Today's challenge

Employees of an organization often utilize portable storage devices to transport vital and sensitive data. Although these auxiliary devices offer convenience, they can also pose threats to information security if exploited or mishandled. As a best practice, the actions and whereabouts of these devices should be closely monitored and managed.

How Device Control Plus fits into your IT framework

Device Control Plus can be leveraged by IT administrators to gain comprehensive control over the numerous peripheral devices within their networks. This robust software solution includes a distinct set of features that enables the creation of flexible file access and transfer control policies. Therefore, by assigning the appropriate level of device permissions, all data transfers conducted via built-in and external devices can be meticulously tracked and regulated.

Highlights

- Auto-detection and management of more than 17 types of peripheral devices and continuous monitoring of network ports.
- Numerous granular settings for file protection policies.
- Meticulous tracing of file locations, users, and endpoints involved in data transfer operations.
- Temporary access provisions to encourage short-term collaboration with third-party users.
- Detailed reports and prompt alerts that enable enhanced visibility over devices and file actions.

Device Control Plus is essential for averting data loss through USB and removable media, and is designed so that both preventative and restorative measures can be implemented effectively. This data leakage prevention tool features capabilities such as blacklisting and blocking data access, which are two of its many methods to deter file-based attacks. In the event of any emergency, out-of-box protocols like file tracing and file shadowing can also be adopted to ensure the diligent preservation of network integrity and retention of brand value.

Features

Device and Port Control

Effectively manage more than 17 types of peripheral devices from a singular console. Automatically discover the active ports within your network, as well as detect which devices are connected to your computers. You are empowered to take proactive actions to prevent malware injections and inadvertent data loss by disabling auto-run on all questionable devices.

File Transfer Control

Regulate the amount and type of data transferred through peripheral devices. By limiting the number of bytes, only information vital to the task at hand is transferred. By restricting the type of file extensions that are allowed to be copied, sensitive files, for example source code, or financial records that include .xml extensions and/or .xls extensions, can be blocked from unauthorized users.

File Access Control

Create and fine-tune file access control policies based on the specific departments and employee functions within your organization. Role-based access control protocol ensures that all users have sufficient access to corporate information pertaining to their roles, while other data irrelevant to their tasks is kept off-limits. Provisions such as granting read-only permissions also minimizes data loss as business-critical information can be restricted to select users.

Device Permissions

Enforce a zero-trust policy in your organization by having all devices blocked by default, with the exception of a few trusted devices that are routinely utilized by core personnel. For heightened security, the option to allow only BitLocker encrypted devices is also available. For each custom group or computer, policies solely for trusted devices can be created. This is advantageous as higher privileges can be assigned just for devices used only by key employees or for special tasks.

File Shadowing

Automatically create mirror copies of the files transferred from a particular device. The copies are then safeguarded in a password protected share. In the event of an emergency, this precautionary measure helps identify the exact contents of transferred files and assists with the development of precise remediation strategies.

Temporary Access

On occasions where greylisted or blocked devices require access to computers for specific tasks, safely assign permissions so that the devices can obtain the necessary information without compromising cyber hygiene. As third-party users or lower-level employees are granted short-term access, ensure that sessions and file actions are closely monitored.