FIRMGUARD CASE STUDY

ASC Group Uses FirmGuard to Manage BIOS and Meet Compliance Requirements

Introduction

ASC Group is a trusted IT services provider based in Georgia, delivering managed and co-managed IT support, cybersecurity, compliance, networking, and more. Since its founding in 1999, the company has built a reputation for staying ahead of the curve and in 2024, they took another leap forward by adopting FirmGuard.

Within months, ASC Group rolled out FirmGuard across all client endpoints and starting in 2025, it became a standard part of their technology stack. Thanks to its intuitive interface and powerful capabilities, FirmGuard is now a go-to tool for the entire ASC team, including junior technicians, who rely on it daily.

> **FirmGuard has quickly become an indispensable part of our tech stack.**
>
> *- John Chesser*
> *Virtual Chief Security Officer (vCSO)*

While ASC Group continues to uncover new use cases for FirmGuard, two key applications quickly stood out and have since become essential to their operations. Here's a look at those core use cases:

Use Case #1 – BIOS Management Policy

Prior to FirmGuard, ASC Group didn't have a well-defined BIOS management policy for their client endpoints. Both BIOS configuration

SUMMARY

ASC Group, a leading IT services company founded in 1999 and based in Georgia, has fully integrated FirmGuard across its client base for BIOS management, regulatory compliance, and reporting. They appreciate FirmGuard's ease of use, as it enables even junior technicians to utilize the product with minimal training.

KEY CHALLENGES

+ Implementing a well-defined and operationally efficient BIOS management policy
+ Helping clients comply with complex and stringent regulatory standards and requirements
+ Increasing technician efficiency without compromising security

PRODUCT/FEATURE USED

+ SecureConfig
+ SecureUpdate
+ SecureWipe
+ SecureCheck
+ SecureSense
+ SecureBeat

changes and updates were done on an ad-hoc basis and only when there was an urgent need. For years, ASC recognized this glaring hole in their security posture and just hoped it didn't cause any unmanageable problems. They understood that hope isn't a strategy and after testing FirmGuard, quickly realized it would solve the nagging issue they knew they had, but didn't know how to solve.

After fully deploying FirmGuard across all endpoints, ASC instituted a two-pronged approach to BIOS management. First, they utilized SecureConfig to ensure that each endpoint was configured with a client-specific default or "golden" BIOS configuration. For example, some clients might want the USB ports on all endpoints to be disabled and others might not. Second, they utilized SecureUpdate—for the first time ever—to perform scheduled firmware updates. The BIOS updates were added to a pre-defined maintenance window that was used to perform OS and other application updates.

One unexpected benefit of the regularly scheduled BIOS updates was a reduction in "ghost issues". These are endpoint problems which appear for no apparent reason such as Bluetooth suddenly stops working. An out-of-date BIOS version was often the cause of these issues and as endpoints started getting regular BIOS updates there was a corresponding drop in ghost issues. This was an unexpected, but very significant operational efficiency that was entirely due to the regular use of FirmGuard.

> **FirmGuard has greatly enhanced our regulatory compliance and reporting.**
>
> *- John Chesser*
> *Virtual Chief Security Officer (vCSO)*

Use Case #2 – Reporting and Compliance

Security compliance, both regulatory and based on internally defined best practices, is a major selling point for ASC Group and is the reason many clients choose them over competitors. ASC often serves as a virtual Chief Security Officer (vCSO) for small clients; and works directly with the CSO or equivalent for larger clients. In both roles, regular and reliable reporting is invaluable to keep clients satisfied and willing to pay a premium for the services they receive.

A financial services client remarked that ASC was the first MSP they had ever engaged with that could provide irrefutable proof that all endpoints had the latest version of BIOS firmware installed. The client faced heavy regulatory scrutiny and was always looking for any extra information they could provide auditors to prove that they were taking endpoint integrity seriously.

Many clients appreciated that ASC could easily provide information about the BitLocker status of each managed endpoint. In the past, ASC would only reluctantly provide this information because it required running scripts and some manual intervention which meant a senior technician had to be involved. With FirmGuard, even the most junior technician, with almost no training, could now provide BitLocker status and other metrics on a proactive basis. This type of efficiency delighted clients and kept operational costs low.

Another standout use case is media sanitization. ASC helps clients meet NIST SP 800-88 guidelines for media sanitization using FirmGuard's SecureWipe. Previously, this process was slow, expensive, and required specialized expertise. With SecureWipe, any authorized technician can securely wipe drives with minimal effort and there is no extra training needed.

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