DELL Technologies

Dell Trusted Workspace

Secure-work-everywhere with hardware and software defenses built for today's cloud-based world.

Today's security challenges include managing an evolving threat landscape with a modern work environment in mind. Cybercriminals are leveraging sophisticated attacks to target multiple vulnerabilities. Reduce the attack surface with a comprehensive portfolio of hardware and software protections exclusive to Dell. Our highly coordinated, defense-based approach offsets threats by combining built-in protections with ongoing vigilance.

Built-on Security: Software protections to secure any fleet.

Prevent, detect and respond to cyberattacks with **Dell SafeGuard and Response**.

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

Detect BIOS tampering with **Dell SafeBIOS**.

Trust hardware is tamper-free on delivery with **Dell SafeSupply Chain**.

Secure user credentials with **Dell SafeID**.

Keep information private with **Dell SafeScreen** and **Dell SafeShutter**.

Built-in & Built-with Security: Hardware and firmware protections available via Dell devices, the industry's most secure commercial PCs[1]

[1] Based on Dell internal analysis, September 2022. Not all features available with all PCs. Additional purchase is required for some features.

Invisible, seamless protection enables smarter, faster experiences.

Dell Trusted Workspace helps secure endpoints for a modern IT environment. Our comprehensive defense framework includes 1) hardware and firmware protections to prevent and detect foundational attacks and 2) software protections to address advanced threats wherever they occur in an increasingly remote/hybrid environment. This powerful combination helps keeps data secure and users productive, protecting employees' workspaces everywhere.

Built-on Security *Advanced protection for any fleet*

Thwart advanced cyberattacks with Dell SafeGuard and Response.

Dell SafeGuard and Response, powered by CrowdStrike® Falcon, VMware® Carbon Black and Secureworks®, provides a comprehensive approach to endpoint threat management. 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.

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

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

Built-in & Built-with Security *via Dell commercial PCs*

Detect tampering with Dell SafeBIOS.

BIOS attacks are notoriously difficult to identify. Dell SafeBIOS alerts you to BIOS tampering so you can take swift action to quarantine and investigate the device. With Dell-exclusive off-host verification, the comparison image remains in a protected and separate location for post-attack forensics.[1]

Trust hardware is tamper-free on delivery with Dell SafeSupply Chain.

Dell Trusted Devices, the industry's most secure commercial PCs[1], are built with industry-leading supply chain defenses and integrity controls. Offers like Secured Component Verification and tamper-evident packaging help ensure devices are safe from the first boot.

Secure user credentials with Dell SafeID.

Only Dell secures user credentials in a dedicated security chip, keeping them hidden from malware that looks for and steals credentials.[1]

Keep information private with Dell SafeScreen and Dell SafeShutter.

Enable users to work from anywhere while keeping private information secure.

Learn more at: Dell.com/Endpoint-Security or contact your dedicated Dell Endpoint Security Specialist today at EndpointSecurity@Dell.com.

[1] Based on Dell internal analysis, September 2022. Not all features available with all PCs. Additional purchase is required for some features.