McAfee Enterprise Security Manager

Erkennung. Reaktion. Compliance.

Die effektivste Sicherheit beginnt mit einer Echtzeit-Übersicht aller Aktivitäten auf allen Systemen, Netzwerken, Datenbanken und Anwendungen. McAfee® Enterprise Security Manager bildet die Grundlage der McAfee-SIEM-Lösungen (Sicherheitsinformations- und Ereignis-Management). Die Software bietet Leistung, umsetzbare Informationen sowie Echtzeitdaten zur Sicherheitslage und stellt sie mit der Geschwindigkeit und Skalierbarkeit bereit, die Sicherheitsorganisationen für Erkennung, Verständnis und Abwehr verborgener Bedrohungen benötigen. Gleichzeitig wird durch das integrierte Compliance-Framework die Einhaltung rechtlicher Vorschriften gewährleistet.

Hauptvorteile

- Übersicht mit Echtzeit- und Verlaufsdaten zur umfassenden Erkennung und Abwehr von Bedrohungen
- Minutenschnelle Bereitstellung priorisierter umsetzbarer Informationen zur schnellen Reaktion auf Bedrohungen
- Durch fortschrittliche Analysen und Datenoptimierung werden Daten zu Sicherheitsinformationen
- Compliance-Framework für mehr als 240 weltweite Vorschriften

McAfee Enterprise Security Manager bietet Echtzeiterkenntnisse über die externe Gesamtlage, d. h. Bedrohungs- und Reputations-Daten sowie den Schwachstellenstatus, und stellt zudem eine Übersicht der Systeme, Daten, Risiken und Aktivitäten innerhalb Ihres Unternehmens bereit. Ihr IT-Team hat nun endlich einen umfassenden und korrelierten Zugriff auf die Inhalte sowie die Kontextinformationen, die für schnelle risikobasierte Entscheidungen und den optimalen Einsatz von Ressourcen in einer dynamischen Bedrohungssituation erforderlich sind. Dies ist unverzichtbar für die Untersuchung heimlicher und langsamer Angriffe, die Suche nach Kompromittierungsindikatoren oder die Problembehebung im Anschluss an Compliance-Kontrollen. Zur Optimierung der Sicherheitsabläufe umfasst McAfee Enterprise Security Manager auch integrierte Tools zur Konfigurations- und Änderungsverwaltung sowie für das Fall-Management und die zentrale Richtlinienverwaltung. Alle diese Komponenten werden für die Verbesserung des Workflows und der Effizienz Ihres Sicherheitsteams benötigt.

Erweiterte Bedrohungsinformationen

Beim Netzwerkverkehr, den Benutzeraktivitäten oder der Anwendungsnutzung kann jede Abweichung von der normalen Aktivität einen Hinweis darauf darstellen, dass eine Bedrohung bevorsteht und Ihre Daten oder Infrastruktur gefährdet. McAfee Enterprise Security Manager berechnet die Basisaktivität für alle erfassten Informationen in Echtzeit und warnt Sie mit priorisierten Benachrichtigungen vor potenziellen Bedrohungen, noch bevor diese auftreten. Zugleich werden diese Daten auf Muster untersucht, die auf eine schwerwiegendere Bedrohung hinweisen können. Zusätzlich nutzt McAfee Enterprise Security Manager Kontextdaten (z. B. Schwachstellen-Scans sowie Systeme zu Identitäts- und Authentifizierungsverwaltung) und ergänzt damit alle Ereignisinformationen, um ein besseres Verständnis darüber zu erhalten, wie sich Sicherheitsereignisse auf reale Geschäftsprozesse auswirken. Mithilfe dieser Informationen können Unternehmen die richtigen Daten den richtigen Mitarbeitern zuweisen, die in Echtzeit Maßnahmen ergreifen und überlegtere Entscheidungen treffen können.

Wichtige Fakten in Minuten – nicht in Stunden

Unsere hochoptimierte Datenbank-Appliance erfasst sowie verarbeitet Milliarden von Protokollereignissen aus mehreren Jahren und setzt sie mit anderen Datenströmen in Beziehung. Dabei erreicht sie die von Unternehmen benötigte Geschwindigkeit. McAfee Enterprise Security Manager kann Milliarden von Ereignissen und Abläufen speichern. Alle Informationen bleiben für sofortige Ad-hoc-Abfragen, forensische Untersuchungen, Regelüberprüfungen und Compliance-Vorschriften verfügbar.

intel Security

Skalierbare Bereitstellungsoptionen

- Hybride Bereitstellungsformen umfassen physische und virtuelle Appliances mit Hochverfügbarkeitslösungen
- Bereitstellungen mit einer einzigen Appliance für kleine Firmen oder verteilte Lösungen für große Unternehmen
- Stark skalierbare Appliances ermöglichen massive Datenerfassung für ein großes Spektrum an Sicherheits- und Infrastruktur-Ressourcen

Der schnelle Zugriff auf Ereignisdaten im Langzeitspeicher ist entscheidend für die Untersuchung heimlicher und langsamer Angriffe oder die Suche nach Hinweisen auf hochentwickelte hartnäckige Bedrohungen (APTs). Er ist auch dann wichtig, wenn ein Compliance-Audit nicht ordnungsgemäß durchgeführt werden konnte. Für alle diese Vorgänge sind der Einblick in ältere Daten sowie der volle Zugriff auf die kompletten Informationen zu jedem spezifischen Ereignis erforderlich.

Entwickelt für Big Data

Umfangreiche Sicherheitsdaten können äußerst wertvoll sein. Gleichzeitig stellen die immer weiter wachsenden Datenmengen zu Ereignissen, Ressourcen, Bedrohungen, Benutzern sowie weiteren relevanten Informationen eine massive Herausforderung für die Sicherheitsteams dar. Um dieses Problem zu lösen, entwickelte McAfee Enterprise Security Manager ein (von Gartner als eine der größten Stärken der McAfee-SIEM-Lösungen anerkanntes) Datenverwaltungssystem, das speziell für SIEM-Abläufe konzipiert wurde.

McAfee Enterprise Security Manager ist darauf ausgelegt, enorme Mengen an Kontextdaten (mit hunderten Millionen Datenpunkten) zu speichern und damit Ereignisinformationen in Echtzeit zu ergänzen. Alle diese Informationen werden umfassend indexiert, normalisiert und zueinander in Beziehung gesetzt, sodass mehr Risiken und Bedrohungen erkannt werden können. McAfee Enterprise Security Manager besitzt ein effizientes Indexierungssystem, das simultane Abläufe in Echtzeit und mit Verlaufsdaten unterstützt und die Untersuchung von Bedrohungen sowie Forensikmaßnahmen ermöglicht. Dadurch kann die McAfee-Lösung schnelle Antworten auf einfache und komplexe Abfragen liefern. Die Analyse umfangreicher Datenmengen auf sicherheitsrelevante Informationen ist eine der wichtigsten Anforderungen an ein SIEM-System. McAfee Enterprise Security Manager greift auf diese großen Datenmengen zu und geht dabei weit über Musterabgleich hinaus, um langfristige Kompromittierungsindikatoren und umsetzbare Bedrohungsdaten bereitzustellen.

Einbeziehung von Kontext und Inhalten

Mithilfe von Kontextinformationen, die von Schwachstellen-Scannern, Systemen zur Identitäts- und Authentifizierungsverwaltung, Datenschutzlösungen oder anderen unterstützten Systemen bereitgestellt werden, wird jedes Ereignis um einen Kontext erweitert. Dies ermöglicht die einfachere Korrelation von Netzwerk- und Sicherheitsereignissen einerseits und tatsächlichen Geschäftsprozessen und Richtlinien andererseits.

Durch die Skalierbarkeit und Leistungsfähigkeit von McAfee Enterprise Security Manager können größere Informationsmengen von einer größeren Anzahl von Quellen erfasst werden, darunter auch Anwendungsinhalte wie Dokumente, Transaktionen und Kommunikation. Diese sind für forensische Untersuchungen sehr wertvoll. Alle diese Informationen werden umfassend indexiert, normalisiert und zueinander in Beziehung gesetzt, sodass mehr Risiken und Bedrohungen erkannt werden können.

Optimierung der Sicherheitsprozesse

McAfee Enterprise Security Manager optimiert die Sicherheitsabläufe und bietet eine zentrale Übersicht der Sicherheitslage, des Compliance-Status und der priorisierten Sicherheitsprobleme eines Unternehmens, die eine Untersuchung erfordern.

Zudem ist McAfee Enterprise Security Manager bereits mit den Standardeinstellungen nutzbar. Die McAfee-Lösung bietet hunderte Berichte, Ansichten, Regeln und Warnungen, die sofort verwendet und problemlos angepasst werden können. Das Dashboard von McAfee Enterprise Security Manager ermöglicht die einfache Darstellung, Untersuchung und Dokumentation der wichtigsten Sicherheitsinformationen. Dies hilft bei der Einrichtung von Schwellenwerten für die typische Netzwerknutzung oder der Anpassung von Warnungen. Dank McAfee Enterprise Security Manager haben Unternehmen umfassenden und korrelierten Zugriff auf die Informationen und Kontextdaten, die sie für schnelle und überlegte Entscheidungen benötigen.

Einfachere Compliance

Durch die Zentralisierung und Automatisierung der Compliance-Überwachung und -Dokumentation macht McAfee Enterprise Security Manager zeitaufwändige manuelle Prozesse überflüssig. Hinzu kommt, dass die Integration in das Unified Compliance Framework (UCF) eine Methodik ermöglicht, bei der Daten einmal erfasst werden und die Compliance mit mehreren Vorschriften gewährleistet wird. Dadurch werden Audit-Aufwand und -Kosten auf einem Minimum gehalten. Die Unterstützung des UCF ermöglicht die effiziente Einhaltung der Compliance-Vorgaben, indem die speziellen Anforderungen jeder Vorschrift normalisiert werden. Dadurch kann eine einmal erfasste Gruppe von Ereignissen ohne weiteres den einzelnen Regelungen zugeordnet werden.

Dank McAfee Enterprise Security Manager mit seinen Hunderten vorinstallierten Dashboards, umfassenden Audit-Protokollen und Berichten für mehr als 240 weltweite und Kontroll-Frameworks wie PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX und SOX wird das Compliance-Management beschleunigt und vereinfacht. Neben der umfangreichen standardmäßigen Unterstützung sind alle Compliance-Berichte, Regeln und Dashboards von McAfee Enterprise Security Manager vollständig anpassbar.

Einbindung Ihrer IT-Infrastruktur

Die Integration in Sicherheits- und Compliance-Lösungen ermöglicht einen größeren Funktionsumfang, als ihn eine einzelne Lösung bereitstellen könnte. Zudem ist so ein bislang einmaliger Überblick über die Sicherheitslage eines Unternehmens möglich. Während McAfee-SIEM-Lösungen die Erfassung wertvoller Daten von hunderten verschiedensten Sicherheitsgeräten innerhalb einer Infrastruktur ermöglichen, erlaubt McAfee Enterprise Security Manager zusätzlich die aktive Integration in die McAfee® ePolicy Orchestrator®-Plattform (McAfee ePO™) zur richtlinienbasierten Endgeräteverwaltung, in McAfee Network Security Manager für Eindringungsschutz sowie in McAfee Vulnerability Manager für Schwachstellen-Scans und -Behebungen.

McAfee Enterprise Security Manager integriert sich in McAfee Threat Intelligence Exchange. Anders als bei den bisher üblichen Sicherheitsansätzen bietet diese Kombination Unternehmen detaillierte geschlossene Arbeitsabläufe von der Erkennung bis zur Eindämmung. Basierend auf der Endgeräteüberwachung aggregiert McAfee Threat Intelligence Exchange wenig verbreitete Angriffe und nutzt dazu weltweite, lokale und externe Bedrohungsdaten. Außerdem kann McAfee Threat Intelligence Exchange auf alle integrierten Security Connected-Produkte wie McAfee Advanced Threat Defense zugreifen, um Dateien weiter zu analysieren und Bedrohungen aufzudecken. Durch diesen Ansatz erhalten Unternehmen kontextbasierte Situationsdaten dazu, wie sich Sicherheitsereignisse auf reale Geschäftsprozesse und Richtlinien auswirken, und können davon ausgehend ihre Sicherheitsmaßnahmen besser konzentrieren.

Diese starke Verzahnung der McAfee-Sicherheitslösungen ergibt eine neue Qualität von Sicherheitsdaten, die überlegte Aktionen über die McAfee Enterprise Security Manager-Konsole ermöglichen. McAfee Enterprise Security Manager nutzt diese Integrationen zur Änderung von Richtlinien auf den Endgeräten, zur Isolierung verdächtiger Systeme im Netzwerk und zur Erfassung wertvoller Bedrohungsdaten mithilfe von Schwachstellen-Scans. All diese Vorgänge erfolgen über die McAfee Enterprise Security Manager-Konsole. Die Integration von McAfee Global Threat Intelligence (McAfee GTI) in McAfee Enterprise Security Manager umfasst Daten von McAfee Labs von mehr als 100 Millionen weltweit verteilten Bedrohungssensoren. Dadurch steht eine permanent aktualisierte Quelle bekannt böswilliger IP-Adressen zur Verfügung. Dank dieser Integrationen kann McAfee Enterprise Security Manager automatisch viele „Erstreaktionen" ausführen lassen, sodass Unternehmen schneller und effizienter auf Angriffe reagieren können.

Die Security Connected-Plattform von McAfee stellt ein einheitliches Framework für Hunderte Produkte, Services und Partner dar, die miteinander kooperieren können. Dank Security Connected-Lösungen wie McAfee Enterprise Security Manager haben Sicherheitsteams die Möglichkeit, kontextspezifische Daten in Echtzeit anzuzeigen. Dadurch erhalten sie einen sofortigen Überblick über die Sicherheitslage der gesamten Infrastruktur des Unternehmens und können die Reaktionszeit von der Entdeckung bis zur Problembehebung optimieren.

Weitere Informationen

Weitere Informationen über McAfee Enterprise Security Manager finden Sie unter **www.mcafee.com/de/products/siem/index.aspx**.

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

Intel und das Intel-Logo sind eingetragene Marken der Intel Corporation in den USA und/oder anderen Ländern. McAfee, das McAfee-Logo, ePolicy Orchestrator und McAfee ePO sind eingetragene Marken oder Marken von McAfee, Inc. oder seinen Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer. Die in diesem Dokument enthaltenen Produktpläne, Spezifikationen und Beschreibungen dienen lediglich Informationszwecken, können sich jederzeit ohne vorherige Ankündigung ändern und schließen alle ausdrücklichen oder stillschweigenden Garantien aus. Copyright © 2014 McAfee, Inc. 61292ds_esm_0914_fnl_ETMG