McAfee Application and Change Control

Proteção abrangente contra alterações indesejadas ou controle não autorizado em aplicativos, endpoints, servidores e dispositivos de função fixa

Ameaças persistentes avançadas (APTs) por meio de ataques remotos ou engenharia social tornam cada vez mais difícil proteger a empresa e podem resultar em violações de segurança, perda de dados e interrupções. Alterações nocivas podem passar despercebidas facilmente, especialmente nos atuais ambientes de nuvem e servidor em constante evolução. Quem tem tolerância zero para ameaças persistentes avançadas deve prestar mais atenção ao software McAfee® Application and Change Control.

O McAfee® Application Control ajuda a TI a derrotar os criminosos cibernéticos e a manter sua empresa segura e produtiva. Utilizando um modelo dinâmico de confiança, inteligência local e global sobre reputação, análise comportamental em tempo real e autoimunização de endpoints, esta solução da McAfee detém imediatamente as APTs — sem exigir um gerenciamento trabalhoso de listas ou atualizações de assinaturas.

O software McAfee® Change Control bloqueia alterações não autorizadas em diretórios, configurações e arquivos de sistema críticos, ao mesmo tempo que simplifica a implementação de novas políticas e medidas de conformidade. Com monitoramento de integridade dos arquivos e prevenção de alterações, o McAfee Change Control impõe políticas de alterações e oferece monitoramento contínuo de sistemas críticos. Ele também detecta e bloqueia alterações indesejadas feitas em locais remotos e distribuídos.

Sua interface de pesquisa intuitiva ajuda os usuários a localizar rapidamente informações sobre eventos de alterações.

A combinação de controle de aplicativos e controle de alterações proporcionada pelo McAfee Application and Change Control assegura a integridade do sistema permitindo somente acesso autorizado aos dispositivos, bloqueando executáveis não autorizados e adotando uma abordagem sistemática para monitorar e prevenir alterações no sistema de arquivos, no Registro e em contas de usuário. Isso ajuda a garantir detecção e proteção contínuas e eficientes no âmbito de toda a empresa.

Inserção inteligente em lista branca

Evite ataques de dia zero e de APT bloqueando a execução de aplicativos não autorizados e permitindo que somente aplicativos sabidamente benignos, incluídos na lista branca, sejam executados.

Principais vantagens

- Aproveite o McAfee Global Threat Intelligence e o McAfee Threat Intelligence Exchange para fornecer a reputação global e local de arquivos e aplicativos
- Reforce a segurança e reduza os custos de propriedade com inclusão dinâmica em lista branca, aceitando automaticamente software novo adicionado através de canais confiáveis
- Imponha controles a servidores conectados ou desconectados, máquinas virtuais, endpoints e dispositivos fixos, como terminais de ponto de venda e sistemas legados
- Permita novos aplicativos com base na classificação do aplicativo ou autoaprovação para melhor continuidade dos negócios

Conecte-se conosco

O McAfee Application and Change Control agrupa por aplicativo e por fornecedor os binários (.EXEs, DLLs, drivers e scripts) espalhados pela empresa, apresenta-os em um formato hierárquico e intuitivo e classifica-os de maneira inteligente como válidos, desconhecidos e conhecidos como nocivos.

Implemente a postura de segurança certa

Para mais flexibilidade no uso de aplicativos em um mundo de negócios conectado à nuvem e a mídias sociais, o McAfee Application and Change Control dá às organizações três opções para maximizar sua estratégia de inserção em lista branca para prevenção de ameaças:

Figura 1. Três maneiras de maximizar uma estratégia de lista branca.

Resposta completa e rápida

A inserção em lista branca é complementada pelo McAfee® Global Threat Intelligence, uma tecnologia exclusiva da McAfee que rastreia a reputação de arquivos, mensagens e remetentes em tempo real, usando milhões de sensores ao redor do mundo.

O McAfee Application Control usa esse conhecimento para determinar a reputação dos arquivos em um ambiente computacional, classificando-os como válidos, nocivos ou desconhecidos.

Quando distribuído com o McAfee® Threat Intelligence Exchange, um módulo opcional vendido separadamente, o McAfee Application and Change Control atualiza a lista branca com base em inteligência local sobre reputação para combater ameaças instantaneamente. Ele também usa o McAfee Threat Intelligence Exchange para se coordenar com o McAfee® Advanced Threat Defense e analisar dinamicamente o comportamento de aplicativos desconhecidos em uma área restrita (sandbox), imunizando automaticamente todos os endpoints contra o malware recém-detectado.

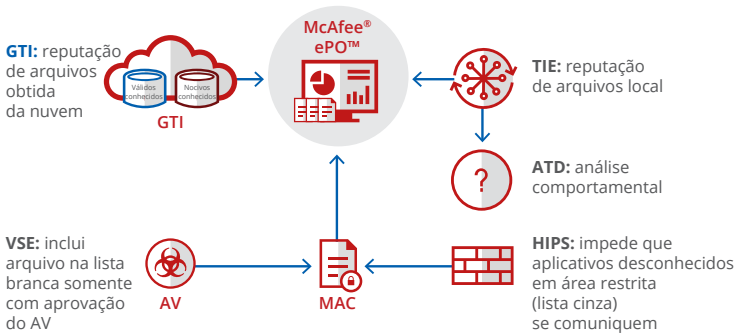

Figura 2. O McAfee Global Threat Intelligence e o McAfee Threat Intelligence Exchange fornecem informações de reputação global e local para o McAfee Application Control.

Principais vantagens (continuação)

- Proporcione visibilidade contínua e gerenciamento em tempo real das alterações feitas em arquivos de conteúdo, configurações e sistemas críticos
- Impeça a adulteração de chaves do Registro e de arquivos críticos por pessoas não autorizadas
- Viabilize uma imposição rigorosa de políticas através do bloqueio proativo de alterações indesejadas e fora de processo antes que elas ocorram

Sugestões internas poderosas

Relatórios predefinidos e pesquisas de inventário ajudam os usuários a gerenciar facilmente questões de vulnerabilidade, conformidade e segurança em ambientes e arquivos relacionados a aplicativos. Isso ajuda a revelar insights úteis, como aplicativos recém-adicionados, binários não certificados, arquivos com reputações desconhecidas e sistemas executando versões de software desatualizadas.

O modo de inventário, novidade no McAfee Application and Change Control 8.3, mantém continuamente inventários atualizados de cada sistema/dispositivo. Isso reduz a utilização de recursos do sistema/dispositivo e da CPU, enquanto mantém conformidade com SWAM/CPE e PCI-DSS. O modo de inventário permite aos usuários rastrear alterações em arquivos e binários no endpoint ao longo do tempo. Opcionalmente, a enumeração de plataforma comum (CPE) correlaciona dados de CPE do NIST com os inventários coletados, para uso na criação de listas brancas e geração de relatórios de conformidade.

Impacto nenhum sobre a continuidade dos negócios

Para evitar interferência na continuidade dos negócios, novos aplicativos são permitidos automaticamente com base na reputação. Para aplicativos desconhecidos, uma interface de sugestões recomenda novas políticas de atualização com base em padrões de execução nos endpoints. Essa é uma maneira excelente de gerenciar exceções geradas por aplicativos bloqueados. Após inspecionar exceções e detalhes do aplicativo bloqueado, simplesmente aprove o arquivo e insira-o na lista branca ou ignore-o para bloquear o aplicativo.

Ajude os usuários a se tornarem parte da solução

No caso de aplicativos desconhecidos, o McAfee Application and Change Control explica aos usuários por que o acesso a aplicativos não autorizados não é permitido, possibilitando e que os usuários sigam os passos necessários para aprovar o aplicativo por meio de autoaprovações ou solicitações de aprovação.

Mantenha os sistemas atualizados

É importante manter os sistemas atualizados com o patch mais recente. O modelo dinâmico de confiança do McAfee Application and Change Control pode atualizar sistemas automaticamente, sem afetar a continuidade dos negócios. Mantenha os sistemas atualizados utilizando usuários confiáveis, grupos locais confiáveis, certificados, processos e diretórios. O McAfee Application Control também impede que aplicativos incluídos em listas brancas sejam explorados por meio de ataques de estouro de buffer de memória em sistemas Microsoft Windows.

Prevenção de alterações e monitoramento de integridade

Frequentemente existe a possibilidade de variação nas configurações sem que haja visibilidade sobre quem realizou a alteração, o que pode resultar em violações de segurança, perda de dados ou interrupções. O McAfee Application and Change Control pode bloquear ou restringir quaisquer tentativas de alteração no sistema/dispositivo que não estejam previstas na política.

Plataformas compatíveis

McAfee Application and Change Control:

- 8.3.x, 8.2.x, 8.1.x, 8.0.x, 7.0.x (sistemas operacionais baseados em Windows)
- 6.4.x, 6.3.x (sistemas operacionais baseados em Linux) 6.2.x, 6.1.x (sistemas operacionais baseados em Windows e em UNIX)
- Linux
- Microsoft Windows

Caso se tente realizar alguma alteração, esta será registrada, proporcionando visibilidade em tempo real sobre quaisquer eventos de alteração. O módulo do controlador do sistema gerencia a comunicação entre o controlador do sistema e os agentes.

Monitoramento avançado da integridade dos arquivos

O McAfee Application and Change Control permite a implementação de software de monitoramento de integridade de arquivos (FIM) e validação de conformidade com PCI-DSS em tempo real, de uma maneira eficiente e econômica. A funcionalidade de FIM do McAfee Application and Change Control proporciona informações essenciais (quem, quando, o quê e por quê), incluindo nome do usuário, hora da alteração, nome do programa e dados de conteúdo do arquivo/Registro — tudo em um único lugar e em tempo real. Além disso, ela pode ajudá-lo a identificar causas raízes ao solucionar problemas em caso de interrupções.

Rastreamento de alterações de conteúdo

O McAfee Change Control permite ao departamento de TI rastrear o conteúdo dos arquivos e alterações em seus atributos. Alterações no conteúdo dos arquivos podem ser visualizadas e comparadas lado a lado para evidenciar o que foi adicionado, excluído ou modificado. Configure filtros de inclusão/exclusão para que apenas alterações relevantes e que exijam ações de resposta sejam capturadas. Alterações em sistemas e dispositivos também podem ser restringidas por usuários, grupos de usuários locais, aplicativos, certificados e/ou serviços Web. Alterações em sistemas e dispositivos podem até mesmo ficar restritas a determinados dias e horários (por exemplo, ao permitir que atualizações do Windows sejam aplicadas somente entre as 2h e as 4h das terças-feiras). Além disso, mecanismos especiais de alerta notificam instantaneamente o departamento de TI sobre alterações críticas para ajudar a evitar interrupções relacionadas a configurações — uma prática recomendada pela biblioteca de infraestrutura de tecnologia da informação (ITIL). Formulários de assessor de segurança qualificado (QSA) são fornecidos para facilitar a geração de relatórios PCI.

Impeça interrupções causadas por alterações não planejadas

O McAfee Change Control permite à TI resolver incidentes com facilidade, automatizar os controles de conformidade regulatória e impedir interrupções relacionadas a alterações. Além disso, ele elimina a necessidade de políticas de conformidade manuais, suscetíveis a erros e que utilizam muitos recursos, geralmente associadas a exigências da lei Sarbanes-Oxley (SOX). O McAfee Application and Change Control permite que os usuários criem uma estrutura automatizada de controle de TI na qual todas as informações necessárias para verificação de conformidade estejam disponíveis em um único sistema de geração de relatórios. Alterações que vão contra as autorizações podem ser validadas automaticamente. Correções de emergência e outras alterações fora de processo são documentadas e reconciliadas automaticamente para facilitar as auditorias.

Gerenciamento centralizado de segurança e conformidade

O software McAfee® ePolicy Orchestrator® (McAfee ePO™) consolida e centraliza o gerenciamento, oferecendo uma visão global da segurança corporativa. Essa plataforma premiada integra o McAfee Application and Change Control ao McAfee® Host Intrusion Prevention e a outros produtos de segurança da McAfee, inclusive antimalware para inserção em lista negra. A instalação e a atualização da distribuição do McAfee Application and Change Control podem ser feitas em uma única etapa no Microsoft System Center. Novos perfis podem ser ativados a qualquer momento para aumentar a proteção — de um simples monitoramento a uma imposição de política à prova de falhas.

Próximos passos

Bloqueie ou restrinja com confiança qualquer forma de execução de aplicativos não autorizados que coloque os dados em risco e adote uma abordagem sistemática para o monitoramento e prevenção de alterações no sistema de arquivos, no Registro e nas contas dos usuários. O McAfee Application and Change Control assegura a integridade dos sistemas permitindo somente acesso autorizado aos dispositivos e bloqueando executáveis não autorizados.

Para obter mais informações, visite www.mcafee.com/br/products/application-control.aspx ou ligue para 0800 891 0168 - opção 2.

Learn More

Para obter mais informações, consulte nosso Guia de ambientes compatíveis — KB87944.

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