McAfee Enterprise Log Manager

Senkung der Compliance-Kosten durch die automatisierte Erfassung, Speicherung und Verwaltung von Protokollen

Durch die richtige Erfassung und Speicherung von Protokollen können Sie die Compliance-Kosten senken und gleichzeitig einen eindeutigen Aktivitätsnachweis erbringen, der nicht angezweifelt werden kann. Mit McAfee® Enterprise Log Manager können alle Protokolldateien effizient erfasst, komprimiert und gespeichert werden. Durch die Integration mit McAfee Enterprise Security Manager stehen erweiterte Funktionen für die Suche, Analyse, Korrelation, Warnung und Berichterstellung zur Verfügung. Bei allen Ereignissen und Warnungen können Sie einfach mit einem Mausklick auf die ursprünglichen Quellprotokolldaten zugreifen. Dadurch werden auch forensische Vorgänge unterstützt.

Hauptvorteile

- Universelle Protokollerfassung und -speicherung zur Einhaltung von Compliance-Anforderungen
- Flexible Speicherung und Archivierung für jede Protokollquelle
- Unterstützung von Nachweisketten und Forensik
- Protokollanalyse und -suche
- Speicherung von Protokollen lokal oder über ein verwaltetes SAN (Storage Area Network)
- Vollständige Integration in McAfee Enterprise Security Manager
- Flexible Hybrid-Bereitstellungsoptionen mit physischen und virtuellen Appliances

McAfee Enterprise Log Manager erfasst, signiert und speichert alle beliebigen Protokolldateien. McAfee automatisiert die Verwaltung und Analyse für alle Protokolltypen. Dazu zählen Microsoft Windows-Ereignisprotokolle, Datenbankprotokolle, Anwendungsprotokolle und Systemprotokolle. Diese werden dabei signiert und geprüft, wodurch ihre Echtheit sowie Integrität sichergestellt und gleichzeitig die Voraussetzung für die Compliance mit gesetzlichen Vorschriften geschaffen wird. Dank der im Lieferumfang enthaltenen Compliance-Regelsätze und Berichte können Sie die Compliance Ihres Unternehmens sowie die Erzwingung von Richtlinien einfach nachweisen.

Diese eng verzahnte Umgebung zur Erfassung, Verwaltung und Analyse von Protokollen stärkt Ihr Sicherheitsprofil und verbessert erheblich die Compliance Ihres Unternehmens mit Standards und Normen wie PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA und SOX.

Intelligente Protokollverwaltung

McAfee Enterprise Log Manager erfasst die Protokolle auf intelligente Weise, speichert die für Compliance-Fragen erforderlichen Protokolle und verarbeitet sowie analysiert die richtigen Protokolle auf sicherheitsrelevante Ereignisse. Sie können die Protokolle so lange wie für Compliance-Anforderungen nötig in ihrem ursprünglichen Format aufbewahren. Da die ursprünglichen Protokolldateien nicht geändert werden, unterstützt McAfee Nachweisketten sowie Maßnahmen zur Unleugbarkeit.

Die Erfordernisse der Informationsaufbewahrung sind von der Protokollquelle sowie den unterschiedlichen Compliance-Anforderungen abhängig, die Sie erfüllen müssen. McAfee Enterprise Log Manager stellt mithilfe einfach anpassbarer Speicher-Pools die ordnungsgemäße Speicherung und Speicherdauer für Ihre Protokolle sicher. Dank Festplattenspeicher auf den Appliances und optionalen Fiber-Channel-Karten für SAN-Speicherung mit Hochgeschwindigkeit können Sie die für Ihre Speicheranforderungen beste Möglichkeit auswählen.

In Protokolldateien finden sich nicht alle benötigten Informationen. Sie enthalten wichtige Beweise und sind eine entscheidende Verbindung beim Aufstellen einer Nachweiskette. Dabei werfen sie jedoch auch wichtige Sicherheitsfragen auf. So finden Sie in einem Zugriffsprotokoll zwar einen Benutzernamen, jedoch keine Informationen zur Rolle oder den Berechtigungen des Benutzers. Sie sehen möglicherweise auch, auf welches System zugegriffen wurde. Es fehlen aber Informationen dazu, welche Datentypen von diesem System verarbeitet werden oder wer darauf zugreifen darf.

intel Security

Integration mit McAfee Enterprise Security Manager

Bei McAfee Enterprise Log Manager handelt es sich um eine optionale, integrierte Komponente von McAfee Enterprise Security Manager. McAfee Enterprise Log Manager speichert die Protokolle, deren Informationen anschließend von McAfee Enterprise Security Manager umfassend verarbeitet, normalisiert und analysiert werden, sodass sie sofort für Echtzeit-Sicherheitsuntersuchungen und die Reaktion auf Störfälle zur Verfügung stehen.

Wenn ein Sicherheitsereignis generiert wird, werden die verarbeiteten Ereignisdateien direkt mit der Quellprotokolldatei sowie dem betreffenden Protokolldatensatz verknüpft. Dadurch können Sie beim Ereignis-Management und bei forensischen Analysen mit nur einem Mausklick darauf zugreifen. Weitere Schritte oder das Öffnen einer zusätzlichen Anwendung sind nicht nötig. Auch das zeitaufwändige manuelle Durchsuchen der Protokolle gehört der Vergangenheit an.

Umfangreicher Kontext für die Analyse

McAfee Enterprise Security Manager und McAfee Enterprise Log Manager liefern zusammen die Kontextinformationen für jedes Protokoll und steigern damit den Wert jedes verarbeiteten Protokolldatensatzes. Folgende Informationen sind enthalten:

- Quell- oder Ziel-IP-Adresse
- Identitätskontext
- Verwendeter Hostname oder Dienst
- Schwachstelleninformationen von einem Schwachstellenbewertungs-Scanner
- Topologische Netzwerkinformationen
- Richtlinien- und Datenschutzinformationen

Flexible Speicher-Pools

Die Speicher-Pools von McAfee Enterprise Log Manager sorgen für mehr Flexibilität bei der langfristigen Aufbewahrung von Protokollen. Speicher-Pools sind virtuelle Gruppen aus nutzbarem Speicher, die auf verschiedene Gruppen physischer Speichergeräte aufgeteilt sein können (z. B. lokaler Speicher, NFS, SAN und CIF), sodass verschiedene Anforderungen an die Protokollverwaltung erfüllt werden können.

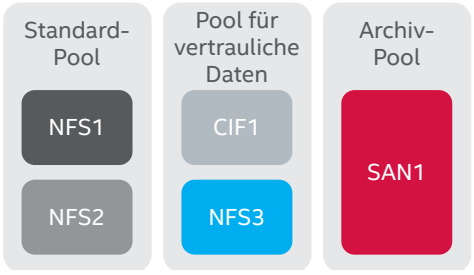

Abbildung 1. Flexible Speicher-Pools unterstützen die benutzerspezifische Protokollaufbewahrung.

Ein Speicher-Pool kann aus mehreren Geräten bestehen. Auf Grundlage des Quellgeräts können die Daten einem bestimmten Pool zugewiesen werden. Dadurch ist es möglich, Protokolle je nach ihrer Relevanz für Sicherheit, Compliance, Vertraulichkeit und andere Kriterien an separaten Orten zu speichern. So können beispielsweise Protokolle, die wichtig für die Compliance sind, in einem Pool aus verschiedenen, redundanten Netzwerkspeichergeräten abgelegt werden. Für weniger wichtige Protokolle sind auch weniger redundante Systeme geeignet. Werden die Protokolle für forensische Untersuchungen benötigt, können sie für schnellere Analysen lokal gespeichert werden.

Schnelle Implementierung

McAfee Enterprise Log Manager und McAfee Enterprise Security Manager können auf einer Kombinations-Appliance oder verteilt implementiert werden. Auf diese Weise werden sogar die größten Unternehmensnetzwerke unterstützt. Für die Bereitstellung können Sie flexibel physische und virtuelle Appliances kombinieren.

Integration in Ihre Infrastruktur

Im Gegensatz zu den meisten Protokoll-verwaltungslösungen arbeitet McAfee Enterprise Log Manager nicht isoliert, sondern zusammen mit anderen Informations-sicherheitssystemen. Über McAfee Enterprise Security Manager verbindet sich die Lösung mit Ihrer übrigen Sicherheitsinfrastruktur und vereinfacht so die Sicherheitsabläufe, verbessert die Gesamteffizienz und senkt Kosten. Sie können die intelligente Protokoll-verwaltung in leistungsstarke Analysen, Netzwerkuntersuchungen, Datenbank-Ereignis-überwachung und andere Funktionen integrieren.

Weitere Informationen 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