McAfee Endpoint Security

Zielgerichtete Sicherheitsfunktionen für proaktive Bedrohungsverwaltung und bewährte Sicherheitskontrollen

Endgerätesicherheit: Welche Prioritäten haben Sie?

In heutigen Unternehmen kann die Sicherheit in den Verantwortungsbereich von einem oder mehreren Teams fallen. In großen Unternehmen sind häufig gleiche mehrere Teams zuständig, z. B. das IT-Verwaltungs- und das Sicherheitsprozess-Team. Unabhängig davon, welcher Ansatz Ihre Rolle im Unternehmen am besten beschreibt, sind bei einer Endgeräteschutzplattform andere Funktionen sowie andere Ergebnisse für Sie wichtig.

Die von Ihnen eingesetzte Endgerätelösung sollte Ihren Prioritäten Rechnung tragen. Unabhängig von Ihrer Rolle erfüllt McAfee® Endpoint Security Ihre wichtigsten spezifischen Anforderungen und entdeckt sowie blockiert nicht nur Bedrohungen, sondern erlaubt auch angepasste Sicherheitskontrollen. Mit den Funktionen von McAfee® MVISION Insights werden Bedrohungen priorisiert, bevor der Angriff erfolgt. Dank der Lösung können Sie die Systemverfügbarkeit für Ihre Benutzer gewährleisten, weitere Automatisierungsmöglichkeiten finden und komplexe Workflows vereinfachen.

Gewährleistung von Verfügbarkeit und Einblicken

Dank präventiver Schutzfunktionen und Behebungs-Tools ermöglicht McAfee Endpoint Security die Reaktion auf Bedrohungen sowie die Verwaltung des Kreislaufs zur Bedrohungsabwehr. Durch automatische Funktionen zur Behebung durch Rollback werden die Systeme in einen fehlerfreien Zustand zurück versetzt, sodass Benutzer und Administratoren produktiv sein können und Zeit sparen, die ansonsten für das Warten auf die Systemwiederherstellung, Behebungsmaßnahmen oder das Installieren eines Images verloren gehen würde. Weltweit erfasste Bedrohungsdaten und Echtzeitinformationen zu lokalen Ereignissen werden zwischen Endgeräten und McAfee® MVISION EDR ausgetauscht. Dadurch können Details zu Bedrohungsereignissen erfasst, Umgehungsmaßnahmen von Bedrohungen erkannt sowie verhindert und zur weiteren Untersuchung dem MITRE ATT&CK-Framework zugeordnet werden. Dank der zentralen Verwaltungskonsole, die sich lokal, per SaaS oder virtuell implementieren lässt, wird die Verwaltung erheblich vereinfacht. MVISION Insights liefert einzigartige Übersicht und Kontrolle über potenziell schwerwiegende Bedrohungen mit großer Angriffswahrscheinlichkeit. Zudem wird ermittelt, ob die Sicherheitsmaßnahmen im Unternehmen Schutz vor dieser Bedrohung bieten können. Damit wird sichergestellt, dass ausreichender Schutz vor kritischen Bedrohungen besteht und Angreifer präventiv abgewehrt werden.

Hauptvorteile

- **Hochentwickelter Schutz vor hochentwickelten Bedrohungen:** Machine Learning, Schutz vor dem Diebstahl von Anmeldeinformationen und Behebung durch Rollback zur Ergänzung der grundlegenden Sicherheitsfunktionen von Windows-Desktop- und Server-Systemen
- **Keine zusätzliche Komplexität:** Verwaltung von McAfee-Technologien, Windows Defender Antivirus-Richtlinien, Defender Exploit Guard- und Windows-Firewall-Einstellungen mit nur einer Richtlinie und Konsole

Folgen Sie uns

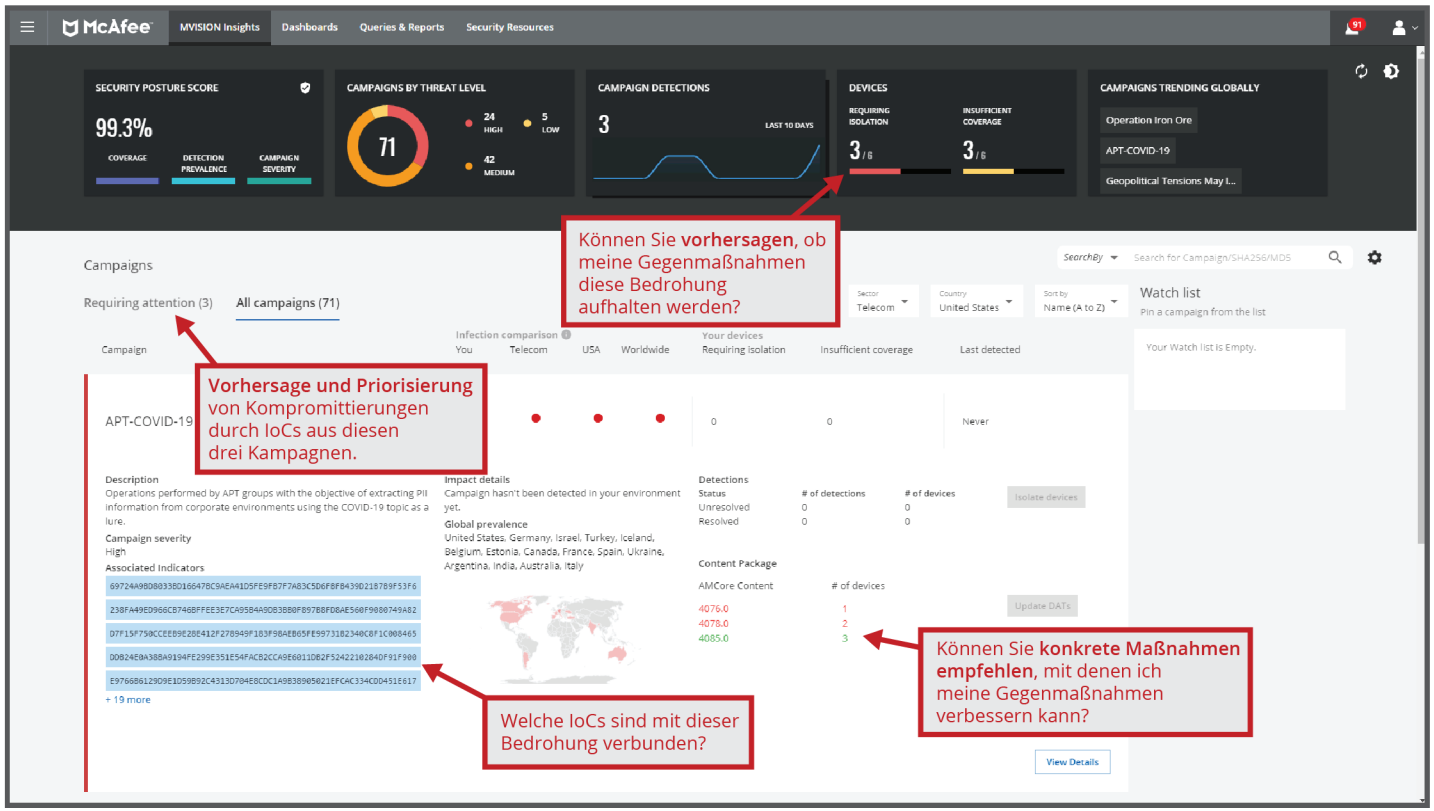

Abbildung 1. Dashboard von MVISION Insights. (Damit MVISION Insights ordnungsgemäß funktioniert, müssen Sie die Erfassung und Übertragung von Telemetriedaten in McAfee Endpoint Security erlauben.)

Mit MVISION Insights erhalten Unternehmen Warnmeldungen und Benachrichtigungen zu priorisierten potenziellen Bedrohungen, die wahrscheinlich ihre jeweilige Branche und Region betreffen werden. Zudem bewertet MVISION Insights die lokale Sicherheitsaufstellung und schätzt ein, ob diese Bedrohungen erfolgreich abgewehrt werden können.

Außerdem identifiziert die Lösung Endgeräte, die für die Bedrohung anfällig sind, und bietet präskriptive Anleitungen zu erforderlichen Aktualisierungen. Damit können Sie proaktive Maßnahmen ergreifen, um wahrscheinlichen Angreifern einen Schritt voraus zu bleiben.

Hauptvorteile (Fortsetzung)

- **MVISION Insights:** Die führende Lösung für umsetzbare Sicherheitsinformationen ermöglicht die sofortige Reaktion auf potenziell aktive Kampagnen, die danach priorisiert werden, ob sie Ihre Branche oder Region angreifen. MVISION Insights sagt voraus, bei welchen Endgeräten Schutzmaßnahmen vor diesen Kampagnen fehlen, und bietet Hinweise zur Verbesserung der Erkennung. Dies ist die einzige Endgeräte-Sicherheitslösung, die Aktionen gleichzeitig priorisieren, vorhersagen und empfehlen kann.

Mithilfe eines einzigen Software-Agenten erfasst McAfee Endpoint Security Bedrohungsinformationen aus mehreren Interaktionsebenen, sodass Redundanzen durch mehrere Einzelprodukte vermieden werden. Bei diesem integrierten Sicherheitsansatz entfällt die manuelle Bedrohungskorrelation. Bedrohungsdetails, die weiter untersucht werden müssen, werden automatisch an den zuständigen Sicherheitsverantwortlichen weitergeleitet. Die Daten zu Bedrohungsereignissen werden in Story Graph in einer benutzerfreundlichen Übersicht mit den relevanten Bedrohungsdetails dargestellt, sodass Administratoren problemlos Details aufschlüsseln und die Quellen der böswilligen Akteure untersuchen können.

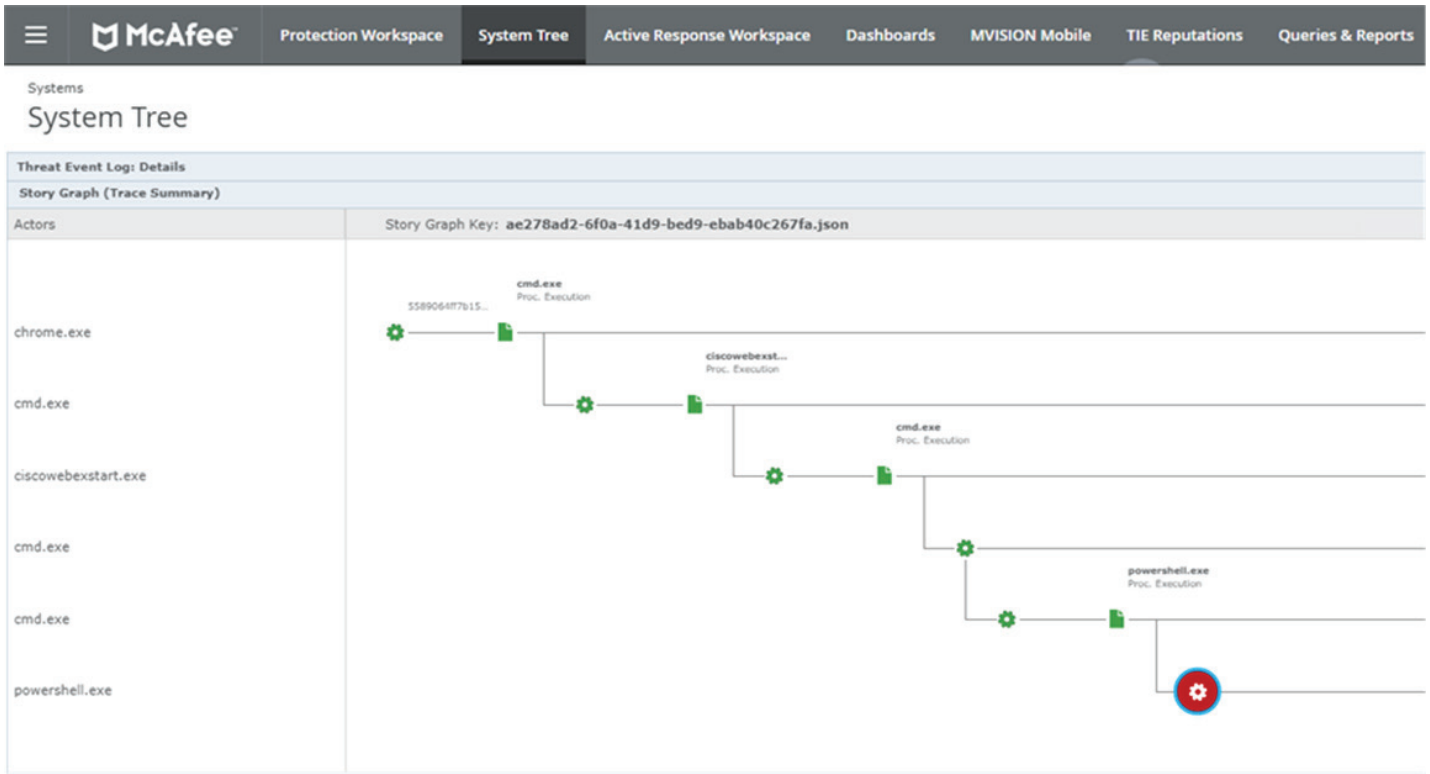

Abbildung 2. Story Graph.

Integrierter Schutz vor hochentwickelten Bedrohungen für automatisierte und schnelle Reaktionen

Im Rahmen des integrierten McAfee Endpoint Security-Frameworks stehen zusätzliche Technologien zur Abwehr hochentwickelter Bedrohungen zur Verfügung, die Unternehmen auch vor den neuesten Bedrohungen schützen.[1] Dazu gehört zum Beispiel die Funktion zur dynamischen Eindämmung von Anwendungsprozessen (Dynamic Application Containment, DAC), die gefundene Greyware und andere neue Malware-Varianten analysiert, geeignete Maßnahmen ergreift sowie die potenzielle Bedrohung isoliert, um Infektionen zu vermeiden.

Real Protect ist eine weitere Technologie, die Machine Learning-Verhaltensklassifizierung zur Erkennung von Zero-Day- und anderer Malware nutzt. Da die signaturlose Klassifizierung in der Cloud durchgeführt wird, werden auf dem Client nur minimale Ressourcen benötigt. Der Schutz erfolgt beinahe in Echtzeit.

Die Bedrohungsinformationen können für Aktionen sowie zur Erstellung von Indikatoren für Angriffe (IoA) und Kompromittierungen (IoC) genutzt werden. Dies ist besonders zur Verhinderung von Bewegungen innerhalb des Netzwerks, zur Erkennung von Patient Null-Infektionen, zur Zuordnung von Bedrohungsakteuren, für forensische Untersuchungen sowie zur Beseitigung von Bedrohungen nützlich. Real Protect beschleunigt auch spätere Analysen, da die Verhaltensklassifizierung automatisch weiterentwickelt wird, um Verhaltensweisen aufzudecken und Regeln hinzuzufügen, mit denen ähnliche Angriffe in Zukunft mithilfe statischer Funktionen sowie zur Laufzeit erkannt werden können.

Um die Infektion sofort zu verhindern und den Zeitaufwand für IT-Sicherheitsadministratoren zu verringern, setzt der Client das Endgerät nach einer Überführung in den letzten als sicher bekannten Zustand zurück.

Intelligenter Endgeräteschutz, damit Sie wissen, was die Angreifer gerade tun

Bessere Aufklärung ermöglicht bessere Ergebnisse. McAfee Endpoint Security gibt die eigenen Beobachtungen in Echtzeit an mehrere Endgeräteschutztechnologien weiter, die über das gemeinsame Framework vernetzt sind. Durch diesen kooperativen Ansatz können die vernetzten Produkte verdächtiges Verhalten schneller erkennen, die Gegenmaßnahmen besser koordinieren und somit besseren Schutz vor gezielten Angriffen sowie Zero-Day-Bedrohungen bieten. Daten wie Datei-Hashes, Quell-URLs, AMSI und PowerShell-Ereignisse werden überwacht und an andere Schutzprodukte sowie Client- und Verwaltungsbenutzeroberflächen weitergegeben, damit Benutzer die Angriffe besser verstehen und Administratoren wertvolle Forensikdaten zu Bedrohungen erhalten.

Außerdem ermöglicht die McAfee® Threat Intelligence Exchange-Technologie die Zusammenarbeit anpassbarer Schutzprodukte mit anderen McAfee-Lösungen, einschließlich Gateways, Sandboxes und unserer SIEM-Lösung (Sicherheitsinformations- und Ereignis-Management). Durch die Erfassung und Verteilung lokaler, globaler und von der Community gemeldeter Sicherheitsdaten wird die Zeit zwischen Angriff, Erkennung und Eindämmung von Wochen oder Monaten auf Millisekunden verkürzt.

In Kombination mit McAfee® Global Threat Intelligence (McAfee® GTI) nutzt das McAfee Endpoint Security-Framework die Cloud, um das gesamte Spektrum aktueller sowie neuer Bedrohungen in Echtzeit überwachen und angemessen reagieren zu können. Dabei werden alle Vektoren abgedeckt: Dateien, Internet, Nachrichten und Netzwerk. Die vorhandenen Endgerätelösungen und das Verwaltungssystem werden durch lokale sowie globale Bedrohungsdaten ergänzt, damit die Abwehr gegen unbekannte und gezielte Malware sofort steht. Mit automatischen Aktionen gegen verdächtige Anwendungen und Prozesse können Reaktionen auf aktuelle und neue Angriffsformen schnell eskaliert werden. Gleichzeitig werden andere Schutzmaßnahmen sowie die globale Community über diese Gefahren informiert.

Kunden, die DAC (Dynamic Application Containment, Funktion zur dynamischen Eindämmung von Anwendungsprozessen) sowie Real Protect nutzen, erhalten Informationen über hochentwickelte Bedrohungen und ihre Verhaltensweisen. Beispielsweise stellt DAC Informationen über eingedämmte Bedrohungen sowie darüber bereit, wie sie Zugang zu erlangen versuchen (z. B. über die Registrierung oder den Arbeitsspeicher.

Für Unternehmen, die mithilfe von Bedrohungsdaten zu Endgeräteprozessen Malware aufspüren und Sicherheitsverantwortliche unterstützen möchten, bietet Real Protect wichtige Informationen zu als böswillig eingestuftem Verhalten sowie zur Klassifizierung von Bedrohungen. Diese Bedrohungsdaten sind besonders hilfreich zur Erkennung von dateibasierter Malware, die sich mit Techniken wie Packen, Verschlüsselung oder Missbrauch legitimer Anwendungen tarnt.

Hohe und effektive Leistung für rechtzeitige Reaktionen

Intelligente Schutzmaßnahmen sind nur wenig effektiv, wenn sie die Benutzer mit langsamen Scans beeinträchtigen, die Installation sehr lange dauert oder die Verwaltung sich als sehr kompliziert darstellt. McAfee Endpoint Security schützt die Produktivität der Benutzer mit einer gemeinsamen Dienstebene und unserem neuen Anti-Malware Core-Modul, das den Ressourcen- und Energiebedarf auf dem Benutzersystem verringert. Endgeräte-Scans beeinträchtigen die Benutzerproduktivität nicht, da sie nur durchgeführt werden, wenn sich das Gerät im Leerlauf befindet. Nach einem Neustart oder dem Herunterfahren des Geräts werden sie nahtlos fortgesetzt.

Mit einem adaptiven Scan-Prozess wird die CPU-Belastung zusätzlich reduziert: Die Lösung lernt, welche Prozesse und Quellen als vertrauenswürdig eingestuft werden, damit die Kapazitäten auf die Prozesse und Dateien konzentriert werden können, die als verdächtig gelten oder aus unbekannten Quellen stammen. McAfee Endpoint Security verfügt über eine integrierte Firewall, die Endgeräte mithilfe von McAfee GTI vor Botnets, DDoS-Angriffen (Distributed Denial-of-Service), hochentwickelten hartnäckigen Bedrohungen sowie riskanten Web-Verbindungen schützt.

Verringerung des Drucks dank reduzierter Komplexität und verbesserter Effizienz

Aufgrund des schnellen Wachstums von Sicherheitsprodukten mit sich überschneidenden Funktionen und getrennten Verwaltungskonsolen ist es für viele Sicherheitsverantwortliche schwer geworden, ein deutliches Bild von potenziellen Angriffen zu erhalten. McAfee Endpoint Security bietet leistungsstarken, langfristigen Schutz dank seines offenen und erweiterbaren Frameworks, das als Grundlage für die Zentralisierung aktueller und zukünftiger Endgerätesicherheitslösungen fungiert. Dieses Framework nutzt den Data Exchange Layer zur technologieübergreifenden Zusammenarbeit vorhandener Sicherheitsinvestitionen. Die vernetzte Architektur integriert nahtlos andere McAfee-Produkte, wodurch technologische Silos aufgebrochen, Sicherheitslücken sowie Redundanzen minimiert werden und gleichzeitig die Produktivität verbessert wird, da Betriebskosten und Verwaltungskomplexität sinken.

McAfee® ePolicy Orchestrator® (McAfee ePO™) verringert die Komplexität zusätzlich, da Sie mit dieser Software eine zentrale Benutzeroberfläche erhalten, über die Sie Endgeräte überwachen, bereitstellen und verwalten können. Anpassbare Ansichten und praktische Workflows in verständlicher Sprache bieten die Voraussetzung für eine schnelle Bewertung der Sicherheitslage, die Suche nach infizierten Systemen sowie die Minimierung der Auswirkungen von Bedrohungen, da Systeme isoliert, böswillige Prozesse angehalten sowie Datenexfiltrationen blockiert werden können. Zudem fungiert McAfee ePO als zentraler Ort für die Verwaltung aller Endgeräte, anderer McAfee-Funktionen sowie mehr als 130 Sicherheitslösungen von Drittanbietern.

Funktion	Warum Sie sie benötigen
Proaktive Erkennung von und Reaktion auf Bedrohungen (MVISION Insights)	▪ Prädiktive und präventive Erkennung potenzieller Bedrohungen basierend auf Ihrer Branche und Region. ▪ Lokale Bewertung der Sicherheitslage anhand potenzieller Bedrohungen und Hinweise zu Verbesserungsmöglichkeiten. ▪ Präventive Abwehr, indem Schutzmaßnahmen noch vor dem Angriff eingerichtet werden.
Real Protect	▪ Machine Learning-Verhaltensklassifizierung erkennt Zero-Day-Bedrohungen nahezu in Echtzeit und liefert umsetzbare Bedrohungsdaten. ▪ Entwickelt die Verhaltensklassifizierung automatisch weiter, um Verhaltensweisen aufzudecken sowie Regeln zu erstellen, mit denen zukünftige Angriffe aufgedeckt werden können.
Endgeräteschutz vor gezielten Angriffen	▪ Ermöglicht die Verringerung der Schutzlücke zwischen Entdeckung und Eindämmung von Tagen auf Millisekunden. ▪ McAfee Threat Intelligence Exchange erfasst Daten aus mehreren Quellen, sodass sich Sicherheitskomponenten sofort miteinander über neue und mehrstufige hochentwickelte Angriffe austauschen können. ▪ Die Protokollierung von AMSI- und PowerShell-Ereignissen deckt dateilose und skriptbasierte Angriffe auf und schützt davor.
Intelligente, adaptive Scans	▪ Verbessern die Leistung und Produktivität, indem Scans vertrauenswürdiger Prozesse vermieden und verdächtige Prozesse sowie Anwendungen mit Priorität überprüft werden. ▪ Adaptive Verhaltens-Scans überwachen, überprüfen und eskalieren verdächtige Aktivitäten anlassbezogen.
Behebung durch Rollback	▪ Von Malware vorgenommene Änderungen werden automatisch zurückgesetzt und Systeme in einen bekannt fehlerfreien Zustand zurückversetzt, damit Ihre Benutzer produktiv bleiben.
Präventive Web-Sicherheit	▪ Gewährleistet sicheres Surfen dank Web-Schutz und Filterung für Endgeräte.
Dynamische Eindämmung von Anwendungsprozessen	▪ Schützt vor Ransomware sowie Greyware und sichert Patient Null ab. [2]
Blockierung böswilliger Netzwerkangriffe	▪ Die integrierte Firewall nutzt Reputationsfaktoren von McAfee GTI zum Schutz von Endgeräten vor Botnets, DDoS-Angriffen, hochentwickelten hartnäckigen Bedrohungen und verdächtigen Web-Verbindungen. ▪ Der Firewall-Schutz erlaubt während des Systemstarts ausschließlich ausgehenden Datenverkehr, damit Endgeräte außerhalb des Unternehmensnetzwerks sicher sind.
Story Graph	▪ Administratoren können schnell erkennen, wo sich Infektionen befinden, warum sie aufgetreten sind und wie lange sie bereits bestehen. Dadurch können sie Bedrohungen besser einschätzen und schneller reagieren.
Zentrale Verwaltung (über die McAfee ePO-Plattform) mit verschiedenen Bereitstellungsoptionen	▪ Die Verwaltung erfolgt absolut zentral, sodass der Überblick verbessert, die Abläufe vereinfacht, die IT-Produktivität erhöht, die Sicherheit vereinheitlicht und die Kosten reduziert werden.
Offenes, erweiterbares Endgerätesicherheits-Framework	▪ Die integrierte Architektur ermöglicht die Zusammenarbeit und Kommunikation zwischen Endgeräteschutzmaßnahmen, um zuverlässigeren Schutz zu erreichen. ▪ Senkt die Betriebskosten, da Redundanzen vermieden und Prozesse optimiert werden. ▪ Vernetzt sich nahtlos mit anderen McAfee- und Drittanbieterprodukten zur Minimierung von Schutzlücken.

Tabelle 1. Wichtige Funktionen und ihre Bedeutung

Ein Vorteil gegenüber Cyber-Bedrohungen

McAfee Endpoint Security bietet Sicherheitsexperten genau die Funktionen, die sie heute benötigen, um die Vorteile der Angreifer zu überwinden: intelligente und kooperative Schutzmaßnahmen sowie ein Framework, das komplexe Umgebungen vereinfacht. Mit der starken Leistung sowie der effizienten Bedrohungserkennung, die in Drittanbietertests bestätigt wurde, können Unternehmen ihre Benutzer schützen, deren Produktivität steigern und Sicherheit bieten.

McAfee bietet als führender Anbieter für Endgerätesicherheit eine vollständige Palette an Lösungen, die dank der Kombination von leistungsstarken Sicherheitsfunktionen und effizienter Verwaltung tiefengestaffelten und proaktiven Schutz ermöglichen. Dadurch können Sicherheitsteams Bedrohungen schneller und mit weniger Ressourcen beheben.

Vereinfachte Migration

In Umgebungen mit aktuellen Versionen von McAfee ePO, McAfee VirusScan® Enterprise sowie McAfee® Agent können bestehende Richtlinien mit unserem automatischen Migrations-Tool innerhalb von maximal 20 Minuten für McAfee Endpoint Security konvertiert werden.[3]

McAfee Endpoint Security bietet zudem folgende Vorteile:

- Scans ohne Beeinträchtigung der Benutzer für mehr Produktivität
- Detailliertere Forensikdaten, die in Story Graph für übersichtliche Einblicke und vereinfachte Untersuchungen zugeordnet werden, vereinfachen die Definition optimaler Richtlinien
- Behebung durch Rollback zur automatischen Zurücksetzung von Malware-Änderungen, um einen fehlerfreien Zustand der Systeme zu gewährleisten
- Von MVISION Insights gelieferte proaktive Erkenntnisse zu priorisierten potenziellen Bedrohungen und präskriptive Anleitungen zur Optimierung der Gegenmaßnahmen
- Weniger zu verwaltende Agenten sowie Vermeidung von Scans, um den manuellen Aufwand zu reduzieren
- Schutzmaßnahmen, die hochentwickelte Bedrohungen gemeinsam abwehren
- Ein Framework der nächsten Generation, das in unsere anderen Lösungen zur Erkennung und Beseitigung hochentwickelter Bedrohungen integriert werden kann

Weitere Informationen

Weitere Informationen zu McAfee Endpoint Security finden Sie hier.

Wenn Sie mehr darüber erfahren möchten, wie McAfee Endpoint Security die McAfee-Produktpalette ergänzt, besuchen Sie folgende Webseiten:

- MVISION Endpoint
- MVISION-Produktfamilie
- McAfee Threat Intelligence Exchange
- MVISION EDR
- McAfee ePolicy Orchestrator
- MVISION Insights

1. In den meisten McAfee-Endgeräte-Suites enthalten. Weitere Informationen erhalten Sie von Ihrem zuständigen Vertriebsmitarbeiter.
2. ebd.
3. Der Zeitaufwand hängt von Ihren bestehenden Richtlinien und Ihrer Umgebung ab.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 3707 0
www.mcafee.com/de

McAfee, das McAfee-Logo, ePolicy Orchestrator, McAfee ePO und VirusScan sind Marken oder eingetragene Marken von McAfee, LLC oder seinen Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer.
Copyright © 2020 McAfee, LLC. 4497_0720
JULI 2020