McAfee Endpoint Threat Protection

Grundlegender und effektiver Schutz, der mit Ihrem Unternehmen wächst

Die Bedrohungslage wird sich zweifellos auch in Zukunft weiterentwickeln. Sie wissen bereits, dass starke Sicherheit auf dem Endgerät beginnt. Die Gewährleistung des notwendigen Schutzes ist jedoch schwierig, wenn durch das stückweise Hinzufügen neuer Technologien eine komplexe Sicherheitsumgebung mit voneinander abgeschotteten Produkten entsteht. McAfee® Endpoint Threat Protection bietet den grundlegenden Schutz, den Sie heute benötigen, und ist auch für die hochentwickelten Bedrohungen von morgen gerüstet. Die Lösung umfasst integrierte Bedrohungsabwehr, Firewall sowie Web-, E-Mail- und Geräteschutzmaßnahmen, die zusammen in Echtzeit Bedrohungen analysieren, blockieren und beseitigen, bevor sie Ihre Systeme sowie Benutzer beeinträchtigen.

Hauptvorteile

- Stärkung Ihrer Sicherheitslage durch mehrschichtige kooperative Schutztechnologien
- Flexible Erweiterung Ihres Schutzes und Anpassung an sich ändernde Anforderungen
- Steigerung der Produktivität durch zentrale Verwaltung sowie Scans ohne Beeinträchtigung der Benutzer und mit minimalen Auswirkungen auf die Systemressourcen

Ein kooperatives Endgeräte-Framework

Die Schutzfunktionen von McAfee Endpoint Threat Protection sind auf optimalen Schutz durch Integration ausgelegt. Sie kooperieren und tauschen erfasste Informationen in Echtzeit aus, um verdächtige Dateien, Webseiten sowie potenziell unerwünschte Programme koordiniert zu erkennen und noch vor der Ausführung zu blockieren.

Anwendungsszenario
Download einer böswilligen Datei aus dem Web

Ein Datei-Hash-Wert wird vom Web-Kontrollmodul an das Bedrohungsschutzmodul gesendet. Dadurch wird ein On-Demand-Scan (ODS) ausgelöst.

Böswillige Dateien werden erkannt und blockiert, bevor sie Vollzugriff auf das System erhalten.

Forensik-Daten werden erfasst (Quell-URL, Datei-Hash etc.).

Ereignisdaten werden an andere Module und McAfee® ePolicy Orchestrator® (McAfee ePO™) weitergegeben und können auf der Client-Benutzeroberfläche angezeigt werden.

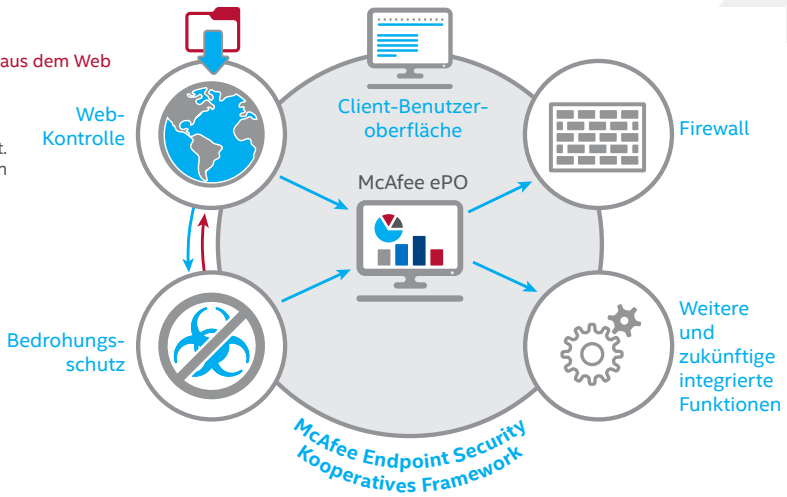

Abbildung 1. Zusammenarbeit der McAfee Endpoint Threat Protection-Schutzfunktionen.

Eine integrierte Lösung für Gegenwart und Zukunft

McAfee Endpoint Threat Protection ersetzt Bereitstellungen mit isolierten Einzelprodukten durch ein vernetztes, kooperatives Framework, das dank verschiedener Sicherheitstechnologien beinahe in Echtzeit Schutz bietet. Dadurch können bessere Bedrohungsanalysen durchführt und gesammelte Bedrohungsdaten an andere Schutzmaßnahmen weitergegeben werden, um die Erkennung sowie Blockierung von Bedrohungen auf anderen Endgeräten oder an anderen Eintrittspunkten zu verbessern und zu beschleunigen.

Die Bereitstellung ist ebenfalls äußerst flexibel möglich. So können Sie den vollen Funktionsumfang installieren und entscheiden, welche Funktionen sofort konfiguriert sowie aktiviert werden sollen. Bisher nicht genutzte Komponenten werden bei Bedarf mit einer einfachen Richtlinienänderung aktiviert.

Und schließlich können Sie mithilfe unseres Frameworks, dessen Architektur die Implementierung zusätzlicher Technologien ermöglicht, problemlos Ihren Schutz erweitern und an veränderte Anforderungen anpassen. So haben Sie jederzeit die Möglichkeit, weitere fortschrittliche Sicherheitsmaßnahmen zum Schutz vor noch raffinierteren Bedrohungen zu implementieren.

Kostengünstig, ohne die Leistung zu beeinträchtigen

McAfee Endpoint Threat Protection bietet ein erweiterbares Framework mit grundlegenden Schutztechnologien, das nicht die Komplexität erhöht oder die Leistung beeinträchtigt, sondern Ihre Produktivität und die Ihrer Benutzer verbessert. Dank der zentralen Verwaltung durch die Software McAfee ePolicy Orchestrator, die eine zentrale Übersicht zur Bereitstellung, Überwachung und Verwaltung von Sicherheitsrichtlinien in Ihrer Umgebung bietet, können Sie Ihre Abläufe effizienter steuern. Kunden mit mehreren Betriebssystemen in ihrer Umgebung steigern ihre Produktivität dank plattformübergreifender Richtlinien für Microsoft Windows-, Apple Macintosh- und Linux-Systeme. Und da die Komponenten von McAfee Endpoint Threat Protection eine gemeinsame Sprache nutzen (McAfee Data Exchange Layer), können Sie die Prozesse zwischen den Technologien optimieren und Reaktionen auf Bedrohungen beschleunigen. Dadurch verringert sich das Anfälligkeitsfenster, was die Risiken minimiert.

Ihre Benutzer profitieren von höherer Produktivität dank Scans, die den Benutzer nicht beeinträchtigen, und Verwaltungsfunktionen, die den Speicher und die CPU-Leistung optimal nutzen, um die Auswirkungen auf die Systeme zu minimieren. Die Lösung bietet eine intuitive Benutzeroberfläche, die Ihnen und Ihren Benutzern schnell einen Überblick darüber gewährt, welche Aktionen warum getroffen wurden.

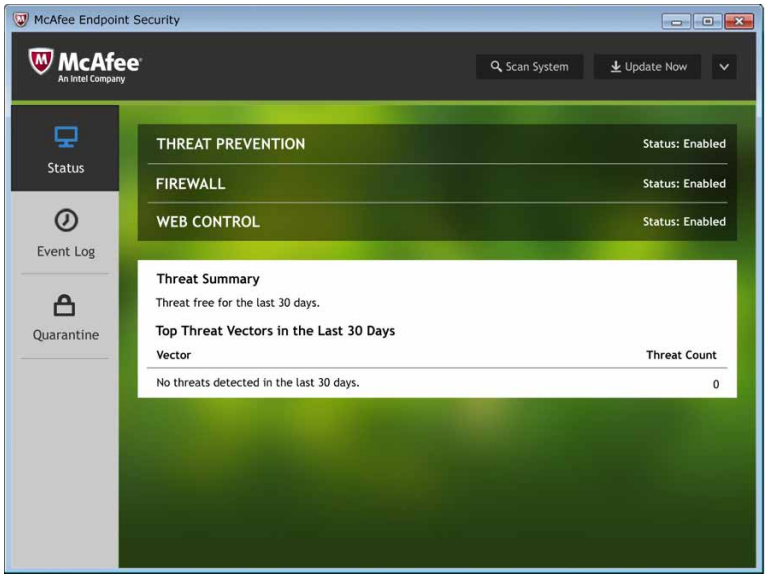

Abbildung 2. Die intuitive Benutzeroberfläche erleichtert Administratoren und Benutzern die Arbeit.

Unterstützte Plattformen

- Windows: 7, To Go, 8, 8.1, 10, 10 November, 10 Anniversary
- Mac OS X 10.5 oder höher
- Linux 32- und 64-Bit-Plattformen: neueste Versionen von RHEL, SUSE, CentOS, OEL, Amazon Linux und Ubuntu

Server:

- Windows Server (2003 SP2 oder höher, 2008 SP2 oder höher, 2012), Windows Server 2016
- Windows Embedded (Standard 2009, Point of Service 1.1 SP3 oder höher)
- CitrixXen
- Citrix XenApp 5.0 oder höher

Komponente	Vorteil	Kundenvorteile	Differenzierung
Bedrohungs-schutz	Bietet umfassenden Schutz, der Malware dank mehrerer Schutzebenen schnell findet, blockiert und beseitigt.	• Blockierung bekannter und unbekannter Malware mithilfe von Heuristik sowie On-Access-Scan-Technologien • Schutz für Windows-, Mac- und Linux-Plattformen dank vereinfachter Richtlinien und Bereitstellungen • Höhere Leistung durch Vermeidung von Scans vertrauenswürdiger und Priorisierung verdächtiger Prozesse	Mehrschichtiger Malware-Schutz, der mit Firewalls sowie Web-Sicherheitsmaßnahmen zusammenarbeitet und Informationen austauscht, um die Analyseleistung zu verbessern sowie potenzielle Bedrohungen mithilfe intelligent angewandter Regeln zu blockieren
Integrierte Firewall	Schützt Endgeräte vor Botnets, Distributed Denial-of-Service-Angriffen (DDoS), nicht vertrauenswürdigen ausführbaren Dateien, hochentwickelten hartnäckigen Bedrohungen (APTs) sowie riskanten Web-Verbindungen.	• Schutz für Benutzer und Produktivität durch Richtlinienerzwingung • Schutz der Bandbreite durch Blockierung unerwünschter eingehender Verbindungen und Kontrolle ausgehender Anfragen • Informiert Benutzer über vertrauenswürdige Netzwerke und ausführbare Dateien sowie riskante Dateien oder Verbindungen	Schutz von Laptops und Desktops durch Richtlinien für Anwendungen sowie Speicherorte – insbesondere bei Nutzung dieser Geräte außerhalb des Unternehmensnetzwerks
Web-Kontrolle	Gewährleistet sicheres Surfen dank Web-Schutz und Filterung für Endgeräte.	• Risikominimierung und Gewährleistung der Compliance durch Warnungen an Benutzer, bevor diese böswillige Webseiten aufrufen • Abwehr von Bedrohungen und Schutz der Produktivität durch Autorisierung oder Blockierung gefährlicher oder unzulässiger Webseiten • Blockierung gefährlicher Downloads, bevor diese Schaden anrichten können	Schutz für Windows-, Mac- und Linux-Systeme sowie verschiedene Browser, der von McAfee Global Threat Intelligence unterstützt wird
McAfee Data Exchange Layer	Vernetzt Sicherheits-lösungen zur Integration und Optimierung der Kommunikation mit Intel Security- sowie Drittanbieterprodukten.	• Risikominimierung und kürzere Reaktionszeit durch Integration • Verringerung von Verwaltungsaufwand und Personalkosten • Optimierung von Prozessen und praktische Empfehlungen	• Austausch der wichtigsten Bedrohungsinformationen zwischen Sicherheitsprodukten • Sofortige Weitergabe von Bedrohungsdaten über Patient Null an alle anderen Endgeräte, um Infektionen zu verhindern und die Schutzmaßnahmen zu aktualisieren
Verwaltungs-plattform McAfee ePO	Bietet einen zentralen Überblick zur stark skalierbaren, flexiblen sowie automatisierten Verwaltung von Sicherheitsrichtlinien, um Sicherheitsprobleme zu erkennen und zu beheben.	• Einheitliche und vereinfachte Sicherheitsabläufe für bewährte Effizienz • Besserer Überblick und größere Flexibilität für fundierte Maßnahmen • Schnelle Bereitstellung und Verwaltung als einzelner Agent mit anpassbarer Richtlinienerzwingung • Verkürzung der Zeit vom Erhalt der Information bis zur Reaktion – mit dynamischen automatisierten Abfragen, Dashboards und Reaktionen	• Mehr Kontrolle, geringere Kosten und schnellere Verwaltung von Sicherheitsabläufen mit einer einzigen Konsole • Bewährte Benutzeroberfläche, deren Konzept branchenweit als ausgezeichnet gilt • Drag & Drop-Dashboards für ein breites Sicherheitsökosystem • Offene Plattform zur schnellen Implementierung von Sicherheitsinnovationen

Weitere Informationen zu den Vorteilen von McAfee Active Response finden Sie unter **www.mcafee.com/de/products/endpoint-threat-protection.aspx**.

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