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 tech stack that hackers are increasingly moving to exploit as other avenues are closed: **UEFI BIOS firmware.**

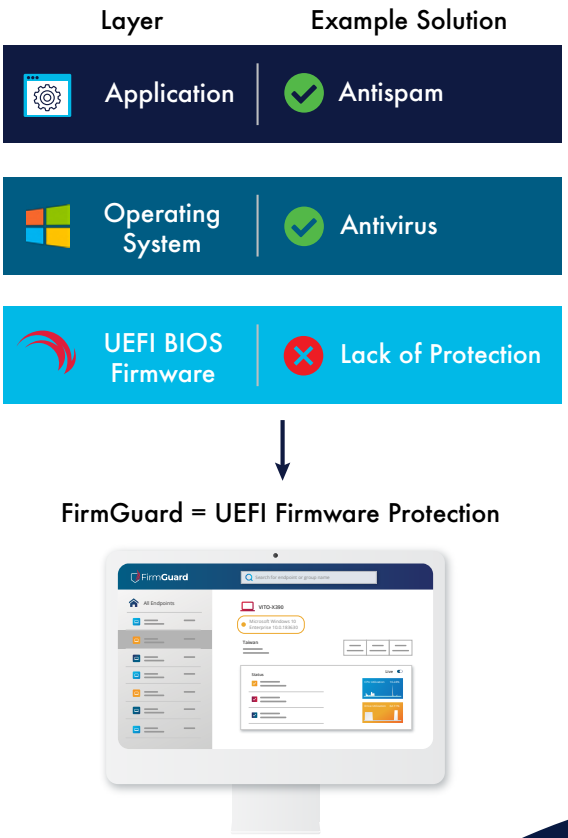
Is your UEFI BIOS Firmware protected?

Organizations that ignore UEFI BIOS firmware vulnerability 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 keeps track of all activities related to UEFI firmware and alerts administrators anytime something with respect to UEFI firmware changes, both good and bad. For example, if an endpoint is legitimately updated with new UEFI firmware, the FirmGuard administrator will be made aware though action is required. In the event an endpoint is infected with UEFI related malware (e.g., bootkit or rootkit), SecureCheck will alert the administrator 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. It leaves the unpatched machines vulnerable to the BlackLotus attack.

BlackLotus is just one of many well-known UEFI vulnerabilities. Others have named 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://www.phoenix.com/security-notifications/