securedrive.com | sales@securedrive.com | 1-424-363-8535

Investigators Trust SecureDrive Encrypted Storage

Remote management and user logging keeps chain of custody intact

Police departments have to protect evidence collected during the investigation of a crime scene. Much of that evidence is now gathered in digital form as images, videos, and audio files. The chain of custody for all evidence in a criminal investigation needs to be preserved to prevent tampering that could render it inadmissible in court.

The Need

Detective Amo Virk works as an investigator with the Office of Protective Services Police in Califfornia. He and his fellow officers regularly investigate suspicious deaths, sexual assaults, dependent abuse cases, financial crimes, and other criminal activity. The department needed a better way to handle sensitive digital case files.

Previously, Protective Services investigators transported critical data on inexpensive USB drives with minimal security features. In order for the data gathered to be evidentiary, it needed to be protected while in transit to preserve the chain of custody. Det. Virk contacted SecureData to help him find the right solution.

The Impact

Our data security team helped Det. Virk identify SecureData's SecureUSB BT drives and deploy them throughout his organization. This created a pool of encrypted and remotely managed flash drives for investigators to collect and securely store evidence, from the crime scene to the secure evidence servers.

By adding our Remote Management (RM) Console, Det. Virk is now able to log, manage and audit these drives and document when, where and by whom they were accessed. In the event of a lost or stolen device, he can remotely disable access or wipe the contents of the drive during the next attempt to access it.

The SecureUSB BT drives together with the RM console also enable Det. Virk to protect the chain of custody for evidence shared between prosecutors and defense attorneys. Any drive can be set to read-only mode and assigned to a new user through the RM console. Access to any drive can be restricted to a specific location or time of day with geo-fencing and time-lock features.

Det. Virk can use the RM console to remotely unlock a drive if a user forgets the password, or to change any drive password. If for any reason the chain of custody is ever challenged, he has a time-stamped log of every attempt to access the drives, when the attempt was made, where, and on which machine.

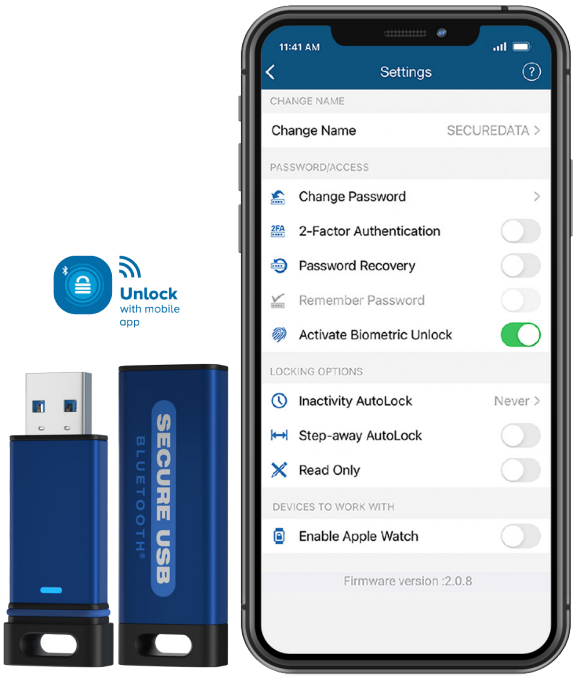
The Solution

Det. Virk wanted a secure solution for safer data handling that was easy to deploy and that could establish a high standard for the protection of digital evidence in criminal investigations. He found exactly what he and his team of investigators needed. "SecureData delivered the perfect solution. Now we can protect and preserve the chain of custody for the data we gather, and we have the user logs to prove it."

Please contact SecureData for an evaluation sample or brief online demo.

SecureUSB® BT

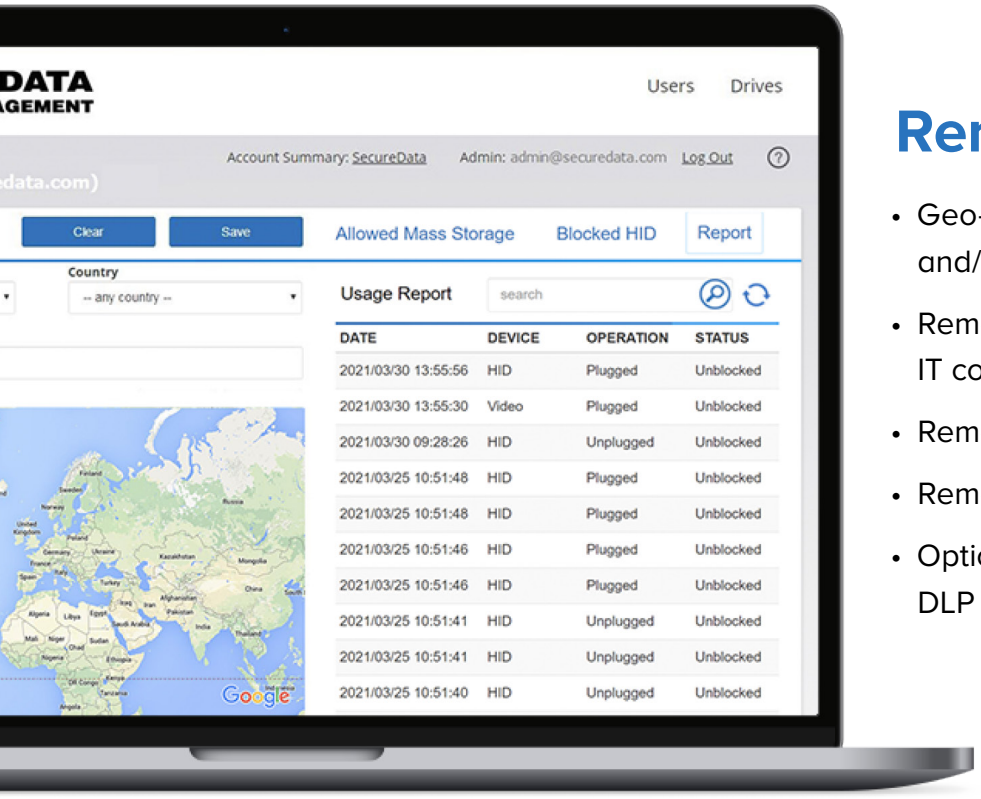
- Unlock with mobile phone and free mobile app
- Remote Management ready to protect customer investment
- Anti-hacking and brute force protection
- Read-only mode, remote wipe, and many more security features
- Free 1st-year subscription to DriveSecurity® (by ClevX®) drive-based antivirus protection



FIPS LEVEL 3 VALIDATED 140-2

CES INNOVATION AWARDS 2019 HONOREE

reddot design award winner 2019



Remote Management

- Geo-lock and Time-fencing to control where and/or when drives can be accessed
- Remote Management Ready to enable IT control, audit and reporting
- Remotely unlock a drive or reset a password
- Remotely wipe a drive if it is lost or stolen
- Optional remote managed SecureGuard DLP software to protect USB ports