



# Protect your fleet at every layer with Intel vPro® platform security

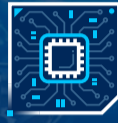
## Deep IT security is a hybrid-workplace necessity.

Here's how Intel vPro® platform devices deliver hardware-based protection for your users, data, and business—no matter where they go.

### Hardware layer

#### Trustworthy components

Feel confident in your investment with complete component traceability, starting at the factory floor.



#### Secure boot-up

Allow only untampered firmware and trusted OS images to load with Intel® BIOS Guard and Secure Boot.

### Firmware and BIOS layer



#### Attestable security status

Use static and dynamic root-of-trust measurements in the Intel® Trusted Platform Module to confirm below-the-OS security and detect abnormalities.



#### Streamlined device recovery

Remotely manage and update devices with a protected hardware channel for in/out-of-band management.

### Application layer



#### Protected data, keys, and identity

Provide passwordless, enhanced sign-in via a hardware-isolated Key Locker—plus accelerated crypto operations and secure key generation.



#### Application and memory security

Employ hardware-based total memory encryption to protect against cold-boot attacks and isolate apps from malware via virtualization-based security.



#### CPU-based threat detection

Ward off malware that evades traditional antivirus software with AI-based CPU threat monitoring.

## Looking for more hybrid workplace IT management insights?

Get additional considerations for your next business PC buying initiative in our fleet management handbook, *Four Essentials for the Hybrid Workplace*.

Download now →

