

Client Solutions: Dell Trusted Device Below the OS White Paper



A deep dive into the foundational, BIOS and hardware level security of Dell Trusted Devices, the world's most secure commercial AI PCs*

March 2026



© 2026 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

*Based on Dell internal analysis, October 2025 (Intel) and March 2026 (AMD). Applicable to PCs on Intel and AMD processors. Not all features available with all PCs. Additional purchase required for some features. Intel-based PCs validated by [Principled Technologies](#), July 2025.

Table of Contents

Preface 6

Introduction 7

The Key Elements of Dell PC Security..... 9

 The Role of BIOS in Security 9

 Secure Design Processes and SDL 10

 Supply Chain Security 11

 Built-In, “Below-the-OS” Security 11

 Dell Trusted Device Application (DTD App) 12

 Industry Collaborations and the Importance of Built-in, Below-the-OS Security 13

 Quantum-Readiness in Device Security 14

Understanding Dell Cybersecurity Using the NIST Framework 15

Identify 17

 Device Identity 17

 Service & Asset Management Tags 17

 Service Tag 17

 Asset Tag..... 17

 Platform Certificates for Machine Identity & Supply Chain Assurance (Secured Component Verification) 18

 HBOM and SBOM 18

 CISA HBOM 19

 TCG Platform Attribute Certificate 19

 Credential Protection: Dell SafeID 19

 SafeID: ControlVault..... 20

 SafeID: TPM and Microsoft Pluton 21

Protect..... 21

 Protecting the PC Boot Process..... 21

 Securing the Boot Chain 22

 The “Root of Trust” 23

 TCG and the Root of Trust 23

 UEFI Secure Boot..... 24

UEFI Secure Boot Expert Key Management	24
Signed Firmware Update	25
NIST SP 800-147 Support.....	25
System Management Mode (SMM) For x86 Systems	25
Trusted Firmware for ARM Systems – Secure Partition Manager (SPM).....	27
BIOS Patch Management	28
BIOS Downgrade Protection.....	29
Embedded Controller: Signed Firmware.....	29
Protecting BIOS Configuration	29
Configuration Side-Channels	31
Best Practices for Secure Configuration	33
Protecting BIOS at Runtime.....	33
Intel Runtime BIOS Resilience	33
AMD SMM Supervisor.....	34
Detect	34
Dell Physical Security and Protection - Overview.....	35
Dell Physical Security Detection and Protection Features	35
Ability to Block Boot after Chassis Intrusion.....	35
TPM integration for Chassis Intrusion events.....	36
Battery Removal Detection	36
SPI Flash Anti-Tamper features	36
Dell Software-Based Detection Capabilities.....	36
Dell Off-Host BIOS and Firmware Verification.....	36
How Off-Host Verification Is Performed	37
Indicators of Attack.....	38
BIOS Image Capture	39
Common Vulnerabilities and Exposures (CVE) Detection and Remediation	40
Security Risk Protection Score	41
Dell Supply Chain-Based Detection Capabilities.....	42
Secured Component Verification (SCV)	42
Additional Dell Device-Based Detection Capabilities	44

TCG Measured Boot	44
Intel® vPro Additions to Built-In Security	44
Code, Configuration, and the TPM Event Log.....	44
NIST 800-155 Measurements.....	45
Advanced: NIST 800-155 Measurements Extraction, Conversion, and Comparison	46
Dell Integrations with Hardware Providers	47
Intel Boot Guard.....	47
Intel Management Engine (ME) Firmware Verification.....	47
Intel vPro Integration for Out of Band Management (OOBM)	47
Microsoft Intune Integration.....	47
Hardware-Assisted Security Dell, Intel and CrowdStrike	48
Below-the-OS Integration with CrowdStrike Dell on AMD.....	48
Below-the-OS Integration with Absolute Dell on Intel, Dell on AMD.....	49
Other Integrations.....	49
Respond and Recover	50
Embedded Controller (EC) Recovery.....	50
BIOS Recovery	50
BIOS Recovery Image Update Flow.....	51
Auto Recovery Flow.....	52
Customer Flexibility: Manual Recovery.....	52
Confirming BIOS Integrity	52
Dell Data Sanitization.....	52
OS Recovery: Dell BIOSConnect.....	53
Additional Dell Security Features and Capabilities	53
Below-the-OS Threat Modeling.....	53
Protected Signing Infrastructure.....	54
The Future of Security.....	55
References.....	56
Dell and Partner References.....	56
Industry Organizations.....	56
Standards and Guidelines.....	57
Quoted Stats.....	57

Disclaimer 57

Preface

Since the original release of this paper, which focused on Dell PCs with Intel x86 processors, Dell is now offering PCs with processors from AMD, Qualcomm and NVIDIA.

Our goal is to provide a high level of security for all commercial PCs. However, there are some differences in how this is implemented from platform to platform. When there is a difference, it will be noted in the text.

The paper also reflects revisions for:

- Naming conventions – Dell introduced a restructure of its PC naming, and this paper has been updated for this.
- Introductions and refinements in current solutions, including Secured Component Verification (SCV) and quantum-upgraded features.
- New strategic software partnerships and deepening of existing partnerships (selected software solutions leverage Dell-unique PC telemetry), improving prevention, detection, response and recovery/remediation.

Introduction

Computer security is a multi-billion-dollar business with thousands of companies competing for organizations' attention and enterprise dollars, and with good reason: it can provide a healthy payday for the attacker. The cost of cybercrime worldwide continues to grow at a brisk rate – [from \\$5.49 trillion USD in 2021 to a projected \\$10.5 to 12 trillion USD in 2025](#). These figures reflect the impact of increasingly sophisticated attacks, including ransomware. Governments are also witnessing growing nation-state level cyberattacks, as countries do battle using these weapons of warfare. The increasing adoption of zero trust methodologies and architectures reinforces that security remains a fundamental aspect of ensuring that an organization can secure its key assets and prevent the damage that even a simple cyberattack can wreak upon its operations.

One of the most critical and fundamental tenets in computer security is transparency. Though highly effective, security features deeply embedded within a client are not always visible. The intent of this publication is to provide transparency into the Dell device security features and technology implementations as provided and enforced by the code responsible for device boot and other fundamental device functions, which we refer to as our BIOS (Basic Input/Output System).

Dell Technologies has created [Dell Trusted Workspace](#), an innovative portfolio of technologies and solutions spanning both hardware and software that is dedicated to helping organizations effectively secure their enterprises while providing visibility to threats. One of the areas where Dell has substantially invested over the last decade is in the security of the endpoint itself, in this case the “client” device (desktops, workstations, and notebooks). The collection of innovative ‘built-in’ security features native to Dell hardware strengthens the ability of Dell client devices to detect, respond to and mitigate stealthy attacks which operate below the purview of the operating system – or below the OS as it is often called. Dell takes this a few steps further. First, Dell offers security software through a partner ecosystem – including CrowdStrike, Absolute and Halcyon – to simplify procurement. When customers purchase a commercial PC, they can add these partners “on the box”. In addition, Dell works with these partners to develop security and manageability integrations (with, e.g. endpoint detection and response (EDR), extended detection and response (XDR), security information and event management (SIEM) and device management solutions, such as Microsoft Intune) to help organizations detect, investigate and respond to a threat with greater effectiveness.

Dell's leading commercial device security is offered on both Intel- and AMD-based devices. There are additional built-in security features from Intel® vPro, an option for Intel-equipped PCs. Though mention will be made, for more in-depth information there is a separate paper dedicated to those features that may be [downloaded here](#). Learn more about the security of Dell and AMD with this [infographic](#).

Even with the latest news about the increase in cyberattacks, there are still organizations that believe that security equals encryption plus antivirus, and that software is all it takes to be secure. They may recognize and appreciate Dell's significant investment in endpoint security but question the need. Why don't firewalls, IDS/IPS, SIEMs, NGAV, EDR and all the various alphabet soup of enterprise-level security tools already cover everything?

Well, those tools may be good at what they do. But they don't do everything. Dell believes that overall infrastructure security not only depends on these tools but also on the built-in security of each endpoint: that each endpoint should serve both as a point of security defense and as a security “sensor”, with both approaches supporting the overall zero-trust posture of the organization. From this perspective, the endpoints,

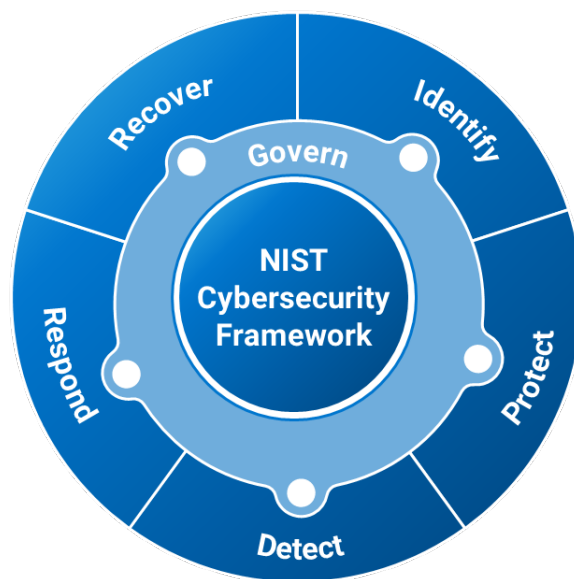
and subsequently each individual device, collectively become the foundation of security for the entire enterprise. Further, as attackers develop more stealthy threats which work at the hardware level, existing security software simply isn't enough to detect and respond to them. Hardware-generated telemetry such as that provided by the Dell Trusted Device Application (DTD App) provides a valuable source of information that can be used to offset these increasing threat vectors – in essence, built-in security. This domain can only be implemented and supported by the OEM, and Dell continues to advance the abilities of its products to protect, detect, respond, and recover from cyberattacks.

This paper was written to provide a thorough introduction to the Dell device BIOS security features and hardening. The BIOS remains an extremely important component in a modern PC, and some of the more foundational (and critical) security hardening aspects of the device start with and depend on the BIOS. This document will unwrap the terminology and lexicon that has tightly attached itself to this area of technology and explain the individual features and components of the BIOS that help to secure enterprise infrastructure from the device up to the cloud.

The audience for this document includes security operation center (SoC) analysts, IT admins and decision makers (ITDMs), IT support personnel, compliance and risk/governance teams, security researchers and analysts, and anyone else interested in learning more about the built-in security offered by the Dell devices via security and hardening of the underlying BIOS and firmware.

Contextually this document is broken into sections that map to specific outcomes described in the [NIST Cybersecurity Framework \(CSF\)](#): Identify, Protect, Detect, Respond and Recover. This should help put each feature included in Dell devices into the perspective of the overall goal of helping to secure each organization's enterprise.

- **Identify:** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. Within the Dell security schema, this refers to tools to help customers categorize these classifications, including asset management and those secure design principles which proactively contribute to security (e.g., Dell Service Tag, Dell SafeID, Threat Modeling).
- **Protect:** Develop and implement appropriate safeguards to ensure delivery of critical services. These include defensive technologies to harden non-volatile storage and the boot process (e.g., Signed Firmware Update, BIOS Passwords).
- **Detect:** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. This includes the ability to convey status when unauthorized changes occur (e.g., BIOS verification, Intel® Boot Guard).
- **Respond:** Develop and implement appropriate activities to respond to a detected cybersecurity incident. Action is taken by the organization using tools and data (telemetry) provided by Dell capabilities described in this paper.



- **Recover:** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. This includes advanced mitigations to quickly remediate issues (e.g., BIOS Recovery, Dell Data Wipe).

Govern was introduced in the 2024 version of the CSF and intended to underlie each of these activities, which are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. From the perspective of an OEM such as Dell, Govern concerns work to be performed by the customer organization to understand organizational context; establish cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and provide for the oversight of cybersecurity strategy. It is not covered in the scope of this document, although it is essential for any organization seeking to implement and manage a robust cybersecurity strategy.

This document concludes with a brief section on our commitment to the ongoing Dell investments helping to shape the future of security. This document is not the end of the conversation about Dell device security; hopefully it's the continuation of a long and bi-directional discourse beneficial to the industry overall.

The Key Elements of Dell PC Security

The Role of BIOS in Security

The "BIOS" in a modern PC remains one of the most misunderstood components of the firmware and software stack. The mere mention of "BIOS" to anyone that's been in the industry for more than a decade evokes memories of resetting the CMOS battery or toggling jumpers on the motherboard to make configuration changes. Many still refer to the BIOS configuration menu, or "BIOS Setup" as the BIOS, but there is so much more to it than that!

For the purposes of this document, the BIOS refers to the pre-boot firmware that the main processor executes at the beginning of every boot and any code that remains resident at runtime that was deployed by the pre-boot firmware. The role of this pre-boot firmware is to initialize memory, configure chipset and discrete devices on the motherboard, provide PC OEM unique features, and to enforce any customer specific configuration settings managed by BIOS Setup. BIOS is largely OS agnostic and persists across OS installs, this means that most of the built-in features and capabilities described in this document work whether the system has Windows, Linux, or even without an operating system at all.

Additionally, more recently the term "UEFI" has become much more prominent when discussing pre-boot firmware on PCs. While architecturally the UEFI ecosystem has had a net positive effect on compatibility and ease of deployment, the term itself has managed to confuse the issue. UEFI, or the Unified Extensible Firmware Interface, is an industry specification that defines the various optional interfaces and protocols used by pre-boot firmware to configure a PC (in most cases). Many experts pedantically correct others that "UEFI has replaced BIOS!" but that's only partly true. The truth is, PC OEMs and most subject matter experts in the field still use the term "BIOS" to refer to any pre-boot firmware designed to bootstrap a modern PC, regardless of whether it is UEFI-based, Linux-based, or completely custom.

One of the other net positive effects of UEFI has been the opportunity to integrate features and device drivers directly into the BIOS development flow that are compatible with the UEFI specification. An excellent example

of this in practice is the [UEFI Tianocore](#) project on GitHub. Tianocore is the current reference implementation for UEFI and is completely open source. Dell and other OEMs use some of this project code as the foundation or “core” BIOS and add differentiated features on top of the open-source core. Another benefit of this open architecture is that UEFI supports multiple instruction sets such as x86-based and ARM-based PCs.

Secure Design Processes and SDL

Dell’s Secure Development Lifecycle (SDL) shown in Figure 1 integrates standards and best practices from a variety of industry consortiums and standards bodies. A primary consideration in SDL is to blend data sources from both internally discovered and externally reported issues, allowing Dell to focus on the most prevalent issues in the Dell device technology space. A second major consideration is industry practices. Dell participates in many industry standards organizations such as SAFECode, TCG and IEEE Center for Secure Design to ensure alignment to industry practices. Lastly, Dell’s Secure Development Lifecycle is aligned with the principles outlined in [ISO/IEC 27034 ‘Information technology, Security techniques, Application security’](#). These practices are tightly integrated into the design and manufacture of Dell products.

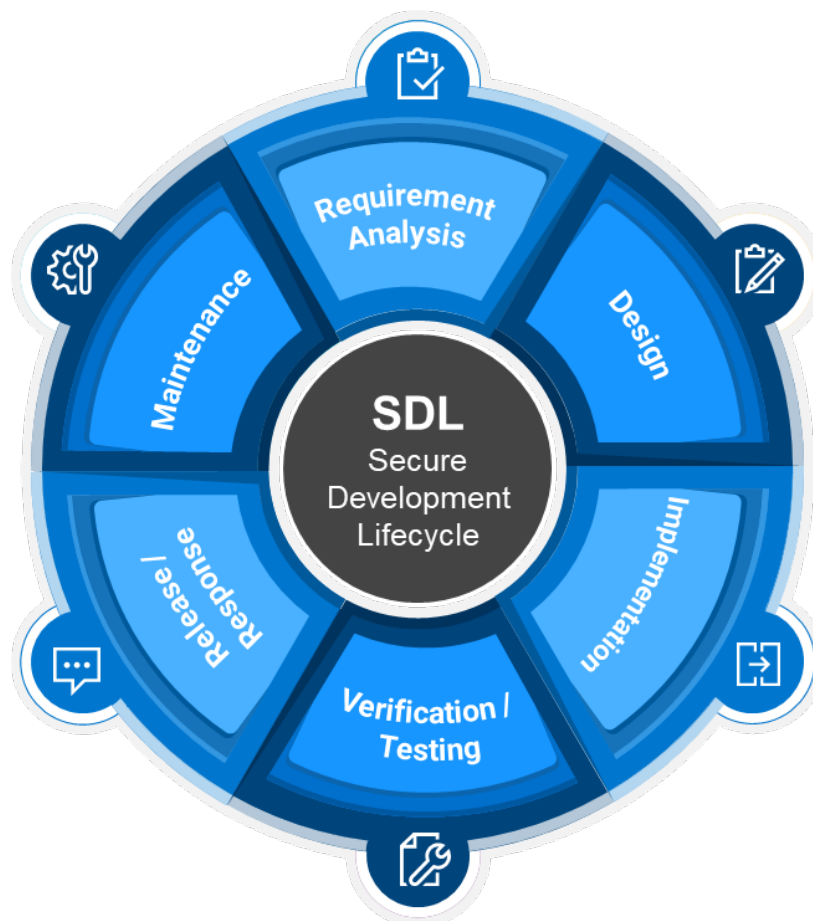


Figure 1: Dell Technologies Secure Development Lifecycle

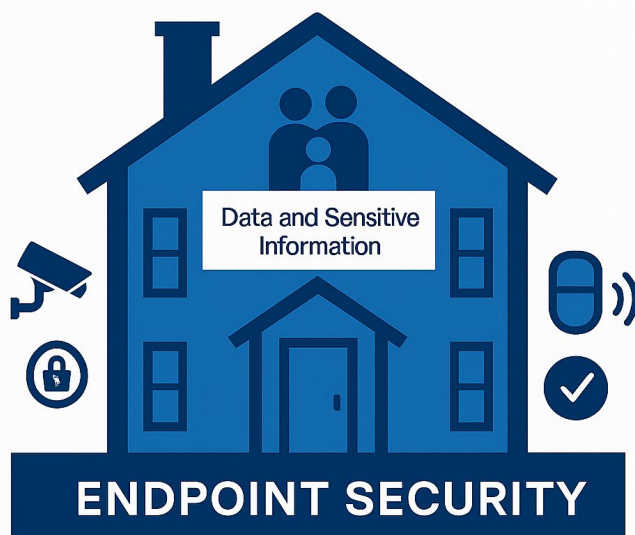
Supply Chain Security

Supply chain assurance and the broader supply chain security concept are complex topics that demand their own volume. Fortunately, the Dell device supply chain falls under the scope of a previously published comprehensive paper on this subject. The latest version of Dell Supply Chain Assurance is available for download [here](#).

Dell has implemented procedures across our commercial desktops, and laptops in accordance with the guidance and recommendations outlined in [NIST SP 800-147](#), Basic Input/Output System (BIOS) Protection Guidelines. Dell's protected BIOS and signed update mechanism help prevent unauthorized modification of the platform firmware and reduce the risk of pre-boot malware or unwanted functionality. From the Dell perspective, "supply chain security" covers more than suppliers, manufacturing sites, and logistics. Dell design, development, validation, and sustaining phases all equate to some parts of the supply chain from the customer perspective. This means that the investments in the features covered in this document can help assist and augment traditional supply chain security. For example, the BIOS verification check is part of the manufacturing process of every Intel and AMD-based commercial PC that Dell produces.

Built-In, "Below-the-OS" Security

The security of endpoints collectively forms the foundation of the entire enterprise. Consider the analogy of a house to represent endpoint security. An organization's most valuable assets – data and sensitive information – are like the family inside this house. Houses, however, are not intrinsically secure, so homeowners must build or buy additional protection like deadbolts, security cameras, and motion sensors to help secure them. Jumping back to the enterprise: there are plenty of players in the security ecosystem which offer these additional protections, but what's the remaining gap in this scenario? The foundation. Any dwelling must be built on a stable foundation to protect the homeowner's investment in security from being subverted from below. That's where Dell commercial client protections and Dell BIOS security comes in.



Caption: An organization's endpoint security is a lot like protecting a house. Both contain valuable assets, and neither is inherently secure on its own. Instead of relying on deadbolts and security cameras, organizations depend on Dell's commercial client security features and built-in BIOS protections to safeguard their most valuable assets – their data and sensitive information.

Dell refers to this stable foundation as “built-In, below-the-OS” security. Based on this analogy, it’s clear that the endpoints and this below-the-OS foundation are valuable targets for adversaries attempting to get a foothold into an enterprise. This critical role in our customers’ security is why Dell has invested in “below-the-OS” security for over a decade and why it’s important that we publicly document SafeBIOS and associated features, along with some of the rationale behind their development.

Dell Trusted Device Application (DTD App)

Among PC OEMs, only Dell integrates device telemetry with industry-leading software to improve fleet-wide security.* Designed for use on Windows PCs, telemetry data is captured and made available through the DTD App. The DTD App is free, downloadable software that provides maximum BIOS protections within the Dell SafeBIOS product portfolio. The DTD App can be downloaded in an automated method for fleet management using [Dell Client Device Manager \(DCDM\)](#). It is also available to download from [Dell.com](#). 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 unexpectedly change, the IT administrator is notified of possible tampering.

The DTD App provides telemetry to enable several features such as Indicators of Attack (IoA) and BIOS verification, which detect tampering of BIOS firmware and BIOS configuration.

- For Intel-equipped PCs using vPro, it also provides Intel Management Engine (ME) Firmware Verification, which verifies the integrity of highly privileged ME firmware by comparing ME firmware found on the platform with previously measured hashes (stored off-host), and our Security Score, a feature that aggregates various indicators into one easy-to-read KPI.
- For AMD-equipped PCs, it provides off-host verification of the AMD Security Processor (ASP) firmware to verify the integrity of this highly privileged firmware using the same methodology, and a Security Score is also determined and provided.

The administrator can find notifications in the Windows Event Viewer, a log of application and system messages, including errors, information messages and warnings. It’s a useful tool for troubleshooting problems and analyzing potential threats as well as attacks that may be ongoing. 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 extensive partner integrations includes third-party security software such as CrowdStrike Falcon and Absolute, as well as endpoint managers such as Microsoft Intune, and SIEMs such as Splunk. They can also view elements in Dell TechDirect, and as of the DTD 6.1 release, local users can view this information via a DTD local console.

Not only do these integrations improve threat detection and response with a brand-new set of device-level data: they also help customers make the most of their software investments by extending security-related PC data from below the OS into tools which increase visibility and support action. Knowing how much our customers value the ability to view notifications such as security alerts within their preferred environments, Dell’s approach provides not just control and defense – it provides visibility to attack activities, and the DTD App is key to this.

Dell continues to release updates to the DTD App, enabling greater integration capabilities. For example, recent releases expanded key feature integrations in the Intune environment for both visibility and effective management for security. Now, Intune administrators can view additional data from BIOS verification, Intel ME Firmware Verification, AMD ASP verification (included in the BIOS verification report) and Secured Component Verification (or SCV, a Dell component integrity check), with added capabilities coming in future DTD releases. Dell has worked with selected software providers to further integrate Dell built-in security with their applications, providing an even higher degree of defense, control and visibility that adds to the existing 'security in layers, security in depth'. These are discussed in detail within the "Detect" section of this paper. The integration of DTD telemetry with Intune supports extensible compliance and enables organizations to use this telemetry to maintain policies they choose to apply.

* Based on Dell internal analysis, October 2025 (Intel) and March 2026 (AMD). Applicable to PCs on Intel and AMD processors. Not all features available with all PCs. Additional purchase required for some features. Intel-based PCs validated by [Principled Technologies](#), July 2025.

Industry Collaborations and the Importance of Built-in, Below-the-OS Security

Industry standards bodies, policy makers, and security researchers have recently started to focus on built-in, below-the-OS security as well. Dell has been very involved in contributing to and building devices that adhere to, recommendations from NIST around firmware security and resilience. [NIST Special Publication SP 800-193](#) outlines overall resilience guidelines for device firmware (including BIOS) and has been helpful in confirming the value in Dell's below-the-OS security investments and direction.

NIST Special Publications that are relevant in this space include [NIST SP 800-147](#), which defines guidelines for protecting the BIOS and specifies that only signed and authorized BIOS should run on the device (see the Dell Client Signed Firmware Update whitepaper [here](#)). [NIST SP 800-88](#) provides direction for data sanitization on hard drives and solid-state drives.

Development of standards and guidelines also involves broader industry input from OEMs involved in the field. Dell is active in multiple industry-wide groups to collaborate with other leading vendors in defining, evolving, and sharing best practices on product security, and in further enhancing the cause of secure development. Examples of industry collaboration include:

- Dell co-founded and currently chairs the Board of Directors of The Software Assurance Forum for Excellence in Code ([SAFECode](#)). Board members include representatives from Microsoft, Adobe, SAP, Intel®, Siemens, CA and Symantec. SAFECode members share and publish software assurance practices and training.
- Dell is an active participant in and long-time member of the Trusted Computing Group ([TCG](#)), a not-for-profit organization formed to develop, define, and promote open, vendor-neutral, global industry specifications and standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms. TCG's core technologies include specifications and standards for the Trusted Platform Module (TPM – a part of Dell SafeID), Trusted Network Communications (TNC) and network security and self-encrypting drives.
- Dell is an active member of the Forum of Incident Response and Security Teams ([FIRST](#)). FIRST is a premier organization and a recognized global leader in incident and vulnerability response.

- Dell is an active participant in The Open Group Trusted Technology Forum ([OTTF](#)). OTTF leads the development of a global supply chain integrity program and framework.
- Dell employees were founding members of the [IEEE Center for Secure Design](#), which was launched under the IEEE cyber security initiative to help software architects understand and address prevalent security design flaws.

It's clear that industry and customer interest for built-in, "Below-the-OS" security (BIOS/firmware security) has risen in the last few years. This awareness is incredibly valuable because it allows Dell to continue to improve these areas year over year and help protect Dell device customers from the most sophisticated adversaries.

Quantum-Readiness in Device Security

Quantum computing introduces significant implications for modern cryptographic systems, particularly those used to protect data confidentiality, system integrity, and device authentication. Most widely deployed public key algorithms—such as RSA, Diffie Hellman, and ECC—are mathematically vulnerable to quantum attacks. Once scalable quantum systems become available, these algorithms will be susceptible to rapid compromise, undermining the trust model that underpins contemporary device and data security.

The associated risk is already operational. Adversaries are conducting *harvest now, decrypt later* (HNDL) operations, in which encrypted data is collected today with the expectation that it can be decrypted once quantum-capable systems mature. This creates long-term exposure for organizations whose sensitive data—intellectual property, operational telemetry, strategic communications, and firmware level configurations—may retain value over extended periods.

Preparing for this threat requires updates at foundational layers of the device security stack. Platform firmware, including the BIOS/UEFI environment, plays a critical role in establishing trust through mechanisms such as secure boot, measured boot, and hardware-anchored roots of trust. These components must adopt *crypto agility*, enabling rapid transition to new cryptographic primitives, and integrate post-quantum cryptographic (PQC) algorithms once standardized. PQC provides quantum-resistant key exchange and signature mechanisms designed to withstand both classical and quantum adversaries.

To support this shift, vendors are beginning to implement firmware-level capabilities that align with emerging PQC standards and enable organizations to migrate away from vulnerable legacy algorithms. Early adoption of crypto-agile BIOS architectures helps ensure that endpoint platforms can maintain verifiable integrity and comply with evolving security requirements as quantum-safe standards mature.

Quantum-resilient device security is no longer a long-term planning exercise. Given ongoing HNDL activity and the multi-year lifecycle of hardware platforms, integrating PQC-ready capabilities into today's systems is essential for mitigating future compromise and preserving the durability of cryptographic protections.

Understanding Dell Cybersecurity Using the NIST Framework

Cybersecurity capabilities can be categorized according to the five functions of the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover. These provide a shared understanding and methodology for classifying technologies and identifying gaps in an organization's cyber security architecture. In the sections which follow, we'll provide details of those features and below-the-OS security technologies that align with these functions and explain how they work and why they are important. There are other frameworks which can be used – Dell has selected the NIST framework for its simplicity and its widespread acceptance within the cybersecurity community. More information about the NIST Cybersecurity Framework can be found here: <https://www.nist.gov/cyberframework>.

The following sections dive into the security capabilities of Dell commercial PCs based upon the NIST framework. The table below maps Dell Trusted Workspace security to NIST pillars of Prevent, Detect and Respond/Recover, noting capabilities that align with the industry baseline, as well as security that is found only on Dell commercial PCs. The items that are starred (*) indicate key features that help make Dell the most secure commercial PCs.

	PREVENT	DETECT	RESPOND / RECOVER
Dell-Unique	Dell BIOS •	Discrete TPM ••	BIOS Image Capture* ••••
	Embedded Controller (EC) Root of Trust •	BIOS Verification* ••••	Third-Party Software Integration: SIEM (Splunk) ••••
	SPI Flash Anti-Tamper Features •	Indicators of Attack* ••••	Third-Party Software Integration: XDR (CrowdStrike Falcon)* ••••
	ControlVault* ••	System on Chip (SoC) Firmware Verification* ••••	Third-Party Software Integration: Endpoint Resilience (Absolute)* ••••
		CVE Detection for BIOS and Firmware* ••••	CVE Remediation for BIOS and Firmware* ••••
		Secured Component Verification •••	Dell BIOS Recovery •
		Security Score ••••	
		Embedded Controller (EC)-based Chassis Intrusion •	
Industry Baseline	Fused Root of Trust •	Runtime BIOS Resilience •	Windows OS Recovery
	UEFI Secure Boot •	TCG Measured Boot •	
	Cryptographically Verified Boot •	Downgrade Protection •	
	System on Chip (SoC) Hardware Flash Protections •	Chassis Intrusion •	
	BIOS Passwords •		
	Authenticated Updates •		
	BIOS Public Keys •		
	Certificate-Based BIOS Configuration •		
	Out of Band Management •		

Color coding: SafeBIOS = blue•, SafeID = green••, SafeSupply Chain = orange•••, Dell Trusted Device = purple••••

Identify

From the NIST Framework: “Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.”

The Dell built-in security features map directly to the Protect, Detect, and Recover/Respond functions of the NIST Cybersecurity Framework. The Identify function maps closely as well but the interaction is a bit more complex. For most enterprises, the Cybersecurity Framework is an effective tool for assessing security risk in their environments, where identifying assets and risk is a broad but valuable exercise. For Dell client devices, the Identify function has four separate and important roles:

- Includes features designed to help identify and asset-manage Dell devices within a customer infrastructure.
- Provides platform certificate-based machine identity which enables device health through proof of authenticity and supply chain assurance.
- Supports human identity secured via dedicated NIST certified biometrics and certificate-based authentication processing and storage SoC.
- Addresses processes and tools used by Dell to Identify customer security risks and threat models of the application and deployment of these devices.

Device Identity

Service & Asset Management Tags

The Dell BIOS supports two independent persistent identifiers (or “tags”) to allow customers to discover and manage their devices in their infrastructure.

Service Tag

The Service Tag is programmed into the BIOS NVRAM (non-volatile random-access memory) during the manufacturing process and is locked in place for the life of the device. This allows the customer and Dell to identify the device for overall asset management in the customer enterprise and enables Dell to confirm the device information for service and warranty support. The BIOS is responsible for displaying the Service Tag in BIOS Setup and in management interfaces such as SMBIOS. The Service Tag is not changeable by the customer.

More information about the Service Tag can be found in the Dell Knowledgebase [here](#).

Asset Tag

The Asset Tag is also stored into BIOS NVRAM and can be set, changed, or cleared by the end customer. The Asset Tag is displayed in text on the Dell boot splash screen on every boot and can be used for additional customer-specific tracking information, logistical messages, or unique branding. The BIOS Administrator password can be used to provide authentication and authorization controls to control Asset Tag modification.

More information about the Asset Tag can be found in the Dell Knowledgebase [here](#).

Platform Certificates for Machine Identity & Supply Chain Assurance (Secured Component Verification)

Supply chains can be vulnerable to disruptions such as tampering, theft, and counterfeiting. Recent geopolitical tensions have thrust supply chain into the spotlight, causing customers to question their electronic product providers and demand visibility as to where products are developed, created, manufactured, and handled.

The US White House issued Executive Order in 2021 to strengthen the resilience of the US supply chain. Extending government action, the DoD recently released a 'blueprint' for the [secure procurement of devices](#), which effectively calls out platform certificates as mandatory for verifying and proving device authenticity, including the criteria for deploying an acceptance test. It provided qualified examples from NIST's NCCoE supply chain assurance program, where Dell was one of the eight industry leaders which participated in developing examples, providing hardware and specifying solutions. Dell used its [Secured Component Verification \(SCV\)](#) solution as the foundation of [NIST Special Publication SP 1800-34](#) – Validating the Integrity of Computing Devices, which builds platform attribute certificates in the factory during manufacturing, thus aligning SCV with the DoD's procurement guidelines.

Platform certificates create secure identities bound to the products during manufacturing which are used to seamlessly connect Dell devices to customer infrastructure or Dell services, creating a foundation from which Dell provides secure attestation methods to our supply chain for the customer. Today, SCV enables dock to dock security by creating a certified manifest of device components bound to the device via TPM. The customer can validate that the device they ordered is the device Dell built and sent them. It ensures that the device was not intercepted or changed at any point during the delivery process. Dell will continue to expand function and capabilities built into the platform certificate and the methods of attesting device hardware, components, software, and firmware to become the root-of-trust for device identity, health, and authenticity.

SCV certificates may be deployed in two ways:

- On cloud, which stores the certificate in a cloud service known as My Account (formerly Dell Digital Locker).
- On device, which stores the certificate on the device drive (HDD or SSD) within the system EFI partition

[Validation of the SCV certificate](#) upon receipt may be accomplished in several ways:

- Through [Dell Trusted Device](#) and extensible to [Microsoft Intune](#), CrowdStrike, or [SIEM](#)
- Through manual or open-source tools such as HIRS. Detailed instructions on how to use this tool can be found at <https://github.com/nsacyber/HIRS>

A more in-depth explanation of [SCV is included later in this paper](#).

HBOM and SBOM

The emergence of SBOM (Software Bill of Materials) and HBOM (Hardware Bill of Materials) reflects a growing regulatory and operational need for transparency in the supply chain. SBOMs list software components used in

a system, while HBOMs extend this concept to hardware, detailing the origin, manufacturer, and attributes of physical components. Both CISA's HBOM and TCG's Platform Attribute Certificate are used by Dell's SCV to describe hardware composition. Though they differ in purpose, structure, and security guarantees they are the same in that they both provide a hardware manifest.

CISA HBOM

- Purpose: Supply chain transparency and risk management.
- Format: Extends SBOM formats (SPDX, CycloneDX) to include hardware attributes.
- Use Case: Primarily for documentation and procurement compliance.

TCG Platform Attribute Certificate

- Purpose: Cryptographic attestation of device identity and composition.
- Format: Signed certificate using Object Identifiers (OIDs) to describe component attributes (e.g., serial numbers, manufacturer, bus location)
- Security: Cryptographically signed by the manufacturer, ensuring integrity and authenticity from factory to field ("dock to dock")
- Use Case: Enables secure attestation and Zero Trust architecture

Dell's SCV platform certificate is a direct implementation of the TCG Platform Attribute Certificate. It is signed in a hardened datacenter during manufacturing and used to verify device integrity post-deployment

Credential Protection: Dell SafeID

Dell SafeID keeps user credentials safe at user and device levels and helps customers stay protected from malware attacks. This hardware-based storage solution for credentials better protects your information by keeping it isolated and out of attackers' reach.

At the device level, SafeID leverages a hardware-based Trusted Platform Module, or discrete TPM, a specialized chip designed to store highly privileged information such as cryptographic keys, provide platform device authentication and protect other secrets and authorizations required for secure operation of the endpoint. The latest version, TPM 2.0, is required for devices running the Windows 11 operating system.

SafeID keeps credentials safe at the user level with the help of ControlVault, a hardware-based security solution built into select Dell systems that provides a hardened, secure "vault" for storing and processing user credentials such as passwords, biometric templates (like fingerprints), and security codes. Instead of keeping these secrets in the main operating system and system memory, ControlVault runs on dedicated hardware and firmware - via a separate security chip—where it handles authentication data locally and isolates it from the Windows environment, reducing exposure to malware or OS-level attacks.

By executing sensitive operations and storing credentials within this protected boundary, ControlVault keeps credentials safe at the device level, helping prevent sniffing, tampering, or theft of authentication data even if the main OS is compromised.

SafelD plays a role in multi-factor authentication, or MFA, through means of the fingerprint reader, a Personal Identity Verification (PIV) card, the camera, or a FIDO2 key on a Dell device. With Dell's Pro and Pro Max (Precision) series there is an option to add ControlVault as a part of the device's configuration. With this feature, the end user can perform Certificate-based email signing via S/MIME and smartcard sign-in to mission critical applications or workspaces. For the ITDM, a policy can be set for the device to use multiple means of authenticating into the device, an application (or workspace).

SafelD: ControlVault

- **Isolated Processing & Storage**

ControlVault's ARM Cortex A7 1GHz processor and storage is not only outside-validated, FIPS 140-3 Level 3 – it is a dedicated security chip, unique to Dell, providing a protective and secure boundary for credential processing and storage enabling multifactor authentication via fingerprint biometrics, smartcard & NFC modalities.

- **Support**

ControlVault works with industry leaders and standards bodies to ensure adherence to customer enterprise needs. Today it supports Windows Hello Enhanced Sign-in Security, Linux fingerprint biometrics, FIDO2 specifications and Imprivata One-Sign, Digital Persona and EntralD.

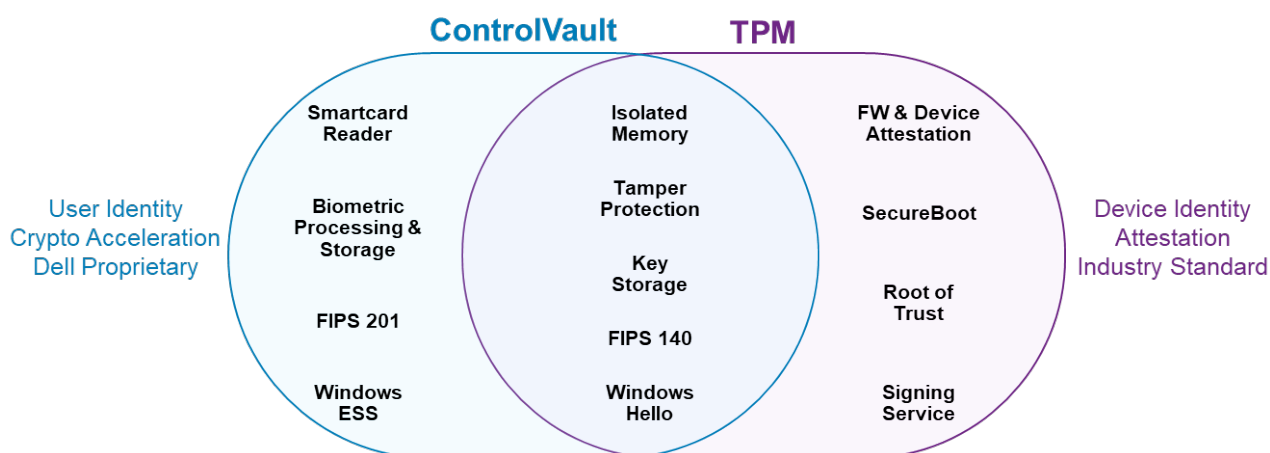
- **Certifications**

EMVco v4.3d, WQHL, NFC Forum, PCI PTS POI, FIPS 140-3 Level 3, FIPS 201-3

SafelD ControlVault & TPM

Isolated security processing – the credential handshake occurs within the boundaries of a dedicated security chip, unique to Dell, providing a protective and secure boundary.

Secure credential storage - protected hardware boundary to store keys keeping them out of sight from attackers.



Caption: While Dell ControlVault and the Trusted Platform Module are separate components that have unique capabilities, they also have commonalities that work together under Dell SafelD: the TPM primarily protects *encryption and signing keys*, while ControlVault protects *user credentials* like passwords and biometric templates.

SafelD: TPM and Microsoft Pluton

Microsoft has developed a security solution known as Pluton, designed as a security processor built into the System on Chip (SoC) that offers enhanced integrated security features in coexistence with an existing hardware TPM.

Dell will continue to include and use a hardware TPM in its commercial devices alongside enabling Pluton where it is available in SoC hardware. Pluton can serve as a security processor for additional OS features. Dell views this as a healthy co-exist strategy, which leverages the advantages of both TPM and Pluton for enabling OS security while also supporting discrete industry standard TPM 2.0 hardware for credential protection.

To learn more about Dell SafelD, read our [data sheet](#) or [blog](#).

Protect

From the NIST Framework: “Develop and implement appropriate safeguards to ensure delivery of critical services.”

The Protect stage of the NIST framework has been an area of significant investment for Dell over the last decade. All the context described in the previous ‘Identify’ section with respect to portfolio details, threat models, and security research has been pulled into the overall direction, strategy, and architecture for protecting the lowest levels of code in Dell devices. These features are truly the “first line of defense” for modern PCs against sophisticated adversaries.

Protecting the PC Boot Process

In theory, bootstrapping a modern personal computer may seem relatively simple. Pull the processor out of reset or low-power sleep state, initialize memory and motherboard hardware devices, enumerate storage, and find a bootloader to load the customer’s operating system of choice. Simple, right? In practice there is much more to it than that, and much of the complexity and additional features in the pre-boot timeframe is there to help protect the PC from executing unauthorized code. Ultimately, the BIOS boot process provides a safe foundation for the operating system and user applications.

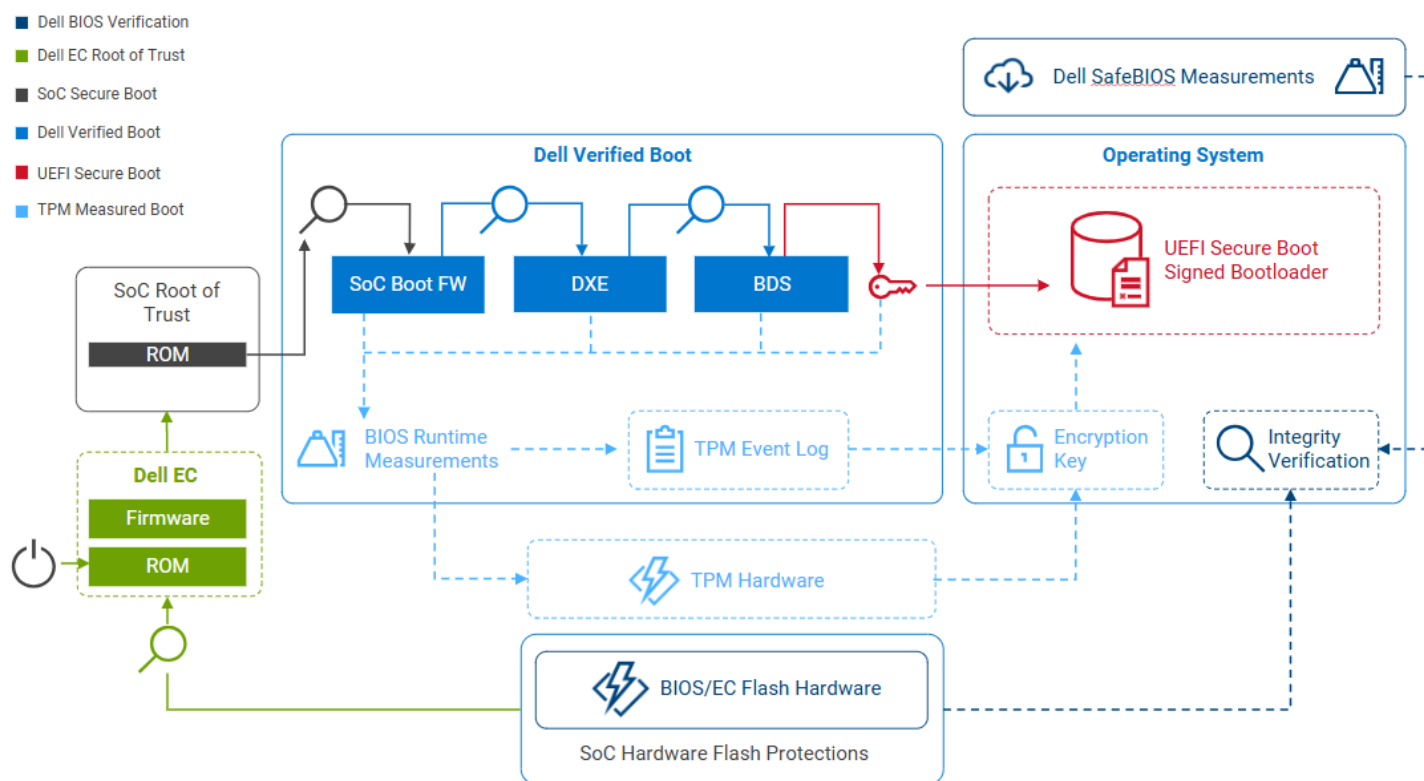


Figure 3: Dell Trusted Boot Chain

Securing the Boot Chain

The PC boot process is a series of configuration steps, events, and procedures that combine to create a tightly linked chain, from the point of time when the Embedded Controller (EC) and/or main processor come out of reset, to the point of handoff to an operating system like Microsoft Windows™, Linux, or Canonical Ubuntu™. Links in this chain protect the boot process by cryptographically verifying each subsequent link using either hashes or digital signatures. 'Golden' or reference hashes are protected by encoding them into an already verified section of code and digital signatures use public keys embedded in the firmware for verification. Note, for commercial devices launching in 2026, the Embedded Controller (EC) offers PQC-ready EC and BIOS signing. These features now include Leighton-Micali Signature (LMS) verification algorithms that are resistant to quantum computing hacks.

The illustration in Figure 3 depicts a high-level overview of the major components in the Dell Trusted Boot Chain. Many of these components, like the Embedded Controller, will be covered in more depth in other sections of this document and this illustration should serve as a helpful reference in understanding how everything ties together.

Like the roots of a tree, the root of trust is the origin point upon which all subsequent trusted events are built. For modern PC's, the processor reset vector is often considered the root of trust.

The “Root of Trust”

Like the roots of a tree, the root-of-trust serves as the foundational starting point for all subsequent trusted operations in a modern PC. Typically, this begins with the processor reset vector, the very first instruction the processor executes after coming out of reset.

In practice it's a bit more complicated than that. Dell devices support multiple roots-of-trust, including both an Embedded Controller and a chipset SoC (System-on-a-chip) security processor, such as Intel's Converged Security and Management Engine (CSME), and AMD Security Processor (ASP) that executes verified boot firmware prior to releasing the chipset and executing BIOS firmware. The EC acts as Dell's primary hardware root-of-trust, running cryptographically verified code to manage the power controls which bring the chipset out of its low-power state. The boot flow begins with the EC verifying its own firmware using Leighton-Micali Signature (LMS) verification

algorithms that are resistant to quantum-computing hacks and the integrity of the SoC chipset firmware before releasing the chipset. Once released, the SoC chipset continues the boot chain by verifying the integrity of the BIOS firmware, ensuring that only trusted code is executed as the platform boots.

TCG and the Root of Trust

The Trusted Computing Group (TCG) provides definitions and specifications for developing secure products. The TCG glossary defines a root of trust as “A component that performs one or more security specific functions, such as measurement, storage, reporting, verification, and/or update. It is trusted always to behave in the expected manner because its misbehavior cannot be detected (such as by measurement) under normal operation.” TCG specifications build on this to define several roots of trust that describe how the BIOS and Trusted Platform Module (TPM) must coordinate during the boot process to maintain authenticity of BIOS measurements; most importantly a Root of Trust for Measurement (RTM) and a Root of Trust for Reporting (RTR).

The Detect section of this document will cover the TCG Measured Boot feature in much more depth but first let's clarify a few words in the context of the boot process and root of trust. TCG Measured Boot uses the PC's TPM as a protected area for storing hashes of BIOS and firmware code that is loaded and executed in the boot process. TPM is designed to store these events in a secure way that can be verified post-boot through a process called attestation. Both Windows and Linux include TPM software stacks that support measured boot attestation.

All Dell commercial PCs use a dedicated TPM chip.

UEFI Secure Boot

One of the most powerful improvements in the last decade for protecting the pre-boot process from executing unauthorized code is UEFI Secure Boot. Unfortunately, there is some confusion in the industry about the benefits and scope of UEFI Secure Boot since the feature name tends to be conflated with the more general “secure boot” concept of executing signed pre-boot code. To avoid this confusion, this document will use the term “verified boot” when referring to executing cryptographically signed code in the pre-boot context when it is outside of the scope of UEFI Secure Boot.

That clarification is not intended to diminish the value of UEFI Secure Boot at all - it’s an effective feature for mitigating threats and exploits that may be delivered via unsigned bootloaders, UEFI shells, or UEFI drivers on add-in devices. To protect against these threats, Dell provisions trusted default certificates into the UEFI Secure Boot databases to allow Dell to manage the UEFI authenticated variables that protect the allowed database – the “db” – and the disallowed database “dbx”. Default provisioning also enforces verification of Windows 10/Windows 11 bootloaders and signed shims for Linux using trusted certificates from Microsoft. Also included by default is a Microsoft Key Exchange Key or “kek” to allow Microsoft-signed db and dbx updates from Windows.

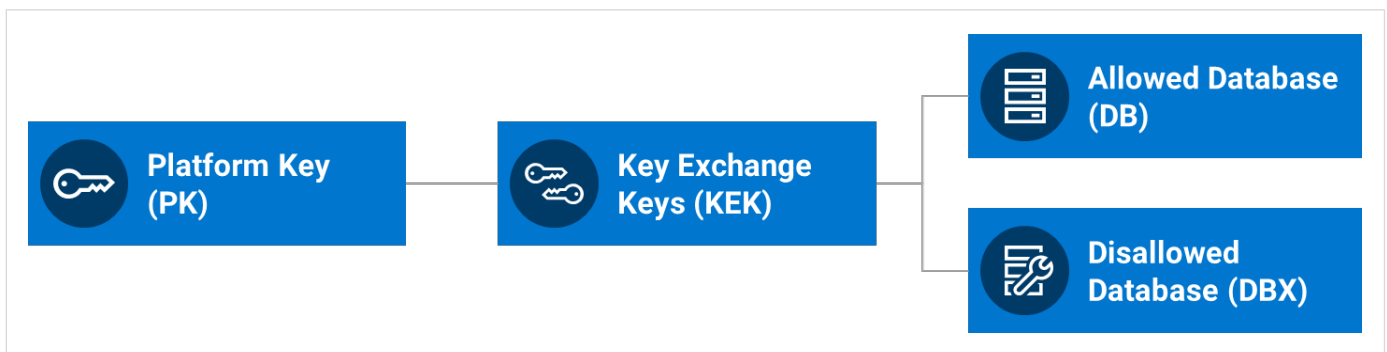


Figure 4: Secure Boot Key Hierarchy

UEFI Secure Boot Expert Key Management

Depending on customer and enterprise threat models, some administrators may want to restrict UEFI Secure Boot to only allow specific bootloaders and/or UEFI drivers. To support this, the Dell BIOS Setup interface supports Custom Mode Key Management settings that allow administrators to modify the contents of the UEFI Secure Boot key management databases through interfaces such as Microsoft’s PowerShell. This privileged operation is available with local physical access only and will temporarily disable UEFI Secure Boot while the certificate databases are being repopulated with custom keys supplied by the administrator. Key databases can also be reset back to the factory default values (including reinstallation of the original Dell PK) by using this interface.

The US DoD issued “[UEFI Secure Boot Customization](#)”, a Cybersecurity Technical Report, in September 2020. The document provides a comprehensive guide for customizing a Secure Boot policy to meet several use cases. Customization enables administrators to realize the benefits of boot malware defenses, insider threat mitigations, and data-at-rest protections, while overcoming incompatibility with hardware and software.

Signed Firmware Update

Previous sections detailed how Dell BIOS protects itself from running unauthorized code during the boot process, but how does it ensure that code cannot be tampered with or replaced on the motherboard BIOS flash storage device (e.g. the Serial Peripheral Interface, or SPI flash storage device) in between boots and during updates? Guidelines for protecting the BIOS against these threats were published by NIST in 2011 as Special Publication 800-147. This NIST document describes requirements for cryptographic authentication of BIOS updates, integrity protection of currently running BIOS, as well as guidelines to prevent bypass which further harden the BIOS against unauthorized modification via “backdoors”. Dell devices implemented these requirements in 2011 and a full whitepaper describing the support is linked in the References section of this document.

NIST SP 800-147 Support

Dell puts significant effort into hardening the BIOS protection and authentication capabilities on its client devices in accordance with [NIST SP 800-147](#) to support Dell’s customers.

BIOS running on a device that supports Signed Firmware Update contains information in its Root of Trust for Update (RTU) that supports a cryptographically hardened verification mechanism which allows only approved BIOS update utilities to modify the BIOS code in storage:

- **BIOS Update Authentication**

All BIOS update images are signed using the RSA PKCS #1 v1.5/v2.1 algorithm with RSA 2048-bit keys as per [FIPS Publication 186-5 Digital Signature Standard \(DSS\)](#). The SHA-256 algorithm was selected to hash the payload in the signing and integrity verification process based on this algorithm’s acceptance in NIST Special Publication 800-131A. Update images are verified by the BIOS using the public key contained in the RTU before the BIOS or other firmware currently running on the device is modified.

- **Integrity Verification**

The RTU and BIOS are protected from unauthorized modification using Dell proprietary flash write cycle trapping and locking mechanisms supported by the device hardware. All programmatic code update attempts that are not approved by the RTU verification mechanisms and any attempts to update BIOS data not approved by the BIOS storage handler are blocked from accessing the device flash memory using flash disable mechanisms.

- **Non-Bypassability**

The Signed Firmware Update mechanism in the RTU that enforces authenticated updates is the exclusive mechanism for modifying the BIOS. This enforcement cannot be bypassed by any firmware or software running on the device that is not controlled by the RTU.

System Management Mode (SMM) For x86 Systems

System Management Mode, or SMM, is a privileged mode of the processor architectures for x86 devices to support handling of high-availability, manufacturer-specific tasks independent of the operating system. Think of SMM as a component of the BIOS that remains resident underneath the operating system (reference the “ring” architecture where ring 3 refers to user mode code, ring 0 is the root, supervisory, or kernel mode of the operating system, and “ring -2” is applied to SMM to highlight the additional privileges that it is allowed over

the device). Dell uses SMM to support persistent storage (e.g., UEFI variables), BIOS configuration interfaces, thermal handling, and other critical-priority events.

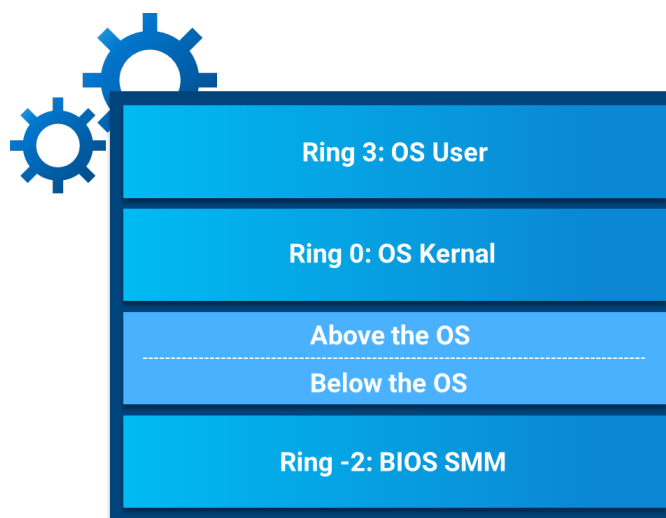


Figure 5: Modern PC Ring Architecture

SMM has been the target of dozens of disclosed vulnerabilities, security conference presentations, and media reports over the years. This has been welcomed attention from a security perspective because it provides helpful insights for SMM threat modeling and security improvements. For example, even though Dell BIOS uses SMM for system management activities, there has been significant investment in hardening the SMM environment and overall reduction in reliance on SMM. Additionally, Dell has integrated several technological advancements to incrementally deprive the SMM code that must be present on the system and mitigate potential impact to other parts of the operating system.

- **Threat: SMM Over-Reliance for BIOS Locking and Signed Update Verification**

The Signed Firmware Update whitepaper released in 2013 is still applicable and relevant to all Dell devices today. It's the baseline for protecting the BIOS from tampering or other unauthorized modification. While the NIST 800-147 specification requires non-bypassability in operation, it does not necessarily consider vulnerabilities that may exist in the code that enforces non-bypassability. In many implementations System Management Mode, or SMM, is the entity that enforces BIOS locking and signed update verification.

- **Mitigation: Intel BIOS Guard**

For Intel x86 equipped PCs, Dell decided to mitigate this reliance on SMM by moving the authority to unlock and update BIOS from SMM to device hardware. Dell devices have implemented Intel BIOS Guard since 2015, which explicitly verifies all BIOS code region writes using public keys fused into the Intel Platform Controller Hub (or PCH). Since the PCH operates between the processor and the flash storage where the BIOS is located, logic within the PCH can block all writes to the BIOS code region before flashing. Intel® BIOS Guard integration required considerable resources and infrastructure to implement, and because of this, was only adopted by a few OEMs. Dell considers this feature a must-have in the current below-the-OS threat landscape.

- **Threat: SMM Access to Hypervisor Memory**

One high-profile threat highlighted by security researchers is the potential for a rogue or malicious SMM handler or code to use SMM privilege to arbitrarily read and write to main memory. Turning this threat from theoretical to practical requires exploiting an unknown or unpatched vulnerability in SMM itself to gain code execution. As a demonstration of potential impact, researchers created proof of concept code that would interact with hypervisor memory and context that was designed to isolate and protect user applications. The end goal for an adversary with this level of access and sophistication could be credential or data theft from applications that were presumed secure.

- **Mitigation: Windows SMM Security Mitigations Table (WSMT)**

The Windows SMM Security Mitigations Table (WSMT) enumerates various methods that BIOS vendors can implement to mitigate SMM threats. Since some of the mitigations in WSMT can cause compatibility issues with legacy systems management software, Dell devices support a WSMT option in BIOS Setup to allow the administrator to enable or disable these mitigations. Once enabled, WSMT mitigations provide strict boundaries for memory access from SMM, e.g. the BIOS SMM handler can only use specific pre-allocated memory address ranges to communicate with system management software. The WSMT structure published by the BIOS provides affirmation to the operating system that the Dell device has implemented and enabled these features.

- **Mitigation: Memory Attribute Table and No Execute (MAT/NX)**

Protecting operating system memory from modification by SMM is just one piece of the runtime defense puzzle. UEFI Runtime Services are supported by BIOS and run within the OS context. To isolate these services, the BIOS implements the EFI_MEMORY_ATTRIBUTES_TABLE, which describes runtime memory organization for the operating system's consumption. This allows the OS to accurately configure page tables to block code execution from EFI data areas and prevent code areas from being overwritten from other potentially malicious code. These may seem like fundamental security features from an OS perspective but the handoff between pre-boot and operating system requires specific coordination to ensure these protections are accurate and do not introduce compatibility issues.

...the handoff between pre-boot and operating system requires specific coordination to ensure these protections are accurate and do not introduce compatibility issues.

Trusted Firmware for ARM Systems – Secure Partition Manager (SPM)

For ARM-based Architecture(s) for Qualcomm and NVIDIA-based PCs, the Secure Partition Manager, or SPM, would be applied by Trusted Firmware.

Privilege Elevation Comparison: SMI vs. Secure World

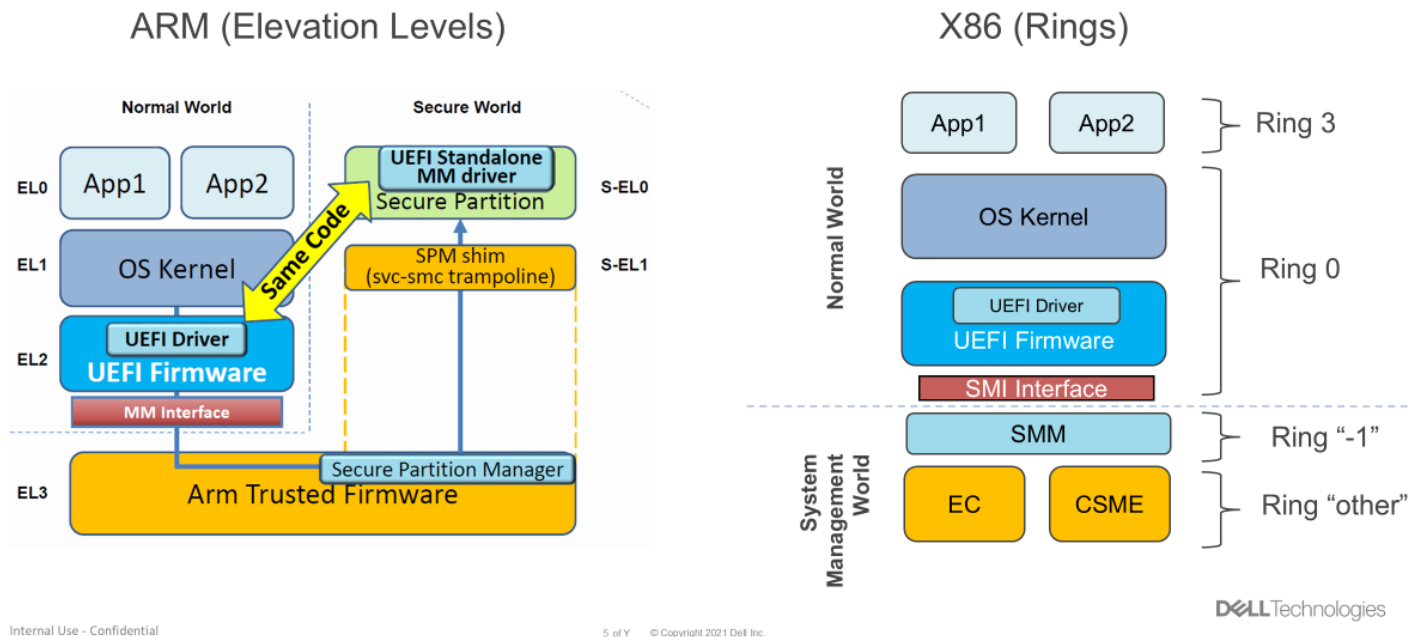


Figure 6: Privilege Elevation Comparison from [UEFI Forum](#)

BIOS Patch Management

Best practices in enterprise security should always include a comprehensive software patch management strategy to ensure that any software updates to mitigate vulnerabilities are deployed as soon as they are available. BIOS upgrades are often overlooked or delayed in the overall patch management strategy, but that's rapidly changing as customer awareness for built-in, "Below-the-OS" security continues to increase. To support this overall initiative, Dell device BIOS updates are posted to both Windows Update (or WU) for Windows 11 systems, and to the Linux Vendor Firmware Service (or LVFS) for Linux systems. This allows seamless integration of BIOS updates into the OS ecosystem without the need for separate BIOS update utilities.

BIOS updates are also provided as a part of the [Dell Trusted Update Experience \(DTUE\)](#), designed to help organizations more easily manage updates to keep devices at optimal operation and security. Of course, updating the BIOS using the Dell BIOS update utility is still supported.

BIOS Downgrade Protection

Sometimes adversaries will attempt to revert or 'rollback' software/firmware to a known vulnerable previous version as an initial step in their attack. A Dell commercial device with SafeBIOS can be configured in the BIOS setup program or remotely using the Dell Command Tool Suite to prevent BIOS reversions, thus mitigating this threat. By default, the Enable BIOS Downgrade BIOS setup option is turned on to support full flexibility for customers to choose the BIOS image appropriate for their infrastructure. However, once this setting is disabled (locally or remotely) only newer BIOS versions will be allowed to flash onto the device and physical presence (i.e. a user in front of the keyboard) is required to revert the setting.

Embedded Controller: Signed Firmware

The embedded controller, or EC, is included on all Dell commercial device notebooks and most modern commercial desktops and workstations. As explained in the section on root of trust, the EC is responsible for low level hardware interface functions such as power and reset management. Dell devices protect the EC firmware updates at two layers while performing firmware updates. First, the BIOS verifies the EC firmware signature prior to sending the update to the EC and blocks any unauthorized direct access to the EC firmware at runtime. Second, the EC update payload is subsequently verified by the EC firmware using public keys embedded in the EC context, independent of the BIOS. Modern Dell devices include cryptographic acceleration and verification capabilities integrated directly into the EC. These capabilities include verified boot support that will block any EC execution of unsigned firmware even if it was programmed onto the device via an unauthorized side-channel, such as direct physical access. This is a good example of the benefits of including physical access into the Dell device threat model and helps to protect this critical root of trust from tampering. For commercial devices launching in 2026, both the EC and BIOS Signing Updates now include Leighton-Micali Signature (LMS) verification algorithms, making them resistant to quantum computing hacks.

Protecting BIOS Configuration

Security research and media coverage of "Below-the-OS" threats focus largely on firmware tampering and/ or escalation of privilege, but the configuration of the client device can also be a potential threat surface. Attackers may use BIOS configuration settings to attempt to manipulate or reconfigure the device into a state that may be at higher risk for exploitation depending on the environment. Dell devices are shipped in a "secure by default" state and customers can protect this state from unauthorized access or modification by enabling a few important features.

Option	Description
Admin Password	Allows you to set, change, or delete the administrator (admin) password. The entries to set password are: • Enter the old password: • Enter the new password: • Confirm new password: Click OK once you set the password  NOTE: For the first time login, “Enter the old password:” field is marked to “Not set”. The password must be set for the first time you login and then you can change or delete the password

Figure 7: BIOS Password Reset

The BIOS Admin Password is the Dell device authorization mechanism for protecting BIOS configuration (such as BIOS settings) and the ability to upgrade or downgrade the BIOS. From a protection perspective, Dell recommends that all customers set a complex BIOS Admin Password to minimize the risk of unauthorized BIOS configuration modifications. The BIOS Admin Password can be set locally through BIOS Setup or remotely using the Dell Command Tool Suite. More information is available in individual device owner’s manuals and administrator guides.

- **Local vs. Remote Configuration**

The BIOS Admin Password protects against local and remote modification of BIOS settings that could be used by adversaries to open an attack surface on the device. Dell devices go one step further to classify specific security settings that are only available with local physical presence (i.e. a user in front of the keyboard) using BIOS Setup. These settings are locked from remote access even if the BIOS Admin Password is supplied through the remote interface. An example list appears in Table 1 below (not exhaustive):

BIOS Configuration Option	Local Access	Remote Access
Secure Boot	Yes	No
Allow BIOS Downgrade	Yes	No
Master Password Lockout	Yes	No
TPM Clear	Yes	No

Table 1: Example Local-only BIOS Options

- **Dell Master Password**

The Dell Master Password is a lesser-known feature of the Dell commercial client device. The Master Password feature is available for commercial device customers who may have forgotten or misplaced the BIOS Administrator Password on their device or fleet of devices. The Dell Master Password uses a shared secret algorithm (i.e. the BIOS and the unlock tool share a common secret) integrated into the BIOS or EC to allow Dell Customer Support to offer a device-specific unlock password only for customers that contact technical support and can provide proof of ownership of the device. Once provided by customer service, the master password must be typed into the device locally to unlock the system, as it cannot be used over any remote BIOS interface. The Master Password feature can also be disabled through a Lockout feature, for situations where the threat profile warrants it.

To the security practitioner, this feature may seem a bit antiquated, especially in a largely connected world running on a firm base of public key cryptography. Dell Customer Support must cover a varied commercial customer base across the world with a large set of challenges, not the least of which are language barriers, connectivity issues, and infrastructure availability. These requirements and overall customer scale combine to drive the need for this somewhat low-tech solution that can be exercised even when network-based remediation is not available.

- **Threat: Online Password Generators**

Dell is aware of several unauthorized online password generators that claim to generate Dell Master Passwords for devices. These generators include algorithms that duplicate the shared secret algorithm that is integrated into the BIOS and can often generate valid passwords for older devices. To combat this activity, Dell has redesigned the Master Password feature using modern cryptographic capabilities and best practices. For example, on newer devices this threat is mitigated by using secure encrypted storage when supported by the Dell commercial device, with broader portfolio coverage increasing year over year.

- **Mitigation: Master Password Lockout**

Certain customers may include targeted attacks against BIOS configuration with direct physical access in their threat model. A successful exploit within this threat model would require an adversary to discover a specific device identification information code and then have direct physical access to BIOS Setup to input the master password without being detected. This is a perfectly valid threat model, especially with today's prevalence of mobile systems. In these cases, Dell recommends enabling the Master Password Lockout feature to completely disable the Dell generated master password. Customers that enable this feature must employ their own independent password management processes since Dell Customer Support can no longer help with misplaced passwords for systems configured in this mode.

Configuration Side-Channels

Investments in protecting the configuration of the Dell device extend beyond interface and feature definitions. Protecting against “side-channels” or attempts to attack the implementation outside the bounds of the intended usage is also part of the Dell device threat model.

- **Threat: Physical Access**

As discussed, direct physical access to a Dell device is a part of the threat model of many customers, but more importantly, it's an assumption that the Dell security teams make during the secure development process. In other words, Dell uses this highest risk profile to promote the broadest resilience capability of

the Dell device. Physical access from the device perspective includes not only access to the local keyboard and display, but also potentially to the motherboard in an extended 'evil maid' class of attack. Adversaries may attempt to tamper with BIOS configuration settings by directly accessing the storage on the motherboard.

- **Mitigation: Encrypted Storage**

To protect against this level of physical access, Dell has incrementally moved BIOS configuration settings that control security policy to encrypted storage within the embedded controller (the EC). The EC includes root keys and cryptographic accelerators to provide resilience against direct physical attacks directed at the EC non-volatile storage. As an additional layer of security, these variables are encrypted with a device specific encryption key to protect against "break once" types of attack scenarios and further reduce the value of this type of attack.

Best Practices for Secure Configuration

BIOS configurations can be managed at scale in the enterprise with the Dell Client Command Suite. Customers interested in securely configuring their systems using the most restrictive policies can consult the [National Security Agency Cybersecurity Report UEFI Defensive Practices Guidance document](#) for overall recommendations. Please see the [Dell Client Command Suite tool documentation](#) to deploy and manage policies aligned to these guidelines.

Protecting BIOS at Runtime

A common misconception in the PC industry is that the BIOS is completely out of the picture once the bootloader and kernel take over execution of the boot process at the point in time where the BIOS hands control over to an operating system which has called the UEFI runtime service `ExitBootServices()`. Of course, this is not the case and even the “Basic Input/Output System” acronym is a reference to this role. A small subset of the BIOS code must persist while the operating system is running to support system management interfaces, UEFI interfaces, and overall system health components like event logging, as well as OEM hardware-specific functionality for power/thermal management.

- **UEFI Runtime Services**

The Dell BIOS allocates and assigns main memory during the boot process as `EFI_MEMORY_RUNTIME` to support specific UEFI services needed by the operating system. These services allow the OS to invoke capsule updates to update BIOS and/or device firmware, set general purpose UEFI variables, and manage the authenticated variables used for Secure Boot configuration. Most of these services are defined by standards (such as UEFI) but may include customization specific to Dell hardware and enhanced security features.

Intel Runtime BIOS Resilience

Intel is an ally in the Dell device security story providing foundational security technologies in processors and chipsets, also extending trusted computing concepts into new architectural areas of Dell devices. One example of this partnership is Runtime BIOS Resilience, which is part of the Intel Hardware Shield group of security features.

Runtime BIOS resilience builds another layer of security within the BIOS by hardening the SMM environment against attacks and protecting the operating system (and ultimately user code and data) from tampering by SMM. The Dell device sets up runtime BIOS resilience early in the boot process by enabling memory paging in SMM and configuring the SMM page tables to only allow access to the memory pages specifically allocated to SMM (in an area of memory called TSEG). This brings architectural capabilities of the processor that have been best practice for operating system memory safety into the realm of BIOS and SMM. These protections help prevent malicious code injection and redirection in the valuable SMM execution environment as well as ensure SMM code cannot affect the operating system (regardless of whether the code is legitimate or potentially rogue).

For more information about other Intel vPro capabilities, visit:

<https://www.intel.com/content/www/us/en/architecture-and-technology/vpro/what-is-vpro.html>.

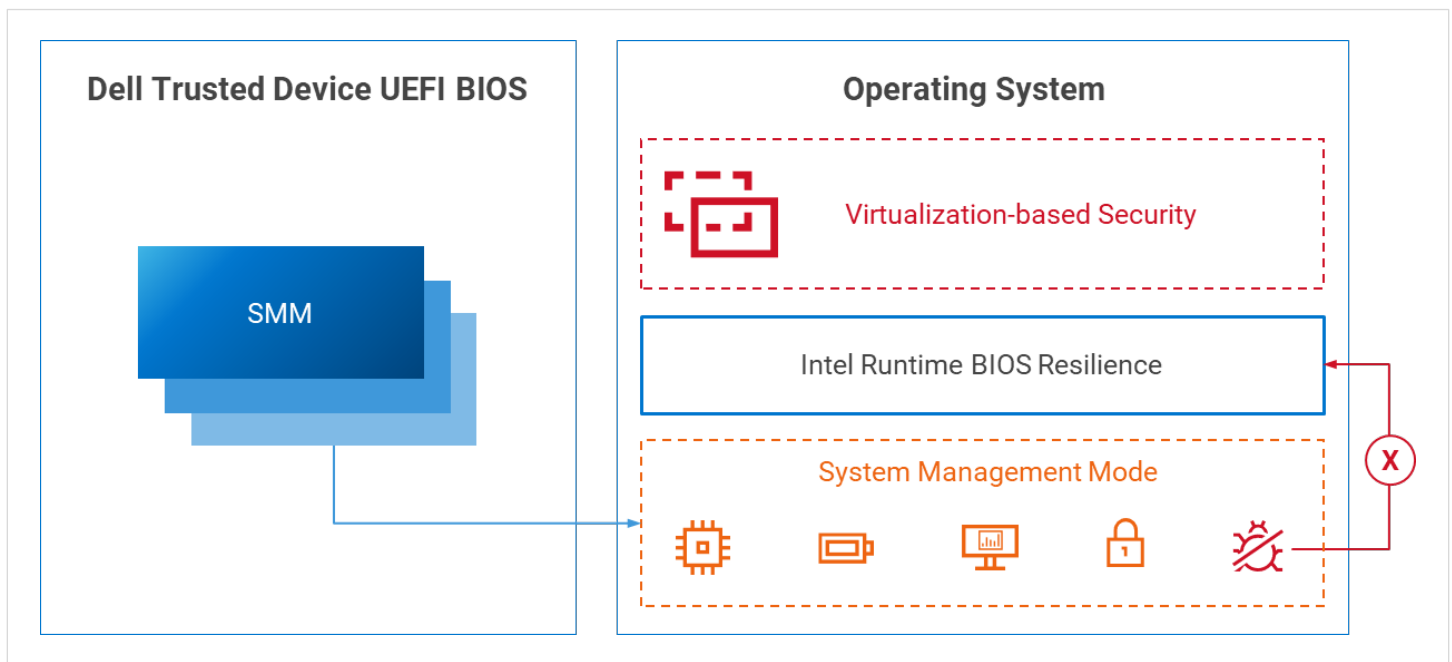


Figure 8: Intel Runtime BIOS Resilience

AMD SMM Supervisor

AMD-based Dell devices implement runtime BIOS resilience by embedding protections below the operating system that continuously monitor, detect, and recover the BIOS against unauthorized changes. Dell leverages NIST SP 800-193 Platform Firmware Resiliency guidelines and AMD security features to ensure that the BIOS can self-heal during runtime, preventing persistent compromise. These AMD features include:

- **AMD Security Processor (ASP):** A dedicated, integrated security co-processor that establishes a hardware root of trust during the boot process, which helps ensure system integrity from boot to runtime.
- **AMD Memory Guard:** Enables comprehensive, full system memory encryption to protect data in the event of physical access to the machine.
- **AMD Shadow Stack:** A hardware-based security feature that helps prevent malware from redirecting the flow of commands, a common exploit technique.

These features are integrated within the Dell BIOS resilience framework to strengthen runtime protections and help mitigate vulnerabilities.

Detect

From the NIST Framework: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

Even a 100% effective protection strategy both above and below the OS may not be enough to thwart the most sophisticated adversaries. Adversaries with this skill level and incentive can move and evolve quickly. Thus, having built-in (not bolted on) detection mechanisms help fill the gap between prevention and response and can provide much needed visibility into new adversarial techniques targeting client PCs.

In line with the expressed goal of 'transparency', Dell provides both hardware and firmware-based checks and detections which enable the customer to know when a device is compromised. These fall into two broad categories:

- Physical security detections and protections, and
- Built-in, below-the OS detection capabilities.

Dell Physical Security and Protection - Overview

Keeping PCs secure requires addressing all potential attack vectors. One important aspect is the physical security of the PC. This area of security aims to detect, alert and ultimately prevent an attacker from gaining physical access to the system, including its data and the credentials and secrets that it stores.

Dell provides physical security for its PCs in several ways:

- **Detecting when the chassis is opened and/or the battery is removed** and allowing the IT manager to decide what actions to take (from stopping boot to alerting via DTD to securely recording and reporting the event to wiping the TPM).
- **Inhibiting exploits which may connect directly to key parts of the circuitry**, providing highly privileged access to BIOS (SPI Tamper).

These physical security features are supported by hardware-based security to protect key credentials – such as smart card and fingerprint reader – with Dell ControlVault, which is unique to Dell and a part of Dell SafeID, as described in the "Identify" portion of this paper. This identity-focused hardware-based feature provides security that's equal to or better than provided by the TPM.

Key components of each of the physical security features are described in the following paragraphs.

Dell Physical Security Detection and Protection Features

Dell commercial devices – including Dell Pro, Dell Pro Max and Dell Pro Precision systems (fixed and mobile) - include chassis intrusion detection circuitry and logging capability that can be monitored via Microsoft Intune/SCCM, Dell Client Command Suite, and other common systems management platforms. Chassis intrusion combines with other built-in, below-the-OS security features to strengthen the Dell device defense in depth layered strategy. Complementary features already implement layers of security for defending below the OS, such as protecting against and detecting tampering, but it's important to also support early detection as soon as the chassis has been opened, which is typically the first sign of a physical attack.

Ability to Block Boot after Chassis Intrusion

An optional BIOS setting prevents system boot when chassis intrusion is detected. This new option, called "Block Boot Until Cleared", will prevent the system from booting when a chassis intrusion event is detected. This option is only available when Chassis Intrusion is set to "Enabled". When the POST message is displayed,

the only option will be to enter setup, where a user can use the “Clear IntrusionWarning” checkbox to acknowledge the intrusion event.

TPM integration for Chassis Intrusion events

When chassis intrusion is detected, an event is recorded in the TPM event log and extended to TPM PCR1. This can be used to protect TPM-sealed keys, such as Microsoft Windows Bitlocker encryption keys, preventing Bitlocker decryption of the hard drive when a chassis intrusion event is detected. The BIOS will record an EV_ACTION event with string “Chassis Intrusion” to the crypto agile log. The event digest will be a hash of the event string and extended to PCR1. When the chassis intrusion warning is cleared, the EV_ACTION event will not be recorded.

Optionally, a BIOS setting can be enabled to completely wipe TPM if a chassis intrusion is detected.

Battery Removal Detection

Removing the battery from a system results in an event being logged in the BIOS event log. To supplement Chassis Intrusion detection events, this new battery removal event can be used by security analysts to detect potential system tampering. When a battery is removed or replaced, this event will appear in the log on the subsequent normal boot: “Alert! Battery previously removed.”

SPI Flash Anti-Tamper features

Dell Commercial Devices also include new technology which detects and prevents tampering with BIOS SPI flash chips on the motherboard. While the system is powered on, the Dell Embedded Controller (EC) monitors electrical signals controlling the BIOS SPI Flash storage chip. If BIOS SPI flash chip tampering is detected by the EC, an event is logged in the BIOS event log, and a warning may optionally be displayed. When the system is powered off, the Dell Embedded Controller will shunt the electrical signals, such that BIOS SPI flash data cannot be accessed with an offline flash programming “chip clip”.

Dell Software-Based Detection Capabilities

Dell’s “below-the-OS” detection capabilities are designed to detect tampering, malware or unauthorized changes at the firmware level, before the OS loads. This helps to protect against advanced threats like rootkits and BIOS-level attacks. This extra layer of defense against firmware-level attacks is particularly valuable in enterprise environments where these threats could bypass traditional antivirus or OS-level defenses. Through the DTD App, data from these detections and defenses can be shared with EDR/XDR solutions, SIEMs and management solutions like Intune.

Dell Off-Host BIOS and Firmware Verification

Dell’s off-host BIOS verification and firmware verification are two capabilities that verify the integrity of the system BIOS (and, on supported platforms, Intel vPro ME/CSME firmware and AMD ASP firmware) against a known-good reference stored in Dell’s cloud, instead of trusting only what’s stored on the endpoint itself.

Unlike pure “self-healing BIOS” designs that only compare to a local backup image, Dell’s approach validates against external, OEM controlled reference measurements and exposes that telemetry outward, which is what makes it “off host”.

At a high level, the workflow involves three main components:

- **Endpoint firmware and BIOS:** Dell commercial PC with a signed, NIST 800 193–aligned BIOS and platform firmware stack.
- **On-host telemetry and agent:**
 - Dell Trusted Device (DTD) Application or Dell Client Device Manager Security module installed in the OS.
 - This module reads BIOS/firmware measurements and sends telemetry/verification results.
- **Off-host verification backend:**
 - The Dell secure cloud that stores known-good BIOS images and firmware measurements per platform and version/SKU.
 - It maintains cryptographic reference hashes and metadata, along with approved Intel ME/CSME firmware builds and AMD ASP firmware builds for relevant platforms.
 - Verification logic that compares endpoint measurements and returns pass/fail, plus events for SIEM/management tools (Intune, CrowdStrike Falcon, TechDirect, etc.).

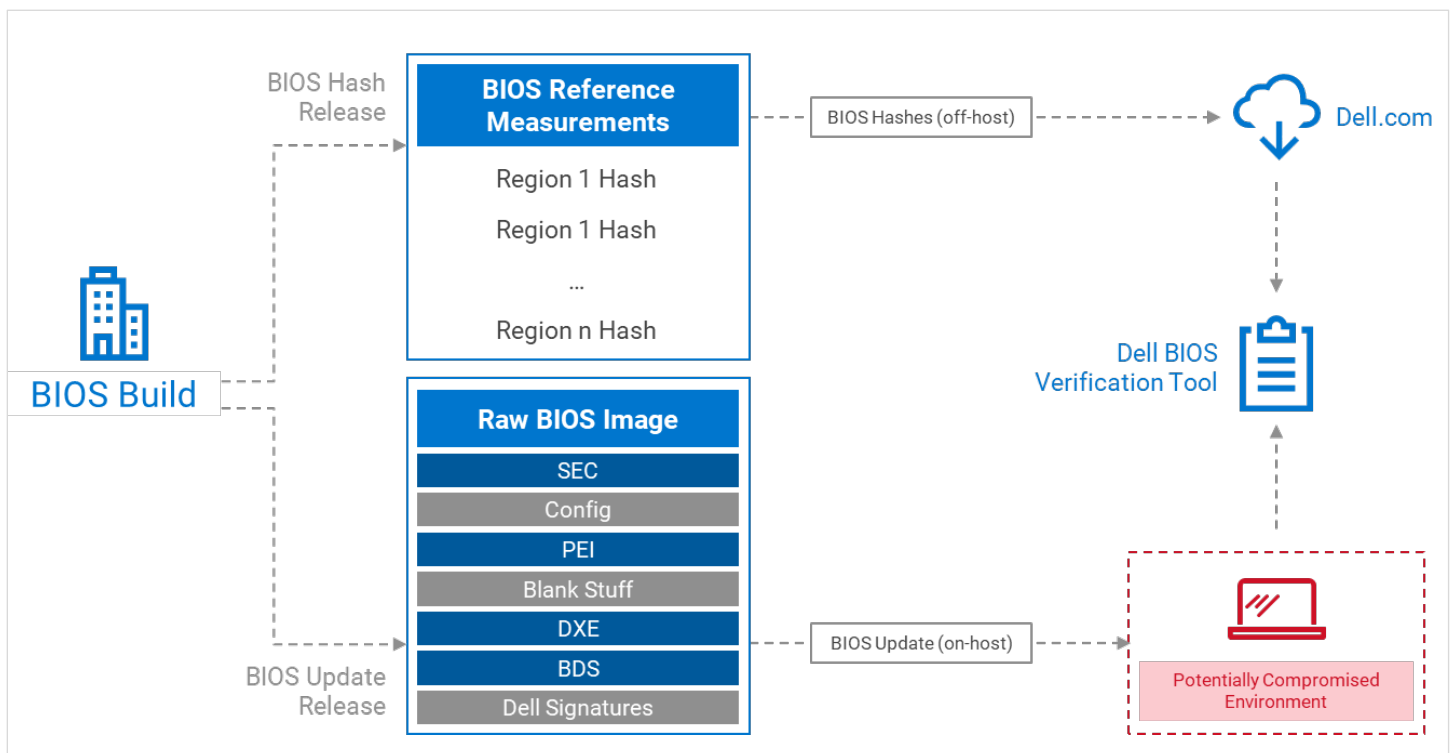


Figure 9: BIOS Verification Flow

Dell BIOS verification now utilizes SHA-512 verification algorithms that are resistant to quantum computing hacks, providing an increased level of protection for the off-host process. More information can be found [here](#).

How Off-Host Verification Is Performed

The DTD App – or Dell Client Device Manager (DCDM) | Security module – runs at each boot and/or per policy (typically scheduled, e.g., every 24 hours or on-demand). On the endpoint, the DTD App (or DCDM):

- Reads the current BIOS/firmware image and configuration metrics from the endpoint.

- Calculates hashes (e.g., SHA-2, SHA-5 family; exact algorithm choice is not specified publicly but is consistent with Dell's cryptographic practices, including encryption that is resistant to quantum computing).
- Packages the measurements along with device identifiers (service tag, model, BIOS version, etc.).

It then sends a telemetry/verification request to Dell's secure cloud over an authenticated, encrypted channel.

In the Dell cloud the verification service takes the following steps:

- Locates the correct reference entry for the device (maps platform ID + BIOS version + ME version → reference record).
- Compares endpoint hashes to these off-host stored hashes:
 - If `H_bios_image == H_bios_image_ref` and `H_me_fw == H_me_fw_ref` (where applicable) and there are no policy violations in configuration, the BIOS/firmware is considered verified.
- Produces a pass/fail result and may also calculate a risk score or attach specific error codes:
 - "Pass" → BIOS (or firmware) is intact, matches known good copy.
 - "Fail – version mismatch" → outdated but not necessarily tampered.
 - "Fail – integrity mismatch" → hash mismatch indicating possible tampering or unapproved modification.

Verification results are pushed back and made available in several ways:

- Windows Event Viewer on the endpoint – detailed event IDs, pass/fail, error details.
- Management and security consoles:
 - Microsoft Intune (via Dell Client Device Manager & DTD integration).
 - Dell TechDirect / Dell Management Portal for fleet wide views, especially when using Client Device Manager and Secured Component Verification (SCV) on Cloud.
 - CrowdStrike Falcon, Absolute – integrated BIOS-level telemetry streams IoA, off-host BIOS verification failures, component tampering alerts into third-party security consoles.

Dell is the only PC OEM documented as providing firmware level threat detection and visibility directly within third party security consoles using this off-host telemetry.

If off-host BIOS verification detects an issue, the DTD App or DCDM logs BIOS verification failure events locally and surfaces them to the configured management plane (Intune, Dell TechDirect, CrowdStrike Falcon, Absolute, etc.).

These can then trigger:

- Conditional access policies (e.g., in Intune).
- Incident workflows in EDR/XDR or SIEM.
- Remediation playbooks.

Indicators of Attack

Dell Indicators of Attack (IoA) extends tamper detection capabilities beyond the code into the BIOS configuration arena. Various compliance and security tools have been able to detect changes to operating system settings and a small subset of BIOS settings (typically only Secure Boot) in the past, but these tools usually lack any kind of temporal context for these detections. These prior solutions were designed for

compliance or drift detection and may still allow an attacker to carry out multiple configuration changes and then revert to a “known good” state to avoid detection.

The Dell IoA feature addresses this gap by using Dell threat modelling exercises and expertise to define specific chains of multiple configuration changes that could introduce risk to the system or signal the early signs of an in-progress attack. These may include behavioral signals and sequences which may indicate a below-the-OS attack (e.g., repeated failed verification, unusual update patterns, suspicious configuration drift). The configuration attributes in each of these chains are continuously monitored by the Dell Trusted Device Application, and risk evaluations are logged as these chains are traversed on the system. This allows the administrator or security analyst to take remediation actions as needed based on incremental risk associations and potentially before the next stage of the attack is deployed against the weakened configuration.

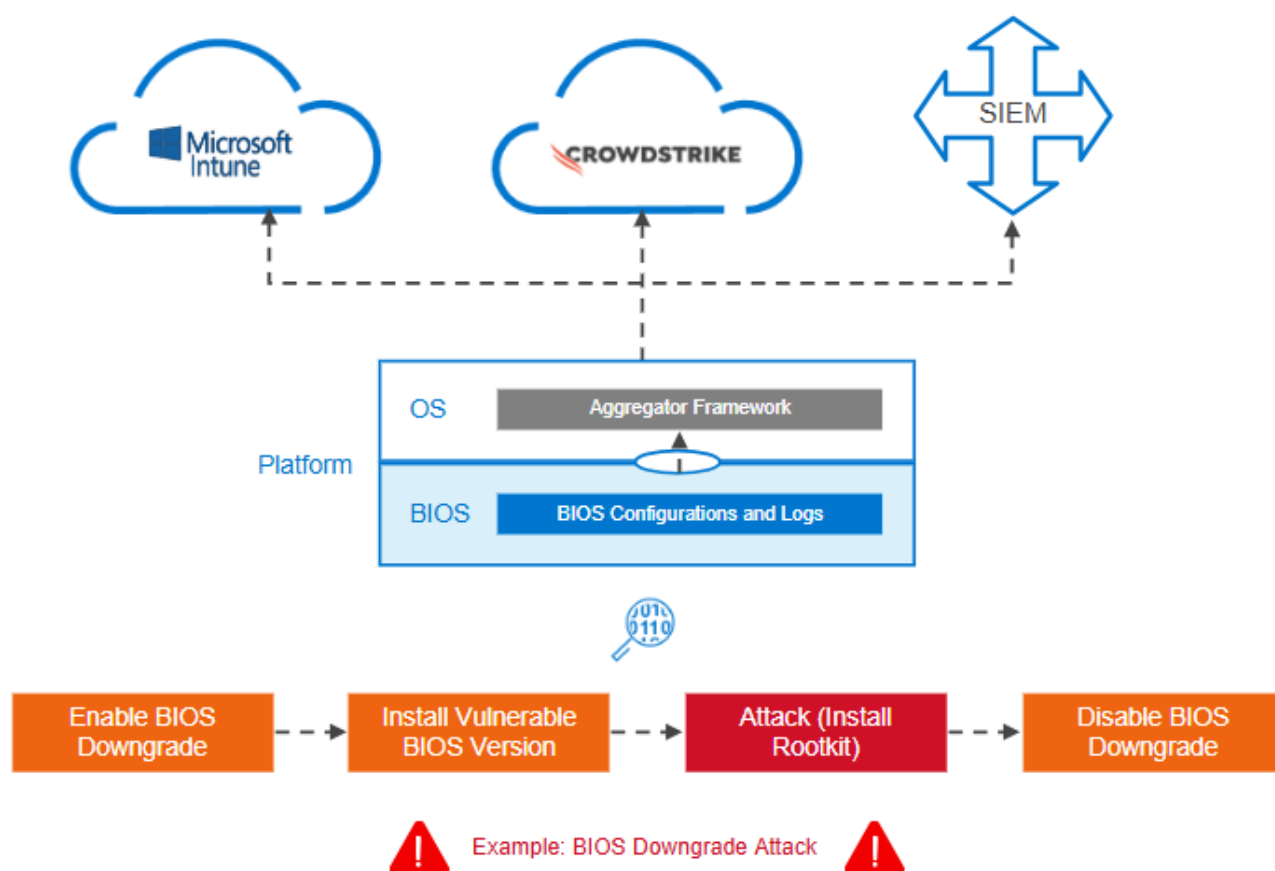


Figure 10: Indicators of Attack

BIOS Image Capture

If BIOS corruption or tampering is detected, the BIOS Image Capture feature, part of the DTD App, can capture the compromised BIOS image for forensic analysis, rather than simply overwriting it immediately. Customers

that are concerned about sophisticated adversaries tampering with BIOS would likely also be concerned about the intention, and even identity, of those adversaries. To support this, the Dell BIOS Recovery feature includes an image capture function to save the tampered or corrupted BIOS to the EFI partition on the system drive (HDD/SSD) during any recovery operation. This image is saved as a simple binary file that can be harvested by system security software such as the Dell Trusted Device Application.

To accomplish this, the DTD App/DCDM security module queries the EFI partition for a corrupt or tampered image.

- If found, copies it to \\%PROGRAMDATA%\Dell\TrustedDevice\ImageCapture.
- If off-host verification fails and tampering is suspected, it can copy images from memory as well to the same location.

A captured BIOS image is retained for a defined period (e.g., 200 days) to support investigations. This image can be collected by a compatible app for analysis at scale. Experienced analysts within customers' security operations control (SoC) can evaluate this file using methods that already exist for analyzing malware during more common hunting operations.

Common Vulnerabilities and Exposures (CVE) Detection and Remediation

This feature permits identification of known vulnerabilities on a Dell device with a built-in security check.

CVE Detection and Remediation uses an intelligent, built-in monitoring feature that scans for publicly reported security flaws on a Dell device and provides recommendations on how to fix them. It proactively assesses device health against a database of publicly disclosed computer security flaws maintained in the U.S. National Vulnerability Database by the National Cybersecurity's federally funded research and development center (FFRDC), operated by the MITRE Corporation and funded in part by the U.S. Department of Homeland Security. It also uses Dell Security Advisories (DSAs) which map specific CVEs to affected Dell models and BIOS/Firmware verifications, as well as the recommended fixed versions and mitigation guidance.

CVE Detection scans for vulnerabilities based on specific PC models and BIOS versions, recommending the relevant patch for swift remediation.

- On each endpoint, the agent collects:
 - Platform identity (model, service tag).
 - Installed BIOS version.
 - Installed firmware versions tracked by DCU/DCDM (as applicable).
- The version is mapped to a CVE, informed by the NVD/MITRE CVE database and Dell security advisories. For each component, the DTD (DCDM) app determines whether there are open CVEs (unpatched on the device) and if there is a remediating BIOS/firmware update existing from Dell. It then aggregates this into a per-component vulnerability status and provides an overall view of outstanding DSAs and CVEs for the device.
- The results are written in the Windows Event Viewer, the DTD local console and/or Dell TechDirect and DMP portal dashboards. These results can also be provided to Intune, CrowdStrike, Absolute, etc. depending on the configuration.
- CVE identification can run as 'detect only' (unmanaged) where it does not automatically patch, and logs which CVEs/DSAs apply, providing recommendations on which BIOS/firmware updates to apply.

- In managed environments such as Intune, CVE auto-remediation can orchestrate the updates for the detected CVEs using the DCDM Update Module or the DCU backend. This data can be used to prioritize patching for high-impact CVEs and critical platforms, to provide a compliance signal and implement conditional access and to implement a CVE Auto-Remediation process through DCDM to reduce the need for manual patching.

Dell CVE Detection and Remediation turns each Dell PC into a self-reporting sensor for BIOS/firmware vulnerabilities, with the option (via DCDM) to make remediation more automatic. It bridges the usual gap between traditional patch management and the firmware layer, which is typically opaque to standard endpoint tools.

Dell CVE Detection and Remediation works today for BIOS vulnerabilities and is being extended to cover all firmware and eventually applications and drivers.

Security Risk Protection Score

Dell's Security Risk Protection Score (or more simply the Security Score) is a composite endpoint-level KPI generated by the DTD App or DCDM. It's meant to provide a single, quantitative signal to plug into policy engines (Intune, SIEM, SOAR, etc.), but it's explicitly derived from several underlying security controls rather than being a black box.

The Security Risk Protection Score is an endpoint-level KPI that expresses how well a device is protected at and below the OS, based on the presence and health of specific controls as observed by the DTD agent.

- It *is not* a generic "vulnerability score" like CVSS.
- It *is not* a behavior-based risk score (e.g., "this device is under active attack").
- It *is* a configuration-/control-centric score that answers: "Given what I can see about this endpoint's foundational protections, how exposed is it?"

It should be treated as a device-hardening and control-coverage signal, not as a replacement for EDR risk scores or SIEM detections.

The score is based on a fixed set of security "solutions" / controls that the agent checks on each endpoint. Currently this list includes:

- Anti-virus status
- Firewall status
- Disk encryption (e.g., BitLocker) status
- TPM use (TPM 2.0, enabled & in use, required for some Dell capabilities)
- BIOS administrator password presence/enforcement
- BIOS verification state (off-host BIOS integrity attestation)
- Intel ME Verification state (for Intel platforms)
- AMD ASP Verification state (for AMD platforms)
- Indicators of Attack (IoA) / BIOS Events status (whether IoA has flagged issues or if BIOS configuration has suspicious changes)

For each of these controls, the DTD App/DCDM determines:

- Whether the control is present and correctly configured.

- Whether it has recently passed its own internal checks (e.g., BIOS verification passed, Intel ME verification passed).
- Whether there are warnings or failures (e.g., control missing, disabled, or showing signs of compromise/misconfiguration).

For each control, DTD computes a per-control assessment (Pass, Pass with warnings or Fail) and aggregates them into the Security Risk Protection Score (per device), written as a comprehensive score event along with the detailed per-control statuses.

While Dell does not expose the exact mathematical formula, you can safely assume that high-impact controls (e.g., BIOS verification, disk encryption, Intel ME verification) are weighed more heavily than softer ones (e.g., AV presence), given the emphasis on below-the-OS security in SafeBIOS and DTD. Additionally, a single Fail on a critical foundational control typically has a material negative impact on the overall score, even if less critical items pass.

DTD scans for the presence and status of each component every 24 hours, and also 15 minutes after the DTD App/DCDM service restarts.

Results persist as timestamped events in Windows Event Viewer under the Dell Trusted Device logs and are also available via integrations (Intune, SIEM, etc.).

The score can be disabled via registry (HKLM\SOFTWARE\Dell\TrustedDevice\DWORD=SecurityScore, 1=enabled, 0=disabled). This is useful if you want to control telemetry volume or prefer to rely solely on raw control-level events.

There are Security Score web service APIs with JWT authentication, indicating that the score is also consumable via Dell's backend or TechDirect-like services for dashboards/fleet KPIs.

Dell Supply Chain-Based Detection Capabilities

Dell offers a number of specific capabilities to enhance the security of devices through manufacture and shipment. The one of highest interest to device security is Secured Component Verification, or SCV.

Secured Component Verification (SCV)

Secured Component Verification (SCV) is a Dell supply-chain assurance feature that provides "as-built" cryptographic proof that upon receipt, a Dell has the same critical hardware that left the factory. This protects against swaps, additions and other types of hardware tampering for key components. It does this by creating and signing a platform certificate (as-built manifest) at the factory which is validated after delivery and at any point during the PC's lifecycle.

SCV is offered both as cloud-based and on-device, depending on the customer's requirements. There is a small charge for the SCV, which is normally included in the PC order. Factory assembly time is the **ONLY** time the SCV certificate is created for that system.

1 Order	2 Build	3 Collect	4 Store	5 Deliver	6 Validate
Customer places order for a PC with Secured Component Verification (SCV) capability.	Order is sent to Dell manufacturing to build.	Dell collects PC component data. A platform certificate is created and signed in-factory.	Dell stores the certificate on the local drive (SCV on Device) or in Dell's secure cloud environment (SCV on Cloud).	PC is delivered to customer or its VAR to validate.	Customer verifies PC configuration.*

**Please note that the customer takes custody upon delivery, and that the device has undergone the intake process and completed certificate validation at Customer (or VAR's) site within 30 days from the day of signature upon receipt of asset.*

- **Order processing** - Once a customer orders a commercial PC with SCV enabled (on Device or on Cloud), the PC is first assembled to the order specification.
- **Build** – Dell builds the device that is ordered.
- **Data collection** - The component data is collected and structured into a manifest for that device, with Dell systems read out of identifiers for critical components (motherboard, CPU, memory, storage, NIC, TPM, etc.). These identifiers are derived from PPID labels / serials / electronic IDs captured as part of Dell's supply-chain traceability infrastructure.
- **Create & sign certificate** - The manifest is turned into a platform certificate (sometimes called a platform or inventory certificate), which is cryptographically signed in the factory by a Dell Certificate Authority (Dell CA) or a hardware security module (HSM)-backed signing process.
- **Store certificate (on-device or in cloud)** – There are two options based upon how the customer has requested the certificate to be provided:
 - **SCV on Device:** the certificate is stored on the local system, typically in a protected UEFI/EFI or dedicated partition so it survives reimaging. This is useful for air-gapped devices and others that cannot be exposed to the internet (and secure cloud where SCV on Cloud certificates are stored).
 - **SCV on Cloud:** the certificate is stored off-host in Dell's secure cloud, accessible via TechDirect / Dell Trusted Device (DTD) and integrated tools like Microsoft Intune.
- **Deliver & accept** – The system ships to the customer, and within a defined window (commonly 30 days for PC SCV on Cloud) a validation step is run to confirm the delivered hardware matches the certificate.
- **Validate** – A validator (Dell Trusted Device App, SCV app, or a third-party verifier for on-device) compares the current hardware inventory with the certificate inventory and cryptographically verifies the certificate chain. The validator then collects the live inventory from the system and compares it with each component in the SCV certificate manifest. A validation report is generated detailing matches/mismatches plus any certificate or chain-of-trust issues.

SCV provides hardware-level attestation that the endpoint matches its known-good “as-built” state. When combined with TPM-based attestation and Dell Trusted Device telemetry, SCV on Cloud allows remote device attestation, aligning with Zero Trust (“never trust, always verify”) guidance and NIST supply chain assurance practices.

More details on SCV can be found in the [Dell knowledge base article](#).

Additional Dell Device-Based Detection Capabilities

TCG Measured Boot

As mentioned in an earlier section, TCG Measured Boot on the Dell device uses the TPM as a protected area for storing hashes of BIOS, firmware, and bootloader code and configuration that is loaded and/or executed in the boot process. The TPM is designed to store these events in a secure way that can be cryptographically verified after the boot completes through a process called attestation. More information about how the TPM works can be found in the TCG [TPM 2.0 Library Specification](#).

The functionality needed to support TCG Measured Boot is built into the TPM using registers with very specific properties called PCRs (Platform Configuration Registers). These PCRs cannot be written to directly: they can only be 'extended.' Extending is a relatively simple operation in practice but is incredibly useful for code integrity. Internal to the TPM, each PCR extension operation takes the current state of the PCR, concatenates it with the incoming message or data to extend, and then hashes it using the selected algorithm, e.g., SHA-256, etc., before recording it to the PCR. This creates a PCR value cryptographically dependent on all extended operations (and their order) that occurred since the PC was reset.

Intel® vPro Additions to Built-In Security

With Intel vPro enabled on Intel-equipped PCs and supplementing Dell SafeBIOS protections, Dell and Intel® provide another routine for managing fleet of Dell platforms. With Intel® Active Management Technology, ITDMs can diagnose issues remotely in a hybrid work scenario. Along with Intel® AMT, vPro has additional features such as a Platform Service Record and Unique Platform Identity (or UPID). Both features rely on one another to play key roles in Dell SafeBIOS prompting tamper detection on Dell platforms through Indicators of Attack.

Code, Configuration, and the TPM Event Log

Each Dell commercial device extends code and configuration information to the TPM PCRs during every boot in accordance to the [TCG PC Client Platform Firmware Profile Specification](#).

There are many PCRs in each TPM. Table 2 provides a high-level overview of some of the TPM PCRs used on the platform. To maximize compatibility across PC vendors, the TCG PC Client Platform Firmware Profile Specification describes which specific PCR indexes in the TPM should be included in each type of measurement during the boot process. For example, pre-boot BIOS code that executes from the internal SPI flash is extended to PCR0 while UEFI drivers that execute from add-in devices are extended to PCR2. Dell devices extend BIOS Setup options that are security related to PCR1 in addition to hardware information such as memory configuration.

PCR Number	Function / Allocation
0	BIOS Code

PCR Number	Function / Allocation
1	BIOS Settings / Platform Configuration
2	UEFI Option ROMs
3	UEFI Option ROM Configuration
4	Boot Loader / Master Boot Loader (MBR)
5	Boot Loader / Master Boot Loader (MBR) Configuration
6	Platform Manufacturer Specific Measurements
7	Secure Boot
8-15	Static Operating System
16	Debug
23	Application Support

Table 2: Standard PCR Allocations

The Dell device BIOS creates a TPM event log entry each time a new measurement is extended to any TPM PCR during the boot process. The TPM event log allows verifiers such as the OS or remote entities to reconstruct the record of code in the event of a mismatch to an expected or known-good value. The TPM measurements persist for one boot cycle. Upon reboot, the TPM PCRs are 'reset', and the TPM event log is cleared. The TPM PCR measurements and the event log are recreated on every boot.

NIST 800-155 Measurements

One unpublicized feature of Dell devices with Intel processors that may be interesting to readers is the inclusion of PCR0 "reference measurements" directly embedded into each BIOS update utility. This feature aligns to the NIST SP 800-155 BIOS Integrity Measurement Guidelines (still in draft revision) and can be used to determine the Dell authorized values for the BIOS code region measurement that the BIOS extends to PCR0. The value can then be compared to the measured value in the TPM event log on the device to verify the BIOS code running on the platform. To export these reference measurements, use the /BIOSMeasurement command line option on any Dell device BIOS update utility. An example of the content and format of the output of this command appears below:

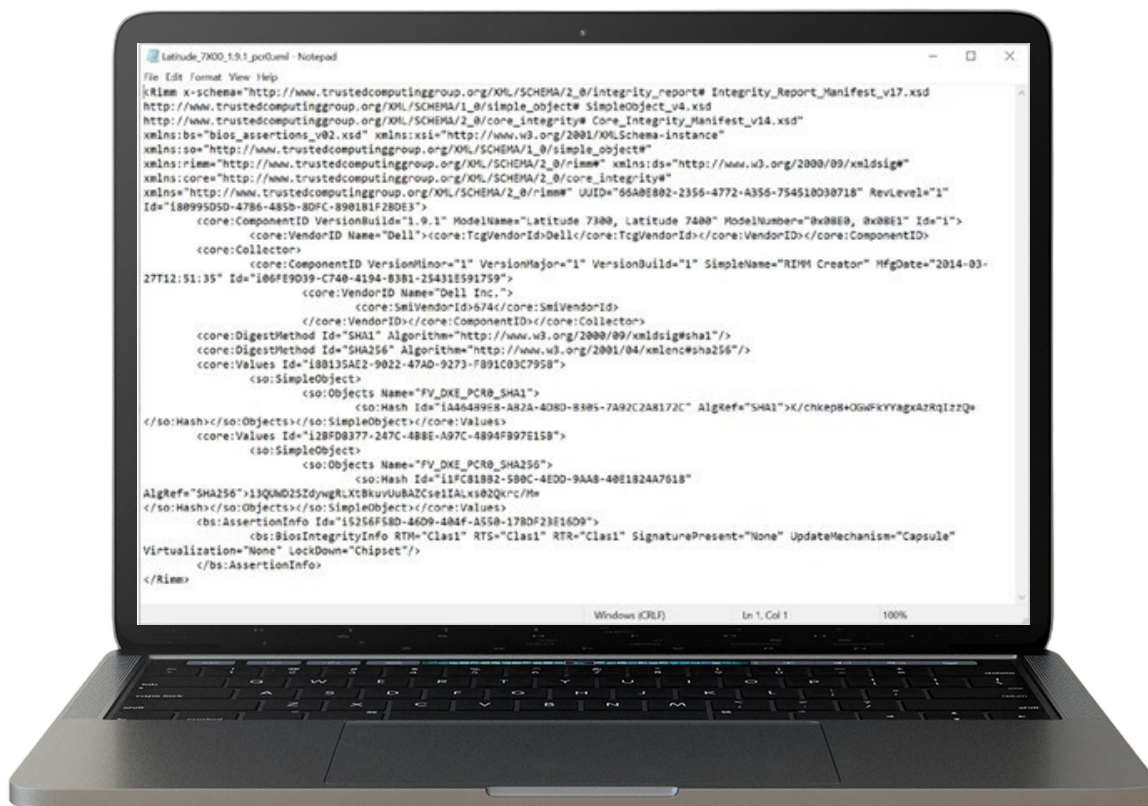


Figure 11: Example BIOS Measurements

Advanced: NIST 800-155 Measurements Extraction, Conversion, and Comparison

Use the following steps to extract and compare the NIST 800-155 measurements from the BIOS update utility with the device's TPM PCR event log measurement.

- Create a NIST800-155 xml output file from the BIOS firmware update utility
 - At a command prompt, execute: Latitude_7X00_1.9.1.exe /BiosMeasurement
 - Locate the output file. e.g., Latitude_7X00_1.9.1_pcr0.xml from the above step.
 - This is the NIST 800-155 Measurement XML file
 - Open the file, and find the SHA1 and / or SHA256 PCR 0 values
 - Convert the BASE64 PCR 0 value to HEX (use an online tool)
 - Save value for comparison.
- Get the TPM PCR Event Log from the device (booted to the OS).
 - Use a tool to read the device's TPM PCR Event Log.
 - Find the PCR0 'EV_Post_Code' entry in the log.
 - Compare this value to 1.e). The values should match.

Dell Integrations with Hardware Providers

Intel Boot Guard

When Intel introduced Boot Guard technology, Dell client PCs implemented it as an additional hardware root of trust for BIOS. Intel Boot Guard serves as an incredibly effective detection mechanism for verifying the integrity of the earliest and most critical code executed by the processor is still intact. Any tampering or corruption of the initial boot block (IBB), the very first piece of BIOS code to be executed by the processor, will be detected by the chipset before the processor comes out of reset. Dell devices are configured with the most restrictive policy for Boot Guard which blocks all code access if the boot block verification fails during the Boot Guard check. This policy “bricks” the system, limits any further adversary activity, and reduces the overall incentive for tampering.

While technologies like Intel Boot Guard offer effective protection and detection capabilities for the root of trust, some customers may be concerned that the Boot Guard checks are only enforced once per boot or that the digital certificates used for verifying the boot block are resident on the endpoint. The BIOS verification included in Dell commercial PCs addresses both concerns. BIOS verification uses an OS-resident application – the Dell Trusted Device, or DTD – to verify the integrity of the BIOS against known-good off-host reference measurements at any time. These reference measurements are generated for each BIOS version during the BIOS build process inside Dell infrastructure. Invoking this capability at a regular cadence greatly reduces the window of time that malicious code can be present on a system before detection, even in the extremely unlikely event that all boot-time prevention capabilities were somehow bypassed.

Intel Management Engine (ME) Firmware Verification

As previously mentioned, the Intel vPro Converged Security and Management Engine (CSME or just “Intel ME”) plays an important and privileged role in the boot process and the overall operation of the system below the OS. The Intel ME Firmware Verification component of Dell Trusted Device detects unauthorized tampering of the early boot stages of this highly privileged firmware. Built exclusively for Dell commercial PCs as an off-host check, this built-in feature provides this additional level of insight for Intel vPro systems.

Intel vPro Integration for Out of Band Management (OOBM)

Dell has an integration with Intel vPro which provides enhanced security and the ability to remediate and securely wipe a device. The Dell Client Command Suite uses the Intel vPro platform's out of band management capabilities to equip administrators with remote keyboard/video/mouse (KVM) to wake a device, wipe its main drive, or initiate an Intel® Firmware Guard assisted firmware update to reliably reduce the possibility of in-the-field system crashes. The integration of these capabilities provides a unique, multilayer defense-in-depth that improves a SecOps team's effectiveness and efficiency as they protect, correct, and respond to evolving cyberthreats. These capabilities are standard with all Intel vPro equipped devices.

Microsoft Intune Integration

Microsoft Intune is a flexible platform that integrates various services for IT administrators, enabling them to oversee and control a range of devices, including mobile devices, desktop computers, virtual machines, embedded devices, and servers.

Administrators can create compliance policies in the Intune admin center to ensure that SafeBIOS and other Dell 'built-in' capabilities – through the DTD application – are protecting Dell computers below the operating system. DTD uses PowerShell scripts and agent-level configuration to communicate endpoint compliance and transmit results to Microsoft Intune.

The DTD Script folder contains the required script and configuration file which can be imported to create and deploy custom policy in Intune. The result is displayed on the Intune compliance page.

More information and instructions are available here: [Dell Trusted Device – Installation and Administration Guide v7.1 | Dell US](#)

Hardware-Assisted Security | Dell, Intel and CrowdStrike

To provide faster threat detection, Dell worked with CrowdStrike and Intel to deliver an endpoint security solution that brings together the power of hardware and software to enhance threat detection and response. The joint "hardware-assisted security" solution allows administrators to combine CrowdStrike's threat intelligence database with below-the-OS device telemetry for greater insight into potential breaches. With the Dell Trusted Device (DTD) Application enabled, Dell commercial PCs push data from multiple built-in security features to the OS, and surface that data for integration with third-party software solutions. With CrowdStrike Falcon XDR added on-the-box, an admin can collect device security data coming from DTD alerts for further investigation within the CrowdStrike console.

This collaboration enhances software security by providing another layer of defense with improved visibility and observability at the firmware level – an area of the device where we have seen an uptick in malicious and persistent threats in recent years. CrowdStrike software can catch activity deviating from the known good, but Dell device telemetry will also surface rapid alerts from, e.g., Indicators of Attack, to ensure timely response and remediation of an affected device.

Dell PCs provide the visibility and actionability needed to disrupt attacks by leveraging BIOS/firmware protections and (when using Intel vPro) Intel® Control-flow Enforcement Technology (Intel® CET) to help shut down the entire class of ROP attacks. CrowdStrike's Hardware Enhanced Exploit Detection (HEED) integrates Intel® Processor Trace (Intel® PT) CPU telemetry to extend memory safety protections for coded injection techniques, across PC fleet generations.

In addition, CrowdStrike has re-imagined how to stop fileless attacks early in the kill chain by using the accelerated memory scanning algorithms of Intel TDT and its ability to offload processing to the Intel® Graphics Technology integrated graphics processor. The resulting 4-7x performance acceleration helps ensure a performant user experience while applying CrowdStrike's dynamic, earlier, IOAs to the memory layer – and it's only available on Intel® processor-based PCs. As fileless attacks attempt to move down the stack, Dell SafeBIOS uses the Intel vPro platform's Intel® System Resource Defense technology to restrict system privileges and malicious access to the OS.

These capabilities are [described in this solution brief](#).

Below-the-OS Integration with CrowdStrike | Dell on AMD

A similar threat detection capability exists for AMD devices. This joint solution allows administrators to combine CrowdStrike's threat intelligence database with Dell below-the-OS device telemetry for greater insight

into potential breaches. With the Dell Trusted Device (DTD) Application enabled, Dell commercial PCs on AMD push data from multiple built-in security features to the OS, and surface that data for integration with third-party software solutions. With CrowdStrike Falcon XDR added on-the-box, an admin can collect device security data coming from BIOS alerts for further investigation within the CrowdStrike console.

This collaboration enhances software security by providing another layer of defense with improved visibility and observability at the firmware level. CrowdStrike software can catch activity deviating from the known good, but Dell device telemetry will also surface rapid alerts from, e.g., Indicators of Attack, to ensure timely response and remediation of an affected device.

Below-the-OS Integration with Absolute | Dell on Intel, Dell on AMD

To strengthen endpoint resilience and improve visibility, Dell partnered with Absolute to deliver a solution that combines Dell's hardware-based security with Absolute's firmware-embedded persistence technology. This integration ensures that security controls remain active and tamper-proof, even if the operating system is reinstalled or the device is wiped.

With Dell Trusted Device (DTD) capabilities enabled, Dell commercial PCs provide telemetry from below-the-OS security features, which Absolute leverages to maintain continuous visibility and control. Absolute's Persistence® technology, embedded in the Dell BIOS, guarantees that the Absolute agent can self-heal if removed or corrupted—providing IT teams with an unbreakable connection to every endpoint.

This collaboration enhances endpoint security by delivering real-time insights into device health, compliance, and risk posture. Administrators can monitor critical security applications, detect anomalies, and remediate threats remotely, even when devices are off-network. By combining Dell's hardware root of trust and BIOS protections with Absolute's resilience platform, organizations gain a layered defense that extends beyond traditional software-based approaches.

The result is a security foundation that is both persistent and adaptive, helping businesses maintain compliance, reduce risk, and respond quickly to emerging threats. Together, Dell and Absolute deliver the visibility and control needed to protect endpoints in today's dynamic threat landscape.

Other Integrations

Security Information and Event Management (SIEM) solutions play a critical role in enhancing the cybersecurity posture of organizations by providing comprehensive tools for real-time monitoring, analyzing, and responding swiftly to security events. These solutions collect and aggregate log data generated throughout the organization's technology infrastructure, including networks, applications, and endpoints. SIEM tools leverage advanced analytics and correlation algorithms to identify patterns and anomalies in the data, helping security teams detect and investigate potential security incidents.

Dell Trusted Device (DTD) can interoperate with SIEM solutions and supports the following features:

- BIOS Verification
- Intel ME Verification / AMD Security Processor Verification
- BIOS Events & Indicators of Attack

- Image Capture
- Security Score
- CVE Detection & Remediation
- Secured Component Verification

The Dell Event Repository must be installed to deliver DTD results to a SIEM solution.

Respond and Recover

From the NIST framework:

Respond: Develop and implement appropriate activities to respond to a detected cybersecurity incident.

Recover: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Respond and Recover are often overlooked functions within the NIST Cybersecurity Framework. Admitting that a failure or attack has occurred or that an unknown vulnerability has been exploited by an adversary can be uncomfortable at times. Being well prepared to handle these incidents and having the confidence to be able to restore the Dell device back to normal operating status as quickly and efficiently as possible can help to minimize the overall cost of these events.

Embedded Controller (EC) Recovery

As mentioned previously, the Dell device embedded controller, or EC, operates as the root of trust of the system at the very lowest level of hardware enablement. This privileged context and critical role requires a high degree of fault tolerance to avoid false positives and keep the beginning of the chain of trust intact, secure, and resilient. To address this, the Dell device EC supports dual firmware images and a failover mode to allow backup firmware to recover the primary image if needed.

BIOS Recovery

In addition to having a secure and resilient EC, it is also critical for the next stage of the boot process that the BIOS, also has a robust recovery mechanism. Dell PCs have a sophisticated set of flexible and tunable features that ensure that the BIOS can be reverted to a known-good copy if compromised. Additionally, once BIOS recovery is invoked, it will securely capture the state of tampering for offline analysis (described in the previous sections) for those customers that require deep insight into their adversaries' techniques.

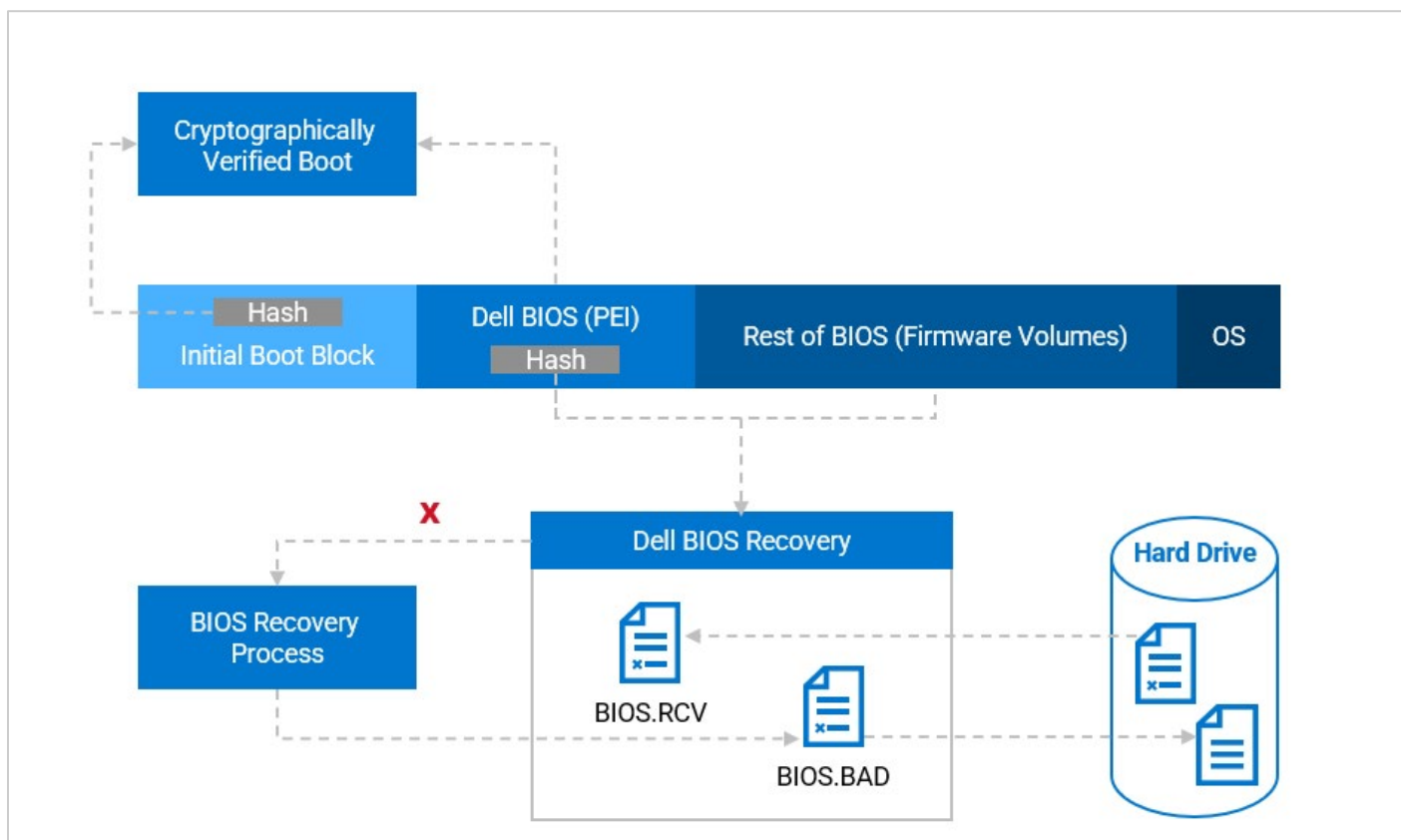


Figure 12: BIOS Recovery Flow

BIOS Recovery Image Update Flow

BIOS recovery is engineered into the Dell BIOS update architecture. Each Dell device is prepared days, months, or even years before any potential trigger to recover is ever required. Essentially this is part of every BIOS update on the system. In addition to updating the BIOS running on the system the BIOS update tool will copy a recovery version of the new BIOS to the secure EFI partition on the hard drive. The EFI partition is a hidden partition that is independent of the operating system HDD/SSD drive partitions. Microsoft Windows uses the EFI System Partition (ESP) as the critical storage area for boot-related files.

When a PC with BIOS (UEFI) firmware starts, the firmware loads boot files from the EFI partition, which contains the Windows Boot Manager, boot configuration data, and other utilities needed to initialize the operating system.

This partition is modifiable with physical or OS administrative access, so it's important to note that the recovery image is signed in the same manner as the updated version and verified by the BIOS RTU prior to performing recovery.

BIOS Recovery

BIOS Recovery from Hard Drive – This option is set by default. Allows you to recover the corrupted BIOS from a recovery file on the HDD or an external USB key.

BIOS Auto-Recovery – Allows you to recover the BIOS automatically.



NOTE: BIOS Recovery from Hard Drive field should be enabled

Auto Recovery Flow

Dell devices can be configured to automatically recover the BIOS to a known-good copy when the early BIOS code detects an integrity violation during pre-boot. To support this, the early BIOS (the Pre-EFI Initialization phase, or PEI, in UEFI terminology) can read the BIOS recovery image from the hard drive or USB and verify the signature of the recovery image using the same Root of Trust for Update (RTU) that protects the BIOS update process (i.e. NIST 800-147).

Customer Flexibility: Manual Recovery

The BIOS Auto-Recovery option is disabled by default on Dell devices. This may at first seem misaligned with the overall security and threat model assumptions of the Dell device. However, this default was designed to support customers whose threat models prioritize detection of BIOS tampering or corruption well above the need for high availability/resilience that may mask potential adversarial activity.

Confirming BIOS Integrity

All Dell commercial BIOS are checked during boot (or per schedule in managed environments) against an off-host, Dell hosted 'golden image' using the BIOS verification capability. This ensures that, whatever the source may be for the replacement BIOS image, the code is always secure and correct for that specific PC. This removes the need to protect a BIOS image with a level of hardware protection used, for instance, for personal credentials, since this off-host check ensures the validity of the code.

Dell Data Sanitization

Dell devices produced since 2017 include the Dell Data Sanitization feature. Dell Data Sanitization allows customers to securely delete data on the internal storage devices in their Dell device. This allows efficient erasure for repurpose or redeployment using industry standard commands based on the NIST 800- 88r1 and IEEE-2883 standards. The feature is supported on internal SATA, SSD, NVMe and eMMC storage devices. It uses industry standard methods such as Enhanced Security Erase for SATA, format NVM for NVMe, and Sanitize for eMMC based devices. (See [NIST Special Publication 800-88r1](#) Guidelines for Media Sanitization and [IEEE Standard for Sanitizing Storage](#) for more details.)

Dell Data Sanitization removes all user data from the storage device. To protect the device from unauthorized wipe of media, the feature is only accessible by a physically present user through the BIOS Setup (F2) interface. Any user who has access to the BIOS Setup Menu can initiate the wipe. The user interface includes multiple confirmation prompts to ensure data wipe cannot be triggered accidentally. So, the user must be physically present until data wipe begins. Once initiated, the data wipe will proceed until all storage devices are wiped.

- Allows user-initiated data wipe of internal storage devices (SATA/SSD/NVMe/eMMC) using industry standard technology.

- Invokes acceptable media purge per NIST SP 800-88 r1 and IEEE-2883 by invoking media specific commands.
- User interface includes multiple confirmation prompts to ensure data wipe cannot be triggered accidentally.
- Commonly referenced DoD 5520.22-m “multi-pass” requirements were defined before ATA SECURITY ERASE and sanitization method table has been removed from 5520-m. NIST SP 800-88r1 and IEEE-2883 both widely accepted as more relevant data sanitization standards, include storage technologies such as NVMe, SSD, etc.

More information about Dell Data Sanitization is available [here](#).

OS Recovery: Dell BIOSConnect

Although not strictly within the scope of below-the-OS security, questions are often asked from the security perspective as to how the operating system may be restored. One way in which this is accomplished is through Dell BIOSConnect, a firmware-resident, network-aware recovery mechanism implemented in the Dell UEFI stack.

BIOSConnect extends Dell’s UEFI firmware with a secure, cloud-integrated recovery service that operates independently of the local operating system. When invoked (either by user selection or as a boot-failure fallback), the firmware initializes an embedded network stack, acquires IP configuration, and establishes a TLS-protected connection to Dell’s recovery infrastructure using OEM-provisioned certificate authorities for server authentication. Over this channel, the platform transmits device identity attributes (such as service tag and platform ID) and requests a model-appropriate recovery payload. The returned image is a UEFI-bootable, Dell-signed recovery environment that is downloaded to memory or temporary storage and validated cryptographically before execution. BIOSConnect then registers a transient UEFI boot entry and transfers control to the verified image, enabling operating system reinstallation and diagnostics even on a blank or corrupted disk. This design provides a hardened, end-to-end path for OS recovery and complements other below-the-OS controls such as SafeBIOS and Secured Component Verification.

For more information, please refer to the Dell Knowledge Base article, “[Using BIOSConnect to Boot to SupportAssist OS Recovery](#)”.

Dell includes physical threats, time-based risk analysis, and persistent storage in the threat model assumptions.

Additional Dell Security Features and Capabilities

Below-the-OS Threat Modeling

Threat modelling is the exercise of using an adversarial mindset to evaluate computer architectures to determine potential vulnerabilities or attack surface early in the development phase. These exercises are

critical to ensure that any latent vulnerabilities are identified and remedied during development. Ongoing programs address client devices in-use as attackers develop new targeted threats.

Most publicly available threat modelling information is focused on software designed to be deployed as web applications or to cloud architecture. Dell uses this powerful tool not only for web and application software, but also as part of the SDL process for BIOS and firmware. Dell includes physical threats, time-based risk analysis, and persistent storage in the threat model assumptions for Dell devices. These expanded assumptions have proven to be significant improvements in finding and mitigating potential vulnerabilities in BIOS, firmware, and hardware design.

Just as hardware and software threat models differ, so do Dell customers' threat models. For example, not every customer includes "Below-the-OS" threats in their own threat models, but a growing number do. Using the most security-sensitive customers' threat models as a baseline for our own allows Dell to design devices that are resilient against the most sophisticated adversaries in addition to the more common threats. Penetration testing, or 'pen-testing', is a form of product validation where authorized attacks are performed for internal evaluation. This has become synonymous with mature security practices across the industry. Dell leverages both in-house teams and external vendors to pen-test Dell devices while these products are still in the engineering phases of development. Like the threat model assumptions made above, these tests focus on physical access and are prioritized based on risk assessments of individual components integrated into Dell devices.

Protected Signing Infrastructure

Code signing and protecting access to private keys and certificates within the signing infrastructure is a critical piece of any software or firmware supply chain. Once again, this vital component of the supply chain is also an area most targeted by sophisticated adversaries.

Threat: Unauthorized Code Signing

There are countless examples of supply chain attacks that resulted in stolen digital signing certificates or credentials being used to sign malware. The danger in this scenario is that it is challenging for customers, anti-virus software, and existing tools to differentiate between legitimate and potentially malicious code signed with the same certificate. One example of this activity can be found [here](#). To add to the growing risk of these sophisticated attacks, quantum computing is poised to undermine the cryptography that protects firmware integrity.

Mitigation: Signing Infrastructure

Dell devices use secure signing infrastructure and hardware security modules, or HSMs, for code signing. This infrastructure is managed by Dell Cybersecurity, includes disaster recovery mechanisms, and is protected from unauthorized access using user access control and hardware binding. The Dell device BIOS signing capability is integrated directly into the automated build processes and developers do not have direct access to sign BIOS updates. This infrastructure signs the outer encapsulated BIOS update and Cryptographically Verified Boot (on Intel devices, this includes: Intel Boot Guard initial boot block (IBB) and Intel BIOS Guard code updates; on AMD devices: AMD Platform Secure Boot, AMD ROM and SPI Write Protection code updates).

Note: The commercial platforms launching in 2026 will leverage Leighton-Micali Signature (LMS) algorithm for payload signing for both the embedded controller (EC) and BIOS updates to help meet emerging Commercial National Security Algorithm (CNSA) Suite 2.0 requirements defined by the United States National Security Agency (NSA) for quantum-safe security.

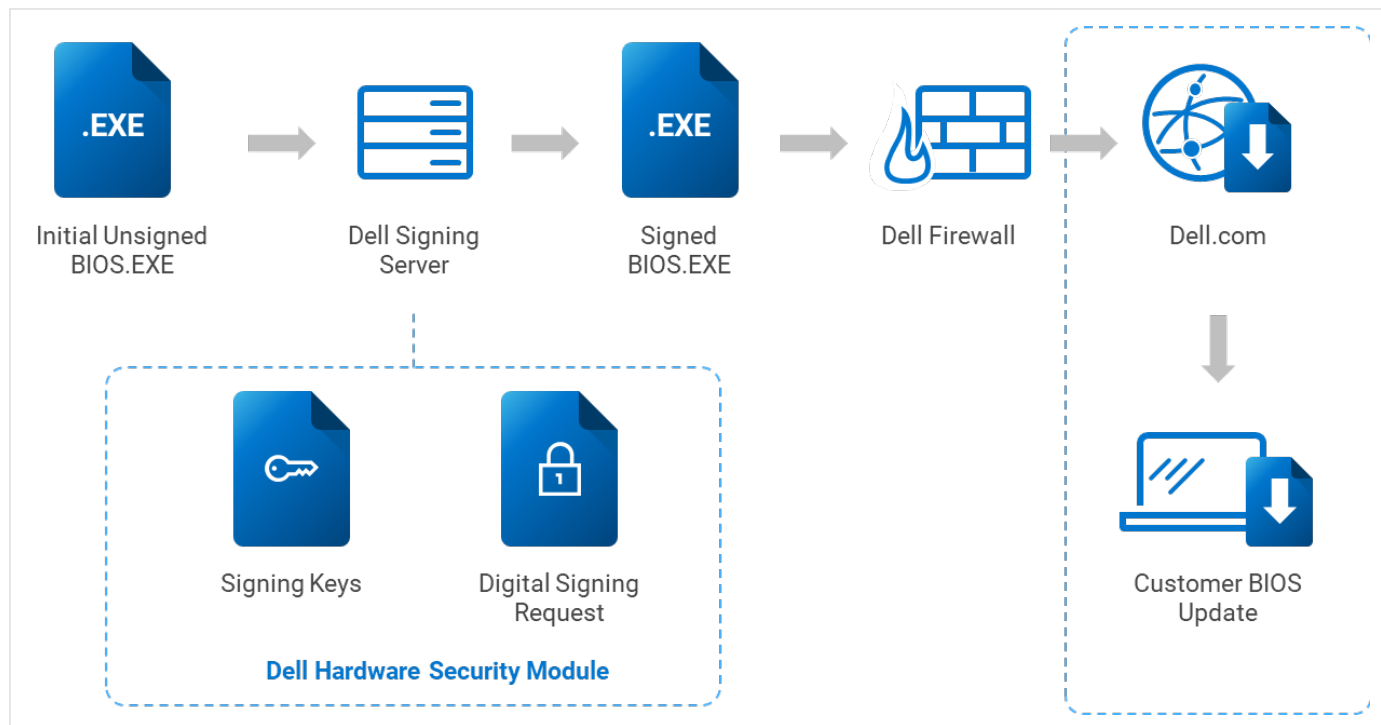


Figure 13: Dell SafeBIOS Signing

The Future of Security

Organizations rely on hardened endpoints to defend against modern and sophisticated adversaries and Dell has invested heavily in the security and resilience of the Dell devices to meet this demand. Transparency remains a critical tenet in computer security and hopefully this document has served to provide a comprehensive look into not only the details and intentions behind these features but also some of the limitations.

We understand that Dell devices are only one piece of the security puzzle for our customers. While our investments in device hardening are an important foundation for overall ecosystem security, we continue to prioritize integrations with security software and solutions that help customers maximize the benefits of what we've built. Integrating into security ecosystems and architectures such as Zero Trust ensure Dell telemetry can be used to enrich user and network access policy tied to the health of the device. This rich telemetry evolves as the landscape evolves and it's exciting to help build the future integrations across not only Zero Trust but to create the basis of data to take full advantage of the AI security evolution over the coming years.

References

Dell and Partner References

- [A Partnership of Trust: Dell Supply Chain Security](#)
- [Achieving pervasive security](#) – Dell Technologies and Intel, June 2025
- [Dell, Intel and CrowdStrike – Joint Solution Brief](#)
- [BIOS Security – The Next Frontier for Endpoint Protection](#) – A Forrester Consulting Thought Leadership Paper Commissioned by Dell – June 2019
- [UEFI on Dell BizClient Platforms](#)
- [Intel Hardware Shield](#)
- Dell KB [Find Your Service Tag or Serial Number](#)
- Dell KB [Using Dell Command Configure to Set the Asset Tag Information of Your Dell Computer](#)
- Dell KB [Dell Data Wipe](#)
- [Dell Trusted Workspace | Dell Endpoint Security webpage](#)
- [Dell SafeBIOS Datasheet](#)
- [Dell SafeID Datasheet](#)
- [Dell SafeSupply Chain Datasheet](#)
- [Dell Secured Component Verification \(SCV\) Datasheet](#)
- [Dell Trusted Device Application Solution Brief](#)
- [Dell Trusted Device – Installation and Administration Guide](#)
- [Dell Client Signed Firmware Update](#)
- [Principled Technologies Most Secure Study ft. Intel](#)
- [Dell Device Security Practices Article](#)
- [Dell Secure AI PC Design Article](#)
- [Dell Anatomy of a Trusted Device Infographic](#)
- [Dell Endpoint Security Blogs](#)

Industry Organizations

- UEFI Tianocore Project – <https://github.com/tianocore/edk2>
- [SAFECode](#) – The Software Assurance Forum for Excellence in Code
- [TCG](#) – Trusted Computing Group

- [FIRST](#) – Forum of Incident Response and Security Teams
- [OTTF](#) – Open Group Trusted Technology Forum
- [IEEE Center for Secure Design](#)

Standards and Guidelines

- [NIST Cybersecurity Framework](#) – NIST Publication "The NIST Cybersecurity Framework (CSF) 2.0" - February 26, 2024
- [NIST Cybersecurity Framework](#) – Main Page
- [NIST Special Publication SP 800-193](#) – Platform Resiliency Guidelines
- [NIST Special Publication SP 800-147](#) – BIOS Protection Guidelines
- [NIST Special Publication SP 800-88 \(r1\)](#) – Guidelines for Media Sanitization
- [NIST Special Publication SP 1800-34](#) – Validating the Integrity of Computing Devices
- [FIPS Publication 186-5](#) – Digital Signature Standard (DSS)
- [National Security Agency Cybersecurity Report UEFI Defensive Practices Guidance](#)
- NSA Cybersecurity Information Sheet: [Procurement and Acceptance Testing Guide for Servers, Laptops, and Desktop Computers](#)
- [ISO/IEC 27034-1:2011](#) – Information Security Techniques for Application Security

Quoted Stats

- [Estimated cost of cybercrime worldwide 2017 – 2028](#) – Statista.com

Disclaimer

The Most Secure Commercial AI PCs claim and related claims about Dell's unique built-in security: Based on Dell internal analysis, October 2025 (Intel) and March 2026 (AMD). Applicable to PCs on Intel and AMD processors. Not all features available with all PCs. Additional purchase required for some features. Intel-based PCs validated by [Principled Technologies](#), July 2025.