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.

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

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."

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
