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

Approach

Dell™ commissioned Principled Technologies to investigate 10 security features in the PC security and system management space:

- Support for monitoring solutions
- BIOS security and protection features
  - Platform integrity validation
  - Device integrity validation via off-site measurements
  - Component integrity validation for Intel® Management Engine (ME) via off-site measurements
  - BIOS image capture for analysis
  - Built-in hardware cache for monitoring BIOS changes with security information and event management (SIEM) integration
- Microsoft Intune management
  - BIOS setting management integrations for Intune
  - BIOS access management security enhancements for Intune
- Remote management
  - Intel vPro® remote management
  - PC management using cellular data

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®. Many of the Dell features relate to the Dell Trusted Device application.

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 Intel® Hardware Shield as well as OEM websites, which we cite in the sections below.[1]

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

Dell	HP	Lenovo
• Dell Trusted Device[2] • Dell Blog – The Secret Sauce Behind Dell Trusted Devices[3] • Dell Trusted Device BIOS Security Whitepaper[4]	• HP Sure Start WhitePaper[5] • HP Sure Start InfoSheet[6]	• Lenovo Think Deploy Blog[7] • Supply Chain Security Solutions from Intel and Lenovo[8]

Findings

Support for monitoring solutions

We looked at how each OEM designs its products for monitoring solutions. We also looked at which specific solutions the manufacturers recommend. We discuss features utilized by SIEM, endpoint detection and response (EDR), unified endpoint management (UEM), and other security tools that collect device data for analysis. We collectively refer to those tools as monitoring solutions.

Dell, HP, and Lenovo have designed their devices to integrate with modern monitoring solutions. For Dell, many of the features we discuss below integrate with monitoring solutions and Microsoft Intune.[9] Dell materials specifically mention Managed Detection and Response with Microsoft, which integrates with Intune and Microsoft Sentinel, as well as VMware® Carbon Black.[10,11] HP discusses designing for SIEM solutions in both its HP Sure Click Enterprise documentation and its HP Wolf Security report.[12,13,14] Lenovo ThinkShield materials discuss partnerships with multiple monitoring solutions, such as SentinelOne, Sepio, and Eclypsium.[15]

BIOS security and protection features

Platform integrity validation

We looked for solutions where the OEM provides a service that validates new PC hardware and firmware against a manifest the manufacturer captured during production. Dell, HP, and Lenovo all provide a path for platform integrity validation via certificates as well as options for implementing verification at scale.[16,17,18]

Device integrity validation via off-site measurements

We looked for solutions where a manufacturer collects measurements on a per-build basis and uses that information to validate the integrity of the BIOS components. The Dell Trusted Device application validates measurements on individual PCs against those Dell has captured. This allows Dell to verify the authenticity of the firmware. Dell is the only OEM of the group that offers the capability to validate BIOS measurements against version-specific BIOS measurements.[19] We did not find similar features for HP or Lenovo.

Component integrity validation for Intel Management Engine via off-site measurements

We looked for device integrity validation tools that use off-site measurements to validate the integrity of the Intel Management Engine component. Using features similar to those in the previous section, Dell supports offsite Intel ME component verification.[20,21] We did not find similar features for HP or Lenovo.

BIOS image capture for analysis

We looked for features that allow administrators to capture an image of the device BIOS as a recoverable file for further analysis. Dell offers a BIOS Image Capture feature. Dell Trusted Device provides the captured BIOS image file only if the system has detected a corrupt or tampered image that differs from the offsite Intel ME component verification measurement we discuss above.[22] We did not find similar features for HP or Lenovo.

Built-in hardware cache for monitoring BIOS changes with SIEM integration

We looked for solutions where the OEMs provide a firmware-enabled cache that records BIOS settings changes and other changes in the system within the firmware, so that monitoring applications can detect possible attack sequences. Under Dell Trusted Device, Dell provides the "Indicators of attack" feature.[23] We did not find similar features for HP or Lenovo.

Microsoft Intune management

BIOS setting management integrations for Microsoft Intune

We looked for OEM integrations specifically designed around managing BIOS settings using Intune. Both Dell and HP simplify package management for administrators by integrating directly with the Intune console and have integrations that simplify managing BIOS settings through Intune. Using Dell Command | Endpoint Configure for Microsoft Intune and Dell Command | Configure, administrators can package BIOS changes and distribute them across their fleet to manage BIOS settings on multiple devices.[24,25] HP also allows for BIOS setting management through Microsoft Intune via HP Connect.[26] Administrators can create and manage policies within Intune and deploy those policies across their fleets.[27] We did not find a similar integration for Lenovo.

BIOS access management security enhancements for Microsoft Intune

We looked for ways that OEMs further secure BIOS access on endpoints using UEM tools beyond passwords. Specifically, we sought tools that integrate with Microsoft Intune and simplify the management of encrypted authentication methods used to access each system's BIOS.

We found such features for both Dell and HP, but did not find them for Lenovo. In Dell Command | Endpoint Configure for Microsoft Intune, Dell supports rotating unique secure passwords for each device through Intune. This solution leverages the Dell Client Connector for Intune to decode encrypted BIOS settings. Whenever this solution makes a change in the BIOS, it automatically changes the BIOS password.[28] HP Connect offers certificate-based authentication BIOS management for PCs through Intune. Administrators can still access the local BIOS using the Sure Admin app.[29]

Remote management

Intel vPro remote management

We looked for ways that OEMs support remote management to remote devices using Intel vPro. Dell, HP, and Lenovo all support Intel vPro, as well as connectivity to devices with remote KVM access over Wi-Fi via Intel Endpoint Management Assistant (Intel EMA).[30,31,32,33]

PC management using cellular data

We looked for OEM security services that utilize cellular data to protect remote devices. HP provides a service to secure remote systems using cellular data with HP Wolf Protect and Trace. It maintains some functionality even when the system is powered off.[34] When we conducted our research, this service supported 32 systems.[35] We did not find similar features for Dell or Lenovo.

Summary of findings

Table 2 summarizes our findings. Based on our research using publicly available materials, it appears that Dell supports nine of the ten PC security features we investigated, HP supports six of them, and Lenovo supports three features.

Table 2: Summary of our findings. Source: Principled Technologies.

	Dell	HP	Lenovo
Support for monitoring solutions	✓	✓	✓
Platform integrity validation	✓	✓	✓
Device integrity validation via off-site measurements	✓	no data	no data
Component integrity validation for Intel Management Engine via off-site measurements	✓	no data	no data
BIOS image capture for analysis	✓	no data	no data
Built-in firmware cache for BIOS changes	✓	no data	no data
BIOS setting management integrations for Microsoft Intune	✓	✓	no data
BIOS access management security enhancements for Microsoft Intune	✓	✓	no data
Intel vPro Remote Management	✓	✓	✓
PC management using cellular data	no data	✓	no data

1. Intel, "Intel Hardware Shield-Below-the-OS Security," accessed April 4, 2024, https://www.intel.com/content/dam/www/central-libraries/us/en/documents/below-the-os-security-white-paper.pdf.
2. Dell, "What is Dell Trusted Device," accessed April 3, 2024, https://www.dell.com/support/kbdoc/en-us/000126098/what-is-dell-trusted-device.
3. Bentz, Tom "The Secret Sauce Behind Dell Trusted Devices," accessed April 3, 2024, https://www.dell.com/en-us/blog/the-secret-sauce-behind-dell-trusted-devices/.
4. Dell, "Client Solutions Dell Trusted Device: BIOS Security," accessed April 3, 2024, https://www.delltechnologies.com/asset/en-gb/products/security/industry-market/dell-trusted-device-below-the-os-whitepaper.pdf.
5. HP, "HP Sure Start – Whitepaper," accessed April 3, 2024, https://h20195.www2.hp.com/v2/getpdf.aspx/4AA7-6645ENW.pdf.
6. HP, "HP Sure Start Infosheet," accessed April 3, 2024, https://h20195.www2.hp.com/v2/getpdf.aspx/4AA7-2562ENW.pdf.
7. Philip Jorgensen, "Think Deploy Blog: Updating Lenovo Thin Installer with Proactive Remediations," accessed April 3, 2024, https://blog.lenovocdrt.com/#/2023/ti_winget_pr?id=monitoring/.
8. Intel and Lenovo, "Supply Chain Security Solutions from Intel and Lenovo," accessed April 3, 2024, https://www.intel.com/content/dam/www/central-libraries/us/en/documents/2022-08/supply-chain-security-solutions-from-intel-and-lenovo-may2020.pdf.
9. Dell, "Dell Trusted Device Installation and Administrator Guide v5.5," SIEM section, accessed April 3, 2024, https://www.dell.com/support/manuals/en-us/trusted-device/trusted_device_cg/siem?guid=guid-dbd44a39-5668-45ab-a83e-ecadc95c0825&lang=en-us/.
10. Dell, "Managed Detection and Response with Microsoft," accessed April 15, 2024, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW19W2x/.

11. CrowdStrike and Dell, "Making cybersecurity fast and frictionless," accessed April 15, 2024, https://www.crowdstrike.com/resources/data-sheets/crowdstrike-and-dell-technologies/.
12. HP, "HP Sure Click Enterprise," accessed April 15, 2024, https://h20195.www2.hp.com/v2/getpdf.aspx/4AA7-6963ENW.pdf.
13. HP Wolf Security, "Blurred Lines and Blindspots," accessed April 15, 2024, https://press.hp.com/content/dam/sites/garage-press/press/press-releases/2021/wolf-security-and-flexworker/2021_HP_Wolf_Security_Blurred_Lines_Report.pdf.
14. HP, "HP Sure Start Whitepaper," accessed April 15, 2024, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6645ENW.
15. Lenovo, "ThinkShield," accessed April 15, 2024, https://www.lenovo.com/us/en/software/thinkshield.
16. Dell, "What is Dell Trusted Device Service Secured Component Verification," accessed April 3, 2024, https://www.dell.com/support/kbdoc/en-us/000221396/what-is-dell-trusted-device-secured-component-verification/.
17. HP, "HP Platform Certificate Datasheet," accessed April 3, 2024, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA8-3109ENW&jumpid=va_05dd58b305/.
18. Intel and Lenovo, "Supply Chain Security Solutions from Intel and Lenovo," accessed April 3, 2024, https://www.intel.com/content/dam/www/central-libraries/us/en/documents/2022-08/supply-chain-security-solutions-from-intel-and-lenovo-may2020.pdf.
19. Dell, "Dell Trusted Device Installation and Administrator Guide v5.5," Intel ME Verification section, accessed April 3, 2024, https://www.dell.com/support/manuals/en-us/trusted-device/trusted_device/intelme-verification?guid=guid-bac1f4e2-2700-4c45-a5e0-b45aab57401a&lang=en-us/.
20. Dell, "Dell Trusted Device Installation and Administrator Guide v5.5," Intel ME Verification section.
21. Bentz, Tom "The Secret Sauce Behind Dell Trusted Devices," accessed April 3, 2024, https://www.dell.com/en-us/blog/the-secret-sauce-behind-dell-trusted-devices/.
22. Dell, "Dell Trusted Device Installation and Administrator Guide v5.5," BIOS Events & Indicator of Attack section, accessed April 15, 2024, https://www.dell.com/support/manuals/en-us/trusted-device/trusted_device/bios-events-indicators-of-attack?guid=guid-8f0b4d74-793e-499f-b41e-46d9445faa9b&lang=en-us/.
23. Dell, "Dell Trusted Device Installation and Administrator Guide v5.5," BIOS Events & Indicators of Attack section.
24. Bentz, Tom, "Streamline Endpoint Security and Manageability with BLOBs," accessed April 15, 2024, https://www.dell.com/en-us/blog/streamline-endpoint-security-and-manageability-with-blobs/.
25. Dell, "Dell Command | Endpoint Configure for Microsoft Intune User's Guide," accessed April 15, 2024, https://dl.dell.com/content/manual52878209-dell-command-endpoint-configure-for-microsoft-intune-users-guide.pdf.
26. HP, "HP Connect," accessed April 15, 2024, https://connect.admin.hp.com/.
27. HP, "HP Connect User Guide," accessed April 15, 2024, https://connect.admin.hp.com/static/HPConnectUserGuide.pdf.
28. Bentz, Tom, "Streamline Endpoint Security and Manageability with BLOBs," accessed April 15, 2024, https://www.dell.com/en-us/blog/streamline-endpoint-security-and-manageability-with-blobs/.
29. HP Developers, "HP Sure Admin step-by-step," accessed April 15, 2024, https://developers.hp.com/hp-client-management/blog/hp-sure-admin-step-step/.
30. Dell, "The Intel-vPro® Platform," accessed April 15, 2024, https://www.dell.com/en-us/lp/intel-vpro-platform.
31. HP, "Intel EVO," accessed April 23, 2024, https://www.hp.com/us-en/laptops/business/intel-evo.html.
32. Lenovo, "What is vPro," accessed April 23, 2024, https://www.lenovo.com/us/en/faqs/pc-life-faqs/what-is-vpro/.
33. Intel, "For IT: A How-to Guide to the Intel vPro® Platform," accessed April 23, 2024, https://plan.seek.intel.com/Guide_to_IntelvPro_REG/.
34. HP, "HP Protect and Trace with Wolf Connect Solution Overview," accessed April 3, 2024, https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA8-3324ENW.
35. HP Wolf Security, "Protect and Trace with Wolf Connect," accessed April 3, 2024, https://www.hpwolf.com/en/legal/ptwc/platforms/.

This project was commissioned by Dell Technologies.

Principled Technologies®

Facts matter.®