Advanced Data Loss Prevention (DLP)

适用于 Acronis Cyber Protect Cloud

提早获取计划

利用专为 MSP 设计的 DLP 解决方案，自动为特定客户创建的策略

由于高达 72% 的员工可以共享公司敏感信息，Ponemon Institute 发现内部人员相关事件占所有数据泄露事件的 45% 也就不足为奇了。然而，使用传统 DLP 解决方案来修复这些风险时，您需要精通安全专业知识才能配置和操作这些解决方案 - DLP 策略并不是通用的，而是与具体业务有关，必须先了解客户独特的业务需求并手动将这些需求映射到 DLP 策略才能进行配置，因此，配置过程是一个冗长且成本高昂的手动过程。

Acronis Advanced DLP 为您提供了无与伦比的调配和管理简便性，可防止通过外围设备和网络通信从客户的工作负载中泄露数据。通过自动生成基准 DLP 策略，您可以准确有效地为每个客户创建特定于业务的策略。

利用简化的数据丢失防护来增强服务栈

上下文和内容感知型 DLP 控制	自动生成特定于客户的基准 DLP 策略	自适应 DLP 策略实施
通过分析数据传输的内容和上下文并实施基于策略的防御控制，防止通过外围设备和网络通信从工作负载中泄露数据，从而保护客户敏感数据的安全。	无需深入了解客户业务细节和手动定义策略。通过监控敏感的传出数据流，自动创建特定于业务的基准 DLP 策略。客户可以在系统实施这些策略之前对其进行验证。	消除手动操作通常需要在首次实施后管理并调整 DLP 策略。自适应策略实施选项可通过在客户工作负载上检测到的之前未使用过的新数据流来自动扩展所实施的策略。

开拓新的盈利机会

- 通过 MSP 管理的高需求 DLP 服务，**提高每位客户的收入**
- 通过可加强客户 DLP 意识的观察模式，向客户展示服务价值，**从而吸引更多客户**
- 通过使用集备份和灾难恢复、新一代防恶意软件、电子邮件安全、工作负载管理和 DLP 于一体的单个平台，实现更加轻松的服务分层，**从而控制您的总拥有成本 (TCO) 并获得更高利润**

提高工作效率并避免成本失控

- 通过自动创建特定于客户的基准 DLP 策略，**减少调配和配置所花费的时间**
- 在创建基准策略期间，可以选择由最终用户为敏感数据传输提供正当理由并在实施之前轻松验证客户，**使 DLP 策略与业务需求保持一致并最大限度地减少错误**
- 通过可配置的日志收集、警报和信息丰富的小组件，**简化合规性报告并提高 DLP 性能的可见性**

降低客户数据泄露风险

- 防止通过外围设备和网络通信泄露敏感信息，**最大限度地降低与客户内部人员相关的数据泄露风险**
- **最大限度地降低人为错误的影响**，并在公司范围内实施可接受的数据使用策略
- 通过保护受法规约束的数据，**加强客户的监管合规性**

让您的 DLP 服务在竞争者中脱颖而出

自动生成 DLP 策略	特定于客户的 DLP 策略	无与伦比的受控渠道系列	全方位 DLP 控制	通过单个中控台提供集中式网络安全保护
最大限度地减少手动操作并降低出错风险。通过为每个客户自动生成基准 DLP 策略来简化调配过程。	监控跨组织的传出敏感数据流，以便自动将客户的业务流程映射到 DLP 策略（可根据具体情况进行调整）。利用可选的最终用户协助来提高准确性，并在实施策略之前请求验证客户。	控制跨本地和网络渠道的数据流，包括可移动存储、打印机、重定向的映射驱动器和剪贴板、电子邮件和 Web 邮件、即时通讯工具、文件共享服务、社交网络和网络协议。	确保对社交媒体、Web 邮件和文件共享服务的数据传输进行独立于 Web 浏览器的控制。在远程和离线计算机上利用传出即时消息的内容检查和图像中的敏感数据检测功能。	通过使用集备份、灾难恢复、新一代防恶意软件、电子邮件安全、工作负载管理和 DLP 于一体的单个解决方案，控制您的总拥有成本（TCO）、减少管理开销并提高利润。

简化客户调配并生成和管理 DLP 策略

要帮助 MSP 简化调配和管理任务，Advanced Data Loss Prevention (DLP) 将在以下两种不同的模式下运行：

观察模式

轻松调配 DLP 服务，消除创建初始策略的复杂性。在观察模式下，代理程序会监控客户的终端计算机是否有传出的敏感数据流，以便自动生成基准 DLP 策略，或者可以选择由最终用户为风险最高的数据传输提供正当理由。

实施模式

在与客户一起验证 DLP 策略后，您可以实施该策略以开始保护客户数据的安全。实施模式允许您选择如何实施 DLP 策略：

- **严格实施** - 按照定义实施 DLP 策略，而不使用新的数据流规则对其进行扩展。除非最终用户请求一次性业务相关例外来允许覆盖数据传输块，否则任何与策略中定义的数据流规则不匹配的数据传输都会被阻止。
- **自适应实施** - 实施 DLP 策略，但可以灵活地使用新规则扩展该策略，以允许之前未观察到的业务相关数据流。