WHITE PAPER

FirmGuard®

REMOTELY SECURE, CONFIGURE AND UPDATE BIOS FIRMWARE

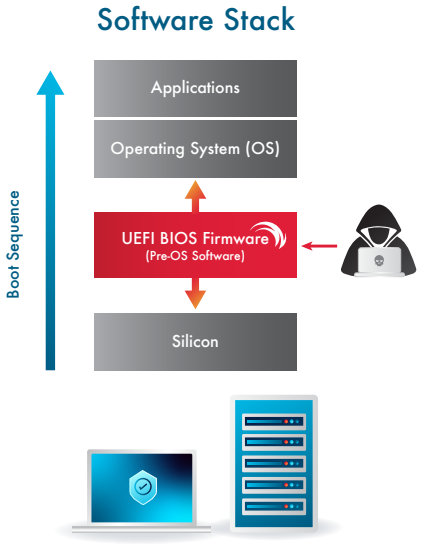
What Is FirmGuard?

FirmGuard is a comprehensive solution for remotely securing, configuring, updating and generally managing BIOS firmware. It goes beyond traditional antivirus and endpoint detection and response (EDR) by safeguarding the UEFI (Unified Extensible Firmware Interface) BIOS firmware of an endpoint, a critical yet often overlooked component of a device's security posture.

FirmGuard ensures BIOS firmware integrity by continually monitoring changes to the BIOS and alerting an administrator whenever some potentially malicious activity occurs (SecureCheck). Additionally, FirmGuard enables remote BIOS configuration (SecureConfig) so administrators can easily optimize BIOS settings, by for example, enabling critical features such as Secure Boot to strengthen defenses against unauthorized access and malware. Further, FirmGuard tracks an endpoint's firmware version (SecureUpdate) and facilitates smooth and consistent UEFI firmware updates. FirmGuard can also be used to forensically wipe (SecureWipe) an endpoint drive(s), complete with a Certificate of Erasure (CoE), to meet compliance requirement. For endpoints still operating in legacy boot mode, FirmGuard identifies these systems so that administrators can recommend removal or update to the more secure UEFI mode (SecureSense).

Importance of BIOS Firmware

Companies have spent billions of dollars protecting endpoints from OS and application-level attacks using EDR/XDR tools. But most have spent almost nothing to protect the BIOS firmware in those same endpoints. This leaves a huge security gap because BIOS is the first software to come up when the power button is pressed, and it is the BIOS which launches the operating system. If BIOS is compromised, that can lead to a hacker taking over complete control of the device, making it critical to have firmware security measures in place.



As CISA notes, hackers are getting better every day at compromising UEFI BIOS firmware and the longer you wait to protect your endpoints, the more likely you are to experience a devastating exploit.

"Adversaries have demonstrated that they already know how to exploit UEFI components for persistence, and they will only get better with practice"

- CISA (DHS)

phoenix technologies

Benefits of FirmGuard

- **Security** – Closing the UEFI BIOS firmware security gap for all endpoints is critical. If you are securing the operating system and applications, but not the firmware, you are only doing two-thirds of the job.
- **Compliance** – FirmGuard helps ensure compliance with industry standards and guidelines such as those set by NIST, ISO and other regulatory bodies.
- **Operational Efficiency** – With FirmGuard an IT admin can remotely configure BIOS settings; update firmware; securely erase an endpoint's hard drive(s); or get detailed information about an endpoint such as BitLocker status, all without ever leaving his or her seat. This reduces the need for onsite visits, shipping endpoints back and forth or writing scripts to obtain data.
- **Increase MRR** - MSPs regularly charge customers for EDR/XDR tools that protect client endpoints at the OS or application level. FirmGuard fits into that same pricing model but protects at the BIOS firmware level which is an often-overlooked component of a device's security posture.
- **Differentiate Yourself** - By incorporating FirmGuard into their service offerings, MSPs can differentiate themselves in a crowded market. By educating clients about the importance of BIOS firmware security and offering tailored solutions, MSPs can build stronger, long-term relationships that drive recurring revenue.

Here is what some of our customers have to say about FirmGuard:

> **"FirmGuard identified a security gap I didn't even realize I had"**
>
> *- Malcolm McGee*
> *President and Ownder of CMIT Solutions San Antonio North Central*

> **"We rely on FirmGuard to secure our clients' BIOS firmware which helps us differentiate our service offering."**
>
> *- Jason Sternad*
> *Systems Analyst Auxi Solutions*

> **"FirmGuard is one of the more unique tools in our arsenal. None of our other tools allows us to remotely manage BIOS across all manufacturers easily within one panel. The team behind FirmGuard is innovative, and we're always excited to see how they're moving the product toward practical uses for MSPs."**
>
> *- Jesse Judkins*
> *IT Operations Specialist*

> **"In a matter of 15 minutes what we thought was going to be a headache turned out to be something simple, thanks to FirmGuard SecureConfig!!"**
>
> *- Ben Gilbertson*
> *Executive Vice President of Healthy Technology Solutions*

phoenix technologies

UEFI BIOS Malware

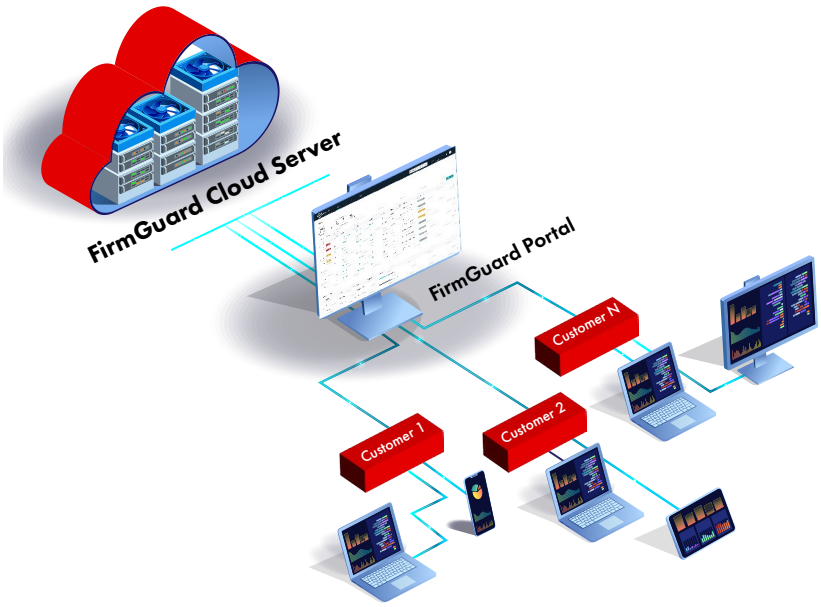
Most organizations don't know much about UEFI BIOS malware. On the FirmGuard website we maintain a list of such attacks and some of the more recent ones come with names such as PKfail, BlackLotus and Moon Bounce. Though these names may sound funny, they are certainly no laughing matter.

BlackLotus UEFI Vulnerability

While many UEFI attacks don't get much press, BlackLotus is one that Microsoft has talked about extensively because it can be very destructive.

One thing that BlackLotus does is disable Secure Boot which is a mechanism to ensure that only an authenticated version of Windows can be launched by the UEFI firmware. This is something a hacker would clearly like to do because without Secure Boot enabled, the hacker can launch any rogue operating system and thereby turn the endpoint into a personal playground. This is where FirmGuard comes into the picture. If an endpoint has FirmGuard installed on it and Secure Boot is disabled because of BlackLotus, or any other reason, an admin is immediately alerted via the dashboard and can then use SecureConfig to take corrective action–stopping an attack in its tracks.

One final point to note about UEFI malware is that it can be so devastating because of persistence. This means that even if you reinstall Windows on an infected endpoint or swap out the hard drive, you still won't solve the problem. The reason is because the UEFI firmware sits in its own dedicated flash memory on the motherboard of the endpoint. So, the only way to solve the problem is to update the firmware and the only way to know about it in the first place is with FirmGuard.



How FirmGuard Works

FirmGuard is a secure, cloud-based solution hosted in Amazon Web Services (AWS). The FirmGuard Cloud Server handles all administrative and technical functionality with a direct interface to each client endpoint. A lightweight FirmGuard agent is installed on each endpoint and is easily deployed using any RMM tool. All monitoring and administration is done via the FirmGuard portal.

phoenix technologies

The FirmGuard Suite of Features

SecureCheck

SecureCheck is a key FirmGuard feature and put simply it is like "antivirus for your UEFI BIOS firmware." SecureCheck keeps track of all activities related to UEFI firmware and alerts administrators anytime something with respect to UEFI firmware changes.

SecureConfig

FirmGuard SecureConfig eliminates the need for physical access to endpoints for BIOS configuration. Admins can remotely adjust BIOS settings, overcoming geographical barriers and administrative complexities.

SecureUpdate

SecureUpdate provides a centralized, secure and standardized way to make UEFI BIOS firmware updates across a heterogeneous mix of endpoints, all with minimal involvement from IT staff.

SecureWipe

SecureWipe is a FirmGuard feature that securely erases endpoint HDD, SSD, and other mass storage devices. It is triggered remotely from the FirmGuard Portal and forensically erases all data and partitions independent of the operating system (OS).

SecureSense

SecureSense provides key endpoint data and information. It detects Legacy Boot Mode, tracks BitLocker status, and provides part/serial numbers for inventory control.

SecureBeat

SecureBeat links the FirmGuard endpoint agent and Cloud Server via a secure, encrypted tunnel, supporting features like SecureCheck, SecureConfig, SecureUpdate, and SecureWipe.

Learn how FirmGuard can help you remotely secure, configure and update UEFI BIOS firmware. Book your 15 minute demo today.

firmguard.com/demo

phoenix technologies

rev. 02.10.25