

Anatomy of a Trusted Device

Learn what makes Dell commercial PCs on the Intel vPro® platform the world's most secure commercial PCs¹



THREAT LANDSCAPE & CHALLENGES

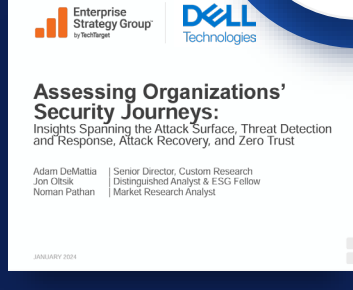
Emerging attack vectors below-the-OS creating new risk

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.



Device-based threats increased 1.5x since 2020.²

69% of organizations report at least ONE device/BIOS-level attack²



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 the Intel vPro platform 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 with the Dell Trusted Device Application. Only Dell integrates PC telemetry with industry-leading software providers to improve fleet-wide security.¹ [Learn more](#) →

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 timebombs

Indicators of Attack, an early-alert feature offered only by Dell, scans for behavior-based threats before they can do damage.¹ [Learn more](#) →



Verify firmware integrity

Dell-exclusive firmware verification, hardware-based security found in Intel processors, protects against unauthorized access to and tampering of highly privileged firmware.¹

Catch known vulnerabilities

Dell-unique Common Vulnerabilities and Exposures (CVE) Detection monitors for publicly reported BIOS security flaws and recommends updates to mitigate risk.¹ [Learn more](#) →

Secure end user credentials

Verify user access with Dell-unique SafeID, a dedicated security chip that keeps user credentials hidden from malware.¹ [Learn more](#) →

Be secure across the PC lifecycle

Rigorous, state-of-the-art supply chain controls and optional add-ons, like Dell-unique Secured Component Verification, provide assurance of PC integrity upon delivery and throughout its lifetime.¹ [Learn more](#) →

INDUSTRY LEADERSHIP

No PC manufacturer offers the BIOS-level visibility Dell does.¹

Learn what it takes to maintain device trust against modern threats.

[Learn More](#) →

A Principled Technologies report: In-depth research. Real-world value.

A comparison of security features in Dell, HP, and Lenovo PC systems

Approach

Dell™ commissioned Principled Technologies to investigate 10 security features in the PC security and system management space:

- Support for monitoring and protection
 - BIOS security and protection features
 - Platform integrity validation
 - Device integrity validation via off-site measurements
 - Component integrity validation for Intel® Management Engine (ME) via off-site measurements
 - BIOS image capture for analysis
 - Built-in hardware cache for monitoring BIOS changes with security information and event management (SIEM) integration
- Microsoft Intune management
 - BIOS setting management integrations for Intune
 - BIOS access management security enhancements for Intune
- Remote management
 - Intel vPro® remote management
 - PC management using cellular data

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

Explore Dell Trusted Devices



[Laptops](#) →



[Desktops](#) →



[Workstations](#) →

Secure anywhere-work with Dell Trusted Workspace



Built-with & Built-in Hardware Security



Built-on Software Security

Visit us

dell.com/endpoint-security

Contact us

global.security.sales@dell.com

Read more

[Endpoint Security Blogs](#) →

Join the conversation

[in delltechnologies](#) [X @delltech](#)

Sources and disclaimers

¹Based 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.

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

³Source: Enterprise Strategy Group, a division of TechTarget, Custom Research Survey Commissioned by Dell Technologies, Assessing Organizations' Security Journeys, November 2023.