempenho.

Determine o risco em minutos

Quando o McAfee Asset Manager identifica um novo sistema na sua rede, ele passa informações detalhadas sobre esse sistema para o McAfee Vulnerability Manager, para que uma varredura específica seja acionada. Em minutos, você sabe o status desse sistema e o risco que ele representa para seu ambiente.

Marque ativos para ganhar eficiência

Também é possível usar políticas de marcação para colocar novos dispositivos em grupos de varredura automaticamente, com base no perfil e risco de cada dispositivo. A varredura pode ser imediata ou parte da próxima varredura periódica, dependendo das políticas definidas.

Detecte vulnerabilidades e malware

Enquanto os outros dão apenas uma olhada superficial nas portas abertas e configurações, o McAfee Vulnerability Manager se aprofunda muito mais. Ele faz avaliações em nível de aplicativo e de sistema que incluem banners de banco de dados, configurações de políticas, chaves de registro, permissões de arquivos e unidades e serviços em execução. O produto testa mais de 450 versões de sistemas operacionais para detectar a mais ampla gama de vulnerabilidades. Nossas inspeções também detectam conteúdo malicioso, incluindo cavalos de Troia, vírus e outros malware.

É possível aumentar as verificações predefinidas e atualizações para ameaças de dia zero escrevendo verificações e scripts personalizados para testar programas próprios e legados. O McAfee Vulnerability Manager também avalia conteúdos de terceiros que seguem XCCDF, OVAL, e outras normas do SCAP.

Preste atenção especial nos aplicativos Web

O McAfee Vulnerability Manager permite que os administradores gerenciem aplicativos Web assim como fazem com os ativos tradicionais com base em rede. Os ativos de aplicativos Web podem ser agrupados e ter seu próprio nível crítico, proprietários de ativos e personalidades. Aproveitando recursos totalmente automatizados, o McAfee Vulnerability Manager faz uma varredura profunda de aplicativos Web por todo o espectro de vulnerabilidades da Web.

Mantenha-se atualizado

Milhões de sensores no mundo inteiro direcionam centenas de pesquisadores do McAfee Labs para as mais recentes mudanças no cenário de ameaças. O McAfee Global Threat Intelligence alimenta as avaliações de risco em tempo real e as recomendações sobre ameaças diretamente no McAfee Vulnerability Manager para deixar você protegido e à frente das ameaças emergentes.

Gerencie, dimensione e integre conforme o necessário

A McAfee oferece flexibilidade para você projetar suas varreduras, seus relatórios e seu gerenciamento para trabalhar da maneira que preferir. Monitore apenas os ativos locais em um mecanismo de varredura ou exiba o andamento de centenas de mecanismos de varredura remotos em um único console. Nossa arquitetura multifacetada pode ser dimensionada para atender às necessidades de organizações de qualquer porte.

O McAfee Vulnerability Manager pode integrar-se com a maioria dos aplicativos por meio de uma interface de programação de aplicativos (API) aberta.

Responda com base no risco

Uma única exibição de vulnerabilidades como base para ações reduz custos com auditoria e correções. Por exemplo, no Patch Tuesdays é possível decidir rapidamente quais máquinas podem ser afetadas por uma nova vulnerabilidade do Microsoft Windows ou da Adobe. Em minutos, sem repetir a varredura de toda a sua rede, o McAfee Vulnerability Manager prioriza e classifica o potencial de risco de novas ameaças com base em pontuações de risco e dados de configuração existentes.

Com essas informações em mãos, é possível selecionar os ativos com base no nível crítico e clicar com o botão direito para executar varreduras específicas e instantâneas.

Obtenha conformidade, tenha confiança

Evidências conclusivas — como falhas na varredura, sistemas não verificados e resultados de varreduras reais e esperados — fornecem documentação indicando que sistemas específicos não estão vulneráveis, um requisito de auditoria cada vez mais comum. Através da combinação de monitoramentos ativos e passivos, testes de penetração, varreduras autenticadas e varreduras não credenciadas, o McAfee Vulnerability Manager permite descobrir vulnerabilidades e violações de políticas com o mais alto nível de precisão. O gerenciamento de vulnerabilidades abrangente nunca foi tão simples.

McAfee
An Intel Company

McAfee do Brasil Comércio de Software Ltda.
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.mcafee.com/br