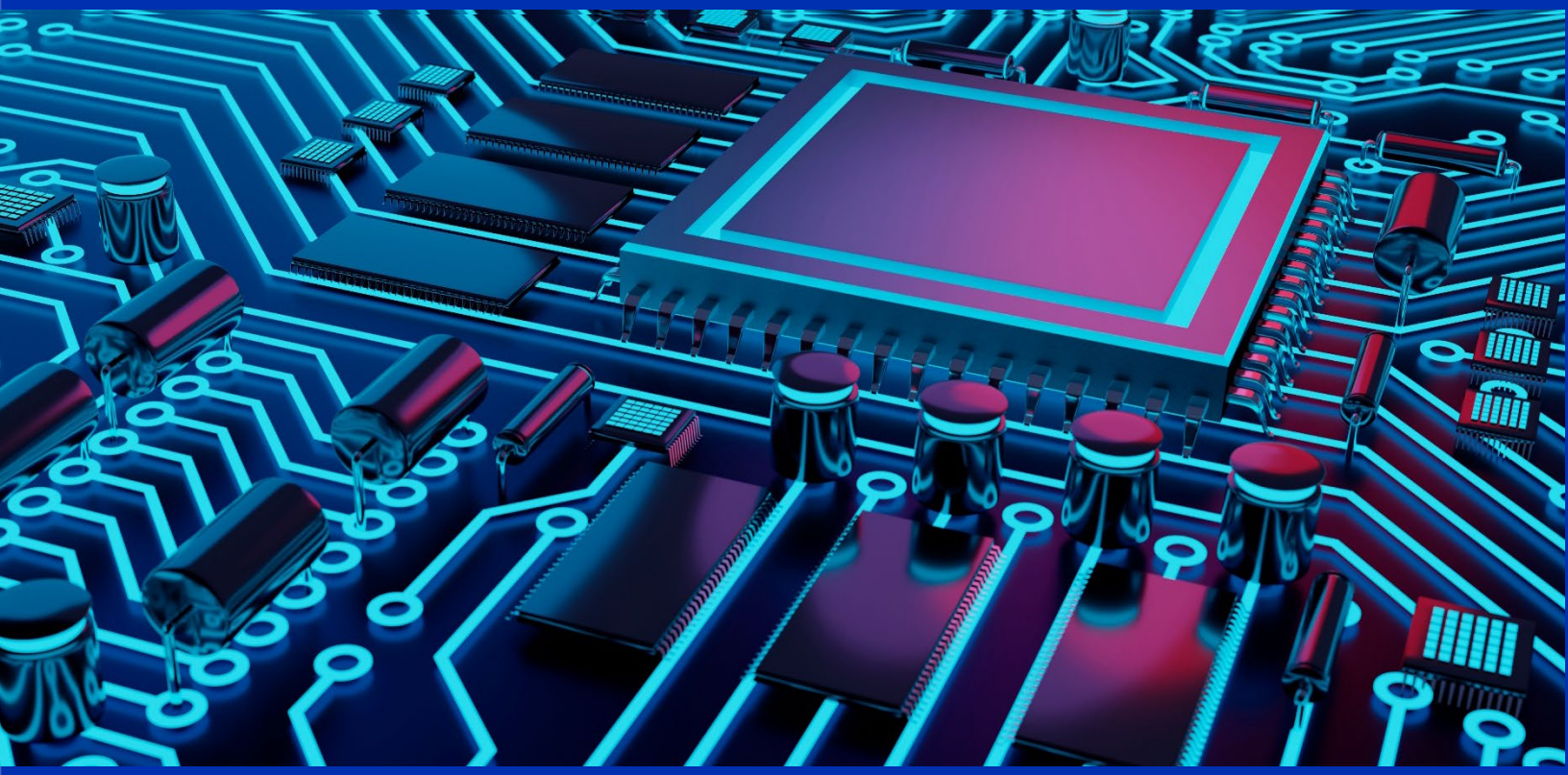
DELL Technologies intel

# Achieving pervasive security above and below the OS

**The world's most secure commercial AI PCs*, delivered by Dell and Intel®. Future-proof your fleet and stay ahead of cyber adversaries with multiple layers of defense.**

July 2025



## Executive Summary


- Keeping business data secure is a challenging task, complicated by the proliferation of endpoints operating outside of the organizational network and the constant evolution of threat vectors.
- AI has arrived on device, expanding innovation, as well as the attack surface. With hundreds of models and AI features now in the mix, sensitive data is now at risk of exposure to applications like GenAI.
- Dell and Intel are committed to keeping commercial customer networks secure with multiple layers of defense.
- Dell combines built-in hardware and firmware security with silicon-based protections from Intel to defend the deepest levels of a device against foundational attacks.
- We bolster these “below-the-OS” defenses with intelligent software from our partner ecosystem for advanced threat protection.
- In addition to this approach, Dell and Intel have invested in practices and policies to continually help secure platforms once they are out in the market and subject to attack from malicious actors.


# Topics covered in this paper

## Security foundation

**Secure Development Lifecycle** Dell and Intel design their products with security as a chief element and test rigorously before release.

**Supply Chain Security** Protections are in place along the supply chain to help ensure devices stay secure after leaving the factory.

## Comprehensive defense framework

**Built-with Security:** Rigorous supply chain controls and optional assurance help ensure customers are secure from first boot.

**Built-in Security:**

- Hardware and firmware-based security capabilities help protect devices from threats that target their foundational layers, e.g., the BIOS.
- Silicon-based protections provide a fundamental layer that underpins the reliability and trustworthiness of the AI PC.

**Built-on security:** Software-based security provides advanced protection for endpoints, networks and cloud environments – crucial to modern device security.

**Ongoing support:** Dell and Intel work to ensure our products remain secure, patch vulnerabilities, and update silicon-based security within the OS.

## Key security trends

1. In Endpoint Security Market Insights, Forrester Research, Inc., March 2025, the company explains "Endpoints … are among the leading targets of external attacks for companies that have experienced a breach within the last 12 months."

2. According to CrowdStrike's 2025 Global Threat Report, fileless malware attacks now comprise 79% of attacks – which means attacks on memory that are harder to detect.

3. According to an Enterprise Strategy Group May 2023 research report, more than 75% of organizations report that they have experienced at least one cyberattack caused by an unknown, unmanaged, or poorly managed endpoint device.

# Introduction

## Your network is as secure as its weakest endpoint

**Security starts way earlier than you may think.** It seems that every few months, another prominent global brand experiences a major security breach and the negative public exposure causes major damage to their reputation. It's enough to keep business owners and security professionals worried that they are also exposed, be it through an overlooked vulnerability baked into their devices or an unknown, exploitable weakness in their software. You might be able to trust your IT team to secure your networks and implement data safe practices, but how can you trust all the endpoints and applications you rely on to do business when you had no oversight over their manufacturing or development?

**Software-only security is not enough.** A common yet flawed approach to address device integrity is attempting to create a false sense of security through software-only solutions without addressing underlying hardware-based vulnerabilities. It is important for business leaders to understand the limitations of this strategy: by relying only on software to protect their businesses, they leave the hardware that the software is running on potentially vulnerable to attacks. In essence, if hardware isn't secure, security applications and technologies running on it cannot be secure either.

Other providers attempt to create a "walled garden" to protect devices, where limitations are built into the apps and services that restrict user flexibility. While this may make sense in a consumer context, it comes at the cost of the freedom to fully leverage devices, a challenge that's only exacerbated in a commercial context. This approach may also lead attackers to increasingly target and break down these systems to expose vulnerabilities in common configurations.

Simply put, what works for direct-to-consumer devices often fails when applied in a commercial environment that represents a more attractive target for attackers. That's why Dell and Intel take a different, holistic approach to security. Dell and Intel know that the only way to reliably secure commercial devices and networks is through a harmonization of hardware and software security technologies working in concert. While our teams have worked together to create a chainmail of closely integrated hardware and software security capabilities, other providers may not have made this investment.

**Hardware-based security for the commercial AI PC**

**Every PC is going to be an AI PC.** Tech market analyst Canalys predicts that AI PCs will take over the entire PC market in the coming six years. This means that PCs without onboard AI capabilities will no longer be sold by 2030. Essentially, to future-proof your business, you need to start now. The good news: Dell and Intel are helping customers navigate the evolving IT and security landscape with commercial AI PCs featuring the foundational built-in security, speed, and efficiency needed to combat modern threats.

But this is no easy task. The complexities and concerns of securing devices and networks are enough to make your head spin – and emerging AI technologies have made this area even more complex. That's why we have made it our mission to provide our customers with devices designed with security in mind to enable them to focus on what really matters - making their businesses run. Dell and Intel's co-engineering relationship spans several decades and has always focused on keeping our customers' data secure, especially in the business-to-business market. Through its partnership with Intel, Dell has established a reputation as a go-to provider of employee devices for companies of all sizes and in every market. What goes into a Dell commercial AI device? It's more than a ramshackle collection of features – Intel and Dell weave technologies, tools, and policies throughout the commercial PC lifecycle to help provide end-to-end security for our customers and their businesses.

**Security by design**
Intel and Dell look beyond today's threats when designing tomorrow's systems to minimize the attack surface and help ensure commercial devices stay secure.

**Protection in transit**
We have technologies and polices in place to help protect the integrity of devices before they are in your hands, helping to maintain security throughout component sourcing, assembly, and delivery.

**Defense against evolving threats**
We employ hardware-based security through Dell Trusted Devices and Intel vPro® Security capabilities to harden devices that address primary cybersecurity use cases for prevention, detection, response, recovery and remediation. In addition, Dell and Intel have security teams dedicated to probing their products and finding new vulnerabilities before attackers do, expediently pushing out patches to help keep you and your team covered.

In this white paper, we'll explore how Dell and Intel have worked together to produce commercial AI PC platforms with security baked in at the deepest levels, helping protect devices across their lifecycle, through your next refresh, and beyond.

## Cybersecurity and GenAI, a double-edged sword

Just as cyber defenders use GenAI for good, cyberattackers look to further their own malicious objectives, launching more sophisticated attacks faster and at scale.

While GenAI use cases are still in their infancy and expanding daily, it's important to keep a few key concepts in mind. First, there are a number of threats that GenAI can pose for organizations including:

- Data privacy and integrity issues
- Compliance issues
- And IP infringement

In addition, we see a number of ways in which GenAI will be able to help in the security fight, including, but not limited to:

- Advanced threat detection
- Specialized and focused training for employees, and
- Automation

Dell and Intel are actively working to enable better threat modelling specific to GenAI. This can include data loss prevention, data rights management, advanced phishing, model tampering, regulatory and compliance - all with the appropriate controls applied.

Dell can also help you test your GenAI landscape when it comes to security with vulnerability management and penetration testing programs to keep up with the evolving threat landscape.

# Security foundation

**Secure Development Lifecycle**

## Securing our platforms starts at the whiteboard

**Planning, assessment, and analysis**
Before designing our newest platforms and chipsets, respectively, experts at Dell and Intel set strict parameters for what a secure platform needs to include to address the security needs of the future and meet required security regulations. This process starts with a roundtable determination of likely future security and privacy risks and the activities necessary to address them. This assessment is used to define the security objectives we will evaluate our architectures against. With this information, security teams from Dell and Intel develop threat models by taking an adversarial mindset to this conceptual architecture, probing for potential vulnerabilities and exploits that must be mitigated against. This exercise has proven to deliver significant improvements in finding and mitigating potential vulnerabilities in BIOS, firmware, and hardware design.

**Security-centric design**
Once the threat assessments are complete and models are created to define the threat surface and where testing should be focused, engineers begin developing the product code. The security objectives defined in the previous stage provide guidance during this phase of development and serve as criteria for determining whether the product is on track to meet our customers' needs.

**Verification and testing**
After the code has been refined to the point of satisfying the security objectives laid out at the start of the development lifecycle, the product moves forward to a rigorous testing process. These tests usually begin with secure code reviews and static code analysis, an automated process that uses special tools for finding and fixing defects. Some products with more complicated code require a manual review process, where security experts perform line-by-line reviews of product code to find previously unknown mistakes and help ensure it has been designed in a safe way. Finally, teams of expert hackers are directed to engage in penetration testing and other red team activities to find potential vulnerabilities that were missed in the earlier phases. These findings are mitigated again based on risk, so that any additional identified exposure has been documented and corrected.

**Release and post-release**
Once the product has been rigorously tested and found to meet or exceed the security objectives defined at the start, it is ready for release into the marketplace. However, these phases represent only a slice of the Secure Development Lifecycle. For Dell and Intel, the security of our platforms is an ongoing effort. Our teams work to discover vulnerabilities before they can be exploited by attackers, then develop and push out security updates to patch them. An example of Dell and Intel's commitment to end-to-end security is our investment in a secure supply chain between assembly and delivery of a device, one of the fastest-growing attack vectors for malicious actors. In the next section, we'll dive into how Dell and Intel mitigate risks along their supply chains to help ensure the device that is delivered to your doorstep is secure from the first boot.

**Supply Chain Security**

## Supply chain assurance is foundational to device security

A lot can happen between the time a component or device leaves the factory and when it arrives at its destination. Each stage in the supply chain represents a new vector that opens your employees, your business, and your customers up to potential attack. Dell and Intel have developed tools, technologies, and processes to help ensure the security of our products before they get to customer businesses and enable self-verification of device authenticity before being deployed to employees.

**Source**
Dell employs a rigorous partner screening process to help ensure the quality and security of devices and their components. These partners also routinely undergo audits to ensure compliance with Dell's comprehensive set of Supply Chain Security Standards.

**Make**
In addition to adhering to Dell's Supply Chain Security Standards, Dell device manufacturers also frequently test parts during manufacturing to help ensure counterfeit products do not sneak into the supply chain. To further mitigate this risk, Unique Piece Part Identification Number (PPID) labels are affixed to specific high-risk components, containing information about the supplier, part number, country of origin, and date of manufacture so that Dell can identify, authenticate, track, and finally validate these components to help ensure the customer receives exactly what was shipped.

**Deliver**
Dell freight is protected through layers of physical security, from tamper-evident seals and door locking mechanisms to a variety of tracking devices designed to detect if the Dell devices inside have been tampered with in transit.

Dell devices themselves also feature tamper detection technologies. Dell SafeSupply Chain solutions cover supply chain security and integrity controls like tamper-evident seals and NIST-level hard drive wipes to help ensure a clean slate for your corporate image.

**Verify**
Dell commercial AI devices ship with cryptographically signed platform certificates that capture snapshot attributes of platforms during manufacturing, assembly, testing, and integration. These platform attributes are then cryptographically linked to the specific device using the Trusted Platform Module (TPM) as the hardware root of trust.

Learn more about Dell and Intel's joint efforts in securing the supply chain. Watch the interview ***with SiliconANGLE***

Dell has implemented Trusted Computing Group (TCG) platform certificates within the Dell Secured Component Verification (SCV) solution for commercial AI PCs with Intel processors (certificate available both on device (for federal organizations and on cloud for commercial customers. SCV delivers cryptographically signed inventory certificates to IT for supported Dell devices. With secure self-verification tools, Dell-unique SCV* helps assure full hardware integrity during transit to IT environments and allows customers to verify that Dell commercial AI PCs and key components arrive as they were ordered and built.

## Comprehensive defense framework

**Below the OS security**

### Built-in security technologies help prevent, detect, respond to and recover from threats

Holistic security means going beyond the legacy model of software protecting software to keep up with new categories of threats against digital security, safety, and privacy. Combining it with hardware-based, "below the OS" security technology helps protect every layer of the compute stack by working to prevent and detect foundational attacks, including threat variants that most commonly occur along the supply chain. Dell and Intel's co-engineering relationship has focused on covering this attack surface with an intricate tapestry of technologies at both the component and platform level.

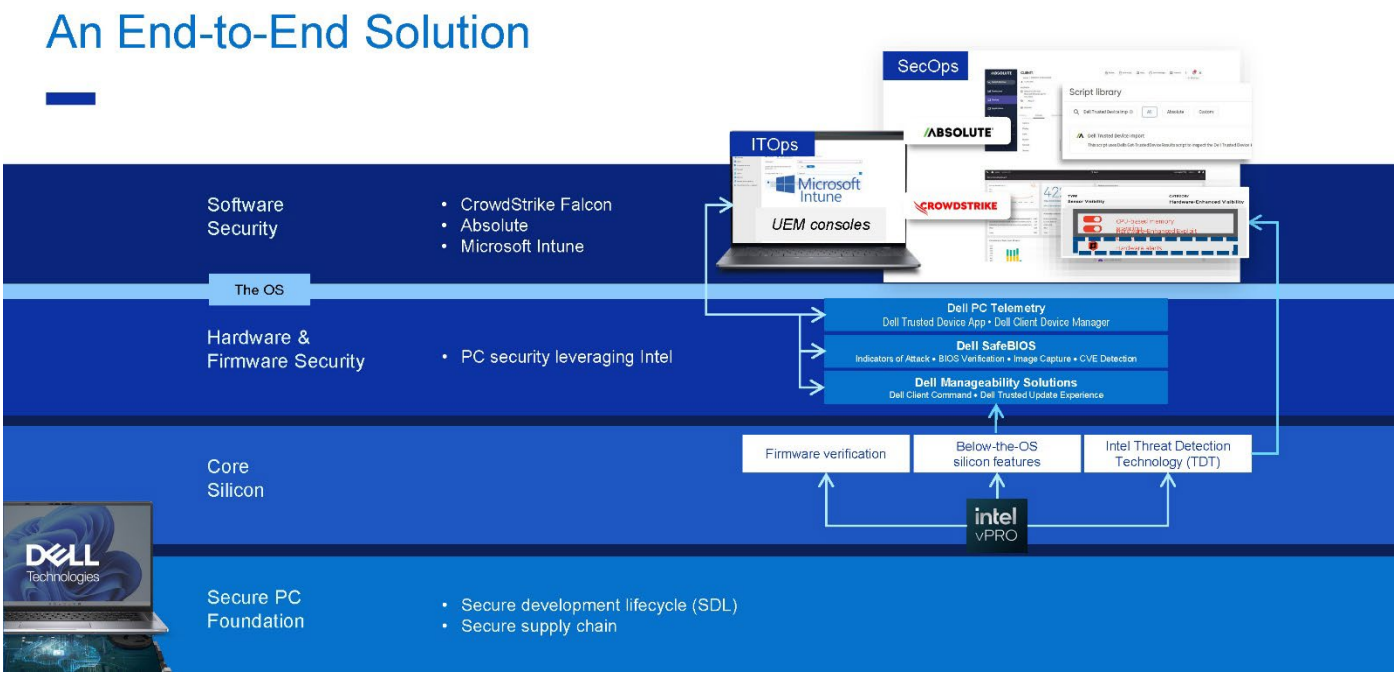



Figure 1: Today, effective security requires multiple layers of attack countermeasures. Dell and Intel work with software partners to deliver defense in depth.

We covered supply chain and the secure AI PC foundation that Dell and Intel offer. Now, let's look at the middle layers.

### Intel vPro® Security

Intel vPro Security is included with every Dell commercial device running on the Intel vPro® platform and delivers hardware-enhanced security features that help protect all layers in the computing stack. This collection of security technologies helps defend against modern threats at each layer: hardware, BIOS/firmware, hypervisor, VMs, OS, and applications.

### Dell Built-in Hardware and Firmware Security

Basic Input Output System (BIOS) protection is crucial to device security. If an attacker manages to corrupt a device's BIOS, they would be able to gain control of the entire device due to BIOS's unique and privileged position within the device architecture. To protect this critical layer, Dell commercial AI devices ship with SafeBIOS, a suite of layered security at the firmware level. The underlying capabilities that constitute SafeBIOS enhances protection, detection and recovery at a BIOS level.

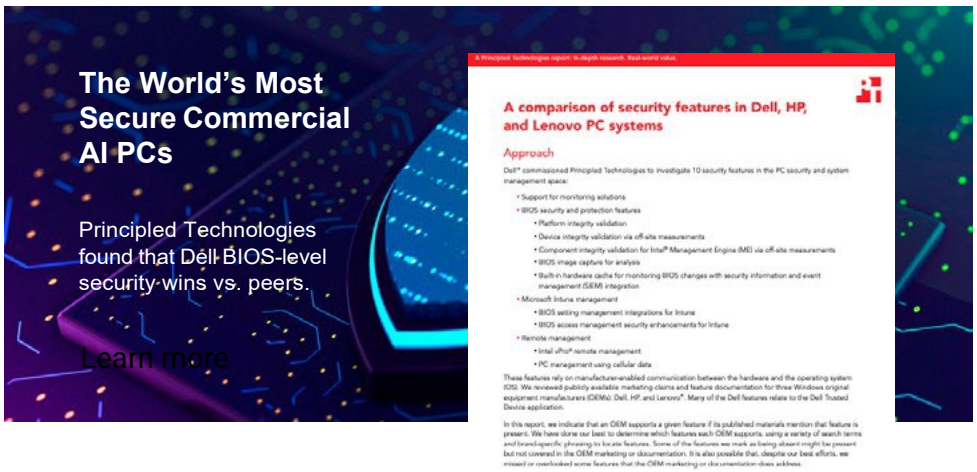



Figure 2: According to Principled Technologies, Dell and Intel deliver the World's Most Secure Commercial AI PCs.*

It is also important to note that effective security includes visibility into the current security posture. Dell makes these below-the-OS events from SafeBIOS visible at the OS level for admins and end-users to view and make decisions with the Dell Trusted Device application (DTD App).
The DTD App detects if the BIOS has been compromised by comparing measurements of the running BIOS image to that of the golden copy secured in the Dell environment, providing our market differentiated off-host BIOS verification. Additionally, Intel Management Engine (ME) firmware verification – available exclusively on Dell commercial PCs – protects against unauthorized access to and tampering of highly privileged firmware.

This Dell-unique PC telemetry (available via the Dell Client Device Manager (DCDM) for managed IT environments or the DTD App console for unmanaged environments) is the secret sauce in the security equation. This telemetry enables integration with third-party consoles, such as CrowdStrike and Absolute for security and Microsoft Intune for management (see Figure 1). In fact, Dell is the only PC manufacturer to provide firmware-level threat detection integration and visibility via third-party security consoles*

Dell also mitigates the growing risk of identity compromise and unauthorized access to sensitive workloads. Select Dell commercial devices include Dell SafeID with ControlVault 3+, a unique FIPS 140-3 level 3 certified security chip* that stores end-user credentials, isolating them from the OS, making them far less vulnerable to attack.

### Below-the-OS security is only one part of the holistic approach Dell takes to securing devices

To more wholly secure Dell commercial AI devices, Dell and Intel have also invested heavily in vetting and curating an ecosystem of industry-leading software security solutions. These capabilities provide protection from advanced threats posed by sophisticated attackers, offering an additional layer of security at the data and application layer.

Again, Dell and Intel can enrich software technologies with below-the-OS PC telemetry to enhance threat detection and response.

**Above the OS security**

## Built-on software security provides advanced threat protection

Given the potential payout from just one successful breach, cyberattackers are highly motivated, often making dozens of attempts on a single device over its lifetime. Compounded over an organization's fleet, this poses a serious concern. Can you hazard an attack slipping through? At this point, one thing is certain: no one solution can block 100% of attacks. This means the endpoints in your fleet, as all as the networks and cloud environments they operate in. Intelligent software solutions can help prevent, detect, respond to, and recover from threats wherever they occur. To this end, the Dell Trusted Workspace endpoint security portfolio includes industry-leading software to simplify procurement and provide business leaders everything they need to defend their endpoints. Capabilities include:

- Prevention, detection, response and remediation across the endpoint, network and cloud environments, leveraging AI and machine learning
- Endpoint geolocation, geofencing, remote data wipe, as well as self-healing for critical apps, on or off network
- Security Service Edge solutions for a data-centric approach to cloud security and access, protecting data and users everywhere

Intel security capabilities, integrated deep in the silicon, such as Intel Control-flow Enforcement Technology, protect against attacks targeting the OS, while other capabilities within Intel vPro® Security help protect below the OS, secure applications and data, and provide advanced threat protections.

**Hardware-assisted security**

## Integrated security

Attackers are increasingly directing their efforts to the organization's entire computing stack, which has traditionally lacked visibility and control. These evolving threats are circumventing legacy endpoint detection and response (EDR) software security tools, which is why PC security is so critical. To stay ahead of modern, fast-evolving threats, it takes deep ecosystem collaboration to adequately connect cross-vendor attack-surface protections into a cohesive solution.

However, that back-end integration work is complex and time- and resource-intensive. To help solve for this, Dell and Intel have leveraged our deep understanding of the adversary and customer pain points to work with partners to develop an integrated hardware and software solution called "Hardware-Assisted Security". Not only does Dell deliver the secure AI PC and source leading software partners, our unique device telemetry* enriches the entire security ecosystem, bringing greater BIOS-level visibility to your fleet. This integration capability is critical to closing the IT-security gap that so many organizations struggle with today. With Dell, Intel and our partner ecosystem, hardware and software talk to each other, improving fleet-wide security and manageability.


Figure 3: Evolving cyber threats circumvent software-only defenses. Help shrink the attack surface of endpoints with hardware-assisted protections.

**Spotlight on Hardware-Assisted Security with Dell, Intel and CrowdStrike**

Dell, Intel and CrowdStrike have co-engineered threat detection and response capabilities that combine the power of Dell Trusted Devices, the world's most secure commercial AI PCs*, with Intel's silicon capabilities and CrowdStrike's Gartner Magic Quadrant, 2024. Working together, CrowdStrike, Dell, and Intel's layered solution reimagines endpoint security for your business, extending beyond software protections to hardware-assisted security.

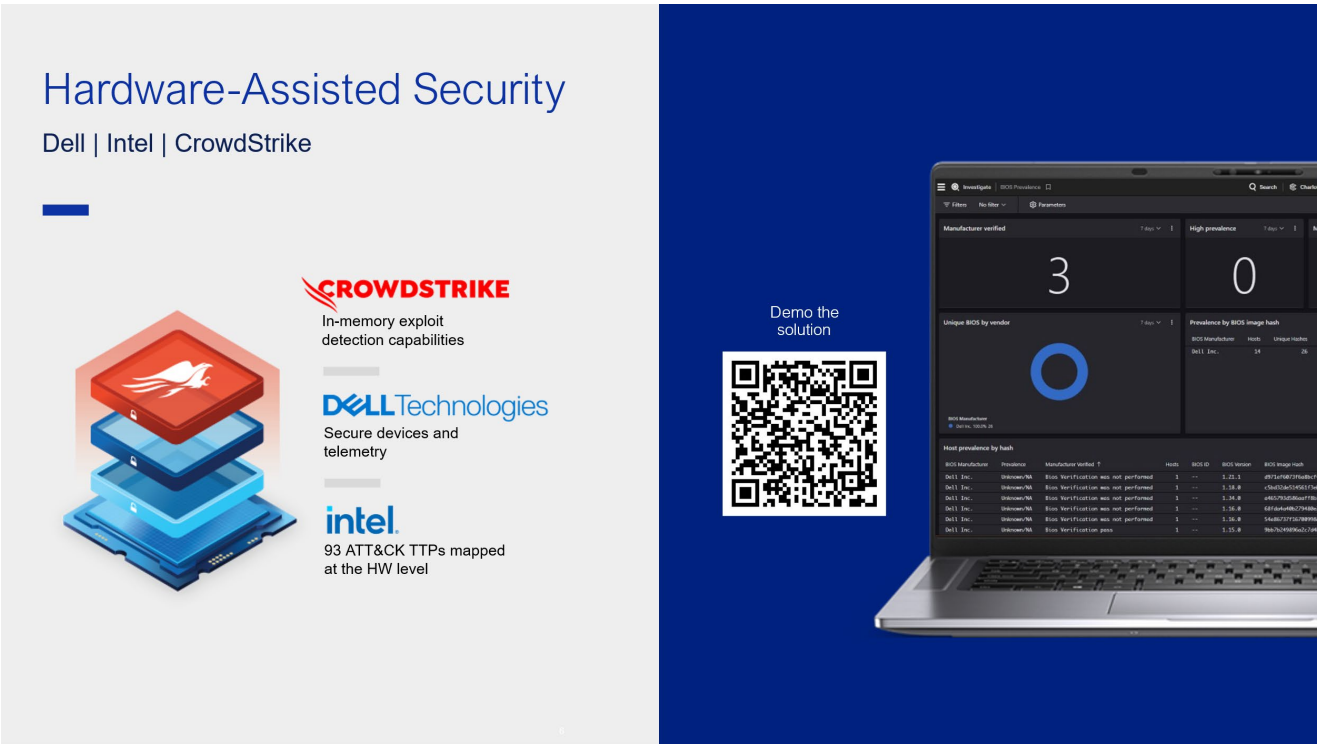



Figure 4: Multi-layer security on Dell commercial AI PCs, integrated with CrowdStrike and Intel.

## Additional value of Intel and CrowdStrike integration on Dell AI PCs

**Advancing Endpoint Security through AI and GPU/NPU acceleration:** Cyber threats are becoming more advanced, and AI PCs are designed to stay ahead by using on-device AI for faster, real-time threat detection while reducing reliance on cloud services. Tools like CrowdStrike can offload malware detection to built-in Neural Processing Units (NPUs), detecting threats quicker with minimal impact on CPU performance. With local data processing and advanced anti-phishing capabilities on Intel-based AI PCs, sensitive information stays secure, reducing exposure to external risks.

Some examples of Intel and CrowdStrike's work (currently in proof-of-concept phase but available publicly in the coming months) to advance endpoint security through AI and NPU acceleration:

- Hardware Enhanced Exploit Detection (HEED): Uses Intel CPU telemetry to trace control flow of apps to identify attacks to memory.
- Accelerated Memory Scanning (AMS): Uses Intel Threat Detection Technology to offload compute intensive memory scanning to the Intel Integrated GPU for up to 7x boosted Memory Scanning capability.

With these two features, Intel is instrumental in feeding CrowdStrike's AI-powered indicators of attack capabilities present on the endpoint and the CrowdStrike security cloud. These capabilities also provide a new lens into the memory layer for CrowdStrike to drop new scan detection models into the future improving security over time.

**Industry-validated defense of AI PC security:** New research from MITRE proves that your choice of PC hardware plays a critical role in enabling security software and OS features to protect your assets effectively.

Security Operations (SecOps) teams deploy powerful agents across endpoint PC fleets to inspect every process for signs of malware. Security software vendors have mapped their capabilities to the MITRE ATT&CK framework to show where they provide solutions. Managed Security Providers help enterprises triage daily alerts in XDR, SIEM, and co-pilot security tools. Pretty sophisticated, but the applicability of hardware security, in the PCs you already own, to real-world attacks has remained a mystery… until now.

In late 2024, MITRE Center for Informed Defense* (CTID) collaborated with over thirty experts from Intel, Microsoft, CrowdStrike, and ATTACK IQ to map and rank the significance of hardware optimized security software features against MITRE ATTACK framework tactics and (sub)-techniques. Together, the group mapped Intel vPro® security features to 150 cumulative and unique threat tactics, (sub)-techniques and procedures (TTPs) where PC hardware delivers out-of- the-box protections with optimized security software.

For mapping and emulation test validation, MITRE used a Dell Pro with an Intel Core Ultra Processor (including the full set of Intel vPro security protections enabled on a typical enterprise class security software stack), which enriches Dell's own unique built-in below-the-OS defenses.

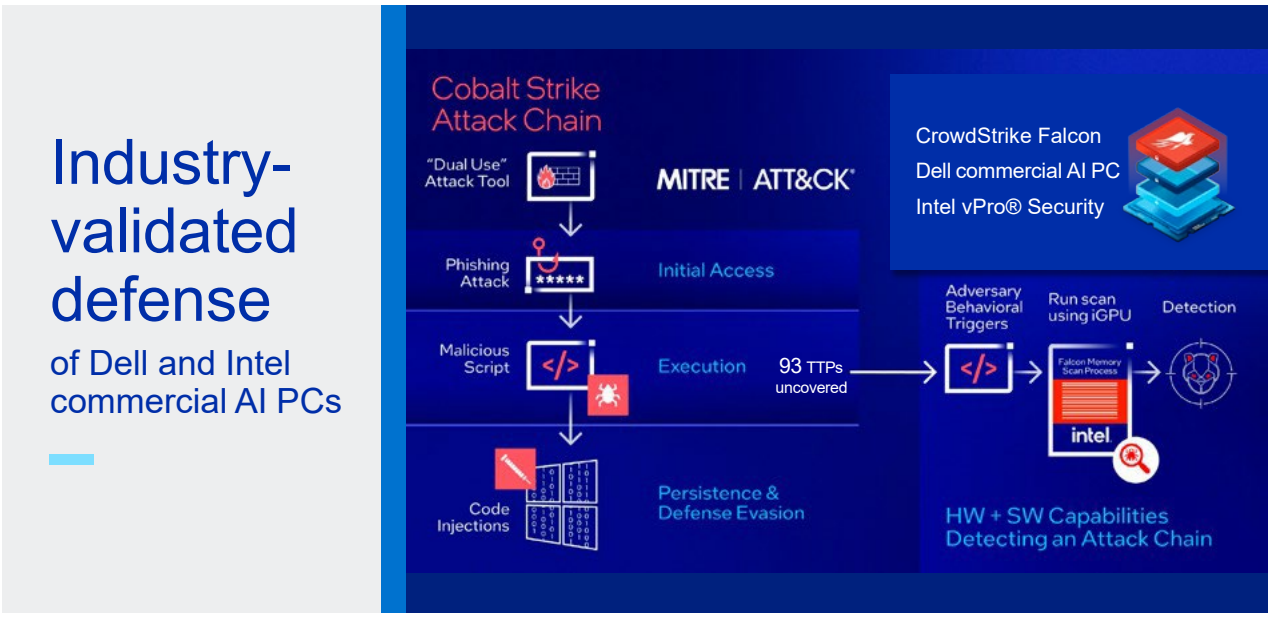



Figure 5: Hardware-assisted security works.

In the example scenario (Cobalt Strike Attack Chain scenario), we show a Cobalt Strike fileless attack to memory and how CrowdStrike Falcon helps provide mitigations leveraging hardware. As mentioned earlier, fileless malware attacks have become popular with adversaries. Almost 75% of all attack types abuse valid system processes, like executing in memory, where they can evade traditional EDR defenses. This is a prime illustration where the hardware in your PC helps to provide the incremental compute power to scan memory without disrupting the user's computing experience. **For CrowdStrike, which uses the accelerated memory scanning algorithms of Intel Threat Detection Technology (Intel TDT) and its ability to offload processing to the Intel Graphics Technology integrated graphics processor, this results in up to 7x performance acceleration which helps ensure a good user experience while delivering the capacity to scan deeper and uncover over 93 TTPs.** (Note: CrowdStrike's memory scanning capability, engineered in their software, works only on Intel vPro PCs.)

Having insights into both software and hardware-based security measures can help enterprises unlock the full potential available on modern AI PCs. The results prove that the choice of PC hardware has a significant impact on the ability of security software and OS features to counter specific threats and protect corporate assets against advanced cyber adversaries.

Dell and Intel's above- and below-the-OS security frameworks offer a holistic approach to protecting commercial devices, but as security experts we know that no device is absolutely secure. That is why we are industry leaders for post-release security investments to help ensure our devices remain secure for years after release.

**Ongoing support**

## Dell and Intel invest in ongoing security of their platforms post release

Dell and Intel have made significant and sustained investments to help assure security throughout a product's lifecycle. Once a device or platform is out in the market, teams at Dell and Intel continue to actively probe their products for vulnerabilities. For Intel, this process includes working together with researchers and universities to find possible exploitations before malicious actors do, quickly patch any vulnerabilities found, and then report them after the security loophole has been closed.

Proactive product security assurance includes efforts to find vulnerabilities internally and through incentives to the external security research community via Bug Bounty programs. In 2024, Intel's investment in proactive product security assurance accounted for 96% of the vulnerabilities discovered and mitigated. The remaining 4% of vulnerabilities addressed by Intel were either not submitted through the Intel Bug Bounty program or were submitted by partners or other organizations that do not seek bounty payments. In all cases, Intel worked with researchers to coordinate the public disclosure of these issues, meaning mitigations were available to customers on the public disclosure date.

To address the common vulnerabilities and exposures (CVEs) found through their extensive programs, Intel regularly pushes out Intel Platform Updates to all systems running on their products. This quarterly process consists of security, functional, and feature updates in microcode, firmware, and system BIOS. Regular updates enable Intel partners to validate and integrate hardware and firmware updates into their platforms on a predictable quarterly schedule, leading to coordinated public disclosure across the ecosystem.

Coordinating the disclosure of and response to identified product vulnerabilities is handled by Dell and Intel's dedicated Product Security Incident Response Teams. Together, they work to help ensure CVEs are handled quickly and securely, effectively mitigating any risks they pose.

Dell and Intel have made these investments to provide ongoing support to our customers and ease the burden on their IT teams. We've hired researchers, security architects, and cyber forensic analysts to help keep your business secure and enable your teams to focus on equipping your employees to do their best work.

## Intel’s investment accounts for 96% of vulnerabilities addressed in 2024

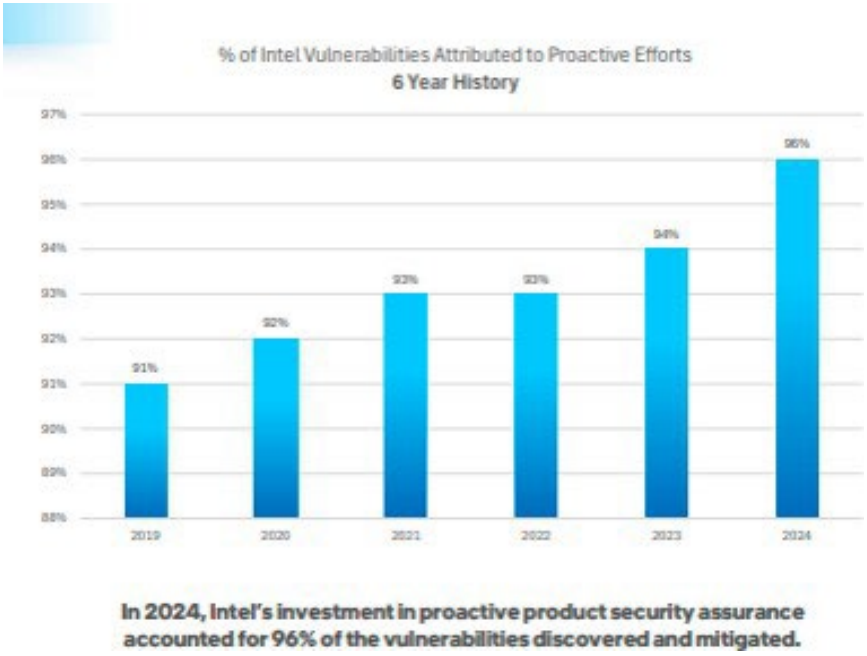
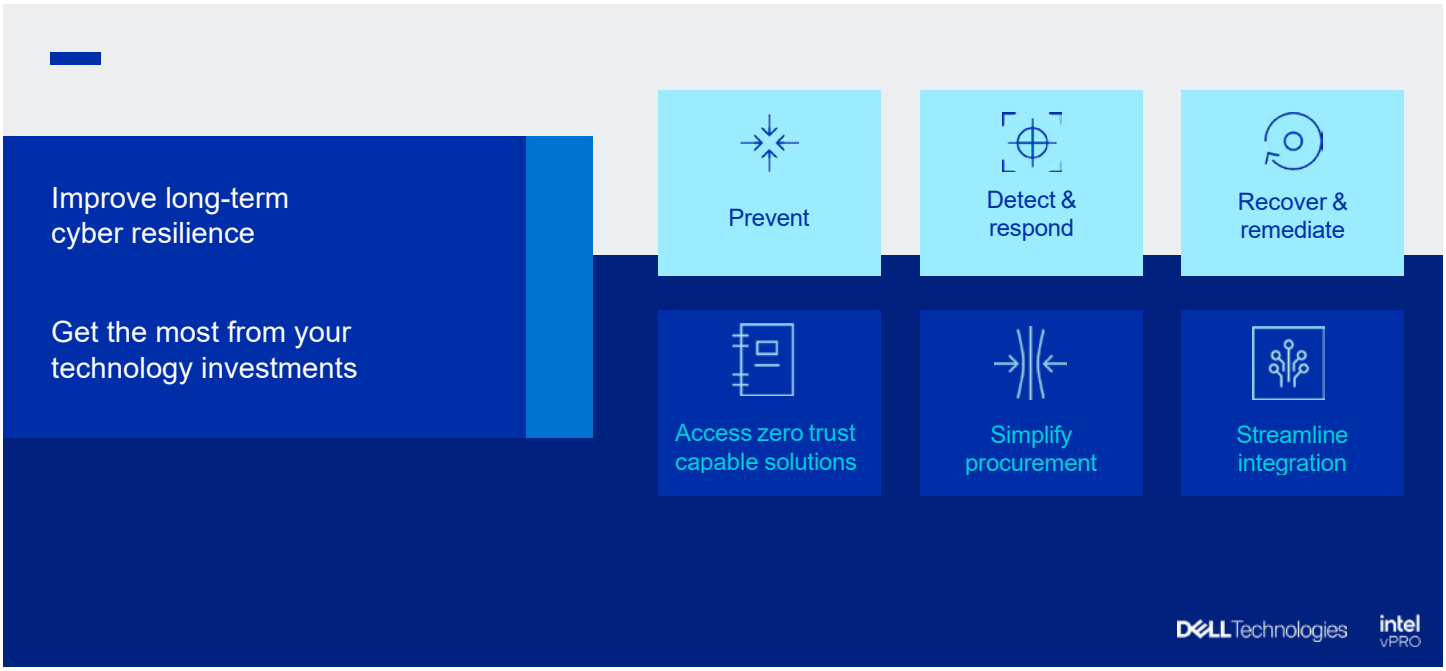



Figure 6: % of Intel vulnerabilities Attributed to Proactive Efforts (source: 2024 Intel Product Security Report)

# Conclusion

## The outcomes of working with Dell and Intel



Dell and Intel are focused on security outcomes and develop solutions based on the adversarial mindset. A key end goal for cyber adversaries: money, which they make by stealing data and selling it or holding it hostage. So, while their method of entry varies (MITRE ATT&CK® framework tracks nine overall initial access methods), cyberattack kill chains play out in very similar ways: recon, initial access (by exploiting a vulnerability=weakness or an exposure=mistake which they found), infiltrate a network, move laterally/gain greater privileged access, snoop around and learn more, exfiltrate data.

We can help you secure any workload with intelligent products, solutions, and services designed with the adversary in mind. Instead of trying to block 100% of attacks (which is impossible), we strip the ego out, assume an attack is inevitable and layer on defenses for the worst-case scenario. We emphasize visibility and actionability across a PC fleet. This helps our customers stay ahead of emerging attack vectors.

With Dell and Intel endpoint security solutions in place, organizations **achieve key security outcomes**:

- **Improve long-term cyber resilience**
- **Get the most from your technology investments**

Meet both cybersecurity use cases…:

- **Reduce the attack surface** – mitigate the risk of an attack slipping through; minimize the vulnerabilities and entry points that can be exploited to compromise the environment.
- **Improve threat detection and response** – actively identify and address potential security incidents and malicious activities with integrated layers of defense that speed detection and response.
- **Enable recovery and remediation** – capture breach data for analysis to guard against future threats and restore endpoints to a previous, known secure and operational state after a security incident.

…as well as ease the operational burden of security:

- Maintain device trust and identity trust with **zero trust capable offerings**
- **Simplify procurement** by consolidating providers and getting access to hardware, software and services all under one roof
- Save time and resources with **streamlined integration**

The battle of cybersecurity is won or lost based on your ability to collect, analyze and respond to threat intelligence. Today's attackers are innovative. Knowing that most security solutions focus above the OS only, adversaries are looking at softer attack surfaces: the below-the-OS layers and the supply chain. To stay ahead of these bad actors and to keep their businesses protected, today's leaders must consider built-in, hardware-based security technologies deep in the silicon as crucial when deploying commercial devices to their employees.

## See what solutions are right for you


Commercial AI PCs

**ASK ABOUT:**

*Hardware & firmware security • Supply chain security • Manageability • Core silicon & AI optimizations*

Software & Integrations

**ASK ABOUT:**

*Licenses available for purchase with Dell PCs • Standalone licenses • Telemetry integrations*

Services

**ASK ABOUT:**

*Managed Detection & Response (MDR) • Incident Recovery*

With world-class supply chain security, hardware-based protections, software for protection against advanced threats, managed services, and ongoing support, Dell and Intel are ready to offer you and your business commercial devices that get the job done and are designed to help keep your business data off the dark web.

*Most Secure Commercial AI PCs: Based on Dell internal analysis, October 2024. Applicable to PCs on Intel processors. Not all features available with all PCs. Additional purchase required for some features. Validated by Principled Technologies. A comparison of security features, April 2024.

---

Learn more about Dell solutions

Contact a Dell Technologies Expert

View more resources

Join the conversation



DELL Technologies

intel