



# McAfee Complete Endpoint Protection – Enterprise

## Intelligente, vernetzte Schutzmaßnahmen für den gesamten Bedrohungszyklus

### Hauptvorteile

- Verhinderung von „Patient-Zero“-Infektionen und Abwehr von Sandbox-bewusster Malware, indem Bedrohungen nachverfolgt und eingedämmt werden, ohne die Sicherheit oder den störungsfreien Geschäftsbetrieb zu gefährden
- Bestbewerteter, umfassender sowie mehrschichtiger Schutz mit intelligentem und gemeinschaftlichem Endgeräteschutz, Eindringungsschutz und Firewall für Desktop-PCs und Laptops, Gerätesteuerung und mehr
- Einheitliche Verwaltung für alle Ihre Endgeräte: PCs, Macs, Linux-Systeme und virtuelle Maschinen
- Reduzierung der Angriffsfläche bei Anwendungen sowie Senkung des Zeit- und Arbeitsaufwands dank dynamischen Whitelists

Endgerätesicherheit sollte Ihr Unternehmen unterstützen und nicht behindern. Schützen Sie das Unternehmen, und unterstützen Sie die Produktivität Ihrer Mitarbeiter. Stark, einfach und schnell: Die McAfee® Complete Endpoint Protection – Enterprise-Suite liefert einen Echtzeitüberblick über die Sicherheitslage sowie Risiken und bietet einheitliche Verwaltung. Nutzen Sie fortschrittlichen Bedrohungsschutz, der auf lokale sowie weltweite Bedrohungsdaten zurückgreift und Ihre Systeme sowie Daten mithilfe von Anwendungskontrollen, Anwendungsprozess-Eindämmung und verhaltensbasiertem Eindringungsschutz vor komplexen, verborgenen Bedrohungen schützt – in einer einfach zu verwaltenden und integrierten Lösung.

McAfee Complete Endpoint Protection – Enterprise-Suite erleichtert die Bereitstellung von Sicherheitsmaßnahmen – von der sofort einsatzbereiten Installation bis zur schnellen Reaktion auf Probleme. Die konsolidierte Lösung deckt alle Geräte in Ihrem Unternehmen ab: PCs, Macs, Linux-Systeme, virtuelle Maschinen und mehr. Sie vereinfacht die Verwaltung, senkt die Kosten und schützt Ihre Endgeräte effektiv vor Rootkits, gezielten Web- und E-Mail-Angriffen sowie hochentwickelten hartnäckigen Bedrohungen. Die Lösung von Intel Security, dem Marktführer bei Endgerätesicherheit, bietet leistungsfähigen, effizienten Schutz sowie optimale Verwaltungsmöglichkeiten.

### Schutz vor hochentwickelten Bedrohungen

Beim Schutz vor Bedrohungen ist McAfee Complete Endpoint Protection – Enterprise die beste Entscheidung. Unsere dynamische Anwendungsprozess-Eindämmung schützt Systeme vor den neuesten Formen von Greyware, Ransomware, „Patient-Zero“-Infektionen sowie anderen hochentwickelten Bedrohungen, bevor diese Zugriff auf Ihre Systeme erlangen. Diese Funktion untersucht das Verhalten potenzieller Bedrohungen, ohne dabei die Sicherheit Ihrer Systeme zu gefährden. Sie haben auch die Möglichkeit, eigene Regeln für die Zugangskontrolle zu erstellen. Da diese ressourcenschonende Funktion keine Cloud-Verbindung benötigt, können Sie auch Benutzer schützen, die nicht mit Ihrem Netzwerk verbunden sind.

## Hauptvorteile (Fortsetzung)

- Umsetzbare Bedrohungsforensik in verständlicher Sprache für besseres Verständnis und schnelle Maßnahmen bei hochentwickelten Bedrohungen
- Verwaltung von Risiken durch Konzentration von Sicherheitsmaßnahmen an den gefährdeten Stellen

## Intel Security – Ein Branchenführer

- Seit 13 Jahren in Folge führend im Gartner Magic Quadrant für Endgeräteschutz-Plattformen. (Gartner)<sup>1</sup>

Intel Security bietet dank mehrschichtiger Sicherheitsmaßnahmen schnellen Schutz, Erkennung und Beseitigung von Malware. Diese Maßnahmen umfassen unter anderem intelligente und kooperative Schutzmaßnahmen sowie Eindringungsschutz-Systeme und Firewalls für Desktop-PCs und Laptops, Gerätesteuerung und mehr. Dank Anwendungskontrolle mit intelligenten Whitelists werden Benutzer vor schädlichen Anwendungen sowie Code aus Zero-Day-Bedrohungen oder hochentwickelten hartnäckigen Bedrohungen (Advanced Persistent Threats, APTs) geschützt.

Mit McAfee Global Threat Intelligence (GTI) 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. Erweitern Sie Ihre weltweiten Bedrohungsdaten mit lokalen Daten von McAfee GTI, um Bedrohungen sofort nach ihrem Auftauchen abzuwehren. 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 bietet Intel Security die besten auf dem Markt verfügbaren weltweiten Bedrohungsdaten.

## Schnelle und intelligente Scans

Zielgerichtete Scans und Maßnahmen ermöglichen ein Sicherheitsniveau, das den reibungslosen Geschäftsbetrieb

bei minimalen Ausfallzeiten gewährleistet. Die hervorragende Leistung auf allen Plattformen wird durch die intelligenten Scan- und Speicherverwaltungstechnologien möglich, die die CPU- und Arbeitsspeichernutzung optimieren. Dank McAfee Application Control und der signaturlosen Aktualisierungen profitieren Sie von der sehr niedrigen CPU- sowie Arbeitsspeichernutzung und vermeiden gleichzeitig übermäßige Scans und DAT-Aktualisierungszyklen.

## Einfache Bereitstellung und zentrale Verwaltung

Mit nur vier Mausklicks und in nur 20 Minuten ist Ihre Sicherheit einsatzbereit. Die einheitliche Echtzeitverwaltung mit McAfee® ePolicy Orchestrator® (McAfee ePO™) ermöglicht dank der zentralen Benutzeroberfläche optimierte Richtlinienverwaltung auf allen Ihren Geräten.

Dank eines dynamischen Vertrauensmodells erweitert McAfee Application Control die Whitelist dynamisch, ohne dass dazu arbeitsintensive Listenverwaltung notwendig ist.

## Anzeige, Verwaltung und Reaktion auf den Bedrohungszyklus

McAfee Complete Endpoint Protection – Enterprise bietet starke präventive Sicherheitsfunktionen, die Ihr Unternehmen vor modernen komplexen Bedrohungen aus allen Vektoren schützen.

## 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.	<ul style="list-style-type: none"><li>• Die dynamische Anwendungsprozess-Eindämmung schützt vor Ransomware, Greyware und „Patient-Zero“-Infektionen, bevor diese Zugriff auf Ihre Systeme erhalten.</li><li>• Die Bedrohungsschutz-Maßnahmen kommunizieren sowie lernen miteinander und informieren einander über neue Bedrohungen.</li><li>• Adaptive und intelligente Scans nutzen Beobachtungen aus mehreren Quellen, um Bedrohungen zu erkennen und einander in Echtzeit über neue Angriffsformen zu informieren.</li><li>• Die Schutzmaßnahmen nutzen lokale sowie weltweite Bedrohungsdaten.</li><li>• Bei verdächtigen Anwendungen und Prozessen werden automatisch Aktionen vorgenommen sowie schnell eskaliert und parallel dazu andere Schutzmaßnahmen sowie die weltweite Community informiert.</li></ul>

Technologie	Beschreibung	Aufgaben
<b>McAfee Threat Intelligence Exchange</b>	Bietet erweiterte Bedrohungsdaten aus weltweiten Quellen sowie von Drittanbietern und erfasst lokale Bedrohungsdaten aus Echtzeit- und Verlaufereignissen.	<ul style="list-style-type: none"> <li>• Sicherheitskomponenten erhalten über Endgeräte, Gateways und andere Sicherheitskomponenten zusätzliche Informationen über Bedrohungen, die Unternehmen weltweit angreifen.</li> <li>• Bedrohungsdetails, die bei Malware-Zwischenfällen erfasst wurden, werden innerhalb von Millisekunden über den Data Exchange Layer übertragen. Dadurch erreichen sie alle Endgeräte und ermöglichen die präventive Immunisierung gegen Bedrohungen.</li> <li>• Ermöglicht die Anpassung der Bedrohungsdaten, z. B. Listen von Herausgeberzertifikaten, Datei-Hash-Werte und Risikotoleranz-Entscheidungen, an die Anforderungen des Unternehmens.</li> </ul>
<b>McAfee Active Response</b>	Erweitert Reaktionsmöglichkeiten bei Zwischenfällen mit detaillierten aktuellen, interaktiven und fortlaufenden Untersuchungsergebnisse und Analysen.	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Ermöglicht Anpassungen an veränderte Angriffsmethoden und automatisiert Datenerfassung, Warnungen sowie Reaktionen bei wichtigen Elementen und die Anpassung von Workflows.</li> <li>• Kontinuierliche und persistente Kollektoren lösen bei der Erfassung von Angriffen Ereignisse aus und benachrichtigen Administratoren und Systeme über die Angriffsaktivitäten.</li> </ul>
<b>McAfee Application Control</b>	Blockiert nicht autorisierte ausführbare Dateien auf Desktop-PCs von Unternehmen und Geräten mit festen Funktionen.	<ul style="list-style-type: none"> <li>• Nutzt ein dynamisches Vertrauensmodell sowie innovative Sicherheitsfunktionen, die hochentwickelte, hartnäckige Bedrohungen vereiteln, ohne Signaturaktualisierungen oder zeitintensive Listenverwaltung zu erfordern.</li> <li>• Integriert McAfee Global Threat Intelligence und bietet Benutzern die Möglichkeit „bekannt gute“ Anwendungen sowie Code zuzulassen und gleichzeitig „als gefährlich bekannte“ sowie „unbekannte gefährliche“ zu blockieren.</li> <li>• 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.</li> </ul>

Hinweis: McAfee Threat Intelligence Exchange, McAfee Active Response und McAfee Advanced Threat Defense sind optionale Module, die für Endpoint Protection-Kunden separat erhältlich sind.

### Die integrierte Intel Security-Architektur

Mit der McAfee Complete Endpoint Protection – Enterprise-Suite können Sie Ihre Sicherheits- sowie Risikolage bei geringeren Kosten und höherer Flexibilität optimieren. Mithilfe eines integrierten Sicherheits-Frameworks – und einer kooperativen erweiterbaren Endgeräte-architektur – können Sie Redundanzen beseitigen, um die Verwaltung zu vereinfachen und Ihre Effizienz bei der Reaktion auf Zwischenfälle zu verbessern. Zudem können Sie auch die Verwaltung zentralisieren, den Sicherheitsaufwand verringern und ein Framework nutzen, auf dem Sie aufbauen

können – heute und morgen. Sie können Schutzmaßnahmen sowie Prozesse zum Vorfall-Management optimieren und automatisieren, um den Sicherheitsaufwand sowie Ineffizienzen zu verringern. Dank der Echtzeit-Sicherheitsverwaltung und der unerreichten weltweiten Bedrohungsdaten unterstützt Intel Security Sie bei der schnellen und einfachen Erkennung, Priorisierung und Behebung von Risiken für Ihr Unternehmen. Weitere Informationen hierzu finden Sie unter [www.mcafee.com/de/products/complete-endpoint-protection-enterprise.aspx](http://www.mcafee.com/de/products/complete-endpoint-protection-enterprise.aspx).

## Umfang der McAfee Complete Endpoint Protection – Enterprise-Suite

### 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.
- Bietet branchenweit führenden, unternehmensgerechten Malware-Schutz mit integriertem Schutz vor Zero-Day-Bedrohungen.
- Ermöglicht die Integration hochentwickelter Bedrohungsschutzlösungen wie McAfee Active Response.

#### Dynamische Anwendungsprozess-Eindämmung

- Überprüft auf sichere Weise das Verhalten von Prozessen und dämmt Bedrohungen wie Ransomware, Greyware und „Patient-Zero“-Infektionen ein; benötigt keine Cloud-Verbindung.

#### Anwendungskontrolle

- Verhindern Sie 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 und Laptops

- Wehren Sie unbekanntes sowie Zero-Day-Bedrohungen ab, und schließen Sie neue Schwachstellen.
- Reduzieren Sie die Dringlichkeit von Patches.
- Erstellen Sie benutzerdefinierte Kontrollen, um Exploits, Angriffe auf den Speicher sowie Bedrohungen zu blockieren, die es auf höhere Berechtigungen abgesehen haben.

#### Global Threat Intelligence

- Wehren Sie anhand von Echtzeit-Bedrohungsanalysen von weltweit Millionen Sensoren neue und zukünftige Bedrohungen aus allen Vektoren ab.
- Dank 100 Millionen Bedrohungssensoren in mehr als 120 Ländern sehen wir mehr und bieten die stärksten weltweiten Bedrohungsdaten auf dem Markt.

### Web- und E-Mail-Sicherheit

#### Web-Kontrolle mit URL-Filterung und sicherer Suche

- Warnen Sie Benutzer vor gefährlichen Webseiten, noch bevor diese geladen werden, und halten Sie auf diese Weise Compliance-Anforderungen ein.
- Setzen Sie Richtlinien für die Internetnutzung durch, indem Sie den Zugriff auf Webseiten erlauben oder blockieren.

#### Malware- und Spam-Schutz für E-Mails

- Schützen Sie die E-Mail-Server, und fangen Sie Malware ab, bevor diese in den Posteingang der Benutzer gelangt.
- Erkennen, bereinigen und blockieren Sie Malware für Microsoft Exchange- und Lotus Domino-Server mit McAfee GroupShield.

### Datenschutz

#### Gerätesteuerung

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

### Verwaltung

#### McAfee ePO

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



McAfee. Part of Intel Security.

Ohmstr. 1  
85716 Unterschleißheim  
Deutschland  
+49 (0)89 37 07-0  
www.intelsecurity.com

1. Erster Bericht veröffentlicht im Jahr 2002. Zu den vorherigen Titeln gehören der Magic Quadrant für Virenschutz in Unternehmen.

Intel und die Intel- und McAfee-Logos, ePolicy Orchestrator und McAfee ePO sind Marken der Intel Corporation oder von McAfee, Inc. in den USA und/oder anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer. Copyright © 2016 Intel Corporation. 370\_0816