

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.

ROUND ROCK, TX, UNITED STATES, April 30, 2026 /EINPresswire.com/ -- As firmware- and hardware-level attacks continue to rise, PC security and endpoint protection have become top priorities for enterprise IT and security decision-makers. 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 AMD Ryzen AI PRO processors, 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 eight critical firmware and hardware capabilities designed to prevent, detect, and remediate advanced threats. The research found that Dell fully supports all eight evaluated security features, while HP and Lenovo lag behind. From the report, “Based on publicly available documentation, Dell appears to support all of the below-the-OS security features we evaluated. HP partially supports three features, while Lenovo fully supports two.”



Principled Technologies®

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

A research-based comparison of security features in Dell, HP, and Lenovo PC systems

How we conducted our research

Dell™ commissioned Principled Technologies to investigate the following eight security features in the PC security and system management space. We conducted our research from February 23, 2026 to March 20, 2026.

- Prevention, detection, and remediation solutions
 - Signed manifest of factory configuration
 - BIOS verification on demand via off-host measurements
 - 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
 - Below-the-OS telemetry integration

All of 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)—Dell, HP, and Lenovo®—focusing on their laptop and desktop systems based on the latest AMD Ryzen™ AI PRO processors.

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'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.

In this report, our stating that an OEM supports a given feature means that the OEM's published materials mention the presence of that feature. We have done our best to determine the features that each OEM supports, and we used a variety of search terms and brand-specific phrasing to locate features. It is possible that a feature we mark as being absent is in fact present but is missing from the OEM marketing and documentation. Despite our best efforts, we might also have missed some features that the marketing and documentation do mention.

Because we did not perform any hands-on validation of the features, we cannot verify their functionality, scope, or reliability. We do not address system requirements or any licensing, services, or additional hardware or software required to use the features.

A research-based comparison of security features in Dell, HP, and Lenovo PC systems April 2026

A research-based comparison of security features in Dell, HP, and Lenovo PC systems

Eight 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 factory configuration manifest
- On-demand BIOS verification using off-host measurements
- AMD Secure Processor (ASP) firmware verification via off-host measurements
- BIOS image capture for forensic and security analysis
- Early and continuous attack sequence detection
- Detection and remediation of common vulnerabilities and exposures (CVEs)
- User credential storage using dedicated hardware
- Below-the-OS telemetry integration for enhanced visibility

Key differentiators in PC security

The report highlights Dell Secured Component Verification (SCV), a unique Dell advantage. SCV enables both on-device and cloud-based signed manifest verification of factory configurations, including an air-gapped verification option designed for high-security environments such as government and federal agencies.

Additionally, Dell was the only OEM of the three to provide off-host BIOS and AMD Secure Processor (ASP) firmware verification against known-good references stored securely in the cloud. This capability enables remote device attestation, directly supporting Zero Trust security architectures and modern compliance requirements.

Why below-the-OS security matters

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 offer industry-leading security and system management depth compared to HP and Lenovo alternatives.

Learn more

To read the full Principled Technologies research report on Dell, HP, and Lenovo PC security and system management, visit <https://facts.pt/uG4rGQm>.

About Principled Technologies

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](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/909389967>

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.