Anatomy of a Trusted Device

Learn what makes Dell the world's most secure commercial AI PCs1



THREAT LANDSCAPE & **CHALLENGES**

Emerging attack vectors below-the-OS creating new risk

Endpoint devices are a major gateway for breaches. As hybrid work expanded the attack surface, concern around device-level security spiked in recent years. Attackers increasingly turned to targeting the supply chain, as well as rootkits and other firmware vulnerabilities which are largely

undetectable by legacy EDR software alone.



Top evaluation criteria when sourcing new PCs: Automated detection of BIOS events3

Addressing high-risk

configurations³

To combat modern threats, devices must be built securely, and they must feature built-in security to help catch and repel attacks.

THE SOLUTION

Prevent, Detect, Respond to & Recover from Foundational Attacks with the World's Most Secure Commercial PCs1

A fleet is only as secure as its individual PCs. But what makes a device trusted and secure? Visibility and actionability. Having access to more data leads to informed decision-making, helping to catch even the sneakiest emerging threats. Automation enables speedier resolution of potential issues.

The hardware and firmware defenses of Dell commercial PCs (on both Intel and AMD) are designed to bring that visibility and actionability to your fleet.

The Anatomy of a Dell Trusted Device

Benefits



Be secure from first boot with rigorous supply chain controls



Maintain BIOS integrity with deep, firmware-level visibility



Protect end-user identity from malware that looks to steal credentials



Enrich OS-level data with 'below-the-OS' telemetry to speed detection, response and remediation

Improve security with PC telemetry Shrink the IT-security gap and enrich software

solutions with below-the-OS insights. Only Dell integrates PC telemetry with industry-leading software providers to improve fleet-wide security.1

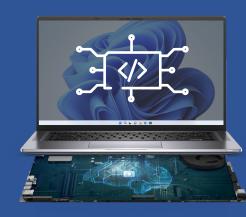
Maintain BIOS integrity Catch and repel threats with Dell-unique

BIOS verification. Assess a corrupt BIOS, repair it and gain insights that reduce exposure to future threats with BIOS Image Capture.¹ Learn more →



Spot ticking

behavior-based threats before they can do damage.1 Learn more →



Verify firmware integrity

Dell-exclusive firmware verification protects against unauthorized access to and tampering of highly privileged firmware. 1

Catch known vulnerabilities Dell-unique Common Vulnerabilities and

Exposures (CVE) Detection and Auto Remediation monitors for publicly reported BIOS security flaws and recommends updates to mitigate risk.1

Verify user access via Dell SafeID with ControlVault, a unique, dedicated security chip

Secure end user credentials

that keeps user credentials hidden from malware. FIPS 140-3 Level 3 certified.

Rigorous, state-of-the-art supply chain controls and optional add-ons, like Dell-unique Secured Component Verification, provide assurance of PC integrity upon

Be secure across the PC lifecycle

delivery and throughout its lifetime.1 Learn more →

INDUSTRY LEADERSHIP

offers the BIOS-level visibility Dell does.^{1, 4} Learn what it takes to maintain device trust against modern threats.

No PC manufacturer

<u>Learn More</u> →

Security features in Dell, HP, and Lenovo PC systems: A research-based comparison

Approach Dell™ commissioned Principled Technologies to investigate nine security features in the PC security and system

· Signed manifest of factory configuration

· BIOS verification on demand via off-host measurements · Intel Management Engine firmware verification via off-host measurements BIOS image capture for analysis

· Early and ongoing attack sequence detection · Common vulnerabilities and exposures detection and remediation · User credentials storage via dedicated hardware

· Integrated hardware and software security solutions · Hardware-assisted security with Dell, Intel, and CrowdStrike Below-the-OS telemetry integration

Manager (DCDM), which consolidate and extend DTD's capabilities for enterprise fleet management. DCDM **Explore Dell Trusted Devices**

These features rely on manufacturer-enabled communication between the hardware and the operating system (OS). We reviewed publicly available marketing claims and feature documentation for three Windows original equipment manufacturers (OEMs) based on Intel® Core™ Ultra processor with Intel vPro®: Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device (DTD) application or the newer Dell Client Device







Secure anywhere-work with



Dell Trusted Workspace

Built-with & Built-in Hardware Security



Built-on Software Security

Contact us

dell.com/endpoint-security

global.security.sales@dell.com

Endpoint Security Blogs →

Read more

Visit us

Join the conversation in delltechnologies X @delltech

²Source: Futurum Group, Endpoint Security Trends, 2023.

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

3 Source: Enterprise Strategy Group, a division of TechTarget, Custom Research Survey Commissioned by Dell Technologies, Assessing Organizations' Security Journeys, November 2023. ⁴Principled Technology study results available for Intel-based devices only.