

# McAfee Embedded Control

Systemintegrität, Änderungskontrolle und Richtlinien-Compliance  
in einer einzigen Lösung

McAfee® Embedded Control gewährleistet die Integrität Ihres Systems, indem nur autorisierter Code ausgeführt sowie autorisierte Änderungen vorgenommen werden können. Es wird automatisch eine dynamische Whitelist des „autorisierten Codes“ im eingebetteten System erstellt. Nach der Erstellung und Aktivierung der Whitelist ist das System in einer als sicher bekannten Konfiguration eingefroren. Lediglich autorisierte Programme oder Code können ausgeführt werden. Nicht autorisierte Änderungen werden verhindert. McAfee Integrity Control kombiniert McAfee Embedded Control mit der McAfee ePolicy Orchestrator® (McAfee ePO™)-Konsole und bietet integrierte Audit- und Compliance-Berichte, die die Einhaltung mehrerer Vorschriften vereinfachen.

## Hauptvorteile

- Minimierung der Sicherheitsrisiken, da der Gerätespeicher geschützt sowie gesteuert werden kann, was auf Ihren eingebetteten Geräten ausgeführt wird
- Gewährung von Zugriff, Gewährleistung der Kontrolle sowie Senkung von Support-Kosten
- Selektive Umsetzung
- Kein weiterer Arbeitsaufwand nach der Ausbringung
- Vorbereitung der Geräte auf Compliance und Audits
- Echtzeittransparenz
- Umfassende Audits
- Durchsuchbares Änderungsarchiv
- Geschlossener Abgleich

McAfee Embedded Control löst das Problem erhöhter Sicherheitsrisiken, die bei Verwendung kommerzieller Betriebssysteme in eingebetteten Systemen auftreten. McAfee Embedded Control ist eine schlanke, unaufwändige und anwendungsunabhängige Lösung, die sofort nach der Implementierung Ihre Unternehmensumgebung schützt. McAfee Embedded Control verwandelt ein System, das auf einem kommerziellen Betriebssystem aufgebaut ist, in eine „Blackbox“, damit es wie ein geschlossenes, proprietäres Betriebssystem aussieht. Dadurch können unbefugte Programme, die sich auf dem Datenträger befinden oder in den Arbeitsspeicher injiziert werden, nicht ausgeführt werden. Zudem verhindert es unzulässige Veränderungen. Mit dieser Lösung können Hersteller die Vorteile eines kommerziellen Betriebssystems nutzen, ohne zusätzliche Risiken einzugehen oder die Kontrolle über die Systemverwendung zu verlieren.

## Garantierte Systemintegrität

### Kontrolle über ausführbare Dateien

Mithilfe von McAfee Embedded Control können ausschließlich Programme ausgeführt werden, die in der dynamischen Whitelist von McAfee enthalten sind. Andere Programme wie EXE- oder DLL-Dateien sowie Skripts werden als unbefugt eingestuft. Ihre Ausführung wird verhindert, und das Fehlschlagen wird standardmäßig protokolliert. Dadurch können Würmer, Viren, Spyware und andere Malware-Formen, die sich selbst installieren, nicht unbefugt ausgeführt werden.

### Kontrolle über den Arbeitsspeicher

Dank Kontrolle über den Arbeitsspeicher können Sie gewährleisten, dass ausgeführte Prozesse gegen böswillige Übernahmen (Hijacking) geschützt werden. Nicht autorisierter Code, der in einen ausgeführten Prozess injiziert wird, wird erkannt, gestoppt und protokolliert. Auf diese Weise werden Versuche, durch Buffer Overflow, Heap Overflow, Stack Overflow oder ähnliche Exploits die Kontrolle über Systeme zu erlangen, verhindert und protokolliert.<sup>1</sup>

### Kontrolle über Änderungen

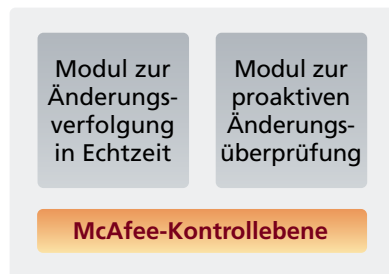
McAfee Embedded Control erkennt Änderungen in Echtzeit und macht die Verursacher dieser Änderungen für Sie sichtbar. Gleichzeitig wird überprüft, ob erwünschte Änderungen auf den richtigen Zielsystemen implementiert wurden, und gewährleistet, dass Änderungen nur mit zulässigen Methoden möglich sind. Zusätzlich erhalten Sie ein Überwachungsprotokoll der Änderungen.

Durch Festlegung zulässiger Änderungsmethoden lassen sich Änderungskontrollprozesse umsetzen. Sie können steuern, wer Änderungen vornehmen kann, welche Zertifikate dafür erforderlich sind, was geändert werden darf (z. B. nur bestimmte Dateien oder Verzeichnisse) und wann Änderungen vorgenommen werden dürfen (z. B. ausschließlich innerhalb bestimmter Update-Zeitfenster).

<sup>1</sup> Nur für Microsoft Windows-Plattformen verfügbar.

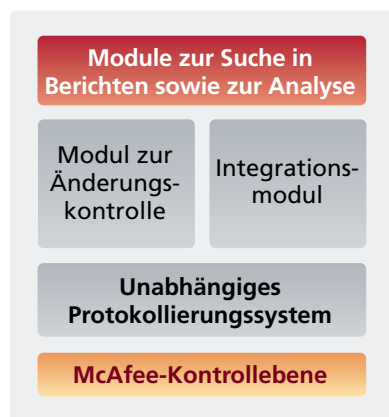
Jede Änderung wird proaktiv überprüft, bevor sie auf die Zielsysteme angewendet wird. Wenn dieses Modul aktiviert ist, können Software-System-Updates nur auf kontrollierte Weise durchgeführt werden.

Das Modul für die Echtzeit-Änderungsnachverfolgung protokolliert alle Systemstatusänderungen – einschließlich Code, Konfiguration und Registrierung. Änderungsereignisse werden in Echtzeit bei ihrem Auftreten protokolliert und an den System-Controller gesendet, wo sie aggregiert und archiviert werden können.



#### **Auf Endgeräten ausgebrachter Änderungsagent**

Das System-Controller-Modul verwaltet die Kommunikation zwischen System-Controller und Agenten. Es aggregiert und speichert Informationen zu Änderungsereignissen von den Agenten im unabhängigen Protokollierungssystem (ISR, Independent System of Record).



#### **Auf Endgeräten ausgebrachter Änderungsagent**

#### **Audits und Richtlinien-Compliance**

McAfee Integrity Control stellt Dashboards und Berichte bereit, die die Einhaltung von Compliance-Anforderungen vereinfachen. Diese können über die McAfee ePO-Konsole abgerufen werden, die eine webbasierte Benutzeroberfläche für Benutzer und Administratoren bereitstellt.

McAfee Embedded Control ermöglicht integrierte, geschlossene Compliance sowie Audits in Echtzeit und umfasst ein vor Manipulationen geschütztes System, mit dem autorisierte Aktivitäten ebenso wie nicht autorisierte Versuche aufgezeichnet werden.

#### **Nächste Schritte**

Weitere Informationen erhalten Sie unter [www.mcafee.com/de/solutions/embedded-security/embedded-security.aspx](http://www.mcafee.com/de/solutions/embedded-security/embedded-security.aspx) oder von Ihrem örtlichen McAfee-Vertriebsrepräsentanten.

#### **Über McAfee-Schutz für eingebettete Systeme**

Mit den McAfee-Sicherheitslösungen für eingebettete Systeme können Hersteller sicherstellen, dass ihre Produkte und Geräte vor Bedrohungen und Angriffen aus dem Internet geschützt sind. McAfee-Lösungen bieten unterschiedliche Technologien wie Anwendungs-Whitelists, Viren- und Malware-Schutz, Geräteverwaltung, Verschlüsselung sowie Risiko-Management und Compliance unterstützt von der branchenführenden McAfee Global Threat Intelligence™. Unsere Lösungen können an die spezifischen Geräte- und Architektur Anforderungen von Herstellern angepasst werden.

Funktion	Beschreibung	Vorteil
<b>Garantierte Systemintegrität</b>		
Schutz vor externen Bedrohungen	Gewährleistet, dass nur autorisierter Code ausgeführt werden kann. Nicht autorisierter Code kann nicht in den Arbeitsspeicher injiziert werden. Autorisierter Code kann nicht manipuliert werden.	<ul style="list-style-type: none"> <li>• Vermeidet Notfall-Patch-Installationen, verringert Anzahl und Häufigkeit der Patch-Zyklen, ermöglicht umfangreichere Tests vor der Patch-Implementierung, senkt Sicherheitsrisiken für schwer zu patchende Systeme.</li> <li>• Reduziert Sicherheitsrisiken durch polymorphe Zero-Day-Angriffe über Malware wie Würmer, Viren, Trojaner sowie Code-Injektionen wie Buffer Overflow, Heap Overflow und Stack Overflow.</li> <li>• Gewährleistet die Integrität autorisierter Dateien, sodass sich das Produktionssystem stets in einem bekannten und bestätigten Zustand befindet.</li> <li>• Senkt die Betriebskosten durch Vermeidung von Ausfallzeiten aufgrund geplanter Patch-Installationen und ungeplanter Wiederherstellungen. Verbessert die Systemverfügbarkeit.</li> </ul>
Schutz vor internen Bedrohungen	Durch die Sperrung lokaler Administratoren auf geschützten Systemen können Sie festlegen, dass Administratoren nur dann Ausführungsautorisierungen ändern können, wenn sie über einen entsprechenden Authentifizierungsschlüssel verfügen.	<ul style="list-style-type: none"> <li>• Schützt vor internen Bedrohungen.</li> <li>• Legt eine Liste der Programme fest, die auf eingebetteten Produktionssystemen ausgeführt werden dürfen, und verhindert sogar Änderungen durch Administratoren.</li> </ul>
<b>Erweiterte Änderungskontrolle</b>		
Sichere autorisierte Hersteller-Updates	Stellt sicher, dass auf eingebetteten Produktionssystemen nur autorisierte Updates installiert werden können.	<ul style="list-style-type: none"> <li>• Stellt sicher, dass auf Produktionssystemen keine außerplanmäßigen Änderungen implementiert werden können. Verhindert nicht autorisierte Änderungen an Systemen und vermeidet dadurch Ausfallzeiten und Support-Anrufe.</li> <li>• Hersteller können wahlweise die Kontrolle über alle Änderungen behalten oder vertrauenswürdige Kunden-Agenten autorisieren.</li> </ul>
Überprüfung, ob Änderungen im zulässigen Zeitfenster vorgenommen werden	Stellt sicher, dass Änderungen nicht außerhalb der autorisierten Änderungs-Zeitfenster ausgebracht werden.	<ul style="list-style-type: none"> <li>• Verhindert nicht autorisierte Änderungen während finanziell sensibler Zeitfenster oder geschäftlicher Spitzenlastzeiten, um Störungen des Betriebs und/oder Vorschriftenverstöße zu vermeiden.</li> </ul>
Autorisierte Aktualisierungsmöglichkeiten	Stellt sicher, dass nur autorisierte Personen oder Prozesse Änderungen an Produktionssystemen vornehmen können.	<ul style="list-style-type: none"> <li>• Stellt sicher, dass auf Produktionssystemen keine außerplanmäßigen Änderungen implementiert werden können.</li> </ul>
<b>Geschlossene Audits und Compliance in Echtzeit</b>		
Änderungsüberwachung in Echtzeit	Überwacht im gesamten Unternehmen Änderungen, während sie auftreten.	<ul style="list-style-type: none"> <li>• Stellt sicher, dass auf Produktionssystemen keine außerplanmäßigen Änderungen implementiert werden können.</li> </ul>
Umfassende Audits	Erfasst vollständige Informationen zu jeder Systemänderung: wer, was, wo, wann und wie.	<ul style="list-style-type: none"> <li>• Stellt eine präzise, vollständige und definitive Aufzeichnung aller Systemänderungen bereit.</li> </ul>
Identifizierung von Änderungsursachen	Verknüpft jede Änderung mit ihrer Ursache: wer die Änderung vorgenommen hat, welche Abfolge von Ereignissen zu ihr geführt hat, welcher Prozess oder welches Programm mitgewirkt hat.	<ul style="list-style-type: none"> <li>• Überprüft genehmigte Änderungen. Identifiziert schnell nicht genehmigte Änderungen. Erhöht die Erfolgsrate von Änderungen.</li> </ul>

(Fortsetzung)



Geringer betrieblicher Zusatzaufwand		
Kein weiterer Arbeitsaufwand nach der Ausbringung	Die Software kann innerhalb von Minuten installiert werden. Es ist keine anfängliche Konfiguration oder Einrichtung sowie keine fortlaufende Konfiguration erforderlich.	<ul style="list-style-type: none"><li>• Funktioniert ohne Vorbereitungs- und Anpassungsaufwand. Ist sofort nach der Installation effektiv. Verursacht keinen fortlaufenden Wartungsaufwand und ist daher ideal als Sicherheitslösungs-Konfiguration mit geringen Betriebskosten.</li></ul>
Keine Regeln, Signaturen oder Trainingsphase erforderlich, anwendungsunabhängig	Hängt nicht von Regeln oder Signaturdatenbanken ab und ist für alle Anwendungen sofort (ohne Trainingsphase) effektiv.	<ul style="list-style-type: none"><li>• Benötigt während des Server-Lebenszyklus sehr wenig Aufmerksamkeit von Administratoren.</li><li>• Schützt Server bis zur Patch-Installation sowie Server ohne installierte Patches und verursacht dabei niedrige fortlaufende Betriebskosten.</li><li>• Die Effektivität hängt nicht von der Qualität von Regeln oder Richtlinien ab.</li></ul>
Geringer Speicherplatzbedarf, geringe Leistungsbeeinträchtigung	Belegt weniger als 20 MB Speicherplatz. Beeinträchtigt nicht die Anwendungsleistung.	<ul style="list-style-type: none"><li>• Bereit für die Ausbringung auf jedem unternehmenskritischen Produktionssystem ohne Auswirkungen auf Leistung und Speicheranforderungen.</li></ul>
Garantiert keine False-Positives oder False-Negatives	Nur nicht autorisierte Aktivitäten werden protokolliert.	<ul style="list-style-type: none"><li>• Die Exaktheit der Ergebnisse bedeutet geringere Betriebskosten als bei anderen Host-Eindringungsschutz-Lösungen, da die Zeit für die tägliche/wöchentliche Analyse von Protokollen drastisch verringert wird.</li><li>• Erhöht die Effizienz von Administratoren. Senkt die Betriebskosten.</li></ul>

