# McAfee Enterprise Security Manager

**Priorisierung. Untersuchung. Reaktion.**

Wirklich effektive Sicherheit beginnt mit einem Überblick über alle Aktivitäten auf Systemen, Netzwerken, Datenbanken und Anwendungen. Die Grundlage für ein effektives Sicherheits-Framework stellt dabei das Sicherheitsinformations- und Ereignis-Management (SIEM) dar. Als Kernkomponente der McAfee-SIEM-Lösung stellt McAfee® Enterprise Security Manager umsetzbare Informationen zur Verfügung und gewährleistet dabei hohe Leistung, Integration, Geschwindigkeit sowie die Skalierung, die IT-Abteilungen in Unternehmen fordern. Die Lösung bietet die Möglichkeit, verborgene Bedrohungen schnell zu priorisieren, zu untersuchen sowie zu beheben und die Compliance-Anforderungen zu erfüllen.

**Hauptvorteile**

- **Intelligent:** Dank erweiterter Analysefunktionen und umfangreichem Kontext können Sie Bedrohungen erkennen und priorisieren.
- **Umsetzbar:** Die erforderlichen Daten werden in dynamischen Übersichten dargestellt, über die Sie weitere Aktionen starten können, z. B. Ereignisse untersuchen, eindämmen und beheben sowie Maßnahmen für wichtige Warnmeldungen und Muster definieren.
- **Integriert:** Die Lösung überwacht und analysiert Daten aus einer vielseitigen, heterogenen Sicherheitsinfrastruktur und bietet dank offener Schnittstellen die Möglichkeit, Daten über zwei Wege zu integrieren. Zudem können für viele Situationen automatische Erstreaktionen definiert werden.

McAfee Enterprise Security Manager liefert Echtzeitinformationen über die externe Gesamtlage (d. h. Bedrohungsdaten und Reputations-Feeds) sowie eine Darstellung der Systeme, Daten, Risiken und Aktivitäten innerhalb Ihres Unternehmens. Die Lösung bietet Ihrem IT-Team umfassenden und korrelierten Zugriff auf die Inhalte sowie Kontextinformationen, die für schnelle risikobasierte Entscheidungen und den optimalen Einsatz von Ressourcen in einer dynamischen Bedrohungssituation sowie Unternehmensumgebung erforderlich sind. Dies ist unverzichtbar für die Untersuchung heimlicher und langsamer Angriffe, die Suche nach Kompromittierungsindikatoren oder die Behebung von Audit-Problemen. Um die Bedrohungs- und Compliance-Verwaltung in die Sicherheitsabläufe einzubinden, stellt McAfee Enterprise Security Manager zusätzlich integrierte Tools zur Verfügung, mit denen die Konfigurations- und Änderungsverwaltung, das Fall-Management sowie die zentrale Richtlinienverwaltung vereinfacht werden. Dadurch wird die Effektivität der Workflows und Sicherheitsverantwortlichen gesteigert. Die außerdem in McAfee Enterprise Security Manager enthaltenen Content Packs (Inhaltspakete) enthalten sofort einsetzbare Konfigurationen für komplexe Anwendungsszenarien, um die Implementierung von Sicherheitsabläufen zu vereinfachen.

## Unterstützung unternehmensgerechter Skalierung

Die aktuellen dynamischen sowie verteilten Unternehmensarchitekturen liefern immer mehr Roh- und Analysedaten. Damit Sicherheitsverantwortliche diese Daten schnell und effizient erfassen sowie untersuchen können, stellt McAfee Enterprise Security Manager ein Datenverwaltungssystem zur Verfügung, das speziell zur Verarbeitung von hohen Datenvolumen entwickelt wurde und bei Branchenanalysten sowie Kunden als einer der Hauptvorteile der McAfee®-SIEM-Lösungen gilt. Um Kompromisse bei

**Skalierbare Bereitstellungsoptionen**

- Dank hybrider Bereitstellungsoptionen können Sie flexibel physische und virtuelle Appliances mit Hochverfügbarkeits-optionen sowie Angebote von Managed Security Service Providern (MSSP) nutzen.
- Die Lösungen wachsen mit Ihrem Unternehmen – von Bereitstellungen mit nur einer Appliance für kleinere Unternehmen bis zu verteilten Lösungen für Großunternehmen.
- Die stark skalierbaren Appliances ermöglichen die Erfassung umfangreicher Datenmengen aus verschiedensten Sicherheits- sowie Infrastruktur-Ressourcen und wandeln die Daten in priorisierte, umsetzbare Informationen um.

der Erfassung, Nutzung und Speicherung der Daten zu vermeiden, erfolgen alle Vorgänge zur Erfassung, Verwaltung sowie Analyse der Informationen mithilfe einer stark skalierbaren Datenarchitektur. Dadurch kann vermieden werden, dass während der Untersuchung wichtige Daten fehlen, Analysen durch langsame Abfrageverarbeitung gebremst werden oder Suchvorgänge aus Leistungsgründen nur eingeschränkt möglich sind.

## Wichtige Fakten in Minuten – nicht in Stunden

Der schnelle Zugriff auf Ereignisdaten im Langzeitspeicher ist entscheidend für Zwischenfalluntersuchungen oder für die Suche nach Hinweisen auf hochentwickelte Bedrohungen. 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.

Unsere hochoptimierten Appliances erfassen sowie verarbeiten Protokollereignisse aus mehreren Jahren und setzen sie mit anderen Datenströmen (z. B. STIX-basierten Bedrohungsdaten-Feeds) in Beziehung. Dabei erreichen sie die von Ihnen 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.

## Einbeziehung von Kontext und Inhalten

Wenn Kontextinformationen (z. B. Bedrohungs-daten und Reputations-Feeds, Daten aus Identitäts- und Zugriffsverwaltungssystemen, Datenschutzlösungen oder anderen unterstützten Systemen) verfügbar sind, wird das entsprechende Ereignis um diesen Kontext ergänzt. Durch diese Zusatzinformationen können Sie Ereignisse besser verstehen und zuverlässiger bewerten, da Sie erfahren, wie Netzwerk- und Sicherheitsereignisse mit Ressourcenattributen sowie tatsächlichen Geschäftsprozessen und Unternehmensrichtlinien in Beziehung stehen.

Durch die Skalierbarkeit und Leistungsfähigkeit von McAfee Enterprise Security Manager können größere Informationsmengen von einer größeren Anzahl von Quellen erfasst werden. Dazu zählen auch Anwendungsinhalte wie Dokumente, Transaktionen und Kommunikationsvorgänge, die für forensische Untersuchungen sehr wertvoll sind. Diese Informationen werden zudem umfassend indexiert, normalisiert und korreliert, um mehr Risiken und Bedrohungen aufzudecken.

## Erweiterte Interpretation von Bedrohungen

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 sind. McAfee Enterprise Security Manager berechnet die Basisaktivität für alle erfassten Informationen 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 und ergänzt damit alle Ereignisinformationen, damit Sie die Auswirkungen der Sicherheitsereignisse auf reale Geschäftsprozesse besser verstehen.

Die in McAfee Enterprise Security Manager enthaltenen Cyber Threat Manager-Dashboards vereinfachen die Echtzeit-Überwachung und verbessern das Verständnis neu aufkommender Bedrohungen. Verdächtige oder bestätigte Bedrohungsinformationen, die über STIX/TAXII, McAfee Advanced Threat Defense bzw. Drittanbieter-Web-URLs gemeldet werden, können praktisch in Echtzeit oder im Nachhinein (per Rückverfolgung) aggregiert sowie mit Ereignisdaten korreliert werden. Dadurch wird für das Sicherheitsteam besser ersichtlich, wie sich Bedrohungen innerhalb einer Umgebung verbreiten. Mithilfe dieser Informationen können Unternehmen die richtigen Daten den richtigen Mitarbeitern zuweisen, die fast in Echtzeit Maßnahmen ergreifen und überlegtere Entscheidungen treffen können.

## Optimierung der Sicherheitsprozesse

Durch die analyseorientierte Benutzerführung können Sie mit McAfee Enterprise Security Manager flexibler agieren, noch einfacher Anpassungen vornehmen und bei Untersuchungen schneller reagieren. Die optimierten Workflows beschleunigen und verbessern die Verwaltung von Zwischenfällen. Dank schnellem und durchdachtem Zugang zu Bedrohungsdaten ist es für Analysten jedes Erfahrungsniveaus – von Anfänger bis Experte – wesentlich leichter, neue Bedrohungen zu priorisieren, zu untersuchen und abzuwehren.

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 sowie bei der Anpassung von Warnmeldungen. Dank McAfee Enterprise Security Manager haben Unternehmen umfassenden und korrelierten Zugriff auf die Informationen sowie Kontextdaten, die sie für schnelle und überlegte Entscheidungen benötigen.

Die von McAfee Enterprise Security Manager angebotenen Content Packs vereinfachen die Sicherheitsabläufe zusätzlich: Sie enthalten vorkonfigurierte Sicherheitseinstellungen, damit Sie schnell auf hochentwickelte Bedrohungs- oder Compliance-Verwaltungsfunktionen zugreifen können. Diese Content Packs sind für typische Sicherheitsanwendungsszenarien gedacht und enthalten Regelsätze, Warnmeldungen, Ansichten, Berichte, Variablen sowie Watchlists. Viele Content Packs umfassen vorkonfigurierte Auslöser für Verhaltensweisen, die möglicherweise zusätzliche Analysen oder automatische Behebungsmaßnahmen erfordern.

## 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 Vorschriften 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

Durch die Integration Ihrer Sicherheits-infrastruktur erhalten Sie einen bislang unerreichten Echtzeit-Überblick über die Sicherheitslage im Unternehmen. McAfee Enterprise Security Manager kann wertvolle Daten von Hunderten Drittanbieter-Sicherheitsgeräten sowie von Bedrohungsdaten-Feeds erfassen. Die Integration von McAfee Global Threat Intelligence (McAfee GTI) liefert zudem Daten von den mehr als 100 Millionen weltweit verteilten McAfee Labs-Bedrohungssensoren. Dadurch steht ein permanent aktualisierter Feed bekannt böswilliger IP-Adressen zur Verfügung.

McAfee Enterprise Security Manager erfasst auch Bedrohungsinformationen, die über STIX/TAXII und/oder Drittanbieter-Web-URLs gemeldet werden. Diese Daten werden analysiert und in Maßnahmen umgewandelt.

Zusätzlich kann McAfee Enterprise Security Manager aktiv mit Dutzenden weiteren Lösungen zur Zwischenfall-Verwaltung und -Analyse vernetzt werden. Dazu gehören McAfee-Lösungen sowie Produkte unserer McAfee Security Innovation Alliance-Partner.

So aggregiert McAfee Threat Intelligence Exchange zum Beispiel die Ergebnisse der Endgeräteüberwachung mit Informationen zu seltenen Angriffen, wobei weltweite, lokale sowie Drittanbieter-Bedrohungsdaten hinzugezogen werden. Zur weiteren Analyse und Bewertung von Dateien nutzt McAfee Threat Intelligence Exchange weitere integrierte Produkte wie McAfee Advanced Threat Defense.

Vorfallreaktionsteams und Administratoren können mit McAfee Active Response nach böswilligen, auf Systemen verborgenen Zero-Day-Dateien sowie im Arbeitsspeicher nach aktiven Prozessen suchen. McAfee Active Response verwendet persistente Kollektoren, um Ihre Endgeräte kontinuierlich auf spezifische Kompromittierungsindikatoren zu überwachen. Wenn ein solcher Indikator in Ihrer Umgebung gefunden wird, werden Sie automatisch benachrichtigt. Anders als bei den bisher üblichen Sicherheitsansätzen bietet diese Kombination Unternehmen detaillierte geschlossene Workflows von der Erkennung bis zur Eindämmung und Behebung.

McAfee bietet ein integriertes Sicherheitssystem, mit dem Sie neue Bedrohungen abwehren und darauf reagieren können. Wir unterstützen Sie dabei, mehr Bedrohungen schneller und mit weniger Ressourcen abzuwehren. Dank der vernetzten Architektur und der zentralen Verwaltung werden die Komplexität verringert sowie die betriebliche Effizienz Ihrer gesamten Sicherheitsinfrastruktur gesteigert. McAfee möchte Ihr Sicherheitspartner Nummer 1 sein und Ihnen einen vollständigen Satz integrierter Sicherheitsfunktionen anbieten.

## Weitere Informationen

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

Weitere Informationen zu integrierten Lösungen finden Sie unter **www.mcafee.com/de/solutions/intelligent-security-operations.aspx**.

**McAfee Ireland Ltd.**
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/de