DELL Technologies

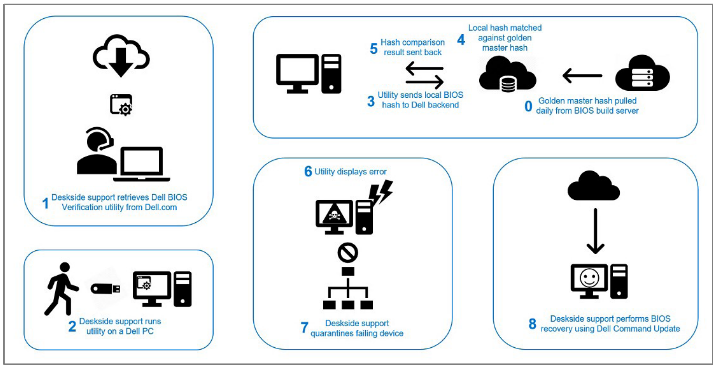
Dell SafeBIOS

BUILT-IN SECURITY ON THE INDUSTRY'S MOST SECURE COMMERCIAL PCs

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

Enhanced BIOS and Firmware Tamper Alert

Keeping organization's data safe, whether it be their intellectual property or customer's 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. With increasingly sophisticated endpoint security solutions like NextGen antivirus and managed endpoint detection and response, the attack vectors are narrowing, and adversaries are forced to look for alternate invasion points.


1 Deskside support retrieves Dell BIOS Verification utility from Dell.com

2 Deskside support runs utility on a Dell PC

0 Golden master hash pulled daily from BIOS build server

3 Utility sends local BIOS hash to Dell backend

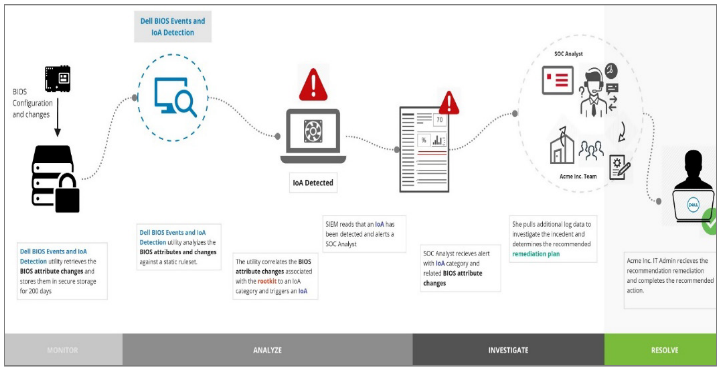
4 Local hash matched against golden master hash

5 Hash comparison result sent back

6 Utility displays error

7 Deskside support quarantines failing device

8 Deskside support performs BIOS recovery using Dell Command Update



Dell BIOS Events and IoA Detection utility retrieves the BIOS attribute changes and stores them in secure storage for 200 days

Dell BIOS Events and IoA Detection utility analyzes the BIOS attributes and changes against a static ruleset.

The utility correlates the BIOS attribute changes associated with the rootkit to an IoA category and triggers an IoA

SIEM reads that an IoA has been detected and alerts a SOC Analyst

SOC Analyst recieves alert with IoA category and related BIOS attribute changes

She pulls additional log data to investigate the incedent and determines the recommended remediation plan

Acme Inc. IT Admin recieves the recommendation remediation and completes the recommended action.

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 BIOS and Firmware-specific 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, but 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 ME 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 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.

Partner Integrations

These combined capabilities provide the ability to identify and remediate potential risks more quickly. The standalone capability is currently available from Dell Support.

VMware Workspace ONE provides IT management with new visibility of BIOS status for unified endpoint management. Integration with VMware Workspace ONE enables IT to set up automated workflows to push over-the-air updates and restore devices to compliance.

The combined power of VMware Carbon Black Audit and Remediation and Dell SafeBIOS provides state of the art security both above and below the OS and enables telemetry from the off-host BIOS verification status on the Dell Commercial PC offering. The integrated solution allows security and IT teams to automate reporting of the verification status so they can take action to remediate compromises resulting from BIOS tampering.

Splunk Integration allows IT management and security analysts gain visibility of BIOS verification status and tamper events through Splunk dashboards, enabling them to take action and maintain device compliance. Integration with Microsoft Endpoint Manager provides IT management with visibility of critical BIOS level telemetry generated by Dell Trusted Device enabling them to remediate threats and compromises. These partnerships reinforce Dell as Industry’s Most Secure Commercial PC provider.

Dell SafeBIOS is part of the larger Dell Trusted Devices endpoint security portfolio with solutions that support the endpoint both above and below the OS for a true comprehensive approach to data protection, 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 and BIOS Events and IoA.
- SafeID: Only Dell secures end user credentials in a dedicated security chip, keeping them hidden from malware that looks for and steals credentials.
- SafeScreen: End users can work anywhere while keeping private information private with an integrated digital privacy screen.
- 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.
- SafeGuard and Response (powered by VMware Carbon Black and Secureworks): Prevent, detect, and respond to advanced malware and cyber-attacks to stay productive and free from the disruption and churn an attack can cause.

Contact your dedicated Dell Endpoint Security Specialist today at endpointsecurity@dell.com to discuss how we can help improve your security posture.

[1] Claim based on internal analysis.

DELL Technologies