McAfee MVISION Endpoint

Hochentwickelte Endgerätesicherheit für Windows-Desktops und -Server

Unternehmen, die nach einfacheren, günstigeren Alternativen zu Endgeräteschutz-plattformen mit vollem Funktionsumfang suchen, wenden sich systemeigenen Sicherheits-lösungen wie Windows Defender zu. Obwohl Windows Defender einen grundlegenden Basisschutz bietet, müssen dennoch hochentwickelte Gegenmaßnahmen wie Machine Learning eingesetzt werden, um umfassend vor raffinierten dateilosen und auf Zero-Day-Malware basierenden Bedrohungen geschützt zu sein. Der Schlüssel zum Erfolg besteht darin, die bereits in Windows-Desktop- und Server-Umgebungen[1] integrierten Sicherheitsfunktionen zu nutzen, zu verstärken und zu verwalten, ohne durch mehrere Konsolen Komplexität entstehen zu lassen.

Sicherheit oder Komplexität?

Da diese Tools in der Regel separat verwaltet werden, stehen Sicherheitsteams vor dem Dilemma, verstärkte Schutzmaßnahmen und zusätzliche Komplexität gegeneinander abwägen zu müssen. Normalerweise sind deshalb auch die erhofften finanziellen und betrieblichen Einsparungen nicht realisierbar.

Die bessere Wahl: hochentwickelte Schutz-maßnahmen und eng verzahnte Verwaltung

Mit McAfee® MVISION Endpoint müssen Sie nicht mehr zwischen Effektivität und Effizienz wählen, da beides möglich ist. Sie erhalten dateibasierte, dateilose und verhaltensbasierte Machine Learning-Analysen für die Erkennung hochentwickelter Bedrohungen sowie zentrale Verwaltung aller Endgeräte in Ihrer Umgebung. Dank einer einheitlichen, zentralen Konsole für die Richtlinienverwaltung von Windows Defender Antivirus, Defender Exploit Guard, Windows-Firewall, McAfee-Schutzmaßnahmen und Mac- oder Linux-Systemen können Sie außerdem komplexe Workflows vermeiden. Durch die gemeinsame Verwaltung und einheitliche Richtlinien entfällt nicht nur der Zeitaufwand für redundante Eingaben, Sie erhalten auch eine bessere Übersicht über Ihre Endgeräteumgebung.

Maximieren Ihrer Schutzmaßnahmen

McAfee MVISION Endpoint bietet erweiterte Erkennungs- und Korrekturfunktionen als stets aktuelle Ergänzung zu den systemeigenen Kontrollmöglichkeiten. Machine Learning, Überwachung auf Diebstahl von Anmeldeinformationen und Behebung durch

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

Einheitlicher Schutz, der die Basissicherheit von Windows 10, Windows Server 2016 und 2019 nutzt, verstärkt und verwaltet

Folgen Sie uns:

Rollback ergänzen die in Windows-Desktop- und Server-Betriebssysteme integrierten grundlegenden Sicherheitsfunktionen wesentlich und wehren hochentwickelte Zero-Day-Bedrohungen effektiv ab. Mit diesem Ansatz gehen Sie der schwierigen Frage aus dem Weg, ob Sie in systemeigene oder Drittanbieter-Technologien investieren sollten, da beides aufeinander abgestimmt wird und Sie von den Vorteilen beider Lösungen profitieren.

Zeitaufwand für Wiederherstellung

Die Machine Learning-Technologie von McAfee bietet eine deutlich höhere Erkennungsrate als signaturbasierte Schutzmaßnahmen allein und weniger False-Positives als Lösungen von Mitbewerbern. So können sich die Administratoren auf die tatsächlichen Bedrohungen in ihren Umgebungen konzentrieren, anstatt Fehlalarmen und nicht böswilligen Aktivitäten nachzugehen.

McAfee MVISION Endpoint kann außerdem die Originalversionen von Dateien, die durch verdächtige Prozesse betroffen wurden, überwachen und wiederherstellen sowie andere möglicherweise hinzugefügte böswillige Dateien oder Prozesse entfernen. Für Benutzer bedeutet dies, dass ihre Produktivität nicht beeinträchtigt wird, da für sie keine behebungs- und wiederherstellungsbedingten Ausfallzeiten entstehen. Administratoren müssen weniger Zeit für das erneute Aufspielen von Images oder die Wiederherstellung kompromittierter Endgeräte aufwenden und haben mehr Zeit dafür, die Produktivität im Unternehmen zu steigern.

Mehr Transparenz

McAfee MVISION Endpoint wird über eine zentrale Konsole verwaltet, die eine Übersicht über Bedrohungen und die Compliance in der Umgebung bietet. Anstatt von einer Konsole zur anderen zu wechseln, um die Zusammenhänge zwischen dem „Was“, „Wo“ und „Wie“ bei einem Bedrohungsereignis herzustellen, werden Sie mit einem benutzerfreundlichen Dashboard und konfigurierbaren Warnmeldungen zu den wichtigsten Daten geführt.

Die Story Graph-Funktion ist ein weiteres Tool, das Administratoren bei Untersuchungen und der Stärkung des Endgeräteschutzes vor Angriffen unterstützt. Dieses Tool liefert Informationen, mit denen Sie die Aktionen nachverfolgen können, die zur Erkennung eines Bedrohungsereignisses geführt haben. Benutzer können diese Aktionen überprüfen und dadurch die Bedrohungsursache besser feststellen.

Flexible Verwaltung

McAfee MVISION Endpoint bietet folgende Optionen:

- **Reine SaaS-Verwaltung:** Mehrmandantenfähig, global skaliert und von McAfee verwaltet
  - *Vorteile:* Zeit- und ortsunabhängiger Zugriff auf die Verwaltungskonsole, automatische Aktualisierungen und Wartung im Hinblick auf niedrigere Gesamtbetriebskosten

Schneller Einstieg

- Sie können standardmäßig enthaltene Richtlinien auf Windows Defender Antivirus anwenden, die Defender Exploit Guard-Verwaltung für wichtige Regeln vereinfachen und empfohlene Regeleinstellungen für die Windows-Firewall anwenden.
- Verwenden Sie die vorhandene McAfee-Verwaltung, oder nutzen Sie für die schnelle Bereitstellung eine SaaS-basierte Konsole.
- Nutzen Sie Story Graph, um schnell Bedrohungen zu visualisieren, Maßnahmen zu ergreifen und festzustellen, wie Sie Ihre Endgeräte besser vor zukünftigen Angriffen schützen können.
- Die geringe Client-Größe gewährleistet kleine und schnelle Downloads.

- **Virtuelle Bereitstellung:** In weniger als einer Stunde vollständig einsatzbereit mit Bereitstellung der Verwaltungsfunktionen in einer Amazon Web Services-Umgebung (AWS)
  - *Vorteile:* Nutzung vorhandener Investitionen in virtualisierte Umgebungen, um Ihre Bereitstellungs- und Wartungskosten zu senken und gleichzeitig die benutzerdefinierte Kontrolle aufrechtzuerhalten
- **Lokale Bereitstellung:** Eine vor Ort lokal installierte Bereitstellung der Verwaltungs-Software auf einem Server
  - *Vorteile:* Nutzung von bereits beim Kunden vorhandenen Bereitstellungen und zentrale Verwaltung mehrerer McAfee-Technologien

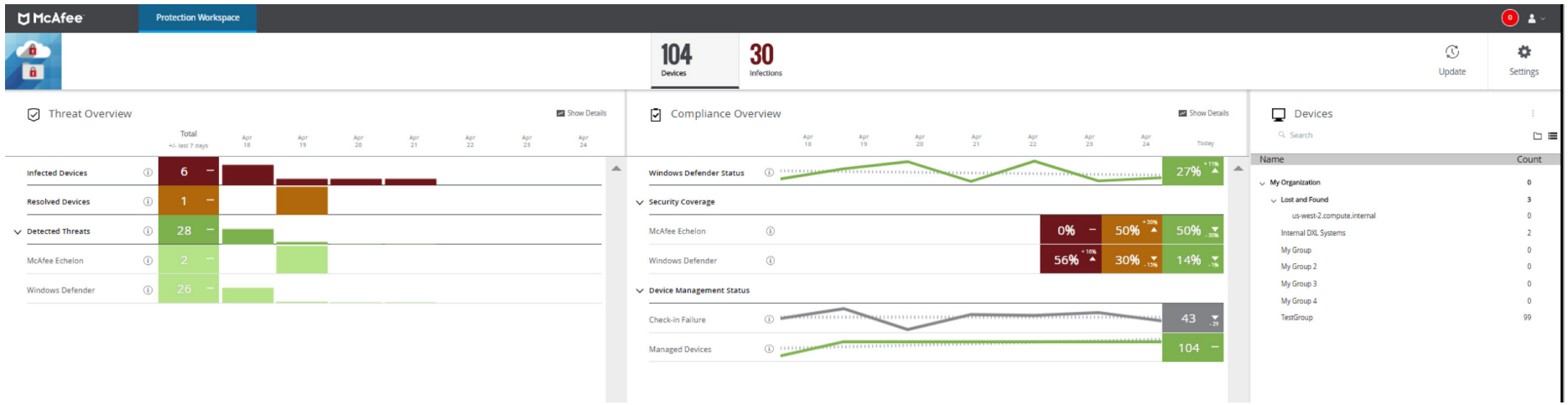

Abbildung 1. Im Bedrohungsschutz-Arbeitsbereich können Sie Bedrohungen und die Compliance für die verschiedenen McAfee- und Microsoft-Technologien anzeigen.

Ausgelegt für maximale Leistung

McAfee MVISION Endpoint ist ressourcenschonend und kompakt, da viele der Funktionen durch Cloud-basierte Dienste bereitgestellt werden. Dadurch ist eine schnelle Inbetriebnahme möglich. Die Client-Datei ist klein, sodass sie schnell heruntergeladen ist und die Bandbreite nicht belastet.

Nach der Installation sind keine Aktualisierungen für Ihre Schutzmaßnahmen erforderlich. Zukünftige Aktualisierungen erfolgen automatisch, das heißt, sie müssen nicht von einem Administrator installiert werden.

Die Auswirkungen auf die Endgeräteumgebung und die Benutzer werden auf ein Minimum reduziert. Dazu kommen standardmäßig ausgewogene Leistungseinstellungen, die im Gegensatz zu ständiger Verfügbarkeit die Rechenleistung und Bandbreite nach Bedarf skalieren.

Eine einheitliche Plattform für die gesamte Umgebung

Angesichts des Wachstums bei BYOD (Bring Your Own Device), Mobilgeräten und IoT-Geräten (Internet der Dinge) benötigen viele Unternehmen Schutz für andere Betriebssysteme und Gerätetypen. Um der zunehmenden Komplexität gerecht zu werden, hat McAfee die innovativen MVISION-Technologien eingeführt, die das strategische Ziel von einfacher Verwaltung, starkem Schutz für Windows-Systeme sowie mobile und IoT-Geräte im McAfee-Portfolio umsetzen.

Die McAfee MVISION-Technologie verwendet einen „Cloud First"-Ansatz für Gerätesicherheit, der Sicherheitsexperten bei der Verwaltung einer umfassenden Palette von McAfee- sowie Drittanbieterlösungen und systemeigenen Betriebssystem-Funktionen durch eine zentrale Konsole für Übersicht und Kontrolle unterstützt.

Mit dem McAfee Device Security-Portfolio erhalten Sie den benötigten Schutz für die gesamte Angriffsfläche: Desktops, Laptops, Tablets, Mobilgeräte, physische und virtuelle Server, Cloud-Workloads und IoT.

Welche Vorteile bietet dies für Ihr Unternehmen?

- Zentrale Verwaltung für alle Geräte
- Hochentwickelte Machine Learning-Schutzmaßnahmen zur Verhaltensanalyse und Erkennung dateibasierter und dateiloser Bedrohungen
- Schutz für Mac-, Linux-, IoT-Geräte und Mobilgeräte
- Niedrigere Gesamtbetriebskosten und optimierte Workflows

Warum sollten Sie McAfee wählen?

- Sie können mit weniger Klicks schneller mehr erreichen.
- McAfee ist der branchenweit einzige Anbieter für kombinierte Verwaltung und standardmäßig optimierte hochentwickelte Schutzmaßnahmen für systemeigene Kontrollmöglichkeiten.
- Sie erhalten ein Übersicht über die gesamte Geräteumgebung.
- Sie profitieren von einem großen offenen Ökosystem mit zahlreichen Integrationen.

Weitere Informationen

Weitere Informationen hierzu finden Sie unter **www.mcafee.com/enterprise/de-de/products/mvision-endpoint.html**.

1. Systeme mit Windows 10, Windows Server 2016 und Windows Server 2019

Die hier genannten Kosten- und Zeiteinsparungen dienen als Beispiele dafür, wie bestimmte McAfee-Produkte bei optimalen Konfigurationen und Bereitstellungen zukünftige Kosten vermeiden und Kosten- und Zeiteinsparungen ermöglichen können. Die tatsächlichen Ergebnisse können je nach Konfiguration und Bereitstellung abweichen. McAfee garantiert keine Zeit- oder Kosteneinsparungen.

McAfee und das McAfee-Logo 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 © 2019 McAfee, LLC. 4342_0819
AUGUST 2019

McAfee Together is power.

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