

Client Solutions Dell Trusted Device: BIOS Security

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

May 2025



© 2025 Dell Inc. or its subsidiaries. All Rights Reserved. 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 2024. Applicable to PCs on Intel processors. Not all features available with all PCs. Additional purchase required for some features. Validated by Principled Technologies. [A comparison of security features](#), April 2024.

Table of Contents

Introduction	4
The Key Elements of Dell Built-In Security.....	6
The Role of BIOS (and what is UEFI?)	6
Secure Design Processes and SDL	7
Supply Chain Security	7
Industry Affiliations	8
Built-In, “Below the OS” Security.....	9
Dell Trusted Device (DTD) Application.....	10
The Importance of Built-In Security	10
Intel® vPro Additions to Built-In Security	11
Understanding Dell Cybersecurity Using the NIST Framework	11
Identify	12
Device Identity	13
User Identity: Dell SafeID.....	14
“Below the OS” Threat Modeling	15
Protect.....	15
Protecting the PC Boot Process.....	16
Securing the Boot Chain	16
The “Root of Trust”	17
TCG and the Root of Trust	17
UEFI Secure Boot.....	17
UEFI Secure Boot Expert Mode	18
Signed Firmware Update.....	18
NIST SP800-147 Support	19
System Management Mode (SMM)	19
BIOS Patch Management.....	21
BIOS Downgrade Protection	22
Embedded Controller: Signed Firmware	22
Protecting BIOS Configuration	22
Configuration Side-Channels	24
Best Practices for Secure Configuration	25
Protecting BIOS at Runtime	25

Runtime BIOS Resilience.....	25
Detect.....	26
Intel Boot Guard.....	26
Intel Management Engine (ME) Firmware Verification.....	27
Hardware-Assisted Security with CrowdStrike and Intel.....	28
Intel® vPro Integration for Out of Band Management.....	28
Microsoft Intune Integration.....	29
Other Integrations for SafeBIOS.....	29
SafeBIOS Indicators of Attack.....	29
Common Vulnerabilities and Exposures (CVE) Detection.....	31
TCG Measured Boot.....	31
Code, Configuration, and the TPM Event Log.....	31
NIST 800-155 Measurements.....	32
Advanced: NIST 800-155 Measurements Extraction, Conversion, and Comparison.....	33
Physical Security Features – Chassis Intrusion.....	34
Respond and Recover.....	34
Embedded Controller Recovery.....	35
BIOS Recovery.....	35
BIOS Recovery Image Update Flow.....	36
Auto Recovery Flow.....	37
Customer Flexibility: Manual Recovery.....	37
SafeBIOS Image Capture.....	37
Dell Data Wipe.....	37
Additional Dell Security Capabilities.....	38
Protected Signing Infrastructure.....	38
The Future of Security.....	39
References.....	39
Dell and Partner References.....	39
Industry Organizations.....	40
Standards and Guidelines.....	40
Quoted Stats.....	40

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 an estimated \\$8.15 trillion USD in 2023](#). 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 and effective portfolio of technologies and solutions – both hardware and software – in this industry to help organizations strive to secure their enterprises. 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 step further through integration with software (EDR/XDR and SIEM) and device management solutions such as Microsoft Intune to enable organizations to take appropriate action and analyze a threat to improve response effectiveness.

Since this paper was originally published, Dell device security has expanded to include additional built-in security features from Intel® vPro. Though mention will be made, for more in-depth information there is a separate paper dedicated to those features that may be [downloaded here](#).

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. 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 (DTD) Application 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., SafeBIOS 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 like 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 Built-In Security

The Role of BIOS (and what is UEFI?)

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 architectures well beyond Intel® x86-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.

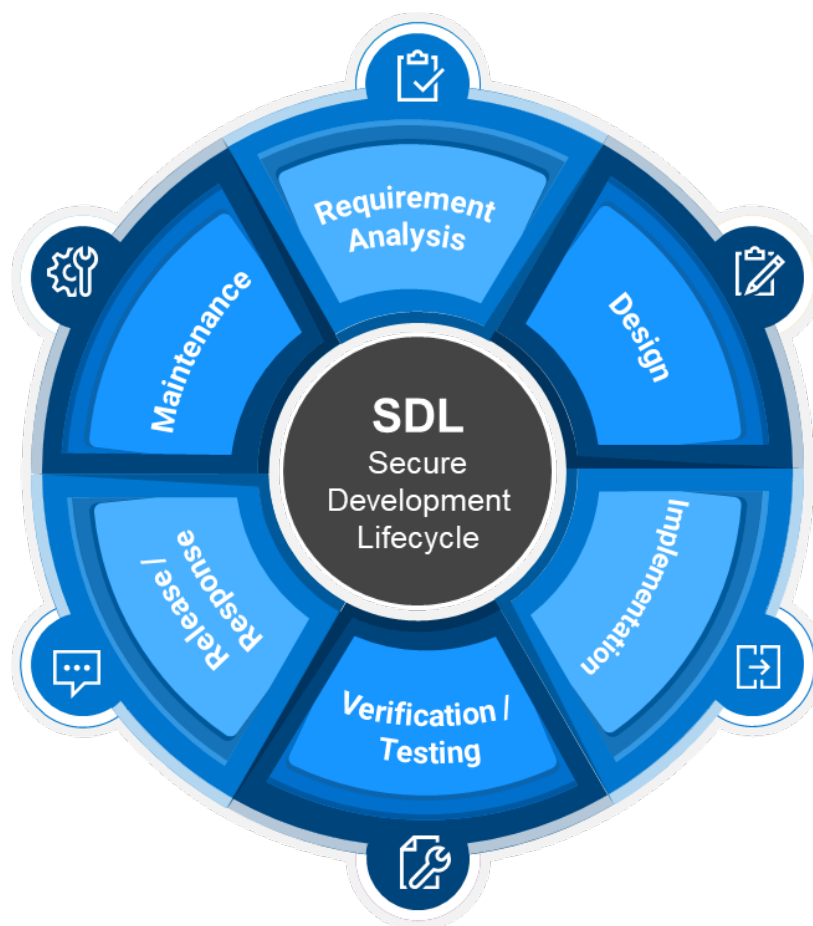


Figure 1: Dell EMC Secure Development Lifecycle

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](#).

The following excerpt is a high-level description of many of the Dell device BIOS protection mechanisms that have been covered in-depth in this document:






- Dell has implemented procedures across our commercial servers, 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 part of the supply chain from the customer perspective. Luckily, this means that the investments in the features covered in this document can help assist and augment traditional supply chain security. For example, the SafeBIOS verification check is part of the manufacturing process of every commercial device that Dell produces.

Industry Affiliations

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.

Built-In, “Below the OS” Security

	Dell Unique	Industry Standard
 Identify	Dell Identity and Asset Management Tags	<ul style="list-style-type: none"> • Service Tag • Asset Tag
 Detect	<ul style="list-style-type: none"> • Discrete TPM • Dell SafeBIOS Verification • Dell SafeBIOS IoA/loC • Dell Secured Component Verification (SCV) • Intel® ME Firmware Verification • CVE Detection 	<ul style="list-style-type: none"> • Runtime BIOS Resilience • TCG Measured Boot • Downgrade Protection
 Respond	<ul style="list-style-type: none"> • Dell SafeBIOS Image Capture • Dell Trusted Device telemetry 	Dell BIOS Recovery
 Protect	<ul style="list-style-type: none"> • Fused Root of Trust • Dell UEFI Secure Boot • BIOS Passwords 	<ul style="list-style-type: none"> • Intel® BIOS Guard • Intel® Boot Guard • Authenticated Updates • BIOS Public Keys
 Recover	<ul style="list-style-type: none"> • Dell BIOS Connect • Dell Support Assist 	Windows OS Recovery

As mentioned in the introduction, 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 protections 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 the Dell commercial client protections and Dell SafeBIOS security comes in.

Dell refers to this stable foundation as Built-In, “Below the OS” security. Based on the analogy above, 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 (DTD) Application

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

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

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. 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 Dell Trusted Device local console.

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

The Importance of Built-In 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.

* Based on Dell internal analysis, September 2023. Applicable to PCs on Intel processors. Not all features available with all PCs. Additional purchase required for some features.

Other 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.

It's clear that industry and customer interest for built-in, "Below the OS" and firmware/BIOS 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.

Intel® vPro Additions to Built-In Security

With Intel vPro enabled 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 the SafeBIOS IoA.

Understanding Dell Cybersecurity Using the NIST Framework

Cyber security 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 to 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>.

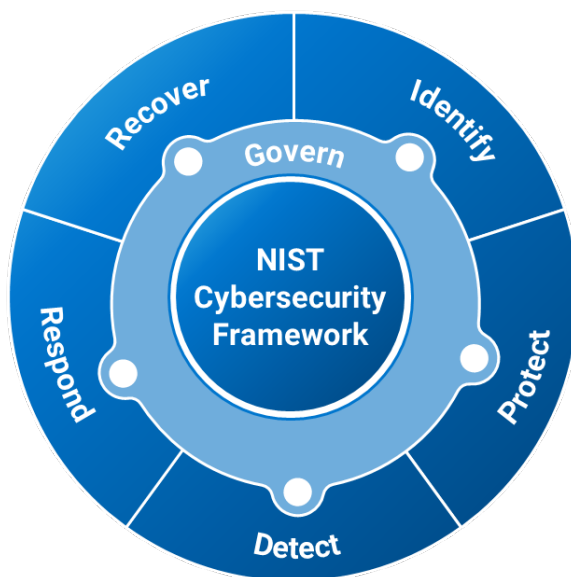







Figure 2: CSF Functions

Dell implements this framework using both Industry Standard and Dell Unique capabilities.

	Dell Unique	Industry Standard
 Identify	Dell Identity and Asset Management Tags	<ul style="list-style-type: none"> • Service Tag • Asset Tag
 Detect	<ul style="list-style-type: none"> • Discrete TPM • Dell SafeBIOS Verification • Dell SafeBIOS IoA/IoC • Dell Secured Component Verification (SCV) • Intel® ME Firmware Verification • CVE Detection 	<ul style="list-style-type: none"> • Runtime BIOS Resilience • TCG Measured Boot • Downgrade Protection
 Respond	<ul style="list-style-type: none"> • Dell SafeBIOS Image Capture • Dell Trusted Device telemetry 	Dell BIOS Recovery
 Protect	<ul style="list-style-type: none"> • Fused Root of Trust • Dell UEFI Secure Boot • BIOS Passwords 	<ul style="list-style-type: none"> • Intel® BIOS Guard • Intel® Boot Guard • Authenticated Updates • BIOS Public Keys
 Recover	<ul style="list-style-type: none"> • Dell BIOS Connect • Dell Support Assist 	Windows OS Recovery

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.
- Platform certificate-based machine identity which enables device health through proof of authenticity and supply chain assurance.
- 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

Supply chains can be vulnerable to disruptions such as tampering, theft, 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 to root-of-trust for device identity, health, and authenticity.

User Identity: Dell SafeID

Dell SafeID keeps user credentials safe 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.

Two options are available:

- Dell SafeID with discrete TPM
- Dell SafeID with ControlVault 3+. CV3+ is unique to Dell* and FIPS 140-3 level 3 certified.

Dell SafeID with discrete TPM: 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.

Dell SafeID with ControlVault: SafeID 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 Precision Mobile and Latitude 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).

- **Isolated Processing & Storage: Dell ControlVault**

ControlVault's ARM Cortex A7 1GHz processor and storage is not only outside-validated, FIPS 140-3 level 3 certified – 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 (on certain platforms with FIPS fingerprint reader).

- **Certifications**

EMVco v4.3d, WQHL, NFC Forum, PCI PTS POI, FIPS 140-3 lvl3 & FIPS 201-3

No other embedded PC biometric solution has achieved this level of external validation from NIST.*

**Based on Dell internal analysis, October 2024. Applicable to PCs on Intel processors. Not all features available with all PCs. Additional purchase required for some features. Validated by Principled Technologies. A comparison of security features, April 2024.*

To learn more about Dell SafeID, read our [datasheet](#).

“Below the OS” Threat Modeling

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

Most threat modeling information that is publicly available is focused on software designed to be deployed as web applications or to cloud architectures. 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 has started to include 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.

Dell has started to include physical threats, time-based risk analysis, and persistent storage in the threat model assumptions

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

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 model, 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.

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.

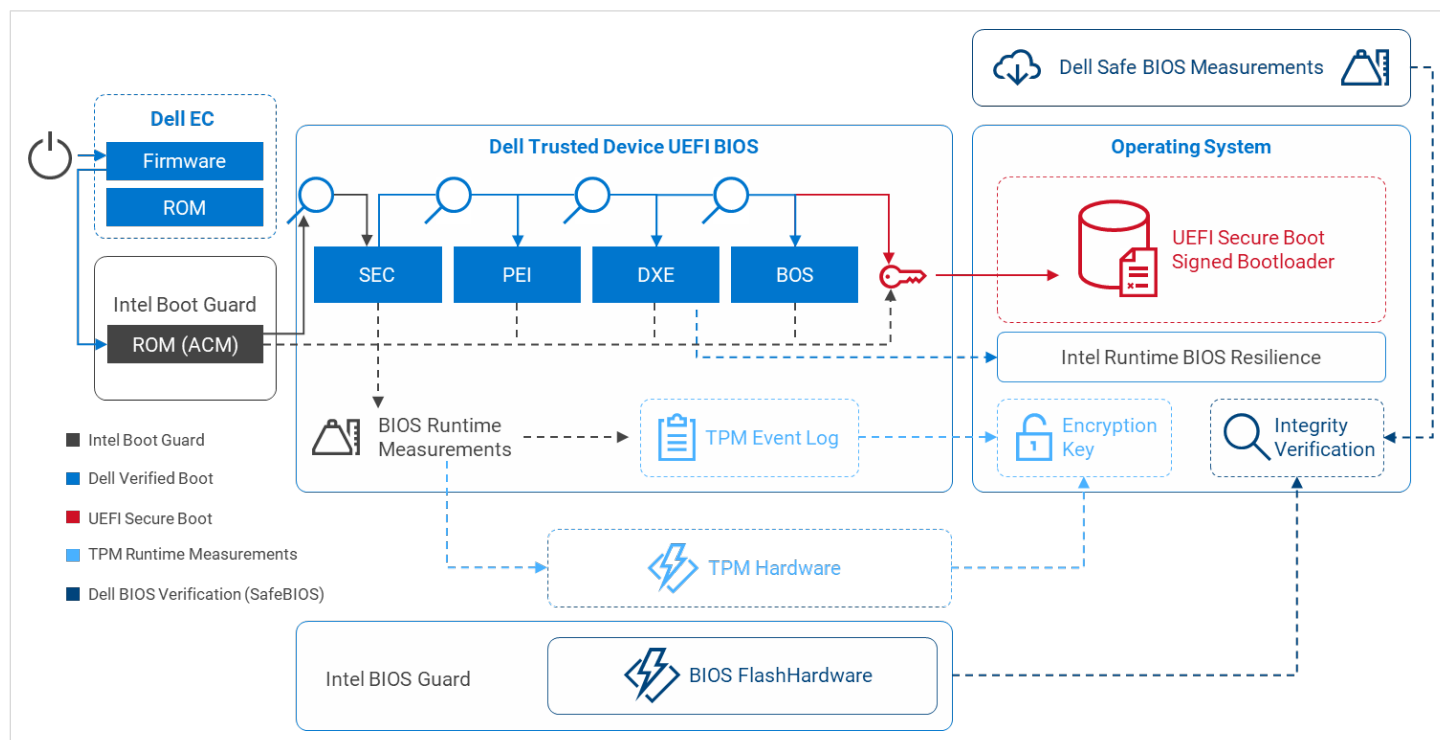


Figure 3: Dell Trusted Device Boot Chain

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 and/or main processor come out of reset, to the point of handoff to an operating system like Microsoft Windows™ 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.

The illustration in Figure 3 depicts a high-level overview of the major components in the Dell device boot chain. Many of these components, like the Embedded Controller (or EC), 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 is the origin point upon which all subsequent trusted events are built. For modern PCs, the processor reset vector is often considered the root of trust. This is the first instruction that the processor fetches after coming out of reset.

Again, in practice it's a bit more complicated than that. Dell devices include both an embedded controller (EC) and typically an Intel® Converged Security and Management Engine (CSME) or AMD® Platform Security Processor (PSP) that execute firmware before the processor wakes up. The Dell EC is the hardware root of trust for these devices since it runs cryptographically verified code that manages the power controls which bring the x86 chipset out of its low-power state. This root of trust boot flow continues by chaining the Intel CSME or AMD PSP to the Dell EC, followed by the BIOS. This flow is like that in Dell devices that contain ARM-based architecture(s).

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. The 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.

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.

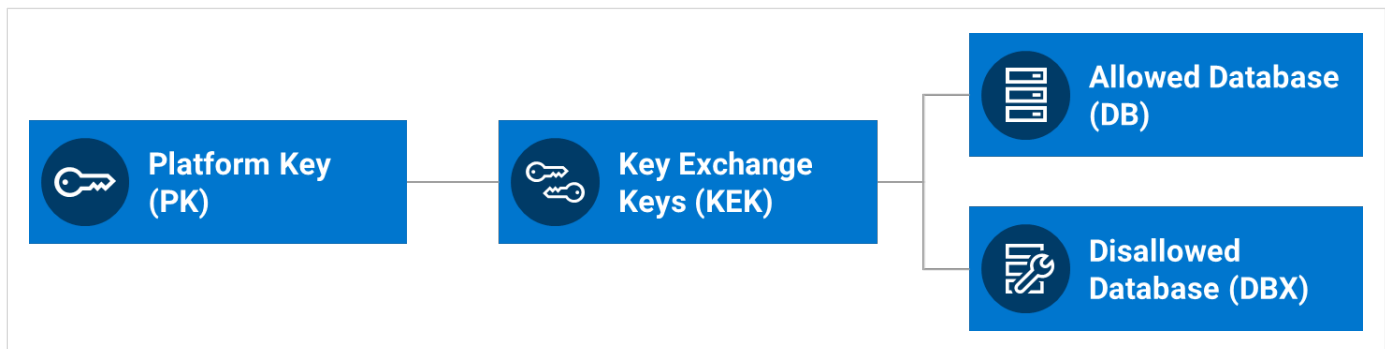


Figure 4: Secure Boot Key Hierarchy

UEFI Secure Boot Expert Mode

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 engine integrates Custom Mode Key Management that allows administrators to modify the entire contents of the UEFI Secure Boot key management database directly. 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 incompatibilities with hardware and software.

Signed Firmware Update

Previous sections detailed how the 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 SP800-147 Support

Dell puts significant effort into hardening the BIOS protection and authentication capabilities on its client devices in accordance with [NIST SP800-147](#) 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)

System Management Mode, or SMM, is a privileged mode of the processor architected 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. For Arm-based Architecture(s) the Secure Partition Manager, or SPM, would be applied by Trusted Firmware.

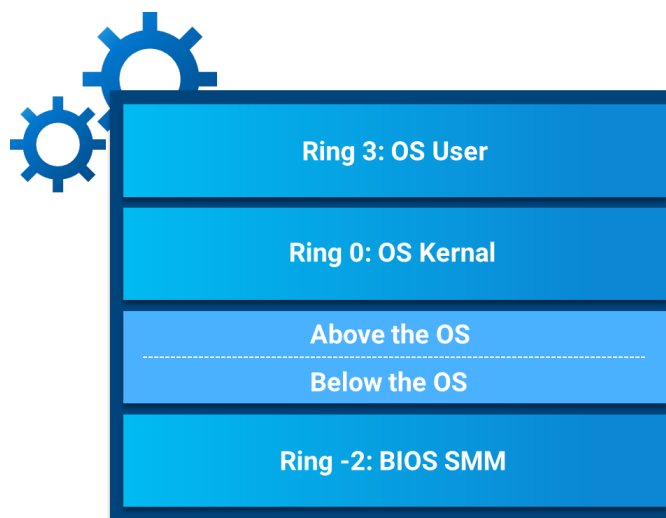


Figure 5: Modern PC Ring Architecture

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 technology 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**

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 the 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 the 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.

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 10/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 User 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.

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	<p>Allows you to set, change, or delete the administrator (admin) password.</p> <p>The entries to set password are:</p> <ul style="list-style-type: none"> • Enter the old password: • Enter the new password: • Confirm new password: <p>Click OK once you set the password</p> <div data-bbox="394 1780 488 1896">  </div> <p>NOTE: For the first time login, "Enter the old password:" field is marked to "Not set". Hence, password has to be set for the first time you login and then you can change or delete the password</p>

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.

Runtime BIOS Resilience

Intel has been another valuable 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 Hardware Shield capabilities, [refer to this paper](#).

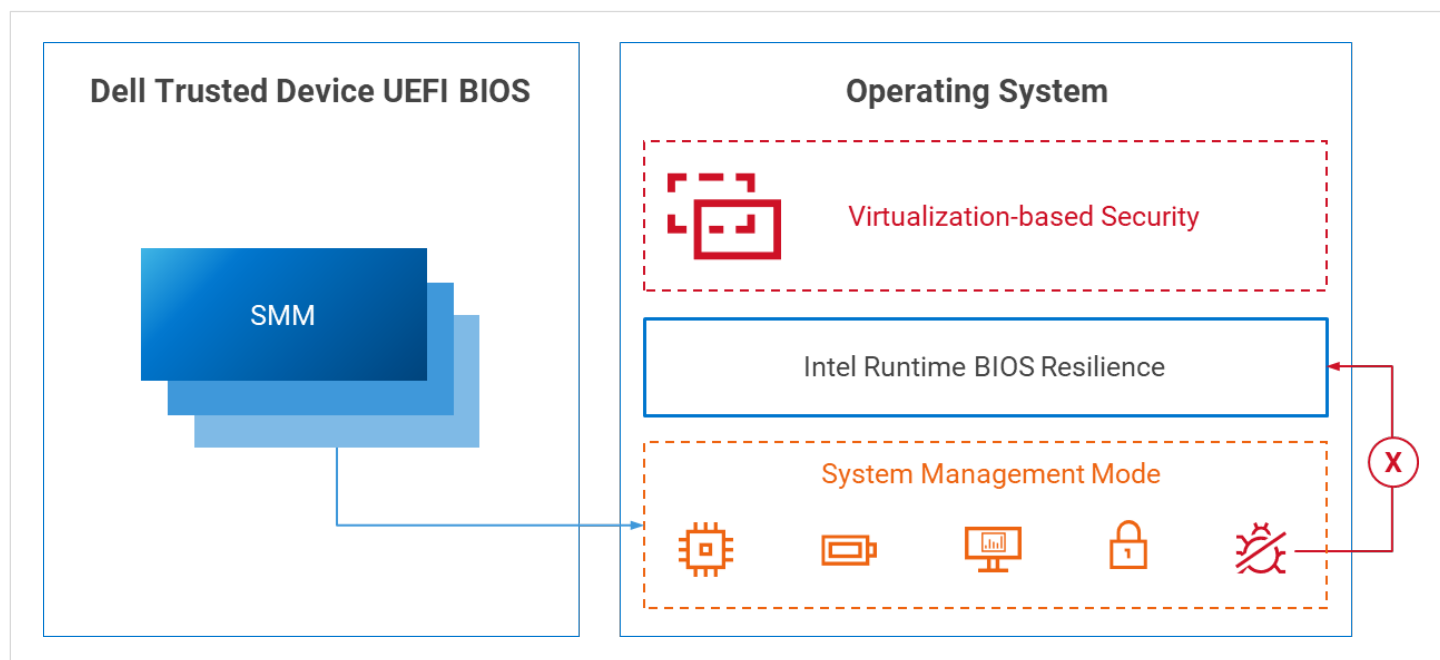


Figure 6: Intel Runtime BIOS Resilience

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.

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, to limit any further adversary activity, and to reduce the overall incentive for tampering.

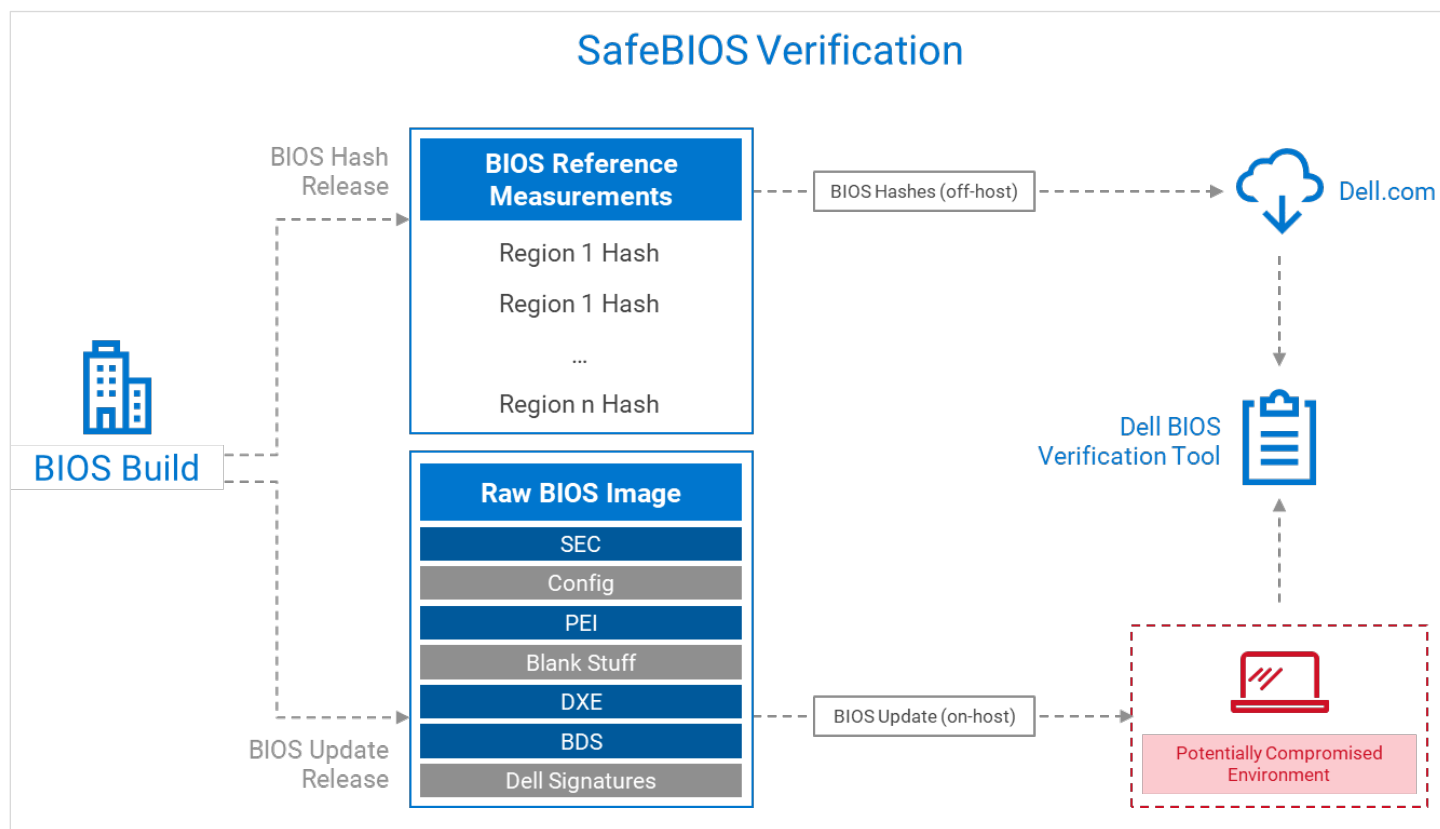


Figure 7: SafeBIOS Verification Flow

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. Dell commercial PCs have a feature called SafeBIOS Verification that addresses both concerns. SafeBIOS 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 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 within the SafeBIOS framework provides this additional level of insight for Intel vPro systems.

Hardware-Assisted Security with CrowdStrike and Intel

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 SafeBIOS 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 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., SafeBIOS 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 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 performance⁹ 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.

The solution is [described in this solution brief](#).

Intel® vPro Integration for Out of Band Management

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 come 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 in Intune compliance page.

More information and instructions are available here: [Dell Trusted Device – Installation and Administration Guide v6.0 | Dell US](#)

Other Integrations for SafeBIOS

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
- BIOS Events & Indicators of Attack
- Image Capture
- Security Score
- CVE Detection

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

SafeBIOS Indicators of Attack

Dell SafeBIOS 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 SafeBIOS IoA feature addresses this gap by using Dell threat modeling 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. 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.

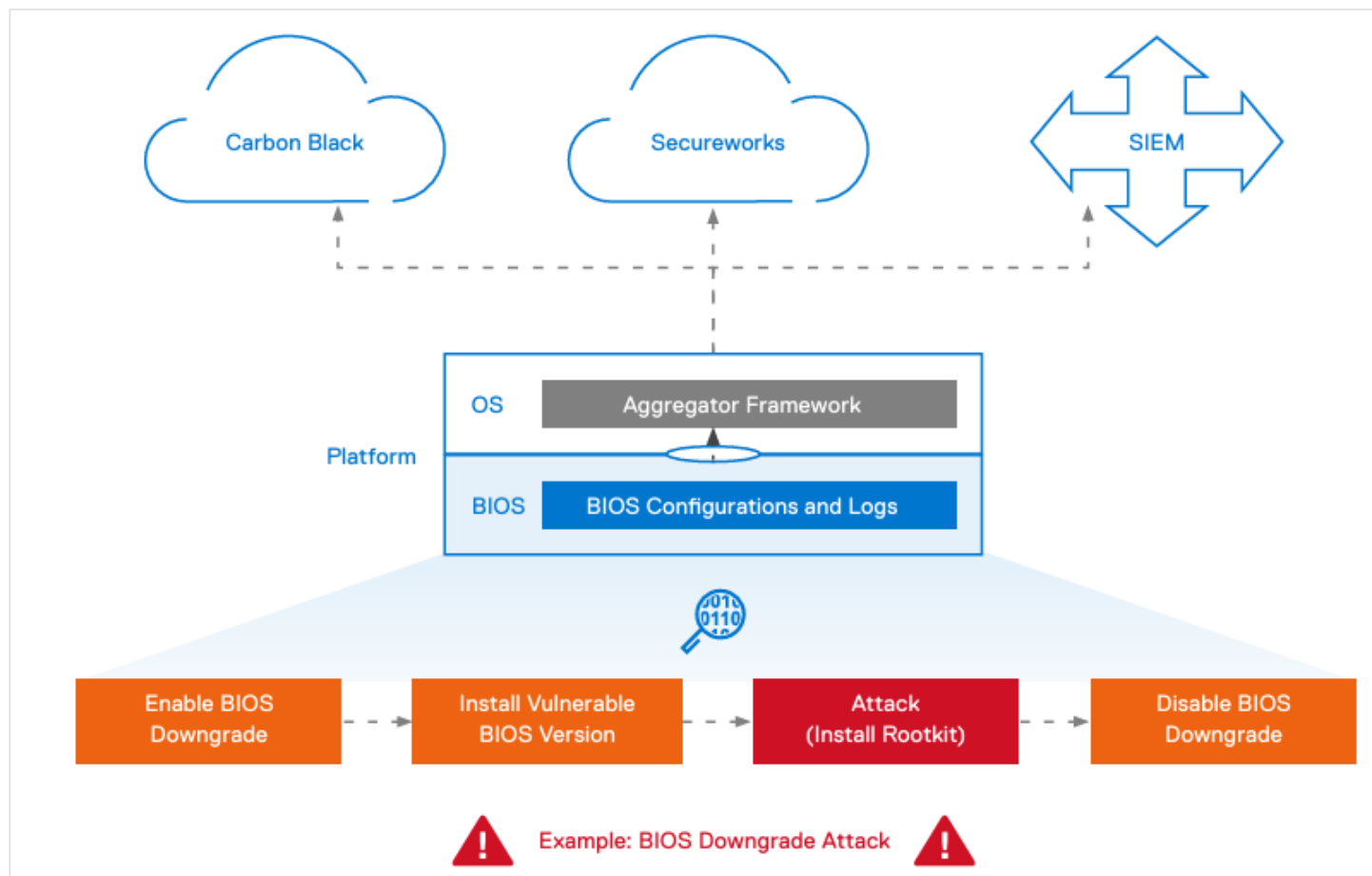


Figure 8: SafeBIOS Indicators of Attack

Common Vulnerabilities and Exposures (CVE) Detection

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

- CVE Detection 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.
- CVE Detection also scans for vulnerabilities based on specific PC models and BIOS versions, recommending the relevant patch for swift remediation. While CVE Detection will eventually be available for BIOS, firmware, applications, and drivers, it will initially launch for BIOS vulnerabilities only.

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, 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.

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 SP800-155 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:

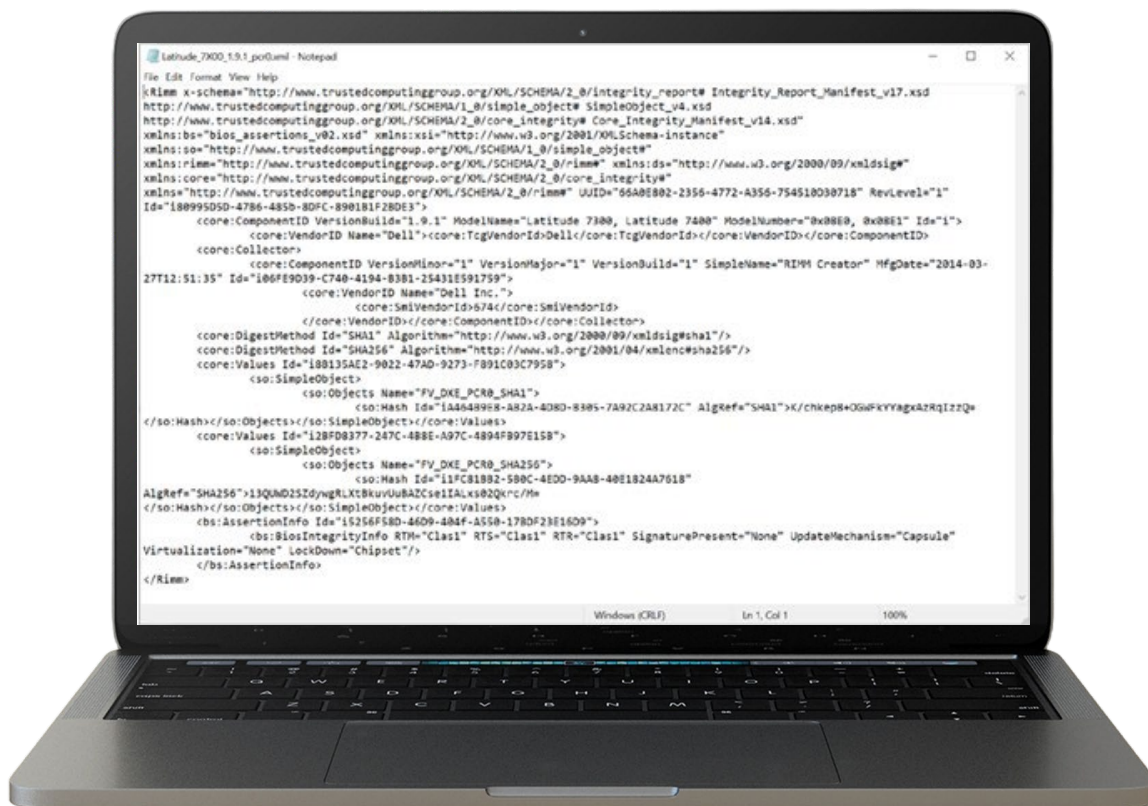


Figure 9: Example BIOS Measurements

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.

Physical Security Features – Chassis Intrusion

Dell commercial devices – including Latitude, OptiPlex and Precision Workstation systems (fixed and mobile) include chassis intrusion detection circuitry and logging capability that can be monitored via Intune/SCCM, Client Command Suite, VMware Workspace ONE 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 operating system, 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

A new 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.

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”.

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 the most 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 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 a backup firmware to recover the primary image if needed.

BIOS Recovery

In addition to having a secure and resilient EC, it is also critical that the next stage of the boot process, the BIOS, also has a robust recovery mechanism. While it may not have been previously included in the overall security conversation, the Dell device has 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 for those customers that require that deep insight into their adversaries’ techniques.

Dell devices have a sophisticated set of flexible and tunable features that ensure that the BIOS can be reverted to a known good copy if compromised.

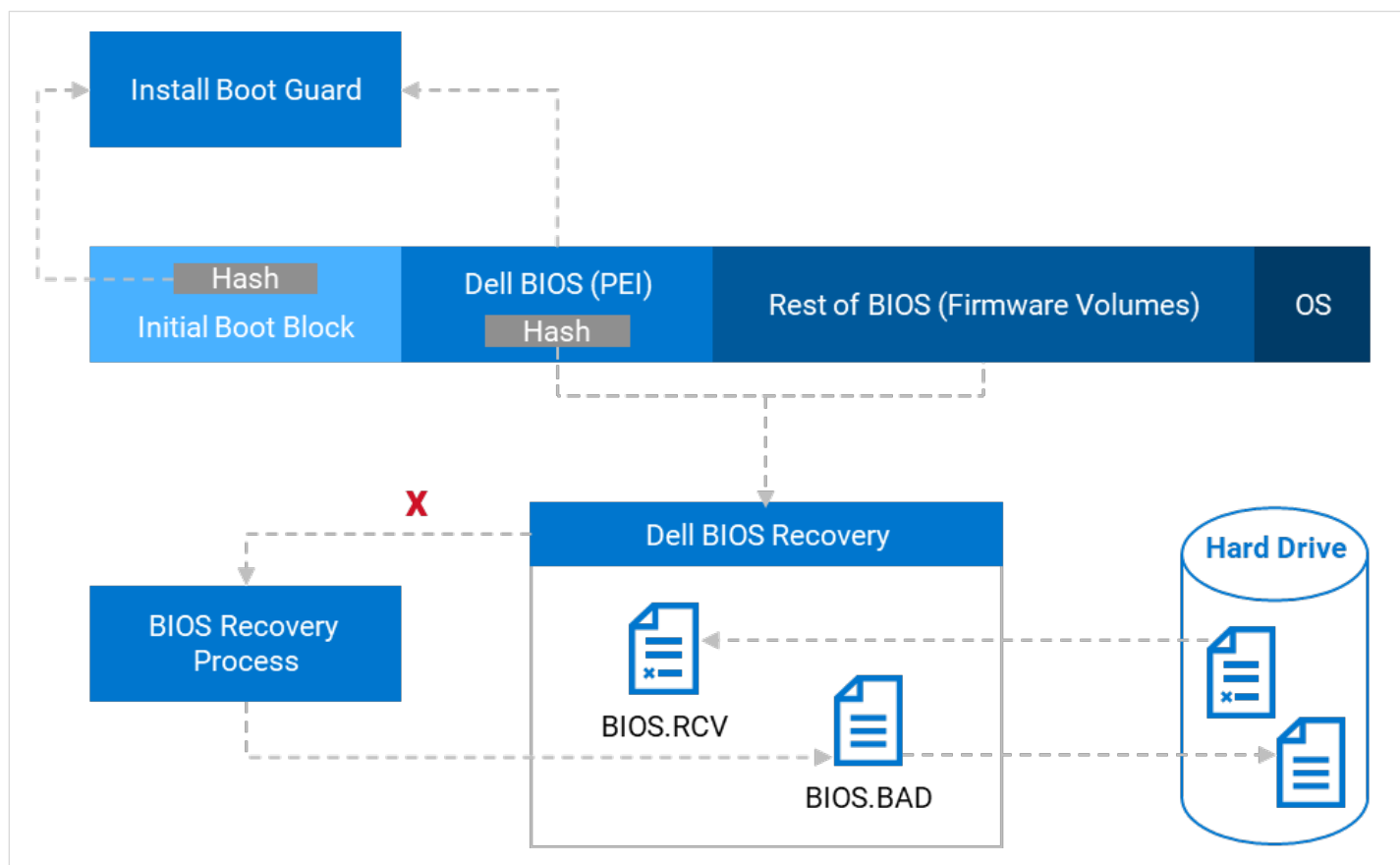


Figure 10: SafeBIOS Recovery Flow

BIOS Recovery Image Update Flow

BIOS recovery is engineered right into the Dell BIOS update architecture, each Dell device can prepare 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 EFI partition on the hard drive. The EFI partition is a hidden partition that is independent of the operating system hard drive partitions. 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	<p>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.</p> <p>BIOS Auto-Recovery – Allows you to recover the BIOS automatically.</p>
	<div data-bbox="394 1654 488 1751"> </div> <p>NOTE: BIOS Recovery from Hard Drive field should be enabled</p>

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 verifying 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.

SafeBIOS Image Capture

As previously discussed, Dell devices include built-in features available to all customers that were designed to support the most advanced customer threat models. 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 SafeBIOS Recovery feature includes an image capture function to save the tampered or corrupted BIOS to the system hard drive 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. Once again, 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.

Dell Data Wipe

Dell devices produced since 2017 include the Dell Data Wipe feature. Dell Data Wipe 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 standard. 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 for more details.)

Dell Data Wipe 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 Special Publication 800-88 Revision 1 Guidelines for Media Sanitization 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 SP800-88r1 widely accepted as more relevant data sanitization standard, most recent update (Dec 2014) includes storage technologies such as NVMe, SSD, etc.

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

Additional Dell Security Capabilities

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](#).

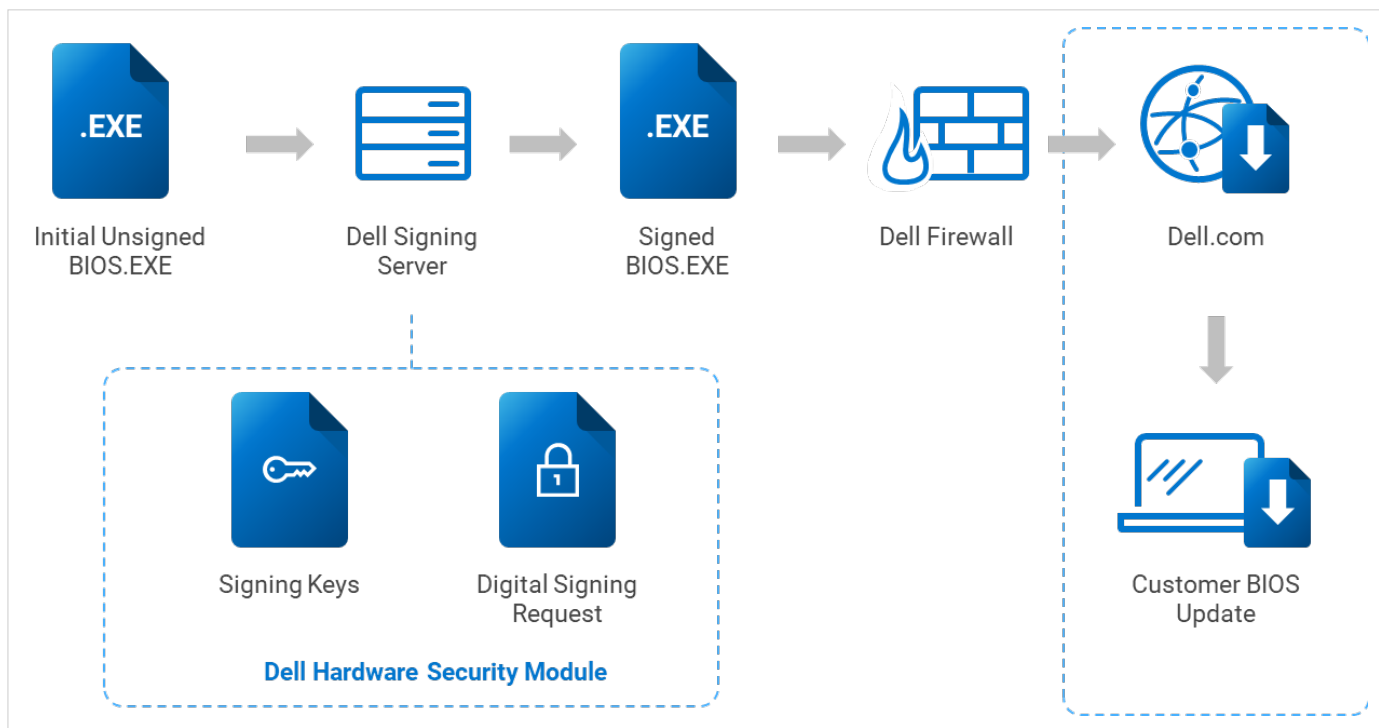


Figure 11: Dell SafeBIOS Signing

- **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, Intel Boot Guard IBB, and Intel BIOS Guard code updates.

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 above, within and below the OS](#) – Dell Technologies and Intel, July 2023
- [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 [Secured Component Verification \(SCV\) Datasheet](#)
- [Dell Trusted Device – Installation and Administration Guide – v6.0](#)
- [Dell Trusted Workspace](#)
- [Dell Client Signed Firmware Update](#)

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](#) – Statistica.com