FIRMGUARD CASE STUDY

HTS HEALTHY TECHNOLOGY SOLUTIONS

FirmGuard

SecureConfig to the Rescue!

Introduction

Healthy Technology Solutions (HTS) had been using FirmGuard successfully for many months to measure and monitor the status of their client endpoints, including UEFI BIOS firmware security. Within the span of less than a month, however, they suddenly had two high priority use cases for SecureConfig—which they had only recently begun to use. The specifics of the two use cases are highlighted below.

Use Case #1: Enable BitLocker

Healthy Technology Solutions had a local client that had recently established an overseas office that was nearly 7,600 miles and 13 time zones away from Las Vegas. The local client had purchased two new laptops and an HTS technician followed the New Computer Setup form to configure the laptops. During setup, he was unable to enable BitLocker because the TPM (Trusted Platform Module) hardware was showing as "unavailable". The fix was obvious, enable TPM in UEFI BIOS firmware settings, however that would require coordination with the local client and with the 13-time zone difference that was going to be complicated.

> **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*

SUMMARY

Healthy Technology Solutions (HTS) is an MSP based in Las Vegas and Central Florida that provides IT services to a diverse set of clients. HTS has been using FirmGuard since December 2022 and currently has over 2,000 endpoints deployed on the FirmGuard platform. HTS utilizes FirmGuard on a daily basis to protect, configure and update BIOS firmware on client endpoints.

KEY CHALLENGES

+ Costly and time consuming to update client endpoint BIOS firmware settings
+ Time zone difference occasionally makes direct interaction with client very difficult

PRODUCT/FEATURE USED

+ SecureCheck
+ SecureBeat
+ SecureSense
+ SecureConfig
+ SecureWipe

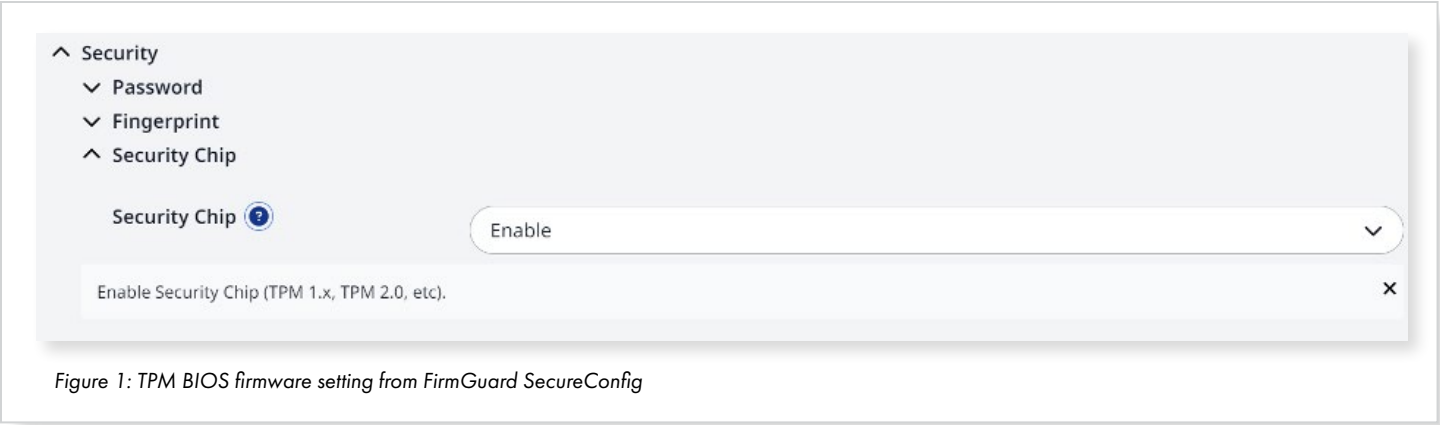
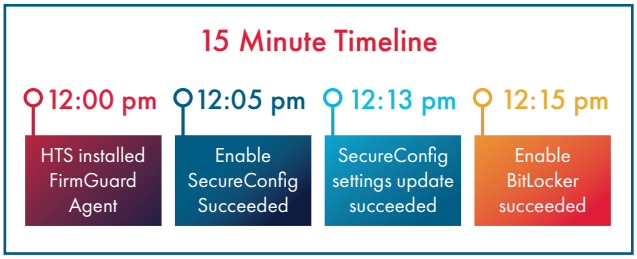


Figure 1: TPM BIOS firmware setting from FirmGuard SecureConfig

The technician was unaware of FirmGuard SecureConfig and presented the problem to one of his colleagues who was very familiar with FirmGuard, but hadn't yet used SecureConfig himself. The pair decided to give it a try. They logged into the FirmGuard portal from Las Vegas, pushed the FirmGuard agent to both laptops and then browsed the available BIOS settings via SecureConfig.

They quickly drilled down and under "Security" found a setting to "Enable" the TPM security chip. After pressing the save button, the endpoint rebooted, and upon restart the drive started encrypting with BitLocker, as expected. What they thought was going to be a time-consuming headache turned out to only take 15 minutes to resolve, thanks to SecureConfig.



Use Case #2: Laptop Camera Not Working

An HTS technician was on the phone with a Dell customer support representative to help resolve an issue with the camera on a client laptop. The Dell laptop camera would suddenly just stop working for no explicable reason. The Dell representative was perplexed and asked the HTS technician to go into BIOS firmware settings on the laptop and disable the camera, so he could further investigate.

Normally, this would have been a challenging and time-consuming task because the HTS technician would have to call the client and step them through the BIOS configuration procedure. This could potentially take days to coordinate a time with the client and execute. To further complicate matters, in this case, HTS didn't have that much time as the Dell laptop warranty was about to expire in the coming days. However, with FirmGuard SecureConfig the HTS technician was able to navigate to the Dell laptop's UEFI BIOS firmware settings page and disable the camera, all while still on the phone with the Dell representative. The camera issue was then promptly resolved and once again it was SecureConfig to the rescue!

WHY FIRMGUARD?

HTS chose Phoenix FirmGuard because of its unique ability to measure, manage and mitigate endpoints at the UEFI BIOS firmware level. UEFI BIOS firmware was an unprotected area in the HTS endpoint security stack that was critical to address, but the solution they chose to "plug that hole" had to be easy to use and offer other unique value adds such as remote BIOS configuration and remote endpoint disk erase. FirmGuard fit the bill completely, so HTS embarked on a full-scale rollout across their client base.

phoenix technologies

2105 S. Bascom Avenue, Suite 316
Campbell, CA 95008.3295
Toll Free: 1.800.677.7305
Tel: +1.408.570.1000
phoenix.com