McAfee Complete Endpoint Protection – Business

Intelligente vernetzte Schutzmaßnahmen mit einfacher zentraler Verwaltung

Hauptvorteile

- Bestbewerteter, umfassender sowie mehrschichtiger Schutz mit intelligentem und gemeinschaftlichem Endgeräteschutz, Eindringungsschutz und Firewall für Desktop-PCs und Laptops, Gerätesteuerung, Verschlüsselung und mehr
- Eindämmung vor der Ausführung zur Isolierung von Ransomware und hochentwickelten Bedrohungen, bevor diese das System infizieren können; Verhaltensklassifizierung in Kombination mit Machine Learning vereinfacht die Identifizierung von Zero-Day-Malware und verbessert die Erkennung von Bedrohungen
- Einheitliche Verwaltung für alle Ihre Endgeräte: PCs, Macs und Linux-Systeme
- Umsetzbare Bedrohungsforensik in verständlicher Sprache für besseres Verständnis und schnelle Maßnahmen bei hochentwickelten Bedrohungen
- Absicherung vertraulicher Daten auf allen Geräten, Wechselspeichermedien und Cloud-Speichern beim sicheren Dateiaustausch

Schützen Sie Ihre Endgeräte mit McAfee® Complete Endpoint Protection – Business. Diese preisgünstige Komplettlösung nutzt gemeinschaftlich weltweit und lokal erfasste Bedrohungsdaten, um hochentwickelte Bedrohungen abzuwehren. Sie schützt Ihre Daten mit Verschlüsselung und kann mithilfe von Endgeräteschutzmaßnahmen wie der dynamischen Eindämmung von Anwendungsprozessen und Machine Learning für Desktop-PCs sowie Laptops gefährliche Zero-Day-Exploits abwehren. Dank der integrierten E-Mail-, Web- und kooperativen Endgeräteschutzmaßnahmen werden zudem Phishing- sowie mehrstufige Angriffe blockiert. Zu guter Letzt reduziert die Verwaltung über die einheitliche Web-Konsole den täglich bei IT-Mitarbeitern anfallenden Verwaltungsaufwand und ermöglicht die schnelle Reaktion auf erkannte Bedrohungen.

Die McAfee Complete Endpoint Protection – Business-Suite ermöglicht wachsenden Unternehmen die Implementierung optimaler Internetsicherheit – mit sofort einsatzbereiter Installation sowie schneller Reaktion auf Probleme. Mit dieser zentralen Lösung können Sie PCs, Macs, Linux-Systeme und vieles mehr abdecken. Sie verringert die Komplexität, senkt die Kosten und bietet Schutz vor Rootkits, gezielten Web- und E-Mail-Angriffen sowie hochentwickelten hartnäckigen Bedrohungen. Die Leistungsfähigkeit, Effizienz und intuitive Verwaltung der Suite erhalten Sie nur von McAfee, dem Marktführer für Endgerätesicherheit.

Schutz vor hochentwickelten Bedrohungen

Ein einziges infiziertes System kann Ihr Unternehmen lahmlegen. Virenschutz allein ist nicht mehr in der Lage, die heutigen raffinierten Bedrohungen abzuwehren. Beim Schutz vor Bedrohungen ist McAfee Complete Endpoint Protection – Business die beste Entscheidung. Dank unseres Endgeräte-Frameworks können Schutzmaßnahmen gemeinsam Daten analysieren, Maßnahmen gegen neue Bedrohungen ergreifen sowie in Echtzeit forensische Daten austauschen.

McAfee – Ein Branchenführer

- Führender Anbieter bei Forrester Wave™ für Endgerätesicherheits-Suites, 4. Quartal 2016[1]
- McAfee Endpoint Security wird von NSS Labs empfohlen[2]

McAfee bietet dank mehrschichtiger Sicherheitsmaßnahmen schnellen Schutz, Erkennung und Beseitigung von Malware. Diese Maßnahmen umfassen unter anderem intelligente Schutzmaßnahmen, die gemeinsam hochentwickelte Bedrohungen abwehren, dynamische Eindämmung von Anwendungsprozessen, Machine Learning für Desktop-PCs und Laptops sowie Gerätesteuerung und Verschlüsselung.

McAfee bietet mehrere Schutzebenen. Dank hochentwickelter Verschlüsselung können Sie vertrauliche Informationen automatisch absichern und dadurch unbefugten Zugriff auf PCs, Macs, Laptops, virtuelle Maschinen, Wechselmedien und Cloud-Speicher wie Box, Dropbox, Google Drive und Microsoft OneDrive verhindern. Schützen Sie Ihre wichtigsten Ressourcen, ohne dabei die Systemleistung zu beeinträchtigen. Mit der zentralen Web-Verwaltungsplattform McAfee® ePolicy Orchestrator® (McAfee ePO™) können Sie Richtlinien auf einfache Weise verwalten und durchsetzen.

Mit McAfee Global Threat Intelligence können Sie mehr sehen, mehr wissen und Ihr Unternehmen besser schützen. Diese Cloud-basierte Lösung zeigt Ihnen das volle Spektrum neuer und zukünftiger Bedrohungen in Echtzeit auf allen Vektoren: Dateien, Internet, Nachrichten und Netzwerke. Dank mehr als 100 Millionen Bedrohungssensoren in über 120 Ländern sowie pro Tag mehr als 45 Milliarden Abfragen, mehr als 1,5 Millionen untersuchten Dateien sowie 1 Million analysierten URLs bieten wir die besten auf dem Markt verfügbaren weltweiten Bedrohungsdaten.

Einfache Bereitstellung und zentrale Verwaltung

Möglicherweise gibt es nicht in allen Ihren Niederlassungen eigene Sicherheitsexperten. Deshalb ist Einfachheit wichtig. Ihre Sicherheit lässt sich mit nur vier Mausklicks installieren und ist anschließend sofort einsatzbereit. Das Sicherheits-Management wird dank McAfee ePO vereinfacht, das einen zentralen Überblick über die Sicherheitslage sowie die Verwaltung der Richtlinien für alle Ihre Geräte ermöglicht.

Starke und effektive Leistung

Dank unseres erweiterbaren Endgeräte-Frameworks können Sie Redundanzen finden und beseitigen, um die betriebliche Effizienz Ihrer IT zu verbessern. Auch die Scans sind auf Hochleistung optimiert: Die Scan-Vorgänge finden in Leerlaufzeiten statt und sind selbstlernend sowie adaptiv, wobei das Verhalten von Dateien und Prozessen berücksichtigt wird, damit höchste Leistung bereit und verfügbar ist, wenn maximale Scan-Intensität erforderlich ist.

Umfang von McAfee Complete Endpoint Protection – Business

Malware-Schutz (PCs, Macs, Linux, virtuelle Maschinen)
McAfee Endpoint Security Kommuniziert mit mehreren Endgeräteschutz-Technologien, um in Echtzeit neue und hochentwickelte Bedrohungen zu analysieren und gemeinsame Maßnahmen zu ergreifen. Dadurch werden die Bedrohungen blockiert und schnell abgewehrt, noch bevor sie Ihre Systeme oder Benutzer beeinträchtigen können.
Dynamische Eindämmung von Anwendungsprozessen Überprüft auf sichere Weise das Verhalten von Prozessen und dämmt Bedrohungen wie Greyware, Ransomware sowie „Patient Zero"-Infektionen ein; benötigt keine Cloud-Verbindung.

Real Protect

- Erkennt und blockiert dank Echtzeit-Verhaltensanalyse sowie Machine Learning hochentwickelte Bedrohungen und Zero-Day-Angriffe. Dabei werden Funktionen noch vor der Ausführung extrahiert sowie Verhaltens- und Speicheranalysen nach der Ausführung durchgeführt, um Bedrohungen zu überführen.
- Schützt vor Malware mit Sandbox-Erkennung, indem die gefährlichen Funktionen ausgeführt sowie in Echtzeit analysiert werden, damit die dynamische Eindämmung von Anwendungsprozessen anschließend automatisch böswillige Aktionen blockiert, bevor die Malware ein System infizieren kann.

Application Control

Verhindert die Installation sowie Ausführung unerwünschter Anwendungen und Malware. Dies hat dabei nur minimale Beeinträchtigungen für Systemleistung, Benutzer oder Administratoren zur Folge.

Eindringungsschutz und Firewall für Desktop-PCs

- Wehrt unbekannte sowie Zero-Day-Bedrohungen ab und schließt neue Schwachstellen.
- Reduziert die Dringlichkeit von Patches.

Global Threat Intelligence

- Wehrt anhand von Echtzeit-Bedrohungsanalysen von weltweit Millionen Sensoren neue und zukünftige Bedrohungen aus allen Vektoren ab.
- Erstellt benutzerdefinierte Kontrollen, um Exploits, Angriffe auf den Arbeitsspeicher sowie Bedrohungen zu blockieren, die höhere Berechtigungen einfordern.

Web- und E-Mail-Sicherheit

Web-Kontrolle mit URL-Filterung und sicherer Suche

- Warnt Benutzer vor gefährlichen Webseiten, noch bevor diese geladen werden, und hält auf diese Weise Compliance-Anforderungen ein.
- Setzt Richtlinien für die Internetnutzung durch, indem der Zugriff auf Webseiten erlaubt oder blockiert wird.

Malware- und Spam-Schutz für E-Mails

- Schützt die E-Mail-Server und fängt Malware ab, bevor diese in den Posteingang der Benutzer gelangt.
- Erkennt, bereinigt und blockiert Malware für Microsoft Exchange- und Lotus Domino-Server mit McAfee Security for Email Servers.

Datenschutz

Gerätesteuerung

Verhindert den Verlust sensibler Daten durch die Einschränkung der Wechselspeichermedien-Nutzung.

Verschlüsselung für vollständiges Laufwerk, Dateien, Ordner, Wechselmedien und Cloud-Speicher

Schützt die vertraulichen Informationen auf PCs, Macs, Laptops, Netzwerk-Servern, Wechselspeichermedien und in Cloud-Speicherdiensten.

Verwaltung

McAfee ePO

- Verwaltet Richtlinien, Compliance-Vorgaben sowie Berichte über eine einzige zentrale Konsole.
- Vereinfacht mithilfe von plattformübergreifenden Richtlinien die Verwaltung in gemischten Betriebssystemumgebungen.

Den gesamten Bedrohungszyklus im Griff

Mit McAfee Complete Endpoint Protection – Business sind Sie dauerhaft geschützt und flexibel. Die Lösung stellt ein kollaboratives Sicherheits-Framework bereit, das die Komplexität von Endgeräte-Sicherheitsumgebungen verringert und bessere Leistung bietet, um Ihre Produktivität sowie die Ihrer Benutzer zu schützen. Außerdem gewährleistet McAfee Complete Endpoint Protection – Business den Überblick über hochentwickelte Bedrohungen, damit die Erkennung und Reaktion beschleunigt werden. Weltweite, Cloud-basierte Bedrohungsdaten stellen sicher, dass bei neuen und hochentwickelten Bedrohungen schnelle und effektive Maßnahmen bereitstehen sowie für Administratoren umsetzbare Forensik zur Verfügung steht. Zu guter Letzt bietet die zentrale webbasierte Verwaltung, die die Integration anderer Drittanbieter- und McAfee®-Produkte ermöglicht, eine erhebliche Entlastung für IT-Teams, die durch den Einsatz mehrerer Lösungen überlastet sind. Nun können sie auf einfachere Weise den Bedrohungszyklus anzeigen, ihn kontrollieren und reagieren. Weitere Informationen hierzu finden Sie unter **www.mcafee.com/de/products/complete-endpoint-protection-business.aspx**.

Funktionsweise der hochentwickelten Bedrohungsschutz-Maßnahmen

Technologie	Beschreibung	Aufgaben
McAfee Endpoint Security 10	Ermöglicht die Kommunikation zwischen verschiedenen Bedrohungsschutz-Maßnahmen zur Erkennung von Zusammenhängen zwischen scheinbar separaten Ereignissen als einem gezielten Angriff.	• Die Bedrohungsschutz-Maßnahmen kommunizieren sowie lernen miteinander und informieren einander über neue Bedrohungen. • Adaptive und intelligente Scans nutzen Beobachtungen aus mehreren Quellen, um Bedrohungen zu erkennen und einander in Echtzeit über neue Angriffsformen zu informieren. • Die Schutzmaßnahmen nutzen lokale sowie weltweite Bedrohungsdaten. • Bei verdächtigen Anwendungen und Prozessen werden automatisch Aktionen vorgenommen sowie schnell eskaliert und parallel dazu andere Schutzmaßnahmen sowie die weltweite Community informiert.
McAfee Threat Intelligence Exchange*	Bietet erweiterte Bedrohungsdaten aus weltweiten Quellen sowie von Drittanbietern und erfasst lokale Bedrohungsdaten aus Echtzeit- und Verlaufsereignissen.	• Sicherheitskomponenten erhalten über Endgeräte, Gateways und andere Sicherheitskomponenten zusätzliche Informationen über Bedrohungen, die Unternehmen weltweit angreifen. • Bedrohungsdetails, die bei Malware-Zwischenfällen erfasst wurden, werden innerhalb von Millisekunden über den McAfee Data Exchange Layer übertragen. Dadurch erreichen sie alle Endgeräte und ermöglichen die präventive Immunisierung gegen Bedrohungen. • Ermöglicht die Anpassung der Bedrohungsdaten, z. B. Listen von Herausgeberzertifikaten, Datei-Hash-Werte und Risikotoleranz-Entscheidungen, an die Anforderungen des Unternehmens.
McAfee Active Response*	Erweitert Reaktionsmöglichkeiten bei Zwischenfällen mit detaillierten aktuellen, interaktiven und fortlaufenden Untersuchungsergebnissen sowie Analysen.	• Erfasst und überwacht automatisch den Kontext sowie den Systemstatus auf Änderungen, die auf Angriffsindikatoren hinweisen, findet „ruhende“ Angriffskomponenten und sendet Erkenntnisse an Analyse-, Operations- und Forensik-Teams. • Ermöglicht Anpassungen an veränderte Angriffsmethoden und automatisiert Datenerfassung, Warnungen sowie Reaktionen bei wichtigen Elementen und die Anpassung von Workflows. • Kontinuierliche und persistente Kollektoren lösen bei der Erfassung von Angriffen Ereignisse aus und benachrichtigen Administratoren und Systeme über die Angriffsaktivitäten.
McAfee Application Control	Blockiert nicht autorisierte ausführbare Dateien auf Desktop-PCs von Unternehmen und Geräten mit festen Funktionen.	• Nutzt ein Vertrauensmodell sowie innovative Sicherheitsfunktionen, die hochentwickelte, hartnäckige Bedrohungen vereiteln, ohne Signaturaktualisierungen oder zeitintensive Listenverwaltung zu erfordern. • Integriert McAfee Global Threat Intelligence und bietet Benutzern die Möglichkeit, „bekannt gute“ Anwendungen sowie Code zuzulassen und gleichzeitig „als gefährlich bekannte“ sowie „unbekannte gefährliche“ Anwendungen zu blockieren. • Bei einer Bereitstellung mit McAfee Threat Intelligence Exchange wird die Whitelist um lokale Bedrohungsdaten ergänzt, um unbekannte und gezielte Malware sofort abzuwehren. McAfee Threat Intelligence Exchange koordiniert sich mit McAfee Advanced Threat Defense, um das Verhalten unbekannter Anwendungen in einer Sandbox dynamisch zu analysieren und alle Endgeräte automatisch gegen die neu entdeckte Malware zu immunisieren.

* McAfee Threat Intelligence Exchange, McAfee Active Response und McAfee Advanced Threat Defense sind optionale Funktionen, die für McAfee Complete Endpoint Protection-Kunden separat erhältlich sind.

1. The Endpoint Security Advantage, Featuring The Forrester Wave™: Endpoint Security Suites (Vorteil durch Endgerätesicherheit, ergänzt um The Forrester Wave™ für Endgerätesicherheits-Suites), 4. Quartal 2016 **www.mcafee.com/de/resources/reports/rp-endpoint-security-advantage-forrester.pdf**
2. Gruppentest 2017 von NSS Labs zu erweitertem Endgeräteschutz (Advanced Endpoint Protection, AEP), **www.mcafee.com/de/resources/reviews/nss-labs-aep-endpoint-security.pdf**

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/de