❯ EXPLORE
Dell Trusted Workspace

Secure anywhere-work

with hardware & software defenses built for today's cloud-based world.

Reduce the attack surface and stay ahead of modern threats with a comprehensive portfolio of hardware and software protections.

Learn more about the portfolio →

Dell secured the highest score
on the IDC Enterprise PC Vendor Trust Perception Index

Source: IDC, The Enterprise PC Trust Perception Index, 2025: Measuring Customer Perception of Trustworthiness (in Security, Privacy, Compliance, and ESG) for Enterprise PC Vendors, Doc #US53220125, March 2025.
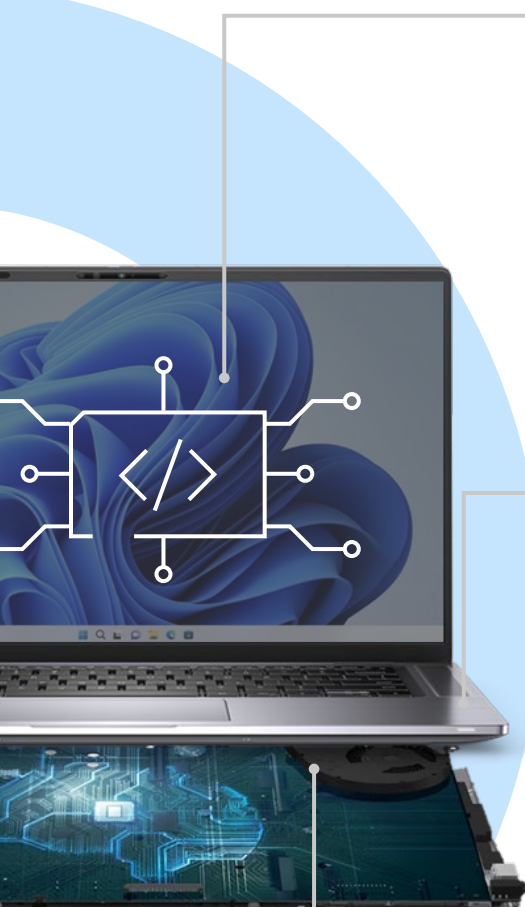
The world's most secure commercial AI PCs[1] →

Software to improve the security of any fleet →

DELLTechnologies

Dell Trusted Workspace

Multiple layers of defense

Built-on
Software Security

Layer on advanced threat protection with software from an expertly selected partner ecosystem. Take advantage of the benefits and efficiencies that come from consolidating security purchases.

Built-in
Hardware & Firmware Security

Prevent and detect foundational attacks with the world's most secure commercial AI PCs.[1] Deep defenses at the BIOS/firmware and hardware levels keep the device protected in-use.

Only Dell integrates PC telemetry with industry-leading software to improve fleet-wide security.[1]

Built-with
Supply Chain Security

Work confidently knowing your device is secure from first boot. Secure PC design, development and testing help reduce the risk of product vulnerabilities. Rigorous supply chain controls reduce the risk of product tampering.

Prevent, detect and respond to threats wherever they occur

Dell SafeGuard and Response

Dell SafeData

Stay protected from evolving threats
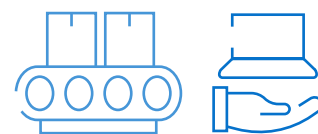
Dell SafeBIOS

Dell SafeID

Trust hardware is tamper-free on delivery

Dell SafeSupply Chain

DELLTechnologies

Dell Trusted Workspace Built-with & Built-in Security

World's most secure commercial AI PCs[1]

Be secure from first boot

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

Secure end user credentials

Verify user access with Dell-unique **SafeID**, a dedicated security chip that keeps user credentials hidden from malware. Now FIPS 140-3 Level 3 certified. [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. [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.

[Learn more](#) →

Catch known vulnerabilities

Dell-unique **Common Vulnerabilities and Exposures (CVE) Detection and Remediation**[2] monitors for publicly reported BIOS security flaws and recommends updates to mitigate risk.
[Learn more](#) →

PT Principled Technologies® *Industry Leadership Validated by Principled Technologies**

Shrink the IT-security gap with PC telemetry

Enrich software solutions with below-the-OS insights. Only Dell integrates PC telemetry with industry-leading software providers to improve fleet-wide security.[1] [Learn more](#) →

Explore Dell Trusted Devices

[Laptops](#) →

[Desktops](#) →

[Workstations](#) →

*Study results available for Intel-based devices only.

Copyright © Dell Inc. All Rights Reserved.

D&LL Technologies

Dell Trusted Workspace Built-on security

Software to improve the security of any fleet

Thwart advanced cyberattacks with **Dell SafeGuard and Response**

Prevent, detect and respond to threats wherever they occur. Artificial intelligence and machine learning proactively detect and block endpoint attacks, while security experts help hunt for and remediate identified threats across the endpoint, network and cloud.

Partner
CrowdStrike Falcon® →

Protect data on the device and in the cloud with **Dell SafeData**

Enable users to collaborate safely from anywhere. Netskope takes a datacentric approach to cloud security and access, protecting data and users everywhere, while Absolute gives IT visibility, protection and persistence outside the corporate firewall.

Partner
Self-healing for endpoints, apps & networks with
Absolute →

Explore Dell Security Services

With Dell, customers can self-manage security or have specialists manage it for them. Engage our fully-managed, 360° SecOps solution designed to prevent, respond and recover from security threats in the IT environment.

Learn more about Managed Detection and Response Pro Plus →

DELLTechnologies
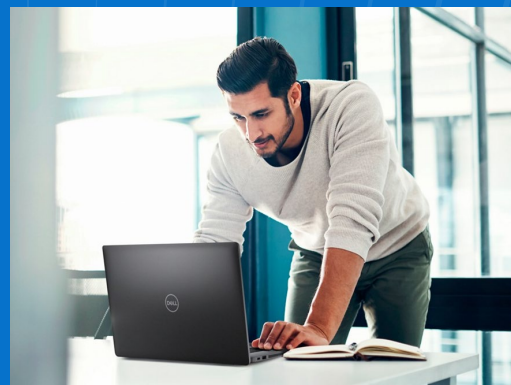
Dell Trusted Workspace Hardware-assisted security

Integrated security

Evolving cyber threats circumvent software-only defenses. Help shrink the attack surface of endpoints with hardware-assisted protections.

To protect against modern threats, hardware and software defenses must work together. That's where Dell can help. We work with industry-leading security partners, combining rich, device-level telemetry with cutting-edge threat detection to improve the security of your fleet.
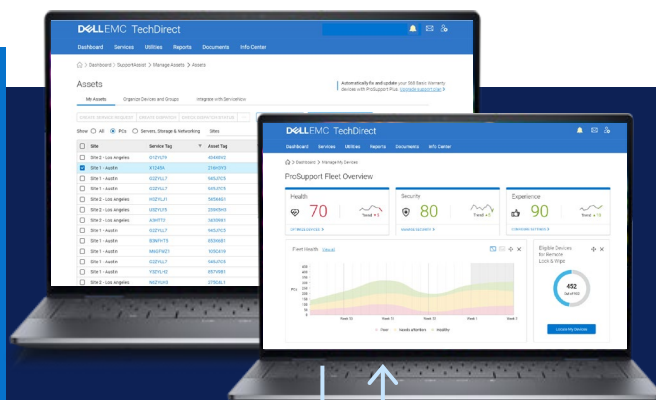
✓ **Reduce the attack surface**

✓ **Improve threat detection**

✓ **Maintain device trust**

✓ **Consolidate providers**

Only Dell integrates PC telemetry with industry-leading software to improve fleet-wide security[1][3]

Built-on Software Security

THE OS

Built-in Hardware & Firmware Security

World's most secure commercial AI PCs[1]

Dell SafeBIOS

PC Telemetry
Dell Trusted Device Application (DTD app) • Dell Client Device Manager (DCDM)

BIOS Verification | CVE Detection | Indicators of Attack

Partner "below-the-OS" silicon features

Built-with Supply Chain Security

Dell SafeSupply Chain[4]

Secured Component Verification
On Device ● On Cloud

DELLTechnologies
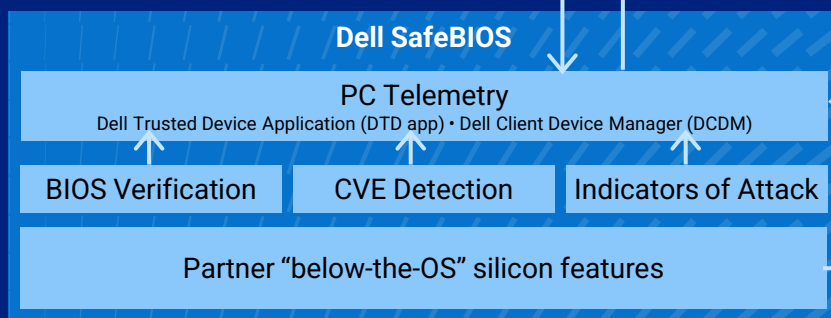
Secure anywhere-work with **Dell Trusted Workspace.**

Built-with & Built-in Hardware Security

Built-on Software Security

Reduce the attack surface and improve long-term cyber resilience with multiple layers of defense.

Visit us
dell.com/endpoint-security

Contact us
global.security.sales@dell.com

Read more
Endpoint Security Blogs →

Join the conversation
LinkedIn /delltechnologies

X @delltech

Sources and disclaimers

[1]Based on Dell internal analysis, October 2024 (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. A comparison of security features, April 2024. [2]Dell Client Device Manager's Security Module includes automated CVE remediation for BIOS and firmware-level flaws for managed environments. For unmanaged environments still using the DTD App, all of the existing features, including CVE Detection for the BIOS is available. (Note: CVE Detection for Firmware is available when Dell Command | Update is installed.) [3]Integrations available for CrowdStrike Falcon Insight XDR and Absolute. [4]Availability varies by region.

DELLTechnologies