Acronis DeviceLock

Complete endpoint data loss prevention (DLP)

Driven by the need to ease business processes and enable remote work, data accessibility is on the rise. Making data more widely accessible, however, greatly increases the risk of sensitive, confidential information being inadvertently or intentionally leaked by employees to unauthorized parties outside the organization.

With 90% of organizations feeling vulnerable to insider threats, there are many channels through which data leaks can occur, including locally through peripheral devices and ports — such as printers and USB — as well as through the network via email, social networks, instant messengers, or cloud-based file sharing. If sensitive data winds up in the hands of unauthorized parties, it can lead to severe financial and reputational damage, loss of trade secrets, and expensive regulatory fines and litigations. Some data access and transfer operations are legitimate, but need to be strictly protected to ensure no inadvertent leakage due to user negligence. Others threaten to share sensitive data with unauthorized third parties, and must be blocked entirely.

ACRONIS DEVICELOCK DLP

Acronis DeviceLock DLP is an endpoint data loss prevention solution that significantly reduces the risk of insider-related data leaks. It enforces fine-grained contextual controls (based on user authentication, security group memberships, data types, device types or network protocol, data flow direction, state of media or SSL encryption, date and time, and other factors) in combination with content analysis and filtering to block or allow data access and transfer operations. Acronis DeviceLock DLP is comprised of multiple complementary, function-specific components, allowing customers to choose the best configuration for their security requirements and budget.

BENEFITS

Easy: Reduces complexity

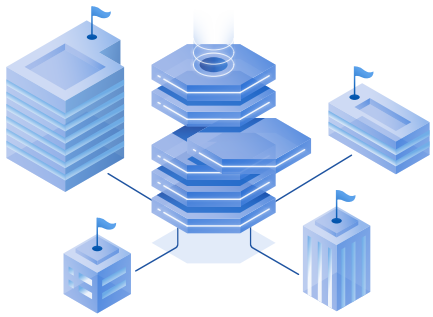
- Centralized management
- Integration with Active Directory
- Modular architecture — minimize total cost of ownership by purchasing only the functionalities you need

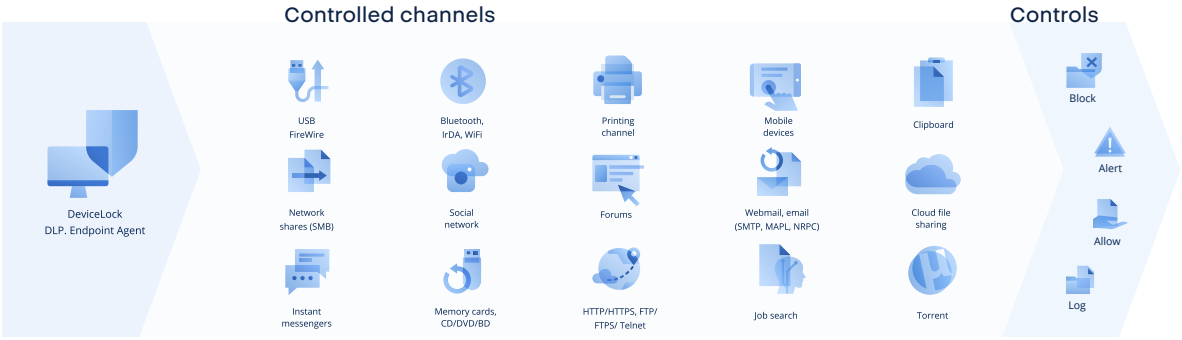
Efficient: Increases productivity

- Help transform internal procedures by mapping them into admin-forced policies that users can't avoid following
- Monitor and log user activity for post-analysis purposes
- Leverage powerful reporting for visibility and compliance

Secure: Prevents data breaches

- Reduce the risk of insider-related data leaks via local and network channels
- Block unauthorized data access and transfer operations
- Allow only legitimate operations necessary for business processes





Acronis DeviceLock Core

A fundamental component and stand-alone product that enforces fine-grained contextual controls along with event logging, data shadowing, and alerting for local data channels on protected systems. These include peripheral devices and storage, ports (USB, FireWire, COM, LPT, IrDA), locally connected mobile devices, redirected ports and mapped drives of remote terminals, screenshot captures, and clipboard operations. Acronis DeviceLock Core provides the base platform as well as all central management and administrative components for other functional modules.

Acronis NetworkLock add-on

An optional add-on to Acronis DeviceLock Core that provides contextual control based on deep packet inspection (DPI) over network communications, including web, email, instant messengers, cloud storage services, file sharing, network protocols, and more. The DPI-based controls are not limited to particular applications or browsers running on the protected computer allowing to control traffic from any web browser, any SMTP email client, any FTP client, and any Torrent agent. Acronis NetworkLock's port-independent protocol detection — along with complete session data reconstruction and extraction — allows for flexible filtering, event logging, alerting, and data shadowing.

Acronis ContentLock add-on

An optional add-on to Acronis DeviceLock Core that implements analysis and filtering of the textual and binary content of data transferred to removable media and plug-and-play devices, as well as of various data objects from network communications that are reconstructed and passed to it by NetworkLock and DeviceLock Core. The content analysis engine can extract textual data from 150+ file formats and data types, and then apply effective and reliable content filtering methods. Content detection of structured data is based on pre-built templates of regular expression (RegExp) patterns and industry-specific keyword dictionaries (HIPAA, PCI, etc.), while data fingerprinting is used to detect unstructured textual and binary content. Acronis ContentLock can recognize, and filter by, classification labels assigned to documents and files by Boldon James Classifier products. The module also has built-in optical character recognition (OCR) for detecting textual content in images across more than 30 graphical formats in files, screenshots, documents, and emails.

Acronis User Activity Monitor (UAM) add-on

An optional add-on component, that provides the ability to monitor end user activities for evidence collection, security investigation and auditing purposes by capturing video of the user's on-screen actions, as well as keystrokes and information about applications running on the computer during recording. Security administrators can view and analyze recorded user activities through built-in viewers.

Acronis DeviceLock Discovery

A separate functional component, providing visibility and protection for exposed sensitive data at rest across organization's IT environment. Automatically scans data residing on network shares, storage systems, Elasticsearch databases, and Windows endpoints, locating files with exposed sensitive content and providing options to protect them with remediation actions. Acronis DeviceLock Discovery can also initiate incident management procedures with real-time alerts to Security Information and Event Management (SIEM) systems or to IT security personnel in the organization.

Acronis DeviceLock Search Server (DLSS)

An optional add-on component that indexes and performs full text searches on data in the central shadowing and event log database. Acronis DLSS is designed to make the labor-intensive processes of information security compliance auditing, incident investigations, and forensic analysis more precise, convenient and time-efficient.

Central management

Acronis DeviceLock DLP is designed to ease the labor-intensive, resource-consuming processes of deploying and managing a DLP solution. It offers a flexible set of central management consoles (based on administrators' needs), which have the same look-and-feel GUI and can be tailored to the requirements of any organization — from small businesses to large enterprises:

Active Directory (AD) environments

The most widely used management console for Acronis DeviceLock DLP is a custom MMC snap-in to the Microsoft Group Policy Management Console. This native integration enables Acronis DeviceLock agents to be deployed and fully managed via Group Policies from an existing Active Directory installation, with no need for a separate DLP policy server or management platform.

Non-Active Directory environments

The Acronis DeviceLock Enterprise Server (DLES) can be used to distribute DLP policies to all managed Acronis DeviceLock agents. In such cases, customers are fully supported by another management console — Acronis DeviceLock Enterprise Manager, a native Windows application that runs on a separate computer.

Directory-less installations (e.g. in a Windows for Workgroups network)

The custom Acronis DeviceLock MMC snap-in can remotely manage agents on a per-endpoint basis. This option is also used to manage Acronis DeviceLock Discovery.

ACRONIS DEVICELOCK DLP FEATURES

To ensure the thorough protection of sensitive data in use, in motion, and at rest, Acronis DeviceLock DLP provides an extensive set of features that greatly decrease the risks from data breaches and support information security auditing and compliance efforts.

Virtual DLP for BYOD devices

Prevent insider data leaks via BYOD devices when using leading desktop and application virtualization solutions like Citrix XenApp/ XenDesktop, Microsoft RDS, and VMware Horizon View. Running on a VDI host or terminal server, DeviceLock "remotes" contextual and content-aware endpoint DLP controls to the connected device to create a virtual endpoint DLP agent that prevents uncontrolled data exchanges to local peripherals, hosted applications, and network connections of the device while in session.

Host–resident optical character recognition (OCR)

The built-in OCR engine in Acronis DeviceLock agent, Acronis DeviceLock Discovery Server, and Acronis DeviceLock Discovery agent allows quick efficient and accurate extraction and inspection of textual data from pictures in documents and graphical files. The OCR engine recognizes more than 30 languages in over 30 graphic formats in both local and network-based data flows.

Tamper protection

The configurable Acronis DeviceLock DLP Administrators feature prevents tampering with Acronis DeviceLock policy settings on Windows and macOS, even by users with local system administration privileges. Only designated Acronis DeviceLock administrators working from an Acronis DeviceLock console or Group Policy Object Editor can uninstall or upgrade the agent, or modify Acronis DeviceLock DLP policies in any way.

True file type control

Acronis DeviceLock looks into a file's binary content to determine its true type (regardless of file name and extension), and enforces preventive, logging, and alerting actions per the applied policy.

Clipboard control

Acronis DeviceLock DLP selectively controls user and group access to objects of different data types on the clipboard, including files, text, images, audio fragments, and even unidentified data types. Content of textual data copied via the clipboard in files, text, and images can be monitored and filtered. In addition, Acronis DeviceLock DLP controls users' and groups' rights to capture screenshots — both through the Windows PrintScreen keyboard function and through third-party applications.

Allowlisiting

Authorize the use of specific USB devices or device models. For offline work purposes, make a temporary allowlist by issuing an access code. Allowlist DVD, Blu-Ray, or CD-ROM disks, uniquely identified by data signature, listing users and groups that can access them. You can also specify allowlisting of network communications based on IP address, address range, subnet masks, or network ports and their ranges, easing administrative efforts.

Auditing

Acronis DeviceLock DLP's auditing capability tracks user and file activity for specified device types, ports, and network resources on a local computer. It can pre-filter audit activities by user/group, by day/ hour, by port/device/protocol type, by reads/writes, and by success/ failure events. Acronis DeviceLock DLP employs the standard event logging subsystem and writes audit records to a Windows Event Log, DeviceLock Log, and Syslog with GMT timestamps. Logs can be exported to many standard file formats or send via Syslog for import into other reporting mechanisms or products. DeviceLock Logs are automatically collected from remote computers and centrally stored in SQL Server. Even users with local admin privileges can't edit, delete, or otherwise tamper with audit logs set to transfer to Acronis DeviceLock Enterprise Server.

Data shadowing

Mirror data copied to external storage devices, printed, or transferred through serial, parallel, and network ports in violation of DLP policies through auto-collection by the Acronis DeviceLock agent. A full copy of the files can be saved to the central DLP log database populated for forensic review. Shadow data can be pre-filtered by user/group, day/hour, file type, and content to narrow down what's captured and collected. Audit and shadowing features are designed for efficient use of transmission and storage resources with stream compression, traffic shaping for quality of service (QoS), local quota settings, and optimal Acronis DLES server auto selection.

Alerting

Leverage SNMP, SYSLOG, and SMTP alerting capabilities for real-time notification of sensitive user activities on protected Windows endpoints across the network.

Removable media encryption integration

Acronis DeviceLock DLP takes an open integration approach to the encryption of data on to removable media. Customers have the option of using the encryption solution that best fits their security scenarios among best-of-breed technologies that include Windows BitLocker To Go, macOS FileVault, Sophos SafeGuard, Symantec Drive Encryption, SecurStar DriveCrypt, TrueCrypt, Infotecs SafeDisk, and Rutoken Disk software products, and Cardwave SafeToGo USB flash drives for pre-encrypted removable media. Any pre-encrypted USB media can be selectively whitelisted with strictly enforced usage.

Reporting

Acronis DeviceLock DLP can generate various reports for compliance and information security auditing purposes, including:

Graphical reports

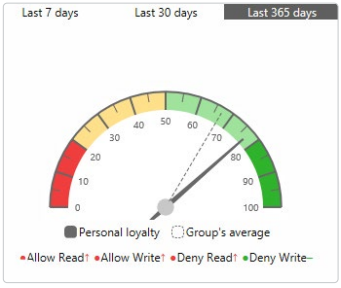
Graphical reports based on audit and shadow logs.

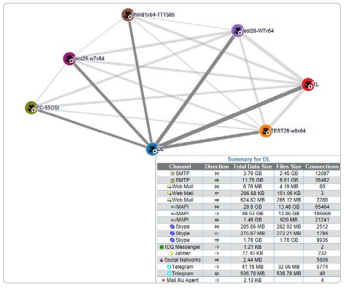
Permissions reports

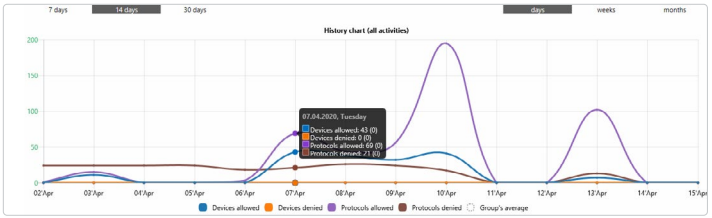
Permissions reports that display permissions and audit rules set on all endpoints across the network.

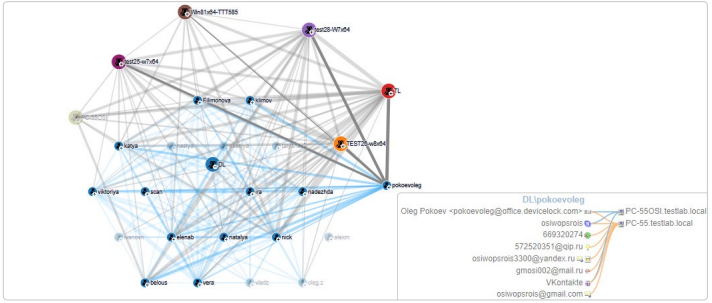
Plug-n-Play devices report

Plug-and-play device reports display USB, FireWire, and PCMCIA devices currently or historically connected to endpoints in the network.









User Dossiers

User dossiers present a collection of end-user action statistics in a graphical format, based on shadow and event logs, as a single user card. These statistics are automatically updated on a schedule or during periods of low server load. User dossiers include a historical chart of user activities in a specified period, and a loyalty dashboard representing the relative deviation of activities during the reporting period from their average in a baseline period, the number of denied and allowed operations in local or network channels, data on the most common operations, and a relations chart that visualizes the frequency of user communications.

SYSTEM REQUIREMENTS

Acronis DeviceLock Agents and Management Consoles

- Windows XP/Vista/7/8/8.1/10 (up to 21H1)/Server 2003-2019 (32/64-bit)
- Apple macOS 10.15 - 11.2.3 (32/64-bit)
- 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-bit)
- Microsoft RDS, XenServer, VMware vSphere Desktop

Directory integration

- Microsoft AD (full native)
- NetIQ (Novell) eDirectory any LDAP (object import)

Databases

- Microsoft SQL Server/Server Express 2005 or newer
- PostgreSQL 9.5 or newer

Acronis

Learn more at
www.acronis.com