SOLUTION BRIEF

FirmGuard® SecureUpdate

REMOTE BIOS UPDATE

Introduction

One of the most critical, yet often overlooked, aspects of endpoint security is keeping the UEFI BIOS firmware up to date. Updating UEFI firmware is crucial for maintaining system stability, security, and performance. Manufacturers regularly release updates to address emerging threats and vulnerabilities, fix bugs, and improve hardware compatibility, ensuring that the endpoint runs smoothly with reduced risk of unauthorized access or malicious attacks. Failing to apply these updates can leave systems exposed to exploits that target outdated UEFI firmware. Attackers often seek out systems with unpatched vulnerabilities, making regular updates crucial for maintaining system integrity and protecting sensitive data.

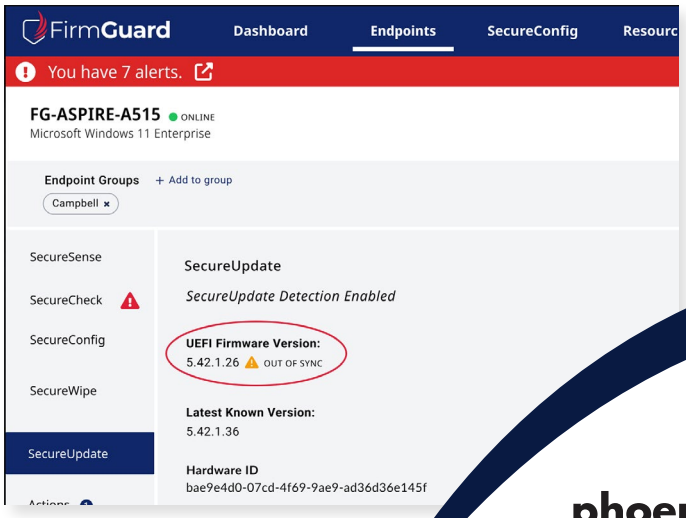
> **SecureUpdate provides a centralized, secure and standardized way to make UEFI BIOS firmware updates across a heterogeneous mix of endpoints, all with minimal involvement from IT staff.**

From a practical standpoint, however, UEFI firmware can be very cumbersome to update because there isn't an automated and consistent way across manufacturers to apply updates, particularly remotely. Furthermore, some IT professionals are intimidated by the process and fear that they might accidentally "brick" an endpoint if they use an incorrect or corrupted version of the UEFI firmware. Each manufacturer offers their own proprietary method to make UEFI firmware updates, some with specialized tools, but what if your environment has endpoints from different manufacturers or you cannot be in front of the endpoint to make an update?

FirmGuard SecureUpdate removes all these obstacles and provides smooth and consistent UEFI firmware updates. So, there is no longer any reason for an endpoint under management to have out-of-date UEFI firmware.

Detect Out-of-Date Firmware

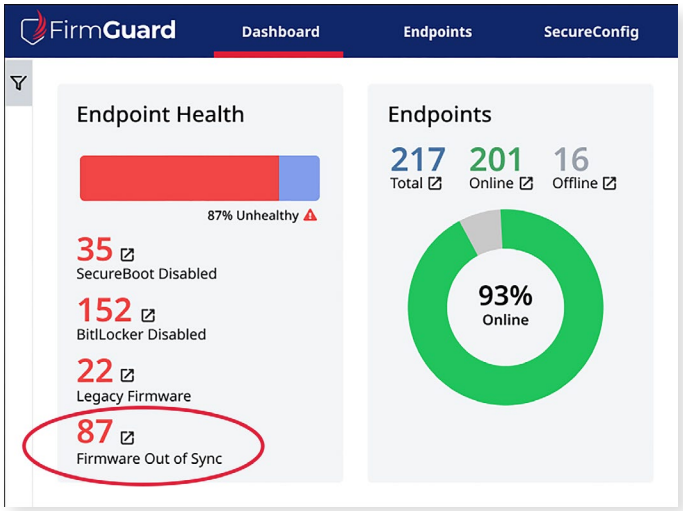
The first step in any update process is to understand which endpoints are out-of- date. FirmGuard continuously monitors all aspects of the UEFI firmware including which version is currently installed on a given endpoint. This graphic shows an Acer Aspire A515 laptop with firmware version 5.42.1.26, but FirmGuard knows that the most recent version is 5.42.1.36 and provides a visual warning to alert the IT administrator.



phoenix technologies

SecureUpdate

FirmGuard is aware of the latest UEFI firmware versions for all major endpoint manufacturers such as Dell, HP, Lenovo, Acer and more. On a periodic basis, FirmGuard SecureUpdate compares the currently installed firmware version to the latest version supplied by the endpoint manufacturer. If there is a mismatch, that means the endpoint firmware is out-of-date, and the first visual indicator will appear on the FirmGuard dashboard in the ***Firmware Out of Sync*** counter. From the dashboard, an IT administrator can determine, at-a-glance, how many endpoints are out-of-date. From there the administrator can manually perform firmware updates or allow SecureUpdate to perform the updates in the background including on a defined schedule.



Capsule Update

An update to UEFI firmware uses a special mechanism called a **capsule update**. It involves packaging the firmware update within a "capsule" file format that is then processed by SecureUpdate. The firmware update is obtained from the manufacturer and is encapsulated in a structured file format, often a binary file, that includes the new firmware image, metadata and other necessary components for the update process. The capsule update includes a digital signature to verify the authenticity and integrity of the update, thus reducing the risk of installing malicious or corrupted firmware. It also often supports rollback protection and version checks to ensure that the endpoint is not downgraded to an insecure version of the firmware.

Capsule updates adhere to the UEFI specification and may comply with security frameworks and standards like NIST, ISO, or CMMC, which require secure firmware update mechanisms. One of the key benefits is safety because the update occurs in a pre-boot environment, thus eliminating the risk of interference from the operating system or other malware. In addition, capsule updates can be automated by SecureUpdate and they are secure because they are done in a controlled environment.

As an example scenario, a laptop manufacturer might issue a UEFI firmware update to address security vulnerabilities. This update would be packaged as a capsule, digitally signed, and distributed by the manufacturer. SecureUpdate obtains this update and FirmGuard schedules the update to be applied on the next reboot--before the operating system loads--ensuring a secure and reliable update process across a heterogenous group of endpoints.

For more details, please
contact your Phoenix representative
or email info@firmguard.com

phoenix technologies

rev. 09.26.24