

Principled Technologies research highlights Dell PC security advantages

Independent research shows Dell PCs deliver more comprehensive below-the-OS security and system management capabilities than HP or Lenovo PCs with Intel vPro.

ROUND ROCK, TX, UNITED STATES, July 24, 2026 /EINPresswire.com/ -- As the prevalence of firmware- and hardware-level attacks rises, enterprise IT and security decision-makers increasingly prioritize PC security and endpoint protection. To help organizations evaluate leading business PCs, Principled Technologies (PT) conducted independent research comparing the security features of Dell, HP, and Lenovo PCs powered by Intel Core Ultra processors with Intel vPro, with a focus on below-the-operating-system (below-the-OS) security and firmware protection.

Using publicly available original equipment manufacturer (OEM) documentation, PT examined support for 10 critical firmware and hardware capabilities that aim to prevent, detect, and remediate advanced threats. The research indicated that Dell fully supports all 10 evaluated security features, while HP and Lenovo lag behind. From the report: "Based on publicly available documentation, Dell appears to support all ten of the below-the-OS security features evaluated. HP fully supports one feature and partially supports three, while Lenovo fully supports two and offers partial support for one other."



Principled Technologies®

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 10 security features in the PC security and system management space. We conducted our research from May 28, 2026 to July 14, 2026.

- Prevention, detection, and remediation solutions
 - Signed manifest of factory configuration
 - Quantum-resistant embedded security controller, BIOS, and embedded controller (EC) signing updates
 - Quantum-resistant 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 (CVEs) 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 PCs based on Intel Core™ Ultra processors with Intel vPro® from three Windows original equipment manufacturers (OEMs): 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 consolidates and extends DTD 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.

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's 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 2026

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

Ten below-the-OS security capabilities evaluated

According to the research, Dell provides full support for the following enterprise-grade security and system management features:

- Signed manifest of factory configuration
- Quantum-resistant embedded security controller, BIOS, and Embedded Controller (EC) signing updates
- Quantum-resistant BIOS verification on demand via off-host measurements
- Intel Management Engine firmware verification via off-host measurements
- BIOS image capture for forensic and security analysis
- Early and ongoing attack sequence detection
- Detection and remediation of common vulnerabilities and exposures (CVEs)
- User credential storage using dedicated hardware
- Hardware-assisted security with Dell, Intel, and CrowdStrike
- Below-the-OS telemetry integration for enhanced visibility

Key differentiators in PC security

The report highlights Dell Secured Component Verification (SCV) as a key Dell advantage. For SCV on Cloud, Dell manages the full verification pipeline in-house through its own cloud infrastructure, maintaining root of trust in the verification process and enabling fleetwide visibility through Microsoft Intune, Dell TechDirect, and CrowdStrike Falcon—without requiring organizations to deploy or maintain dedicated verification server infrastructure.

Dell was the only OEM of the three to provide off-host BIOS verification—now strengthened with quantum-resistant hashing—and off-host Intel Management Engine firmware verification against known-good references stored securely in Dell's cloud infrastructure. These capabilities enable remote device attestation, directly supporting Zero Trust security architectures and modern compliance requirements.

The report also highlights the Dell, Intel, and CrowdStrike partnership as a unique differentiator. Dell Trusted Device provides native integration with the CrowdStrike Falcon platform, surfacing BIOS verification results, Indicators of Attack, Intel ME Firmware Verification, CVE Detection, and Secured Component Verification telemetry directly within Falcon—with more than 60 custom indicators of compromise jointly developed for Dell infrastructure. Additionally, Dell ControlVault 3+ achieved FIPS 140-3 level 3 certification, the highest credential security level among the OEMs evaluated.

The importance of below-the-OS security

Firmware and hardware attacks can bypass traditional endpoint security tools, making below-the-OS protections essential for organizations seeking stronger resilience, compliance, and risk reduction. As cyber threats increasingly target firmware, independent research confirms Dell PCs powered by Intel vPro offer industry-leading security and system management depth compared to HP and Lenovo alternatives.

Learn more

Read the full [Principled Technologies research report](#).

About Principled Technologies

Principled Technologies, Inc. is the leading provider of fact-based marketing and competitive analysis backed by transparent methodologies.

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](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/928905410>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.