FIRMGUARD CASE STUDY

RQM Consulting Finds New Ways to Use FirmGuard

Introduction

The main proponent of FirmGuard within RQM Consulting is Jesse Judkins who is an IT Operations Specialist and works closely with the President, Rod Miller. Jesse did the initial assessment of FirmGuard and rolled it out cautiously to the RQM client base, but he admits in retrospect, because the install process was so seamless, that he could have done it all within a matter of days.

> It installed easily and didn't intrude on much.
>
> *- Jesse Judkins*
> *IT Operations Specialist, RQM Consulting*

Since RQM uses FirmGuard on a daily basis they have many different use cases. Here are three use cases that are particularly impactful:

Use Case #1 – How can I better understand the capabilities of the endpoints I am managing?

FirmGuard's SecureConfig feature is meant to be used by administrators to remotely configure endpoint BIOS settings and RQM certainly uses it for that purpose. However, one day after Jesse loaded the FirmGuard agent onto each Lenovo laptop of a long-standing client, he began to browse the various BIOS settings that were exposed via SecureConfig. He noticed a specific parameter that each of these Lenovo machines supported called "Bottom Cover Tamper Detection."

He had never heard of this capability, but after a quick Google search,

SUMMARY

RQM Consulting is an emerging MSP based in Oklahoma. RQM has deployed FirmGuard across their entire customer base and utilizes it every day to protect their clients' BIOS, increase technician efficiency and meet developing compliance requirements.

KEY CHALLENGES

- Understanding the hardware and software capabilities of new endpoints under management
- Helping clients comply with complex and stringent media sanitization standards and requirements
- Increasing technical efficiency without compromising security

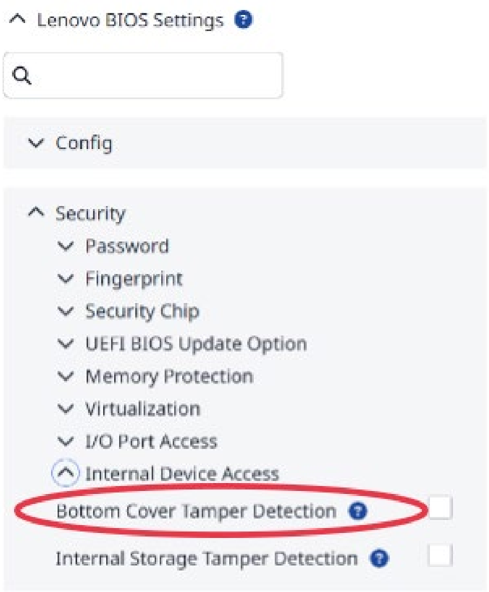
PRODUCT/FEATURE USED

- SecureCheck
- SecureBeat
- SecureSense
- SecureConfig
- SecureWipe

found that if enabled (it is disabled by default) the system detects tampering with the bottom cover, and on the next boot automatically asks for the admin password before the boot to the operating system will continue. The result is you get informed if someone tampers with the laptop enclosure. Jesse was amazed that RQM had this client for 15 years, but it is only now because of FirmGuard that they found this valuable capability that was sitting there right under their nose all these years.

> **I did not know that [bottom cover tamper detection] was an option.**
>
> *- Jesse Judkins*
> *IT Operations Specialist, RQM Consulting*

From this experience, Jesse came up with a novel use case for SecureConfig that he continues to use. Each time he browses SecureConfig settings he gains a better understanding of the features and capabilities of the endpoints he manages for his clients.



Use Case #2 – SecureWipe and Compliance

RQM Consulting has a client in Oklahoma that is particularly security conscious and goes through annual security audits for various aspects of their business. One area the client is sensitive about is media sanitization or endpoint erasure. By virtue of the client's business, they maintain personally identifiable information (PII) on their customers and thus have to make sure none of that data remains behind when endpoints are disposed of or recycled. Below is a snippet of three recommendations made by the client's auditor with respect to media sanitization (the name of the [AUDITOR] and [CLIENT] have been replaced with brackets to protect their identify):

- [AUDITOR] recommends that [CLIENT] follow Oklahoma Office of Management and Enterprise Services Information Security Policies, Procedures, Guidelines Appendix E, Section 3; it provides state-approved guidance for media sanitization and disposal. The disposition of un-sanitized hard drives is, by policy, acceptable but not recommended because [CLIENT] maintains PII. https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf
- AUDITOR] recommends that [CLIENT] follow the disposition practices in their documentation and perform sanitization before disposition.
- [AUDITOR] recommends that [CLIENT] review NIST SP800-88, Guidelines for Media Sanitization when creating the "Information Retention and Disposal Policy" mentioned in [CLIENT] documentation: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

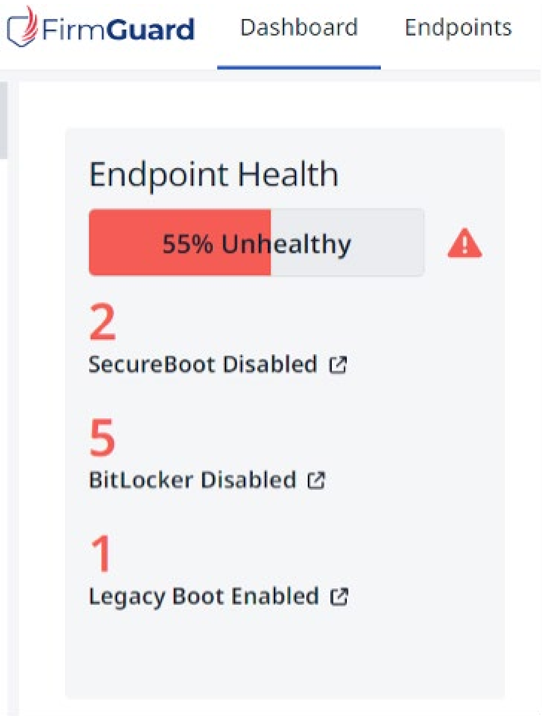
> **This client has some pretty heavy-handed requirements as far as cybersecurity goes.**
>
> *- Jesse Judkins*
> *IT Operations Specialist, RQM Consulting*

The auditor is very explicit in his recommendations which the client intends to follow religiously. In previous years, RQM Consulting didn't have any products or services that could help its client conform to these rules and regulations. However, in this year's review they gladly informed the client about FirmGuard SecureWipe and everyone agreed that it conformed to the audit requirements and specifically pages 51, and 82-83 of the OMES document were relevant to SecureWipe. Also, page 84 describes "Secure Erase" which SecureWipe supports, and the document also contains references to NIST SP800-88, so it comes full circle.

Use Case #3 – How many endpoints have BitLocker enabled?

One day, the President of RQM Consulting, Rod, came by Jesse's desk and asked him if he knew what percentage of their endpoints under management had BitLocker enabled. Rod didn't expect Jesse to have the answer at his fingertips, but Jesse had the FirmGuard dashboard open on his computer screen, so he just glanced over and let him know that only about 30% had it enabled. Rod was surprised at how low the number was, and that Jesse had such easy access to the information. In fact, this one interaction prompted Rod to accelerate the rollout of FirmGuard to more RQM Consulting clients.

In the past, Jesse could get the information, but it required some scripting on his part and also the data wasn't dynamic, meaning he would have to run a script each time he wanted the information. With FirmGuard, the information is available at a glance, and updates automatically anytime something changes on the endpoint.



Endpoint Health

55% Unhealthy

2
SecureBoot Disabled

5
BitLocker Disabled

1
Legacy Boot Enabled

> **What can I say, FirmGuard just makes my life easier**
>
> *- Jesse Judkins*
> *IT Operations Specialist, RQM Consulting*

WHY FIRMGUARD?

RQM Consulting went from demo to trial to production customer in a matter of weeks and hasn't looked back. They have uncovered novel uses for SecureConfig and continue to push the boundaries with respect to their product usage. In addition to protecting their clients' BIOS from compromise, technician efficiency has increased dramatically with FirmGuard as they no longer have to go onsite to deal with BIOS related matters but instead handle it all remotely from the comfort of their offices in Oklahoma.

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