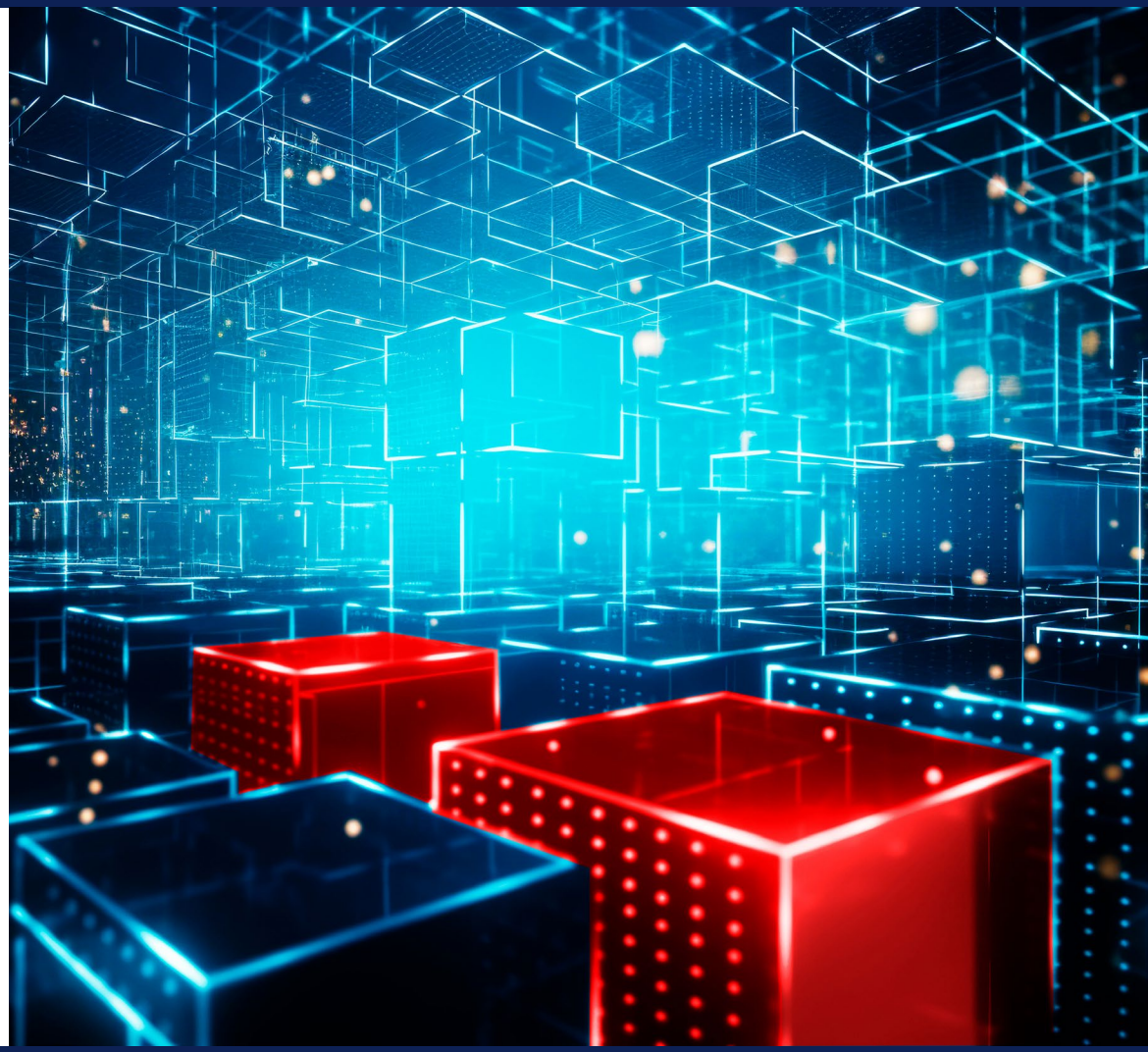
DELL Technologies

intel

How to secure the use of AI at the endpoint

Defend on-device AI workloads with secure, modern devices and an adversarial mindset.



CROWDSTRIKE /ABSOLUTE®

Executive summary

On-device AI has huge benefits, but it also comes with cyber risk. In this eBook, we'll walk through how to position your organization securely to take advantage of AI innovation at the endpoint.

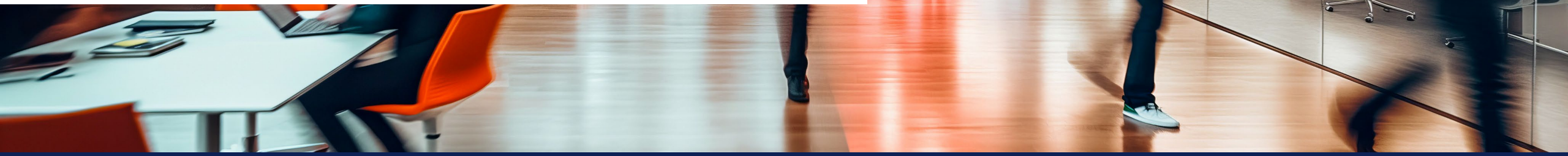
Table of Contents

The attack surface of on-device AI

What can be attacked

All emerging technologies come with cybersecurity risk for one reason: It's new territory. You're dealing with the unknown. We've seen this with cloud computing, with blockchain, and numerous other technologies. The same is true for on-device AI. The key to mitigating this risk, as always, is to shed light on the unknown.

Before we can talk about what security we need to minimize the attack surface, it helps to talk about what we are securing and why. Think about this like a system of pipes in a commercial building which houses multiple businesses. These pipes carry water, gas, etc. throughout the building for a variety of use cases. If the matter flowing through the pipes is contaminated or interrupted, it can't do its job. If the pipes carrying the matter are damaged or corrupted, they can't do their job. Both the pipes and their contents need to be in good working order to meet the needs of their respective use cases.▶



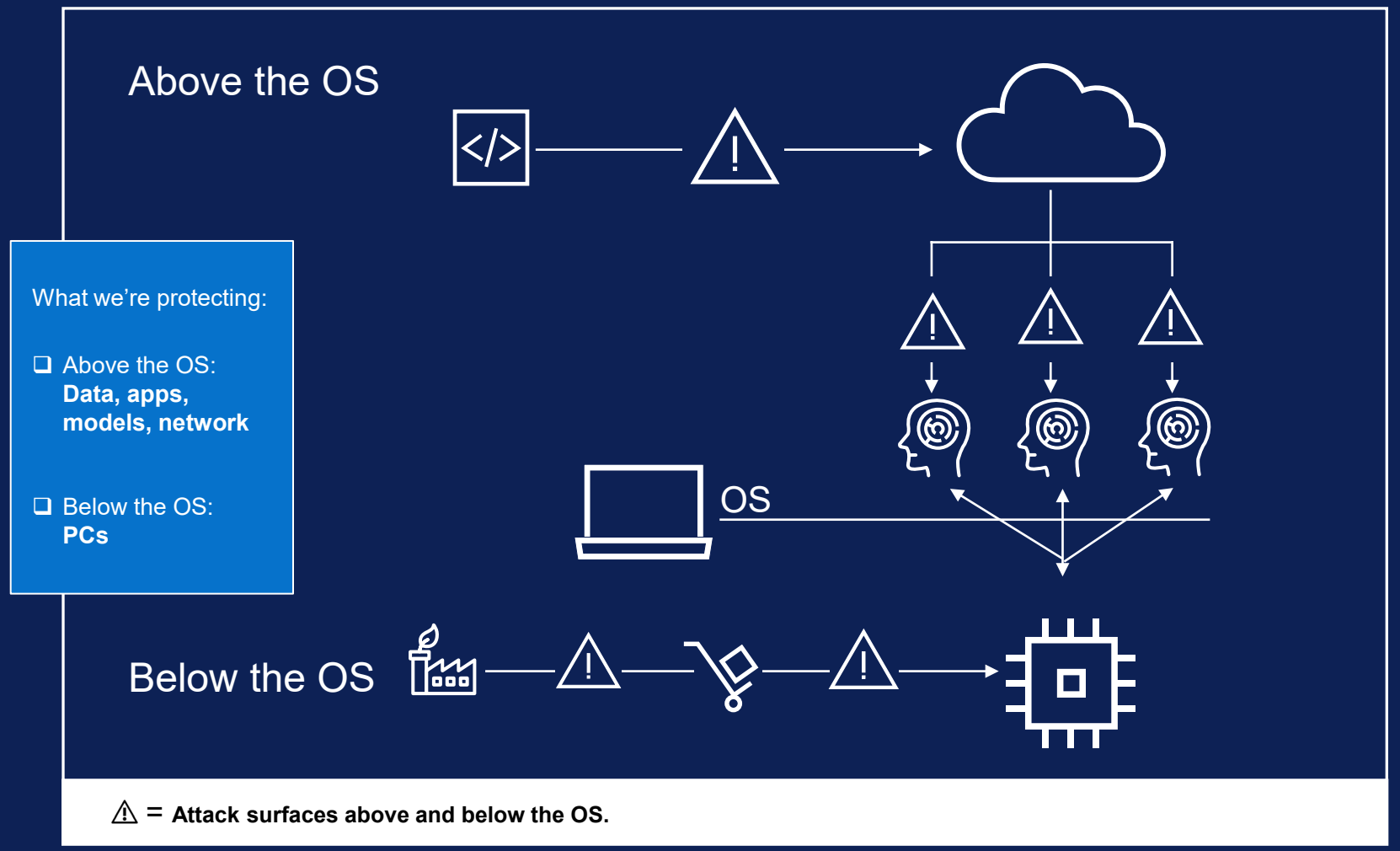
The attack surface of on-device AI, cont'd

What can be attacked, cont'd

Bringing it back to AI at the endpoint:

- The pipes are your infrastructure – your PCs, your corporate networks. The how and where you work.
- The contents flowing through the pipes are the data, apps and models that fuel various AI use cases. The assets and resources you need to do your work.

And you guessed it. Cyber adversaries target both. They may steal IP to hold for ransom or poison data or models to impact operations. In any case, the consequences can be severe, leading to financial and reputational damage and/or triggering regulatory reviews.►



Security risks at the endpoint

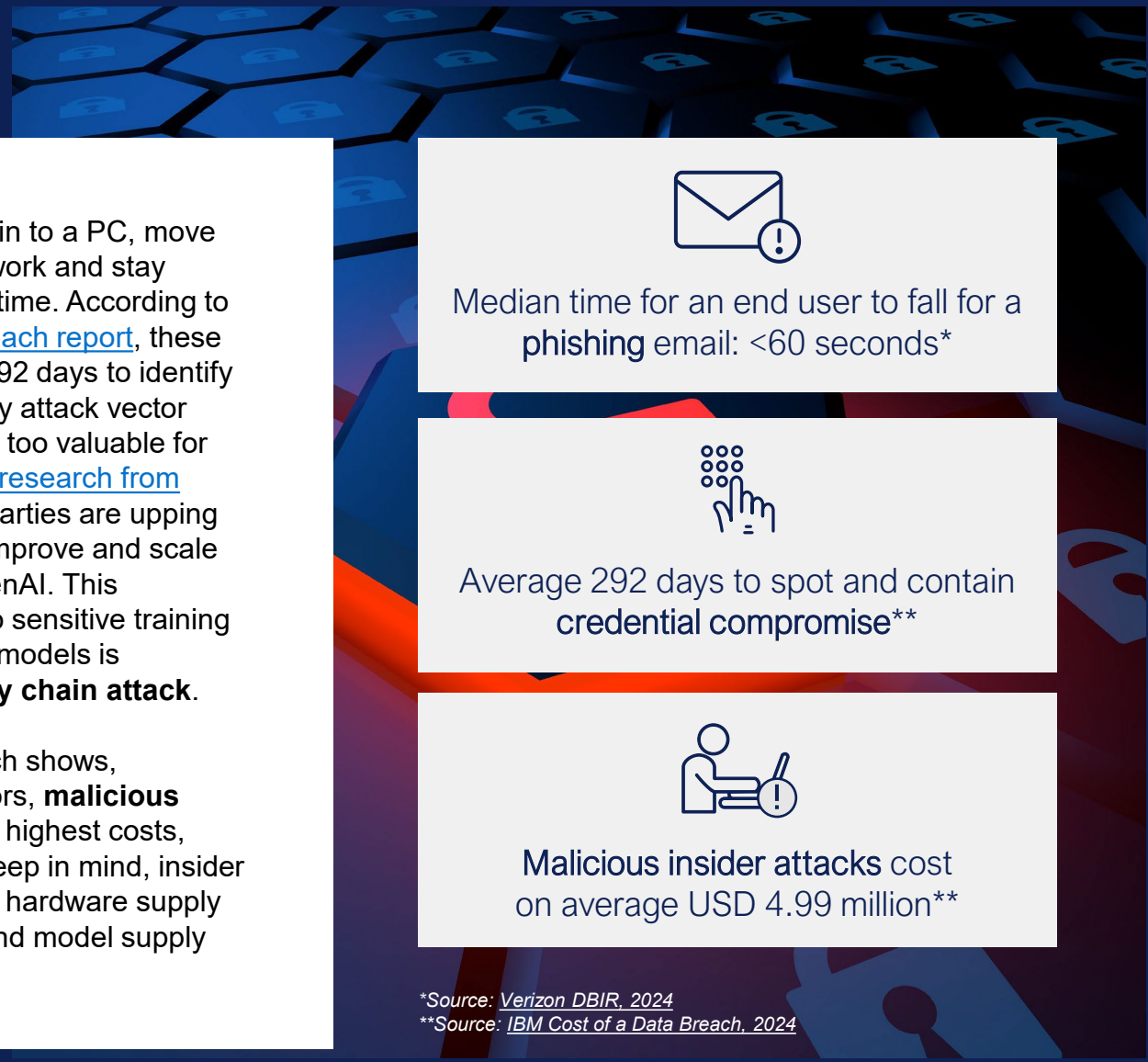
Tactics attackers use to gain entry

Now, we'll talk about methods attackers might use to access both targets.

Device compromise. As we see in Endpoint Security Market Insights, Forrester Research, Inc., March 2025, PCs are among the leading targets of modern cyber threats. This type of attack can happen way before the on-device AI work begins, i.e., a **hardware or software supply chain attack**. There are dozens, if not hundreds, of points during the supply chain where a malicious party may be able to tamper with components – e.g., circuitry, firmware – to introduce weaknesses that can be exploited later. Imagine the pending disaster of an investment firm receiving a brand-new shipment of PCs with counterfeit components.

Identity compromise. Breaches involving stolen or compromised credentials are one of the fastest growing attack vectors. It's no wonder. Attackers using valid credentials can log in to a PC, move freely within the corporate network and stay undetected for long periods of time. According to IBM's latest Cost of a Data Breach report, these breaches took an average of 292 days to identify and contain—the longest of any attack vector studied. That level of access is too valuable for threat actors to ignore. In fact, research from Zscaler shows that malicious parties are upping their credential theft game to improve and scale phishing attacks by utilizing GenAI. This unauthorized access applied to sensitive training or inference data or directly to models is categorized as a **model supply chain attack**.

Insider threat. Recent research shows, compared to other attack vectors, **malicious insider attacks** resulted in the highest costs, averaging USD 4.99 million. Keep in mind, insider attacks can happen across the hardware supply chain, software supply chain and model supply chain.►



Median time for an end user to fall for a **phishing** email: <60 seconds*

Average 292 days to spot and contain **credential compromise****

Malicious insider attacks cost on average USD 4.99 million**

*Source: Verizon DBIR, 2024
**Source: IBM Cost of a Data Breach, 2024

Countermeasures to have in place

What mitigates risk

None of these attack targets are fundamentally new. Neither are the attackers' end goals. As always, we want to focus on keeping your fleet secure and resilient. **Layering on countermeasures** can help reduce the attack surface and shed light on any suspicious behavior immediately.

A **zero trust mindset** will mitigate risk across your fleet. These principles – never trust, always verify and monitor continuously – help keep you ahead of attackers. It is impossible to block 100% of attacks. For a strong security posture, you need **visibility and control** across your IT ecosystem.

With that framework in mind, reassess your infrastructure – especially systems and processes that interact with AI. What countermeasures minimize the risk of device compromise, identity compromise and insider threat?►

Zero trust principles help defend against risk and reduce the blast radius of cyber activity

Countermeasures to have in place, cont'd

What mitigates risk, cont'd

There are two overall countermeasure categories.

"Below-the-OS" security protects the AI devices you work on. We can break this into two parts:

- Defend your fleet with devices that are **built securely**. This means using AI PCs that are secure by design – i.e., they were developed with secure design principles and in a secure supply chain.
- Defend your fleet with devices that have **security built in**. Secure AI PCs include layers of embedded protection that provide visibility – down to the BIOS and silicon layers – right out of the box.

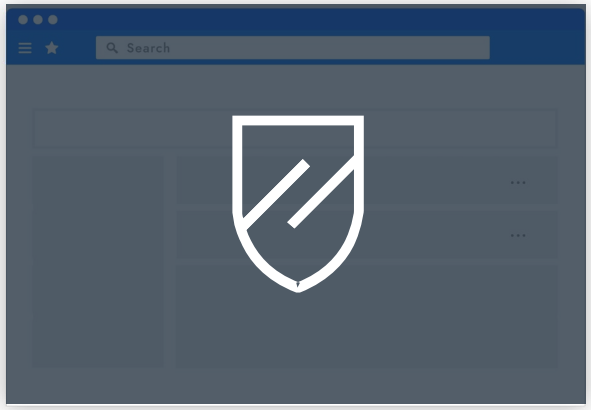
"Above-the-OS" security protects access to AI models. Defend the data and models that you work *with* and corporate networks you work *in* with **software security**. It is essential to protect machine learning security operations and monitor network traffic of deployed AI workloads.►

Below the OS security

Secure AI PCs

Hardware & firmware security, Supply chain security, core silicon

Above the OS security



Software Security

Additional layer of security for endpoints, networks & cloud environments

Security Services and expertise available to tie it all together.

Applying best practices to your fleet

How Dell AI PCs bring foundational security for your fleet

This is where Dell Trusted Workspace can help. Our technologists devise and design the security of our commercial AI PCs with a deep understanding of the adversarial mindset.

Below the OS, secure design, robust supply chain controls and optional supply chain assurance help ensure PCs are secure from first boot. Built-in hardware and firmware security keeps the PC protected while in use, e.g., Dell-unique* BIOS-level tamper detections (Dell SafeBIOS) and passwordless credential security (Dell SafeID) to protect against unauthorized access. Additionally, Intel® silicon technologies help provide a foundation to protect various aspects of AI as it is used by AI PC clients. For example, Intel helps secure AI data at rest on the client with acceleration for model encryption on disk.►

Applying best practices to your fleet, cont'd

How Dell AI PCs help bring foundational security for your fleet, cont'd

To supplement this below-the-OS security, our partner Absolute's Persistence technology can be embedded in the factory for even greater visibility and control across the PC lifecycle, enabling, e.g., geolocation for devices en route and self-healing of critical apps in the worst-case scenario.

In fact, Dell has curated an ecosystem of software partner solutions, including CrowdStrike Falcon XDR and Absolute Secure Access, that activate zero trust principles to protect your model supply chain from unauthorized access **above the OS**. Using these solutions, you can create and enforce policies with granular access controls (e.g., role-based access control or RBAC) to mitigate the risk of malicious insiders accessing or manipulating your AI models.►

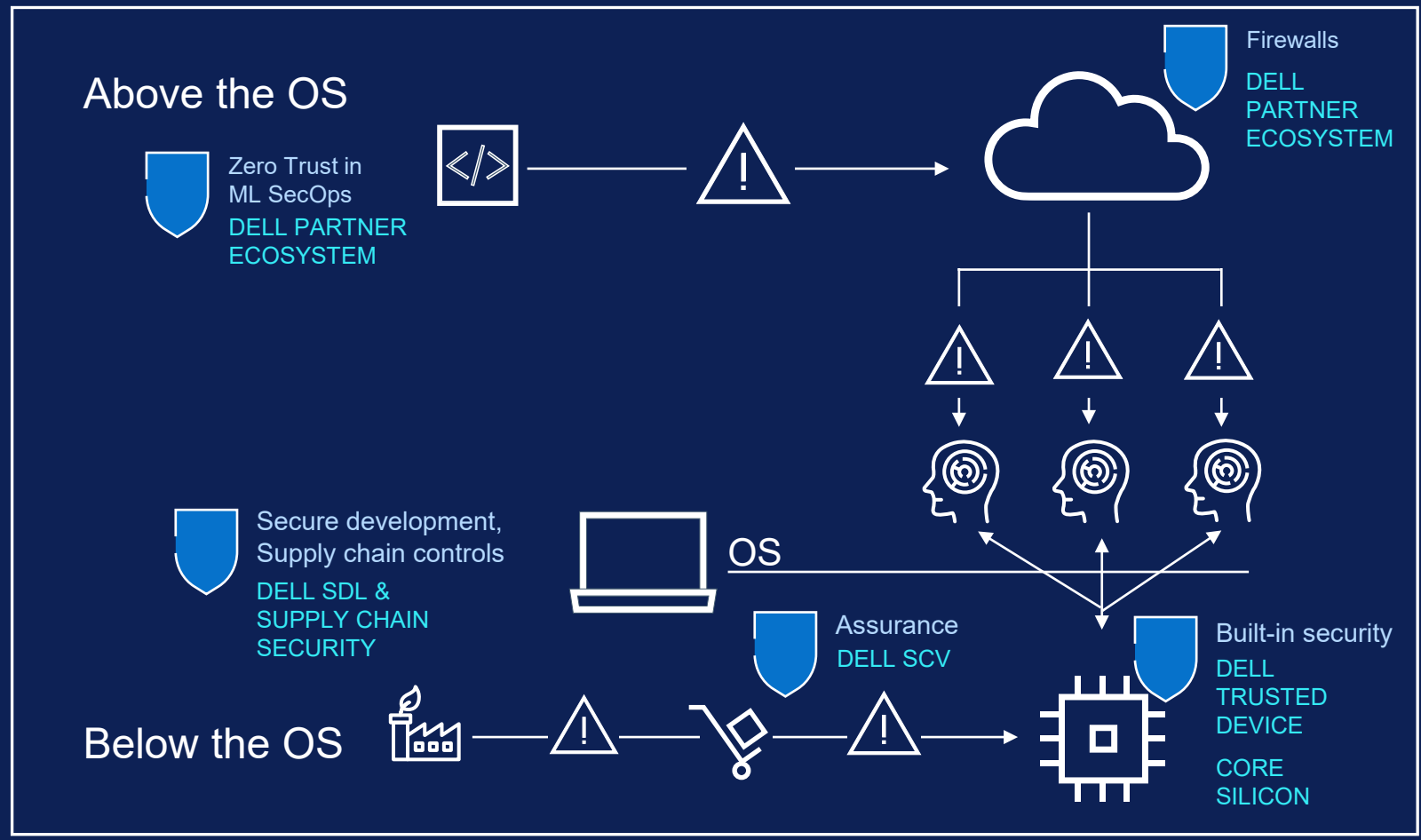
Applying best practices to your fleet, cont'd

How Dell AI PCs help bring foundational security for your fleet, cont'd

This together is ***Security for AI.*** These capabilities defend on-device AI workloads from cyberattacks, allowing you to stay focused on innovation and winning business. ►

Stop advanced endpoint attacks with coordinated hardware and software defenses

Dell works with Intel and CrowdStrike to integrate the below- and above-the-OS layers with Hardware-Assisted Security. *Learn more >*



Key takeaways and next steps

Secure AI at the Endpoint with Dell

Businesses are excited for AI, but AI readiness is lagging according to a recent survey of CISOs conducted by Absolute. An analysis of millions of devices revealed a PC population unable to absorb new AI capabilities broadly. **Dell can help bring it all together.**

Develop and deploy AI models on a secure, modern foundation. Windows 10 support ends in October 2025. PCs will no longer receive security updates, feature updates and Windows 10 support. Older devices may not meet Windows 11 requirements and may lack the latest built-in performance, security and AI enhancements. Upgrade to **Dell Pro** or **Dell Pro Max based on Intel® Core™ Ultra processors with Intel vPro®** to unlock security benefits and defend AI workloads with the **world's most secure commercial AI PCs.*** ►

Windows 10 support ends in October.

Upgrade to the latest Dell AI PCs on Intel to unlock security benefits and AI enhancements:

Shop Dell Pro ● Dell Pro Max

*The World's Most Secure Commercial AI PCs**

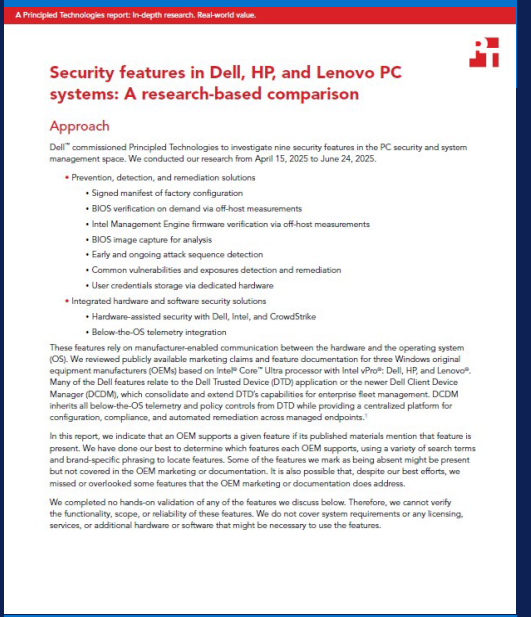
Explore value-added software and services to improve your security posture:

Software & Integrations

Services

INDUSTRY LEADERSHIP

Principled Technologies found that Dell and Intel commercial AI PC security wins vs. peers


A Principled Technologies report: In-depth research. Real-world value.

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.

Read the Study

Disclaimers

*Based on third-party analysis by Principled Technologies when comparing Dell commercial AI PCs on Intel processors vs. HP and Lenovo, July 2025. Backed by Dell internal analysis of worldwide PC market, October 2025. Applicable to PCs on Intel processors. Not all features available with all PCs. Additional purchase required for some features.

To learn more:

Contact us: Global.Security.Sales@Dell.com

Visit us: Dell.com/Endpoint-Security

Follow us: LinkedIn @DellTechnologies | X @DellTech

About Dell Endpoint Security

Security is a daunting topic for organizations of all sizes. **Engage an experienced security and technology partner to modernize endpoint security**.

Dell Trusted Workspace helps secure endpoints for a modern, zero trust-ready IT environment. Reduce the attack surface and improve cyber resilience with a comprehensive portfolio of hardware and software protections exclusive to Dell. Our highly coordinated, defense-based approach offsets threats by combining built-in protections with ongoing vigilance. End users stay productive, and IT stays confident with security solutions built for today's cloud-based world.