With increasingly sophisticated endpoint security solutions continually thwarting legacy attack techniques, cybercriminals are always looking for more advanced ways to access target organizations’ valuable systems and data. The attack vectors are narrowing, but adversaries continue to search for alternative invasion points within the gaps of organizations’ security postures.

One technique gaining traction among sophisticated attackers is the malicious tampering of the BIOS firmware. Because most endpoint security solutions focus on the local OS and the applications layered above it, they leave the BIOS firmware—the lowest level of the PC stack—vulnerable to malicious attacks that can incapacitate your entire system.

BIOS is an extremely high-impact compromise, attacking the root of trust for the device, and making it an equally stealthy and persistent threat. This gaping vulnerability has become an area of increasing concern as it becomes increasingly easy for attackers to execute as part of their campaign.

Extending endpoint security below the OS
VMware Carbon Black has partnered with Dell to develop a joint solution to help security teams detect and more effectively remediate attacks that tamper with BIOS firmware on their Dell Trusted Devices.

This integrated solution allows security and IT teams to automate reporting on BIOS verification status and enables them to remotely remediate attacks that attempt BIOS tampering. This partnership between VMware Carbon Black and Dell extends endpoint security below the OS, making Dell Trusted Devices the most secure corporate endpoint in the market.
How SafeBIOS verification works
With the growing frequency of BIOS-specific attacks, organizations need a more sophisticated way to not only protect their systems, but confidently verify that their systems have not been compromised. Dell integrates post-boot verification into its Dell Trusted Devices, giving IT the assurance that employees’ BIOS have not been altered.

Rather than storing BIOS information on the hardware itself, which is susceptible to corruption, Dell SafeBIOS delivers an off-host BIOS verification capability that compares an individual BIOS image against the official measurements provided by Dell.

Querying and remediating BIOS corruption
Using VMware Carbon Black® Cloud Audit and Remediation™, security teams can now query their entire fleet of Dell Trusted Devices to report on the SafeBIOS verification status at scale. Queries can also be scheduled to run on a daily, weekly or monthly basis, allowing teams to completely automate reporting on this attack technique.

If any devices return a failed status, an administrator can instantly quarantine that device to isolate it from your network and the internet.

After the device is safely isolated, the administrator can gain remote access to the device via Live Response and run a simple script developed by our threat engineers to pull back a full dump of BIOS status for downstream analysis.

LEARN MORE
To set up a personalized demo, visit carbonblack.com/trial.

For more information, email contact@carbonblack.com or visit carbonblack.com/epp-cloud.