

McAfee SaaS Endpoint & Email Protection Suite

Unverzichtbarer Schutz für PCs, Server und E-Mails für kleine und mittlere Unternehmen

Internetkriminelle nehmen immer häufiger KMUs ins Visier und verwenden bei ihren Angriffen raffinierte E-Mail- und Web-Browser-Tricks, um ihre datenkompromittierende Malware auf Ihre PCs und Server zu bringen. McAfee® SaaS Endpoint & Email Protection Suite schützt Ihr Unternehmen vor Malware, Phishing, Spam sowie den neuesten hochentwickelten Hackerbedrohungen mit einer preisgünstigen und einfach zu verwaltenden Lösung. Sie haben keine IT-Abteilung? Kein Problem. McAfee SaaS Endpoint & Email Protection Suite wird von McAfee gehostet und verwaltet. Cloud-basierte Sicherheit bietet den effektivsten und aktuellsten Schutz, ohne dass dazu ein Verwaltungs-Server erforderlich ist – ideal für Ihr Unternehmen und Ihr Budget.

Hauptvorteile

Cloud-basierte Sicherheit

- Kein Server erforderlich
- Keine Vor-Ort-Verwaltung erforderlich
- Einfache Nutzung und Verwaltung

Weitere Vorteile

- Ständig aktive und aktuelle Sicherheit
- Rund um die Uhr verfügbarer Kunden-Support
- Nutzt McAfee Global Threat Intelligence

Wichtige Funktionen

Viren- und Spyware-Schutz

Die vollautomatische Lösung McAfee SaaS Endpoint & Email Protection Suite schützt die Computer und Server in Ihrem Netzwerk vor Viren und Spyware. Sie aktualisiert sich automatisch und sucht kontinuierlich nach Bedrohungen, die sich in Dateien und Programmen, E-Mails und Kommunikationsvorgängen von innerhalb und außerhalb des Netzwerks sowie in Webseiten verbergen. Die Lösung erkennt schnell Viren, Spyware, Würmer, Trojaner und andere potenzielle Bedrohungen, die von Geräten, Wechseldatenträgern oder über das Netzwerk, z. B. über E-Mails, übertragen wurden.

Bei jedem Zugriff auf eine Computerdatei wird diese mithilfe des Viren- und Spyware-Schutzes gescannt, um sicherzugehen, dass sie frei von potenziellen Bedrohungen ist.

Desktop-Firewall-Schutz

Die McAfee-Desktop-Firewall errichtet eine Barriere zwischen Computern und dem Internet bzw. anderen Computern in Ihrem lokalen Netzwerk. Dabei überprüft sie den Kommunikationsverkehr im Hintergrund auf verdächtige Aktivitäten. Bei Bedarf werden erforderliche Maßnahmen ergriffen, z. B. die Aktion blockiert.

Browser-Sicherheit

McAfee SaaS Endpoint & Email Protection Suite nutzt McAfee SiteAdvisor® zur Anzeige von Informationen zu Webseiten, um Benutzer vor webbasierten Bedrohungen zu schützen. Benutzer können während des Surfens oder bei Suchvorgängen Sicherheitsbewertungen und Sicherheitsberichte zur jeweiligen Webseite anzeigen. Mithilfe der Web-Filterung können Administratoren den Zugriff auf Webseiten basierend auf ihrer Sicherheitsbewertung, Inhaltskategorie oder bestimmten URLs kontrollieren.

Cloud-basierte Dienste

E-Mail-Schutz

Die Dienste werden auf unternehmensgerechten McAfee-Rechenzentren gehostet. Die E-Mail-Schutzfunktionen erkennen und entfernen Bedrohungen bereits auf unserem Server, also noch bevor sie Ihr Netzwerk erreichen. Dadurch wird riskanter E-Mail-Verkehr vermieden und Ihre Netzwerkbandbreite weniger belastet.

Die Filterfunktion für ein- und ausgehende E-Mails schützt Ihre Mitarbeiter und Kunden vor allen E-Mail-basierten Malware-Varianten. Sobald Directory-Harvest-Angriffe, Spam, Phishing-Angriffe, Viren und andere per E-Mail übertragene Bedrohungen in Nachrichten und Anhängen erkannt werden, werden die entsprechenden Nachrichten blockiert oder isoliert.

Die Funktion für unterbrechungsfreie E-Mail-Nutzung gewährleistet, dass Ihre Geschäftsabläufe auch dann funktionieren, wenn Ihr E-Mail-Netzwerk ausfällt. Dazu bietet die Lösung von jedem beliebigen Browser aus Zugriff auf die E-Mails der letzten 60 Tage.

Webbasierte Verwaltungskonsole

Die integrierte Web-Verwaltungskonsole stellt von jedem beliebigen Browser mit Internet-Zugriff aus eine umfassende Übersicht über die Sicherheitslage aller Ihrer Endgeräte bereit.

- Die zentrale Konsole McAfee SecurityCenter bietet eine einfache Möglichkeit zur Verwaltung der Sicherheitsfunktionen aller Ihrer Geräte. Dazu benötigen Sie weniger als 15 Minuten am Tag.
- Sie können diese Konsole jederzeit mit jedem Internet-fähigen Gerät aufrufen.
- Sicherheitsberichte können in regelmäßigen Abständen erstellt und per E-Mail zugestellt werden.
- Definieren Sie Sicherheitsrichtlinien, und konfigurieren Sie sie für einzelne Geräte oder Gerätegruppen unabhängig von deren Standort.

Spezifikationen

Die folgenden Angaben sind Mindestanforderungen. Wo zutreffend, stehen empfohlene Anforderungen in Klammern. Die tatsächlichen Anforderungen können je nach Art der Umgebung abweichen.

Systemanforderungen

- Intel Pentium-Prozessor oder eine damit kompatible Architektur
- 1 GB (2 GB empfohlen)

Viren- und Spyware-Schutz

Client-Computer:

- Microsoft Windows 8 (32-Bit- oder 64-Bit-Versionen)
- Microsoft Windows 7 Ultimate, Professional, Home Premium, Home Basic (32-Bit- oder 64-Bit-Versionen)
- Microsoft Windows Vista Ultimate, Enterprise, Business, Home Premium, Home Basic (32-Bit- oder 64-Bit-Versionen)
- Microsoft Windows XP Home oder Professional (32-Bit- oder 64-Bit-Versionen) mit SP2 oder SP3; Desktop-Firewall-Schutz wird bei 64-Bit-Versionen von Windows XP nicht unterstützt

Server:

- Microsoft Windows Server 2012
- Microsoft Windows Server 2011: Small Business Server
- Microsoft Windows Server 2008 R2: Standard, Enterprise
- Microsoft Windows Server 2008 (32-Bit- oder 64-Bit-Version): Standard, Enterprise, Small Business Server
- Microsoft Windows Small Business Server 2003 R2
- Microsoft Windows Server 2003 mit Service Pack (32-Bit und 64-Bit-Version): Standard, Enterprise, Small Business Server

Desktop-Firewall-Schutz

- Wie oben, mit den unten angegebenen Ausnahmen
- Nicht unterstützt unter Microsoft Windows XP Professional 64-Bit

Browser-Schutz und Web-Filterung

- Wie oben, mit den unten angegebenen Ausnahmen
- Keine Unterstützung für Apple Safari für Windows

E-Mail-Sicherheitsdienst

- Sie benötigen eine eigene E-Mail-Domain (etwa musterdomain.com) mit einer statischen IP-Adresse oder einem Host-Namen, der in eine IP-Adresse aufgelöst wird, sowie einen dedizierten E-Mail-Server, entweder im eigenen Haus oder bei einem ISP.
- Die Aktivierung beginnt mit einer einfachen Mail eXchange-Eintragsumleitung (MX).

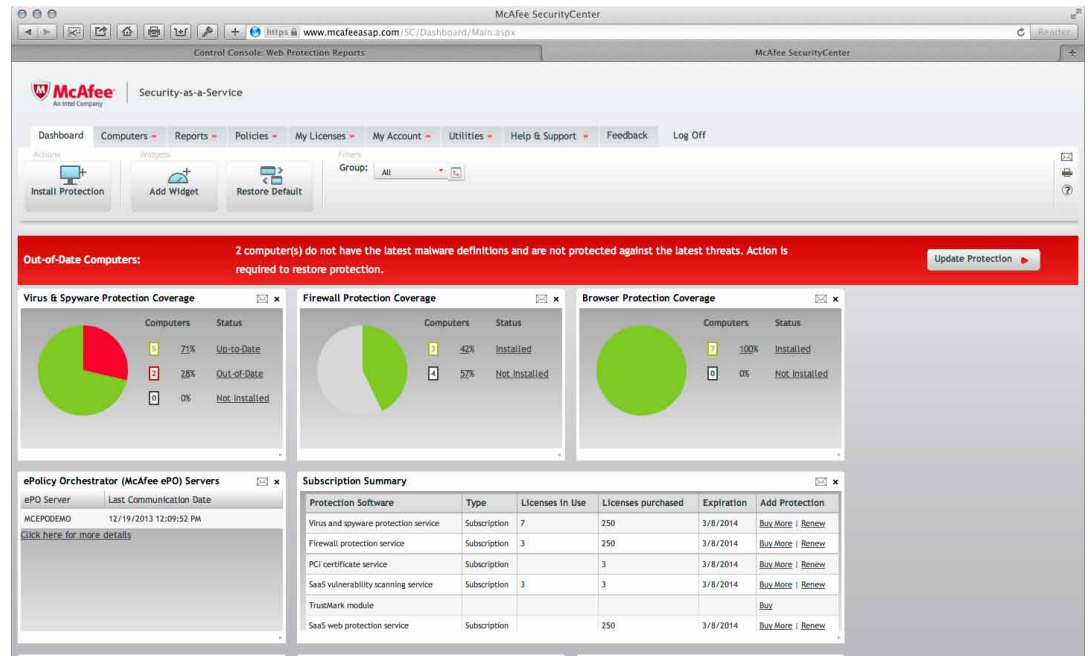


Abbildung 1. McAfee SecurityCenter bietet zentrale Verwaltung von Installationen, Berichten und Richtlinien.

Kostenlose 30-Tage-Testversion

Machen Sie sich mit einer kostenlosen 30-Tage-Testversion mit den Vorteilen der Cloud-basierten McAfee-Sicherheitslösungen vertraut. Weitere Informationen erhalten Sie unter www.mcafee.com/de/small-business-security/saas-endpoint-and-email-protection.html.

Partner-Services für McAfee-Lösungen

McAfee-Partner bieten professionelle Services von der Installation bis zur Verwaltung. Wenden Sie sich an McAfee, um zu erfahren, welche Services zur Verfügung stehen.

Weitere Informationen

Weitere Informationen finden Sie unter www.mcafee.com/de/small-business-security/index.html.



McAfee GmbH
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.mcafee.com/de

McAfee, das McAfee-Logo und SiteAdvisor sind Marken oder eingetragene Marken von McAfee, Inc. oder der Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer. Die in diesem Dokument enthaltenen Produktpläne, Spezifikationen und Beschreibungen dienen lediglich Informationszwecken, können sich jederzeit ohne vorherige Ankündigung ändern und schließen alle ausdrücklichen oder stillschweigenden Garantien aus. Copyright © 2014 McAfee, Inc. 60709ds_saas-endpt-email-protect_0114_fnl_ETMG