SOLUTION BRIEF

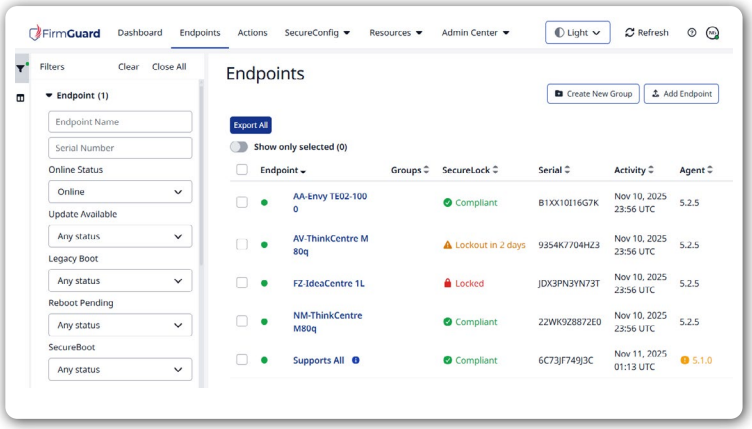
FirmGuard® SecureLock™

FREEZE ENDPOINTS UNTIL UNLOCKED

What is SecureLock?

In highly secure environments, organizations must ensure endpoints regularly communicate with management servers to remain compliant and secure. However, some endpoints operate in restricted networks or go offline for extended periods, creating blind spots that attackers could exploit.

SecureLock™ helps ensure endpoints remain up to date and compliant by requiring periodic check-ins with FirmGuard servers. If a device fails to connect within the defined period, the system will lock at the BIOS level, preventing the OS from loading until a valid unlock code is entered. This helps prevent potentially unsafe connections from devices that haven't checked in for regular updates and may be missing the latest security and compliance patches.



How SecureLock Works:

1. **Check-in:** Endpoints must connect to FirmGuard servers within a set interval (e.g., every 14 days).
2. **Warning Notifications:** Users are warned with dismissible reminders as lock time approaches.
3. **Lock Enforcement:** SecureLock prevents boot when an endpoint fails to check in. For maximum protection, SecureLock works best when paired with:
   a. Secure Boot – Prevents unauthorized software from loading.
   b. BitLocker – Keeps your data encrypted and safe.
   c. BIOS/UEFI Password – Locks down firmware settings from tampering.

Together, these safeguards create a powerful defense against unauthorized access and security breaches—right from power-on.

4. **Unlock Process:**
   a. The user calls their MSP when locked.
   b. The MSP retrieves an unlock code from the FirmGuard portal.
   c. The user enters the unlock code, restoring access.
5. **Offline-Ready:** SecureLock operates without requiring live network connectivity during both lock and unlock — codes are validated locally and timers reset. Once unlocked, the user must connect to a network within 30 minutes, or the machine will lock again.

Benefits of SecureLock

SecureLock delivers a reliable, offline-capable enforcement mechanism to ensure compliance and protect sensitive endpoints:

- **Guaranteed Compliance:** Forces endpoints to check in with FirmGuard servers within defined intervals.

FirmGuard

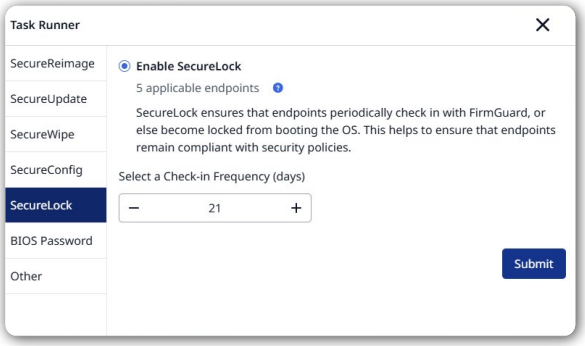
SecureLock

- **Boot-Level Protection:** Lock occurs before the OS loads, making bypass attempts significantly harder.
- **Offline Unlock:** MSPs can provide unlock codes even without internet connectivity.
- **Security Hardening:** Protects networks from connections by potentially unsafe endpoints, and endpoints from continuously running in an insecure or non-compliant state; employing additional safeguards such as BitLocker, Secure Boot, BIOS password, and disabled USB boot minimize bypass risks.
- **User Awareness:** Clear, escalating warnings notify users well in advance of lockouts.
- **MSP Visibility:** Admins can view lock status, unlock codes, and next lock times directly in the FirmGuard portal.

Use Cases

SecureLock addresses common security and compliance challenges for MSPs and organizations:

- **Air-Gapped Environments:** Ensure endpoints that rarely connect to the internet are forced to connect at regular intervals to receive security and compliance updates.
- **High-Security Deployments:** Enforce strict boot controls in industries like defense, finance, and healthcare.
- **Remote Workforce Management:** Prevent unmanaged devices from running indefinitely without check-in.



- **Theft & Tamper Resistance:** Protect devices at a boot level to reduce risk of data exfiltration or bypass.

Why SecureLock is the Best Choice for Endpoint Boot Protection

SecureLock ensures that endpoints remain both connected and compliant by enforcing mandatory check-ins and locking at BIOS level if requirements aren't met. Unlike traditional endpoint controls that depend on continuous connectivity, SecureLock works entirely offline for both locking and unlocking, ensuring resilience in restricted networks.

In combination with boot-level enforcement, strong encryption (BitLocker), firmware protection (Secure Boot), and MSP-controlled unlock codes, SecureLock creates a hardened safeguard that attackers cannot easily bypass.

With clear user warnings, MSP visibility, and simple unlock workflows, SecureLock balances strong protection with practical usability. This makes it the ideal solution for high-security, compliance-driven environments.

Book your FirmGuard demo today.

firmguard.com/demo

FirmGuard