SOLUTION BRIEF

FirmGuard® SecureCheck™

ANTIVIRUS FOR UEFI BIOS FIRMWARE

Introduction

Endpoint protection is a standard part of every organization's technology stack and has evolved over time from antivirus and spam protection to Zero Trust, EDR, XDR and so forth. The acronyms keep changing, but fundamentally endpoint protection still means protecting applications and the operating system in some form. The problem with these paradigms is that they ignore a glaring hole in the software stack that hackers are increasingly moving to exploit as other avenues are closed: **UEFI BIOS firmware.**

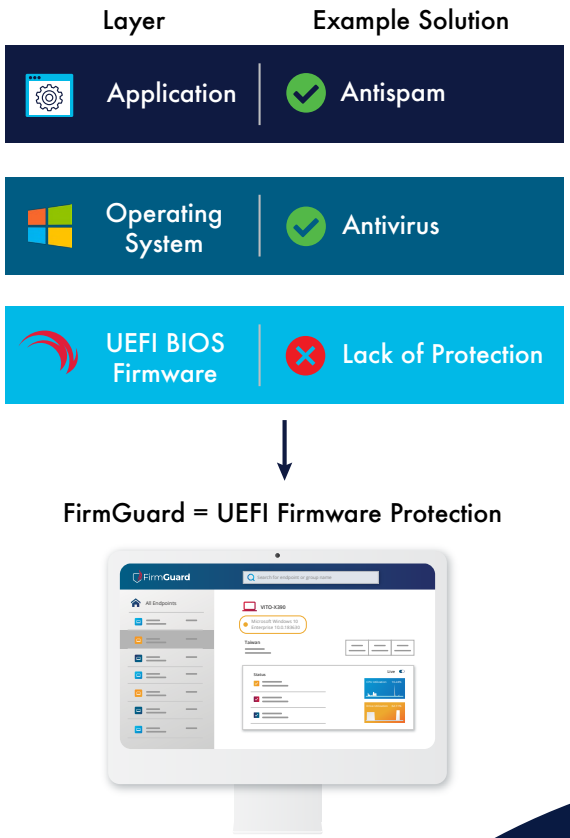
Is your UEFI BIOS Firmware protected?

Organizations that ignore UEFI BIOS firmware vulnerabilities, do so at their own peril and are setting themselves up for a potentially devasting attack. But what is UEFI? How do we protect endpoints from UEFI BIOS vulnerabilities? And what types of vulnerabilities are there?

Unified Extensible Firmware Interface (UEFI) is a modern firmware specification first introduced in 2005 (now on version 2) that is implemented on everything from low-cost desktop computers to high-end servers. The UEFI Forum maintains the specification and there are over 250 member companies including hardware and software vendors. UEFI is the default firmware for modern computers and is the very first software to run when an endpoint is powered on. UEFI begins with hardware initialization and is responsible for successfully loading the Operating System (OS). After the OS takes over, UEFI is still in the picture as it maintains control over many diverse system settings related to hardware, security, system startup and networking.

If UEFI firmware is compromised, the hacker has complete control over the endpoint including which OS runs and with what forms of malware.

Endpoint Software Stack



phoenix technologies

SecureCheck

The best way to protect vulnerable endpoints is to enable FirmGuard SecureCheck on every managed endpoint.

SecureCheck is a key feature of FirmGuard and put simply it is like "antivirus for your UEFI BIOS firmware." SecureCheck identifies changes related to UEFI firmware and alerts administrators anytime something changes with respect to UEFI firmware, the operating system boot loader, and certain security settings–both good and bad. For example, if an endpoint is legitimately updated with new UEFI firmware, the FirmGuard administrator will be made aware, though no action is required. In the event an endpoint is infected with UEFI related malware (e.g., bootkit or rootkit), SecureCheck will alert the administrator of unexpected changes and recommend remediation actions to resolve the situation. With SecureCheck in place, administrators can rest assured that they have closed one of the last remaining major open holes for endpoint exploitation.

BlackLotus UEFI Vulnerability

In April 2023 Microsoft published an Incident Response report regarding a new UEFI bootkit dubbed BlackLotus. Microsoft noted, "UEFI bootkits are particularly dangerous as they run at computer startup, prior to the operating system loading, and therefore can interfere with or deactivate various operating system (OS) security mechanisms such as BitLocker, hypervisor-protected code integrity (HVCI), and Microsoft Defender Antivirus."

BlackLotus is called a bootkit because it hijacks the normal UEFI boot process by injecting malware during the boot sequence. The malware disables key security features, including antivirus, thus opening up the system to full exploitation by hackers. The bootkit persists across endpoint reboots and so for remediation Microsoft suggests, "If a device is determined to have been infected with BlackLotus, the device should be removed from the network and reformatted (both the OS partition and EFI partition) or restored from a known clean backup that includes the EFI partition."

To make matters worse, the vulnerable binaries (malware) have not been added to the UEFI revocation list in order not to "brick" computers that have not been patched yet. This leaves the unpatched machines vulnerable to the BlackLotus attack.

BlackLotus is just one of many well-known UEFI vulnerabilities. Others have names such as PixieFail, CosmicStrand, Moon Bounce, LogoFail and still others are unnamed. For an up to date, comprehensive list of UEFI vulnerabilities please consult:
https://firmguard.com/security-notifications

SecureCheck helps maintain ISO and NIST compliance

SecureCheck helps FirmGuard customers, and their clients comply with a variety of industry standards. The list below provides a detailed breakdown of compliance with specific standards including individual clauses within the standard.

ISO 27001 Clause 9.4.2 (User Access Management)	**SecureCheck** audits and ensures compliance with access management policies, verifying that only authorized users have access.
ISO 27001 Clause 12.4 (Logging and Monitoring)	Ensures compliance with logging and monitoring requirements using **SecureCheck's** comprehensive auditing capabilities.
ISO 27001 Clause 12.6.1 (Management of Technical Vulnerabilities)	**SecureCheck** aids in the timely identification and remediation of technical vulnerabilities.
ISO 27001 Clause 16.1.1 (Management of Information Security Incidents)	**SecureCheck** has an insight dashboard that assists in determining potential incidents, enhancing incident management processes.
ISO 27001 Clause 18.2.2 (Compliance with Security Policies and Standards)	**SecureCheck** can verify compliance for internal security policies and standards, mitigating compliance risks.
NIST SP 800-53 RA-5 Vulnerability Scanning	**SecureCheck** scans for vulnerabilities to identify security weaknesses and enhance cyber defenses.
NIST SP 800-53 SI-4 (System Monitoring)	**SecureCheck** can monitor system activities, helping to detect unauthorized changes and activities in real time.
NIST SP 800-53 CA-7 / NIST Cybersecurity Framework DE.CM-7 (Continuous Monitoring)	**SecureCheck** continuously monitors security controls, ensuring ongoing compliance and security posture management.
NIST Cybersecurity Framework ID.RA-2 (Threat Identification)	**SecureCheck** helps identify potential cybersecurity threats, ensuring proactive risk management.

Learn how FirmGuard can help you remotely secure, configure and update UEFI BIOS firmware. Book your 15 minute demo today.

firmguard.com/demo

phoenix technologies

rev. 02.10.25