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

Approach

Dell™ commissioned Principled Technologies to investigate 10 security features in the PC security and system management space. We conducted our research from May 28, 2026 to July 14, 2026.

- Prevention, detection, and remediation solutions
  - 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 analysis
  - Early and ongoing attack sequence detection
  - Common vulnerabilities and exposures (CVEs) 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 PCs based on Intel Core™ Ultra processors with Intel vPro® from three Windows original equipment manufacturers (OEMs): 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 consolidates and extends DTD 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's 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 OEMs' 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 Below the OS white paper[2] • "Maintain Device Trust with Dell" blog[3] • "How To Weather the Cyber Identity Crisis" blog[4]	• HP Sure Start white paper[5]	• Firmware Resiliency with Lenovo ThinkShield white paper[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 differentiators in several important areas.

- **Dell differentiators:**
  - **Ease of use, visibility, and reporting:** For SCV on Cloud, Dell manages the full verification pipeline in house with the Dell Trusted Device application through its own cloud infrastructure, maintaining root of trust in the verification process. DTD allows admins to view results and reports within the Microsoft Intune environment and Dell TechDirect as well as CrowdStrike Falcon. Organizations gain automated, fleetwide visibility without deploying or maintaining dedicated verification server infrastructure.[7]
  - **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.[8]

- **HP and Lenovo limitations:**
  - The HP platform certificate solution supports two retrieval paths: Customers can obtain certificates via the HP API service or download them manually through HP Client Management Script Library (CMSL). CMSL supports local integrity verification and scripted fleet-wide deployment, though validation remains on-device. Organizations requiring off-host remote attestation must deploy Host Integrity at Runtime and Start-up (HIRS), where the endpoint reports TPM measurements to a customer-managed attestation server. HP provides a preconfigured HIRS deployment option, but organizations are responsible for owning, deploying, and maintaining the underlying server infrastructure. Off-host attestation requires internet connectivity and customer-managed infrastructure.[9]
  - Lenovo ThinkShield® Build Assure implements the Intel Transparent Supply Chain service for platform certificate verification. While this leverages the Intel established security and supply chain infrastructure, the Lenovo approach delegates aspects of trust establishment to its hardware partner rather than maintaining a Lenovo-owned pipeline.[10,11,12]

Quantum-resistant embedded security controller, BIOS, and EC signing updates

We looked for evidence that each OEM has applied quantum-resistant cryptography to the security controllers and firmware verification mechanisms that protect commercial PCs below the OS. Both Dell and HP have upgraded their embedded security controllers to use Leighton-Micali Signature (LMS) verification, a NIST SP 800-208 stateful hash-based signature scheme,[13] to verify firmware signatures before execution. The HP Endpoint Security Controller (ESC) applies LMS alongside RSA to verify ESC and BIOS firmware on-device, and both must verify successfully before the ESC allows code to run.[14] The Dell embedded controller similarly uses LMS to verify EC firmware before releasing the chipset at boot.[15] Dell also applies quantum-resistant cryptography to off-host BIOS verification (where SHA-512 hashing is used when comparing BIOS measurements against the Dell cloud-stored reference) and firmware update packages (where quantum-resistant code signing ensures firmware delivered to devices cannot be forged or tampered with).[16]

We found no evidence that Lenovo has applied quantum-resistant cryptography to its ThinkShield Engine firmware verification or firmware update signing process, though it is possible this capability exists but is not covered in publicly available documentation from Lenovo.[17]

Quantum-resistant BIOS verification on demand via off-host measurements

We looked for solutions where each 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.[18,19,20] Dell extends this with off-host BIOS verification, now strengthened with quantum-resistant hashing,[21] 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.[22] HP offers runtime BIOS integrity checks at regular intervals and on device shutdown, hibernation, or sleep with a supported Intel processor, checking against a locally embedded copy of the BIOS.[23] 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.**

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. All three OEMs protect the ME firmware during the boot process and support automatic recovery using locally stored backups.[24,25,26] **Dell extends this with recurring post-boot verification on a scheduled basis and off-host validation—using Dell Trusted Device—comparing local measurements against a known-good reference stored off-host in the Dell secure infrastructure.**[27] We found no evidence that HP or Lenovo support validation against an external reference.

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.[28] 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 corrupted BIOS image during the recovery process.[29,30] **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 Indicators of Attack (IoA), which monitors below-the-OS changes and applies threat models it's developed 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.[31]

HP detects firmware changes using saved system configurations stored in protected non-volatile memory accessible only to its Endpoint Security Controller. When the ESC detects a change, it automatically restores the BIOS and firmware from a previously saved good configuration and generates alerts accessible through the HP ESC and Windows Event Viewer. HP implementations respond to individual detected changes but do not appear to accumulate event sequences or draw on external sources to build threat models.[32]

As part of Lenovo ThinkShield offerings, Lenovo PCs can use ThinkShield Firmware Defense, powered by Eclypsium®, to collect and monitor firmware telemetry and detect anomalies including configuration drift and below-the-OS integrity changes. The solution uses known-good databases—either existing references or custom organization-defined ones—to maintain device integrity and recognize threats. Lenovo ThinkShield Firmware Defense also claims "cross-correlation."[33] Additionally, Lenovo ThinkShield offers a solution powered by SentinelOne that applies AI analytics to correlate activities and threats to protect against malicious actors.[34]

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 separately licensed 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 and firmware against common vulnerabilities and exposures listed in the U.S. National Vulnerability Database, using Dell Security Advisories to surface relevant issues.[35] Dell Client Device Manager can work in conjunction with an endpoint management service such as Intune to prioritize CVEs and implement auto-remediation processes to reduce manual patching time.[36] 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.[37,38] **Of the OEMs 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.[39] However, Dell supplements this with a dedicated credential security chip. Dell SafeID with ControlVault isolates credential processing—including fingerprint biometrics, smartcard, NFC, and FIDO2 authentication—in a standalone hardware module, offering stronger protection against firmware and OS-level threats.[40] In April 2025, Dell ControlVault 3+ achieved Federal Information Processing Standards (FIPS) 140-3 Level 3 certification.[41]

Lenovo claims FIPS 140-3 certification for the ThinkShield portfolio, though it doesn't list which level or identify a certified component. HP claims FIPS 140-3 Level 1 certification for its Endpoint Security Controller. 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 FIPS 140-3 Level 3 validation to isolate and protect a full range of user credentials in a standalone chip, according to its published documentation.

Integrated hardware and software security solutions

Hardware-assisted security with Dell, Intel, and CrowdStrike

Dell has partnered with Intel and CrowdStrike to provide companies with endpoint detection below the OS level. Dell Trusted Device provides telemetry data from its off-host BIOS verification with a custom, off-the-shelf integration with the CrowdStrike Falcon platform, appearing alongside Falcon XDR (extended detection and response) data in a consolidated cloud-native view. In September 2025, Dell and CrowdStrike extended their integration. With CrowdStrike Next-Generation security information and event management (SIEM), customers can extend visibility to all Dell Trusted Device telemetry inside the Falcon console. Utilizing the Dell Trusted Device parser with CrowdStrike software, customers can ingest and operationalize deep hardware-level security data, including: Indicators of Attack, BIOS Image Capture, Intel ME Firmware Verification, CVE Detection for BIOS and Firmware, and Secured Component Verification.[44] This means IT administrators can view more activity below the OS for more comprehensive threat detection without requiring additional agents or integration work. According to Dell promotional material, Dell and CrowdStrike have also jointly developed more than 60 custom indicators of compromise (IOCs) tailored to Dell infrastructure, surfaced within the Falcon AI-powered SIEM with severity rankings and forensic data to accelerate analyst response.[45]

As of March 2026, the collaboration has expanded to address the rise of AI PCs. With AI workloads increasingly processed locally on the device, the endpoint attack surface has grown considerably. CrowdStrike and Intel have optimized the Falcon platform for Intel processor-powered AI PCs, adding data discovery and protection for on-device AI workflows.[46] In addition, Intel and CrowdStrike work together to disrupt attacks, combining Intel Control-flow Enforcement Technology (CET), CrowdStrike Hardware Enhanced Exploit Detection (HEED), and Intel Processor Trace telemetry to protect against return-oriented programming (ROP) attacks and extend memory protections.[47] Intel and CrowdStrike also combine to help stop fileless attacks by leveraging the Intel Threat Detection Technology (TDT) memory-scanning algorithms with the CrowdStrike indicator-of-attack database to recognize attacks faster and earlier.[48] With Intel Active Management Technology (AMT), recovery and fleet management are available even when the OS is powered off or compromised.[49] These Intel silicon capabilities are available to organizations running CrowdStrike Falcon on Intel vPro processor-based PCs across OEMs.[50]

HP and Lenovo do address below-the-OS vulnerabilities, but not with CrowdStrike directly. Lenovo allows BIOS, firmware, and hardware telemetry data to integrate with third-party SIEM platforms. ThinkShield telemetry data also combines with Intel below-the-OS monitoring that works with extended detection and response (XDR) and SIEM platforms.[51] Lenovo also partners with SentinelOne to combine hardware telemetry with an endpoint detection and response platform.[52] HP keeps its approach in house with a two-pronged protection system: Hardware-enforced microvirtual machines (μVM) isolate any task deemed risky, and a cloud-based insight system combines information gathered during events with other threat intelligence sources to create AI-driven analytics for teams to use to fine-tune security policies.[53]

While all three OEMs offer integration paths with security platforms, Dell is the only OEM in this comparison to surface its own BIOS verification results and firmware alerts natively within CrowdStrike Falcon through a direct partnership.

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 Security, and SIEM solutions, without the need for custom connectors or middleware.[54,55,56]

HP surfaces firmware events through Windows Event Viewer, but it requires custom workflows for monitoring.[57] Lenovo provides similar telemetry through two paths. First, ThinkShield Firmware Assurance surfaces this telemetry to SIEM platforms through native integration hooks.[58] As a complementary option, ThinkShield Firmware Defense, delivered via a separate deployment of the Eclypsium platform, supports integration with tools like Intune and Splunk, though this capability depends on third-party infrastructure and does not tie directly into Lenovo native management tools.[59]

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 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.

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 via cloud	✓	▲*	▲§
Quantum-resistant embedded security controller, BIOS, and 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 analysis	✓	✗	✗
Early and ongoing attack sequence detection	✓	✗	✓†
Common vulnerabilities and exposures detection and remediation	✓	✗	✗
User credentials storage via dedicated hardware	✓	▲††	✗
Hardware-assisted security with Dell, Intel, and CrowdStrike	✓	✗	✗
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.
§ Handled through a partner while Dell maintains the process in-house.

1. Tom Bentz, "Maintain Device Trust with Dell," accessed June 15, 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 June 15, 2026, https://www.delltechnologies.com/asset/en-us/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
3. Tom Bentz, "Maintain Device Trust with Dell," accessed June 15, 2026, https://www.dell.com/en-us/blog/maintain-device-trust-with-dell/.
4. Charles Robison, "How To Weather the Cyber Identity Crisis," accessed June 15, 2026, https://www.dell.com/en-us/blog/how-to-weather-the-cyber-identity-crisis/.
5. HP, "HP Sure Start," accessed June 15, 2026, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
6. Lenovo, "Firmware Resiliency with Lenovo ThinkShield," accessed June 15, 2026, https://www.lenovo.com/us/en/resources/data-center-solutions/whitepapers/firmware-resiliency-with-lenovo-thinkshield/.
7. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed June 15, 2026, https://www.delltechnologies.com/asset/en-us/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
8. NIST, "NIST SP 800-207: Zero Trust Architecture," accessed June 15, 2026, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.
9. HP, "HP Platform Certificate Datasheet," accessed June 15, 2026, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA8-3109ENW.
10. Lenovo, "Lenovo and Intel Collaborate on ThinkShield Build Assure to Enhance Supply Chain Cyber Security," accessed June 15, 2026, https://news.lenovo.com/pressroom/press-releases/intel-collaborate-thinkshield-build-assure-supply-chain-cyber-security/.
11. Intel, "Intel® Transparent Supply Chain," accessed June 15, 2026, https://www.intel.com/content/www/us/en/software/transparent-supply-chain.html.
12. Intel, "Intel® Transparent Supply Chain (TSC)," accessed June 16, 2026, https://docs.trustauthority.intel.com/main/articles/articles/tsc/tsc-windows-verify.html.
13. NIST, "Recommendation for Stateful Hash-Based Signature Schemes: NIST SP 800-208," accessed June 15, 2026, https://csrc.nist.gov/news/2020/stateful-hash-based-signature-schemes-sp-800-208.
14. Tommy Charles, "Designing PC Firmware Protection for the Quantum Era," accessed June 15, 2026, https://threatresearch.ext.hp.com/designing-pc-firmware-protection-for-the-quantum-era/.
15. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed June 15, 2026, https://www.delltechnologies.com/asset/en-us/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
16. Rick Martinez, "Quantum Resilience Built In," accessed June 15, 2026, https://www.dell.com/en-us/blog/quantum-resilience-built-in/.
17. Lenovo, "Firmware Resiliency with Lenovo ThinkShield," accessed June 15, 2026, https://www.lenovo.com/us/en/resources/data-center-solutions/whitepapers/firmware-resiliency-with-lenovo-thinkshield/.
18. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed June 15, 2026, https://www.delltechnologies.com/asset/en-us/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
19. HP, "HP Sure Start," accessed June 15, 2026, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
20. Lenovo, "Firmware Resiliency with Lenovo ThinkShield," accessed June 15, 2026, https://www.lenovo.com/us/en/resources/data-center-solutions/whitepapers/firmware-resiliency-with-lenovo-thinkshield/.
21. Rick Martinez, "Quantum Resilience Built In," accessed June 15, 2026, https://www.dell.com/en-us/blog/quantum-resilience-built-in/.
22. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed June 15, 2026, https://www.delltechnologies.com/asset/en-us/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
23. HP, "HP Sure Start," accessed June 15, 2026, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
24. Dell Technologies, "Dell Trusted Device Installation and Administrator Guide v8.0," Intel ME Verification section, accessed June 15, 2026, https://www.dell.com/support/manuals/en-us/trusted-device/trusted_device-ag/intel-meverification?guid=guid-bac1f4e2-2700-4c45-a5e0-b45aab57401a.
25. HP, "HP Sure Start," accessed June 15, 2026, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
26. Lenovo, "Firmware Resiliency with Lenovo ThinkShield," accessed June 15, 2026, https://www.lenovo.com/us/en/resources/data-center-solutions/whitepapers/firmware-resiliency-with-lenovo-thinkshield/.
27. Tom Bentz, "The Secret Sauce Behind Dell Trusted Devices," accessed June 15, 2026, https://www.dell.com/en-us/blog/the-secret-sauce-behind-dell-trusted-devices/.

28. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed June 15, 2026, https://www.delltechnologies.com/asset/en-us/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
29. HP, "HP Sure Start," accessed June 15, 2026, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
30. Lenovo, "Firmware Resiliency with Lenovo ThinkShield," accessed June 15, 2026, https://www.lenovo.com/us/en/resources/data-center-solutions/whitepapers/firmware-resiliency-with-lenovo-thinkshield/.
31. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed June 15, 2026, https://www.delltechnologies.com/asset/en-us/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
32. HP, "HP Sure Start," accessed June 15, 2026, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
33. Lenovo ThinkShield, "Solution Overview," accessed June 15, 2026, https://thinkshield.lenovocloudsoftware.com/portal/en/kb/articles/solution-overview.
34. SentinelOne and Lenovo, "ThinkShield XDR powered by SentinelOne," accessed June 15, 2026, https://www.sentinelone.com/resources/datasheets/assets/lenovo-fy26/lenovo-thinkshield-xdr-en.
35. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed June 15, 2026, https://www.delltechnologies.com/asset/en-us/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
36. Tom Bentz, "Maintain Device Trust with Dell," accessed June 15, 2026, https://www.dell.com/en-us/blog/maintain-device-trust-with-dell/.
37. HP, "Security Bulletins," accessed June 15, 2026, https://support.hp.com/us-en/security-bulletins.
38. Lenovo, "Lenovo Product Security Advisories and Announcements," accessed June 15, 2026, https://support.lenovo.com/us/en/product_security/home.
39. Microsoft, "Windows 11 Specifications," System Requirements section, June 15, 2026, https://www.microsoft.com/en-us/windows/windows-11-specifications#table1.
40. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed June 15, 2026, https://www.delltechnologies.com/asset/en-us/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
41. Charles Robison, "How To Weather the Cyber Identity Crisis," accessed June 15, 2026, https://www.dell.com/en-us/blog/how-to-weather-the-cyber-identity-crisis/.
42. HP, "HP Sure Start," accessed June 15, 2026, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
43. Lenovo, "Business security for uncompromised innovation," accessed June 15, 2026, https://techtoday.lenovo.com/sites/default/files/2026-01/thinkshield-extended-solutions-guide-ww-en.pdf.
44. Dell Technologies, "CrowdStrike Falcon," accessed July 14, 2026, https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/selling-competitive/dell-crowdstrike-data-sheet-reference-document.pdf
45. Dell Technologies, "Dell Technologies Strengthens Data Protection Security, Speeds Threat Response," accessed June 15, 2026, https://www.dell.com/en-us/blog/dell-technologies-strengthens-data-protection-security-speeds-threat-response/.
46. CrowdStrike, "CrowdStrike Expands Strategic Collaboration with Intel to Secure Next Generation of AI PCs," accessed June 15, 2026, https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-expands-strategic-collaboration-intel-secure-next.
47. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed June 15, 2026, https://www.delltechnologies.com/asset/en-us/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
48. CrowdStrike, "CrowdStrike Expands Strategic Collaboration with Intel to Secure Next Generation of AI PCs," accessed June 15, 2026, https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-expands-strategic-collaboration-intel-secure-next.
49. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed June 15, 2026, https://www.delltechnologies.com/asset/en-us/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
50. Intel, "White Paper: Intel vPro® Security Overview," accessed June 15, 2026, https://www.intel.com/content/www/us/en/content-details/838959/white-paper-intel-vpro-security-overview.html.
51. Lenovo, "Advancing enterprise security grounded in Zero Trust Architecture," accessed June 15, 2026, https://techtoday.lenovo.com/sites/default/files/2025-12/advancing-enterprise-security-zta-whitepaper-ww-en.pdf.
52. Lenovo, "Smarter, Simpler Security—New Lenovo ThinkShield Solutions Offering," accessed June 15, 2026, https://news.lenovo.com/pressroom/press-releases/smarter-simpler-security-new-lenovo-thinkshield-solutions-offering/.
53. HP, "Endpoint Isolation," accessed June 15, 2026, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA8-1794ENW.

54. Tom Bentz, "Maintain Device Trust with Dell," accessed June 15, 2026, https://www.dell.com/en-us/blog/maintain-device-trust-with-dell/.

55. Dell Technologies, "Client Solutions: Dell Trusted Device Below the OS White Paper," accessed June 15, 2026, https://www.delltechnologies.com/asset/en-us/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.

56. Javier Madriz, "Visibility is an Absolute Must for Security," accessed June 15, 2026, https://www.dell.com/en-us/blog/visibility-is-an-absolute-must-for-security/.

57. HP, "HP Sure Start," accessed June 15, 2026, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.

58. Lenovo, "Advancing enterprise security grounded in Zero Trust Architecture," accessed June 15, 2026, https://techtoday.lenovo.com/sites/default/files/2025-12/advancing-enterprise-security-zta-whitepaper-ww-en.pdf.

59. Eclypsium, "Eclypsium Collaborates with Lenovo on Digital Supply Chain Assurance," accessed June 15, 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: Cassandra O.

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.®