

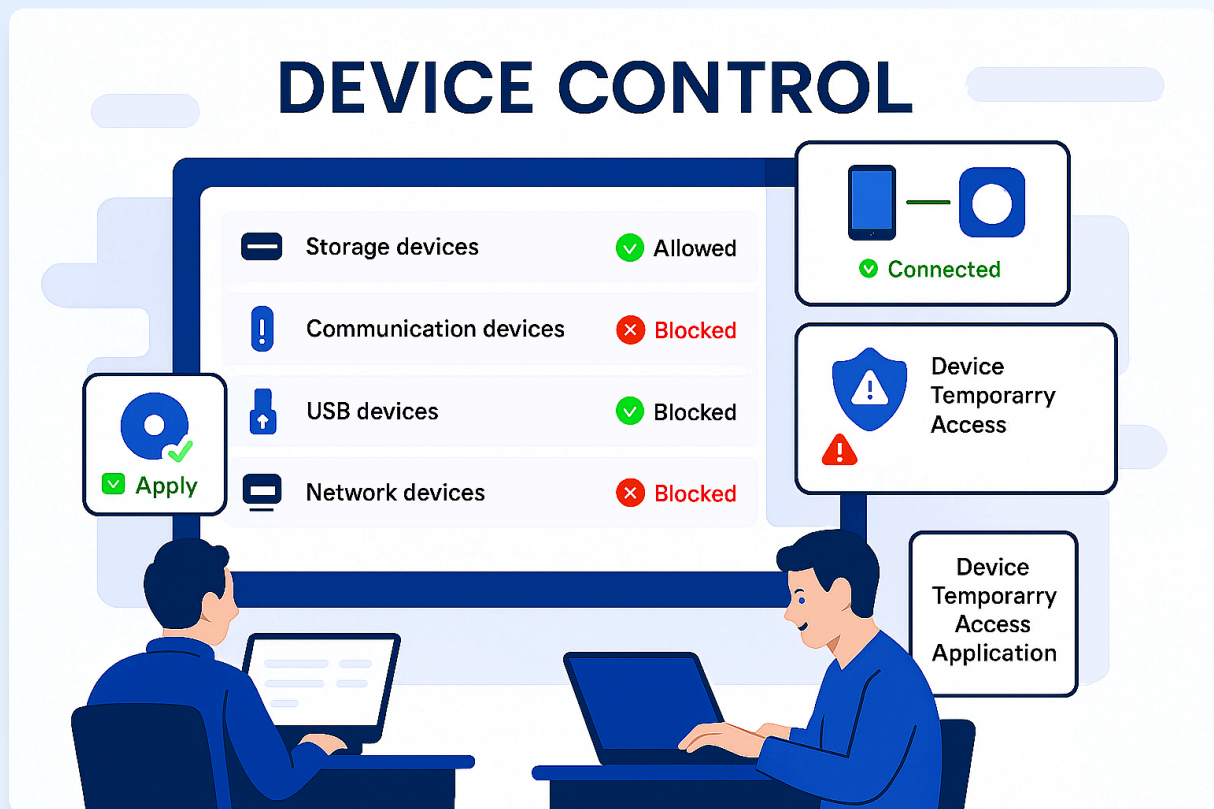


AnySecura

Device Control

Comprehensive peripheral security management solution

Monitor · Restrict · Secure · Audit · Manage





Module Overview

AnySecura Device Control integrates five core capabilities, providing enterprises with complete control over peripheral devices to prevent unauthorized access and data leakage through external devices.



Device Control

Control usage permissions for various device types including storage devices, communication devices, USB devices, network devices, and other peripherals.



Mobile Intelligent Terminal

Control mobile device access via portable devices, USB storage, and mobile assistants, with file transmission monitoring capabilities.



ADB Control

Prevent external devices from accessing computers in ADB mode to protect against unauthorized debugging and data extraction.



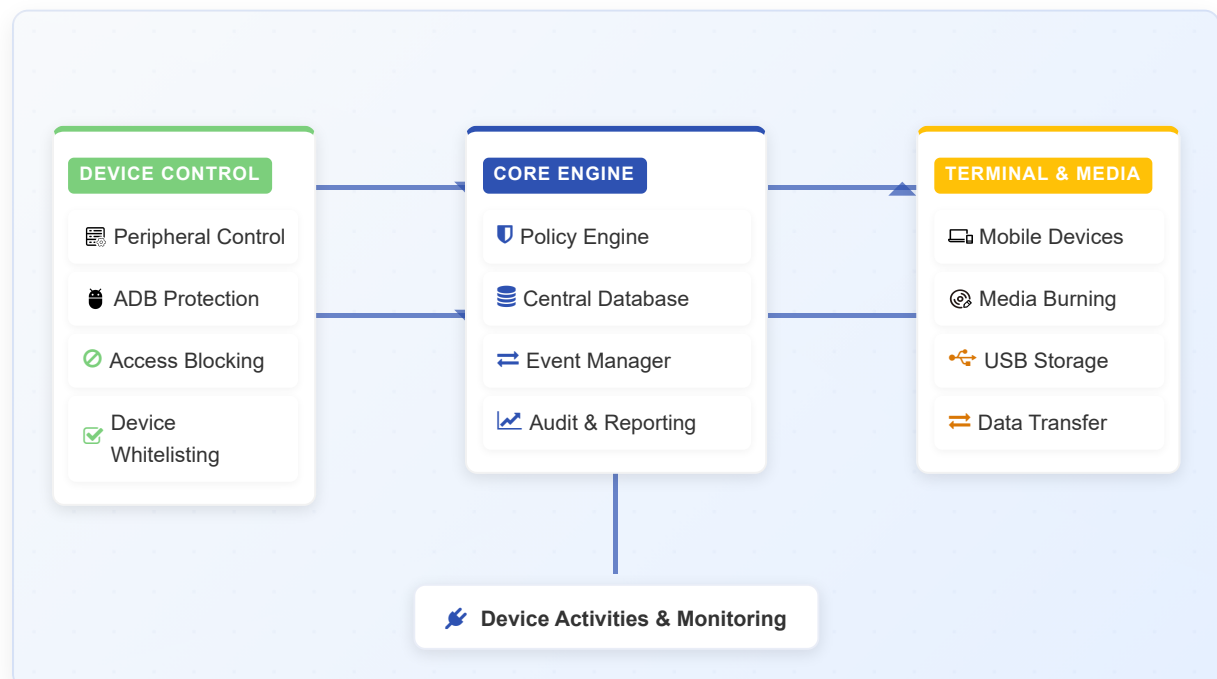
Burning Control

Restrict burning activities to approved tools only, with temporary permission options through approval workflows or self-filing.

Device Usage Application



Allow users to temporarily lift device restrictions through application processes, or use specific devices after self-filing and registration on the client. This flexible mechanism balances security needs with operational efficiency, ensuring proper oversight while minimizing workflow disruptions.

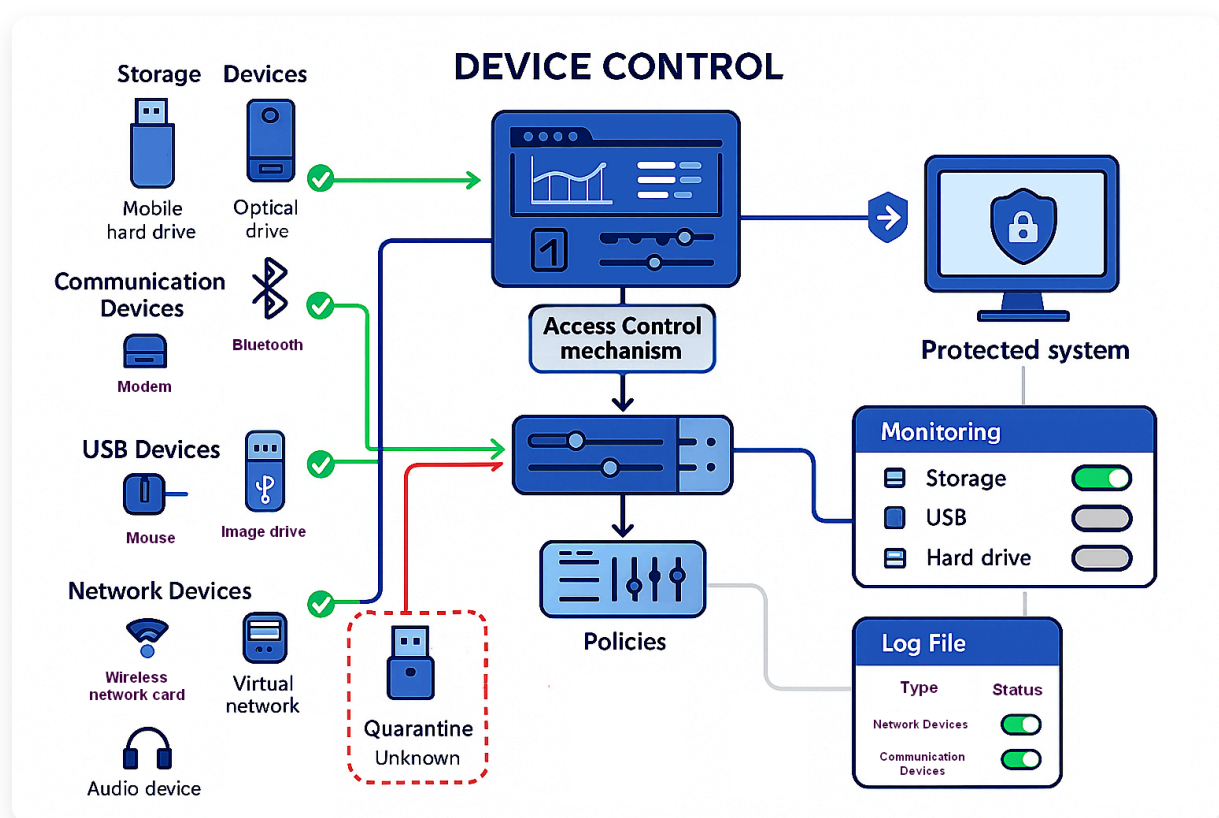




Device Control

Granular control over various peripheral devices to prevent unauthorized access and protect sensitive data from leakage through external devices.

- ➡ **Storage Devices:** Control access to USB flash drives, mobile hard drives, floppy drives, optical drives, tape drives, and other storage devices.
- ➡ **Communication Devices:** Manage permissions for serial/parallel ports, SCSI, 1394, Bluetooth, infrared, MODEM, and direct connection cables.
- ⌨ **USB Devices:** Control USB keyboards, mice, MODEM, imaging devices, storage devices, optical drives, and hard drives.
- 📶 **Network Devices:** Manage wireless network cards, plug-and-play network cards, and virtual network cards to prevent unauthorized network access.
- 🔊 **Other Devices:** Control audio devices, virtual optical drives, and other peripheral devices based on security policies.
- 🚫 **Unknown Device Blocking:** Prohibit access to any newly added devices that haven't been authorized or classified.





Mobile Intelligent Terminal

Comprehensive control over mobile device access and data transmission to prevent sensitive information leakage through smartphones and portable devices.



Access Control: Manage mobile device access through portable devices, USB storage, and mobile phone assistants.



Transmission Monitoring: Control file external transmission through mobile devices with complete tracking capabilities.



File Backup: Automatically back up files transmitted via mobile devices for audit and compliance purposes.



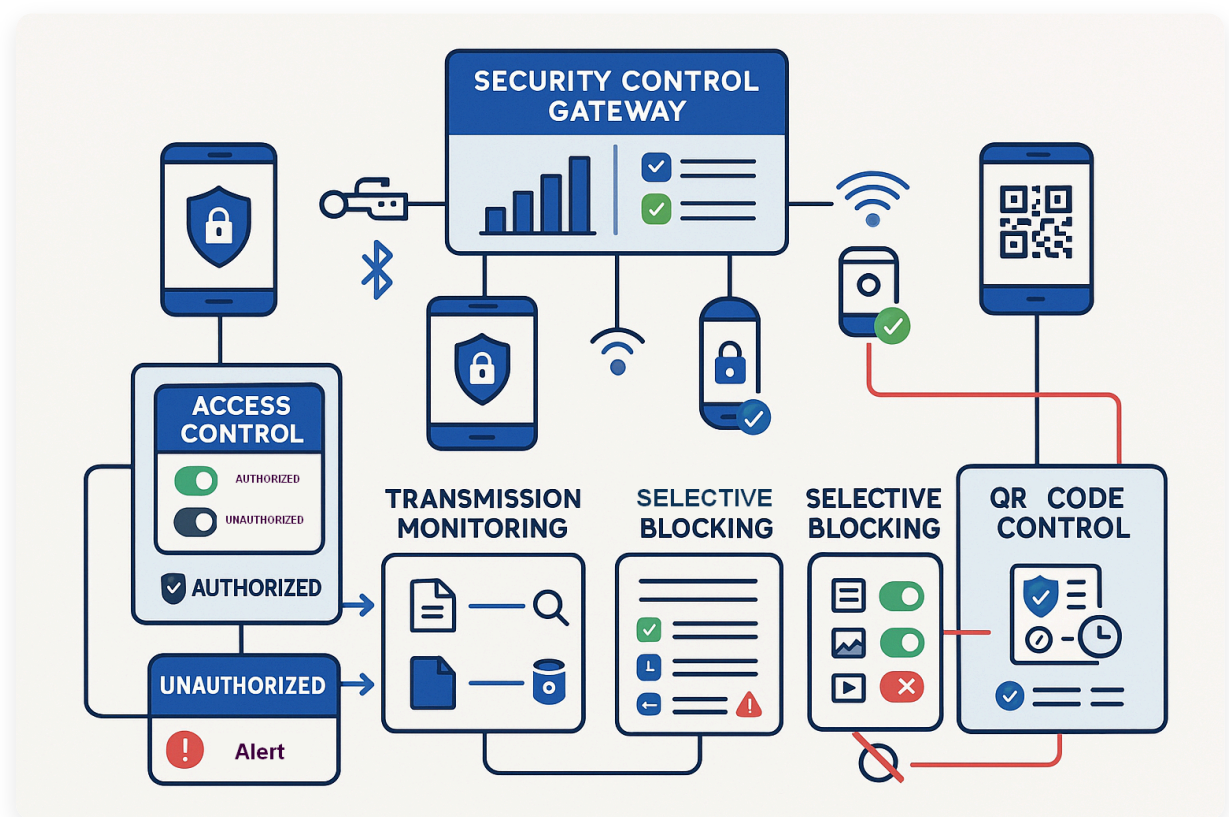
Activity Recording: Maintain detailed logs of all mobile device interactions, including file transfers and connection attempts.



Selective Blocking: Prohibit smartphone access entirely or restrict specific types of data transfers based on policies.



QR Code Control: Manage data transfer via QR codes with scanning restrictions and logging capabilities.

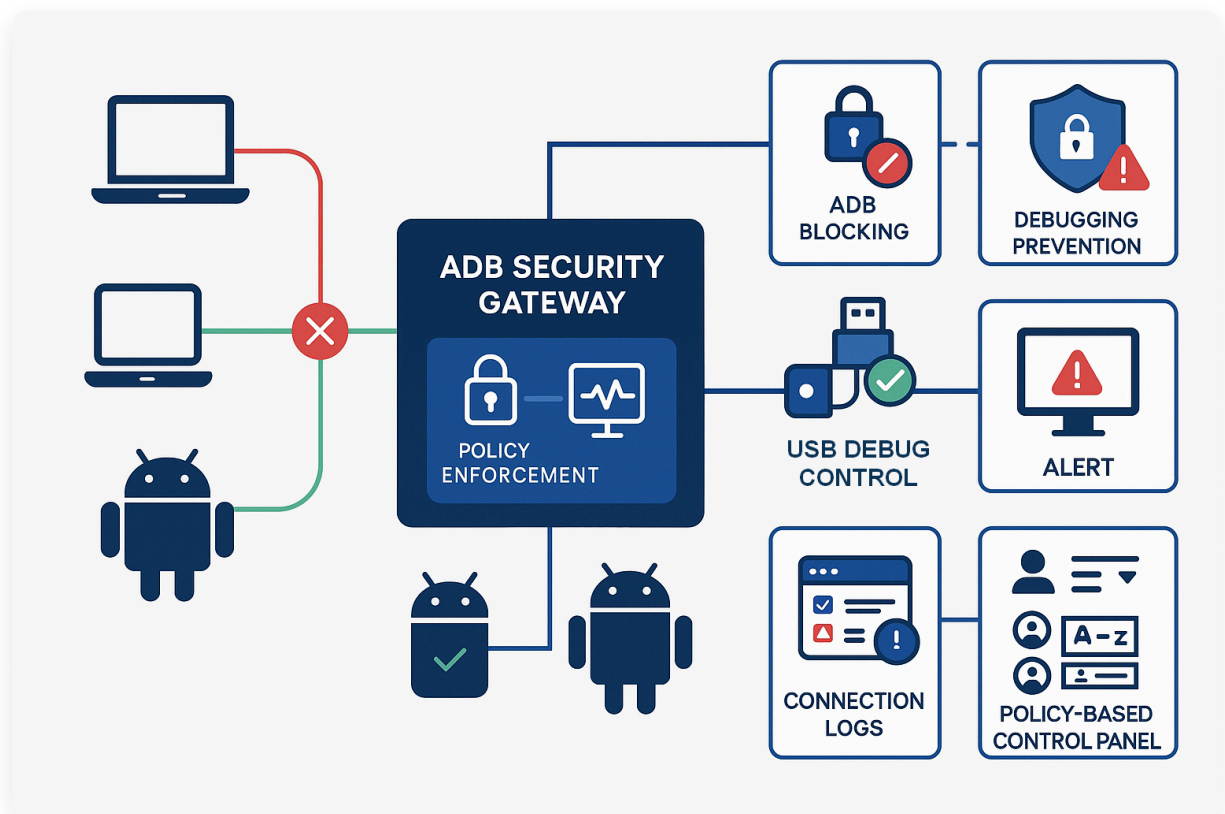




ADB Control

Advanced protection against unauthorized debugging and data extraction through Android Debug Bridge access control mechanisms.







- 🚫 **ADB Blocking:** Prevent external devices from accessing computers in ADB (Android Debug Bridge) mode.
- 🔧 **Debugging Prevention:** Block unauthorized debugging activities that could expose sensitive data.
- 🔌 **USB Debug Control:** Manage and monitor USB debugging permissions for mobile devices.
- 🔔 **Real-time Alerts:** Receive notifications of attempted ADB connections for security monitoring.
- 📖 **Connection Logging:** Maintain detailed records of all ADB connection attempts and activities.
- ⚙️ **Policy-based Controls:** Apply different ADB access policies based on user roles, device types, and organizational units.

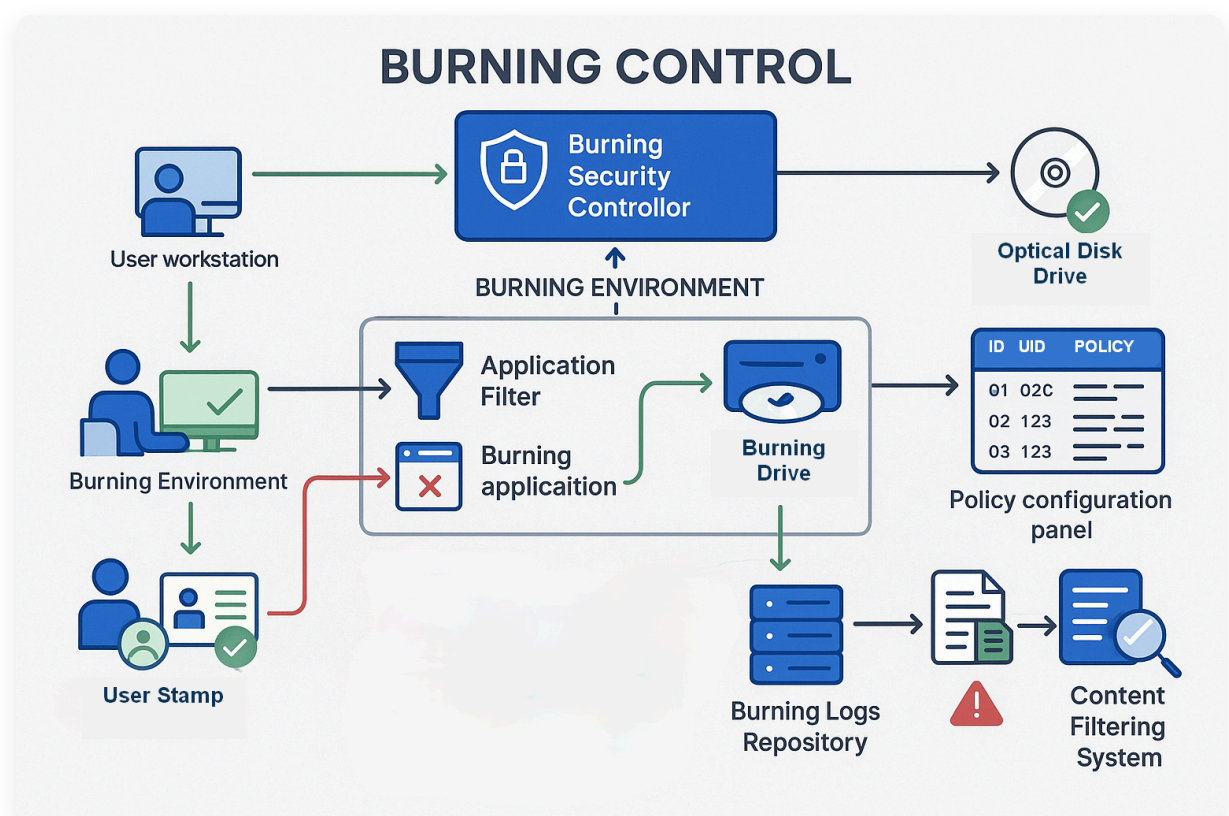




Burning Control

Comprehensive management of optical disc burning activities to prevent unauthorized data duplication and distribution.

-  **Tool Restriction:** Prohibit users from using unauthorized burning tools, allowing only approved software.
-  **Temporary Permissions:** Allow temporary burning rights through application and approval workflows.
-  **Self-filing Option:** Enable burning functionality through self-filing processes for traceability.
-  **Burning Logs:** Record details of all burning activities including user, time, and content information.
-  **Policy Configuration:** Set granular policies for different user groups and burning scenarios.
-  **Content Filtering:** Apply content inspection rules to prevent sensitive information from being burned to discs.

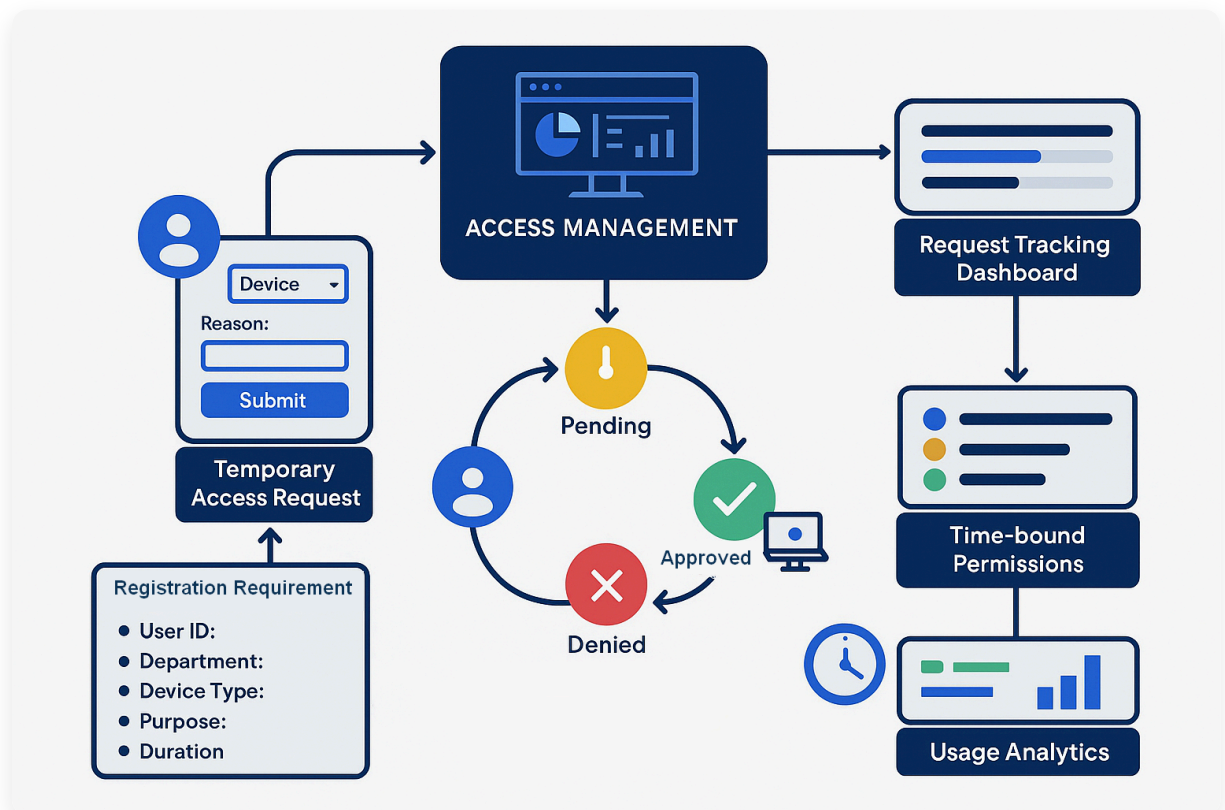




Device Usage Application

Flexible mechanisms for requesting temporary device access while maintaining security controls and comprehensive audit trails.

- ✔ **Temporary Access Requests:** Allow users to apply for temporary lifting of restrictions on specified devices.
- 🕒 **Time-bound Permissions:** Grant device access for specific time periods with automatic expiration.
- 📄 **Self-filing Mechanism:** Enable device usage after user registration and self-filing on the client.
- ➡ **Registration Requirements:** Collect necessary information during self-filing for accountability.
- 👥 **Approval Workflows:** Configurable multi-level approval processes based on device type and user role.
- 🔍 **Request Tracking:** Monitor status of all device access requests with complete audit trails.
- 📊 **Usage Analytics:** Track temporary device access patterns to optimize security policies.



Application Scenarios

1. USB Device Control

The Challenge

A financial institution faces significant data leakage risks due to uncontrolled USB device usage. Employees frequently use unauthorized USB drives to copy sensitive financial data, creating potential security breaches.

The Solution with AnySecura

Implementing comprehensive **Device Control** capabilities:

1. Block all unauthorized USB storage devices by default
2. Create whitelists for approved USB devices with unique identifiers
3. Log all USB connection attempts and file transfer activities
4. Allow temporary USB access through formal application processes

Results Achieved

- ✓ Eliminated unauthorized data copying via USB devices
- ✓ 100% visibility of all USB-related activities
- ✓ 95% reduction in data leakage incidents from removable media

2. Mobile Device Security

The Challenge

A healthcare organization struggles with protecting patient data from leakage through smartphones. Medical staff frequently connect mobile devices to workstations, creating potential HIPAA compliance violations.

The Solution with AnySecura

Leveraging **Mobile Intelligent Terminal** and **ADB Control** capabilities:

1. Implement strict controls on smartphone connections to workstations
2. Block ADB mode access to prevent unauthorized data extraction
3. Log all mobile device file transfers with content backups
4. Allow approved mobile device usage through formal application processes

Results Achieved

- ✓ 100% HIPAA compliance for mobile device usage
- ✓ Complete visibility of all mobile device interactions with protected health information
- ✓ Significant reduction in unauthorized mobile data transfers



Core Values & Benefits



Enhanced Data Security

Prevent unauthorized data leakage through peripheral devices with granular control over all external connections and transfers.



Complete Visibility

Full visibility into all device activities with comprehensive logging and monitoring of peripheral usage across the enterprise.



Regulatory Compliance

Meet industry compliance requirements with controlled device access, complete audit trails, and data transfer monitoring.



Flexible Control

Balance security with productivity through temporary access mechanisms, approval workflows, and self-filing options.

Ready to Secure Your Peripheral Devices?

 [Learn More About Solutions](#)

 [Contact Our Experts](#)



www.anysecura.com



support@anysecura.com

© 2025 AnySecura SOFTWARE PTE. LTD. All rights reserved. Enterprise-grade security solutions.