DELL Technologies

Dell Trusted Devices

The industry's most secure commercial PCs[1]

Dell Technologies understands that 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. An effective endpoint security strategy must address the entire attack surface. That is why Dell takes a comprehensive approach to securing devices above and below the operating system for optimal resilience and devices you can trust.

Above the OS:
Integrated security is part of the plan.

Below the OS:
Intrinsic security is in the design.

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**.

Invisible, seamless protection enables smarter, faster experiences.

Dell Trusted Devices create a secure foundation for the modern, mobile workforce. Our comprehensive family of endpoint security solutions work together to secure devices both above and below the operating system. This powerful combination keeps data secure and users productive — no matter where they choose to work.

Above the OS

Thwart advanced cyberattacks with Dell SafeGuard and Response.

Dell SafeGuard and Response, powered by 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. Dell Encryption provides granular security capabilities to encrypt all the data on the drive, shared multi-user data and individual user data with multiple encryption keys, all managed from a single dashboard to help meet compliance. 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.

Below the OS

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 are built with industry-leading supply chain security and integrity controls. Tamper-evident seals ensure that the device arrives in an untampered state. For high-value systems, you can reset the hard drive to NIST specifications to ensure a clean slate for your corporate image.

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: Delltechnologies.com/endpointsecurity or contact your dedicated Dell Endpoint Security Specialist today at endpointsecurity@dell.com.

[1] Based on Dell internal analysis, January 2020.