

# McAfee Embedded Control

Integridade do sistema, controle de alterações e conformidade com políticas em uma única solução

O McAfee® Embedded Control mantém a integridade do seu sistema permitindo que apenas código autorizado seja executado, e que apenas alterações autorizadas sejam realizadas. Ele cria automaticamente uma lista branca dinâmica de “código autorizado” no sistema incorporado. Depois que a lista branca é criada e ativada, o sistema só aceita a linha de base tida como segura. Nenhum programa ou código fora desse conjunto autorizado pode ser executado, e nenhuma alteração não autorizada pode ser realizada. O McAfee Integrity Control, que combina o McAfee Embedded Control e o console do McAfee ePolicy Orchestrator® (McAfee ePO™), proporciona relatórios de auditoria e conformidade integrados para ajudá-lo a satisfazer várias normas de conformidade.

## Principais vantagens

- Minimize seu risco de segurança controlando o que é executado em seus dispositivos incorporados e protegendo a memória desses dispositivos
- Ofereça acesso, mantenha o controle e reduza os custos de suporte
- Cumprimento seletivo
- Distribua e esqueça
- Prepare seus dispositivos para conformidade e auditoria
- Visibilidade de tempo real
- Auditoria abrangente
- Arquivo de alterações pesquisável
- Reconciliação de ciclo fechado

O McAfee Embedded Control se concentra na solução do problema do crescente risco de segurança motivado pela adoção de sistemas operacionais comerciais em sistemas incorporados. O McAfee Embedded Control é uma solução independente de aplicativo e que apresenta baixo consumo de recursos e pouca sobrecarga, proporcionando segurança “distribuir e esquecer”. O McAfee Embedded Control converte um sistema que tem como base um sistema operacional comercial em uma “caixa preta” para que ele se pareça com um sistema operacional proprietário fechado. Isso impede que programas não autorizados presentes no disco ou injetados na memória sejam executados e impede alterações não autorizadas em uma linha de base autorizada. A solução permite que os fabricantes aproveitem os benefícios de uso de um sistema operacional comercial sem riscos adicionais e sem perder o controle sobre a forma como os sistemas são usados em campo.

## Garantia de integridade do sistema

### Controle de executáveis

Com o McAfee Embedded Control, apenas programas contidos na lista branca dinâmica da McAfee podem ser executados. Outros programas (exes, dlls, scripts) são considerados como não autorizados. Sua execução é impedida, e a falha é registrada por padrão. Isso impede que worms, vírus, spyware e outros tipos de malware que se instalam sejam executados de forma ilegítima.

### Controle de memória

O controle de memória garante que os processos em execução estejam protegidos contra tentativas maliciosas de sequestro. O código não autorizado injetado em um processo em execução é aprisionado, interrompido e registrado. Dessa forma, tentativas de obtenção de controle de um sistema por meio de estouro de buffer, estouro de heap, execução de pilha e explorações semelhantes são anuladas e registradas.<sup>1</sup>

### Controle de alterações

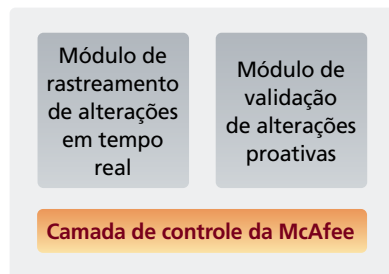
O McAfee Embedded Control detecta alterações em tempo real. Ele oferece visibilidade sobre as fontes de alterações e verifica se as alterações foram distribuídas nos sistemas de destino corretos; proporciona uma trilha de auditoria das alterações; e permite que as alterações sejam realizadas apenas por meios autorizados.

Ele permite cumprir processos de controle de alterações especificando os meios autorizados para realização de alterações. Você pode controlar quem pode aplicar alterações, quais certificados são necessários para permitir alterações, o que pode ser alterado (por exemplo, você pode restringir a alteração de certos arquivos ou diretórios) e quando as alterações podem ser aplicadas (por exemplo, as janelas de atualização podem ser abertas apenas em certos momentos da semana).

<sup>1</sup> Disponível apenas em plataformas Microsoft Windows.

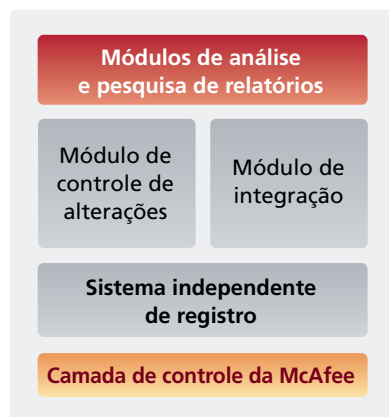
A alteração proativa verifica cada alteração antes que ela seja aplicada nos sistemas de destino. Com esse módulo ativado, as atualizações em sistemas de software só podem ser realizadas de maneira controlada.

O módulo de rastreamento de alterações em tempo real registra todas as alterações no estado do sistema, incluindo o código, a configuração e o Registro. Os eventos de alteração são registrados quando ocorrem, em tempo real, e são enviados para o controlador do sistema para fins de agregação e arquivamento.



**Agente de alterações distribuído em terminais**

O módulo do controlador do sistema gerencia a comunicação entre o controlador do sistema e os agentes. Ele agrega e armazena informações de eventos de alteração dos agentes no ISR (Independent System of Record).



**Agente de alterações distribuído em terminais**

### Conformidade com políticas e auditoria

O McAfee Integrity Control oferece dashboards e relatórios que irão ajudá-lo a atender aos requisitos de conformidade. Eles são gerados pelo console do McAfee ePO, que oferece uma interface com base na Web para usuários e administradores.

O McAfee Embedded Control oferece auditoria e conformidade completas e integradas, em ciclo fechado e em tempo real, com sistema à prova de adulteração de registros de atividade autorizada e tentativas não autorizadas.

### Próximas etapas

Para obter mais informações, visite [www.mcafee.com/br/solutions/embedded-security/embedded-security.aspx](http://www.mcafee.com/br/solutions/embedded-security/embedded-security.aspx) ou entre em contato com o representante local da McAfee.

### Sobre a segurança incorporada da McAfee

As soluções de segurança incorporada da McAfee ajudam os fabricantes a garantir que seus produtos e dispositivos estejam protegidos contra ataques e ameaças cibernéticas. As soluções da McAfee abrangem uma vasta gama de tecnologias, incluindo listas brancas de aplicativos, proteção antivírus e antimalware, gerenciamento de dispositivos, criptografia e risco e conformidade, sempre tirando proveito da tecnologia líder de indústria McAfee Global Threat Intelligence™. Nossas soluções podem ser adequadas às necessidades específicas de design do dispositivo de um fabricante e suas arquiteturas.

Recurso	Descrição	Vantagem
<b>Garantia de integridade do sistema</b>		
Defesa contra ameaças externas	Garante que apenas código autorizado possa ser executado. Código não autorizado não pode ser injetado na memória. Código autorizado não pode ser adulterado.	<ul style="list-style-type: none"> <li>Acaba com as correções de emergência, reduz a quantidade e a frequência dos ciclos de correções, permite mais testes antes da aplicação das correções, reduz os riscos de segurança em sistemas nos quais é difícil aplicar correções.</li> <li>Reduz o risco de segurança diante de ataques polimórficos e de dia zero causados por malware como worms, vírus, cavalos de Troia, injeções de código como estouro de buffer, estouro de heap e estouro de pilha.</li> <li>Mantém a integridade de arquivos autorizados, garantindo que o sistema em produção esteja em um estado conhecido e verificado.</li> <li>Reduz os custos das operações reduzindo os tempos de inatividade planejados para aplicação de correções e os não planejados para recuperações, além de aumentar a disponibilidade do sistema.</li> </ul>
Defesa contra ameaças internas	O bloqueio de administrador local oferece a flexibilidade de impedir que até mesmo administradores alterem o que tem autorização para ser executado em um sistema protegido, a não ser que uma chave autêntica seja apresentada.	<ul style="list-style-type: none"> <li>Protege contra ameaças internas.</li> <li>Limita o que pode ser executado em sistemas incorporados em produção e impede que até mesmo administradores façam alterações.</li> </ul>
<b>Controle avançado de alterações</b>		
Atualizações autorizadas seguras por fabricante	Garante que apenas atualizações autorizadas possam ser implementadas nos sistemas incorporados em campo.	<ul style="list-style-type: none"> <li>Garante que nenhuma alteração urgente seja distribuída nos sistemas em campo. Impede alterações não autorizadas no sistema antes que resultem em tempo de inatividade e gerem chamadas ao suporte.</li> <li>Os fabricantes podem optar por manter o controle sobre todas as alterações, ou autorizar apenas agentes de clientes confiáveis a controlar alterações.</li> </ul>
Verificar se as alterações ocorreram na janela aprovada	Garante que as alterações não tenham sido distribuídas fora das janelas de alterações autorizadas.	<ul style="list-style-type: none"> <li>Impede alterações não autorizadas durante janelas de tempo críticas do ponto de vista fiscal ou em horários comerciais de pico para evitar interrupções nas operações e/ou violações de conformidade.</li> </ul>
Atualizadores autorizados	Garante que apenas atualizadores autorizados (pessoas ou processos) possam implementar alterações em sistemas de produção.	<ul style="list-style-type: none"> <li>Garante que nenhuma alteração urgente seja distribuída nos sistemas de produção.</li> </ul>
<b>Auditoria e a conformidade de ciclo fechado em tempo real</b>		
Rastreamento de alterações em tempo real	Rastreia alterações assim que elas acontecem na empresa.	<ul style="list-style-type: none"> <li>Garante que nenhuma alteração urgente seja distribuída nos sistemas de produção.</li> </ul>
Auditoria abrangente	Captura informações completas sobre todas as alterações do sistema: quem, o que, onde, quando e como.	<ul style="list-style-type: none"> <li>Um registro preciso, completo e definitivo de todas as alterações no sistema.</li> </ul>
Identificar as fontes de alterações	Vincula as alterações às suas fontes: quem fez a alteração, a sequência de eventos que levaram a ela, o processo/ programa que a afetou.	<ul style="list-style-type: none"> <li>Valida alterações aprovadas; identifica rapidamente alterações não aprovadas; aumenta a taxa de sucesso.</li> </ul>

(continuação)



Baixa sobrecarga operacional		
Distribua e esqueça	O software é instalado em minutos, sem a necessidade de configuração inicial. Não é necessária uma configuração contínua.	<ul style="list-style-type: none"><li>• Já vem pronto para o uso. Eficaz imediatamente após a instalação. Não tem sobrecarga de manutenção contínua, sendo uma boa escolha para uma configuração de solução de segurança de baixo custo operacional.</li></ul>
Sem regras, sem assinaturas, sem período de aprendizado, independente de aplicativo	Não depende de bancos de dados de assinaturas ou regras, é eficaz imediatamente em todos os aplicativos sem período de aprendizado.	<ul style="list-style-type: none"><li>• Exige muito pouca atenção do administrador durante o ciclo de vida do servidor.</li><li>• Protege o servidor até que as correções sejam aplicadas, com baixo custo operacional contínuo.</li><li>• Sua eficácia não depende da qualidade de quaisquer regras ou políticas.</li></ul>
Não exige muito do sistema e tem baixa sobrecarga no tempo de execução	Ocupa menos de 20 MB de espaço em disco. Não interfere no desempenho de tempo de execução dos aplicativos.	<ul style="list-style-type: none"><li>• Pronto para distribuição em qualquer sistema de produção de missão crítica sem afetar seu desempenho de tempo de execução ou seus requisitos de armazenamento.</li></ul>
Garantia de nenhum falso positivo ou falso negativo	Apenas a atividade não autorizada é registrada.	<ul style="list-style-type: none"><li>• A precisão dos resultados reduz os custos operacionais em comparação a outras soluções de prevenção contra intrusões no host, diminuindo drasticamente o tempo necessário para a análise diária/semanal de registros.</li><li>• Aumenta a eficiência do administrador, reduz os custos operacionais</li></ul>

