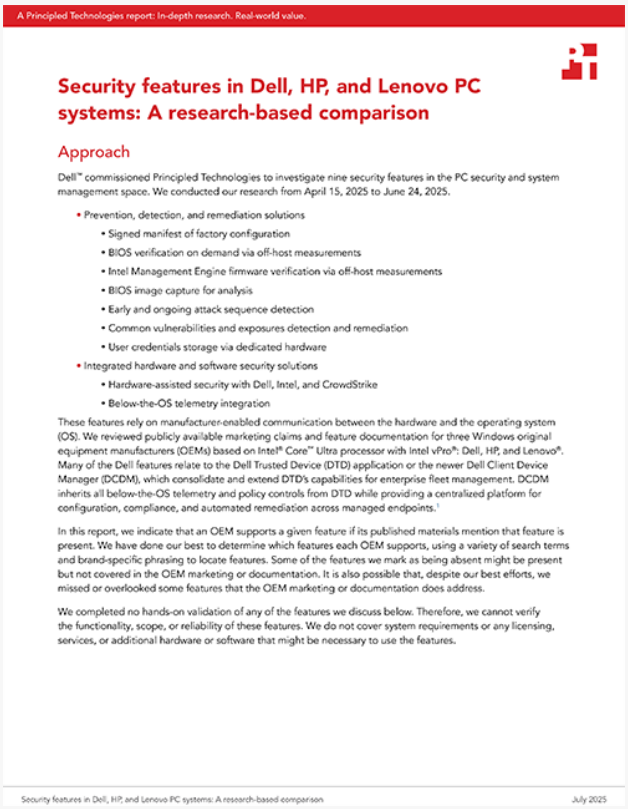
New third-party research report reveals Dell Technologies advantages in the PC security and system management space

A comprehensive suite of below-the-operating-system (OS) features set Dell apart from competitors HP and Lenovo.

ROUND ROCK, TX, UNITED STATES, August 19, 2025 /EINPresswire.com/ -- PC security is a major concern for decision-makers who understand the high cost of potential breaches. To help those considering purchasing Dell Technologies, HP, or Lenovo PCs, Principled Technologies (PT) conducted research into nine security features using the published materials of each original equipment manufacturer (OEM). PT found that Dell fully supports nine critical security capabilities designed to prevent, detect, respond to, and remediate firmware and hardware threats, ensuring enterprise devices remain secure and compliant:


A Principled Technologies report: In-depth research. Real-world value.

Security features in Dell, HP, and Lenovo PC systems: A research-based comparison

Approach

Dell™ commissioned Principled Technologies to investigate nine security features in the PC security and system management space. We conducted our research from April 15, 2025 to June 24, 2025.

- Prevention, detection, and remediation solutions
  - Signed manifest of factory configuration
  - BIOS verification on demand via off-host measurements
  - Intel Management Engine firmware verification via off-host measurements
  - BIOS image capture for analysis
  - Early and ongoing attack sequence detection
  - Common vulnerabilities and exposures detection and remediation
  - User credentials storage via dedicated hardware
- Integrated hardware and software security solutions
  - Hardware-assisted security with Dell, Intel, and CrowdStrike
  - Below-the-OS telemetry integration

These features rely on manufacturer-enabled communication between the hardware and the operating system (OS). We reviewed publicly available marketing claims and feature documentation for three Windows original equipment manufacturers (OEMs) based on Intel® Core™ Ultra processor with Intel vPro®: Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device (DTD) application or the newer Dell Client Device Manager (DCDM), which consolidate and extend DTD's capabilities for enterprise fleet management. DCDM inherits all below-the-OS telemetry and policy controls from DTD while providing a centralized platform for configuration, compliance, and automated remediation across managed endpoints.[1]

In this report, we indicate that an OEM supports a given feature if its published materials mention that feature is present. We have done our best to determine which features each OEM supports, using a variety of search terms and brand-specific phrasing to locate features. Some of the features we mark as being absent might be present but not covered in the OEM marketing or documentation. It is also possible that, despite our best efforts, we missed or overlooked some features that the OEM marketing or documentation does address.

We completed no hands-on validation of any of the features we discuss below. Therefore, we cannot verify the functionality, scope, or reliability of these features. We do not cover system requirements or any licensing, services, or additional hardware or software that might be necessary to use the features.

Security features in Dell, HP, and Lenovo PC systems: A research-based comparison July 2025

Security features in Dell, HP, and Lenovo PC systems: A research-based comparison

- Signed manifest of factory configuration—available both on device* and via cloud (Secured Component Verification)
- BIOS verification on-demand via off-host measurements
- Intel Management Engine firmware verification via off-host measurements
- BIOS image capture for analysis
- Early and ongoing attack sequence detection (Indicators of Attack)

- Common vulnerabilities and exposures (CVE) detection and remediation
- User credentials storage via dedicated hardware (SafeID with ControlVault 3+)
- Hardware-assisted security with Dell, Intel, and CrowdStrike
- Below-the-OS telemetry integration

The report states, “Based on publicly available documentation, Dell appears to support all nine of the below-the-OS security features evaluated. HP fully supports one feature and partially supports two, while Lenovo fully supports one and offers partial support for one other.”

PT found that among the unique advantages Dell offers is Secured Component Verification (SCV), which offers both on-device and cloud-based signed manifest verification for factory configurations. This includes an air-gapped option ideal for high-security environments such as federal agencies. Dell is also the only OEM providing off-host BIOS and Intel Management Engine firmware verification against known-good references stored securely in the cloud, enabling remote attestation aligned with Zero Trust principles.

At a time when enterprises face increasingly sophisticated cyber threats targeting firmware and hardware layers, it’s critical to prioritize PC security. To explore the Principled Technologies report about industry-leading security solutions from Dell, visit https://facts.pt/B4rJQgV.

*Availability based on select SKUs in North America market.

About Principled Technologies, Inc.
Principled Technologies, Inc. is the leading provider of technology marketing and learning & development services.

Principled Technologies, Inc. is located in Durham, North Carolina, USA. For more information, please visit www.principledtechnologies.com.

Sharon Horton
Principled Technologies, Inc.
press@principledtechnologies.com
Visit us on social media:
LinkedIn
Facebook
YouTube
X
