McAfee Data Loss Prevention Endpoint

Geraten Sie nicht wegen einer Datenkompromittierung in die Schlagzeilen

Verlieren Sie Daten, ohne es zu wissen? Kundeninformationen, Finanzdaten, Personalakten und Ihr geistiges Eigentum könnten in diesem Moment aus Ihrem Unternehmen gestohlen werden. Und die Täter sind nicht unbedingt Hacker – es können auch Ihre eigenen Mitarbeiter sein. Versehentliche oder böswillig herbeigeführte Datenverluste können sich mithilfe gängiger Wege wie E-Mails, Internetveröffentlichungen, USB-Laufwerke oder Cloud-Uploads ereignen, und die dadurch verursachten Kosten können in die Millionen gehen. Tag für Tag werden Unternehmen Opfer erheblicher Datenverluste durch versehentliches oder böswillig herbeigeführtes Durchsickern von Informationen. Was wäre, wenn Sie Datenverluste einfach und wirkungsvoll verhindern könnten? Was, wenn Sie Branchenvorschriften und gesetzliche Compliance-Regelungen einhalten und gleichzeitig Ihr geistiges Eigentum schützen könnten? Nun haben Sie diese Möglichkeit – mit der umfassenden Lösung McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint).

Schutz vor Datenverlusten – vom Endgerät bis zur Cloud

McAfee DLP Endpoint integriert sich mit MVISION Cloud DLP. Lokale DLP-Richtlinien können mit einem einzigen Mausklick in weniger als einer Minute auf die Cloud erweitert werden.[1] Lokale DLP-Klassifizierungs-Tags werden mit Cloud-DLP-Richtlinien geteilt, um sicherzustellen, dass Datenkompromittierungen konsistent erkannt werden.

Fortschrittliche Schutzmaßnahmen

McAfee DLP Endpoint bietet umfassenden Schutz für alle potenziellen Exfiltrationskanäle, beispielsweise Wechseldatenträger, die Cloud, E-Mails, Sofortnachrichten, das Web, Ausdrucke, die Zwischenablage, Screenshots, Anwendungen zum Dateiaustausch uvm.

Hauptvorteile

- **Schutz vor Datenverlusten vom Endgerät bis zur Cloud:** Ausdehnung der lokalen DLP-Richtlinien auf die Cloud, damit Datenkompromittierungen konsistent erkannt werden können
- **Fortschrittliche Schutzmaßnahmen:** Nutzung von Fingerprinting, Klassifizierung und Dateikennzeichnung zur Absicherung sensibler, unstrukturierter Daten wie geistigem Eigentum und Geschäftsgeheimnissen
- **Zentrale Verwaltung:** Optimierung des Richtlinien- und Notfall-Managements mit McAfee® MVISION ePolicy Orchestrator® (MVISION ePO™)[2]
- **Durchsetzung von Compliance-Vorgaben:** Gewährleistung der Compliance durch Kontrolle der tagtäglichen Benutzeraktionen, z. B. E-Mails, Veröffentlichungen in der Cloud, Downloads auf Wechselmediengeräte uvm.

Folgen Sie uns:

Die Durchsetzungsoptionen in McAfee DLP Endpoint umfassen:

- Zuweisung von Microsoft AIP-Labels (Azure Information Protection) für übertragene Daten sowie Erkennung von Dateien mit AIP-Label.[3]
- Integration von Drittanbieter-Verhaltensanalysen (UEBA) zur Erkennung von Bedrohungen durch Insider: Mithilfe von Sicherheitsanalysen können Sie ungewöhnliches sowie hochriskantes Verhalten von Benutzern und Entitäten aufdecken
- Manuelle Klassifizierung, damit Benutzer Dokumente manuell klassifizieren können und gleichzeitig das Bewusstsein der Mitarbeiter bezüglich des Datenschutzes erhöht sowie der Verwaltungsaufwand reduziert werden
- Von Benutzern initiierte Scan-Vorgänge und Behebungsmaßnahmen, damit Benutzer auf ihren Endgeräten Scan-Vorgänge und automatische Behebungsmaßnahmen durchführen können
- Flexible Einstufung mithilfe von Wörterbüchern, regulären Ausdrucken und Validierungsalgorithmen, registrierten Dokumenten sowie Unterstützung für Drittanbieterlösungen zur Klassifizierung durch Benutzer
- Einzigartige Kennzeichnungstechnologie zur Identifizierung von Dokumenten anhand ihrer Quelle, damit vertrauliche Informationen aus Web- und Netzwerkanwendungen sowie Netzwerkfreigaben nicht mehr dupliziert, umbenannt oder über die Unternehmensperipherie hinaus übertragen werden können
- Erweiterte Unterstützung von Virtualisierung zum Schutz von Remote-Desktops und VDI-Lösungen (Virtual Desktop Infrastructure)

Zentrale Verwaltung

- Die Verwaltung erfolgt über die Cloud-native Verwaltungskonsole MVISION ePO, um das Richtlinien- und Zwischenfall-Management zu vereinfachen.[4]
- Die Lösung nutzt die gleichen Richtlinien- sowie Klassifizierungs-Module und Workflows wie McAfee® MVISION Cloud (CASB) und McAfee® Network DLP.
- Dank zahlreicher Richtlinien und wiederverwendbarer Regelsätze besteht die Möglichkeit zur Festlegung mehrerer DLP-Richtlinien für das gesamte Unternehmen sowie zur Erstellung von Richtlinien für bestimmte Abteilungen, Geschäftsbereiche, Vorschriften uvm.
- Die erweiterte Detailanzeige bei der Verwaltung von Zwischenfällen kann jede Eigenschaft eines Zwischenfalls abfragen, filtern und anzeigen (z. B. Seriennummer des Geräts, Nachweisdateiname und Gruppen).
- Ereignisverwaltung und -überprüfung erfolgt zentral.
- Umfasst verbesserte rollenbasierte Zugangskontrollen (auch als Abgrenzung der Verantwortungsbereiche bezeichnet) für Richtlinienverwaltung sowie zur Untersuchung von Vorfällen.
- Einfacher Zugriff auf die Helpdesk-Oberfläche.
- **Benutzerschulungen:** Echtzeitrückmeldungen über informative Pop-Up-Fenster zur Stärkung der Sicherheitswahrnehmung und -kultur im Unternehmen

Unterstützte Plattformen

- Windows 10 (32-Bit- und 64-Bit-Version)
- Windows 8 und 8.1 (32-Bit- und 64-Bit-Versionen)
- Windows 7 (32-Bit- und 64-Bit-Version)
- Windows Server 2019
- Windows Server 2016 (64-Bit-Version)
- Windows Server 2012 (64-Bit-Version) und Windows Server 2012 R2 (Bit-Version)
- Windows Server 2008 (64-Bit-Version) und Windows Server 2008 R2 (32-Bit- und Bit-Version)
- macOS Catalina 10.15 oder höher
- macOS Mojave 10.14 oder höher
- macOS High Sierra 10.13 oder höher
- macOS Sierra 10.12 oder höher
- OS X El Capitan 10.11 oder höher
- OS X Yosemite 10.10 oder höher
- OS X Mavericks 10.9.0 oder höher

Unterstützte Browser

- Internet Explorer 11 oder höher
- Mozilla Firefox 48 oder höher
- Google Chrome 65 oder höher

Durchsetzung von Compliance und Schulung von Benutzern

Da die einstmals scharf abgegrenzte Unternehmens-peripherie in Auflösung begriffen ist, haben die zuständigen Abteilungen immer größere Schwierigkeiten, Compliance-Vorschriften durchzusetzen. Deshalb unterstützt McAfee DLP Endpoint Sie dabei, das alltägliche Benutzerverhalten zu überwachen und durch Benutzerschulungen die Compliance zu gewährleisten. McAfee DLP Endpoint ermöglicht mit nur einem Klick Ereignisüberwachung und die Ausgabe detaillierter Berichte, mit denen Sie gegenüber Prüfern, Vorstandsmitgliedern sowie anderen Interessengruppen die Einhaltung unternehmensinterner und gesetzlicher Richtlinien nachweisen können.

Die Lösung bietet Richtlinienvorlagen für Vorschriften und Anwendungsfälle, sodass die Einhaltung von Compliance-Vorgaben ein Kinderspiel wird. Zudem erhalten Ihre Benutzer Echtzeit-Rückmeldungen über Durchsetzungsmaßnahmen basierend auf Ihrer Unternehmensrichtlinie. Diese kleinen Schritte verbessern das Sicherheitsbewusstsein der Benutzer und helfen Ihnen, eine stärkere Sicherheitskultur in Ihrem Unternehmen aufzubauen.

1. Basierend auf einheitlichen internen McAfee-Labortests.
2. McAfee DLP Endpoint 11.5 oder höher
3. ebd.
4. ebd.

Unterstützte McAfee ePO-Software

- McAfee ePO 5.9.1 und 5.10 for DLP 11.1 oder höher

Unterstützung für McAfee MVISION ePO (SaaS)

- Für DLP 11.5 oder höher muss keine Software oder DLP-Erweiterung installiert werden. Für den Zugriff auf MVISION ePO sind Benutzername und Kennwort erforderlich.

Eine vollständige Liste der unterstützten Plattformen, Browser und Software finden Sie in der McAfee-KnowledgeBase.

Weitere Informationen

Weitere Informationen finden Sie unter www.mcafee.com/de/products/dlp-endpoint.aspx.

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