DATALOCKER®
SIMPLY SECURE

DATALOCKER PORTBLOCKER

MAINTAIN CONTROL OF YOUR USB PORTS

PortBlocker is a simply secure approach to Data Loss Prevention (DLP) for removable storage that limits which USB mass storage devices can be utilized on a user's workstation. With PortBlocker, users can only transfer data to approved, secure encrypted devices, which prevents data breaches due to unauthorized usage and access. PortBlocker is integrated with SafeConsole, the leading central management solution for secure encrypted storage. All endpoint activity, such as when and where a device is blocked, is reported back to the SafeConsole audit logs for the Admins to review.

PORTBLOCKER FEATURES

- **Endpoint Port Control** - Approve and whitelist USB storage devices by Vendor ID (VID), Product ID (PID), and serial number through SafeConsole.
- **Computer-Based Policy Enforcement** - Policies are applied based on the workstation location in Active Directory. If required, individual policies can be created down to the workstation level.
- **Quick Disable/Enable** - Administrators can remotely "Allow All" and "Block All" devices through SafeConsole.
- **Activity Audits** - All events, such as when a device is blocked, when an endpoint is registered, and when there are policy edits or changes are all reported to SafeConsole in the Audit Logs.
- **Read Only** - Set USB ports in read only mode to disable write capabilities on USB storage devices. Policy allows read only access to all devices marked as Blocked and also devices that are unlisted.
- **Geofence** - Devices can be automatically blocked when the workstation is being used outside of the geolocation policy that is applied and configured through SafeConsole.

HOW DOES PORTBLOCKER WORK?

Always On Protection. Once installed by an admin, PortBlocker will start automatically and run in the background of the user's machine. It cannot be disabled or uninstalled without admin privileges.

Policy Enforcement. Restrict USB mass storage devices through SafeConsole Whitelist policy (VID,PID, and Serial Number). Policies are updated automatically from SafeConsole.

Real-Time Reporting. Central management of PortBlocker through SafeConsole makes it easy to audit who, what, when, and where a threat occurred.

MINIMUM REQUIREMENTS

- Active SafeConsole account (v5.4.0+)
- Windows™ 7 or 10 (macOS support coming Q4 2019)
- 512MB of RAM
- 1GB of available hard-disk space
- Connection to SafeConsole server for registration and policy updates
- Intel Quad Core Atom processor, or equivalent x86 - x64 processor
- Uses the WinINET (Internet Explorer) system user's proxy settings. Manual proxy settings or a pac script are supported.

A SafeConsole Account is required in order to utilize and deploy PortBlocker. For new SafeConsole Accounts, a one-time base fee is also required. A valid PortBlocker license is then required for each workstation/system where PortBlocker is deployed (licenses available for 1 or 3 years).

datalocker.com
sales@datalocker.com
+1 855 897 8755 or +1 913 310 9088