DELL Technologies

Solution Brief

What is the Dell Trusted Device App?

Key Benefits

Maximize SafeBIOS Capabilities

The DTD App maximizes SafeBIOS capabilities such as Indicators of Attack, Image Capture and Forensic Analysis, as well as a fleet-level view of your BIOS security.

Gain insights within leading IT environments

The DTD App works within top IT environments. Gain valuable security insights into the health of your fleet and create and enforce compliance policies from leading endpoint management environments. Insights and notifications can also be found in Windows Event Log or in TechDirect.

Enables Secured Component Verification*

The DTD App provides the device telemetry needed to power our supply chain security solution, Secured Component Verification (on Cloud). SCV assures that Dell devices and their components arrive from the factory tamper-free through the use of platform certificates that list a manifest of hardware components.

Overview

Dell is unique among PC OEMs in providing data from its built-in "below the OS" security capabilities, such as SafeBIOS. This data – or more accurately, telemetry – 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. DTD software 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 unexpectedly 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 (IoA):** early alert feature that scans for behavior-based threats
- **CVE Detection:** an intelligent, built-in monitoring feature that scans for publicly reported security flaws on a device and provides recommendations on how to fix them
- **BIOS and Firmware Verification:** off-host features for verifying the integrity of highly privileged BIOS and Management Engine (ME) Firmware by comparing ME firmware found on the platform with previously measured hashes (stored off-host)
- **Security Score:** aggregates various indicators into one easy-to-read metric for device health

View DTD Insights within Top IT Environments

In fact, only Dell integrates device telemetry with industry-leading software to improve fleet-wide security.**

One of the benefits of the DTD App is that it is designed to work within top IT environments. Whether users work in endpoint management tools such as Microsoft Intune or Carbon Black Cloud, SIEMs such as Splunk, or even via Windows Event Viewer, admins will be able to gain key insights into a fleet's BIOS health – all without leaving their favorite third party tools.

Admins can see notifications within the Windows Event Viewer, a log of application and system messages, including errors, information messages and warnings. Or they can find this information in their endpoint management tool or SIEM, as device telemetry obtained via the DTD App can be viewed.

Within many of these environments, IT admins can view the BIOS health of their fleet of devices and create and enforce compliance rules and policies through Dell-created and unique scripts. Admins can view additional data from BIOS Verification, Intel ME Firmware Verification, and our platform certificate offering, Secured Component Verification (on Cloud)*.

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 security alerts within their preferred environments, Dell continues to release new DTD updates that enable greater capabilities within these endpoint management environments.

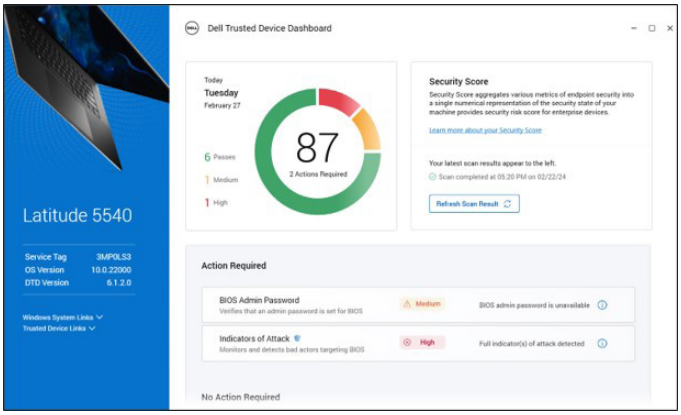
View BIOS Results in TechDirect or the Dell Trusted Device Local Console

In addition to top endpoint management environments, the DTD App also works within Dell tools such as TechDirect and our recent new feature, the Dell Trusted Device local console.

With TechDirect, optimize your IT support and streamline your PC fleet management through a modern, intelligent end-to-end experience. From a centralized dashboard, TechDirect offers a simplified and efficient approach to handle device life cycles, providing customizable BIOS updates, Secured Component Verification (SCV) results, a dashboard security score of your fleet, data-driven insights, proactive alerts, and 24/7 support. Elevate your IT operations and effortlessly manage your entire fleet with actionable insights at your fingertips.

Our new Dell Trusted Device local console provides similar dashboard views of their BIOS health. With this feature, end users can gain visibility into the underlying health of their device for possible BIOS security issues.

The Dell Trusted Device local console provides dashboard view of the device's BIOS health.



Free, Downloadable App with Frequent Updates

The DTD App comes pre-installed on all Dell commercial devices that utilize the standard image. Should your organization use its own corporate image, the app can still be downloaded by visiting the Dell Support site and downloading the app.*** For fleet installation, we recommend using the SupportAssist for Business App for efficient DTD deployments.

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 *Secured Component Verification (on Cloud) is an additional service that offers increased supply chain security to those who require it using platform certificates. The DTD App enables the SCV (on Cloud) solution and is required for it to function.

****For organizations that wipe the standard image off devices and use their own corporate image, the DTD App must be downloaded and installed.*

Learn more about Dell solutions

Contact a Dell Technologies Expert

View more resources

Join the conversation

DELL Technologies