McAfee Embedded Control

Einfacher Schutz für wichtige Geräte

Die Angriffsfläche wird heute von neuartigen Endgeräten dominiert, die von Wearable-Fitnessgeräten bis hin zu kritischen verbundenen Sensoren reichen, die die Generierung und Verteilung steuern. Mit der Zahl der verbundenen Geräte wächst auch die Gefahr durch Malware und Angriffe. McAfee® Embedded Control gewährleistet die Integrität Ihrer Systeme, indem nur autorisierter Zugriff auf Geräte zugelassen wird, während nicht autorisierte ausführbare Dateien blockiert werden.

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 der 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

Hauptvorteile

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

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.[1]

Integration von McAfee GTI: Der klügste Umgang mit weltweiten Bedrohungen in voneinander getrennten Umgebungen

McAfee® Global Threat Intelligence (McAfee GTI) ist mithilfe von Millionen weltweit verteilten Sensoren eine exklusive McAfee-Technologie zur Echtzeitüberwachung der Reputation von Dateien, Nachrichten und Absendern. Diese Funktion nutzt Cloud-Daten zur Feststellung der Reputation aller Dateien in Ihrer Computerumgebung, die daraufhin als gut, schlecht oder unbekannt eingestuft werden. Dank der Integration von McAfee GTI wissen Sie sicher, ob eine Malware unabsichtlich auf die Whitelist gesetzt wurde. Die GTI-Reputationsdaten können über Internet-verbundene sowie isoliert betriebene McAfee® ePolicy Orchestrator® (McAfee ePO™)-Software-Umgebungen abgerufen werden.

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 in McAfee Embedded Control 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. bestimmte Zeitfenster innerhalb der Woche für Microsoft Windows-Updates).

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.

Abbildung 1. McAfee-Kontrollebene

Das System-Controller-Modul verwaltet die Kommunikation zwischen System-Controller und Agenten. Es aggregiert und speichert von den Agenten erfasste Informationen zu Änderungsereignissen im unabhängigen Protokollierungssystem.

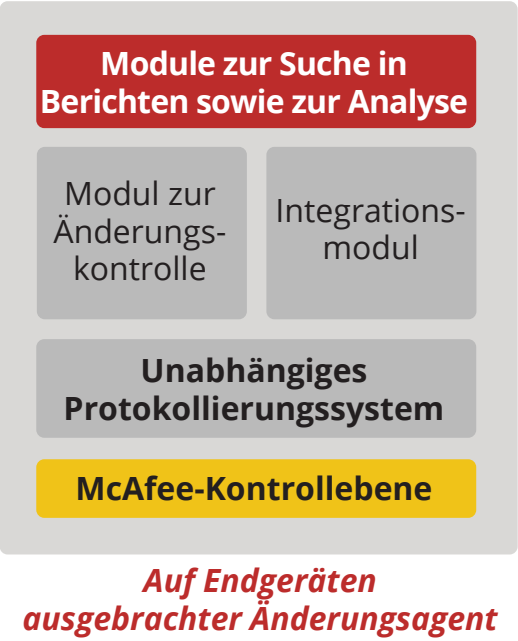

Abbildung 2. Module zur Suche in Berichten sowie zur Analyse

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.

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 Architekturanforderungen von Herstellern angepasst werden.

Funktion	Beschreibung	Vorteil
Garantierte Systemintegrität		
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.	▪ 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. ▪ Reduziert Sicherheitsrisiken durch polymorphe Zero-Day-Angriffe über Malware wie Würmer, Viren, Trojaner sowie Code-Injektionen wie Buffer Overflow, Heap Overflow und Stack Overflow. ▪ Gewährleistet die Integrität autorisierter Dateien, sodass sich das Produktionssystem stets in einem bekannten und bestätigten Zustand befindet. ▪ Senkt die Betriebskosten durch Vermeidung ungeplanter Patch-Installationen und Wiederherstellungen; verbessert die Systemverfügbarkeit.
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.	▪ Schützt vor internen Bedrohungen. ▪ Legt eine Liste der Programme fest, die auf eingebetteten Produktionssystemen ausgeführt werden dürfen, und verhindert sogar Änderungen durch Administratoren.
Erweiterte Änderungskontrolle		
Sichere autorisierte Hersteller-Updates	Stellt sicher, dass auf eingebetteten Produktionssystemen nur autorisierte Updates installiert werden können.	▪ Stellt sicher, dass auf Produktionssystemen keine außerplanmäßigen Änderungen implementiert werden können. Verhindert nicht autorisierte Änderungen an Systemen und vermeidet dadurch Ausfallzeiten und Support-Anrufe. ▪ Hersteller können wahlweise die Kontrolle über alle Änderungen behalten oder vertrauenswürdige Kunden-Agenten autorisieren.
Überprüfung von Änderungen, die innerhalb eines zulässigen Zeitfensters vorgenommen werden	Stellt sicher, dass Änderungen nicht außerhalb der autorisierten Änderungs-Zeitfenster ausgebracht werden.	▪ Verhindert nicht autorisierte Änderungen während finanziell sensibler Zeitfenster oder geschäftlicher Spitzenlastzeiten, um Störungen des Betriebs und/oder Vorschriftenverstöße zu vermeiden.
Autorisierte Aktualisierungs-möglichkeiten	Stellt sicher, dass nur autorisierte Personen oder Prozesse Änderungen an Produktionssystemen vornehmen können.	▪ Stellt sicher, dass auf Produktionssystemen keine außerplanmäßigen Änderungen vorgenommen werden können.

Funktion	Beschreibung	Vorteil
Geschlossene Audits und Compliance in Echtzeit		
Änderungsüberwachung in Echtzeit	Überwacht im gesamten Unternehmen Änderungen, während sie auftreten.	▪ Stellt sicher, dass auf Produktionssystemen keine außerplanmäßigen Änderungen vorgenommen werden können.
Umfassende Audits	Erfasst vollständige Informationen zu jeder Systemänderung: wer, was, wo, wann und wie.	▪ Erstellt eine präzise, vollständige und definitive Aufzeichnung aller Systemänderungen.
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.	▪ Überprüft genehmigte Änderungen. Identifiziert schnell nicht genehmigte Änderungen. Erhöht die Erfolgsrate von Änderungen.
Geringer betrieblicher Zusatzaufwand		
Kein weiterer Arbeitsaufwand nach der Ausbringung	Die Installation dauert nur wenige Minuten und erfordert weder eine Erstkonfiguration noch Einrichtung oder fortlaufende Konfiguration.	▪ 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.
Keine Regeln, Signaturen oder Trainingsphase erforderlich, anwendungsunabhängig	Hängt nicht von Regeln oder Signaturdatenbanken ab und ist für alle Anwendungen sofort (ohne Trainingsphase) effektiv.	▪ Benötigt während des Server-Lebenszyklus sehr wenig Aufmerksamkeit von Administratoren. ▪ Schützt Server bis zur Patch-Installation sowie Server ohne installierte Patches und verursacht dabei niedrige fortlaufende Betriebskosten. ▪ Die Effektivität hängt nicht von der Qualität von Regeln oder Richtlinien ab.
Geringer Speicherplatzbedarf, geringe Leistungsbeeinträchtigung	Belegt weniger als 20 MB Speicherplatz. Beeinträchtigt nicht die Anwendungsleistung.	▪ Bereit für die Ausbringung auf jedem unternehmenskritischen Produktionssystem ohne Auswirkungen auf Leistung und Speicheranforderungen.
Garantiert keine False-Positives oder False-Negatives	Nur nicht autorisierte Aktivitäten werden protokolliert.	▪ 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. ▪ Erhöht die Effizienz von Administratoren. Senkt die Betriebskosten.

Nächste Schritte

Weitere Informationen erhalten Sie unter **www.mcafee.com/de/partners/oem-alliances/index.aspx** oder von Ihrem örtlichen McAfee-Vertriebsrepräsentanten.

1. Nur für Microsoft Windows-Plattformen verfügbar.

McAfee™
Together is power.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 3707 0
www.mcafee.com/de