VMware Carbon Black Cloud BIOS Firmware Protection

Detect and respond to firmware tampering on Dell Trusted Devices

DELL SAFEBIOS

- Integrates post-boot verification into commercial PCs
- Compares an individual BIOS image against official measurements
- Automates the early detection of BIOS
- Surfaces vulnerable endpoints and alerts IT as the risk increases

VMWARE CARBON BLACK CLOUD AUDIT AND REMEDIATION

- Directly queries endpoints for the current status
- Stores query results in a cloud-based platform
- Automates reporting via scheduled queries
- Provides unified data across security and IT teams
- Leverages the same agent and console as the next-generation antivirus (NGAV) and endpoint detection and response (EDR) platform

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.

REMEDIATION STEPS

- The query will return a failed report
- Quarantine the device from VMware Carbon Black Cloud™
- Remotely access devices using Live Response
- Run a script to pull back a full dump of BIOS status

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*.

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.

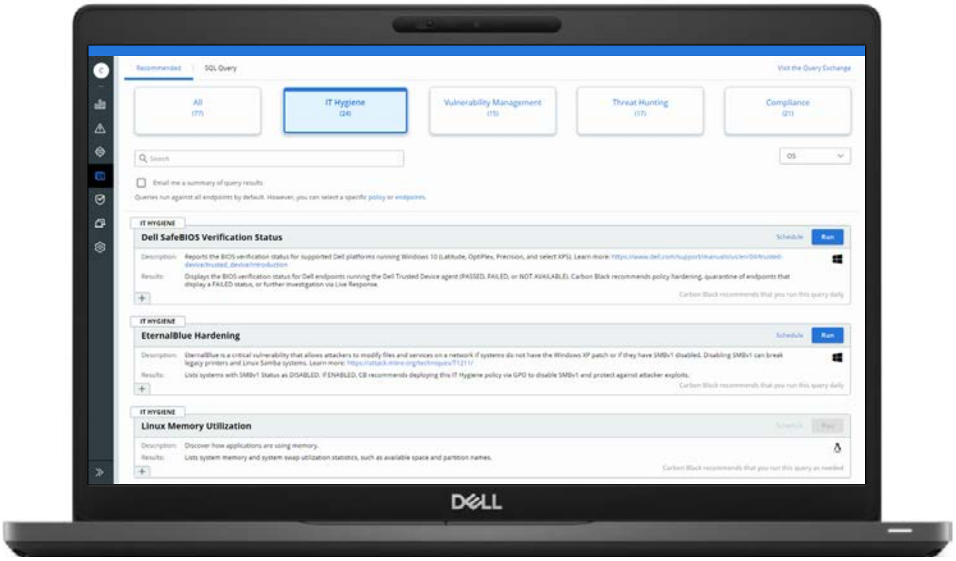
Rather than storing BIOS information on the hardware itself, which is susceptible to corruption, Dell SafeBIOS delivers an off-host BIOS verification capability that compares an individual BIOS image against the official measurements provided by Dell.

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.



□ Email me a summary of query results

Queries run against all endpoints by default. However, you can select a specific policy or endpoints.

IT HYGIENE

Dell SafeBIOS Verification Status

Description: Reports the BIOS verification status for supported Dell platforms running Windows 10 (Latitude, OptiPlex, Precision, and select XPS). Learn more: https://www.dell.com/support/manuals/us/en/04/trusted-device/trusted_device/introduction

Results: Displays the BIOS verification status for Dell endpoints running the Dell Trusted Device agent (PASSED, FAILED, or NOT AVAILABLE). Carbon Black recommends policy hardening, quarantine of endpoints that display a FAILED status, or further investigation via Live Response.

Carbon Black recommends that you run this query daily

IT HYGIENE

EternalBlue Hardening

Description: EternalBlue is a critical vulnerability that allows attackers to modify files and services on a network if systems do not have the Windows XP patch or if they have SMBv1 disabled. Disabling SMBv1 can break legacy printers and Linux Samba systems. Learn more: https://attack.mitre.org/techniques/T1211/

Results: Lists systems with SMBv1 Status as DISABLED. If ENABLED, CB recommends deploying this IT Hygiene policy via GPO to disable SMBv1 and protect against attacker exploits.

Carbon Black recommends that you run this query daily

IT HYGIENE

Linux Memory Utilization

Description: Discover how applications are using memory.

Results: Lists system memory and system swap utilization statistics, such as available space and partition names.

Carbon Black recommends that you run this query as needed

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com