McAfee Application Data Monitor

Detecte ameaças ocultas com inspeção da camada de aplicativos

O appliance McAfee® Application Data Monitor leva a segurança e a conformidade além dos limites do gerenciamento de logs ao monitorar até a camada de aplicativos. É possível inspecionar completamente o conteúdo dos aplicativos para obter uma visibilidade com o máximo de detalhamento de como sua rede está sendo utilizada.

O appliance McAfee Application Data Monitor decodifica uma sessão de aplicativo inteira até a camada 7, oferecendo uma análise completa de tudo, desde protocolos subjacentes e integridade da sessão até o conteúdo do aplicativo em si (como o texto de um e-mail ou seus anexos). Esse nível de detalhamento possibilita uma análise precisa do uso real do aplicativo, ao mesmo tempo que permite cumprir as políticas de uso de aplicativos e detectar tráfego malicioso e oculto.

Essa inspeção detalhada é compatível com a conformidade, rastreando todo o uso de dados confidenciais na rede. Quando o appliance McAfee Application Data Monitor detecta uma violação, ele preserva todos os detalhes daquela sessão de aplicativo para utilizá-la na perícia e resposta a incidentes ou para exigências de auditoria de conformidade.

Ao mesmo tempo, o appliance McAfee Application Data Monitor proporciona visibilidade sobre ameaças que podem se disfarçar de aplicativos legítimos:

- Ameaças avançadas na camada de aplicativo
- Uso não autorizado ou roubo de dados confidenciais
- Ataques que tenham como origem ou destino “pontos cegos” da segurança
- Uso de código legado perigoso
- Roubo ou uso indevido de credenciais de usuário
- Transmissão de dados confidenciais por meio de qualquer aplicativo
- Processos de negócios interrompidos

Principais vantagens

- Decodifica toda a sessão de aplicativo, até a camada 7, para centenas de aplicativos
- Vem com regras de detecção predefinidas para dados confidenciais e controlados
- É compatível com dicionários e regras que podem ser definidos pelo usuário, para proporcionar personalização
- Gera uma trilha de auditoria completa de eventos de aplicativos, para fins de conformidade
- Funciona de forma passiva, para não afetar os aplicativos
- Integra-se com o McAfee Enterprise Security Manager para possibilitar a correlação do conteúdo dos aplicativos com eventos ou outros canais de dados
- Opções flexíveis e híbridas que incluem appliances físicos e virtuais

Perda de dados e violações de conformidade

O appliance McAfee Application Data Monitor pode detectar quando as informações confidenciais são transmitidas em anexos de e-mails, mensagens instantâneas, transferências de arquivos, posts HTTP ou qualquer outro aplicativo, notificando imediatamente, para que a perda de dados seja reduzida.

Você pode detectar dados confidenciais (como informações de cartões de crédito e números de CPF) imediatamente ou personalizar as capacidades de detecção do appliance McAfee Application Data Monitor definindo seus próprios dicionários de informações confidenciais. O appliance McAfee Application Data Monitor detectará esses tipos de dados confidenciais, alertará a equipe adequada e registrará a infração para manter uma trilha de auditoria.

Descoberta de documentos

O appliance McAfee Application Data Monitor descobre mais de 500 tipos de documentos enquanto eles são intercambiados na rede através de e-mails, bate-papo, ponto a ponto (P2P), compartilhamento de arquivos, entre outros meios. O appliance McAfee Application Data Monitor descobre documentos, independente da extensão, que se disfarçam como sendo de outro tipo na tentativa de contornar gateways de e-mail e sistemas de detecção de intrusões (IDS) e de prevenção de intrusões (IPS). Mesmo os documentos incorporados em outros documentos, além daqueles arquivados, compactados e codificados, são descobertos através de parâmetros, como nome de arquivo e operação sendo realizada, com base nos quais é possível executar ações.

Ameaças na camada de aplicativo

As ameaças novas e sofisticadas exploram as vulnerabilidades de aplicativos comuns de negócios para penetrar em sua rede e exportar dados confidenciais. Embora seja difícil detectar essas ameaças na camada de aplicativo com o uso de firewalls, sistemas de detecção de intrusões (IDS) e sistemas de prevenção de intrusões (IPS) tradicionais, o appliance McAfee Application Data Monitor consegue analisar todo o conteúdo de um aplicativo, inclusive os protocolos subjacentes, para detectar cargas ocultas, malware e até mesmo canais de comunicação disfarçados, como executáveis incorporados em documentos PDF.

Anomalias de protocolo

A detecção de anomalias pode identificar as ameaças iminentes de forma proativa, reduzindo riscos e minimizando perdas. Enquanto as soluções de segurança convencionais limitam-se à análise dos fluxos de rede, o appliance McAfee Application Data Monitor eleva essa abordagem a um novo patamar. Visualizamos além do comportamento da rede para detectar anomalias em aplicativos e protocolos, proporcionando uma metodologia de detecção de riscos mais forte e proativa.

Sem interferência nos aplicativos

Como o appliance McAfee Application Data Monitor funciona em uma porta SPAN, o desempenho ou a confiabilidade do aplicativo não serão afetados nem haverá latência.

Compatibilidade com mais de 500 aplicativos e protocolos

- **Protocolos de rede de baixo nível:** TCP/IP, UDP, RTP, RPC, SOCKS e DNS, entre outros
- **E-mail:** MAPI, NNTP, POP3, SMTP e Microsoft Exchange
- **Webmail:** AOL Webmail, Hotmail, Yahoo! Mail, Gmail, Facebook e e-mail do MySpace
- **Mensagens instantâneas:** AOL, ICQ, Jabber, MSN, SIP e Yahoo!
- **Protocolos de transferência de arquivos:** FTP, HTTP, SMB e SSL
- **Protocolos de compactação e extração:** BASE64, GZIP, MIME, TAR, ZIP e outros
- **Arquivos compactados:** arquivos RAR, ZIP, BZIP, GZIP, BinHex e arquivos com codificação UU
- **Pacote de instalação:** pacotes Linux , arquivos .cab do InstallShield e arquivos .cab da Microsoft
- **Arquivos de imagem:** GIFs, JPEGs, PNGs, TIFFs, AutoCAD, Photoshop, Bitmaps, Visio, Digital RAW e ícones do Windows
- **Arquivos de áudio:** WAV, MIDI, RealAudio, Dolby Digital AC-3, MP3, MP4, MOD, SHOUTCast etc.
- **Arquivos de vídeo:** AVI, Flash, QuickTime, RealMedia, MPEG-4, Vivo, Digital Video (DV), Motion JPEG etc.
- **Outros aplicativos e arquivos:** bancos de dados, planilhas, faxes, aplicativos da Web, fontes, arquivos executáveis, aplicativos do Microsoft Office, jogos e ferramentas de desenvolvimento de software

Integração com sua infraestrutura

Embora a maioria das soluções de monitoramento de rede funcionem sozinhas, o appliance McAfee Application Data Monitor trabalha em conjunto com outros sistemas de segurança de 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 a detecção de perdas e fraudes com análise eficiente, inspeção de rede, monitoramento de eventos do banco de dados e muito mais.

Exemplos de casos de uso

O appliance McAfee Application Data Monitor pode detectar uma série de atividades não autorizadas, violações de políticas, roubo e fraude. Veja a seguir alguns exemplos.

Roubo de informações confidenciais

Um funcionário conectado como joaosouza@empresa.com enviou um e-mail para cumplice@gmail.com. O e-mail continha um arquivo chamado shoo.doc, que possuía as palavras "fórmula secreta". O e-mail foi enviado às 12h20min do host desktop0232 (192.168.0.36), utilizando o servidor SMTP (10.0.2.13) com este assunto: entendi.

Uso de aplicativos não autorizados

Um funcionário violou uma política ao transferir músicas, utilizando um aplicativo de compartilhamento de arquivos de ponto a ponto que ele instalou. Esse funcionário enviou arquivos grandes durante o expediente, consumindo uma quantidade importante da largura de banda. Uma investigação mais detalhada revelou que se trata de um infrator frequente. Ele utiliza o Jabber e o IRC, além de executar um servidor da Web não autorizado em seu computador desktop.

Navegação improdutiva (cyberslacking) no local de trabalho

Há uma funcionária que, às escondidas, também é investidora. Durante o expediente, ela fica conectada em sites de negociações financeiras por cerca de uma hora pela manhã e mais uma hora à tarde. Além disso, ela utiliza o sistema VoIP (SIP) da empresa para fazer, em média, seis chamadas por dia e ainda passa horas conectada no Yahoo! Messenger como "joaoinvestidor", conversando com "betoinvestidor" e "anainvestidora".

Usuários com senhas fracas

A política de segurança de sua empresa exige o uso de senhas fortes para todas as contas de usuário, do sistema e de aplicativos. As contas do Microsoft Active Directory são gerenciadas rigorosamente. Contudo, dezenas de senhas fracas são utilizadas em servidores FTP de conexão externa, servidores de e-mail e aplicativos críticos da Web que não utilizam o Active Directory.

Compatibilidade com mais de 500 aplicativos e protocolos (continuação)

- **Outros protocolos:** impressora de rede, acesso via shell, VoIP e P2P

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

61322ds_app-data-monitor_0914
SETEMBRO DE 2014