McAfee ePolicy Orchestrator

Zentrale Erfassung, Visualisierung, Freigabe und Umsetzung von Sicherheitserkenntnissen

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 mehr Schaden verursachen können. Zudem ist das Team der Cyber-Sicherheitsexperten begrenzt und benötigt Unterstützung bei der Verwaltung der komplexen Cyber-Sicherheit. Die Verwaltungsplattform McAfee® ePolicy Orchestrator® (McAfee ePO™) übernimmt die zeitaufwändigen sowie potenziell fehleranfälligen manuellen Schritte und bietet den Sicherheitsverantwortlichen die Möglichkeit, die Maßnahmen schneller und effizienter zu verwalten.

Grundlegende Sicherheit

Beginnen Sie mit den Grundlagen. Die wichtigste Funktion der Sicherheitsarchitektur ist die Überwachung sowie Kontrolle der Endgeräte und Systeme – ein Muss laut Branchenstandards für Sicherheit und Privatsphäre wie den **CIS Controls** des Center for Internet Security und **NIST SP 800-53** des National Institute of Standards Technology. 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 und Durchsetzung von Richtlinien für mehrere Sicherheitsprodukte in Ihrem Unternehmen erfolgt über eine zentrale Konsole, wodurch die Verwaltung mehrerer Produkte vereinfacht wird. Grundlegende Sicherheitsmaßnahmen sind die Voraussetzung für IT-Sicherheits-Compliance.

Bewährte hochentwickelte Sicherheitsverwaltung

Mehr als 30.000 Unternehmen und Organisationen verwenden die McAfee ePO-Konsole für die Verwaltung ihrer Sicherheit, Optimierung und Automatisierung der Compliance-Abläufe sowie Verbesserung des Gesamtüberblicks über Endgeräte, Netzwerk und Sicherheitsabläufe. Große Unternehmen verlassen sich auf die hochskalierbare Architektur der McAfee ePO-Konsole, die die Verwaltung hunderter und tausender

Folgen Sie uns

Knoten über eine zentrale Konsole unterstützt. Dank der McAfee ePO-Konsole können Unternehmenssicherheitsadministratoren die Richtlinienverwaltung vereinfachen, über den 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 besiegt 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. Dabei geht McAfee diese Anforderungen mit dem „Together is Power"-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 Steuerung der Compliance und Verwaltung für zahlreiche Sicherheitsprodukte. Sie 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.

Beispiele für Produkte, die über McAfee ePO verwaltet werden können

McAfee-Produkte	Drittanbieterprodukte
McAfee Endpoint Protection (Module Bedrohungsschutz, Firewall, Webkontrolle)	Guidance Software: enCase Enterprise
McAfee Drive Encryption	Avecto: Privilege Guard
McAfee File and Removable Media Protection	AccessData: AccesData Enterprise
McAfee Active Response	Autonomic Software: Power Manager, Patch Manager
McAfee Management for Optimized Virtual Environments (McAfee MOVE)	Xerox MFP
McAfee Data Loss Prevention (McAfee DLP)	DXL
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	

Beispiele für Anwendungsszenarien: Zentrale Verwaltung der Sicherheitsprodukte über die McAfee ePO-Konsole

Produkt und Technologie	Anwendungsszenario für zentrale Verwaltung	Vorteil
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 gefährlicher Endgeräte
McAfee ePO McAfee DLP McAfee Enterprise Security Manager	McAfee Enterprise Security Manager erkennt wichtige Daten-exfiltrationen 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
Avecto Defendpoint McAfee ePO DXL McAfee Threat Intelligence Exchange	Implementieren und verwalten Sie die branchenführende Berechtigungsverwaltungslösung Avecto Defendpoint über McAfee ePO. Konfigurationsänderungen in Avecto Defendpoint erfolgen basierend auf den Reputationsdaten von McAfee Threat Intelligence Exchange.	Geringere Komplexität Keine zusätzliche Infrastruktur erforderlich, daher geringere Gesamtbetriebskosten Berechtigungsänderungen basierend auf Bedrohungsdaten
Rapid7 Nexpose McAfee ePO DXL	McAfee ePO tauscht die Ressourcenlisten mit Nexpose aus. Daher erhalten Sie über Ihre McAfee ePO-Konsole einen Überblick über die 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 – über ein Dashboard
Check Point NGTX Check Point NGTP McAfee ePO DXL McAfee Active Response McAfee Enterprise Security Manager	Diese Integration unterstützt den bidirektionalen Echtzeitdaten-austausch zwischen Netzwerk und Endgeräten. Ereignisse werden über die DXL-Community ausgetauscht.	Schnellere Erkennung Blockierung und Behebung von Bedrohungen

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

	Integrierte Unternehmen	Nicht integrierte Unternehmen
Weniger als fünf Kompromittierungen im vergangenen Jahr	78 %	55 %
Bedrohungen innerhalb von acht Stunden erkannt	80 %	54 %

2016 Penn Schoen Berland

Erweiterbare Workflows für optimierte Prozesse

Die McAfee ePO-Datenbank bietet flexible, automatisierte Verwaltungsfunktionen, damit Sie Schwachstellen, Änderungen der Sicherheitslage sowie bekannte Bedrohungen schnell erkennen, verwalten und darauf reagieren können – alles über eine Konsole. 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.

Typische Anwendungsszenarien

- Zeitersparnis und Verzicht auf redundante arbeitsintensive Aufgaben durch Planung von Berichten zur Sicherheits-Compliance entsprechend den Anforderungen verschiedener Verantwortlicher
- Dank umfangreicher APIs unkomplizierte Integration der McAfee ePO-Konsole in bestehende Geschäftsprozesse und Funktionen für mehr Einblicke und beschleunigte Workflows, z. B. Ticket-Systeme, Web-Anwendungen oder Self-Service-Portale
- Dank Synchronisierung der McAfee ePO-Konsole mit Active Directory Gewährleistung der Sicherheit durch Bereitstellung von Agenten und Sicherheitslösungen, sobald neue Maschinen zum Unternehmensnetzwerk hinzugefügt werden

„McAfee ePolicy Orchestrator ist derzeit die leistungsstärkste Plattform für Endgeräteverwaltung und das grundlegende Verwaltungs-Tool für alle Sicherheitsprodukte im Unternehmen. Es bietet die Leistung und Flexibilität, die Unternehmen suchen. Die breit gefächerten Sicherheitsfunktionen sind über ein gemeinsames Richtlinienmodul und einen Datenstrom eng miteinander vernetzt.“

– Forrester Wave: Endpoint Security Suites (Endgeräte-sicherheits-Suites), 2016

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. 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 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 des Endgeräts mit rigoroseren Richtlinien

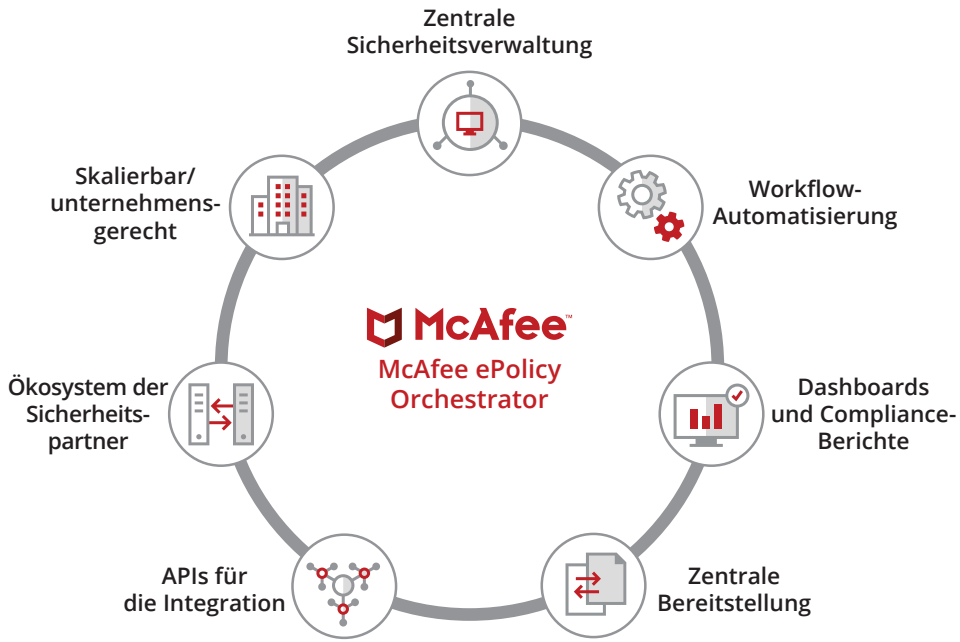

Abbildung 1. Zentrale Sicherheitsverwaltung über die McAfee ePO-Konsole

Schutz des gesamten Unternehmens dank McAfee ePO-Konsole

Zentrale Sicherheitsverwaltung

- Dedizierte Konsole für zentrale Verwaltung und Transparenz für bis zu hunderttausende Knoten im gesamten Unternehmen
- Offenes Framework zur allgemeinen Sicherheitsverwaltung von Systemen, die von McAfee und Drittanbieterlösungen geschützt werden
- Erweiterbare Plattform, die sich in die vorhandene IT-Infrastruktur integriert und sie optimal nutzt, um Bruchstellen zwischen Betriebsabläufen zu minimieren

Kürzere Reaktionszeiten bei optimaler Sicherheit

- Umfassende Übersichten und Erkenntnisse zur proaktiven Behebung interner sowie externer Sicherheitsprobleme
- Schnelle zentrale Bereitstellung von Sicherheits-Updates und -Definitionen, damit Endgeräte vor den aktuellsten Bedrohungen geschützt sind
- Kürzere Reaktionszeiten dank umsetzbarer Dashboards sowie erweiterter Funktionen für Abfragen und Berichte

Geringere Komplexität und optimierte Prozesse

- Möglichkeit zur schnellen Einrichtung mit geführter Konfiguration, automatisierten Arbeitsabläufen zur Richtlinienverwaltung sowie vordefinierten Dashboards
- Tag-basierte Richtlinienzuweisung zur genauen Zuweisung von vordefinierten Sicherheitsprofilen für einzelne Systeme oder Systemgruppen basierend auf ihrem Einsatzzweck oder Risikostatus
- Task-Katalog und automatisierte Verwaltungsfunktionen zur Optimierung von Verwaltungsprozessen und Verringerung des Verwaltungsaufwands
- Nur ein Agent zur Verwaltung mehrerer Endgeräteprodukte zur Reduzierung von Endgerätekonflikten

Skalierung für Bereitstellungen in großen Unternehmen

- Unternehmensgerechte Architektur zur Verwaltung von hunderttausenden Geräten über einen einzigen Server
- Für komplexe, heterogene IT-Umgebungen unterstützt und bewährt
- Unternehmensgerechte Berichte mit aggregierten Übersichten über Sicherheitslage und Compliance

„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, Information Security Engineer, Computer Sciences Corporation

McAfee
Together is power.

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