Acronis DeviceLock

全方位的终端数据丢失防护 (DLP)

在简化业务流程和支持远程工作需求的驱使下，数据可访问性呈上升趋势。然而，更广泛的数据访问权限会大大增加机密敏感信息被员工无意或故意泄露给组织外的未经授权方的风险。

90% 的组织发现自己容易受到内部威胁，许多渠道都可能会发生数据泄漏，包括通过本地外围设备和端口（如打印机和 USB）泄露了数据，以及在网络中通过电子邮件、社交网络、即时通讯工具或基于云的文件共享工具泄露了数据。如果敏感数据落入未经授权方的手中，可能会导致严重的财务和声誉损失、商业机密丢失，以及高昂的监管罚款和诉讼费用。虽然某些数据访问和传输操作是合法的，但是需要受到高度保护，以确保不会发生由于用户疏忽而导致在无意中泄露数据的情况。必须完全阻止要与未经授权的第三方共享敏感数据的其他威胁。

ACRONIS DEVICELOCK DLP

Acronis DeviceLock DLP 是一款终端数据丢失防护解决方案，可极大地降低因内部原因而导致的数据泄露风险。这款解决方案与内容分析和过滤功能相结合，执行细粒度的上下文控制（基于用户身份验证、安全组成员资格、数据类型、设备类型或网络协议、数据流方向、介质或 SSL 加密状态、日期和时间以及其他因素），以阻止或允许数据访问和传输操作。Acronis DeviceLock DLP 由多个特定于功能的互补组件组成，允许客户根据其安全要求和预算来选择最佳配置。

优势

易用：降低复杂性

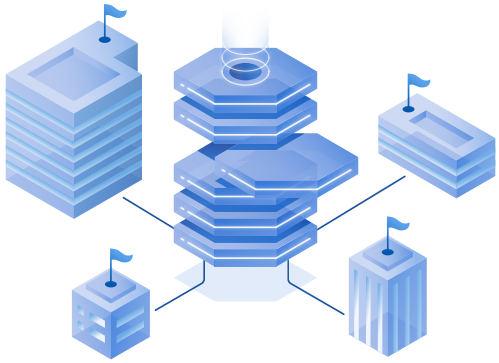
- 集中式管理
- 与 Active Directory 集成
- 模块化架构 - 通过只购买所需的功能来最大限度降低总拥有成本

高效：提高工作效率

- 通过将内部程序映射到用户必须遵守且由管理员实施的策略，帮助转换内部程序
- 监控并记录用户活动，以便执行后期分析
- 利用强大的可见性和合规性报告

安全：防止数据泄露

- 降低因内部原因导致从本地通道和网络通道泄露数据的风险
- 阻止未经授权的数据访问和传输操作
- 仅允许业务流程所需的合法操作



Acronis DeviceLock Core

这既是一个基础组件，也是一个独立产品，它可以为受保护系统上的本地数据通道实施细粒度的上下文控制、事件记录、数据影子和警报功能。其中包括外围设备和存储、端口（USB、FireWire、COM、LPT、IrDA）、本地连接的移动设备、远程终端的重定向端口和映射驱动器、屏幕截图捕获和剪贴板操作。Acronis DeviceLock Core 可以为其他功能模块提供基础平台以及所有中央管理组件。

Acronis NetworkLock 附加组件

这是 Acronis DeviceLock Core 的一个可选附加组件，可通过网络通信（包括 Web、电子邮件、即时消息、云存储服务、文件共享、网络协议等）来提供基于深度数据包检测 (DPI) 的上下文控制。基于 DPI 的控制不限于在受保护计算机上运行的特定应用程序或浏览器，允许控制来自任何 Web 浏览器、任何 SMTP 电子邮件客户端、任何 FTP 客户端和任何 Torrent 代理程序的流量。Acronis NetworkLock 借助独立于端口的协议检测以及完整会话数据重建和提取功能，实现了灵活过滤、事件记录、警报和数据影子功能。

Acronis ContentLock 附加组件

这是 Acronis DeviceLock Core 的一个可选附加组件，可以对传输到可移动媒体和即插即用设备的数据中的文本和二进制内容，以及由 NetworkLock 和 DeviceLock Core 重构并传递的网络通信中的各种数据对象的文本和二进制内容进行分析和过滤。内容分析引擎可以从 150 多种文件格式和数据类型的内容中提取文本数据，然后应用有效且可靠的内容过滤方法。结构化数据内容检测基于正则表达式（RegExp）模式和行业特定关键字词典（HIPAA、PCI 等）的预构建模板，而数据指纹则用于检测非结构化文本和二进制内容。Acronis ContentLock 可以识别由 Boldon James Classifier 产品分配给文档和文件的分类标签并依据这些标签进行过滤。该模块还具有内置的光学字符识别 (OCR) 功能，此功能可以检测文件、屏幕截图、文档和电子邮件中 30 多种图形格式的图像中的文本内容。

Acronis User Activity Monitor (UAM) 附加组件

这是一个可选附加组件，可通过捕获用户屏幕操作和击键的视频以及在录制期间在计算机上运行的应用程序的相关信息来监控最终用户的活动，以实现证据收集、安全调查和审核目的。安全管理员可通过内置查看器来查看并分析所记录的用户活动。

Acronis DeviceLock Discovery

这是一个单独的功能性组件，可以为整个组织的 IT 环境中公开的静态敏感数据提供可见性和保护。自动扫描驻留在网络共享、存储系统、Elasticsearch 数据库和 Windows 终端上的数据，找到含有公开敏感内容的文件，并提供相应的补救选项。Acronis DeviceLock Discovery 还可以启动事件管理程序，并向安全信息系统和事件管理 (SIEM) 系统或组织的 IT 安全人员发出实时警报。

Acronis DeviceLock Search Server (DLSS)

这是一个可选附加组件，可对中央影子数据库和事件日志数据库中的数据建立索引并执行全文搜索。Acronis DLSS 旨在让信息安全合规性审核、事件调查和取证分析等劳动密集型过程变得更加精确、方便和省时。

集中式管理

Acronis DeviceLock DLP 旨在简化部署和管理 DLP 解决方案等劳动密集型资源消耗过程。它提供了一组灵活的集中式管理中控台（基于管理员的需求），具有外观相同的 GUI，可以根据任何组织（从小型企业到大型企业）的需求进行量身定制：

Active Directory (AD) 环境

Acronis DeviceLock DLP 最常用的管理中控台是 Microsoft 组策略管理中控台的自定义 MMC 管理单元。这种本机集成支持通过现有 Active Directory 安装中的组策略来部署和完全管理 Acronis DeviceLock 代理程序，而无需使用单独的 DLP 策略服务器或管理平台。

非 Active Directory 环境

Acronis DeviceLock Enterprise Server (DLES) 可用于将 DLP 策略分发到所有托管的 Acronis DeviceLock 代理程序。在这种情况下，客户可获得另一个管理中控台 (Acronis DeviceLock Enterprise Manager) 的全面支持，后者是一个运行在独立计算机上的本地 Windows 应用程序。

无目录安装（例如在 Windows for Workgroups 网络中）

自定义 Acronis DeviceLock MMC 管理单元可以按终端远程管理代理程序。此选项也可用于管理 Acronis DeviceLock Discovery。

ACRONIS DEVICELOCK DLP 功能

为了全面保护使用中、动态和静态的敏感数据，Acronis DeviceLock DLP 提供了一套广泛的功能，可极大地降低数据泄露风险并支持信息安全审核和合规性操作。

适用于自带 (BYOD) 设备的虚拟 DLP

当使用领先的桌面和应用程序虚拟化解决方案（例如 Citrix XenApp/XenDesktop、Microsoft RDS 和 VMware Horizon View）时，需要防止通过 BYOD 设备泄露内部数据。DeviceLock 在 VDI 主机或终端服务器上运行，可以对所连接的设备实施“远程”上下文控制和内容感知型终端 DLP 控制，并创建一个虚拟终端 DLP 代理程序，用于防止在会话期间与本地外围设备、托管的应用程序和设备网络连接进行不受控的数据交换。

常驻于主机的光学字符识别 (OCR)

利用 Acronis DeviceLock 代理程序、Acronis DeviceLock Discovery Server 和 Acronis DeviceLock Discovery 代理程序中的内置 OCR 引擎，可以从文档和图形文件内的图片中快速准确地提取文本数据并执行检查。OCR 引擎可在本地数据流和基于网络的数据流中识别 30 多种图形格式的图片中的 30 多种语言文本。

防篡改

可配置的 Acronis DeviceLock DLP 管理员功能可防止在 Windows 和 macOS 上篡改 Acronis DeviceLock 策略设置（甚至可防止具有本地系统管理员权限的用户进行篡改）。只有使用 Acronis DeviceLock 中控台或组策略对象编辑器的指定 Acronis DeviceLock 管理员才能卸载或升级代理程序，或以任何方式修改 Acronis DeviceLock DLP 策略。

实际文件类型控制

Acronis DeviceLock 可以检查文件的二进制内容，从而确定其真实类型（而不管文件名和扩展名为何），并根据所应用的策略实施防御、记录和警报操作。

剪贴板控制

Acronis DeviceLock DLP 可以有选择地控制用户和组对剪贴板上不同数据类型（包括文件、文本、图像、音频片段，甚至是无法识别的数据类型）的对象的访问权限。可以监控并过滤从剪贴板复制到文件、文本和图像中的文本数据内容。此外，Acronis DeviceLock DLP 可以控制用户和组捕获屏幕截图（通过 Windows PrintScreen 键盘功能和第三方应用程序）的权限。

白名单

授予使用特定 USB 设备或设备型号的权限。为了能够离线工作，请通过发布访问代码来生成临时白名单。将 DVD、Blu-Ray 或 CD-ROM 磁盘（由数据特征码唯一标识）列入白名单，其中列出可访问这些磁盘的用户和组。您还可以根据 IP 地址、地址范围、子网掩码或网络端口及其范围来指定网络通信白名单，从而简化管理工作。

审核

Acronis DeviceLock DLP 的审核功能可以跟踪本地计算机上指定设备类型、端口和网络资源的用户和文件活动。它可以按用户/组、按天/小时、按端口/设备/协议类型、按读/写操作和按成功事件/失败事件预先过滤审核活动。Acronis DeviceLock DLP 使用标准事件记录子系统，并将审核记录写入 Windows 事件日志、DeviceLock 日志和带有 GMT 时间戳的 Syslog。可以将日志导出为许多标准文件格式或通过 Syslog 发送日志，以便将其导入到其他报告机制或产品中。可自动从远程计算机中收集 DeviceLock 日志，并将其集中存储在 SQL Server 中。即使具有本地管理员权限的用户也无法编辑、删除或以其他方式篡改审核日志（设置为传输到 Acronis DeviceLock Enterprise Server）。

数据影子

利用 Acronis DeviceLock 代理程序提供的自动收集功能，将镜像数据复制到外部存储设备、印刷或通过串行、并行和网络端口传输到其他地方（违反 DLP 策略）。可以将文件的完整副本保存到中央 DLP 日志数据库中，以供取证审核。影子数据可以按用户/组、天/小时、文件类型和内容进行预先过滤，以便缩小捕获和收集的范围。审核和影子功能旨在通过流压缩、服务质量 (QoS) 流量编整、本地配额设置和最佳 Acronis DLES 服务器自动选择功能，有效地使用传输和存储资源。

警报

利用 SNMP、SYSLOG 和 SMTP 警报功能，针对网络中的受保护 Windows 终端上的敏感用户活动发出实时通知。

可移动媒体加密集成

Acronis DeviceLock DLP 使用开放式集成方法来加密可移动媒体上的数据。客户可以从众多的先进技术中选择最适合其安全场景的加密解决方案，包括 Windows BitLocker To Go、macOS FileVault、Sophos SafeGuard、Symantec Drive Encryption、SecurStar DriveCrypt、TrueCrypt、Infotecs SafeDisk 和 Rutoken Disk 软件产品，以及用于预加密可移动媒体的 Cardwave SafeToGo USB 闪存驱动器。任何预加密的 USB 媒体都可以有选择地列入白名单，并按照严格的要求加以使用。

报告

出于合规性和信息安全审核目的，Acronis DeviceLock DLP 可生成各种报告，包括：

图形报告

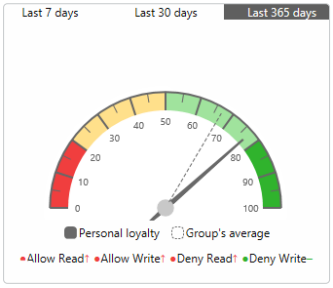
图形报告基于审核和影子日志。

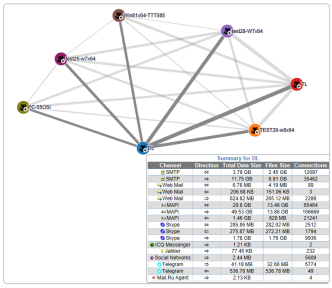
权限报告

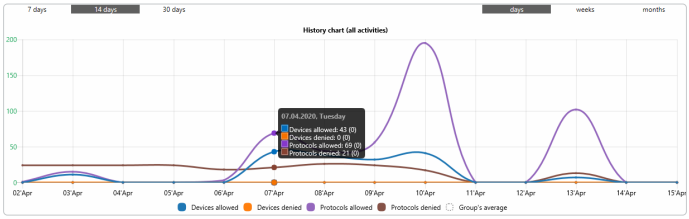
权限报告显示网络中所有终端上设置的权限和审核规则。

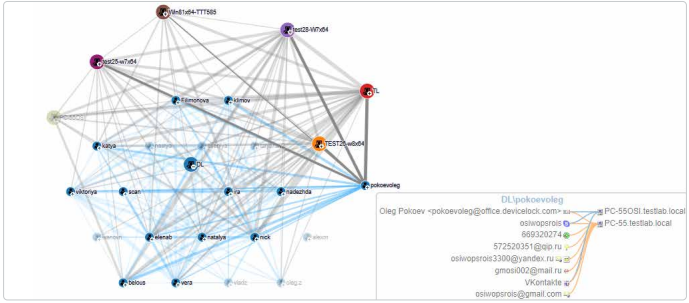
即插即用设备报告

即插即用设备报告显示当前或过去连接到网络内的终端上的 USB、FireWire 和 PCMCIA 设备。









用户档案

用户档案报告在一张用户卡片中以图形格式显示最终用户的行为统计数据集合（基于影子和事件日志）。这些统计数据会按计划或在服务器负载较低时自动更新。用户档案报告包括指定时间段内用户活动的历史图表、用于显示报告期内的活动与其基准期内的平均值出现相对偏差的忠诚度仪表板、本地或网络通道中被拒绝和被允许的操作数量、最常用操作的相关数据，以及用于显示用户通信频率的关系图。

系统要求

Acronis DeviceLock 代理程序和管理中控台

- Windows XP/Vista/7/8/8.1/10（最高为 21H1）/Server 2003-2019（32/64 位）
- Apple macOS 10.15 - 11.2.3（32/64 位）
- Microsoft RDS、Citrix XenDesktop/XenApp、XenServer、VMware Horizon View
- VMware Workstation、VMware Player、Oracle VM VirtualBox、Windows Virtual PC

Acronis DeviceLock Enterprise Server、Discovery Server、Search Server

- Windows Server 2003-2019（32/64 位）
- Microsoft RDS、XenServer、VMware vSphere Desktop

Directory 集成

- Microsoft AD（完全本机集成）
- NetIQ（Novell）eDirectory any LDAP（对象导入）

数据库

- Microsoft SQL Server/Server Express 2005 或更高版本
- PostgreSQL 9.5 或更高版本