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

Approach

Dell™ commissioned Principled Technologies to investigate nine security features in the PC security and system management space. We conducted our research from April 15, 2025 to June 24, 2025.

- Prevention, detection, and remediation solutions
  - Signed manifest of factory configuration
  - 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 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 three Windows original equipment manufacturers (OEMs) based on Intel® Core™ Ultra processor with Intel vPro®: 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 consolidate and extend 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, 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 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.

Table 1 lists the primary sources we used for each OEM. We consulted the OEM websites, which we cite in the sections below.

Table 1: The primary sources we used for each OEM. Source: Principled Technologies.

Dell	HP	Lenovo
• Dell Trusted Device BIOS Security Whitepaper[2] • "Maintain Device Trust with Dell" Blog[3] • How To Weather the Cyber Identity Crisis"[4]	• HP Sure Start Whitepaper[5]	• Lenovo Firmware Resiliency Whitepaper[6]

Prevention, detection, and remediation solutions

Signed manifest of factory configuration

We looked for solutions where the OEM provides tools to verify a device's hardware and firmware configuration against its original factory state using signed component manifests. While Dell, HP, and Lenovo all offer capabilities that enable this form of supply chain integrity validation at time of delivery and options for implementing verification at scale, Dell Secured Component Verification (SCV) has advantages in several important areas.[7,8,9]

- **Dell advantages:**
  - **Choice:** 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, providing an air-gapped option (i.e., those that are isolated from unsecured systems and networks) for those organizations that require it (e.g., federal agencies).
  - **Visibility/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, fleet-wide visibility without the use of a third-party Host Integrity at Runtime and Start-up (HIRS) verifier tool (an open-source tool that verifies firmware hashes, boot variables, and secure boot settings).
  - **Alignment with Zero Trust:** Dell SCV on Cloud supports remote device attestation, aligning with Zero Trust principles (e.g., "never trust, always verify"). Dell SCV on Cloud enables integrity verification outside the local device, consistent with NIST guidance to minimize implicit trust in endpoints.[10]
- **HP and Lenovo limitations:**
  - HP's platform certificate solution requires retrieving certificates from HP's API service, creating a hybrid scenario that neither fully supports remote attestation nor offers a completely offline method. Attestation is additionally reliant on HIRS, which may result in a gap in making telemetry available to the HP ecosystem.
  - Lenovo implements Intel's Transparent Supply Chain service for platform certificate verification. While this leverages Intel's established security and supply chain infrastructure, Lenovo's approach delegates aspects of trust establishment to its hardware partner rather than directly maintaining the root of trust.

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.[11,12,13] Dell extends this with off-host BIOS verification, 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.[14] **Dell is the only OEM in this group that validates BIOS integrity against an external reference.** HP offers runtime BIOS integrity checks at regular intervals with a supported Intel processor, but these are limited to comparisons against a locally embedded copy of the BIOS.[15] We did not identify any comparable post-boot or off-host BIOS verification capabilities from Lenovo.

Intel Management Engine firmware verification via off-host measurements

We looked for solutions that verify the integrity of Intel Management Engine (ME) firmware, given its privileged access to platform hardware. **Dell is the only OEM in this group that verifies ME firmware during boot and on a recurring schedule—using Dell Trusted Device—comparing local measurements against a known-good reference stored off-host in Dell's secure infrastructure.**[16,17] HP and Lenovo offer automatic recovery of corrupted Intel ME firmware using locally stored backups, but we found no evidence that either supports validation against an external reference or provides administrator-facing telemetry for independent attestation.[18,19]

BIOS image capture for analysis

We looked for solutions that 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.[20] HP and Lenovo both support automatic BIOS restoration using locally validated backups, but do not document any ability for administrators to retain or export the tampered BIOS image during the recovery process.[21,22] **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

We looked for solutions that monitor BIOS-level activity over time to detect the early stages of an attack, such as configuration drift or tampering attempts. Dell delivers this capability through SafeBIOS Indicators of Attack (IoA), which monitors below-the-OS changes and applies Dell-developed threat models to identify suspicious activity sequences. The Dell Trusted Device application makes alerts available through the Dell Client Device Manager, the DTD App Console, Windows Event Viewer, Dell TechDirect, and integrated third-party tools.[23] HP and Lenovo also detect firmware anomalies during boot and runtime, but their implementations rely on isolated event triggers and manual log review.[24,25] **Neither HP nor Lenovo support cumulative threat modeling or natively correlates BIOS-level indicators across time and devices as Dell does with SafeBIOS IoA.**

Common vulnerabilities and exposures detection and remediation

We looked for solutions that detect known firmware vulnerabilities and provide actionable remediation. Dell proactively scans BIOS and firmware against common vulnerabilities and exposures (CVEs) listed in the U.S. National Vulnerability Database, using Dell Security Advisories to surface relevant issues.[26] With Dell Client Device Manager, administrators can automatically apply updates to resolve identified vulnerabilities, linking detection directly to remediation without manual intervention.[27] 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.[28,29] **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

We looked for hardware-based solutions purpose-built to 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.[30] However, only Dell supplements this with 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.[31] In April 2025, Dell ControlVault 3+ achieved FIPS 140-3 level 3 certification, further cementing its leadership in credential security. No other embedded PC biometric solution has achieved this external validation from NIST.[32,33] 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.[34,35] **Of the OEMs we researched, only Dell offers a hardware solution purpose-built to isolate and protect a full range of user credentials.**

Integrated hardware and software security solutions

Hardware-assisted security with Dell, Intel, and CrowdStrike

We looked for solutions that enhance BIOS/firmware-level threat detection using PC telemetry. In collaboration with Intel and CrowdStrike, Dell integrates signals from features embedded in both the Dell Trusted Device application and the Intel platform directly into the CrowdStrike Falcon console. This allows Dell on Intel to detect advanced threats that operate below the operating system, including stealthy techniques that traditional monitoring tools may miss, e.g., firmware-based attacks or fileless malware attacks. With the three-way integration in place, Dell streams SafeBIOS alerts (e.g., BIOS verification and Indicators of Attack) into Falcon without requiring additional agents or integration work.[36] Additionally, to strengthen this defense-in-depth, Intel vPro extends Dell Client Command Suite's system management capabilities to out-of-band computers that are offline or have inaccessible operating system, enabling them to remotely manage—i.e., remediate—an endpoint's BIOS, wipe a device's hard drive, and simultaneously update multiple PCs.[37] We could not find any evidence that HP and Lenovo offer comparable hardware-assisted integrations. **Of the OEMs we researched, only Dell combines firmware-level visibility with processor-level context in a unified endpoint security platform.**

Below-the-OS telemetry integration

We also looked for how the OEMs integrate BIOS and firmware telemetry into broader enterprise management tools beyond CrowdStrike Falcon. 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 tools such as Microsoft Intune, Absolute, and SIEM solutions, without the need for custom connectors or middleware.[38,39,40] HP surfaces firmware events through Windows Event Viewer, but requires custom workflows for monitoring.[41] Lenovo provides similar telemetry through its ThinkShield Firmware Defense solution, delivered via a separate deployment of the Eclypsium platform. While Lenovo supports integration with tools like Intune and Splunk, this capability depends on third-party infrastructure and does not tie directly into Lenovo's native management tools.[42] **Dell is the only OEM we researched that offers natively integrated 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 nine of the below-the-OS security features evaluated. HP fully supports one feature and partially supports two, while Lenovo fully supports one and offers partial support for one other.

Table 2: Summary of available below-the-OS security features, based on public documentation. Source: Principled Technologies.

	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	✓	✗	✗
Intel Management Engine firmware verification via off-host measurements	✓	✗	✗
BIOS image capture for analysis	✓	✗	✗
Early and ongoing attack sequence detection (Indicators of Attack)	✓	✗	✗
Common vulnerabilities and exposures detection and remediation	✓	✗	✗
User credentials storage via dedicated hardware (SafeID with ControlVault 3+)	✓	▲	✗
Hardware-assisted security with Dell, Intel & CrowdStrike	✓	✗	✗
Below-the-OS telemetry integration	✓	▲	▲

*Availability based on select SKUs in North America market.

✓ full support

▲ partial support

✗ no support

1. Dell Technologies, "Maintain Device Trust with Dell," accessed May 5, 2025, https://www.dell.com/en-us/blog/maintain-device-trust-with-dell/.
2. Dell Technologies, "Client Solutions Dell Trusted Device: BIOS Security," accessed May 5, 2025, https://www.delltechnologies.com/asset/en-ae/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
3. Dell Technologies, "Maintain Device Trust with Dell," accessed May 5, 2025, https://www.dell.com/en-us/blog/maintain-device-trust-with-dell/.
4. Charles Robison, "How To Weather the Cyber Identity Crisis," accessed May 24, 2025, https://www.dell.com/en-us/blog/how-to-weather-the-cyber-identity-crisis/.
5. HP, "HP Sure Start," accessed May 5, 2025, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
6. Lenovo, "Firmware Resiliency with Lenovo ThinkShield," accessed May 5, 2025, https://www.lenovo.com/us/en/resources/data-center-solutions/whitepapers/firmware-resiliency-with-lenovo-thinkshield/.
7. Dell Technologies, "Secured Component Verification," accessed May 5, 2025, https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/technical-support/secured-component-verification-datasheet.pdf.

8. HP, "HP Platform Certificate Datasheet," accessed May 5, 2025, 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 May 5, 2025, https://news.lenovo.com/pressroom/press-releases/intel-collaborate-thinkshield-build-assure-supply-chain-cyber-security/.
10. NIST, "NIST SP 800-207: Zero Trust Architecture," accessed June 24, 2025, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.
11. Dell Technologies, "Client Solutions Dell Trusted Device: BIOS Security," accessed May 5, 2025, https://www.delltechnologies.com/asset/en-ae/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
12. HP, "HP Sure Start," accessed May 5, 2025, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
13. Lenovo, "Firmware Resiliency with Lenovo ThinkShield," accessed May 5, 2025, https://www.lenovo.com/us/en/resources/data-center-solutions/whitepapers/firmware-resiliency-with-lenovo-thinkshield/.
14. Dell Technologies, "Client Solutions Dell Trusted Device: BIOS Security," accessed May 5, 2025, https://www.delltechnologies.com/asset/en-ae/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
15. HP, "HP Sure Start," accessed May 5, 2025, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
16. Dell Technologies, "Dell Trusted Device Installation and Administrator Guide v6.5," Intel ME Verification section, accessed May 5, 2025, https://www.dell.com/support/manuals/en-us/trusted-device/trusted_device-ag/intel-me-verification?guid=guid-bac1f4e2-2700-4c45-a5e0-b45aab57401a.
17. Bentz, Tom, "The Secret Sauce Behind Dell Trusted Devices," accessed May 5, 2025, https://www.dell.com/en-us/blog/the-secret-sauce-behind-dell-trusted-devices/.
18. HP, "HP Sure Start," accessed May 5, 2025, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
19. Lenovo, "Firmware Resiliency with Lenovo ThinkShield," accessed May 5, 2025, https://www.lenovo.com/us/en/resources/data-center-solutions/whitepapers/firmware-resiliency-with-lenovo-thinkshield/.
20. Dell Technologies, "Client Solutions Dell Trusted Device: BIOS Security," accessed May 5, 2025, https://www.delltechnologies.com/asset/en-ae/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
21. HP, "HP Sure Start," accessed May 5, 2025, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
22. Lenovo, "Firmware Resiliency with Lenovo ThinkShield," accessed May 5, 2025, https://www.lenovo.com/us/en/resources/data-center-solutions/whitepapers/firmware-resiliency-with-lenovo-thinkshield/.
23. Dell Technologies, "Client Solutions Dell Trusted Device: BIOS Security," accessed May 5, 2025, https://www.delltechnologies.com/asset/en-ae/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
24. HP, "HP Sure Start," accessed May 5, 2025, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
25. Lenovo, "Firmware Resiliency with Lenovo ThinkShield," accessed May 5, 2025, https://www.lenovo.com/us/en/resources/data-center-solutions/whitepapers/firmware-resiliency-with-lenovo-thinkshield/.
26. Dell Technologies, "Client Solutions Dell Trusted Device: BIOS Security," accessed May 5, 2025, https://www.delltechnologies.com/asset/en-ae/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
27. Dell Technologies, "Maintain Device Trust with Dell," accessed May 5, 2025, https://www.dell.com/en-us/blog/maintain-device-trust-with-dell/.
28. HP, "Security Bulletins," accessed May 5, 2025, https://support.hp.com/us-en/security-bulletins.
29. Lenovo, "Lenovo Product Security Advisories and Announcements," accessed May 5, 2025, https://support.lenovo.com/us/en/product_security/home.
30. Microsoft, "Windows 11 Specifications" System Requirements section, May 14, 2025, https://www.microsoft.com/en-us/windows/windows-11-specifications#table1.
31. Dell Technologies, "Client Solutions Dell Trusted Device: BIOS Security," accessed May 5, 2025, https://www.delltechnologies.com/asset/en-ae/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.

32. Dell Technologies, "Client Solutions Dell Trusted Device: BIOS Security."
33. Charles Robison, "How To Weather the Cyber Identity Crisis," accessed May 24, 2025, https://www.dell.com/en-us/blog/how-to-weather-the-cyber-identity-crisis/.
34. HP, "HP Sure Start," accessed May 5, 2025, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
35. Lenovo, "Converged security to protect the workforce of the future," accessed May 5, 2025, https://techtoday.lenovo.com/sites/default/files/2022-08/Security-ThinkShield-Solutions-Guide-MW.pdf.
36. Dell Technologies, "Client Solutions Dell Trusted Device: BIOS Security," accessed May 5, 2025, https://www.delltechnologies.com/asset/en-ae/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
37. Dell Technologies, "Client Solutions Dell Trusted Device: BIOS Security."
38. Dell Technologies, "Maintain Device Trust with Dell," accessed May 5, 2025, https://www.dell.com/en-us/blog/maintain-device-trust-with-dell/.
39. Dell Technologies, "Client Solutions Dell Trusted Device: BIOS Security," accessed May 5, 2025, https://www.delltechnologies.com/asset/en-ae/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
40. Dell Technologies, "Visibility is an Absolute Must for Security," accessed May 5, 2025, https://www.dell.com/en-us/blog/visibility-is-an-absolute-must-for-security/.
41. HP, "HP Sure Start," accessed May 5, 2025, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
42. Eclypsium, "Eclypsium Collaborates with Lenovo on Digital Supply Chain Assurance," accessed May 5, 2025, https://eclypsium.com/press-release/eclypsium-collaborates-with-lenovo-on-digital-supply-chain-assurance/.

This project was commissioned by Dell Technologies.

Facts matter.®