DATALOCKER®
SIMPLY SECURE

SAFECONSOLE PORTBLOCKER

PortBlocker

Centralized USB Port Security and Endpoint Device Control

MANAGED BY SAFECONSOLE®

SafeConsole PortBlocker delivers robust, automated protection against unauthorized USB access across your organization. Through seamless integration with the SafeConsole management platform, real-time monitoring, and centralized policy control, PortBlocker ensures that only approved USB devices can connect to protected workstations—significantly strengthening data security, reducing malware risk, and preventing data loss.
PortBlocker operates continuously in the background, enforcing security without disrupting user workflows, while giving administrators full visibility and control over USB access across the network.

Easy and Automatic Device Blocking

PortBlocker automatically blocks unapproved USB devices the moment they are inserted into a USB port. Administrators are notified immediately, and every event is logged in the SafeConsole audit logs. With a few clicks, approved devices can be whitelisted or permanently.

Seamless Integration with SafeConsole

PortBlocker is fully integrated with the SafeConsole management platform, enabling centralized USB port control while supporting existing SafeConsole policies. Once installed, it runs silently in the background to provide continuous protection without interrupting productivity.

Active Monitoring and Reporting

USB ports are actively monitored in real time. All activity is logged in SafeConsole device audit logs, providing administrators with visibility into endpoint status and enabling informed, rapid security decisions.

Always-On Protection

Once deployed, PortBlocker runs automatically in the background and cannot be disabled by non-privileged users. Updates are securely distributed by administrators according to organizational policies and procedures, ensuring consistent protection across endpoints.

Policy Enforcement

SafeConsole enforces whitelist policies based on VID, PID, and serial numbers, with real-time policy updates that ensure only approved USB devices can connect to protected systems.

Real-Time Endpoint Auditing

USB-related activity is logged and reported to SafeConsole, providing detailed endpoint audit reports within the central management platform for rapid investigation and response.

MINIMUM REQUIREMENTS

Windows™ 7, 10 and 11, macOS (64-bit)

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 system user's proxy settings. Manual proxy settings or a pac script are supported.

LICENSING

A valid SafeConsole account is required to deploy PortBlocker. A PortBlocker license is required per workstation, available in 1-year or 3-year license terms.

DATALOCKER®
SIMPLY SECURE

Get a Custom Demo

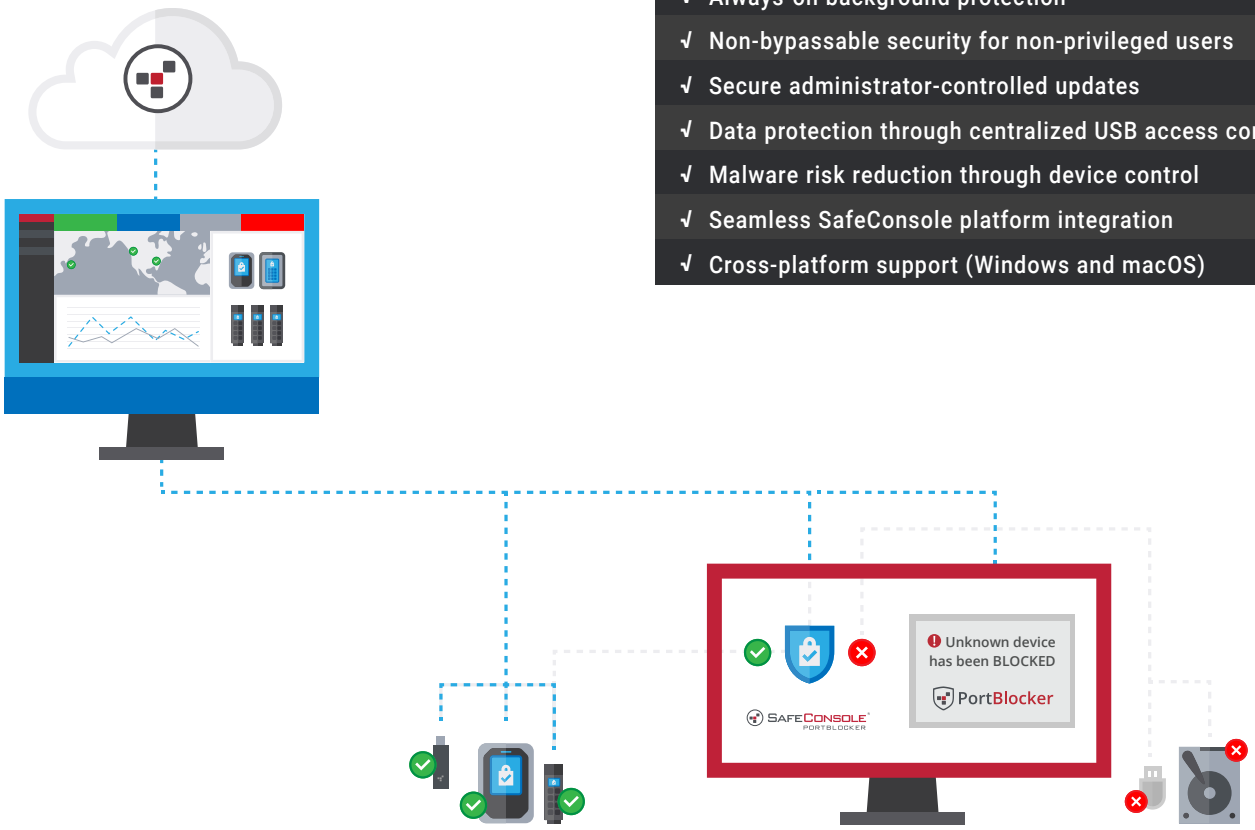
datalocker.com | sales@datalocker.com

Deployment and Platform Support

- Cross-platform compatibility: Windows and macOS
- Centralized management through SafeConsole
- Secure administrative update distribution
- Scalable enterprise deployment model

PORTBLOCKER FEATURES

- √ Automatic blocking of unapproved USB devices
- √ Centralized USB policy management via SafeConsole
- √ Device whitelisting
- √ VID, PID, and serial-number based device identification
- √ Real-time USB activity monitoring
- √ Real-time alerting
- √ USB-related audit logging
- √ Centralized reporting and visibility
- √ Always-on background protection
- √ Non-bypassable security for non-privileged users
- √ Secure administrator-controlled updates
- √ Data protection through centralized USB access control
- √ Malware risk reduction through device control
- √ Seamless SafeConsole platform integration
- √ Cross-platform support (Windows and macOS)



Also Available:

SafeConsole USB Device Management

Secure USB Device Management
Manage and monitor your encrypted USB drives with centralized auditing and security controls.

SafeConsole USB Data Erasure

USB Certified Data Erasure
Certified, cryptographic erasure with automated proof-of-erasure, tamper-proof certificates, and NIST SP 800-88 compliance reporting.

SafeConsole Anti-Malware

Anti-Malware for Secure USB Devices
Protect your USB drives with onboard anti-malware that scans and reports malware threats directly to SafeConsole.

DataLocker Simply Secure

Get a Custom Demo

datalocker.com | sales@datalocker.com