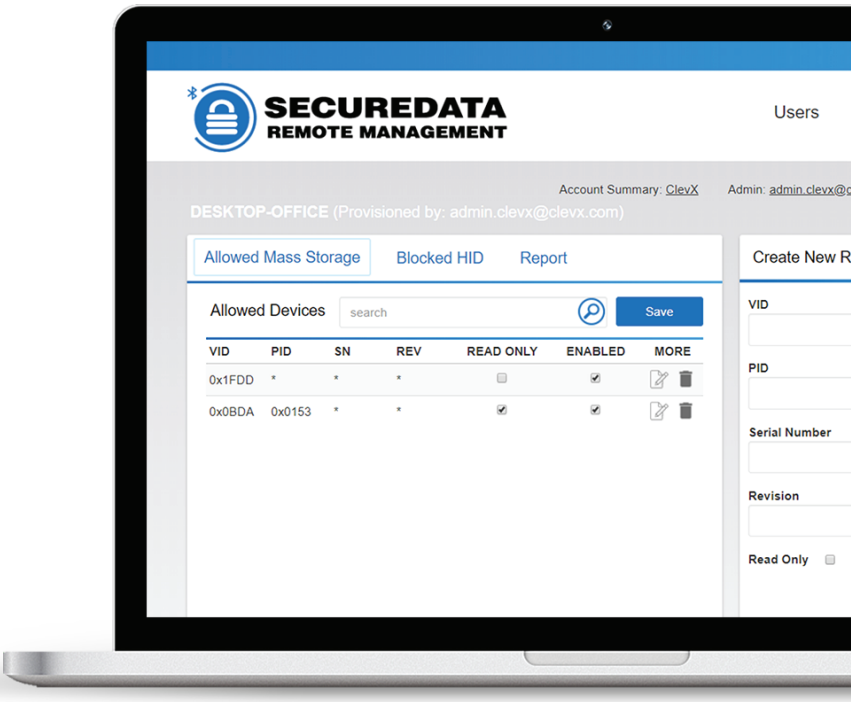
SECURE GUARD

Data Loss Prevention solution managed via
easy-to-use SecureData Remote Management Console

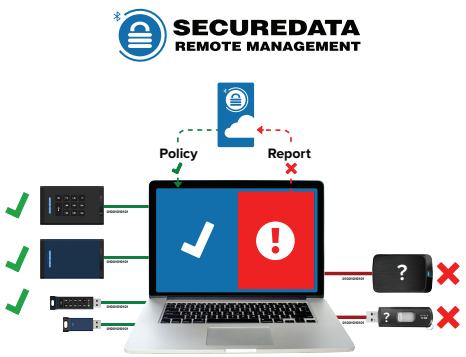
SecureGuard USB

The SecureGuard USB software application is an easy-to-use Data Loss Prevention (DLP) service that is managed via the SecureData Remote Management Console/Services — a subscription-based SaaS. It helps companies avoid painful and costly data leaks by enforcing the use of only authorized USB devices on company-wide computers that have USB ports. It allows Admins/IT Managers to safeguard sensitive information by whitelisting authorized removable storage media and blacklisting prohibited USB pluggable devices to prevent data breaches or virus and malware uploads. Admins/IT Managers have control over device authorization through the cloud-based Remote Management console.



Data Loss Prevention software offers always-on protection with USB-blocking functions:

- Limits computer access throughout the organization to authorized USB devices only
- Allows blacklisting and whitelisting specific USB devices via Remote Management Console
- Blocks access to computer when an unauthorized device is inserted
- Prevents viruses and malware from entering via unauthorized USB devices
- Allows authorized USB storage devices to be set in Read Only mode
- Works with SecureData and other portable, external data storage devices



Devices blocked:

- Portable, external data storage devices (USB, HDD, SSD, etc.)
- HIDs/Human interface devices (mouse, keyboard, headset, etc.)
- Mobile and photo/video devices (phone, tablet, camera, etc.)
- Card readers
- Printers and scanners
- And more

Learn more at **securedrive.com/rm**

Call us at **1-800-875-3230**

SECURE DATA

SECURE GUARD

Data Loss Prevention solution managed via
easy-to-use SecureData Remote Management Console

Main Features

WHITELISTING & BLACKLISTING

The program's default setting is to blacklist all USB mass storage devices inserted into a port. Admin may specify devices by Vendor ID (VID), Product ID (PID), Serial Number (SN) or Revision to whitelist them for use on a computer. Admin may also blacklist USB devices. This prevents data loss, costly data breaches and undesirable public exposure.

RESTRICTED ACCESS

When an unauthorized device is inserted into a USB port, a screen appears notifying the user that an unauthorized device has been detected. No action can be taken on the computer until the device is removed. Admin may also customize whitelisted devices to access files in Read Only mode for breach prevention, and to prevent the spread of viruses and malware via USB devices.

REMOTE MANAGEMENT

Devices can be remotely whitelisted and blacklisted by individual computer through a user-friendly, cloud-based console. Through this service, Admin can add additional administrators, customize options and review a log that provides details of authorized and unauthorized devices being used, including product information of the device, date and time used and action the SecureGuard program took on it.

ALWAYS-ON PROTECTION

Once installed on a computer, the program will not need internet access to function.

Easy setup and use

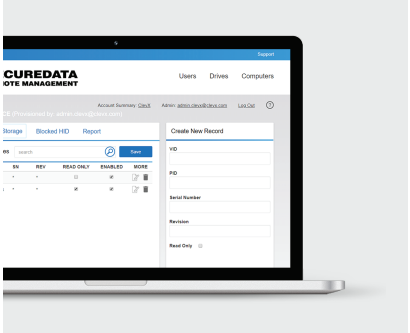
STEP 1

Set up Remote Management account and download software pack from link provided

STEP 2

Install on computers throughout organization

STEP 3



Authorize devices allowed for use

Learn more at **securedrive.com/rm**

Call us at **1-800-875-3230**

SECURE DATA

26.01.2021