

# Anatomy of a Trusted Device

Learn what makes Dell the world’s most secure commercial AI PCs<sup>1</sup>



## 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.<sup>2</sup>



Top evaluation criteria when sourcing new PCs:

- Automated detection of BIOS events<sup>3</sup>
- Addressing high-risk configurations<sup>3</sup>

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 PCs<sup>1</sup>

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.<sup>1</sup>

[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.<sup>1</sup> [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.<sup>1</sup> [Learn more →](#)



### Verify firmware integrity

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

### 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.<sup>1</sup> [Learn more →](#)

### Secure end user credentials

Verify user access via Dell SafeID with ControlVault, a unique, dedicated security chip that keeps user credentials hidden from malware. *FIPS 140-3 Level 3 certified*.<sup>1</sup> [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.<sup>1</sup> [Learn more →](#)

## INDUSTRY LEADERSHIP

No PC manufacturer offers the BIOS-level visibility Dell does.<sup>1, 4</sup>

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

[Learn More →](#)



## 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](https://dell.com/endpoint-security)

### Contact us

[global.security.sales@dell.com](mailto:global.security.sales@dell.com)

### Read more

[Endpoint Security Blogs →](#)

### Join the conversation

[in delltechnologies](#)

[X @delltech](#)

### Sources and disclaimers

<sup>1</sup>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.

<sup>2</sup>Source: Futurum Group, Endpoint Security Trends, 2023.

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

<sup>4</sup>Principled Technology study results available for Intel-based devices only.