

FirmGuard® SecureEndurance™

KEEP FIRMGUARD PROTECTED ON EVERY ENDPOINT



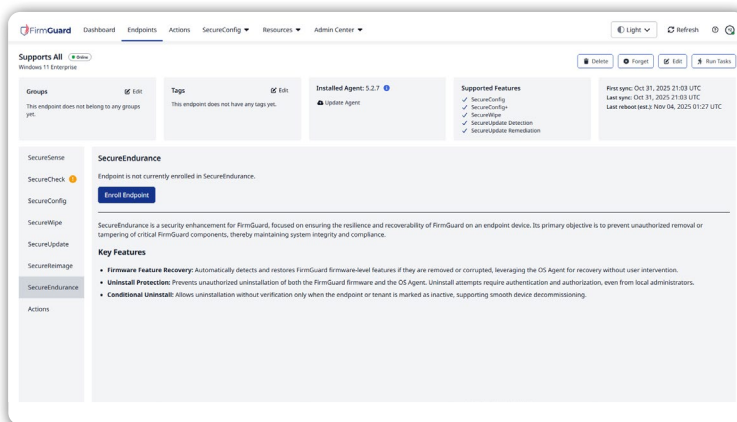
What is SecureEndurance?

Even the strongest security stack is only effective when it stays active. Accidental removals, misinformed troubleshooting, or unauthorized uninstalls can all leave endpoints unprotected, and organizations blind to critical threats.

SecureEndurance™ ensures your FirmGuard protection stays in place at all times.

It prevents accidental or non-admin removal of key FirmGuard components such as the FirmGuard Agent and Launcher, ensuring continuous visibility, compliance, and BIOS-level defense across every endpoint.

By requiring a secure uninstall token, SecureEndurance ensures that only authorized administrators can remove FirmGuard — keeping protection consistent, reliable, and tamper-resistant.



How SecureEndurance Works:

1. **Activation:** Once SecureEndurance is enabled, each tenant receives a unique uninstall token securely stored in the FirmGuard Portal.
2. **Protection Enforcement:** Devices enrolled in SecureEndurance will not allow the FirmGuard Agent or Launcher to be removed without that token. Any uninstall attempt without it is blocked, with a clear on-screen message explaining that administrative authorization is required.
3. **Administrative Control:**
 - a. Authorized admins can view, regenerate, or revoke uninstall tokens via the FirmGuard Portal.
 - b. Non-enrolled devices behave normally — no workflow changes or restrictions.
4. **Future Expansion:** Upcoming versions will extend SecureEndurance protection deeper into firmware and logging layers, introducing stronger tamper resistance and persistence mechanisms at the BIOS and pre-OS levels.

Benefits of SecureEndurance

SecureEndurance delivers uninterrupted endpoint protection and operational control for managed environments:

- **Continuous Protection:** Prevents accidental or unauthorized uninstallations that could disable key security functions.

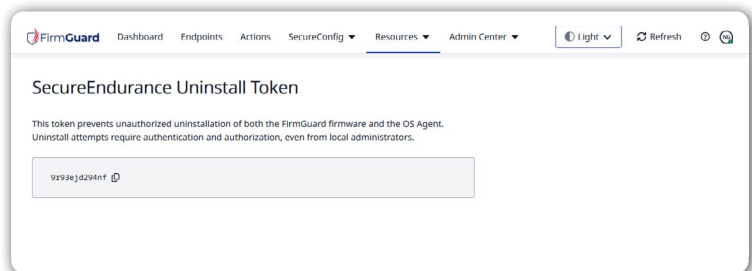
SecureEndurance

- **Administrative Authority:** Ensures only authorized personnel can remove or modify FirmGuard software.
- **Consistent Visibility:** Maintains full monitoring coverage across all endpoints for compliance and incident response.
- **Reduced Downtime:** Eliminates gaps in protection caused by human error or misconfiguration.
- **Tamper Resistance:** Lays the foundation for BIOS-level persistence and future-proofed firmware protection.

Use Cases

SecureEndurance strengthens endpoint resilience for organizations where BIOS security is non-negotiable:

- **Managed IT & MSP Environments:** Prevent clients or users from removing agents critical to monitoring and response.
- **Regulated Industries:** Maintain compliance visibility and uninterrupted security coverage for financial, defense, and healthcare systems.
- **High-Availability Systems:** Ensure security tools remain operational in mission-critical infrastructures.
- **Incident Response Readiness:** Keep FirmGuard agents active to support pre-OS recovery and remediation workflows.



Why SecureEndurance is the Best Choice for Continuous Endpoint Protection

SecureEndurance ensures that FirmGuard's BIOS-level protection stays active - always. By requiring a secure uninstall token for removal, it gives administrators complete control while preventing accidental security lapses caused by human error or unauthorized changes.

Unlike traditional software-based uninstall protections, SecureEndurance operates at a deeper level of system integration - maintaining persistence and integrity from firmware up. Combined with future enhancements for tamper resistance and pre-OS durability, SecureEndurance strengthens every layer of your endpoint defense.

Book your FirmGuard demo today.

firmguard.com/demo

