Client Solutions Dell Trusted Device: BIOS Security

An introduction to the Dell Trusted Device BIOS and security features.

Author: Rick Martinez

Initial Release – September 2020

DELL Technologies

Table of Contents

Executive summary

Computer security is a multi-billion dollar business with thousands of companies competing for organizations' attention and enterprise dollars. Dell Technologies has created an innovative and effective portfolio of technologies and solutions in this industry to help organizations secure their enterprises. One of the areas where Dell has substantially invested over the last decade is security of the endpoint itself, in this case the "client" device (desktops, workstations, and notebooks) known as the Dell Trusted Device.

This investment in the endpoint is significant for security of course but don't firewalls, IDS/IPS, SIEMs, NGAV, EDR and all the various alphabet soup of enterprise-level security tools already cover everything? Well, yes and no. Dell believes that the security of the infrastructure not only depends on these tools, but also on the intrinsic security of each individual endpoint. From this perspective the endpoints, and subsequently each individual device, collectively become the foundation of security for the entire enterprise comprising of edge devices, networks, IoT devices, and beyond.

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 Trusted 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).

This whitepaper was written to provide a thorough introduction to the Dell Trusted Device BIOS and, more specifically, the 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 intended 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 intrinsic security offered by the Dell Trusted Device via security and hardening of the underlying BIOS and firmware. Contextually this document is broken into sections that map to the five functions defined in the NIST Cybersecurity Framework: Identify, Protect, Detect, and Recover. This should help put each feature included in the Dell Trusted Device into the perspective of the overall goal of helping to secure each organization's enterprise.

Examples of topics covered within this context in the remaining sections are:

- **Identify:** asset management and secure design principles proactively contributing to security (e.g. Dell Service Tag, Threat Modeling)
- **Protect:** defensive technologies to harden non-volatile storage and the boot process (e.g. Signed Firmware Update, BIOS Passwords)
- **Detect:** ability to convey status when unauthorized changes occur (e.g. SafeBIOS Verification, Intel Boot Guard)
- **Recover:** advanced mitigations to quickly remediate issues (e.g. BIOS Recovery, Dell Data Wipe)

This document concludes with a brief section on Supply Chain Assurance and a commitment to the ongoing Dell investments helping to shape the future of security. This document is not the end of the conversation about the Dell Trusted Device: hopefully it's the beginning of a long and bi-directional discourse beneficial to the industry overall.

The Key Elements of Dell BIOS Security

What is BIOS? 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.

Additionally, more recently the term "UEFI" has become much more prominent when discussing pre-boot firmware on PCs, and 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 forum and 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 that are compatible with the UEFI specification directly into the BIOS development flow. 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.

The Importance of "Below the OS" Security

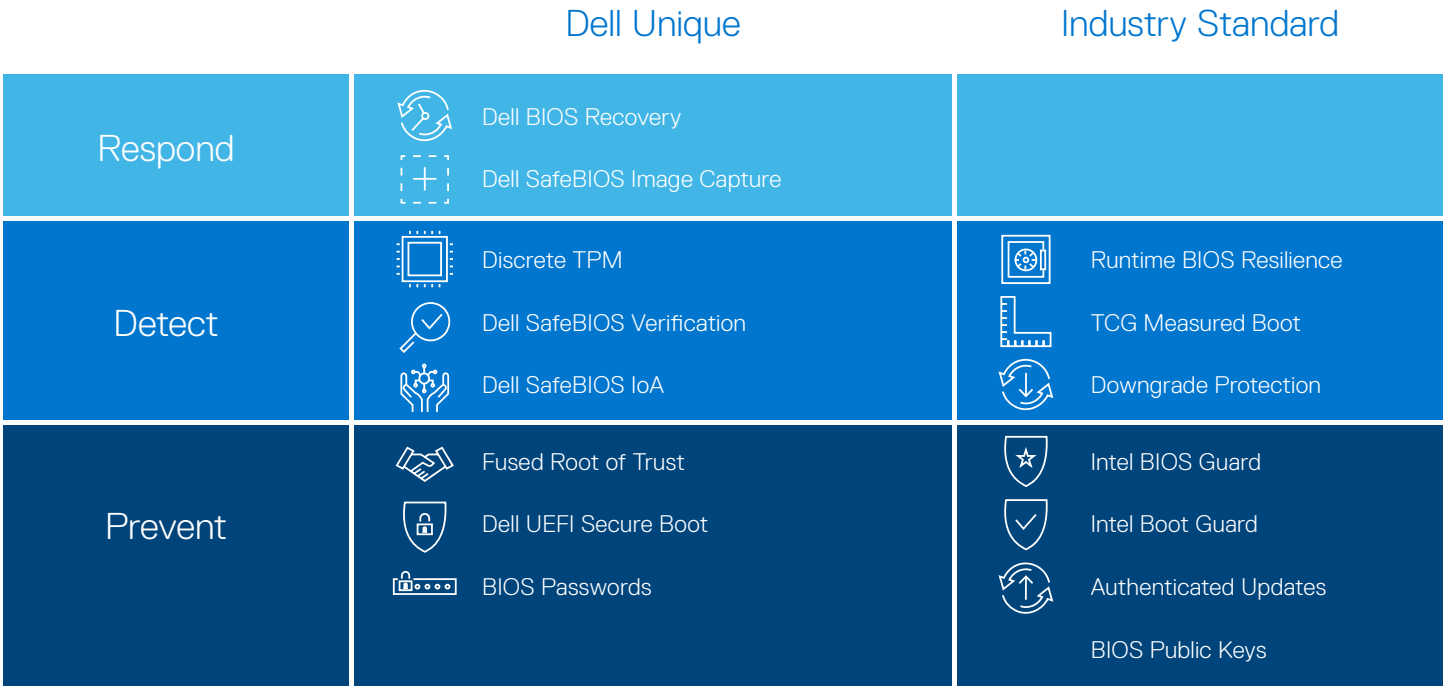


Figure 1 Trusted Device: Dell SafeBIOS Framework

As mentioned in the executive summary, the security of endpoints collectively form 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 Trusted Device and BIOS security comes in!

Dell refers to this stable foundation as "Below the OS", and the Dell SafeBIOS Framework refers to all security features implemented to secure the device beneath the operating system. 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 the SafeBIOS features and some of the rationale behind their development.

Industry standards bodies, policy makers, and security researchers have recently started to focus on 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. Most recently, NIST Special Publication SP800-193 has outlined 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.

Other NIST Special Publications that are relevant in this space include NIST SP800-147, 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 SP800-88 provides direction for data sanitization on hard drives and solid-state drives.

It's clear that industry and customer interest for "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 Trusted Device customers from the most sophisticated adversaries.

NIST Cybersecurity Framework

BIOS security can be categorized according to the five functions of the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover. The remaining sections of this document will detail the BIOS features and below the OS security technologies that align to these functions and explain how they work and why they are important. More information about the NIST Cybersecurity Framework can be found here: https://www.nist.gov/cyberframework.

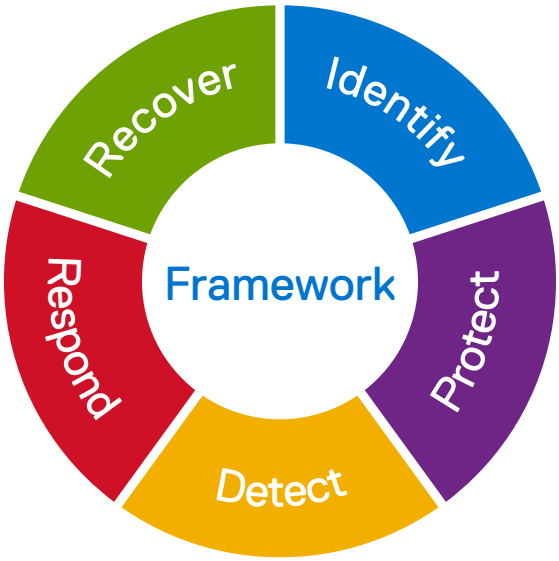


Figure 2 NIST Cybersecurity Framework - Five Functions

Identify

The Dell Trusted Device and BIOS 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 the Dell Trusted Device the Identify function has two important but separate roles:

1. Includes features designed to help identify and asset-manage Dell Trusted Devices in a customer infrastructure.
2. Addresses processes and tools used by Dell to Identify customer security risks and threat models of the application and deployment of these devices.

Identity and Asset Management Tags

The Dell Trusted Device 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 https://www.dell.com/support/contents/en-us/category/product-support/self-support-knowledgebase/locate-service-tag.

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 https://www.dell.com/support/article/sln70985/.

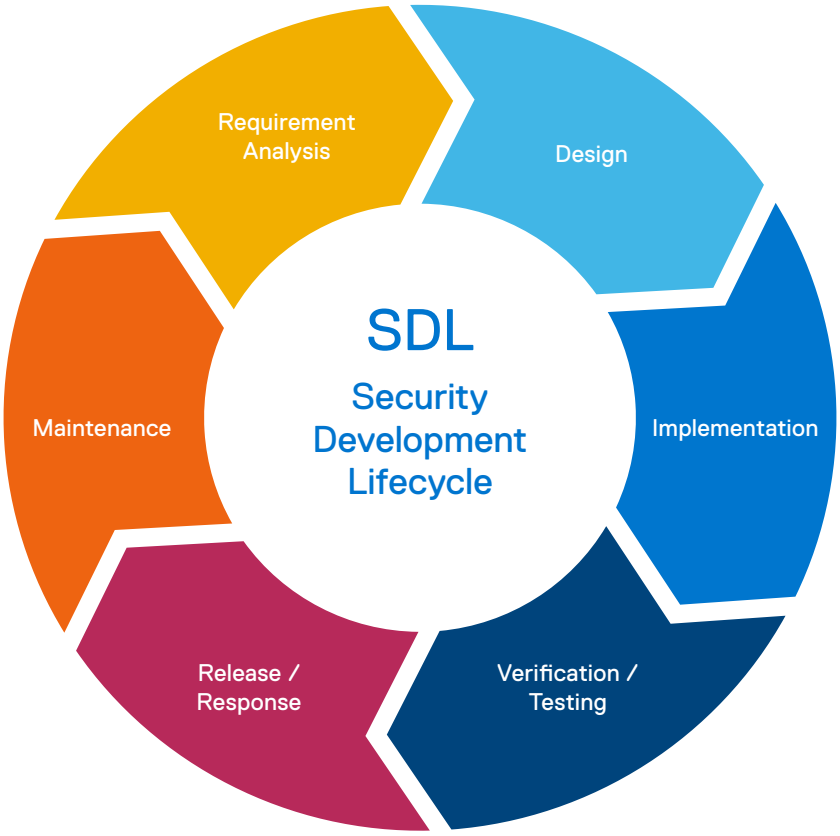


Figure 3 Dell EMC Security Development Lifecycle

Secure Design Processes and SDL

Dell's Secure Development Lifecycle (SDL) shown in Figure 3 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 Trusted Device technology space. A second major consideration is industry practices. Dell participates in many industry standard organizations such as SAFECode, BSIMM, 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'.

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: https://www.safecode.org). Other 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 member of the Forum of Incident Response and Security Teams (FIRST: https://www.first.org). 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: http://www.opengroup.org/getinvolved/forums/trusted). OTTF leads the development of a global supply chain integrity program and framework.
- Dell was among the 9 companies that were first assessed by the Building Security In Maturity Model (BSIMM: https://www.bsimm.com/) project back in 2008 and has continued to be part of the project. A Dell representative is part of the BSIMM Board of Advisors.
- 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.

"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. 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 Trusted 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

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 'pentesting', 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 pentest Dell Trusted 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 the Dell Trusted Devices.

Protect

The second stage of the Dell Trusted Device strategy, the Protect stage, 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 the Dell Trusted Device. These features are truly the "first line of defense" for modern PCs against sophisticated adversaries.

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.

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 4 depicts a high-level overview of the major components in the Dell Trusted Device boot chain. Many of these components, like the Dell 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.

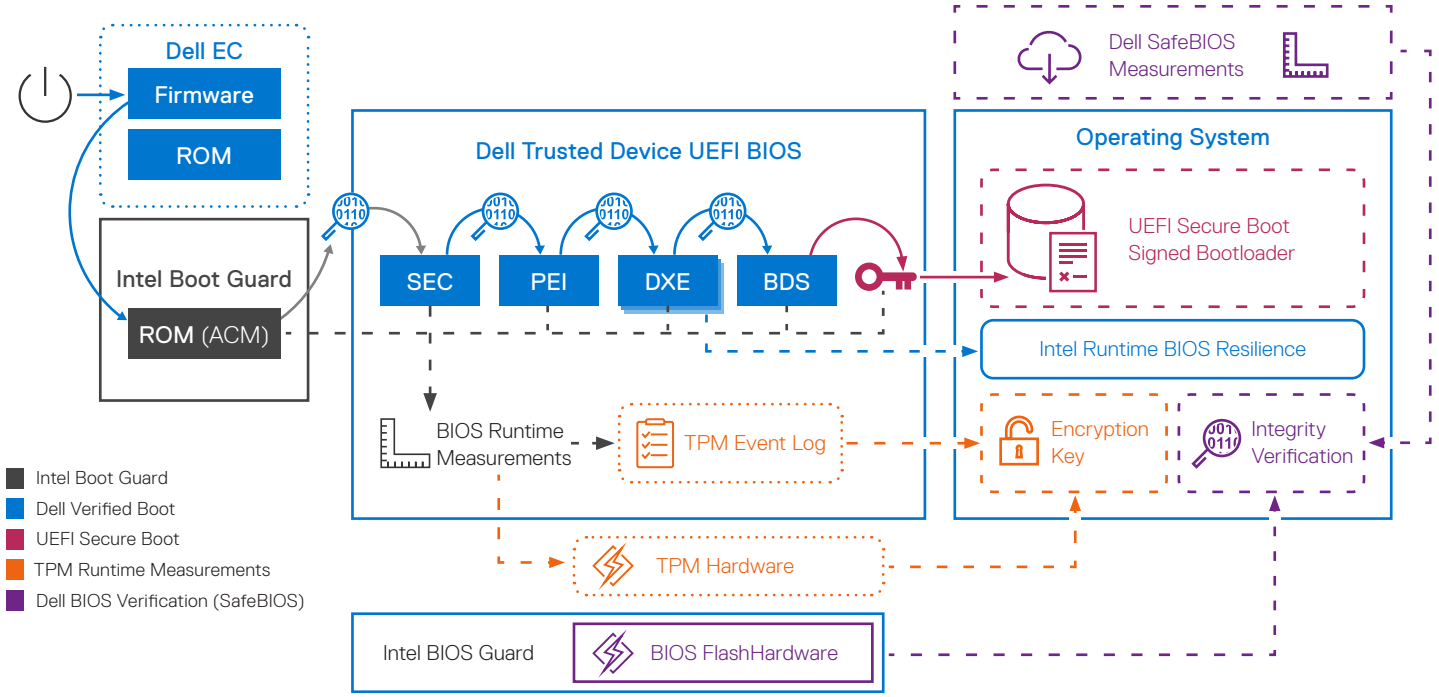


Figure 4 Dell Trusted Device Boot Chain

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 PC's, 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 if 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.

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.

TCG and the Root of Trust

The Trusted Computing Group (TCG) is an industry standards organization which 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.

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 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.

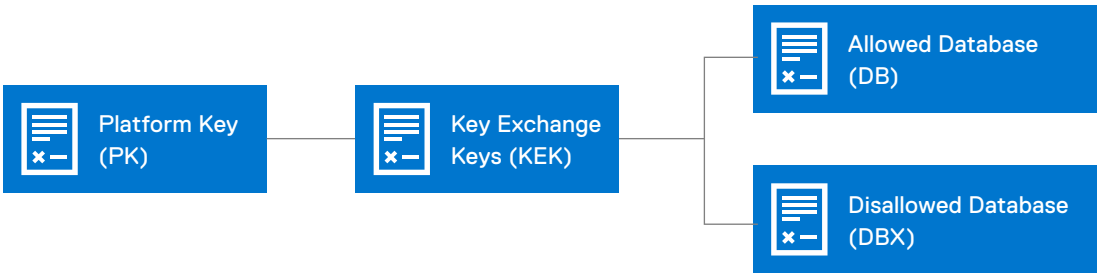


Figure 5 Secure Boot Key Hierarchy

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.

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 non-bypassability guidelines to further harden the BIOS against unauthorized modification via "backdoors". Dell Trusted 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 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 186-3 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.

Mitigating SMM Threats with Intel BIOS Guard

The Signed Firmware Update whitepaper released in 2013 is still applicable and relevant to all Dell Trusted 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. SMM has been the subject of a considerable amount of security research over the last decade.

What is SMM?

System Management Mode, or SMM, is a privileged mode of the processor that was 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.

How can SMM be a potential threat? Well, the same properties that make SMM valuable from a Dell perspective also make them an attractive target for security researchers and adversaries. If an adversary were to potentially find and exploit an unknown vulnerability in SMM code, they may be able to masquerade as authorized ring -2 code. They could then attempt to bypass BIOS locking or signature verification if those features are solely enforced by SMM code.

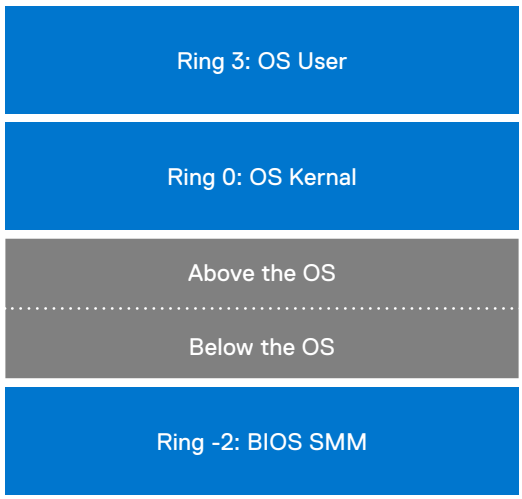


Figure 6 Modern PC Ring Architecture

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 Trusted 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 is able to block all writes to the BIOS code region before it gets to flash. 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.

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 new vulnerabilities are deployed as soon as they are available. BIOS upgrades are often overlooked in the overall patch management strategy, but that's rapidly changing as customer awareness for "Below the OS" security continues to increase. To support this overall initiative, Dell Trusted Device BIOS updates are posted to both Windows Update (or WU) for Windows 10 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. Of course, updating the BIOS using the Dell BIOS update utility is still supported as an alternative to these services.

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 Trusted 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.

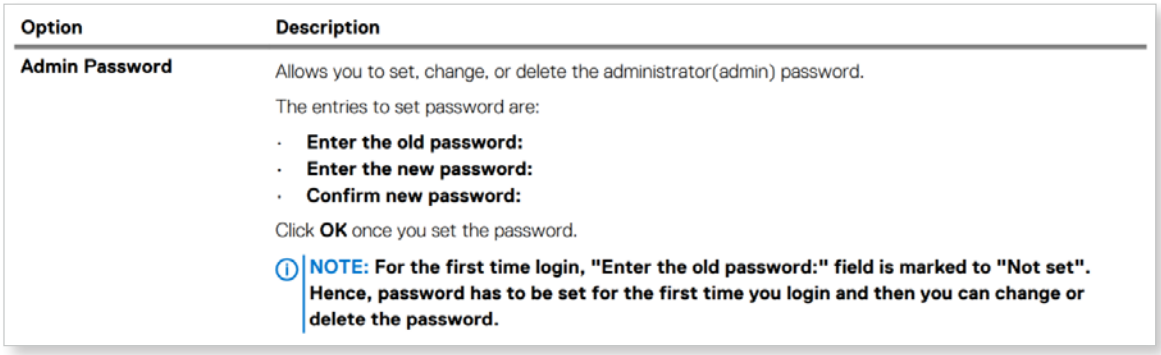
Embedded Controller: Signed Firmware

The embedded controller, or EC, is included on all Dell Trusted 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 Trusted 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 Trusted 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 Trusted 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 Dell Trusted 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 exploit depending on the environment. Dell Trusted Devices are shipped in a "secure by default" state and customers can protect this state from unauthorized access or modification by enabling a few important features.



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

The BIOS Admin Password is the Dell Trusted 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 Trusted 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

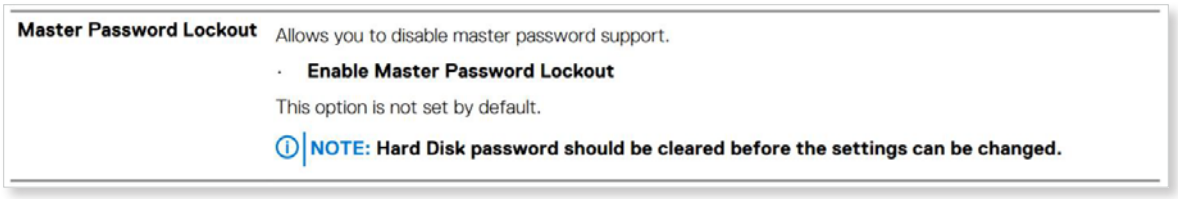
The Dell Master Password is perhaps one of the most powerful, yet misunderstood, features of the Dell Trusted Device. The Master Password feature is available for customers who may have forgotten or misplaced the BIOS Administrator Password on their device or fleet of devices. The Dell Master Password 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, it cannot be used over any remote BIOS interface.

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 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 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 Trusted 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 Trusted 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 Trusted Device threat model.

Threat: Physical Access

As discussed, direct physical access to a Dell Trusted 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 Trusted 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 (https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/ctr-uefi-defensive-practices-guidance.pdf?ver=2018-11-06-074836-090) for overall recommendations. Please see the Client Command Suite tool documentation in order to deploy and manage policies aligned to these guidelines on Dell Trusted Devices.

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.

System Management Mode (SMM)

System Management Mode, or "SMM", has been the target of dozens of disclosed vulnerabilities, security conference presentations, and media reports over the years. This has been welcome attention from a security perspective, because it provides helpful insights for SMM threat modeling and security improvements. For example, even though the 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 deprivilege the SMM code that must be present on the system and mitigate potential impact to other parts of the operating system. These enhancements will be described in the following sections paired with the threats that they specifically mitigate.

Sidebar: Windows WHCP Requirements

The Microsoft Windows Hardware Compatibility Program (WHCP) has been a welcome and effective lever to assist the PC industry to adopt and evolve security requirements for BIOS. Full requirements can be found here: https://docs.microsoft.com/en-us/windows-hardware/design/compatibility/whcp-specifications-policies. The Dell Trusted Device BIOS has taken advantage of this incentive to develop features that meet the most rigorous requirements in the WHCP. The DeviceGuard and SystemGuard sections of the WHCP define a subset of additional security requirements that are listed as "If-Implemented" per the program specification. The Dell Trusted Device BIOS implements all these requirements as a target baseline. This is particularly relevant to the SMM threats and mitigations described in this section.

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. 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) is not technically a mitigation, but it 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, the Dell Trusted 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 Trusted 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 also 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.

Runtime BIOS Resilience

Intel has been another valuable ally in the Dell Trusted Device story providing foundational security technologies in processors and chipsets, also extending trusted computing concepts into new architectural areas of the Dell Trusted 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 Trusted 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:
https://www.intel.com/content/www/us/en/architecture-and-technology/hardware-shield.html

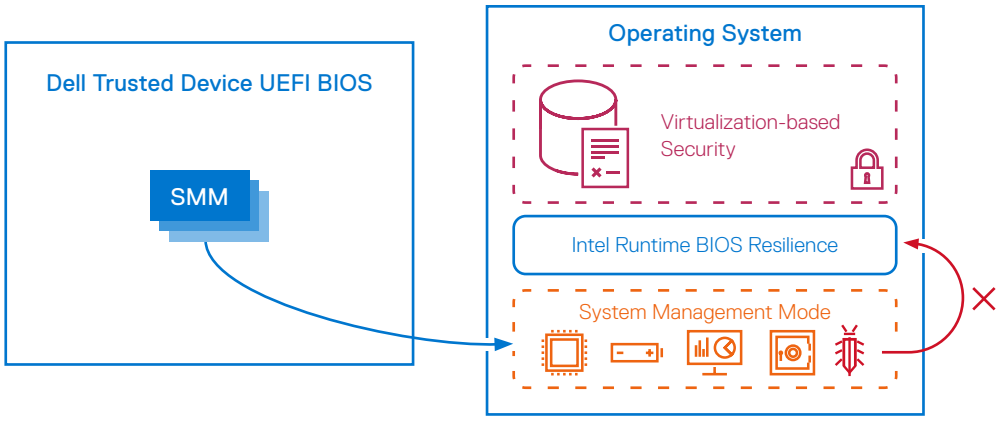


Figure 7 Intel Runtime BIOS Resilience

Detect

One could presume that a 100% effective protection strategy both above and below the OS would be enough to thwart even the most sophisticated adversaries. While this may be true in some cases and within certain threat models, 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 PC's 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 Trusted 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.

SafeBIOS Verification

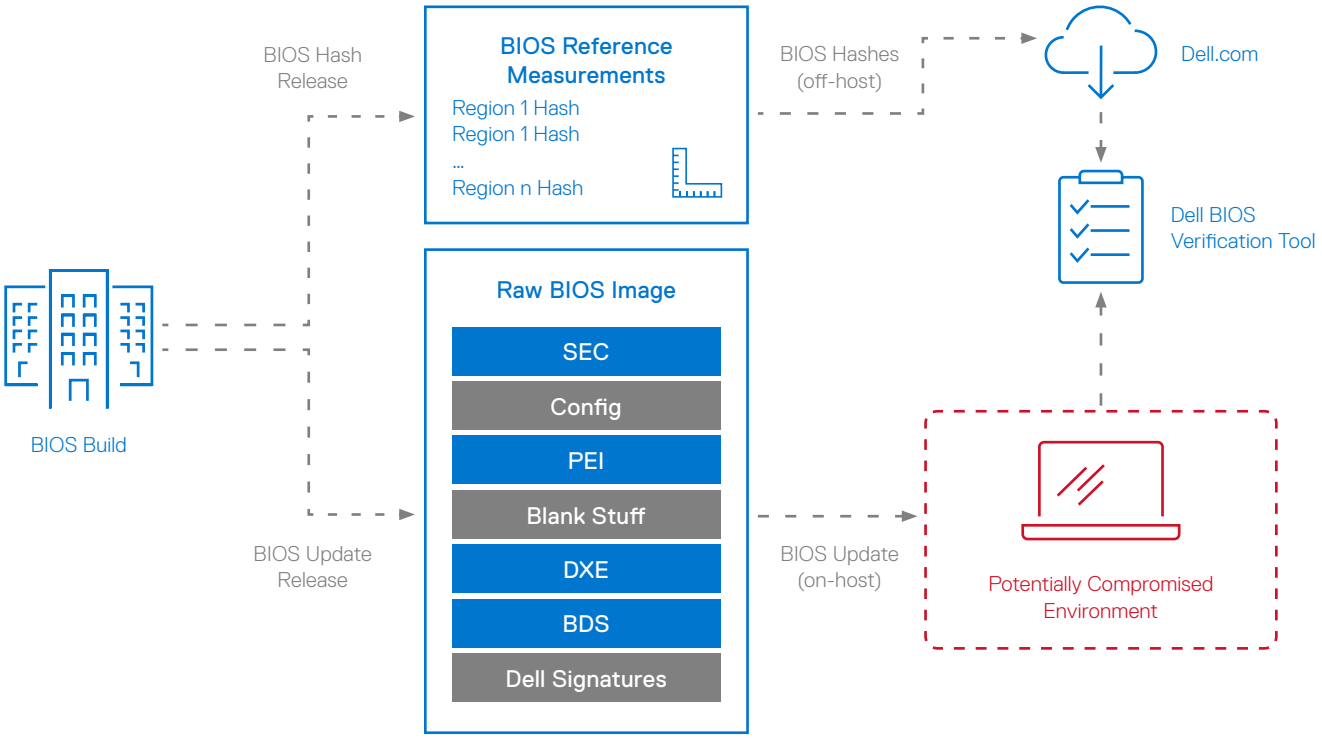


Figure 8 SafeBIOS Verification Flow

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 has introduced a feature called SafeBIOS Verification that addresses both of these concerns. SafeBIOS Verification uses an OS-resident agent application 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.

VMware Carbon Black Integration

As mentioned, Dell Trusted Devices include many layers of protection and detection to prevent against BIOS tampering. This places BIOS-based attacks, and more importantly successfully executed BIOS-based attacks, into the extremely uncommon category for almost all customers. The scarcity of this activity and the ability for adversaries to choose their target means that it takes a massive deployment scale to find these types of exploits. A collaboration between Dell and VMware Carbon Black addresses this need for scale by allowing customers to integrate SafeBIOS verification alerts and image capture ability directly within the VMware Carbon Black Audit & Remediation infrastructure. This is supported with existing installations via the VMware Carbon Black Security Cloud Live Response API.

More information and instructions for monitoring the Dell Trusted Device agent with VMware Carbon Black Security Cloud Live Response APIs is available here: https://github.com/carbonblack/cbapi-python/tree/master/examples/defense/cblr/DellBiosVerification

BIOS 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 back to a "known good" state in an attempt 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 agent 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.

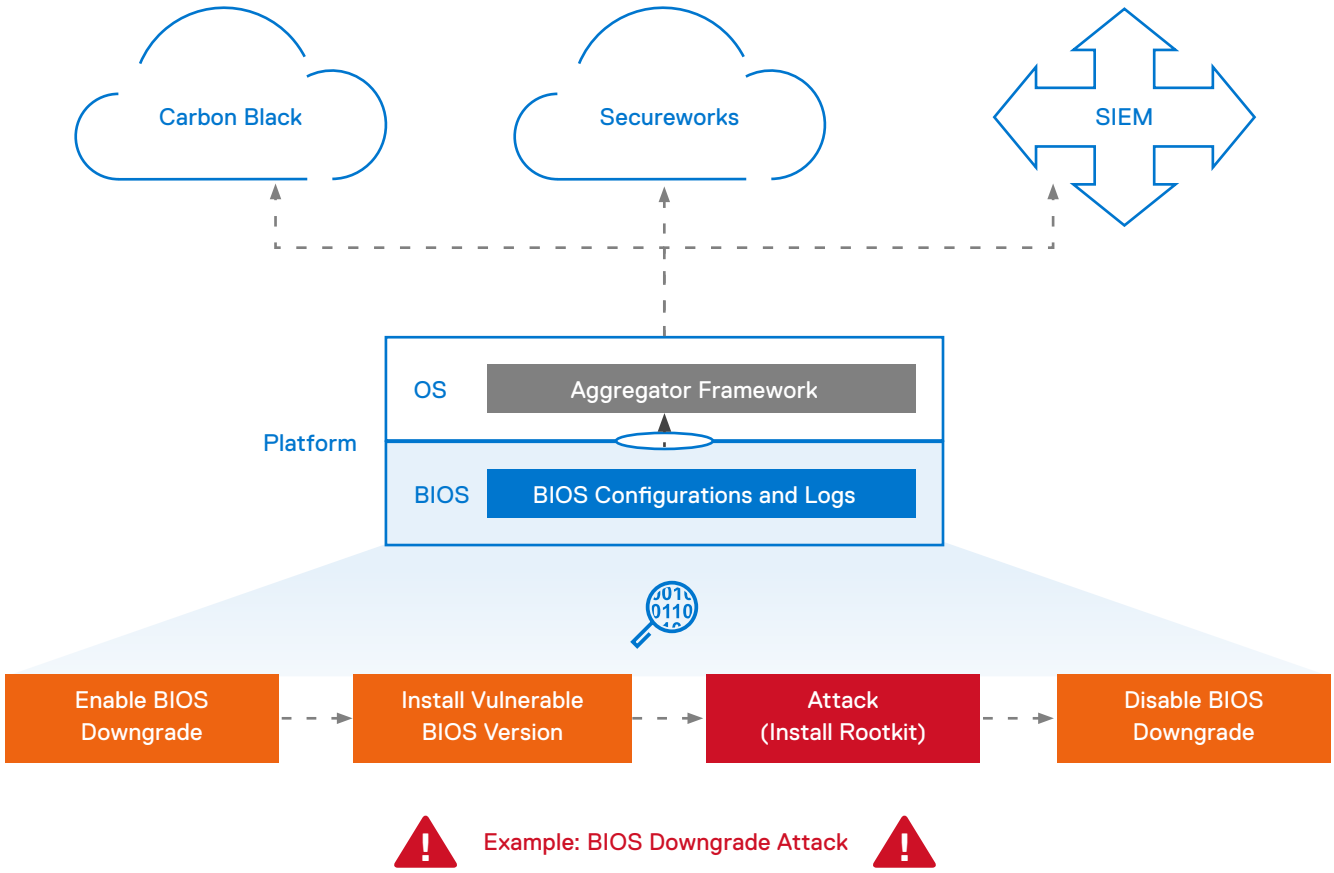


Figure 9 SafeBIOS Indicators of Attack

Chassis Intrusion

Dell OptiPlex and Precision Fixed Workstation systems include chassis intrusion detection circuitry and logging capability that can be monitored via SCCM, Client Command Suite, VMware Workspace ONE and other common systems management platforms. Leveraging the Dell Trusted Device physical access threat model assumptions, this feature will be transitioned onto select Dell Latitude and Precision Mobile systems incrementally year over year. Chassis intrusion combines with other below the OS security features to strengthen the Dell Trusted 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, typically the first sign of a physical attack.

TCG Measured Boot

As mentioned in an earlier section, TCG Measured Boot on the Dell Trusted 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: https://trustedcomputinggroup.org/resource/tpm-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. Internally 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 that is cryptographically dependent on all the extend operations (and their order) that have occurred since the PC was reset.

Code, Configuration, and the TPM Event Log

The Dell Trusted Device extends code and configuration information to the TPM PCRs during every boot in accordance to the TCG PC Client Platform Firmware Profile Specification: https://trustedcomputinggroup.org/resource/pc-client-specific-platform-firmware-profile-specification/

There are many PCRs in each TPM. Table 1 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. The Dell Trusted Device extends 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
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 Trusted 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 PCR's 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 the Dell Trusted Device 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 Trusted Device BIOS update utility. An example of the content and format of the output of this command appears below:

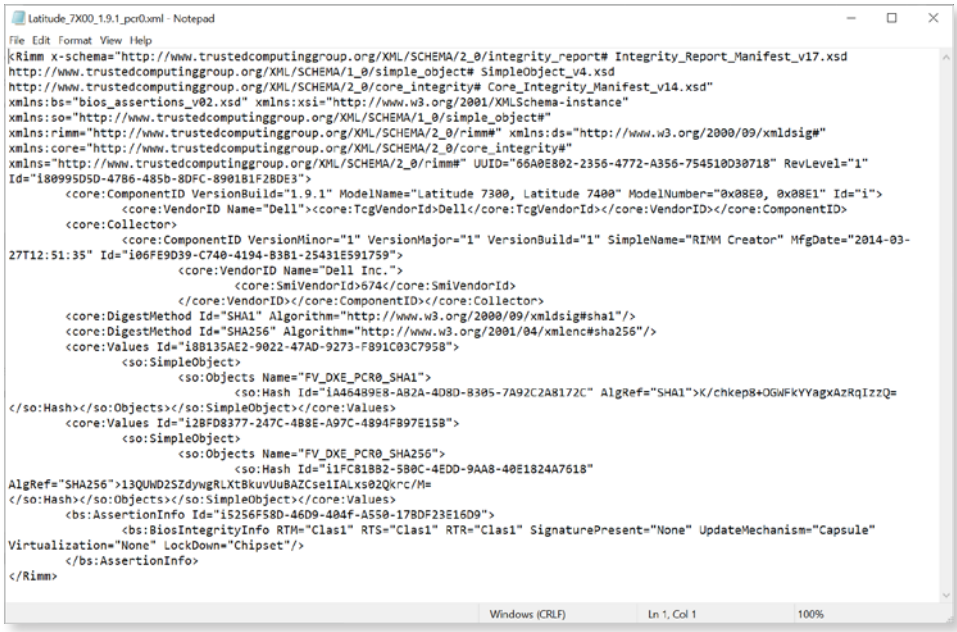


Figure 10 Example BIOS Measurements

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.

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

Recover

Recover and Respond 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 Trusted Device back to normal operating status as quickly and efficiently as possible can help to minimize the overall cost of these events.

Dell Trusted 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.

Embedded Controller Recovery

As mentioned previously the Dell Trusted 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 Trusted 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 Trusted 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 is will securely capture the state of tampering for offline analysis for those customers that require that deep insight into their adversaries' techniques.

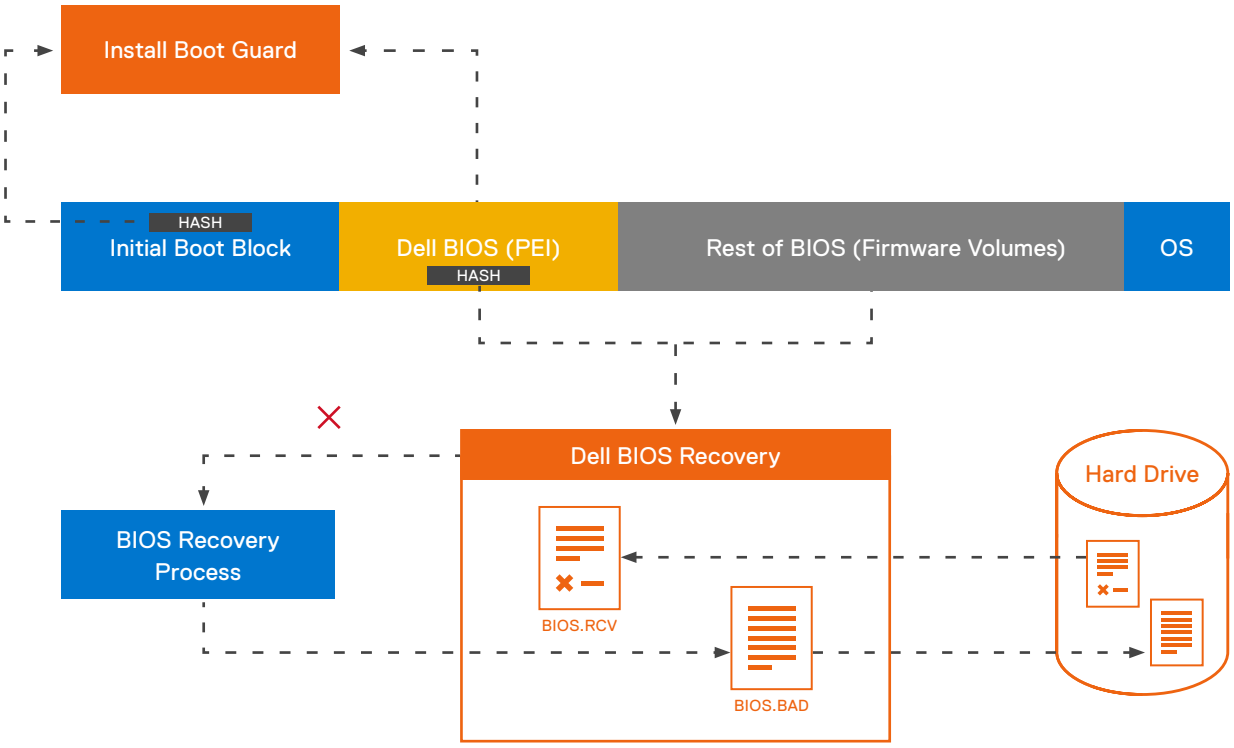


Figure 11 SafeBIOS Recovery Flow

BIOS Recovery Image Update Flow

BIOS recovery is engineered right into the Dell BIOS update architecture, so the Dell Trusted 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 update version and verified by the BIOS RTU prior to performing recovery.

Bios Recovery	**BIOS Recovery from Hard Drive**—This option is set by default. Allows you to recover the corrupted BIOS from a recovery file on the HDD or an external USB key. **BIOS Auto-Recovery**— Allows you to recover the BIOS automatically. **NOTE: BIOS Recovery from Hard Drive field should be enabled.**

Auto Recovery Flow

The Dell Trusted Device 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) is capable of reading 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 Trusted Devices. This may at first seem misaligned with the overall security and threat model assumptions of the Dell Trusted 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.

BIOS Image Capture

As previously discussed, the Dell Trusted 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 BIOS 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 agent. Once again, this image can be collected by the VMware Carbon Black Audit & Remediation solution for analysis at scale if necessary. 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 Trusted 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 Trusted Devices. 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, formatNVM 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.

Dell Data Wipe – Key features:

- 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: https://www.dell.com/support/article/sln312291/

Supply Chain Assurance

Supply chain assurance and the broader supply chain security concept are complex topics that demand their own volume. Fortunately, the Dell Trusted 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:
https://www.dell.com/learn/us/en/vn/corpcomm_docs/supply-chain-assurance.pdf

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

Dell has also 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 Trusted Device 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 Dell Trusted Device features covered in this document can help assist and augment traditional supply chain security. For example, the SafeBIOS BIOS verification check is part of the manufacturing process of every Dell Trusted Device that Dell produces.

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: https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/

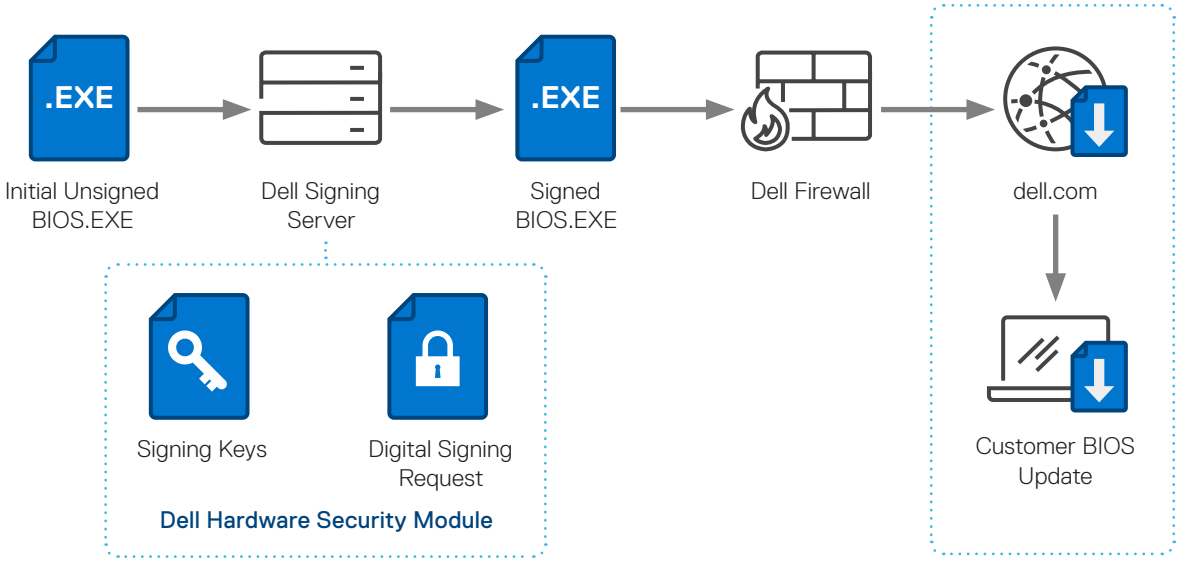


Figure 12 Dell SafeBIOS Signing

Mitigation: Signing Infrastructure

Dell Trusted 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 Trusted Device BIOS signing capability is integrated directly into the automated build processes and developers to 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.

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 Trusted Device 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.

The Future of Security

Security is a fast-moving discipline and Dell continues to look forward to the future state of computing and, as expected, the future state of the adversarial landscape. Dell security strategists and architects are continuously monitoring the evolving needs of organizations and threats to those organizations and defining and building layers of defense, protection, detection, and recovery on top of the existing Dell Trusted Device foundation. Attackers are not going away, hardening the Dell Trusted Device is an ongoing focus for Dell and an ongoing commitment to organizations that choose Dell.

Appendix

Referenced Links

1. Dell Signed Firmware Update (NIST SP800-147)
2. NIST Special Publication 800-155 BIOS Integrity Measurement Guidelines
3. Dell Supply Chain Assurance
4. BIOS Security - The Next Frontier for Endpoint Protection
5. Dell Data Wipe KB Article
6. UEFI Tianocore Github
7. UEFI on Dell Business Client Platforms
8. Dell Trusted Device
9. Dell.com/Security
10. NSA Cybersecurity Report: UEFI Defensive Practices Guidance
11. Dell Firmware Security, Justin Johnson, Platform Security Summit 2018
12. NIST Cybersecurity Framework
13. Window SMM Mitigation Table (WSMT)
14. Presentation: Attacking Hypervisors via Firmware and Hardware
15. Presentation: A New Class of Vulnerabilities in SMI Handlers
16. Dell Client Command Suite
17. Dell SafeBIOS Verification with Carbon Black Audit & Remediation
18. Windows Hardware Compatibility Program Specifications and Policies

Learn More

Visit https://www.delltechnologies.com/endpointsecurity for more information on Dell Trusted Devices.

Acknowledgements

Documents of this scale are not created in a vacuum and I am eternally grateful for the hundreds of hours of collective reviews from Dell employees as well as industry experts outside of Dell. Without your guidance, support, and extensive feedback this document would still be on the “we should really write all this down” back log somewhere. Thank you!

About the author

Rick Martinez is a Sr. Distinguished Engineer with a 20+ year career at Dell. In his current role, Rick leads security strategy for Dell PCs focused on trusted and resilient platforms. In addition to his role as a strategist he is an expert resource in secure development governance and execution for Dell PCs and pan-Dell secure supply chain efforts. Rick is active in the Trusted Computing Group and serves as Dell representative on the TCG Board of Directors. In his past roles Rick has led security strategy and architecture for BIOS and implemented many fundamental platform security features including Signed Firmware Update (NIST 800-147), TPM, and Trusted Execution Technology.