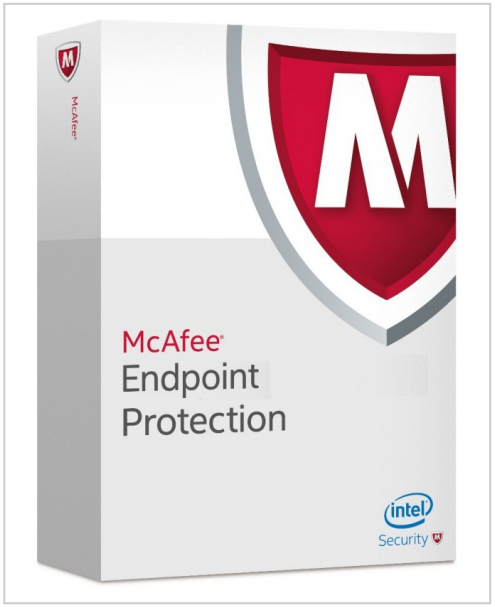
Trellix McAfee Application Control for Servers inkl. 1 Jahr Gold Support Win/Lin, Multilingual (Lizenzstaffel 1-25 User)



Artikelnummer	991170254
Gewicht	1kg
Länge	1mm
Breite	1mm
Höhe	1mm

Produktbeschreibung

McAfee Application Control for Servers

Produktbeschreibung:

Schneller, flexibler und skalierbarer Schutz vor Zero-Day- sowie hochentwickelten hartnäckigen Bedrohungen

McAfee Application Control blockiert nicht autorisierte ausführbare Dateien auf Servern, Desktop-Rechnern von Unternehmen und Geräten mit festen Funktionen.

Blockierung von Bedrohungen ohne Listenverwaltung oder Signaturaktualisierungen

Mit einem dynamischen Vertrauensmodell, lokalen und weltweiten Reputationsdaten, Echtzeit-Verhaltensanalysen und Selbstschutz von Endgeräten sparen Sie Zeit und senken die Kosten.

Abwehr unerwünschter Anwendungen

Blockieren Sie ausführbare Dateien, Bibliotheken, Treiber, Java-Apps, ActiveX-Steuerelemente, Skripts und speziellen Code.

Schutz für Systeme mit fester Funktion, ältere Systeme und moderne IT-Investitionen

Die Lösung schützt sowohl ältere Betriebssysteme wie Microsoft Windows NT, Windows 2000 und Windows XP als auch die neuesten Betriebssysteme wie Microsoft Windows 10.

Weniger Patch-Zyklen bei gleichzeitigem Speicherschutz

Sie können die regulären Patch-Zyklen beibehalten und verhindern, dass Anwendungen in der Whitelist auf Windows 32- und 64-Bit-Systemen per Buffer Overflow ausgenutzt werden.

Bedrohungsabwehr dank intelligenter Whitelists

Minimierung der Risiken durch nicht autorisierte Anwendungen und Code

Informieren Sie sich mit dem McAfee Global Threat Intelligence-Dienst, der eine Kategorisierung in "gut", "schlecht" und "unbekannt" vornimmt, sowie mithilfe der lokalen Bedrohungsdaten aus dem separat erhältlichen optionalen Modul McAfee Threat Intelligence Exchange in Echtzeit über die Bewertung jeder Datei und Anwendung in Ihrer Umgebung.

Drei Whitelist-Optionen

Die Option "Default Deny" (Standardablehnung) ermöglicht die Ausführung von Software basierend auf einer genehmigten Whitelist oder Autorisierung durch vertrauenswürdige Channel. Bei der Option "Detect and Deny" (Erkennen und Blockieren) wird die Ausführung von Software durch signaturlose Reputationsprüfung zugelassen, wohingegen bei "Verify and Deny" (Verifizieren und Ablehnen) die Ausführung von Anwendungen erlaubt wird, die in Sandbox-Tests geprüft wurden.

Gleichgewicht aus Schutz und Leistung

Zusätzliche Erkennungsmodule, darunter für Signaturen, Reputation und Echtzeit-Emulation, verringern die Anzahl der Dateien, für die eine ressourcenintensivere Malware-Sandbox-Analyse durchgeführt werden muss.

Weitere Informationen zu den Funktionen finden Sie **hier**.

Systemvoraussetzungen:

Die folgenden Angaben sind die Mindestanforderungen an die Systeme. Die tatsächlichen Anforderungen können je nach Art der Umgebung abweichen.

Microsoft Windows

Embedded: XPE, 7E, WEPOS, POS Ready 2009, WES 2009, 8, 8.1 Industry, 10

Server: 2008, 2008 R2, 2012, 2012 R2

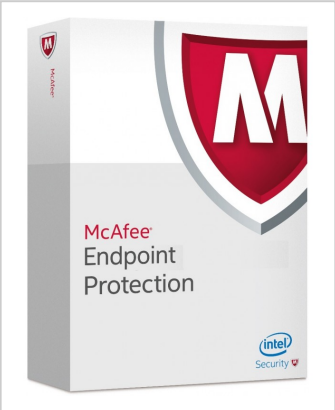
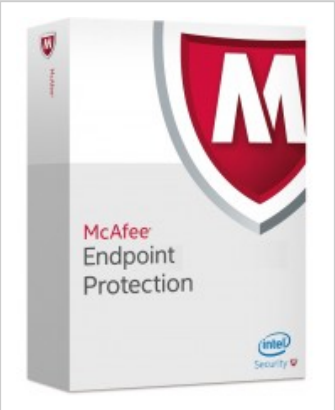
Desktop: NT, 2000, XP, Vista, 7, 8, 8.1, 10

Linux

Red Hat Enterprise Linux/CentOS 5, 6, 7

SUSE/openSUSE 10, 11

Oracle Enterprise Linux 5, 6, 7

Ubuntu 12.04

Weitere Bilder