McAfee Application Control

Minimierung der Risiken durch nicht autorisierte Anwendungen und Kontrolle von Endgeräten, Servern sowie Geräten mit fester Funktion

Hochentwickelte hartnäckige Bedrohungen (APTs) per Remote-Angriff oder Social Engineering erschweren zunehmend den Schutz Ihres Unternehmens. Mit McAfee® Application Control bleiben Sie Cyber-Kriminellen einen Schritt voraus und können die Sicherheit und Produktivität Ihres Unternehmens gewährleisten. Dank eines dynamischen Vertrauensmodells sowie innovativer Sicherheitsfunktionen, wie z. B. lokaler und globaler Bewertungsdaten, Verhaltensanalysen in Echtzeit und Selbstschutz von Endgeräten, blockiert die McAfee-Lösung hochentwickelte hartnäckige Bedrohungen sofort. Dabei sind weder zeitintensive Listenverwaltung noch Signaturaktualisierungen erforderlich. Wenn Sie Zero-Day-Bedrohungen keine Chance lassen wollen, ist McAfee Application Control für Sie sicher interessant.

Intelligente Whitelists

McAfee Application Control blockiert die Ausführung nicht autorisierter Anwendungen und schützt so vor Zero-Day- sowie APT-Angriffen. Mit dieser Funktion zur Anwendungsintenventarisierung können Sie anwendungsbezogene Dateien einfach finden und verwalten. Diese Funktion gruppiert Binärdateien (EXE- und DLL-Dateien, Treiber und Skripte) im gesamten Unternehmen nach Anwendung und Anbieter, stellt sie in einem intuitiven, hierarchischen Format dar und kategorisiert sie als bekannt gut, unbekannt bzw. bekannt schlecht. Mithilfe dieser Whitelist können Sie Angriffe durch unbekannte Malware verhindern, da nur solche Anwendungen ausgeführt werden, die in der Whitelist als bekannt gut eingestuft sind.

Implementierung eines geeigneten Sicherheitsansatzes

Da Benutzer mehr Flexibilität bei der Nutzung von Anwendungen in sozialen Netzwerken und Cloud-Umgebungen fordern, bietet McAfee Application Control drei Möglichkeiten, die Whitelist-Strategie zur Bedrohungsabwehr optimal einzusetzen.

Abbildung 1. Drei Möglichkeiten zur Optimierung Ihrer Whitelist-Strategie.

Hauptvorteile

- Schutz vor Zero-Day- und hochentwickelten hartnäckigen Bedrohungen auch ohne Signaturaktualisierungen
- Nutzung weltweiter und lokaler Reputationsinformationen zu Dateien und Anwendungen aus McAfee Global Threat Intelligence und McAfee Threat Intelligence Exchange
- Verbesserte Sicherheit und geringere Betriebskosten dank dynamischer Whitelists, die neue Software automatisch akzeptieren, wenn diese über vertrauenswürdige Kanäle hinzugefügt wird
- Effiziente Kontrolle des Anwendungszugriffs mit McAfee® ePolicy Orchestrator® (McAfee ePO™), der zentralen Verwaltungsplattform für McAfee-Sicherheitslösungen
- Verringerung der Patch-Zyklen mit sicheren Whitelists und fortschrittlichem Speicherschutz
- Hält Systeme über vertrauenswürdige Update-Funktionen mit aktuellen Patches auf dem neuesten Stand

Effektive, integrierte Vorschläge

Dank der Inventarsuche und vordefinierter Berichte können Sie Schwachstellen, Compliance- und Sicherheitsprobleme in Ihrer Umgebung schnell finden und beheben. Sie erhalten nützliche Zusatzinformationen (z. B. kürzlich hinzugefügte Anwendungen, nicht zertifizierte Binärdateien, Dateien mit unbekannter Reputation, Systeme mit veralteten Software-Versionen), können schneller Schwachstellen lokalisieren und die Compliance von Software-Lizenzen überprüfen.

Vollständige und schnelle Reaktion

Die Whitelist wird ergänzt mithilfe der weltweiten Bedrohungsdaten von McAfee Global Threat Intelligence (McAfee GTI), einer exklusiven McAfee-Technologie zur Echtzeitüberwachung der Reputation von Dateien, Nachrichten und Absendern, die auf Millionen weltweit verteilten Sensoren basiert. McAfee Application Control nutzt diese Daten zur Feststellung der Reputation der Dateien in Ihrer Rechenumgebung, die daraufhin als gut, schlecht oder unbekannt eingestuft werden.

In Kombination mit McAfee Threat Intelligence Exchange (einem optional erhältlichen Modul) aktualisiert McAfee Application Control die Whitelist mit lokalen Reputationsdaten, damit Bedrohungen sofort abgewehrt werden können. Mithilfe von McAfee Threat Intelligence Exchange koordiniert sich McAfee Application Control mit McAfee Advanced Threat Defense, um das Verhalten unbekannter Anwendungen in einer Sandbox dynamisch zu analysieren und Endgeräte automatisch gegen die neu entdeckte Malware zu immunisieren.

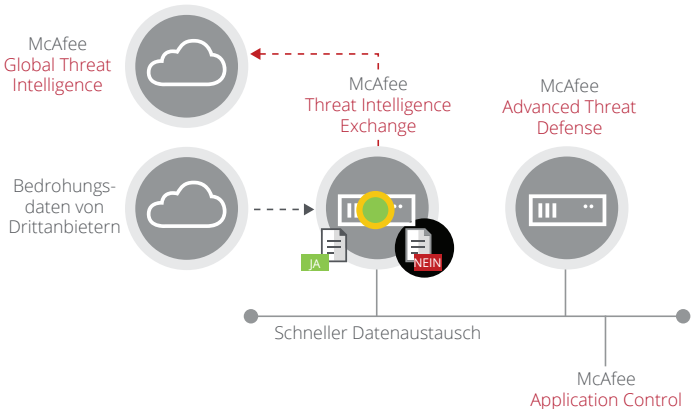

Abbildung 2. McAfee GTI überwacht permanent die Reputation von Dateien und Absendern. In Kombination mit McAfee Threat Intelligence Exchange aktualisiert McAfee Application Control die Whitelist automatisch basierend auf lokalen Reputationsdaten und koordiniert sich mit McAfee Advanced Threat Defense, wenn weitere Dateiinformationen erforderlich sind.

Störungsfreier Geschäftsbetrieb

Zur Vermeidung von Störungen des Geschäftsbetriebs werden neue Anwendungen automatisch in Abhängigkeit von der Anwendungsreputation zugelassen. Bei unbekannten Anwendungen wird eine Übersicht mit Vorschlägen angezeigt, die neue Aktualisierungsrichtlinien anhand von Ausführungsmustern auf den Endgeräten vorschlagen. Auf diese Weise können Sie ganz leicht Ausnahmen verwalten, die von blockierten Anwendungen generiert werden. Nachdem Sie die Ausnahmen und Details der blockierten Anwendung untersucht haben, bestätigen Sie die Datei und nehmen sie in die Whitelist auf oder ignorieren sie, um sie zu blockieren.

Hauptvorteile (Fortsetzung)

- Durchsetzung von Kontrollen auf verbundenen oder getrennten Servern, virtuellen Maschinen, Endgeräten, Geräten mit fester Funktion (z. B. Terminals) sowie älteren Systemen (z. B. Microsoft Windows XP)
- Bestätigung neuer Anwendungen anhand der Anwendungsbewertung oder Selbstfreigabe für unterbrechungsfreien Geschäftsbetrieb
- Gewährleistung der Benutzerproduktivität und Server-Leistung durch eine Lösung mit geringem Verwaltungsaufwand
- Einfacher Schutz für ältere Systeme und moderne Technologieinvestitionen

Unterstützte Plattformen

Microsoft Windows (32- und 64-Bit-Versionen)

- Eingebettete Systeme: Windows XPE, 7 Embedded, WEPOS, POSReady 2009, WES 2009, Embedded 8, 8.1 Industry, 10
- Server: Windows Server 2008, 2008 R2, 2012, 2012 R2
- Desktop: Windows NT, 2000, XP, Vista, 7, 8, 8.1, 10

Linux

- Red Hat/CentOS 5, 6, 7
- SUSE/openSUSE 10, 11
- Oracle Enterprise Linux 5, 6, 7
- Ubuntu 12.04

Benutzer werden zu Helfern

Bei unbekannten Anwendungen stellt McAfee Application Control dem IT-Team verschiedene Möglichkeiten zur Verfügung, wie Benutzer neue Anwendungen installieren können:

- **Benutzerbenachrichtigungen:** Benutzer werden in einem Pop-Up-Fenster darüber informiert, warum der Zugang zu nicht autorisierten Anwendungen unzulässig ist. Diese Meldungen fordern die Benutzer auf, eine Genehmigung per E-Mail oder über den Helpdesk einzuholen.
- **Selbstfreigaben durch Benutzer:** Benutzer mit entsprechender Berechtigung können neue Software installieren, ohne auf die Bestätigung durch das IT-Team warten zu müssen. Die IT-Mitarbeiter überprüfen anschließend diese Selbstfreigaben und erstellen unternehmensweit gültige Richtlinien, die diese Anwendung auf allen Systemen freigeben – oder sperren.

Aktualisierung Ihrer Systeme

Es ist von größter Wichtigkeit, dass Ihre Systeme mit aktuellen Patches auf dem neuesten Stand gehalten werden. Daher bieten wir ein dynamisches Vertrauensmodell an, mit dem Sie Ihre Systeme automatisch aktualisieren können, ohne den Geschäftsbetrieb zu unterbrechen. Dies kann über vertrauenswürdige Benutzer, Zertifikate, Prozesse und Verzeichnisse erfolgen. McAfee Application Control verhindert auch, dass Anwendungen in der Whitelist auf 32- und 64-Bit-Windows-Systemen per Buffer Overflow ausgenutzt werden.

Erweiterte Ausführungskontrolle

Für zusätzlichen Schutz erlaubt McAfee Application Control die Kombination von Regeln basierend auf Dateinamen, Prozessnamen, Namen des übergeordneten Prozesses, Befehlszeilenparametern sowie Benutzernamen. Mit dieser erweiterten Ausführungskontrolle wehren Sie Angriffe ab, die Datei-Ein- und -Ausgaben umgehen, können den interaktiven Modus für System-Interpreter blockieren und die Ausnutzung durch System-Tools verhindern. Zudem steht zur Erstellung von Richtlinien der stärkere und zuverlässigere SHA-256-Algorithmus zur Verfügung.

McAfee ePolicy Orchestrator: Eine zentrale Übersicht

Die Software McAfee ePO konsolidiert sowie zentralisiert die Verwaltung und bietet eine lückenlose Gesamtübersicht der Unternehmenssicherheit. Diese preisgekrönte Plattform vernetzt McAfee Application Control mit McAfee Host Intrusion Prevention und weiteren McAfee-Sicherheitsprodukten wie Blacklists zum Malware-Schutz. Die Ein-Schritt-Installation und Aktualisierung von McAfee Application Control ist auch über das Microsoft System Center möglich.

Überwachungsmodus: Zuschauen und lernen

Im Überwachungsmodus können Sie Richtlinien für dynamische Desktop-Umgebungen erstellen, ohne eine Sperrung durch Whitelists durchführen zu müssen. Dieser Modus lässt eine schrittweise Bereitstellung von McAfee Application Control in Vorproduktionsumgebungen oder frühen Produktionsumgebungen zu, ohne dabei Anwendungen zu stören. Dank McAfee Application Control benötigen Administratoren nur eine Richtlinienerkennungsseite zur Beobachtung und Selbstfreigabe von Richtlinienanfragen.

Schutz für ältere Systeme und aktuelle Technologieinvestitionen

Möchten Sie ältere Betriebssysteme wie Microsoft Windows NT, Windows 2000 und Windows XP schützen? Obwohl diese veralteten Betriebssysteme nicht mehr von Microsoft und anderen Sicherheitsanbietern unterstützt werden, hält McAfee Application Control Ihnen den Rücken frei. Zudem unterstützt McAfee Application Control aktuelle Betriebssysteme wie Microsoft Windows 10.

Nächste Schritte

Weitere Informationen finden Sie unter **www.mcafee.com/de/products/application-control.aspx**, oder rufen Sie uns unter +49 (0)89 37 07-0 an.

McAfee
Together is power.

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