McAfee Host Intrusion Prevention for Desktop

Verbesserter Schwachstellenschutz für Desktops und Laptops

Hauptvorteile

Besserer Schutz

- Durchsetzung von umfassendstem IPS- und Zero-Day-Bedrohungsschutz auf allen Ebenen: Netzwerk, Anwendungen und Systemausführung

Geringere Kosten

- Verringerung des Zeit- und Kostenaufwands mit einer leistungsstarken, zentralen Konsole für Bereitstellung, Verwaltung, Reporting und Audits von Vorfällen, Richtlinien und Agenten
- Verringerte Häufigkeit und Dringlichkeit von Endgeräte-Patches

Vereinfachte Compliance

- Verwaltung der Einhaltung mit leicht verständlichen, umsetzbaren Ansichten, Workflows, Ereignisüberwachung und Reporting für prompte und gründliche Untersuchungen und Analysen

Systemanforderungen

Unterstützte Betriebssysteme

- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7 SP1 (32- oder 64-Bit-Versionen): Business, Enterprise, Ultimate

Aufgrund der wachsenden Anzahl profitorientierter Internetkrimineller sowie der heutigen ausgefeilten Bedrohungen werden die Verwaltung der Sicherheit sowie die Steuerung der Internetverbindung für Desktops und Laptops in Unternehmen zu einer immer größeren Herausforderung. Auch die zunehmende Mobilität der Mitarbeiter setzt die IT-Abteilung unter Druck. Muss sie doch gewährleisten, dass Benutzer eine sichere Verbindung zum Unternehmensnetzwerk herstellen können. Darüber hinaus benötigen Unternehmen Zero-Day-Schutz vor Bedrohungen, um die notwendigen Patches ohne Zeitdruck angemessen priorisieren, testen und bereitstellen zu können.

Die Herausforderung

Virenschutz allein reicht nicht aus, da Angriffe auf Schwachstellen immer schneller erfolgen und komplexer werden. Die Lösung besteht darin, eine präventive Sicherheitsstrategie zu implementieren, die verhindert, dass Angriffe überhaupt stattfinden. Mit einem präventiven Sicherheitsansatz für Endgeräte können IT-Abteilungen sicherstellen, dass alle Endgeräte und vertraulichen Daten geschützt sind und die Geschäftskontinuität aufrechterhalten wird.

McAfee Host Intrusion Prevention for Desktop

Als zentraler Bestandteil der Intel® Security-Endgerätesicherheits-Suites bietet McAfee® Host Intrusion Prevention for Desktop herausragenden Schutz vor bekannten und unbekannten Zero-Day-Bedrohungen, indem signatur- und verhaltensbasierter Eindringungsschutz (IPS) mit einer dynamischen, statusbasierten Firewall kombiniert wird. McAfee Host Intrusion Prevention for Desktop reduziert die Häufigkeit und Dringlichkeit von Patches, gewährleistet störungsfreien Geschäftsbetrieb sowie Mitarbeiterproduktivität, schützt die Vertraulichkeit von Daten und vereinfacht die Einhaltung von Compliance-Vorschriften.

Hochentwickelter Schutz vor Bedrohungen durch unsere dynamische, statusbasierte Desktop-Firewall

Im Gegensatz zu herkömmlichen System-Firewalls, die mit festgelegten Regeln arbeiten, verfügt McAfee Host Intrusion Prevention for Desktop dank der McAfee Global Threat Intelligence (McAfee GTI)-Integration über Reputationsdaten zu Netzwerkverbindungen, sodass Desktops und Laptops vor hochentwickelten Bedrohungen wie Botnets, DDoS-Angriffen (Distributed Denial-of-Service) sowie neuem böswilligem Datenverkehr geschützt werden können, noch bevor ein Angriff beginnen kann. In Anbetracht der steigenden Anzahl hochentwickelter Bedrohungen stellt McAfee GTI einen der ausgereiftesten Schutzdienste dar.

intel Security

- Microsoft Windows Embedded Standard 7 SP1 (32- oder 64-Bit-Version)
- Microsoft Windows Vista (32- oder 64-Bit-Versionen): Business, Enterprise, Ultimate
- Microsoft Windows XP Professional (32-Bit-Version)
- Microsoft Windows XP Professional for Embedded Systems (32-Bit-Version)
- Microsoft Windows XP Embedded (32-Bit-Version)

Unterstützte Virtualisierungs-plattformen

- Citrix XenServer: 5.0, 5.5
- Citrix XenDesktop: 3.0, 4.0, 7.5, 7.6
- Citrix XenApp: 5.0, 6.0, 6.5
- Citrix Provisioning Services 6.1
- Microsoft App-V: 4.5, 4.6
- Microsoft Hyper-V Server: 2008, 2008 R2
- Microsoft Windows Server: 2008, Hyper-V 2008, 2008 R2, 2012 R2
- Microsoft VDI (Bundle)
- MED-V: 1.0, 1.0 SP1
- SCVMM: 2008, 2008 R2
- SCCM: 2007 SP2, 2007 R2
- SCOM: 2007, 2007 R2
- VMware ACE: 2.5, 2.6
- VMware ESX: 3.5, 4.0, 5.0
- VMware ESXi 5.1
- VMware Player: 2.5, 3.0, 5.0
- VMware Server: 1.0, 2.0
- VMware ThinApp: 4.0, 4.5
- VMware vSphere 4.0
- VMware View: 3.1, 4.0
- VMware Workstation: 6.5, 7.0, 8.0, 9.0
- XP-Modus unter Microsoft Windows 7: (32- und 64-Bit-Versionen)

Zusätzliche Firewall-Funktionen wie Richtlinien für Anwendungen und Speicherorte sichern Laptops sowie Desktops weiter und besonders dann ab, wenn sie außerhalb des Unternehmensnetzwerks genutzt werden.

Durchführung von Betriebssystem- und Anwendungs-Patches ist seltener, weniger dringlich und nach eigenem Zeitplan möglich

Ein großer Teil der Angriffe erfolgt innerhalb von drei Tagen nach Entdeckung einer Schwachstelle. Viele Unternehmen benötigen jedoch bis zu 30 Tage, um Patches auf allen Endgeräten zu testen und zu implementieren. McAfee Host Intrusion Prevention for Desktop schließt diese Sicherheitslücke und macht den Patch-Prozess einfacher und effizienter.

- McAfee Host Intrusion Prevention for Desktop schützt vor Zero-Day-Exploits und ungepatchten Schwachstellen. Der Schutz umfasst dabei Schwachstellen in Microsoft- sowie Adobe-Anwendungen.
- Der Schwachstellenschutz aktualisiert Signaturen automatisch, um Endgeräte vor Angriffen auf Schwachstellen zu schützen.
- Für vertrauenswürdigen Schutz können Signatur-Updates automatisch und regelmäßig heruntergeladen werden.

Endgeräte sind während des Systemstarts nicht mehr gefährdet

Weil Sicherheitsrichtlinien während des Systemstarts noch nicht greifen, sind Laptops und Server zu diesem Zeitpunkt besonders gefährdet. In dieser Phase sind Endgeräte beispielsweise für netzwerkbasierte Angriffe anfällig. Zudem könnten Sicherheitsdienste deaktiviert werden. McAfee Host Intrusion Prevention for Desktop blockiert Angriffe während dieses sensiblen Zeitfensters per Firewall und Eindringungsschutzsystem.

- Der Firewall-Schutz beim Systemstart lässt während des Startvorgangs so lange nur ausgehenden Datenverkehr zu, bis die komplette Firewall-Richtlinie greift.
- Der IPS-Schutz beim Systemstart verhindert die Deaktivierung unserer Sicherheitsdienste, bis die komplette IPS-Richtlinie durchgesetzt wurde.

Vereinfachte und optimierte Verwaltung

Für große Unternehmen ist die Erstellung und Verwaltung mehrerer Firewall- und IPS-Richtlinien eine unbedingt erforderliche, gleichzeitig aber auch mühsame und zeitaufwändige Aufgabe. Dank der in McAfee Host Intrusion Prevention for Desktop enthaltenen Richtlinien- und IPS-Kataloge wird diese Arbeit optimiert. Zudem können Sie mehrere Firewall- und IPS-Richtlinien erstellen sowie verwalten und bei Bedarf auf verschiedene Benutzergruppen anwenden sowie wiederverwenden.

Mit unserer Konsole McAfee ePolicy Orchestrator® (McAfee ePO™) zur zentralen Überwachung und Verwaltung aller Schutzmaßnahmen können Sie die Verwaltung zusätzlich optimieren und vereinfachen. Durch die vollständige Vernetzung mit McAfee ePO werden Ihre Abläufe erheblich effizienter, sodass Sie Zeit und Geld sparen.

Kompatibilität mit den größten Virtualisierungsplattformen

Dank der Virtualisierung können Sie Ihre Kosten senken und Produkte einfacher verwalten. McAfee Host Intrusion Prevention for Desktop ist mit den drei größten Virtualisierungsplattformen, d. h. VMware, Citrix und Microsoft, kompatibel.

Mehr Informationen finden Sie unter **www.mcafee.com/de/products/host-ips-for-desktop.aspx**.

McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com

62140ds_hips-desktop_1015