

McAfee Data Loss Prevention Endpoint

Bir sonraki veri kaybı istatistiği siz olmayın

Farkına bile varmadan veri kaybediyor olabilir misiniz? Müşteri listeleri, fikri mülkiyetleriniz, finansal talbolarınız ya da personel özlük dosyaları kurum sınırlarınızı şuan çıkartılıyor olabilir. Bunun faileri yalnızca dış tehditlerden oluşmuyor, failer kaza eseri veya kötü niyetle bazen çalışanınız da olabiliyor. Veri kayıpları email, web paylaşımları, USB sürücüler ve bulut gibi yaygın kullanılan veri çıkış kanalları ile gerçekleşebilir. Bu kayıplar potansiyel olarak size büyük zararlar verebilirler. Şirketler kötü niyetle veya kaza ile gerçekleşen bilgi sızıntıları nedeniyle büyük kayıplara uğramaktadırlar. Peki veri kayıplarını kolayca ve etkili bir şekilde durdurabilseydiniz? Sektörel ve yasal uyumluluğu sağlayıp, aynı zamanda da fikri mülkiyetlerini koruyabilseydiniz? Kapsamlı McAfee Data Loss Prevention Endpoint (McAfee DLP Endpoint) ile bunu yapabilirsiniz.

Cihazdan Buluta DLP

McAfee DLP Endpoint, MVISION Cloud DLP ile entegredir. On-premise DLP politikaları bir tıkla kolayca ve bir dakikadan az bir sürede bulut ortamına genişletilebilir. On-premise DLP sınıflandırma etiketleri bulut DLP ile paylaşılır ve istikrarlı veri kayıp denetimi gerçekleştirilir.

Gelişmiş Koruma Yeteneği

McAfee DLP Endpoint çıkarılabilir depolama aygıtları, bulut ortamı, email, anlık mesajlaşma, web, çıktı alma, işletim sistemi kopyalama panosu, ekran görüntü alıntısı, dosya paylaşım uygulamaları ve daha birçok sızıntı ihtimali taşıyan kanallar için kapsamlı koruma sunmaktadır.

Önemli Avantajları

- **Cihazdan buluta DLP:** Tutarlı bir veri kaybı denetimi için on-premise DLP politikalarını kolayca bulut ortamına genişletin.
- **Gelişmiş koruma becerileri:** Parmak izi oluşturma, sınıflandırma ve dosya etiketleme becerilerini kullanarak fikri mülkiyeti ve ticari sırlar gibi hassas ve yapılandırılmamış verileri güvence altına alın.
- **Merkezi yönetim:** McAfee MVISION ePolicy Orchestrator (MVISION ePO) ile sağlanan entegrasyon, politika ve olay yönetimini hızlandırır.
- **Uyumluluk Sağlama:** Email gönderme, bulut paylaşımı yapma, çıkarılabilir medya aygıtlarına indirme yapma gibi günlük kullanıcı hareketlerine yönelik yasal uyumluluk sağlayın.
- **Kullanıcı eğitimi:** Eğitimsel pop-up'lar vasıtası ile gerçek zamanlı sağlanan geri bildirimler, kurumsal güvenlik farkındalığını ve kültürünü şekillendirmenize yardımcı olur.

Bizimle iletişime geçin



BILGI FORMU

McAfee DLP Endpoint dahilindeki anahtar özellikler:

- Data-in-motion için Microsoft Azure Information Protection (AIP) etiketleri oluşturabilme ve AIP etiketli dosyaları tanıyabilme becerisi
- Üçüncü parti kullanıcı davranış analizi (UEBA) ile sağlanan entegrasyon, iç tehditleri savuşturur. Güvenlik analizi yaparak olağandışı ve yüksek riskli kullanıcı ve varlık davranışlarını tespit eder.
- Manuel sınıflandırma ile kullanıcılar dokümanları elle sınıflandırabilir, çalışan veri koruma farkındalığı artırılır ve yönetimsel yükler azaltılır.
- Kullanıcı tarafından başlatılabilen tarama ve onarma faaliyeti sayesinde kullanıcılar uç noktalarda keşif taramaları yapabilir ve kendi kendine onarma aksiyonları gerçekleştirebilirler.
- Sınıflandırmalar esnek ve sözlükleri, regex'i, doğrulama algoritmalarını, kayıtlı dokümanları, ve üçüncü parti sınıflandırma çözümlerine verilen destekleri içerir.
- Eşsiz etiketleme teknolojisi, belgeleri kaynaklarına göre tanımlar ve web/network uygulamalarından veya ağ paylaşımlarından gelen hassas verilerin kopyalanmasını, yeniden adlandırılmasını veya şirket sınırlarından çıkmasını engellemeye yardımcı olur.
- Geliştirilmiş sanallaştırma desteği, uzak masaüstlerini ve sanal masaüstü altyapı (VDI) çözümlerini korur.

Merkezeleştirilmiş Yönetim

- Hızlı politika ve olay yönetimi için Bulut tabanlı konsol -MVISION ePO- tarafından yönetilir.
- McAfee MVISION Cloud (CASB) ve McAfee Network DLP ile aynı politika, sınıflandırma motorlarını ve olay akışlarını paylaşır.
- Çoklu politikalar ve yeniden kullanılabilir kural setleri, organizasyon genelinde çoklu DLP politikaları tanımlamanıza ve ofis, departman, ve regülasyonlara göre politikalar oluşturmanıza olanak sağlar.
- Olay yönetiminde genişletilmiş granüler yapı ile, olayları her türlü özelliğe göre sorgulayabilir, filtreleyebilir ve görüntüleyebilirsiniz. (örn. Cihaz seri numarası, kanıt dosya ismi ve gruplar).
- Merkezi hale getirilmiş olay görüntüleme ve denetleme becerileri.
- Politika yönetimi ve olay inceleme için geliştirilmiş rol tabanlı erişim kontrolü (sorumluluk ayrımı olarak da bilinir).
- Kolay erişimli help desk arayüzü.

Desteklenen Platformlar

- Windows 10 (32-bit ve 64-bit)
- Windows 8 or 8.1 (32-bit ve 64-bit)
- Windows 7 (32-bit ve 64-bit)
- Windows Server 2019
- Windows 2016 (64-bit)
- Windows 2012 (64-bit) ve Windows 2012 R2 (64-bit)
- Windows 2008 (32-bit ve 64-bit) ve Windows 2008 R2 (32-bit ve 64-bit)
- macOS Catalina 10.15 ve sonrası
- macOS Mojave 10.14 ve sonrası
- macOS High Sierra 10.13 sonrası
- macOS Sierra 10.12 ve sonrası
- OS X El Capitan 10.11 ve sonrası
- OS X Yosemite 10.10 ve sonrası
- OS X Mavericks 10.9.0 ve sonrası

Desteklenen Platformlar

- Internet Explorer versiyon 11 veya üzeri
- Mozilla Firefox 48 veya üzeri
- Google Chrome 65 veya üzeri

BILGI FORMU

Uyumluluk Sağlama ve Kullanıcı Eğitimi

Kurumsal sınırların ortadan kalkması nedeniyle, şirketlerin uyumluluk sağlamaları gitgide zorlaşmaktadır. McAfee DLP Endpoint hem günlük kullanıcı davranışlarını takip etmenize, hem de kullanıcı eğitimi sunarak uyumluluk sağlamanıza yardımcı olmaktadır. McAfee DLP Endpoint, dahili ve idari uyumluluk önlemlerinin alınmış olduğunu denetçilere, üst yönetime ve diğer

hissedarlara kanıtlayabilecek detaylı raporları sadece bir tık ile sunmaktadır. Düzenleme ve kullanım vakalarına dair şablon politikalar sunarak uyumlu halde kalmanızı kolaylaştırmaktadır. Kullanıcılarınız ayrıca kurum politikanıza göre uygulama pop-up'ları yoluyla gerçek zamanlı geri bildirimler almaktadır. Bu küçük boyutlu eğitim imkanları, daha güçlü bir kurumsal güvenlik kültürü oluşturmanıza yardımcı olmaktadır.

Desteklenen McAfee ePO Yazılımı

- DLP 11.1 veya üzeri için McAfee ePO 5.9.1 ve 5.10

McAfee MVISION ePO (SaaS) için destek

- DLP 11.5 ve üzeri için herhangi bir yazılım veya DLP uzantı kurulumu gerekmemektedir. MVISION ePO erişimi sağlayacak doğrulama için kullanıcı adı ve şifre gerekmektedir.

Desteklenen platformların, tarayıcıların ve yazılımların tam listesi için lütfen McAfee Knowledge Base sitesini ziyaret edin.

Daha fazlası bilgi alın:

- Daha fazla bilgi için <https://www.banasorun.net/category/mcafee-enterprise/> sitesini ziyaret edin.



McAfee çözümlerinin ağınızı gizli ve gelişmiş tehditlere karşı nasıl güvence altına alabileceği hakkında daha fazla bilgi için müşteri temsilcinizle iletişime geçin veya www.banasorun.net/category/mcafee-enterprise/ adresini ziyaret edin.

