McAfee ePolicy Orchestrator

Inspiration und Unterstützung für Sicherheitsexperten

Für die Sicherheitsverwaltung müssen die Verantwortlichen mühsam zwischen Tools und Daten wechseln. Das verschafft den Angreifern einen Vorteil, da sie mehr Zeit für die Ausnutzung nicht erkannter Lücken zwischen Tools erhalten und dadurch mehr Schaden verursachen können. Das Team der Cyber-Sicherheitsexperten ist zahlenmäßig begrenzt und benötigt daher Unterstützung beim Koordinieren komplexer Cyber-Sicherheitsumgebungen.

Ihr Unternehmen muss schnell auf Bedrohungen für Geräte jeder Art reagieren, um den Schaden zu minimieren, und die Führungsetage verlangt Nachweise für die Effektivität der Sicherheitsmaßnahmen. Die als lokale und als Cloud-Bereitstellung verfügbare Verwaltungsplattform McAfee® ePolicy Orchestrator® (McAfee ePO™) übernimmt die zeitaufwändigen sowie potenziell fehleranfälligen manuellen Schritte und hilft den Sicherheitsverantwortlichen, die Maßnahmen schneller und effizienter zu verwalten.

Grundlegende Sicherheit

Lassen Sie uns zuerst einen Blick auf die unverzichtbaren Funktionen werfen: Die wichtigste Funktion der Sicherheitsarchitektur ist die Überwachung sowie Kontrolle der Geräte und Systeme. Laut Branchenstandards wie den CIS Controls™ und Benchmarks des Center for Internet Security sowie den in NIST SP 800-53 des National Institute of Standards Technology aufgeführten Sicherheits- und Datenschutzmaßnahmen ist die Überwachung und Kontrolle von Sicherheitsinfrastrukturen ein Muss. Über die McAfee ePO-Konsole erhalten Sie den wichtigen Überblick über die Situation. Zudem können Sie automatisch Richtlinien festlegen und durchsetzen, um in Ihrem Unternehmen zuverlässige Sicherheit zu gewährleisten. Die Verwaltung mehrerer Produkte wird vereinfacht, da die Richtlinienverwaltung und -erzwingung für das gesamte Unternehmen über eine zentrale Konsole erfolgt. Grundlegende Sicherheitsverwaltungsfunktionen sind die Voraussetzung für IT-Sicherheits-Compliance.

Hauptvorteile

- Einfache Handhabung einer branchenweit anerkannten zentralen Verwaltung mit einzigartiger integrierter und zentraler Übersicht – über die Cloud oder lokal verfügbar
- Automatisierte Workflows zur Optimierung administrativer Aufgaben und zur Steigerung der Effizienz
- Offene, umfassende Plattform, die neben McAfee mehr als 150 Drittanbieterlösungen integriert und damit schnellere und präzisere Reaktionen ermöglicht
- Gemeinsame Sicherheitsverwaltung für die meisten auf dem Markt erhältlichen Geräte
- Nutzt und erweitert die in Betriebssysteme integrierten systemeigenen Kontrollmöglichkeiten (z. B. Windows Defender)
- Für hunderte oder tausende Geräte skalierbar mit Abdeckung vom Gerät bis in die Cloud

Folgen Sie uns

Bewährte hochentwickelte Sicherheitsverwaltung – jetzt vereinfacht

Mehr als 36.000 Unternehmen und Organisationen verwenden die McAfee ePO-Konsole für die Verwaltung ihrer Sicherheit, Optimierung und Automatisierung der Compliance-Abläufe sowie Verbesserung des Gesamtüberblicks über Geräte, Netzwerke und Sicherheitsabläufe. Große Unternehmen verlassen sich auf die hochskalierbare Architektur der McAfee ePO-Konsole, die die Verwaltung hunderter und tausender Knoten über eine integrierte zentrale Oberfläche unterstützt. Mithilfe dieser Dashboard-Ansicht können Sie Aufgaben im Zusammenhang mit Risiken priorisieren und erhalten in einem neuen Schutzarbeitsbereich eine grafische Übersicht über die Sicherheitslage Ihrer gesamten digitalen Umgebung.

Administratoren können bestimmte Ereignisse im Detail betrachten, um zusätzliche Erkenntnisse zu gewinnen. Diese Übersicht reduziert den Zeitaufwand für Berichterstellung sowie Datenoptimierung und vermeidet auch bei manuellen Eingriffen potenzielle Fehler. Dank der McAfee ePO-Konsole können Unternehmenssicherheitsadministratoren die Richtlinienverwaltung vereinfachen, über unsere branchenführende Kommunikationsstruktur Data Exchange Layer (DXL) Drittanbieter-Bedrohungsdaten einbeziehen sowie Richtlinien für zahlreiche Produkte bidirektional integrieren. Diese operative Effizienz reduziert den Aufwand für alltägliche Abläufe und Datenaustausch, sodass Reaktionen schneller sowie präziser möglich sind.

Effizienz der offenen Plattform bändigt Vielfalt

Laut einer Umfrage von ESG verwenden 40 % aller Unternehmen 10 bis 25 Tools, während bei 30 % für die Verwaltung neuer Bedrohungen und Geräte 26 bis 50 Tools zum Einsatz kommen. Diese Produktvielfalt schafft einerseits Komplexität und sorgt andererseits dafür, dass die operativen Vorteile einer einheitlichen Verwaltung – von der Installation bis zur Berichterstellung – umso größer sind. Über die Hälfte der Unternehmen schätzt die Verbesserung durch die Integration von Sicherheits-Tools auf mehr als 20 % ein (MSI-Umfrage 2018). Dabei geht McAfee diese Anforderungen mit dem Offene-Plattform-Ansatz für die Sicherheitsverwaltung an, der die Konsolidierung der Vielfalt ermöglicht und gleichzeitig die verschiedenen Ressourcen schützt, Bedrohungsdaten unterstützt, Open-Source-Daten verwaltet sowie Drittanbieterprodukte integriert. McAfee ermöglicht die zentrale Kontrolle der Compliance und Verwaltung für zahlreiche Sicherheitsprodukte. Analysten können schnell zwischen den verschiedenen Produkten wechseln, um die wichtigen Daten zu finden und die erforderlichen Richtlinienaktionen auszuführen. Dank der McAfee ePO-Konsole können Sie zudem in Technologien der nächsten Generation investieren und diese über dasselbe Framework mit bestehenden Ressourcen vernetzen.

Unsere offene Plattform bietet eine Reihe von Integrationsansätzen (mit Skripts, mit APIs, ohne APIs und mit minimalem Aufwand durch die Open-Source-Kommunikationsstruktur DXL). So können Sie den für Ihre Anforderungen am besten geeigneten

Branchenanalysten nennen McAfee ePO als Grund dafür, dass Kunden dauerhaft zu McAfee wechseln.

Vorteile einer integrierten Plattform
Unternehmen mit integrierten Plattformen sind besser geschützt und erreichen kürzere Reaktionszeiten als Unternehmen ohne integrierte Plattformen.

Unternehmen mit integrierten Plattformen
- 78 % verzeichneten weniger als fünf Kompromittierungen im vergangenen Jahr
- 80 % erkannten Bedrohungen innerhalb von acht Stunden

Unternehmen ohne integrierte Plattformen
- Nur 55 % verzeichneten weniger als fünf Kompromittierungen im vergangenen Jahr
- Nur 54 % erkannten Bedrohungen innerhalb von acht Stunden

Quelle: 2016 Penn Schoen Berland

Ansatz wählen und benötigen keine umfassenden Anpassungen oder Services. Durch das McAfee® Security Innovation Alliance-Programm können wir die Entwicklung interoperabler Sicherheitsprodukte beschleunigen, die Integration dieser Produkte in komplexe Kundenumgebungen vereinfachen und ein wirklich integriertes und vernetztes Sicherheitsökosystem bereitstellen, mit dem Kunden den Wert vorhandener Sicherheitsinvestitionen maximieren können. Das McAfee Security Innovation Alliance-Programm bietet mehr als 150 Partnerintegrationen.

Zudem verbindet und optimiert die Kommunikationsstruktur Data Exchange Layer (DXL) die Sicherheitsmaßnahmen verschiedener Anbieterprodukte sowie intern entwickelter Lösungen. Mit der Integration von Cisco pxGrid und DXL erhalten Sie Zugriff auf Daten aus 50 weiteren Sicherheitstechnologien. McAfee ePO ist eine wichtige Komponente für die Verwaltung unserer robusten offenen Plattform.

Erweiterte Gerätesicherheit: Verwaltung systemeigener Sicherheits-Tools

Die erweiterbare McAfee ePO-Plattform verwaltet verschiedenste Geräte, einschließlich Geräte mit systemeigenen Kontrollmöglichkeiten. McAfee erweitert die bereits in Microsoft Windows 10 integrierten Sicherheitsfunktionen und verwaltet diese gemeinsam mit dem Betriebssystem. Dadurch erhalten Unternehmen optimierten Schutz und können gleichzeitig die systemeigenen Microsoft-Systemfunktionen nutzen. McAfee ePO verwaltet McAfee® MVISION Endpoint, eine Lösung, die speziell optimierte hochentwickelte Machine Learning-Funktionen mit der systemeigenen Sicherheit von Microsoft-Betriebssystemen kombiniert. Dabei entfallen die zusätzliche Komplexität sowie die Kosten einer weiteren Verwaltungskonsole. McAfee ePO bietet gemeinsame Verwaltungsfunktionen mit gemeinsamen Richtlinien für Windows 10-Geräte sowie sämtliche Geräte in heterogenen Unternehmen und gewährleistet dadurch Konsistenz und Einfachheit.

Zeitersparnis

Eine aktuelle MSI-Umfrage aus dem Jahr 2018 ergab, dass Kunden überzeugt sind, mit integrierten Sicherheits-Tools Zeitersparnisse von bis zu 20 % erzielen zu können.

Der Nutzen der Integration

- Höhere Effizienz von Tools und Prozessen: 61 %
- Geringere Komplexität und weniger manuelle Eingriffe, sodass sich Sicherheitsexperten auf Aufgaben konzentrieren können, die kritisches Denken erfordern: 61 %
- Verbesserte Transparenz durch die Anzeige von Daten in Mustern und im Kontext: 58 %
- Schnellere Reaktionen dank optimierter Workflows: 57 %

Quelle: MSI-Umfrage 2018

Konsistenz durch automatisierte Workflows

Die McAfee ePO-Software bietet flexible, automatisierte Verwaltungsfunktionen, damit Sie Schwachstellen, Änderungen der Sicherheitslage sowie bekannte Bedrohungen schnell erkennen, verwalten und darauf reagieren können – alles über eine Konsole. Eine 2018 im Auftrag von McAfee durchgeführte MSI-Umfrage ergab, dass Unternehmen damit rechnen, durch die Automatisierung wiederholbarer oder wiederholter Aufgaben ihren täglichen Zeitaufwand um etwa 25 % reduzieren zu können. Mit McAfee ePO können Sie Sicherheitsrichtlinien einfach über eine zentrale Ansicht bereitstellen und durchsetzen, indem Sie sich durch einige logische Schritte klicken. Die zentrale Übersicht bietet relevanten Kontext, während Sie die Aufgaben durcharbeiten, und zeigt Ihnen die Zusammenhänge zwischen den einzelnen Schritten. Dies verringert die Komplexität und minimiert die Fehlerwahrscheinlichkeit. Sie können festlegen, wie die McAfee ePO-Konsole Warnmeldungen und Sicherheitsreaktionen handhaben soll. Diese basieren auf dem Typ und dem Schweregrad der Sicherheitsereignisse in Ihrer Umgebung sowie auf den vorhandenen Richtlinien und Tools. Um die Entwicklungs- und Sicherheitsabläufe zu unterstützen, können Sie mit der McAfee ePO-Plattform automatisierte Workflows zwischen Ihren Sicherheits- und IT-Ablaufsystemen erstellen und so Probleme schnell beseitigen. Über die McAfee ePO-Konsole lassen sich zudem Behebungsmaßnahmen Ihrer IT-Schutzsysteme auslösen, zum Beispiel strengere Richtlinien zuweisen.

Dank Programmierschnittstellen für Web-Anwendungen (APIs) wird der manuelle Aufwand reduziert. Sie können vorschreiben, dass neue oder aktualisierte Richtlinien oder Tasks vor ihrer Einführung einen Genehmigungsprozess durchlaufen müssen und so das Risiko von Fehlern verringern und eine Qualitätskontrolle gewährleisten.

Typische Anwendungsszenarien

- Zeitersparnis und Verzicht auf redundante arbeitsintensive Aufgaben durch Planung von Berichten zur Sicherheits-Compliance entsprechend den Anforderungen verschiedener Verantwortlicher
- Einfache Integration der McAfee ePO-Konsole in vorhandene Geschäftsprozesse und -funktionen dank der robusten APIs (Application Programming Interfaces), um mehr Erkenntnisse zu gewinnen und Workflows zu beschleunigen (z. B. durch die Integration Ticket-Systeme, Web-Anwendungen oder Self-Service-Portale)
- Dank Synchronisierung der McAfee ePO-Konsole mit Microsoft Active Directory Gewährleistung der Sicherheit durch Bereitstellung von Agenten und Machine Learning-basierten Sicherheitslösungen, sobald neue Maschinen zum Unternehmensnetzwerk hinzugefügt werden

Schnelle Behebung

Die McAfee ePO-Plattform verfügt über integrierte, hochentwickelte Funktionen, damit das Sicherheitsteam Bedrohungen effizienter beseitigen oder Änderungen zur Wiederherstellung der Compliance vornehmen kann.

„Die Software McAfee ePO hebt sich von anderen Lösungen ab. Sie ist die zentrale Lösung für unseren Endgeräteschutz. Ich sehe alle Informationen, die ich aus allen unseren McAfee-Produkten benötige, auf einem Blick. Die benutzerfreundlichen Dashboards und integrierten Funktionen vereinfachen alle Schritte erheblich – Überblick, Berichterstellung, Bereitstellung, Aktualisierungen, Wartung, Entscheidungsfindung."

– Christopher Sacharok, Datenschutzbeauftragter, Computer Sciences Corporation

Mit der McAfee ePO-Funktion „Automatische Reaktion“ können Aktionen basierend auf einem eingetretenen Ereignis ausgelöst werden. Die möglichen Aktionen reichen dabei von einfachen Benachrichtigungen bis zu vorab bestätigten Behebungsmaßnahmen.

Typische Anwendungsszenarien für automatische Reaktionen

- Benachrichtigung des Administrators per SMS oder E-Mail über neue Bedrohungen, fehlgeschlagene Aktualisierungen oder Fehler mit hoher Priorität basierend auf festgelegten Schwellenwerten
- Anwendung von Richtlinien basierend auf Client- oder Bedrohungsereignissen, z. B. einer Richtlinie zur Verhinderung externer Kommunikation bei einem kompromittierten Host (zur Blockierung von Command-and-Control-Aktivitäten) oder zur Blockierung von Datenexfiltration/ausgehenden Datenübertragungen bis zur Zurücksetzung der Richtlinie durch den Administrator
- Kennzeichnung von Systemen und Durchführung zusätzlicher Aufgaben zur Behebung, z. B. On-Demand-Speicher-Scans bei erkannten Bedrohungen
- Auslösung registrierter ausführbarer Dateien zur Ausführung externer Skripte und Server-Befehle, z. B. Erstellung eines Tickets beim Service Desk oder Integration in andere Geschäftsprozesse
- Automatische Isolierung von Workloads oder Containern (alle Geräte) mit strengeren Richtlinien

Cloud-basierte Sicherheitsverwaltung

Unternehmen müssen die Bereitstellung von Lösungen zur Abwehr hochentwickelter Bedrohungen vereinfachen und beschleunigen. Viele erkennen die Effizienz einer Cloud-basierten Sicherheitsverwaltung, die durch das Eliminieren der Kosten und der Verwaltung einer lokalen Infrastruktur möglich ist. McAfee ePO kann mit zwei alternativen Bereitstellungsoptionen von überall aus der Cloud und jederzeit über die Cloud implementiert werden: McAfee ePO in Amazon Web Services (AWS) oder McAfee MVISION ePO. Beide Lösungen können in weniger als einer Stunde einsatzbereit sein.

- Mit McAfee ePO in AWS können Unternehmen viele systemeigene AWS-Dienste (z. B. automatische Skalierung und Amazon RDS) nutzen, anstatt eine separate Datenbank zu kaufen und zu verwalten. Dadurch können sich die Administratoren auf kritische

Sicherheitsaufgaben konzentrieren und müssen sich nicht mit der Infrastruktur befassen. McAfee ePO in AWS verwaltet McAfee® Endpoint Security, McAfee® Data Loss Prevention, McAfee® Cloud Workload Security, Data Exchange Layer sowie in McAfee ePO integrierte Drittanbieterlösungen.

- McAfee® MVISION ePO baut auf den Vorteilen von McAfee ePO als SaaS-Angebot (Software-as-a-Service) auf. Dadurch wird die Verwaltung der Plattform deutlich vereinfacht, sodass Sie sich um kritische Sicherheitsaufgaben kümmern können. Plattformaktualisierungen erfolgen transparent über ein Modell mit kontinuierlicher Bereitstellung. Da die Gerätesicherheit nach der Bereitstellung Ihres Agenten automatisch unternehmensweit bereitgestellt wird, entfällt die manuelle Installation oder Aktualisierung der Sicherheitsmaßnahmen für jedes einzelne Gerät, und die Erzwingung strengerer Bedrohungsabwehrmaßnahmen ist sichergestellt. Dies bedeutet, dass Unternehmen McAfee MVISION Endpoint und den Data Exchange Layer von überall aus über eine zentrale Konsole verwalten können. Mit McAfee MVISION ePO erhalten Sie von Geräten wichtige Erkenntnisse für Ihr Sicherheitsinformations- und Ereignis-Management (SIEM) und können sicherstellen, dass Ihre Analysten direkt auf relevante Daten zugreifen können, um die Bedrohungssuche und die Behebungsmaßnahmen zu verbessern.

Von McAfee ePO verwaltete McAfee-Produkte

McAfee-Produkte*
McAfee® Endpoint Protection (Module Bedrohungsschutz, Firewall, Webkontrolle)
McAfee MVISION Endpoint ergänzt Microsoft Defender mit Schutz vor hochentwickelten Bedrohungen
McAfee® MVISION Mobile
McAfee® Drive Encryption
McAfee® File and Removable Media Protection
McAfee® Active Response
McAfee® Management for Optimized Virtual Environments (McAfee MOVE)
McAfee Data Loss Prevention (McAfee DLP)
McAfee® Policy Auditor
McAfee® Enterprise Security Manager
McAfee® Threat Intelligence Exchange
McAfee® Application Control
McAfee® Cloud Workload Security
McAfee® Advanced Threat Defense
McAfee® Content Security Reporter
McAfee® Database Activity Monitoring
Data Exchange Layer (DXL)

**Für lokale McAfee ePO-Bereitstellungen*

Flexible Bereitstellung

Ausbringung	Hauptvorteile
Lokale McAfee ePO-Bereitstellung	Volle Kontrolle über Daten und Funktionen
McAfee ePO in AWS	Eliminiert die mit einer lokalen Lösung verbundene Hardware-Wartung
McAfee MVISION ePO ePO Software-as-a-Service*	Mehrmandantenfähiges SaaS-Angebot, bei dem die Wartung von Infrastruktur und Upgrades entfällt

**Nicht alle ePO-Funktionen sind in McAfee MVISION ePO verfügbar.*

Anwendungsszenarien: Zentral verwaltete Sicherheitslösung mit der McAfee ePO-Konsole

Produkt und Technologie	Anwendungsszenario	Vorteil
McAfee MVISION ePO McAfee MVISION Endpoint Windows 10	McAfee MVISION ePO verwaltet McAfee MVISION Endpoint, wodurch die systemeigenen Kontrollmöglichkeiten von Microsoft Windows 10 mit erweiterten Schutzfunktionen ergänzt werden. Mit einer gemeinsamen Verwaltungsplattform und einheitlichen Richtlinien für Windows und McAfee Endpoint Security können Sie hochentwickelte Bedrohungen leicht erkennen und verwalten.	Besserer Schutz für systemeigene Kontrollmöglichkeiten für Windows sowie bewährte effizientere Verwaltung
McAfee ePO McAfee Endpoint Security	McAfee Endpoint Security erkennt eine bekannte böswillige Datei auf einem Endgerät. Die McAfee ePO-Konsole legt für das Endgerät eine strengere Richtlinie fest, um die Bedrohung zu isolieren. Dieser Schritt erfolgt über eine gemeinsame Verwaltungsoberfläche.	Schnelle Eindämmung infizierter Endgeräte
McAfee ePO McAfee Data Loss Prevention McAfee Enterprise Security Manager	McAfee Enterprise Security Manager erkennt erhebliche Datenexfiltrationen auf einem Endgerät und kennzeichnet das Gerät in der McAfee ePO-Konsole. Die McAfee ePO-Konsole wendet Richtlinien zum Schutz vor Datenkompromittierung an, um die Daten zu blockieren und den Benutzer darüber zu informieren, dass er gegen Compliance-Vorgaben verstößt.	Automatisierte Durchsetzung von Richtlinien zum Schutz vor Datenkompromittierung

Beispiele für Integration

Produkt und Technologie	Anwendungsszenario für Integration	Vorteil
McAfee ePO McAfee Endpoint Security DXL Cisco Identity Service Engine (ISE) Cisco PxGrid	McAfee Endpoint Security kennzeichnet einen verdächtigen Host. Die McAfee ePO-Konsole löst zusätzliche Scans aus. Diese Information wird über PxGrid und den DXL-Austausch (über die McAfee ePO-Konsole) an Cisco ISE weitergegeben. Cisco ISE kann den Host isolieren, bis er als akzeptabel einstuft wird.	Verstärkter proaktiver Schutz
Rapid7 Nexpose McAfee ePO DXL	McAfee ePO tauscht die Ressourcenlisten mit Nexpose aus. Daher erhalten Sie über Ihre McAfee ePO-Konsole einen Überblick über Ihre Risikolage, damit Sie Richtlinien angemessen festlegen können. Schwachstellendaten werden mit der DXL-Community der Anbieter geteilt.	▪ Reduzierung der Komplexität ▪ Umfassender Überblick, zuverlässige Sicherheit und Priorisierung der Maßnahmen zur Risikominimierung – alles über ein Dashboard
Check Point NGTX Check Point NGTP McAfee ePO DXL McAfee Active Response McAfee Enterprise Security Manager	Diese Integration unterstützt den bidirektionalen Echtzeitdatenaustausch zwischen Netzwerk und Endgeräten. Ereignisse werden ebenfalls über die DXL-Community ausgetauscht. Der Blade-Server der Check Point Anti-Bot-Software blockiert Befehls- und Steuerungsdatenverkehr (Command and Control, C&C) und informiert McAfee ePO sowie weitere integrierte Sicherheitslösungen von Drittanbietern über allgemeine DXL-Themen. Anhand dieser Daten initiiert McAfee automatisch einen relevanten Behebungs-Workflow für Endgeräte. Darüber hinaus können Check Point und McAfee Zero-Day-Angriffe erkennen und in bekannte Angriffsmuster überführen. Dabei spielt es keine Rolle, ob die Angriffe vom Netzwerk oder vom Endgerät ausgehen. Durch den Austausch kritischer Daten in Echtzeit können unsere jeweiligen Produkte dank der Integration automatisiert Bedrohungen erkennen, blockieren und beheben.	▪ Schnellere Erkennung ▪ Blockierung und Behebung von Bedrohungen

Für die Nutzung der Funktionen und Vorteile der McAfee-Technologien muss das System entsprechend konfiguriert werden, und möglicherweise müssen Hard- bzw. Software oder Services aktiviert werden. Kein Computersystem kann absolut sicher sein.

McAfee hat keinen Einfluss auf und überprüft nicht die Benchmark-Daten oder Webseiten Dritter, auf die in diesem Dokument Bezug genommen wird. Kunden sollten die verlinkten Webseiten besuchen und sich selbst davon überzeugen, dass die angeführten Daten zutreffen.

McAfee
Together is power.

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