McAfee Complete Endpoint Threat Protection

Fortschrittlicher Bedrohungsschutz vor raffinierten Angriffen

Hauptvorteile

- Bleiben Sie Zero-Day-Bedrohungen, Ransomware und Greyware mit Machine Learning und dynamischer Eindämmung stets einen Schritt voraus.
- Beschleunigen Sie die Behebung, und schützen Sie Ihre Produktivität mit automatisierten Aktionen und Analysen.
- Vereinfachen Sie Ihre Umgebung, Bereitstellung und Betriebsabläufe mit zentraler Verwaltung.

Ihr Unternehmen ist Bedrohungen ausgesetzt, die einen guten Überblick notwendig machen und Tools erfordern, mit denen Sie den gesamten Zyklus der Bedrohungsabwehr beherrschen. Ihre Sicherheitsspezialisten benötigen daher Hilfsmittel, mit denen sie präziser agieren können und genauere Informationen über hochentwickelte Bedrohungen erhalten. McAfee® Complete Endpoint Threat Protection bietet hochentwickelte Schutzmaßnahmen, die Zero-Day-Bedrohungen sowie raffinierte Angriffe analysieren, eindämmen und Gegenmaßnahmen ergreifen. Der grundlegende Endgeräteschutz bietet integriertes Machine Learning und dynamische Eindämmung, um Zero-Day-Bedrohungen fast in Echtzeit zu erkennen und noch vor der Erstinfektion zu klassifizieren und zu blockieren. Umsetzbare forensische Daten sowie Berichte halten Sie auf dem Laufenden und unterstützen Sie, damit Sie nicht mehr nur auf Ausbrüche reagieren, sondern die Bedrohungen untersuchen und Ihre Schutzmaßnahmen verbessern können. Da die Lösung auf einem erweiterbaren Framework basiert, können Sie jederzeit problemlos weitere hochentwickelte Schutzmaßnahmen hinzufügen, wenn Ihre Anforderungen und die Sicherheitslage dies erforderlich machen.

Automatisierte hochentwickelte Bedrohungsabwehr

Sie müssen raffinierte Bedrohungen abwehren, noch bevor diese sich festsetzen können. Aus diesem Grund enthält McAfee Complete Endpoint Threat Protection die Funktion zur dynamischen Eindämmung von Anwendungsprozessen sowie Real Protect[1]. Wenn böswilliges Verhalten erkannt wird, werden dank der dynamischen Eindämmung von Anwendungsprozessen Greyware sowie verdächtige Zero-Day-Bedrohungen automatisch isoliert, sodass Ihre Systeme nicht infiziert und Ihre Benutzer nicht beeinträchtigt werden. Real Protect nutzt Machine Learning zur Untersuchung und Klassifizierung von Bedrohungen und speichert sowie verwendet diese Informationen, um in Zukunft automatisch Aktionen durchzuführen.

intel Security

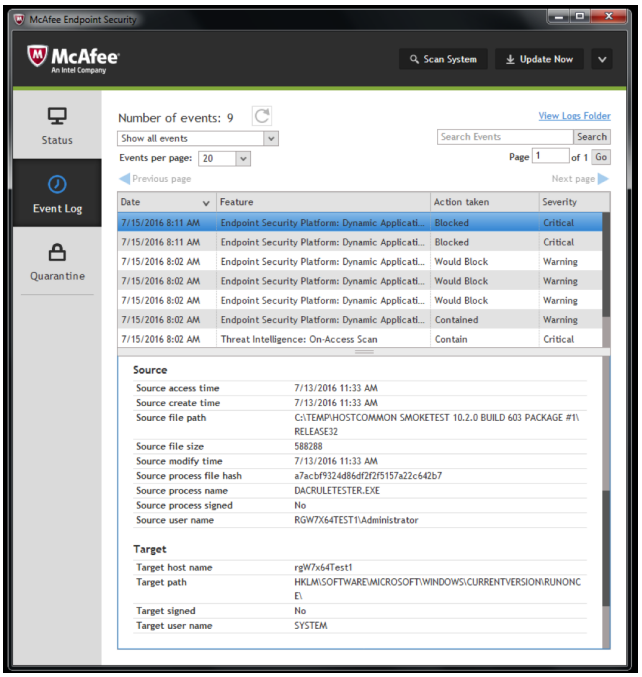

Abbildung 1. Die dynamische Eindämmung von Anwendungsprozessen blockiert und isoliert Bedrohungen entsprechend ihres Schweregrades.

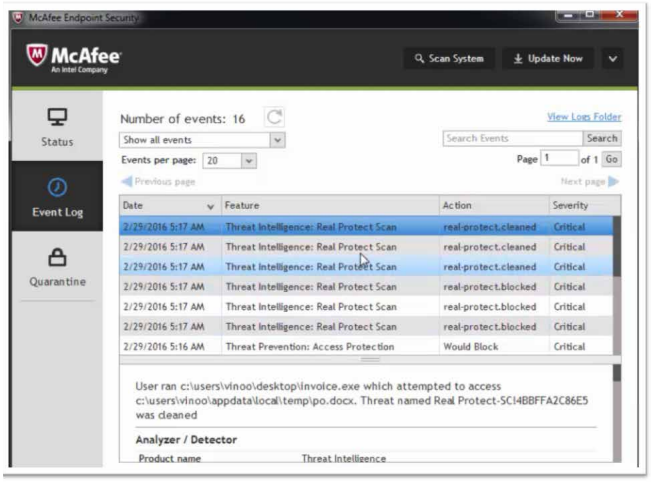

Abbildung 2. Real Protect kann Zero-Day-Malware, die bei signaturbasierten Scans häufig übersehen wird, mithilfe von Machine Learning beinahe in Echtzeit erkennen.

Minimierung der Komplexität

Mehr Komplexität bedeutet weniger Effizienz. Jetzt müssen Sie nicht mehr aufwändig verschiedene Einzellösungen mit unterschiedlichen Benutzeroberflächen und Verwaltungskonsolen im Blick behalten. McAfee Complete Endpoint Threat Protection wird über eine einzige Konsole verwaltet: McAfee® ePolicy Orchestrator® (McAfee ePO™). In dieser zentralen Übersicht können Sie schneller Implementierungen durchführen, den Bereitstellungszeitraum verkürzen und die laufende Verwaltung vereinfachen. Kunden mit mehreren Betriebssystemen in ihrer Umgebung steigern ihre Produktivität dank plattformübergreifender Richtlinien für Microsoft Windows-, Apple Macintosh- und Linux-Systeme.

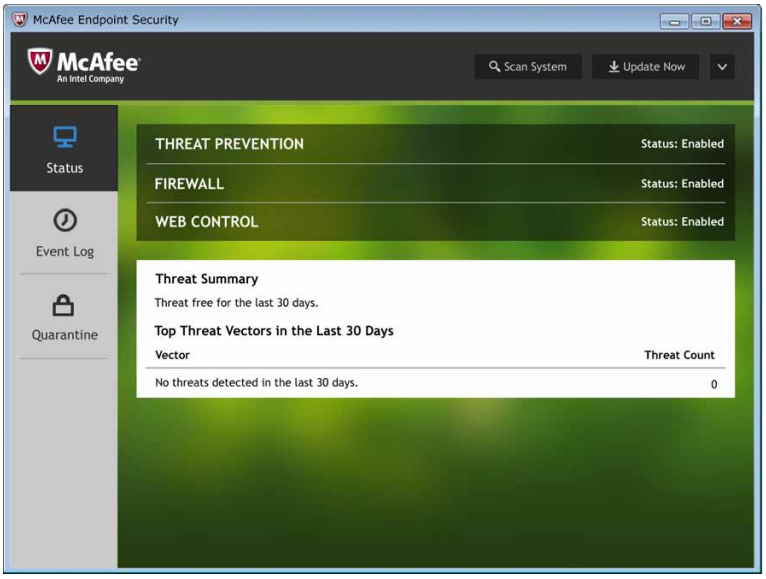

Abbildung 3. Die intuitive Benutzeroberfläche erleichtert Administratoren und Benutzern die Arbeit.

Ein flexibles Framework für Gegenwart und Zukunft

McAfee Complete Endpoint Threat Protection stellt ein vernetztes kooperatives Framework bereit, das dank verschiedener Sicherheitstechnologien beinahe in Echtzeit Schutz bietet. Dies erlaubt nicht nur eine genauere Analyse der Bedrohungen, sondern ermöglicht auch den Austausch der erfassten Bedrohungsforensikdaten mit anderen Schutzmaßnahmen, um ihre Möglichkeiten zu steigern. Dieser Informationsaustausch zwischen grundlegenden Endgeräteschutzlösungen mit den hochentwickelten Bedrohungsschutzmaßnahmen erfolgt über die gemeinsame Kommunikationsebene.

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, Ihren Schutz erweitern und an veränderte Anforderungen anpassen.

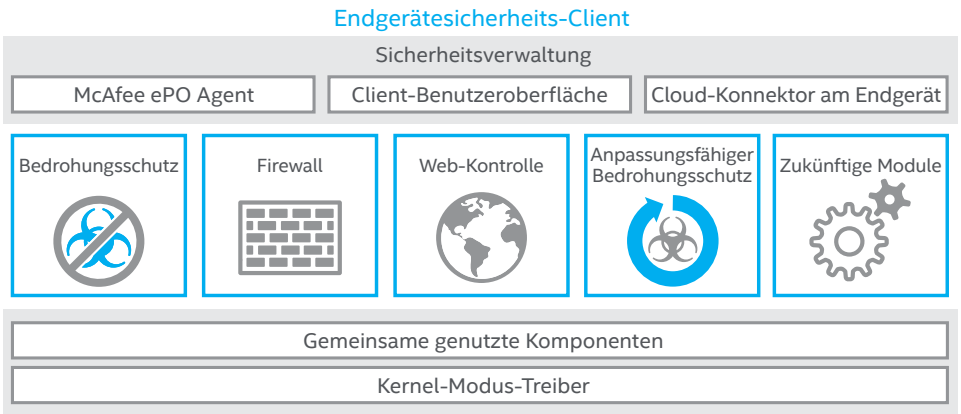

Abbildung 4. Das Framework der Endgerätesicherheits-Clients.

Unterstützte Plattformen

- Microsoft 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

Weitere Informationen zu den Vorteilen von McAfee Complete Endpoint Threat Protection finden Sie unter **www.mcafee.com/de/products/complete-endpoint-threat-protection.aspx**.

Komponente	Vorteil	Kundenvorteile	Differenzierung
Dynamische Eindämmung von Anwendungsprozessen	Schützt Patient Null, indem verhindert wird, dass Greyware böswillige Änderungen an Endgeräten vornimmt.	• Erweiterter Schutz ohne Beeinträchtigung der Endbenutzer oder vertrauenswürdiger Anwendungen • Kürzere Zeit von der Entdeckung bis zur Eindämmung – mit minimalen Eingriffen • Absicherung von Patient Null und Isolierung des Netzwerks von Infektionen	• Funktioniert mit und ohne Internetverbindung und erfordert keine externen Eingaben oder Analysen • Transparent für die Benutzer • Beobachtungsmodus bietet sofortige Bedrohungsübersicht zu potenziellem Exploit-Verhalten innerhalb der Umgebung
Real Protect	Nutzt Machine-Learning-Verhaltensklassifizierung zur Blockierung von Zero-Day-Bedrohungen vor deren Ausführung und wehrt aktive Bedrohungen ab, die vorherige Erkennungsfunktionen umgehen konnten.	• Einfache Abwehr von mehr Zero-Day-Malware, einschließlich gut verborgener Objekte wie Ransomware • Automatische Demaskierung, Analyse und Beseitigung von Bedrohungen ohne manuelle Eingriffe • Anpassung von Schutzmaßnahmen mithilfe automatisierter Klassifizierung und einer vernetzten Sicherheitsinfrastruktur	• Erkennung von Malware, die nur durch dynamische Verhaltensanalysen entdeckt werden kann • Enge Vernetzung, sodass aktualisierte Reputationsinformationen in Echtzeit ausgetauscht und die Sicherheitseffizienz aller Sicherheitskomponenten verbessert werden
Bedrohungsschutz	Bietet umfassenden Schutz, der Malware dank mehrerer Schutzebenen schnell findet, blockiert und beseitigt.	• Blockierung bekannter und unbekannter Malware mithilfe von Heuristik, Verhaltensanalyse sowie On-Access-Scan-Technologien • Schutz für Desktops und Server auf Windows-, Mac- und Linux-Computern dank vereinfachter Richtlinien und Bereitstellungen • Höhere Leistung durch Vermeidung von Scans vertrauenswürdiger und Priorisierung verdächtiger Prozesse	Mehrschichtiger Malware-Schutz, der mit Web- und Firewall-Sicherheitsmaßnahmen zusammenarbeitet und stärkere Analysen sowie Bedrohungsschutz bietet
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 von Webseitenzugriffen • Blockierung gefährlicher Downloads, bevor diese Schaden anrichten können	Schutz für Windows, Mac und zahlreiche Browser
McAfee Data Exchange Layer	Vernetzt Sicherheitslösungen 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 Sicherheitsmaßnahmen
Verwaltungsplattform 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 intuitiven Dashboards und Berichten	• 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

1. Die Lösung nutzt in den USA gehostete Rechenzentren, in denen die Dateireputation überprüft und Daten gespeichert werden, die für die Erkennung verdächtiger Dateien relevant sind. Die Cloud-Anbindung ist für die Funktion zur dynamischen Eindämmung von Anwendungsprozessen zwar nicht zwingend erforderlich, zur optimalen Nutzung jedoch unerlässlich. Für den vollständigen Funktionsumfang der dynamischen Eindämmung von Anwendungsprozessen sowie von Real Protect sind Cloud-Zugang und aktiver Support notwendig. Zudem gelten die Cloud-Service-Geschäftsbedingungen.

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