DELL Technologies

Data Sheet

Dell SafeBIOS

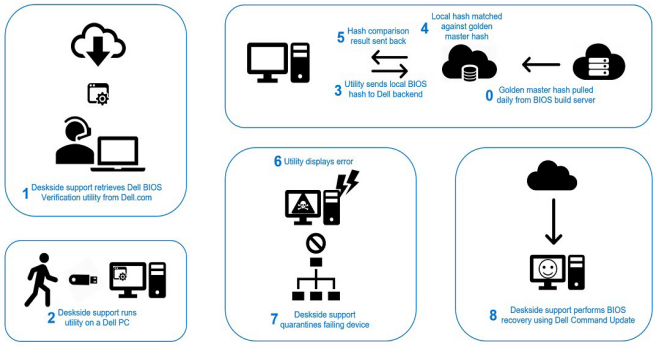
Built-in security on the industry's most secure commercial PCs[1]

Dell SafeBIOS mitigates the risk of BIOS and firmware tampering with integrated attack detection

Enhanced BIOS and Firmware Tamper Alert

Keeping organizations' data safe, whether it be their intellectual property or Personally Identifiable Information (PII), is foundational to data security.

Hackers have become increasingly sophisticated, and as commonplace threats are being thwarted more frequently, cyber criminals are looking for more advanced ways to gain this critical information. As organizations have hardened the attack surface in recent years with next-gen antivirus and endpoint detection and response solutions, adversaries are forced to look for softer targets.



Protecting the BIOS is critical to an organization's security posture

Popular endpoint security solutions primarily focus on the local operating system and the applications layered above it, leaving the lowest level of the PC stack, the BIOS, vulnerable to malicious attacks that can incapacitate your entire system. When malware owns the BIOS, it owns the PC and access into the network. BIOS attack is an extremely high impact compromise - attacking the root of trust for the PC and thus are very persistent. If an attacker gains access to the BIOS, they can compromise all of the device's endpoint security capabilities, as well as an organization's entire network. This type of attack is highly technical and when executed, very damaging. This gaping vulnerability has become an area of increasing concern as attackers look for new vectors of attack.

Dell SafeBIOS responds to this security paradigm shift

With the growing frequency of below-the-OS attacks, and new malware variants possessing the ability to reinstall themselves within the BIOS and firmware, organizations need a more sophisticated way to not only protect their systems, also confidently verify that their systems have not been compromised.

Dell integrates post-boot verification into its commercial PCs giving IT the assurance that employees' BIOS and firmware have not been altered. Rather than storing BIOS and firmware information on the hardware itself, which is susceptible to corruption, Dell SafeBIOS delivers an off-host BIOS and Intel Management Engine (ME) Firmware Verification capability. SafeBIOS uses a secure cloud environment to compare an individual BIOS and firmware image against the official measurements held in the cloud.

DELL Technologies

intel vPRO

Dell automates the early detection of BIOS Events and Indicators of Attack and high-risk configurations by bringing visibility to the BIOS configuration history. The continuous extraction and analysis of BIOS configurations and events will surface vulnerable endpoints and alert IT as the risk increases allowing them to take remediation.

Should the BIOS get corrupted or tampered with, Dell gives customers flexible reimage options so that the contaminated BIOS can be analyzed to understand the nature of the attack empowering customers to verify BIOS integrity using the off-host process without interrupting the boot process. SafeBIOS provides added visibility to BIOS changes along with extra assurances to keep threats at bay.

Additionally, should a BIOS get compromised, the image of the BIOS is captured automatically for analysis and remediation after going through the BIOS recovery process.

Maximize SafeBIOS Capabilities with the Dell Trusted Device Application

Among PC manufacturers, only Dell integrates device telemetry with industry-leading software to improve fleet-wide security.[1] This data is captured and made available through the Dell Trusted Device (DTD) Application. The DTD App is free, downloadable software that provides maximum BIOS protections within the Dell SafeBIOS product portfolio. The DTD App maximizes SafeBIOS capabilities by communicating endpoint telemetry between the device and a secure Dell cloud, providing unique below-the-OS insights into security "health." The data transmitted provides assurance that the BIOS is being measured. If any feature reports change, the IT administrator is notified of possible tampering.

The DTD App provides telemetry to enable several features under Dell SafeBIOS such as **Indicators of Attack, BIOS Verification** and **CVE Detection for BIOS** Intel **ME Firmware Verification,** and our **Security Score**, a feature that aggregates various indicators into one easy-to-read KPI.

The administrator can find notifications in the Windows Event Viewer, a log of application and system messages, including errors, information messages and warnings. They can also find this information in their endpoint management tool or SIEM, as Dell integrates device telemetry with industry-leading software to improve fleet-wide security. Our list of partner integrations includes third-party security software such as CrowdStrike Falcon, as well as endpoint managers such as Microsoft Intune and SIEMs such as Splunk. They can also view elements in Dell TechDirect.

Not only do these integrations improve threat detection and response with a brand-new set of device-level data, but they also help customers make the most of their software investments. Knowing how much our customers value the ability to view (e.g., security alerts) within their preferred environments, Dell continues to release updates to the DTD App, enabling more capabilities within the Intune environment. Now, Intune administrators can view additional data from BIOS Verification, Intel ME Firmware Verification and Secured Component Verification (or SCV, a Dell supply chain security offering that enables platform certificate verification), with added capabilities coming in future DTD releases. The integration of DTD telemetry with Intune supports extensible compliance and enables organizations to use this telemetry to maintain policies they choose to apply.

To learn more about the security of our commerical PCs, read the **Dell Trusted Device Below-the-OS White Paper.**

Dell SafeBIOS is part of the Dell Trusted Workspace endpoint security portfolio with solutions both above and below the OS for a true comprehensive approach, including:

- **SafeBIOS:** Gain visibility to hidden and lurking attacks with BIOS and Firmware tamper alert through Dell exclusive off-host BIOS and Firmware verification[1], BIOS Image Capture[1], CVE Detection[1], and BIOS Events and Indicators of Attack[1], all made possible with the Dell Trusted Device App.[2]
- **SafeID:** Only Dell secures end user credentials in a dedicated security chip, keeping them hidden from malware that looks for and steals credentials.[1]
- **SafeData:** Protect sensitive data on device to help meet compliance regulations, and secure information in the cloud giving end users the freedom to safely collaborate.[1]
- **SafeGuard and Response:** Prevent, detect, and respond to advanced malware and cyberattacks to stay productive and free from the disruption and churn an attack can cause.[1]
- **SafeSupply Chain:** Trust hardware is tamper-free on delivery with optional paid add-ons such as Secured Component Verification for extra supply chain assurance.

[1]Based on Dell internal analysis, September 2023. Applicable to PCs on Intel processors. Not all features available with all PCs. Additional purchase required for some features.
[2]The Dell Trusted Device App is available via download and can be found at dell.com/support.

Learn more about Dell solutions

Contact a Dell Technologies Expert

View more resources

Join the conversation

DELL Technologies