Hybrid work exposed organizations to new attack vectors. With adversaries using increasingly sophisticated techniques, effective endpoint security today requires multiple layers of defense that protect the device, network and cloud.

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

Learn more about the portfolio →

The industry’s most secure commercial PCs¹ →

Software to improve the security of any fleet →
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 industry’s most secure commercial PCs. 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**
Dell Trusted Workspace  Built-with & Built-in Security

Industry’s most secure commercial PCs

Be secure from first boot
Rigorous, state-of-the-art supply chain controls and optional add-ons, like Dell-exclusive 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.

Secure end user credentials
Verify user access with Dell-unique SafeID, a dedicated security chip that keeps user credentials hidden from malware. Learn more

Maintain BIOS integrity
Catch and repel threats with Dell-unique BIOS verification SafeBIOS. 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
Common Vulnerabilities and Exposures (CVE) Detection monitors for publicly reported BIOS security flaws and recommends updates to mitigate risk. Learn more

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. Learn more

Explore Dell Trusted Devices

Latitude ➤

OptiPlex ➤

Precision ➤
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.

Partners
CrowdStrike Falcon® →
Secureworks® Taegis™ XDR →

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.

Partners
Self-healing for endpoints, apps and networks with Absolute →
Explore Security Service Edge solutions with Netskope →

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 →
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\(^1\)\(^2\)

Integrated security

THE OS

- Dell SafeBIOS
- Dell Trusted Device Application
- BIOS Verification
- CVE Detection
- Indicators of Attack
- Partner “below-the-OS” silicon features

Dell SafeSupply Chain\(^1\)

- Secured Component Verification
  - On Device
  - On Cloud

Built-in Hardware & Firmware Security

Built-on Software Security

Built-with Supply Chain Security

Copyright © Dell Inc. All Rights Reserved.
Secure anywhere-work with Dell Trusted Workspace.

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

Sources and disclaimers

1Based on Dell internal analysis, September 2023. Applicable to PCs on Intel processors. Not all features are available with all PCs. Additional purchase required for some features. Availability varies by region.

2Integrations available for CrowdStrike Falcon Insight XDR.

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

Copyright © Dell Inc. All Rights Reserved.