SOLUTION BRIEF

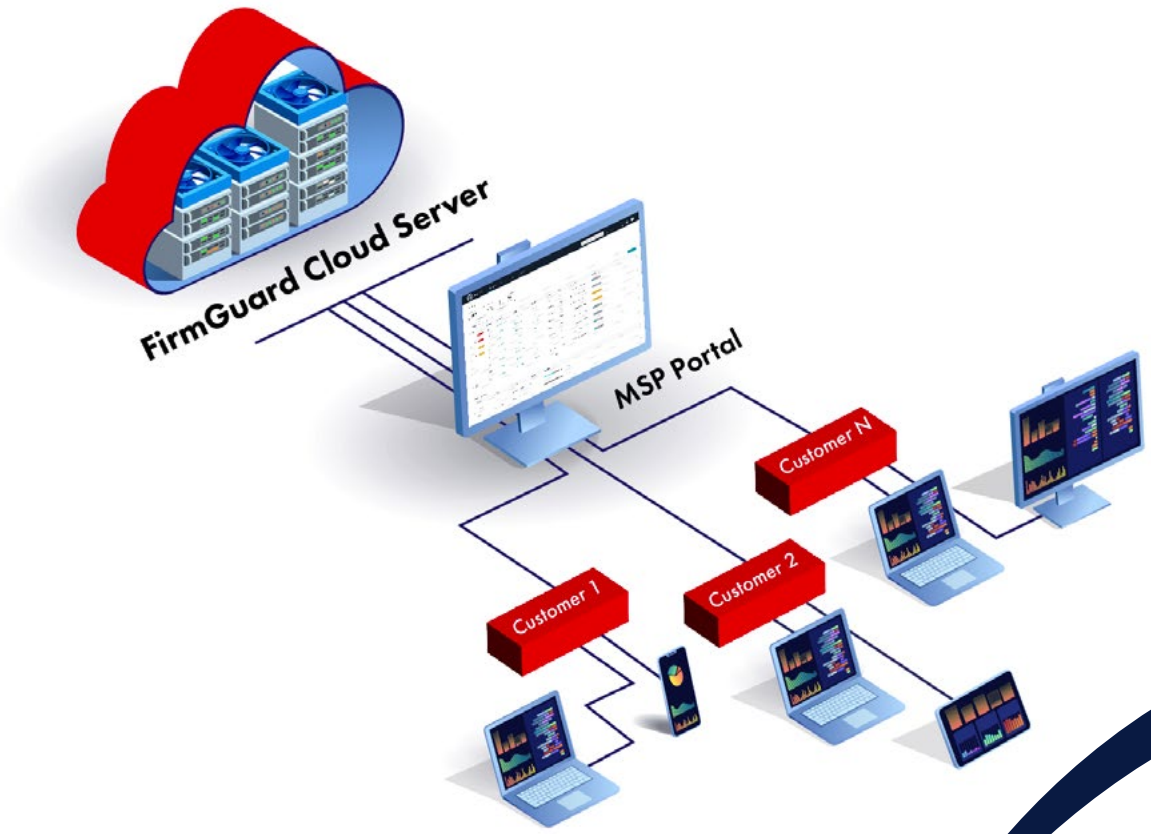
Phoenix FirmGuard®

FIRMWARE RISK MANAGEMENT

What Is Phoenix FirmGuard?

FirmGuard is a solution for Managed Service Providers (MSPs) to seamlessly manage the firmware in their customer endpoints from a single pane of glass. FirmGuard is backed by Phoenix Technology's 40+ years of technology and market leadership in endpoint firmware. Phoenix was founded in 1979 and created the first IBM clone compatible BIOS—well before the term "endpoint" was ever used. With FirmGuard, Phoenix takes their wealth of knowledge, expertise, and intellectual property in firmware to offer a scalable, best-in-class solution to combat the increasing problem of endpoint vulnerability.

FirmGuard is a secure, cloud-based solution that is hosted in Amazon Web Services (AWS). The FirmGuard Cloud Server handles all administrative and technical functionality with a direct interface to each customer endpoint. An MSP can easily and securely manage all of their customer endpoints from a single pane of glass called the MSP Portal.



phoenix technologies

Why Should MSPs Care About Firmware?

Companies have spent billions of dollars protecting their endpoints from OS level attacks with some success. But most have spent almost nothing to protect the firmware in those same endpoints. In fact, Gartner Group estimates that "70% of organizations that do not have a firmware upgrade plan in place will be breached due to a firmware vulnerability". This is because hackers are becoming more sophisticated, and they now realize that firmware is an underappreciated attack vector which is relatively easy to exploit if not properly protected.

Only 13%-25% of enterprises view security below the operating system as a priority.

- IDC

Your customers today are almost certainly experiencing firmware vulnerabilities and don't even know it. With FirmGuard you can offer them a brand-new service which will immediately scan their endpoints to find vulnerabilities. Armed with that data, you can educate them on this new attack surface and offer a solution to help solve the problem. This will differentiate you from other MSPs and solidify your position as the MSP of choice for your current and future customers. This will then naturally lead to more revenue for your company.

The best part is, for a limited time, you can do all of this free of charge with the FirmGuard Foundation Pack. See details below.

The total number of medium to high-risk firmware vulnerabilities tracked by Phoenix has more than quadrupled in less than five years.

- Phoenix Technologies

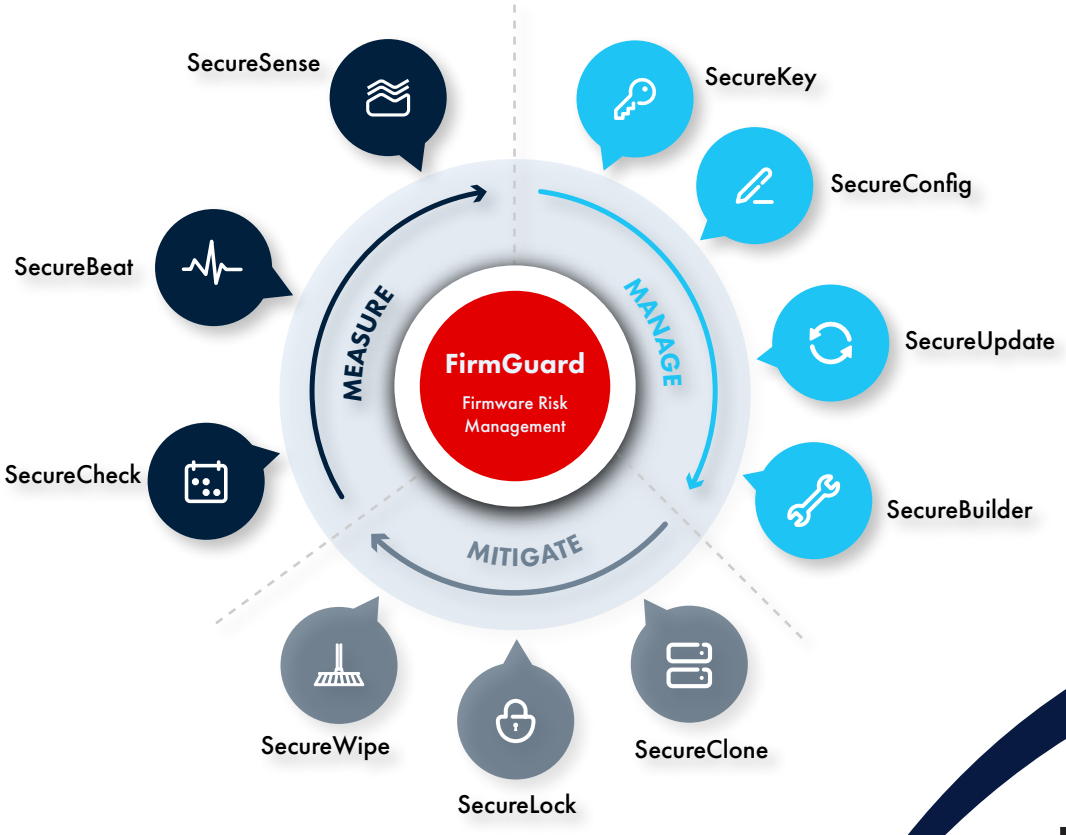
phoenix technologies

Tell Me About the Technology

FirmGuard supports MSPs in implementing security best practices via our three pillars of security: **Measure**, **Manage**, and **Mitigate**.

The first pillar is ***measure*** and as the name implies this is when key information related to firmware and other endpoint metrics are collected and analyzed. Once the MSP has a baseline measurement of each endpoint, the next is ***manage*** and this is where an MSP can remotely manage the endpoints to update critical firmware settings and software as well as set and enforce specific security policies such as multi-factor authentication (MFA). Finally, if firmware or other security issues arise with a given endpoint, FirmGuard provides a suite of features to ***mitigate*** the problem ranging from cloning a hard drive to temporarily locking it or in an extreme case completely forensically wiping the drive. Collectively we call the pillars the ***"3Ms"***.

For each pillar of security, there is a suite of FirmGuard features that specifically addresses the needs of that pillar. For example, in the measurement phase there is "SecureCheck", "SecureBeat", and "SecureSense". Following are short descriptions of each "Secure" feature.



phoenix technologies

Features

SecureCheck: Revalidates an endpoint's chain of trust, ensuring secure operation by establishing that the correct OS version is running and confirming the root of trust between hardware, firmware, and OS. This feature can be run manually or at automatically scheduled intervals such as weekly or monthly. An MSP administrator can check device firmware status at a glance via an indicator in the portal.

SecureBeat: Maintains a secure heartbeat between the endpoint and the FirmGuard cloud server. A loss of beat is the first indication or alert of possible endpoint related issues. With SecureBuilder workflows can be constructed to automatically take mitigation steps (e.g., lock hard drive) if the beat is missing for an unexpected period.

SecureSense: Remotely monitor endpoint status and health to detect unusual or suspicious behavior. The feature specifically monitors firmware status (i.e., vendor, version, last update, etc.), endpoint inventory (i.e., system make/model, OS version, etc.) and endpoint metrics (i.e., CPU, disk and memory utilization, etc.).

SecureKey: Firmware enforced multi-factor authentication (MFA) using a physical key such as a FIDO/FIDO2 compliant device or USB storage device. The operating system (OS) will not load without the configured secure key. Configurations can be done remotely by an MSP administrator via the portal.

SecureConfig: Remotely configure BIOS settings across an array of endpoints. Greatly streamlines and consolidates administration of BIOS settings across an entire organization. With this feature MSP administrators can easily enable or disable firmware settings to ensure proper security configurations.

SecureUpdate: Identifies the current firmware version and provides an indication when a newer version is available. An administrator can remotely update to the latest (or older) version across an array of endpoints. Adheres to UEFI capsule update guidelines NIST SP 800-147 & NIST SP 800-193. One of the best ways to prevent a firmware level attack is to proactively update to the latest firmware version.

SecureBuilder: An automation and workflow engine that can be used to pre-schedule tasks or trigger certain actions. For example, it could be used to regularly schedule (e.g., monthly) a SecureCheck initiated reboot of select endpoints. Both simple and complex workflows can be constructed and may involve any other feature such as SecureBeat, SecureLock or SecureWipe.

SecureClone: A method to duplicate an endpoint's hard drive contents to a different location. The duplication can be easily performed from the same single pane of glass (portal) that is utilized by all other features. The duplication can be part of a workflow or done proactively to perform forensic analysis or recover lost work.

SecureLock: Locks hard drive at the firmware level to prevent unauthorized access without the administrator generated password key. Without entering the key and unlocking the hard drive the endpoint cannot boot the operating system. Can potentially prevent ransomware attacks that seek to lock the hard drive contents. Protects data at rest, even if the hard drive is moved to a different system.

SecureWipe: Remotely performs a forensic wipe (at the bit level) of SSD, HDD and other mass storage devices independent of the operating system. Supports hardware erase methods such as ATA and NVMe secure erase, OPAL password/PSID revert, and multiple industry standard software algorithms such as DoD5220.22-M

phoenix technologies

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

phoenix technologies

rev. 10.23.23