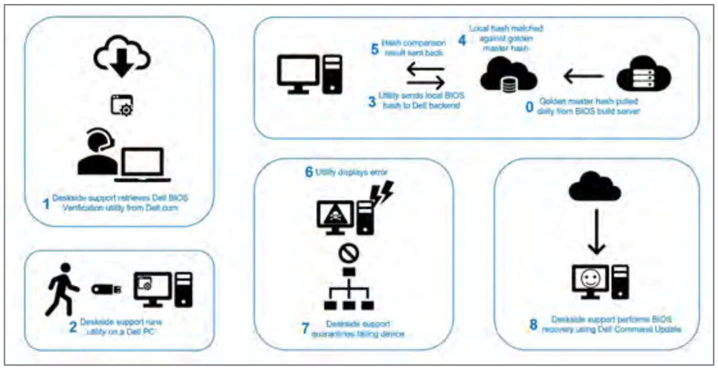
Dell SafeBIOS

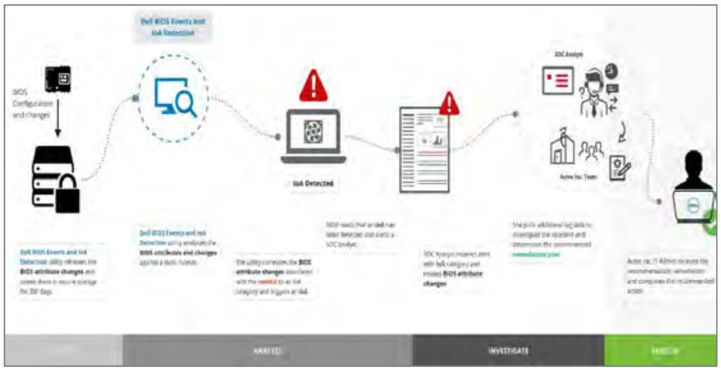
Built-in Security on Trusted Devices

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

Enhanced BIOS 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 next-gen 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
3 Utility sends local BIOS hash to Dell backend
4 Local hash matched against golden master hash
5 Hash comparison result sent back
0 Golden master hash pulled daily from BIOS build server
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
BIOS Configuration and changes
IoA Detected
SOC Analyst
Acme Inc. Team
ANALYZE
INVESTIGATE

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 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 a 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-specific attacks, and new malware variants possessing the ability to reinstall themselves within the BIOS, organization’s 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 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. SafeBIOS uses a secure cloud environment to compare an individual BIOS image against the official measurements held in the BIOS lab.

Additionally, 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 more quickly identify and remediate potential risks. The standalone capability is currently available from Dell Support.

The ability to tie measurements into Secureworks threat intelligence, Carbon Black and VMware Workspace ONE device health provides an additional level of monitoring and visibility.

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.

Customers can leverage Secureworks threat intelligence to not only identify compromises but provide analysis and remediation.

Dell SafeID is part of the larger Dell Trusted Security portfolio including:

- **Trusted Devices**: The foundation to a modern workforce environment with invisible and seamless protection to ensure smarter, faster experiences. End users stay productive and IT stays confident with modern security solutions.
  - SafeBIOS: Gain visibility to hidden and lurking attacks with BIOS tamper alert through Dell exclusive off-host BIOS verification[1], BIOS Image Capture and Indicators of Attack.
  - SafeID: Only Dell secures end user credentials in a dedicated security chip, keeping them hidden from malware that looks for and steals credentials.[1]
  - 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.
- **Trusted Data**: Dell constantly monitors and protects the endpoint ecosystem with Dell SafeGuard and Response, while giving IT confidence that data is secure even while end users collaborate freely with Dell SafeData.

Establish a mature security framework:

Proactively managing your organization’s cybersecurity maturity is essential for defending against targeted cyber-attacks. Establishing a set of mature, robust security controls and understanding that prevention alone is not enough, can help you prepare proactively and enable your organization to successfully deal with the next security event.

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