

McAfee 设备到云 DLP

统一数据保护

为了让员工更加灵活方便地访问核心业务应用程序, 大大小小的公司都在采用基于云的服务(如 Microsoft Office 365)。内部部署数据保护解决方案通常不能监控云服务(例如 Office 365)中的数据, 并且不能在云中控制协作或共享。许多组织在考虑为自己的云环境添加单独的云保护解决方案, 但是这样会导致他们的策略、报告和事件响应碎片化。这还会提高运营开销, 并且导致跨设备、网络和云服务的数据保护不一致。

McAfee® 设备到云 DLP 集成了两大行业领先技术, 可跨终端、网络和云提供统一数据保护: McAfee® Data Loss Prevention (McAfee DLP) 和 McAfee® MVISION Cloud。这种集成可以为组织提供无缝统一的数据保护体验, 在最大限度提高运营效率的同时, 将数据丢失风险降至最低。

碎片化的数据保护解决方案效率低下

为了在云中实现 DLP, 以前需要在云中重新构建已为内部部署上下文创建的 DLP 规则。内部部署 DLP 规则还缺乏“云原生协作”或“与云服务中的第三方共享”的上下文。这导致在复制已经为设备和网络上的数据完成的现有工作时花费的时间过长, 并且在不同的 DLP 引擎中, 策略强制实施可能不

一致。内部部署的 DLP 无法监控由于协作或云中共享链接造成的数据丢失。

轻松连接和同步内部部署 DLP 和云 DLP

McAfee® ePolicy Orchestrator® (McAfee ePO™) 软件大大简化了设备到云 DLP 工作。通过将 MVISION Cloud 与 McAfee ePO 软件配合使用, 可以比以往更快地保护任何云服务中的数据, 并具备云原生协作与共享的完整上下文。轻轻一点, 两款解决方案不到一分钟就可以实现连接。¹您在 McAfee ePO 软件中为自己的设备和网络构建的 DLP 规则会被推送至 MVISION Cloud, 其中可将它们应用至任何云服务以及绕过您的网络的任何云原生流量。您的数据分类会被

主要优势

无缝集成

- 在 McAfee ePO 软件中一次性分类数据, 并将分类用于设备、网络和云上上下文。
- 轻轻一点即可在一分钟内连接内部部署和云 DLP

一致的数据丢失防护

- 跨多个环境发挥作用的共享策略和分类引擎。
- 无需在多个控制台上执行更改。

涵盖所有事件管理和报告的统一视图

- 依靠对多个环境中的事件的集中式管理。
- 无需切换控制台即可查看事件和报告。

联系我们



产品简介

同步, 确保终端和云中的数据丢失防护一致。所有事件都会发送至 McAfee ePO 软件, 为您提供从设备到云的单一 DLP workflows。

企业如何通过设备到云 DLP 实现运营效率

采用 McAfee ePO 软件的客户已利用该集成尽可能简化了云服务中 DLP 的强制实施及其相应操作。例如, 一家大型食品服务制造商在需要确定云中数据位置的终端和网络文件共享上使用了 McAfee DLP, 并制定了策略来保护数据。该组织从 McAfee® Web Gateway 开始, 通过分析 Web 流量, 确定最常用的用户目的地, 以及云中保留公司数据的位置。由此, 组织发现它的大部分数据其实集中在 Microsoft Office 365 中。

这家公司对云中数据的保护要求其实与内部部署并无差别, 但云中的文件共享和协作等上下文差异带来了新的挑战。例如, 该公司需要按需扫描 Office 365 中的数据(类似于内部部署扫描), 同时还需要对进出 Office 365 的数据强制实施 DLP 规则, 这是云独有的, 超出了他们的网络监控范围。该公司确定云访问安全代理 (CASB) 是解决这些需求的最佳解决方案, 并评估了市场上的多种产品。最终, 该组织采用了 MVISION Cloud, 因为它可以紧密地与其 McAfee ePO 软件中的现有 DLP 规则集成。安全团队从 McAfee ePO 软件将内部部署数据分类推送至 MVISION Cloud, 然后使用预先构建

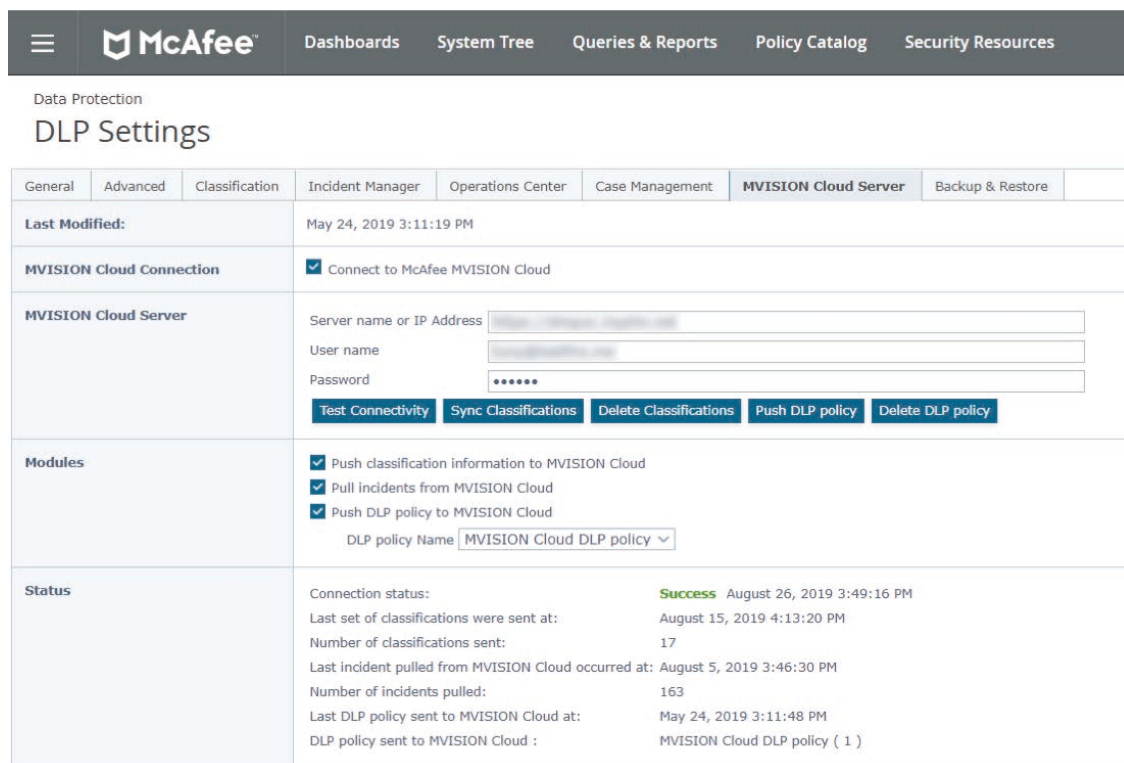


图 1. 在 McAfee ePO 软件中将 DLP 策略同步到 MVISION Cloud。

的分类为 Office 365 制定策略。现在, 无论是在设备上还是在云中, 该组织都有单一的位置来管理数据分类、DLP 事件、以及来自 McAfee Web Gateway 的 Web 流量报告 - 一切都在 McAfee ePO 软件中实现。

产品简介

“之所以选择 McAfee MVISION Cloud 作为我们的 CASB，正是因为它可以监控我们的数据去向以及谁有权访问数据，同时还可以让我们轻松了解云服务的相关风险。”

— 一家全球物联网制造商的 CISO

集中式事件管理和报告

借助 McAfee ePO 软件，用户管理所有 DLP 违规和报告时可以获得单一管理控制台体验。不管 DLP 违规来自企业设备还是云应用程序，您无需切换控制台即可查看事件和生成报告。通过对多个环境中的敏感数据进行监控，这一集中式控制台还有助于降低审核和法规合规性方面的复杂性。

摘要

随着在云中创建和发送到云中的数据日益增加，配置一套可以防范数据的任何泄露媒介（不管是企业终端、非托管设备还是网络，甚至包括云应用程序）的一致 DLP 策略的重要性也日益凸显。

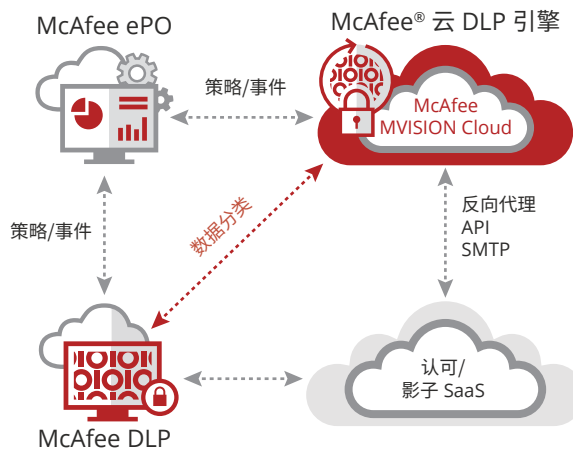


图 2. 用于 McAfee 设备到云 DLP 事件管理的一般架构。

McAfee 设备到云 DLP 为组织提供跨多个环境的无缝和统一的数据保护体验，通过提高运营效率可节省时间，并有助于将数据丢失的风险降至最低。

了解更多信息

要了解详细信息，请访问

mcafee.com/dataprotection



北京市东城区北三环东路 36 号
北京环球贸易中心 D 座 18 层, 100013
电话: 8610 8572 2000
www.mcafee.com/cn

McAfee 和 McAfee 徽标、ePolicy Orchestrator，以及 McAfee ePO 是 McAfee, LLC 或其子公司在美国和其他国家/地区的商标或注册商标。其他商标和品牌可能已声明为其他公司的财产。Copyright © 2019 McAfee, LLC. 4352_0819
2019 年 8 月

1. 基于一致的 McAfee 内部实验室测试。