DELL Technologies

Have it all

How to secure your AI-powered workforce with Dell Technologies, Microsoft and Intel.

Windows 11

intel

Executive Summary

The move to hybrid work has introduced new complexity and attack vectors — and endpoints, networks and clouds are expanding attack surfaces. And the race to adopt GenAI is raising the stakes further - introducing new security considerations, including data and IP leakage as well as high-speed contextual attacks.

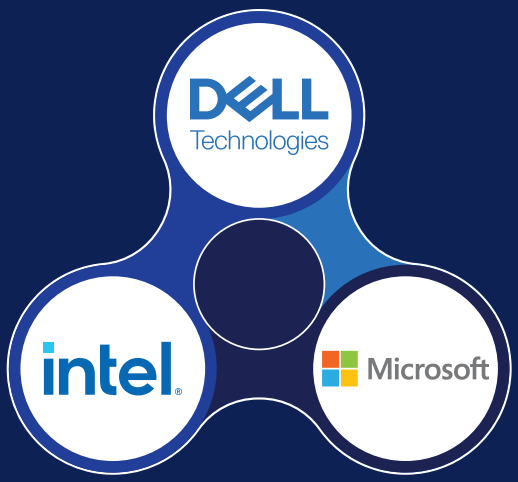
What's more, attackers now employ sophisticated techniques that target different layers of the computing stack, blending in with valid system processes. Some methods even allow attackers to gain privileged access and disable software protections, completely undetected.

It takes a village…

No single provider can address all of these issues alone, which is why Dell, Intel and Microsoft work strategically together to remove the burden for organizations.

Our holistic approach to security integrates hardware-based "below the OS" capabilities that help defend against attack, with silicon-based protections from Intel that target the deepest levels of a device.

We then ensure that Windows 11, Dell modern devices and software work together to shrink the attack surface, protect system integrity, and shield users and valuable data.



Better together. Better for you.

Dell Technologies, unique built-with/built-in security integrates all the security innovations from our partners Intel and Microsoft, so you can protect your hybrid workforce from evolving security threats.

Only 33% of IT decision makers are employing a holistic end-to-end security strategy, integrating both hardware- and software-based protections.

Source: Dell Innovation Index, 2023

Topics covered in this paper

Security foundation

Secure Development Lifecycle

Dell Technologies, Intel and Microsoft work in close collaboration to build in security from the chip to the cloud. An example of this being Dell Trusted Devices, the industry's most secure commercial PCs.*

Supply chain security

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

* Based on Dell internal analysis, September 2022. Not all features available with all PCs. Additional purchase is required for some features.

Comprehensive defence framework – enabling Zero Trust security

AI-driven security

Leverage AI to automate user protection, offering game-changing security solutions straight out of the box.

Below the OS security

Hardware-based security capabilities help protect devices from threats that target their foundational layers.

Above the OS Security

Software-based security technologies and silicon-based protections are both crucial to holistic device security.

Windows 11 Security

Out-of-the box protection with layers of tightly integrated software and hardware across OS, applications, identity and cloud.

Ongoing support

Dell, Intel and Microsoft ensure their solutions remain secure, by patching vulnerabilities, and updating silicon-based security within the OS.

Your business network is as secure as its weakest endpoint

It seems that every few months, another prominent global brand experiences a major security breach and the negative public exposure causes serious 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 device, or an unknown 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 throughout their manufacture or development?

Dell, Microsoft and Intel know that the only way to reliably secure business devices and networks is through a harmonization of hardware and software security technologies. 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.

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, Microsoft and Intel take a different, holistic approach to security.

Your business network is as secure as its weakest endpoint

Dell, Microsoft and Intel provide built-in, hardware-based security

The complexities and concerns of securing devices and networks are enough to make your head spin. 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, Microsoft 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 Microsoft and 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 device? It's more than a random collection of features – together, we 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
Microsoft, 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 Device technologies and Intel® Hardware Shield capabilities to harden device defenses through a framework of prevention, detection, and response. In addition, Dell, Microsoft and Intel have security teams dedicated to probing products and finding new vulnerabilities before attackers do – expediently pushing out patches to help keep you and your team covered.

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

Securing our platforms begins at the whiteboard

Planning, assessment, and analysis

Before designing their newest platforms, chipsets and software, respectively, experts at Dell, Microsoft and Intel set strict parameters for what a secure platform needs to include, to address the security needs of the future, meet required regulations and address future security needs. This process starts with a roundtable determination of likely future security and privacy risks plus the activities necessary to mitigate them. This assessment is used to define the security objectives we will evaluate our architectures against.

With this information, security teams from Dell, Microsoft and Intel develop threat models by adopting an adversarial mindset to this conceptual architecture, probing for potential vulnerabilities and exploits which must be addressed. 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 to determine if the product is on track to meet our customers' needs.

Securing our platforms begins at the whiteboard

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 which uses special tools for finding and fixing defects. Some products with more complicated code then move to a manual review process, where security experts perform line-by-line reviews of product code to find previously overlooked 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, missed in the earlier phases. These findings are mitigated again based on risk, so that any additional identified exposure is 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 beginning, 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 our commitment to end-to-end security is our investment in a safe 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 door is secure from the first boot.

Supply chain assurance is foundational to device security

A lot can happen between the time a component or device leaves the factory and arrives at its destination. Each step in the supply chain represents a new vector that opens your employees, business, and customers up to potential attack. Dell and Intel have developed tools, technologies, and processes to help ensure the security of our products before they reach 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 so that 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 so 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 tools designed to detect if the Dell devices inside have been tampered with in transit.

Dell devices themselves also feature tamper detection technologies. Dell Technologies Safe SupplyChain 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.

Supply chain assurance is foundational to device security

Verify

Dell commercial 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.

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

Similarly, Intel has been enabling vendors with base digital supply chain transparency and traceability for many years. Intel®Transparent Supply Chain (Intel®TSC) delivers TCG platform certificates and component data for supporting Intel-based platforms using a cloud API available to IT through the Intel®TSC web portal. Although Dell and Intel opted to implement independent solutions, TCG platform certificates are a common ingredient between Intel®TSC and Dell SCV. This commonality provides compatibility and interoperability that enable enterprise and government buyers to deploy TCG platform certificates for improved digital supply chain security assurance for Intel-based devices.

Comprehensive defence framework – enabling Zero Trust security

Organizations advancing their cybersecurity maturity are building an actionable roadmap that identifies ways to reduce their attack surface, detect and respond to cyber threats, and implement ways to recover from cyber attacks, all with Zero Trust enabling capabilities.

To address increasingly sophisticated cyber threats, Dell utilizes the built-in security capabilities in our solutions and those of our partners including Microsoft and Intel to help our customers achieve Zero Trust that aligns to our customers business objectives.

77%

have yet to explore/ build a Zero Trust architecture*

* Dell Technologies, Innovation Index, 2023: https://www.dell.com/en-us/dt/perspectives/innovation-index.htm

Dramatically simplify Zero Trust adoption for your workforce with a fully integrated architecture

Dell, Microsoft, and Intel collaborate to facilitate a seamless and secure hybrid work environment, enabling customers to fulfill the three principals of Zero Trust:

1.Verify explicitly

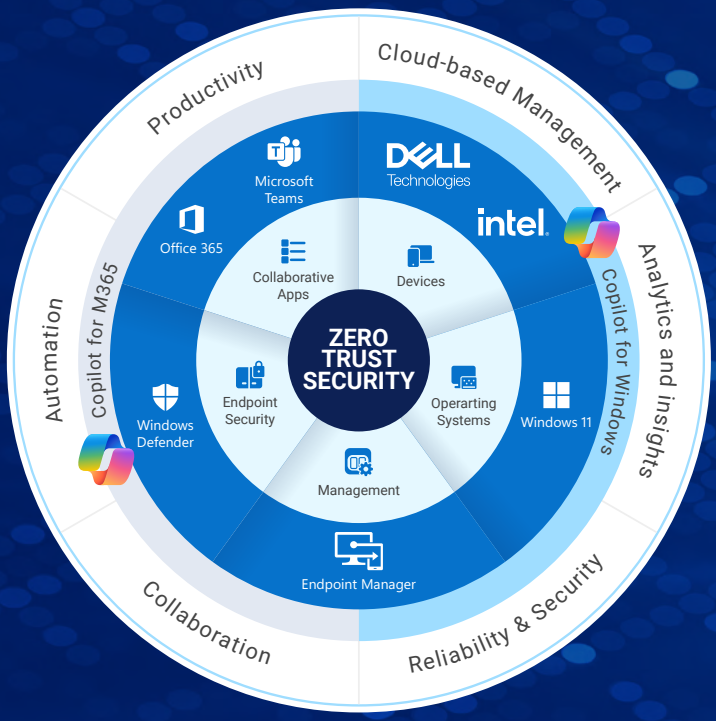
Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

2. Use least privileged access

Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity.

3.Assume breach

Operate in a manner that minimizes blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.



Our joint solutions help organizations implement a Zero Trust security model by verifying every access attempt and enforcing strict security policies based on identity, device health, location, and risk level, thereby reducing the risk of unauthorized access and mitigating the impact of security breaches.

Achieved by integrating:

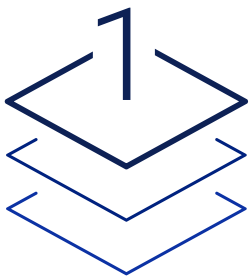
Dell commercial PCs BIOS/firmware security, hardware security, supply chain assurance, threat management software (EDR, XDR, VDR), network and cloud data protection software combined with Intel VPro.

Microsoft's comprehensive suite of tools and technologies for identity and access management, endpoint security, network security, data protection, threat intelligence, security analytics, policy enforcement, and continuous monitoring and response. These include Azure Active Directory, Microsoft Defender for Endpoint, Azure Firewall, Azure Information Protection, Microsoft Threat Intelligence, Azure Sentinel, Microsoft Endpoint Manager, and Microsoft Security Center.

AI-driven security

Game-changing AI-driven security right out of the box.

Dell, Intel, and Microsoft and Intel leverage AI to automate user protection, collectively offering game-changing security solutions straight out of the box. These innovative measures are designed to prevent and detect today's more sophisticated attacks, incorporating hardware-based security, advanced encryption, and malware protection, all powered by Intel® Core™ Ultra Processors on Intel vPro® and Windows 11 Pro operating systems, seamlessly integrated into modern Dell devices. Working together, this collaboration significantly reduces the attack surface by implementing multiple layers of defenses, focusing on three key areas:

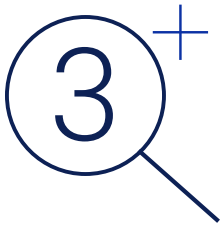


1. Below the OS:

- Dell and Intel have closely collaborated on Dell SafeBIOS, a robust defense mechanism against BIOS and firmware attacks, complete with off-host verification to ensure the integrity of BIOS and vPro firmware.
- Dell vPro devices achieve Windows 11 Secured Core PC Level 3 certification, incorporating a suite of tightly integrated protections.
- For instance, the Intel System Security Report provides assurance to the OS regarding the securely executed boot process, ensuring integrity from the outset.
- These protections are inherent and seamlessly operational right out of the box.

2. Application & Data Protection:

- Advanced capabilities are in place to safeguard user credentials, such as the isolation of user credentials facilitated by Windows Hello through Intel virtualization technologies.
- Multi-key total memory encryption empowers Windows 11 virtual machines with encrypted memory, effectively isolating processes and their associated data.
- These protective measures are pre-configured for immediate use or can be conveniently adjusted via the Windows security center.



3. Advanced Threat Detection:

- Intel® Threat Detection Technology stands out as the only silicon-enabled AI threat detection solution capable of thwarting ransomware and crypto-jacking attacks.
- Given ransomware's heavy reliance on CPU for encrypting critical business content, Intel TDT employs AI-driven threat detection to scan CPU telemetry for attack indicators, promptly flagging malicious processes for action by security software like Microsoft Defender, facilitating their quarantine or termination.

AI-driven security

Our collaboration extends to offering Accelerated Memory Scanning for Early Detection of File-less Malware, providing an added layer of security to deny malware attacks. Through our partnership with Microsoft Defender and Intel Threat Detection Technology, we optimize compute-intensive scanning processes by offloading them to the GPU, freeing up the CPU for uninterrupted productivity. In the event of a potential attack, the GPU proactively communicates with MSFT Defender, enabling a more comprehensive scanning approach.

This capability **benefits organizations** in **three ways:**

Reduction in the volume of fileless attacks, which have become the predominant method of entry for various cyber threats.

Early detection of ransomware and other malicious threats at the initial memory access stage

Preservation of a high-performing user experience while security protection scans are underway.

By leveraging Accelerated Memory Scanning, organizations can bolster their defense against evolving cyber threats while ensuring optimal operational efficiency and user productivity.

In essence, the collaboration between Dell, Microsoft and Intel yields comprehensive security solutions that encompass hardware-based protection, secure boot processes, application and data security, and advanced threat detection capabilities, all meticulously crafted to address the evolving cyber threats of today.

Built-in security technologies help prevent, detect, and respond to 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, Microsoft 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. In addition to other Dell and Intel tools and technologies, Intel® Hardware Shield and Dell's SafeBIOS framework provide built-in, hardware-based protection to Dell commercial device users.

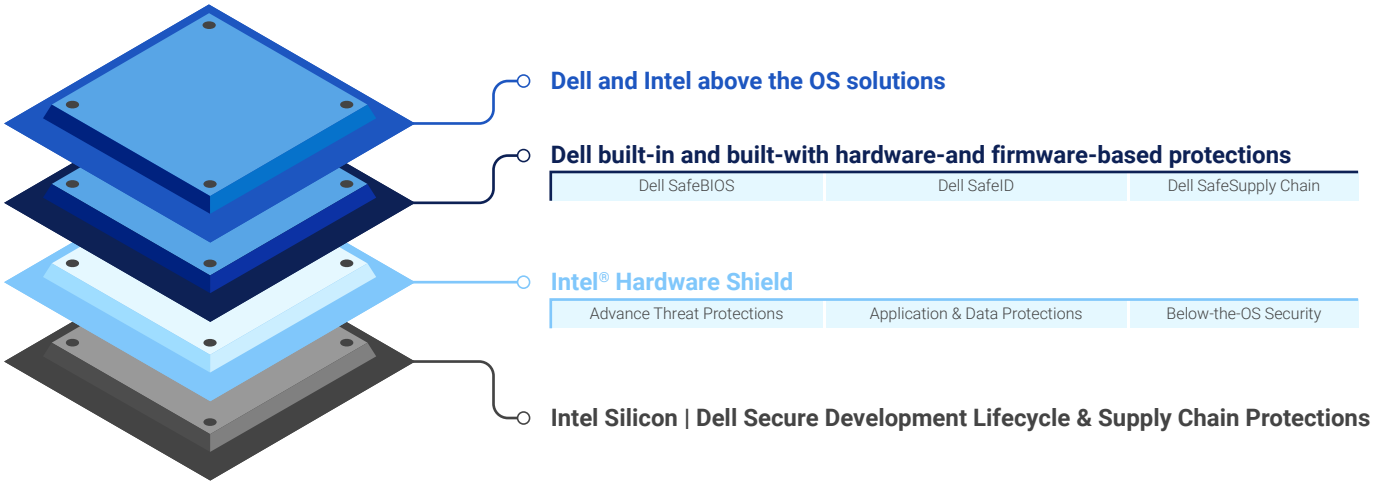


Figure 1: Intel® Hardware Shield and Dell hardware-based protections are security layers that help defend against foundational level attacks

Intel® Hardware Shield

Intel Hardware Shield 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.

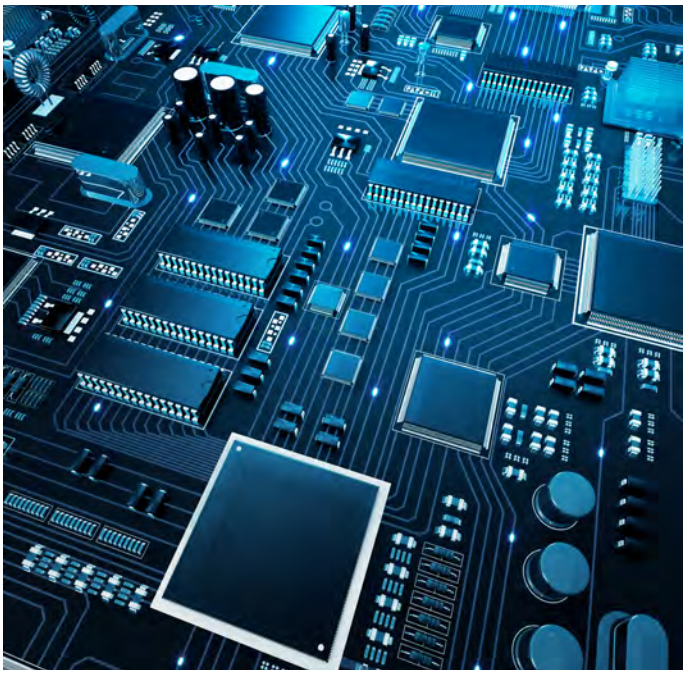
Intel Hardware Shield consists of Advanced Threat Protections, Application and Data Protections, and Below the OS Security, which encompass over twenty innovative security technologies. Dell has harnessed almost every one of these capabilities to develop security solutions that draw on their foundational features to provide customers with one of the most secure commercial devices on the market. These solutions include the Dell SafeBIOS framework, Dell SafeID, and Dell SafeSupply Chain, together helping to offer an even greater level of security assurance against current and future threats.

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

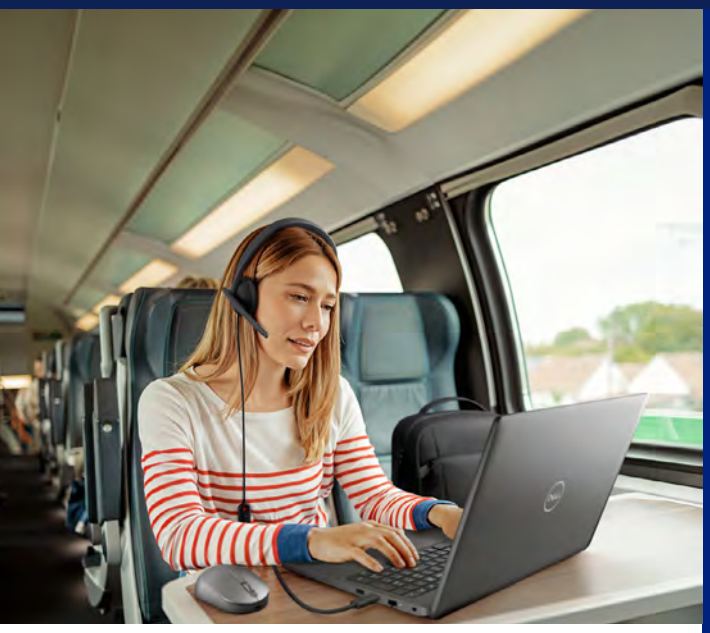
Dell SafeBIOS framework, Dell SafeID and Dell SafeSupply Chain

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 devices ship with SafeBIOS, a suite of tools that help prevent BIOS attacks, detect if the BIOS has been compromised, and respond by alerting IT if irregularities are found.

Selected Dell commercial devices also include Dell SafeID, which secures end user credentials in a dedicated security chip to keep them hidden from malware that looks for and steals access credentials, a breach that could potentially compromise an entire business network. For extra assurance of product safety, Dell offers optional add-on features like Secured Component Verification and tamper-evident packaging via Dell SafeSupply Chain.



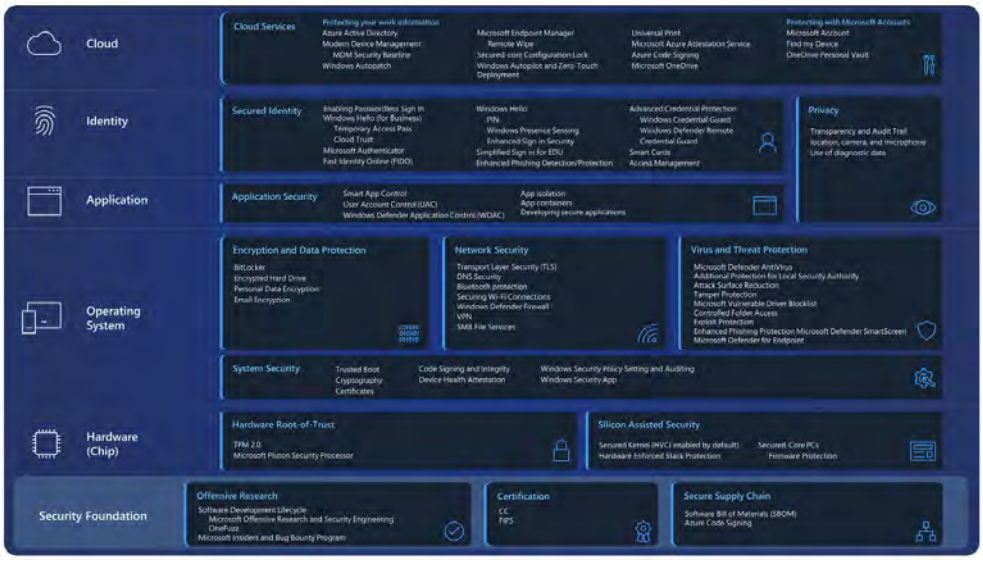
Dell and Intel's above-the-OS solutions help keep endpoints secure



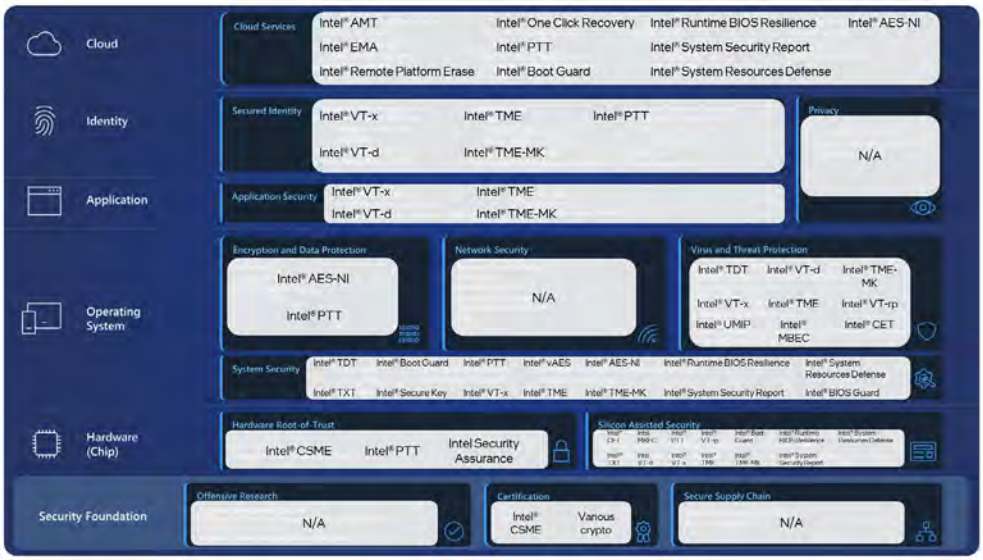
Despite the rising threat of below-the-OS attacks, protection above-the-OS is more important than ever before. With the number of end users who are working remotely and on-the-go increasing exponentially, you need intelligent solutions that prevent, detect, and respond to threats wherever they occur. The Dell Trusted Workspace endpoint security portfolio includes optional software like Dell SafeGuard and Response, along with Dell SafeData to give business leaders what they need to protect their endpoints. 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 Hardware Shield protect below the OS, secure applications and data, and provide advanced threat protections.

Next we layer in software security from Microsoft which runs from the Security Foundation through to the Cloud. In Windows 11, hardware and software work together to protect sensitive data from the core of your PC all the way to the cloud. Comprehensive protection helps keep your organization secure, no matter where people work. The following page shows the layers of protection in Windows 11.

Dell, Microsoft and Intel's above-the-OS solutions help keep endpoints secure



Intel then integrate the additional hardware protections across each layer of Microsoft's Security vision. These are then built into the Dell Client solutions.



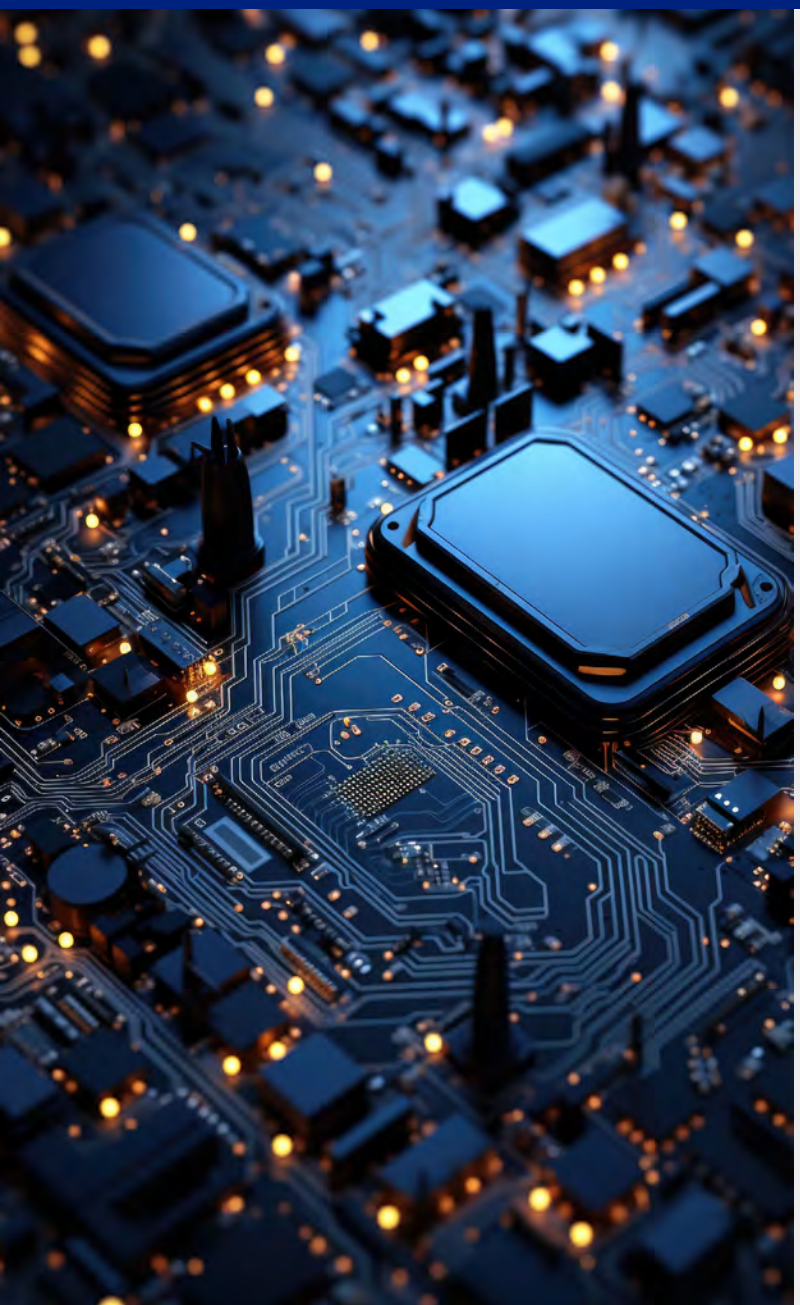
Partnering to deliver powerful protection by default.

Dell Technologies', unique built-with/built-in security integrates all the security innovations from our partners Intel and Microsoft, so you can protect your hybrid workforce from evolving security threats.

Windows 11 Security

End-to-end protection with modern management.

Windows 11 is the most secure Windows ever as most security features are enabled out of the box. The hardware and software work together to protect sensitive data from the core of your PC all the way to the cloud, with layers of protection at each level of the hardware, operating system, applications, identity and cloud – all improving productivity, security and resilience anywhere.



Hardware (Chip)

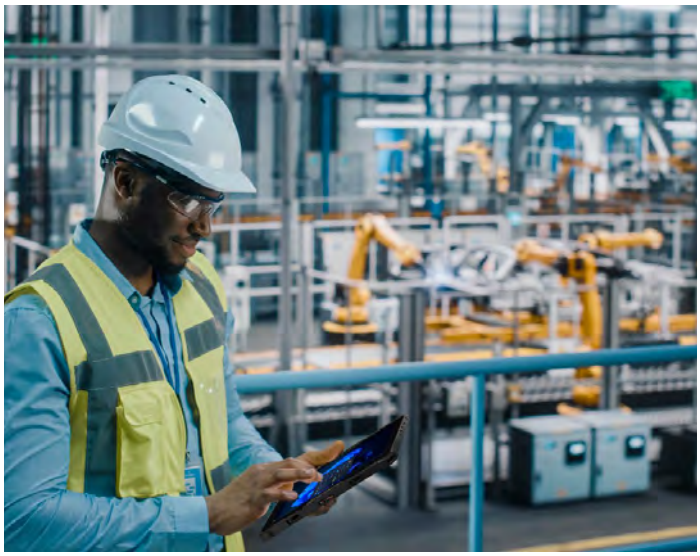
Hardware root-of-trust

A hardware root-of-trust helps protect and maintain the integrity of the system as the device powers on, loads firmware, and then launches the operating system, meeting important system security goals.

Trusted Platform Module (TPM)

Trusted Platform Module (TPM) technology is designed to provide hardware-based, security related functions. TPMs provide security and privacy benefits for system hardware, platform owners, and users. Windows Hello, BitLocker, System Guard (previously called Windows Defender System Guard), and other Windows features rely on the TPM for capabilities such as key generation, secure storage, encryption, boot integrity measurements, and attestation.

Windows 11 Security



Operating system

System security

Trusted Boot (Secure Boot + Measured Boot)
Windows 11 requires all PCs to use Unified Extensible Firmware Interface (UEFI)'s Secure Boot feature. When a Windows 11 device starts, Secure Boot and Trusted Boot work together to prevent malware and corrupted components from loading.

Encryption and Data Protection

BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers.

Secured-core PCs

Microsoft has worked with Dell to offer a special category of devices called Secured-core PCs (SCPCs). The devices ship with additional security measures enabled at the firmware layer, or device core, that underpins Windows.

Network Security

To help reduce an organization's attack surface, network protection in Windows prevents people from accessing dangerous IP addresses and domains that may host phishing scams, exploits, and other malicious content. Using reputation-based services, network protection blocks access to potentially harmful, low-reputation domains and IP addresses.

Virus and Threat protection

Microsoft Defender SmartScreen
Microsoft Defender SmartScreen protects against phishing, malware websites and applications, and the downloading of potentially malicious files.

Windows 11 Security

Application

Smart App Control

Smart App Control prevents users from running malicious applications on Windows devices by blocking untrusted or unsigned applications. Smart App Control goes beyond previous built-in browser protections by adding another layer of security that is woven directly into the core of the OS at the process level.

Application Isolation

Win32 app isolation is a new security feature in public preview designed to be the default isolation standard on Windows clients. It is built on AppContainer, and offers several added security features to help the Windows platform defend against attacks that leverage vulnerabilities in applications or third-party libraries.

Identity

Enabling passwordless sign-in

Windows Hello can enable passwordless sign-in using biometric or PIN verification and provides built-in support for the FIDO2 passwordless industry standard. Windows Hello for Business extends Windows Hello to work with an organization's ActiveDirectory and Microsoft Entra ID accounts. It provides single sign-on access to work or school resources such as OneDrive for Business, work email, and other business apps.

Advanced credential protection

In addition to adopting passwordless sign-in, organizations can strengthen security for user and domain credentials in Windows 11 with Credential Guard and Remote Credential Guard.

Privacy transparency and controls

Prominent system tray icons show users when resources and apps like microphones and location are in use. A description of the app and its activity are presented in a simple tooltip that appears when you hover over an icon with your cursor. Apps can also make use of new Windows APIs to support Quick Mute functionality.

Windows 11 Security

Cloud

Microsoft Entra ID

Microsoft Entra ID (formerly Azure Active Directory) is a comprehensive cloud-based identity management solution that helps enable secure access to applications, networks, and other resources and guard against threats.

Microsoft Intune

Microsoft Intune is a comprehensive endpoint management solution that helps secure, deploy, and manage users, apps, and devices. Intune brings together technologies like Microsoft Configuration Manager and Windows Autopilot to simplify provisioning, configuration management, and software updates across the organization.

Microsoft Azure Attestation Service

Remote attestation helps ensure that devices comply with security policies and are operating in a trusted state before they are allowed to access resources. Microsoft Intune integrates with Microsoft Azure Attestation Service to review Windows device health comprehensively and connect this information with Microsoft Entra ID Conditional Access.

Dell, Microsoft and Intel invest in ongoing, post-release platform security

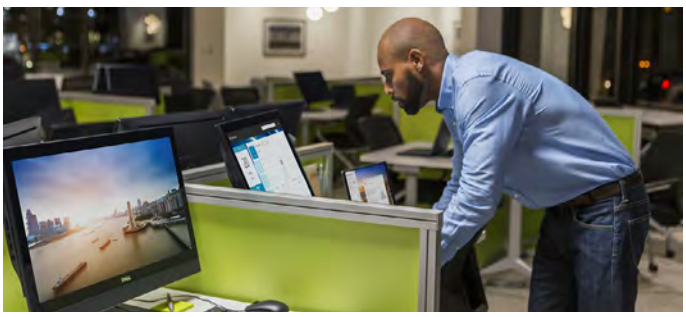
$46.4B

our combined R&D in 2023*

* Macrotrends.net – R&D spend in 2023: Dell Technologies $2.88 billion, Intel $16.046 billion, Microsoft $27.524 billion

Dell, Microsoft and Intel have made significant and sustained investments to help assure security throughout a product's lifecycle. Once a device or platform is in the market, teams at Dell, Microsoft 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, quickly patch any vulnerabilities found, and then report them after the security loophole has been closed.

As part of this effort, Intel funds a bug bounty program that is one of the best in the industry, accounting for 86% of externally found vulnerabilities in 2021. The CVEs (Common Vulnerabilities and Exposures) found through this program and by internal or external researchers are logged in a public database. As a proud leader in post-release vulnerability monitoring and reporting, Intel has logged and patched more potential vulnerabilities than most competitors, staying ahead of chip manufacturers who do not match this commitment to transparency and device security.



To address the CVEs found through their extensive programs, Intel regularly pushes out Intel Platform Updates to all systems running on their products. This rollout is an extensive process that requires validation from Intel's partner ecosystem, including CSPs, ISVs, OEM/ODMs, and SIs.

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, Microsoft 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.

Dell, Microsoft and Intel are committed to helping you secure your growing business

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. Understanding that most security solutions focus on securing software only, they are looking at below-the-OS layers and the supply chain as new vectors to compromise your security and exploit businesses like yours.

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.

Dell, Microsoft and Intel have been partnering in the commercial device space for decades and have earned our customers' trust with some of the most secure commercial devices in the industry. Our joint expertise and co-engineering relationship enable us to stay ahead of hackers through our consistent research, diligence, and innovation. As leaders in the commercial device space for many years, we see more and stop more – constantly acting on an immense set of data and telemetry to continually help deliver and improve the security of our joint customers' commercial devices. Our thought leaders meet regularly to discuss what comprehensive security looks like today, what it will look like tomorrow, and the investments needed to ensure our products remain at the leading edge of commercial cybersecurity.

With world-class supply chain security, hardware-based protections, software for protection against advance threats and ongoing support, Dell, Microsoft and Intel are ready to offer you and your business commercial devices that not only get the job done but are also designed to help keep your business data off the dark web. Speak to your Dell sales rep today to learn more about our commercial device programs and how we can help you achieve your business objectives.

Click here to

Have it all

DELL Technologies

Windows 11

intel