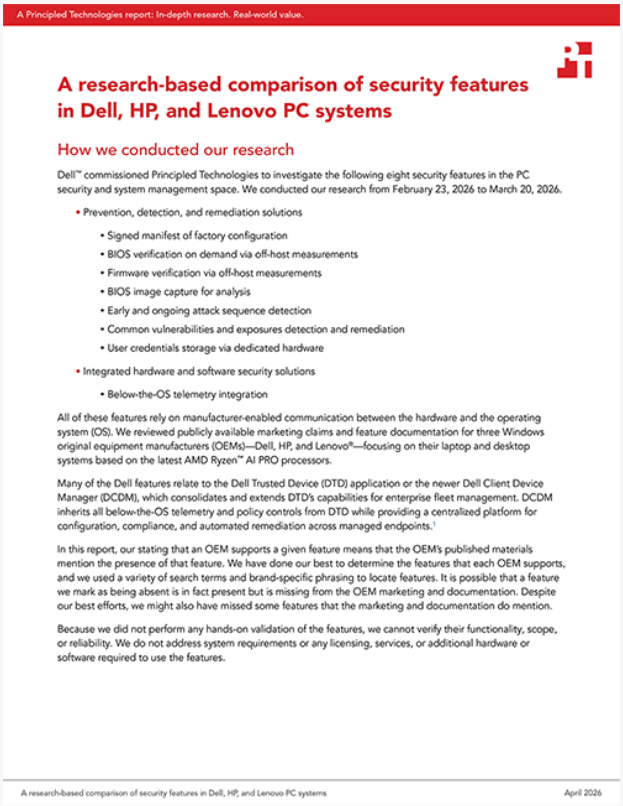
Principled Technologies research highlights Dell PC security advantages

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



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

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.”

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 manifestOn-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
