DELL TRUSTED DEVICES
Let’s start at the endpoint where all attack vectors need to be taken into consideration. This includes attacks that target the endpoint layers above the operating system like Data and Apps.

As well as those that target below the operating system layers like BIOS and Firmware.
Built-In Security

Dell Trusted Devices endpoint security protection begins with the built-in protection provided on our commercial PCs through Dell SafeBIOS.
Dell SafeBIOS

At the lowest level of the PC stack, the BIOS (Basic Input/Output System) is a critical component that should not be overlooked when thinking about endpoint security.

Off-host BIOS Verification uses a secure cloud environment to conduct a “point in time” check for the integrity of the BIOS.
If a BIOS appears compromised, the BIOS image is captured for forensic analysis.
With over 300 BIOS configurations possible, which may appear like normal administrative actions, an attack could easily go undetected. With BIOS Indicators of Attack (IoA), attacks are identified and the IT administrator is alerted.
Below the OS Features

Now that the BIOS layer is protected, other considerations on the device must be made, like multifactor authentication and digital privacy.

Keep your devices safe and help them stay protected from malware attacks with our exclusive ControlVault security chip that stores end users’ authentication credentials.
Below the OS Features

Dell’s innovative solution uses the backlight to narrow the endpoint screen’s field-of-view and maintain visual security.
SafeSupply Chain² mitigates risks that could be introduced in the network between the factory and final destination, covering supply chain security and integrity controls like tamper evident seals and NIST level hard drive wipe.
Dell SafeData

Now that supply chain and hardware are secured, data needs to be protected so that you stay compliant.
Absolute Persistence repairs and restores endpoint applications to their original safe state in case of malicious attacks.
With comprehensive data protection on any endpoint, Dell Encryption offers simple, flexible encryption that maintains productivity and seamlessly integrates with existing systems management and authentication processes.
Data that is created, collaborated on and used in the cloud is often left unprotected. Netskope provides visibility, monitoring and data loss prevention for cloud-based applications.
Dell SafeGuard and Response

The final layer of endpoint protection safeguards your device from malware, ransomware, non-malware and unknown attacks.
Starting with VMware Carbon Black Endpoint Standard, our next-generation antivirus and endpoint detection and response protects against the full spectrum of modern day cyber attacks from a cloud-based platform.
Secureworks Threat Detection and Response (TDR) is a cloud-native application that automatically analyzes security telemetry to alert users to known and unknown threats across endpoints, network and cloud environments. TDR provides customers that single view of threat intel across endpoint, network and cloud.
Dell Trusted Devices

The industry’s most secure commercial PCs.¹

Dell SafeGuard and Response

Secureworks TDR
VMware Carbon Black Cloud

Dell SafeBIOS

Off-Host BIOS Verification
BIOS Image Capture
BIOS Indicators of Attack

Dell SafeData

Netskope
Dell Encryption
Absolute

Dell SafeScreen

Dell SafeID

Dell SafeData

Safety Supply Chain²

¹Based on Dell internal analysis, January 2020. Specifications cited in this brochure may be used in the following countries: Asia, China, Europe, France, Germany, Hong Kong, India, Israel, Korea, South Africa, Taiwan, United States, and Vietnam. Support Summary: Comparison of security features capability to competitors is updated Jan 2020. Dell wins with DDPE and CC certifications for full disk encryption (available on all models); Dell SafeBIOS - BIOS verification (included on all models); Dell SafeID - ControlVault (included on select models); and Corrupt BIOS Image Capture (included on all models).

²North America Only