SOLUTION BRIEF

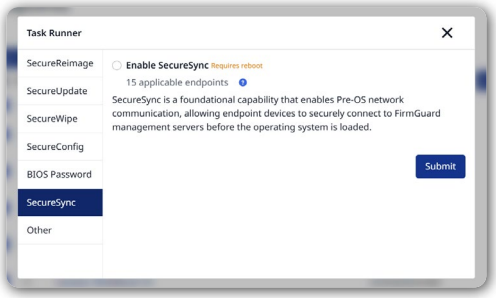
FirmGuard® SecureSync™

STAY CONNECTED WITH PRE-OS/NO-OS CONTROL VIA LAN OR WI-FI

What is SecureSync?

Modern incident response relies on continuous endpoint connectivity, yet OS failures, network outages, or attacks can leave devices unreachable. SecureSync™ ensures FirmGuard-managed endpoints remain connected and controllable, even before the OS loads.

It establishes a secure, firmware-level channel via wired or wireless NICs, allowing devices to "phone home" or receive commands at the BIOS/UEFI stage. Communications are cryptographically authenticated to ensure that only authorized administrators can interact with the device.



SecureSync provides tamper-resistant, firmware-level out-of-band control, keeping endpoints reachable and supporting rapid, remote incident response.

How SecureSync Works:

1. **Activation:** When SecureSync is enabled, each enrolled endpoint establishes a secure communication channel with the FirmGuard cloud using credentials unique to that endpoint.
2. **Connection Establishment:** At every boot, the endpoint establishes an encrypted connection to the FirmGuard cloud over LAN or Wi-Fi. This functions as an independent pre-OS channel. Status updates, logs, and commands are transmitted securely, and unauthorized connection attempts are automatically blocked.
3. **Administrative Control:** Authorized admins can send pre-OS commands (diagnostics, device lock, SecureWipe, OS reimage) and gather endpoint status.

Benefits of SecureSync

SecureSync delivers resilient, firmware-level connectivity and response readiness for FirmGuard managed endpoint:

- **Pre-OS/No-OS Connectivity:** Provides a firmware-level out-of-band communication channel for endpoints, ensuring devices remain reachable even if their primary OS is unbootable.
- **Rapid Incident Response:** Accelerates remediation by allowing immediate actions (lock, wipe, or reimage) on compromised endpoints without waiting for the OS to boot. Administrators can regain control quickly during an emergency without booting to a compromised OS.
- **Secure Management:** Uses strong encryption technologies to ensure only authorized users can issue pre-boot commands. Unauthorized commands are blocked.

FirmGuard

SecureSync

- **Broad Compatibility:** Works over both ethernet and Wi-Fi connections, letting you reach devices in diverse environments (offices, branch sites, or remote locations) with no dependency on an OS.

Use Cases

SecureSync enhances endpoint resilience and incident readiness across many scenarios:

- **Incident Response & Forensics:** Lets IR teams remotely manage devices that have crashed, been locked by malware, or otherwise compromised. Through pre-OS connectivity, diagnostic tools can be used to collect evidence and execute recovery.
- **Managed IT & MSP Environments:** Enable service providers to deliver firmware-level pre-OS out-of-band management. Even if a client's OS is unbootable, MSP technicians can diagnose issues, push fixes, or recover data by communicating at the firmware level.
- **Critical Infrastructure:** Ensure servers, industrial PCs, and other mission-critical systems stay under control during pre-boot and no OS scenarios. With SecureSync, you can quickly reboot, reconfigure, or lock down equipment before an incident escalates.
- **Regulated & High-Security Environments:** Helps government, finance, and healthcare organizations meet compliance requirements by providing remote access to systems regardless of OS health or malware attacks. Pre-OS connectivity provides insight into system issues and a method for recovery with auditable pre-boot actions.
- **Remote & Branch Offices:** Enhances FirmGuard's capabilities for maintaining secure remote management of endpoints, including those deployed outside the core network in diverse and remote areas. With SecureSync, technicians can interact and remediate issues remotely even when the OS is unbootable or untrusted. Pre-OS connectivity provides firmware-level access, reducing the need for technicians to go onsite in order to manage and mitigate issues.

Why SecureSync is the Best Choice for Endpoint Connectivity

SecureSync ensures that FirmGuard can reach your endpoints – regardless of what happens at the OS level. By building communication into the firmware, it gives your administrators visibility and control of each device during the boot process. Unlike traditional, OS-dependent management tools, SecureSync provides connectivity even when the OS fails. Paired with SecureEndurance and other FirmGuard features, it closes the gaps in your defense by ensuring that endpoints remain in contact with your security team. In short, SecureSync turns previously inaccessible endpoints into manageable assets – strengthening your incident response capability.