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.[1]

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.

Table 1 lists the primary sources we used to research each OEMs' security features. We also consulted the OEM websites, which we cite in the sections below.

Table 1: The primary sources we used to research each OEM's security features.

Dell	HP	Lenovo
• White paper: "Client Solutions: Dell Trusted Device Below the OS White Paper"[2] • Blog post: "Maintain Device Trust with Dell"[3] • Blog post: "How To Weather the Cyber Identity Crisis"[4]	• White paper: "HP Sure Start"[5]	• White paper: "Firmware Resiliency with Lenovo ThinkShield"[6]

Prevention, detection, and remediation solutions

Signed manifest of factory configuration

We researched whether each OEM provides tools to verify a device's hardware and firmware configuration against its original factory state using signed component manifests. We found that all three of the OEMs we looked at offer capabilities that enable this form of supply chain integrity validation at time of delivery and options for implementing verification at scale. However, **Dell Secured Component Verification (SCV) differs from the HP and Lenovo offerings in several important ways**.[7,8,9]

- Dell differentiators:
  - **Collecting platform certificates without internet connection:** The Dell SCV on Device solution provides the option for a platform certificate on the device, eliminating the need for customers to connect to the internet to collect the certificate. This is advantageous for organizations, such as federal agencies, that require an air-gapped option isolated from unsecured systems and networks.[10]
  - **Ease of use, visibility, and reporting:** For SCV on Cloud, Dell uses an in-house verification method (the Dell Trusted Device application) that integrates with third-party solutions. This allows admins to view results and reports within the Microsoft Intune environment and Dell TechDirect, providing automated, fleetwide visibility. Because Dell manages the verification pipeline through its own cloud infrastructure, organizations gain off-host attestation without deploying dedicated verification infrastructure.[11]
  - **Alignment with Zero Trust:** According to Dell, "SCV provides hardware-level attestation that the endpoint matches its known-good 'as-built' state. When combined with TPM [Trusted Platform Module]-based attestation and Dell Trusted Device telemetry, SCV on Cloud allows remote device attestation, aligning with Zero Trust ('never trust, always verify') guidance and NIST [National Institute of Standards and Technology] supply chain assurance practices."[12]

- HP and Lenovo limitations:
  - HP's platform certificate solution requires retrieving certificates from the HP API service or downloading them manually via HP Client Management Script Library (CMSL). After retrieving the certificate, CMSL enables local integrity verification and supports scripted fleet-wide deployment, though attestation remains on-device. For off-host remote attestation, HP relies on Host Integrity at Runtime and Start-up (HIRS), where the endpoint reports TPM measurements to a customer-managed attestation server. HP offers a preconfigured HIRS deployment option, though the customer still owns the underlying infrastructure and is responsible for its deployment and configuration.[13] This provides organizations with multiple verification paths, though each requires internet connectivity and customer-managed infrastructure.
  - Lenovo offers certificate-based supply chain attestation through ThinkShield® Build Assure, which enables customers to electronically verify device integrity from manufacturing through deployment. However, all available technical documentation for Build Assure doesn't address AMD processor platforms, and we did not identify technical documentation confirming its availability on AMD processor-based commercial PCs.[14,15]

BIOS verification on demand via off-host measurements

We looked for solutions where the OEM verifies the integrity of the BIOS during boot or through on-demand validation against a known-good version. Dell, HP, and Lenovo all perform BIOS verification at boot and support automatic recovery using a locally stored, signed image.[16,17,18] Dell extends this with off-host BIOS verification, now quantum-ready,[19] which allows administrators to perform on-demand integrity checks by comparing the BIOS hash against a known-good reference securely stored in the Dell cloud infrastructure.[20] HP offers runtime BIOS integrity checks every time the device is powered off or put into hibernate or sleep mode, checking against a locally embedded copy of the BIOS.[21] We did not identify any comparable post-boot or off-host BIOS verification capabilities from Lenovo. **Dell is the only OEM in this group that validates BIOS integrity against an external reference.**

Firmware verification via off-host measurements

AMD provides silicon root of trust via the AMD Secure Processor (ASP) that forms the foundation. This dedicated on-chip co-processor authenticates the initial firmware during startup, ensuring the system boots into a known good state before the operating system even loads. We researched solutions that verify the integrity of ASP firmware, given its privileged access to platform hardware. All three OEMs protect ASP firmware during the boot process and support automatic recovery using locally stored backups. **Dell extends this by comparing local measurements against a known-good reference stored off-host in it's secure cloud infrastructure.**[22,23] We found no evidence that HP or Lenovo support ASP validation against an external reference.[24,25]

BIOS image capture for analysis

We determined whether solutions not only restore the BIOS after corruption but also preserve the compromised image for forensic review. Dell supplements its automated recovery process with BIOS image capture through SafeBIOS recovery, allowing administrators to retain a copy of the corrupted firmware for analysis.[26] HP and Lenovo both support automatic BIOS restoration using locally validated backups, but they do not document any ability for administrators to retain or export the tampered BIOS image during the recovery process.[27,28] **Of the OEMs we researched, Dell is the only one to provide BIOS image capture as part of its recovery workflow.**

Early and ongoing attack sequence detection

Solutions that monitor BIOS-level activity over time detect the early stages of an attack, such as configuration drift or tampering attempts. Dell delivers this capability through Indicators of Attack (IoA), which monitors below-the-OS changes and applies threat models developed by Dell to identify suspicious activity sequences. The Dell Trusted Device application makes alerts available through the Dell Client Device Manager, the DTD Local Console, Windows Event Viewer, Dell TechDirect, and integrated third-party tools.[29]

HP relies on using saved system configurations and settings stored in a protected non-volatile memory store accessible only by its HP Endpoint Security Controller (ESC) device to verify authenticity and detect changes. If any change is detected, it auto-heals the BIOS, firmware, and more by reloading the previously saved good configuration. It creates alerts and events that users can access via the HP ESC and Microsoft Event Viewer. HP does not appear to accumulate threats or use external sources to model threats.[30]

As part of Lenovo ThinkShield offerings, Lenovo PCs can use Firmware Defense powered by Eclypsium software to collect and monitor telemetry to analyze and detect anomalies including configuration drift, below-the-OS integrity, and more. It uses existing known-good databases or custom-made organization databases to maintain device integrity and recognize threats. Lenovo ThinkShield Firmware Defense also claims to have "cross-correlation."[31] Additionally, Lenovo ThinkShield offers a solution powered by SentinelOne that uses AI analytics to correlate activities and threats to protect against malicious actors.[32]

Dell is the only OEM in this comparison to deliver this capability through a first-party application included with its commercial PCs. Lenovo offers comparable detection and correlation through third-party partner solutions.

Common vulnerabilities and exposures detection and remediation

We looked for solutions that detect known firmware vulnerabilities and provide actionable remediation. Dell proactively scans BIOS against common vulnerabilities and exposures (CVEs) listed in the US National Vulnerability Database, using Dell Security Advisories to surface relevant issues.[33] The Dell Client Device Manager can work in conjunction with an endpoint management service such as Intune to prioritize CVE vulnerabilities and implement auto-remediation processes to reduce manual patching time.[34] HP and Lenovo publish CVE advisories and release firmware updates in response, but neither OEM offers built-in detection, telemetry, or automated remediation capabilities integrated into their device management workflows.[35,36]
Of the vendors we researched, Dell is the only one to combine vulnerability detection with automated firmware remediation at scale.

User credentials storage via dedicated hardware

Purpose-built hardware-based solutions can isolate and protect user credentials such as passwords, encryption keys, and biometric data. All three OEMs use TPM 2.0 to secure cryptographic keys and support Windows Hello as required by Windows 11.[37] However, Dell also offers the option of a dedicated credential security chip. Dell SafeID with ControlVault isolates credential processing in a standalone hardware module, offering stronger protection against firmware and OS-level threats.[38] In April 2025, Dell ControlVault™ 3+ achieved Federal Information Processing Standards (FIPS) 140-3 level 3 certification.[39] Lenovo claims FIPS 140-3 certification for the ThinkShield portfolio, though doesn't list which level or identify a certified component.[40] HP claims level 1 FIPS 140-3 certification for its Endpoint Security Controller.[41] HP uses its Endpoint Security Controller to protect credential data as part of a broader security architecture, while Lenovo limits hardware-based isolation to biometric data and TPM-based key storage.[42,43]
Of the OEMs we researched, only Dell offers a hardware solution, purpose-built with the highest-level FIPS validation, to isolate and protect a full range of user credentials.

Below-the-OS telemetry integration

We also looked for how the OEMs integrate BIOS and firmware telemetry into broader enterprise management tools. Dell enables native integration through the Dell Trusted Device and Dell Client Device Manager applications. Organizations can use these platforms to stream BIOS telemetry directly into third-party tools without the need for custom connectors or middleware.[44,45,46] For example, Dell offers CrowdStrike Falcon Prevent as an optional software add-on at purchase. With both the DTD app and CrowdStrike Falcon sensor installed, below-the-OS security alerts integrate directly with the CrowdStrike Falcon console.[47] Similar integrations are also available with Microsoft Intune, Absolute Security, and Security Information and Event Management (SIEM) solutions.

HP surfaces firmware events through Windows Event Viewer but requires custom workflows for monitoring.[48] Lenovo provides similar telemetry through two paths. First, ThinkShield Firmware Assurance surfaces this telemetry to SIEM platforms through native integration hooks.[49] As another option, ThinkShield Firmware Defense, delivered via a separate deployment of the Eclypsium platform, supports integration with tools such as Intune and Splunk®. However, this capability depends on third-party infrastructure and does not tie directly into Lenovo's native management tools.[50] **While HP provides partial support and Lenovo provides full support in this category, Dell is the only OEM we researched that offers natively integrated BIOS and firmware telemetry and policy controls through a single, vendor-managed endpoint security and management stack.**

Summary of findings

Table 2 summarizes our findings. 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.

Table 2: Summary of available below-the-OS security features, based on publicly available documentation.

	Dell	HP	Lenovo
Signed manifest of factory configuration – available on device	✓	✗	✗
Signed manifest of factory configuration – available via cloud	✓	▲*	✗
BIOS verification on-demand via off-host measurements	✓	✗	✗
AMD Secure Processor firmware verification via off-host measurements (via Dell BIOS verification noted above)	✓	✗	✗
BIOS image capture for analysis	✓	✗	✗
Early and ongoing attack sequence detection	✓	✗	✓†
Common vulnerabilities and exposures detection and remediation	✓	✗	✗
User credentials storage via dedicated hardware	✓	▲††	✗
Below-the-OS telemetry integration	✓	▲¶	✓

✓ full support

▲ partial support

✗ no support

* Customer-managed infrastructure required.
† Provided through separately licensed third-party partner solutions.
†† Multi-purpose security controller; not dedicated to credential isolation.
¶ Windows Event Viewer only; custom workflows required.

1. Tom Bentz, "Maintain Device Trust with Dell," accessed March 20, 2026, https://www.dell.com/en-us/blog/maintain-device-trust-with-dell/.
2. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed March 20, 2026, https://www.delltechnologies.com/asset/en-ae/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
3. Tom Bentz, "Maintain Device Trust with Dell," accessed March 20, 2026, https://www.dell.com/en-us/blog/maintain-device-trust-with-dell/.
4. Charles Robison, "How To Weather the Cyber Identity Crisis," accessed March 20, 2025, https://www.dell.com/en-us/blog/how-to-weather-the-cyber-identity-crisis/.
5. HP, "HP Sure Start," accessed March 20, 2026, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
6. Lenovo, "Firmware Resiliency with Lenovo ThinkShield," accessed March 20, 2026, https://www.lenovo.com/us/en/resources/data-center-solutions/whitepapers/firmware-resiliency-with-lenovo-thinkshield/.
7. Dell Technologies, "Secured Component Verification," accessed March 20, 2026, https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/technical-support/secured-component-verification-datasheet.pdf.
8. HP, "HP Platform Certificate Datasheet," accessed March 20, 2026, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA8-3109ENW.
9. Lenovo, "Lenovo and Intel Collaborate on ThinkShield Build Assure to Enhance Supply Chain Cyber Security," accessed March 20, 2026, https://news.lenovo.com/pressroom/press-releases/intel-collaborate-thinkshield-build-assure-supply-chain-cyber-security/.
10. Note: The SCV on Device option is available in only North America and possibly only on specific devices. Dell Technologies, "Dell SafeSupply Chain," accessed March 20, 2026, https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/technical-support/dell-safe-supply-chain-datasheet.pdf.
11. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed March 20, 2026, https://www.delltechnologies.com/asset/en-ae/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
12. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper."
13. HP, "HP Platform Certificate Datasheet," accessed March 20, 2026, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA8-3109ENW.
14. Lenovo, "Lenovo and Intel Collaborate on ThinkShield Build Assure to Enhance Supply Chain Cyber Security," accessed March 20, 2026, https://news.lenovo.com/pressroom/press-releases/intel-collaborate-thinkshield-build-assure-supply-chain-cyber-security/.
15. Intel, "Transparent Supply Chain," accessed March 20, 2026, https://www.intel.com/content/www/us/en/security/security-practices/transparent-supply-chain.html.
16. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed March 20, 2026, https://www.delltechnologies.com/asset/en-ae/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
17. HP, "HP Sure Start," accessed March 20, 2026, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
18. Lenovo, "Firmware Resiliency with Lenovo ThinkShield," accessed March 20, 2026, https://www.lenovo.com/us/en/resources/data-center-solutions/whitepapers/firmware-resiliency-with-lenovo-thinkshield/.
19. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed March 20, 2026, https://www.delltechnologies.com/asset/en-ae/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
20. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper."
21. HP, "HP Sure Start," accessed March 20, 2026, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
22. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed March 20, 2026, https://www.delltechnologies.com/asset/en-ae/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
23. Tom Bentz, "The Secret Sauce Behind Dell Trusted Devices," accessed March 20, 2026, https://www.dell.com/en-us/blog/the-secret-sauce-behind-dell-trusted-devices/.
24. HP, "HP Sure Start," accessed March 20, 2026, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
25. Lenovo, "Firmware Resiliency with Lenovo ThinkShield," accessed March 20, 2026, https://www.lenovo.com/us/en/resources/data-center-solutions/whitepapers/firmware-resiliency-with-lenovo-thinkshield/.
26. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed March 20, 2026, https://www.delltechnologies.com/asset/en-ae/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.

27. HP, "HP Sure Start," accessed March 20, 2026, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
28. Lenovo, "Firmware Resiliency with Lenovo ThinkShield," accessed March 20, 2026, https://www.lenovo.com/us/en/resources/data-center-solutions/whitepapers/firmware-resiliency-with-lenovo-thinkshield/.
29. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed March 20, 2026, https://www.delltechnologies.com/asset/en-ae/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
30. HP, "HP Sure Start," accessed March 20, 2026, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
31. Lenovo, "Solution overview," accessed March 20, 2026, https://thinkshield.lenovocloudsoftware.com/portal/en/kb/articles/solution-overview.
32. SentinelOne and Lenovo, "Lenovo ThinkShield XDR," accessed March 20, 2026, https://www.sentinelone.com/resources/datasheets/assets/lenovo-fy26/lenovo-thinkshield-xdr-en.
33. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed March 20, 2026, https://www.delltechnologies.com/asset/en-ae/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
34. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper."
35. HP, "Security Bulletins," accessed March 20, 2026, https://support.hp.com/us-en/security-bulletins.
36. Lenovo, "Lenovo Product Security Advisories and Announcements," accessed March 20, 2026, https://support.lenovo.com/us/en/product_security/home.
37. Microsoft, "Windows 11 Specifications," accessed March 20, 2026, https://www.microsoft.com/en-us/windows/windows-11-specifications#table1.
38. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed March 20, 2026, https://www.delltechnologies.com/asset/en-ae/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
39. SentinelOne and Lenovo, "How To Weather the Cyber Identity Crisis," accessed March 20, 2026, https://www.dell.com/en-us/blog/how-to-weather-the-cyber-identity-crisis/.
40. Lenovo, "ThinkShield Extended Solutions Guide," accessed March 20, 2026, https://techtoday.lenovo.com/sites/default/files/2026-01/thinkshield-extended-solutions-guide-ww-en.pdf.
41. HP, "HP Sure Start," accessed March 20, 2026, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
42. HP, "HP Sure Start."
43. Lenovo, "Converged security to protect the workforce of the future," accessed March 20, 2026, https://techtoday.lenovo.com/sites/default/files/2022-08/Security-ThinkShield-Solutions-Guide-MW.pdf.
44. Tom Bentz, "Maintain Device Trust with Dell," accessed March 20, 2026, https://www.dell.com/en-us/blog/maintain-device-trust-with-dell/.
45. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed March 20, 2026, https://www.delltechnologies.com/asset/en-ae/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
46. Javier Madriz, "Visibility is an Absolute Must for Security," accessed March 20, 2026, https://www.dell.com/en-us/blog/visibility-is-an-absolute-must-for-security/.
47. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed March 20, 2026, https://www.delltechnologies.com/asset/en-ae/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
48. HP, "HP Sure Start," accessed March 20, 2026, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
49. Lenovo, "Advancing enterprise security grounded in Zero Trust Architecture," accessed March 20, 2026,https://techtoday.lenovo.com/sites/default/files/2025-12/advancing-enterprise-security-zta-whitepaper-ww-en.pdf
50. Eclypsium, "Eclypsium Collaborates with Lenovo on Digital Supply Chain Assurance," accessed March 20, 2026, https://eclypsium.com/press-release/eclypsium-collaborates-with-lenovo-on-digital-supply-chain-assurance/.

This project was commissioned by Dell Technologies.

Primary contributors

Tech: Joseph H.

Writing: Laura W.

Design: Emily B.

PM: Scott Luchene

How we created this report

A PT team, which includes the contributors we've listed and others, created this report and performed the technical work behind it.

Principled Technologies®

Facts matter.®