Achieving pervasive security above and below the OS

Dell and Intel apply Zero Trust principles to their commercial PCs to help keep businesses and their employees secure

April 2022

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
- Dell and Intel's decades long co-engineering relationship is founded on their commitment to keeping commercial customer networks secure
- Our holistic approach to security employs both software-based, "above the OS" protections against traditional attacks but also hardware-based, "below the OS" capabilities that help defend against attacks targeting the deepest levels of a device
- 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	Supply Chain Security
Dell and Intel design their products with security as a chief element and test rigorously before release	Protections are in place along the supply chain to help ensure devices stay secure after leaving the factory

Comprehensive defense framework

Below the OS security	Above the OS security	Ongoing support
Hardware-based security capabilities help protect devices from threats that target their foundational layers	Software-based security technologies remain a crucial component to a holistic approach to device security	Dell and Intel work tirelessly to help ensure their products remain secure and to patch exploitable vulnerabilities

Key security trends

78% **78% of security professionals** surveyed said **attacks increased** as a result of employees **working from home**[1]

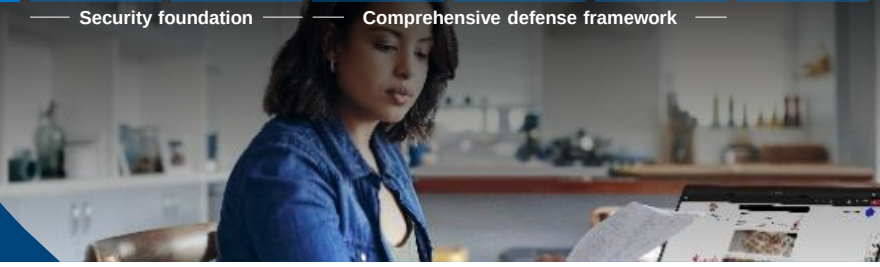
62% **62% of supply chain attacks** investigated by the European Union Agency for Cybersecurity were the **result of misplaced trust in a supplier**[2]

8% Ransomware remains the number one threat for most organizations, **rising 8% YoY in 2021**[3]

44% A recent study found that **44% of organizations** experienced at least one **hardware-level or BIOS attack** over the past 12 months and **16% have had more than one attack**[4]

1. Surge in Cyberattacks Targets the Anywhere Workforce, VMware, 2021
2. Threat Landscape for Supply Chain Attacks, ENISA, 2021
3. 2021 State of the Threat, Secureworks, 2021
4. Dell Technologies Intrinsic Security Helps Businesses Build Cyber Resilience, Dell Technologies, 2020

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 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?

Dell and Intel know that the only way to reliably secure business 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.

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 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 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 device? It's more than a ramshackle collection of features – 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

We look beyond today's threats when designing tomorrow's systems to minimize the attack surface and help ensure Dell 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 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 whitepaper, we'll explore how Dell 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 starts at the whiteboard

Planning, assessment, and analysis

Before designing their 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 which 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 what the threat surface is 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.

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 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 their 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 doorstep 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 when it arrives to its destination. Each step 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 their 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 Technologies 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 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.

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 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.

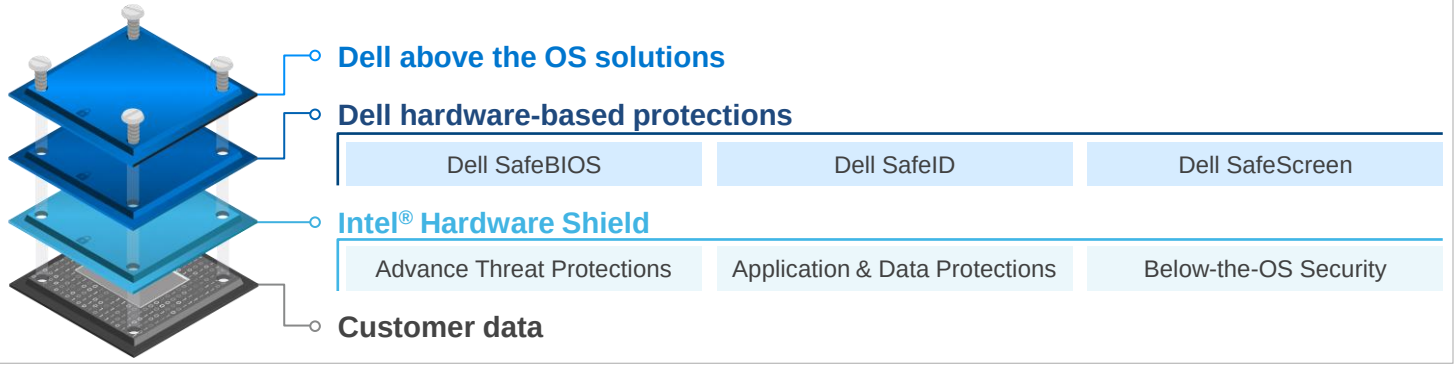


Figure 1: Intel® Hardware Shield and Dell hardware-based protections are security layers that help defend against foundational level attacks

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 SafeScreen, together helping to offer an even greater level of security assurance against current and future threats.

Dell SafeBIOS framework, Dell SafeID, and Dell SafeScreen

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 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.

Select 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.

In addition, Dell enables end users to work from anywhere while keeping private information private by including Dell SafeScreen on select commercial devices. Dell SafeScreen helps keep sensitive information and credentials safe from physical threats with an integrated digital privacy screen and sensor-enabled webcam.

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

To more wholly secure Dell commercial devices, Dell has also invested heavily in security solutions above the OS. These capabilities do more to help protect devices from advanced threats posed by sophisticated attackers by offering an additional layer of protection at the data and application layer.

Dell'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 Devices endpoint security portfolio includes optional software like Dell SafeGuard and Response, Dell SafeData, and VMware Workspace ONE® to provide business leaders what they need to protect their endpoints.

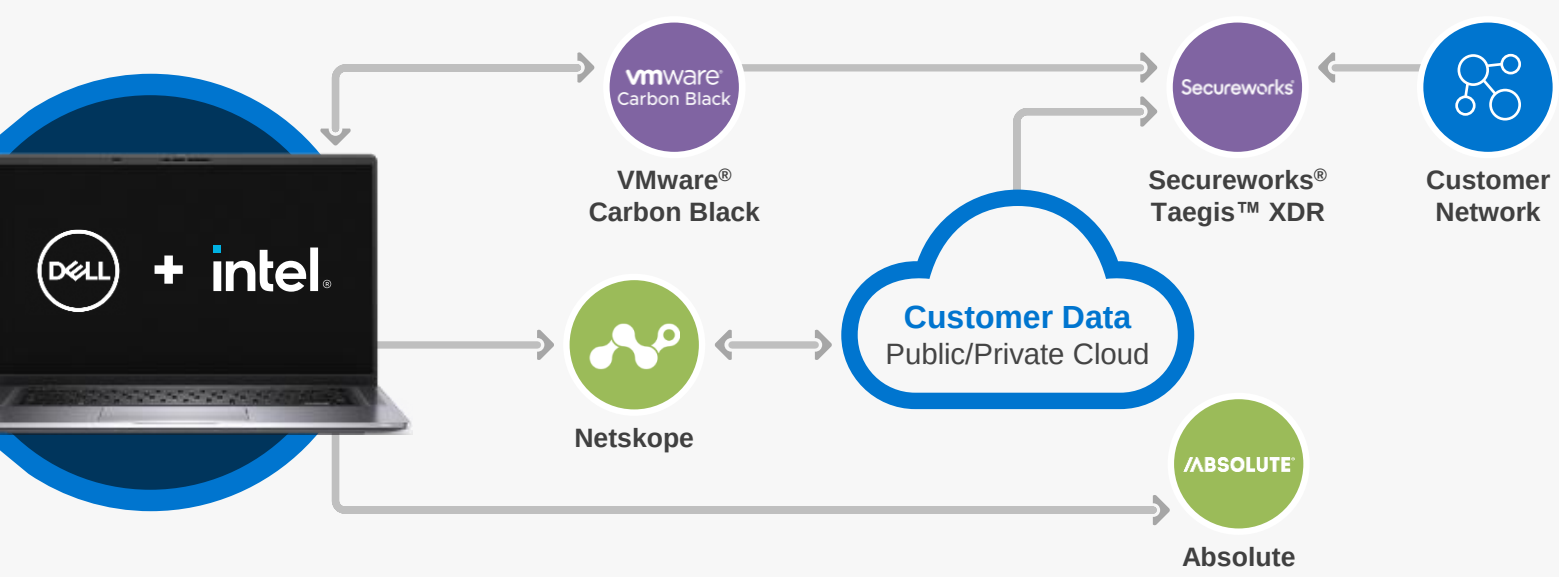


Figure 2: The Dell Trusted Device endpoint security portfolio includes above the OS protections

Dell SafeGuard and Response is powered by **VMware® Carbon Black** and **Secureworks® Taegis™ XDR**, combining a next-generation antivirus with security telemetry analysis on endpoint, network, and cloud. Dell SafeGuard and Response helps businesses detect, investigate, and respond to advanced threats across their organization.

Dell SafeData encrypts sensitive information and protects data with **Netskope** and **Absolute.** These applications provide visibility, monitoring, and data loss prevention for cloud-based applications and restore endpoint applications to their original safe state in the case of malicious attacks.

VMware Workspace ONE® is an intelligence driven digital workspace platform that simply and securely delivers and manages any app on any device by integrating access control, application management, and multiplatform endpoint management. With the recent integration of Intel vPro® platform technologies with VMware Workspace ONE, IT teams can now benefit from better security and chip-to-cloud management of endpoints

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.

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.

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 our 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 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.

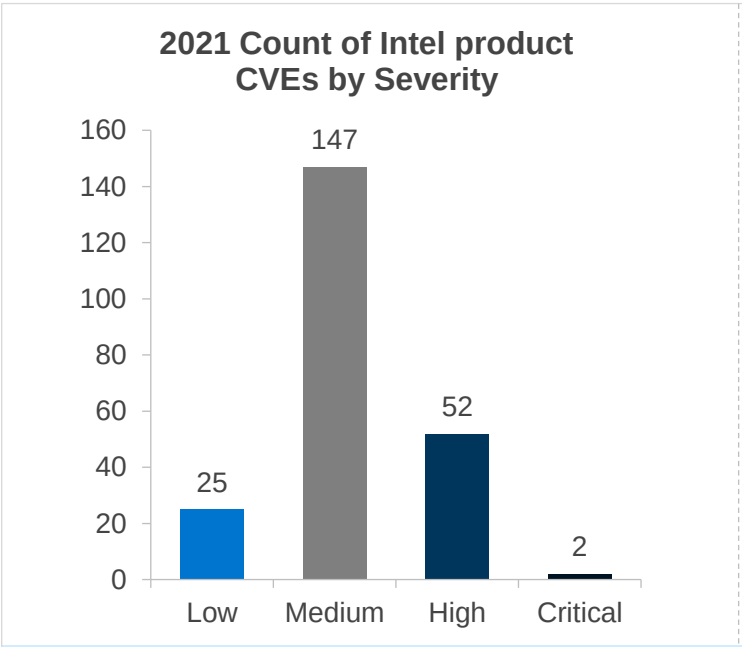


Figure 3: Count of Intel product CVEs found by internal and external researchers in 2021

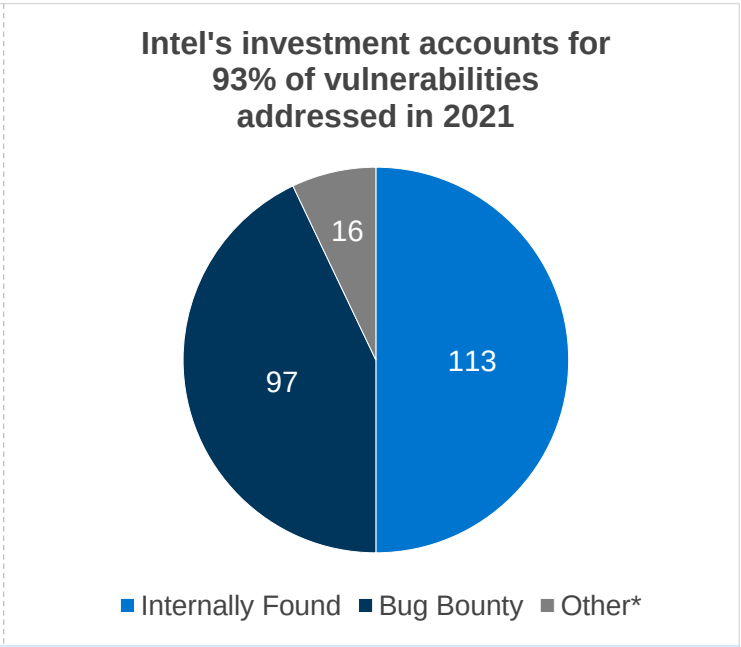


Figure 4: Internal and external teams worked to find vulnerabilities in Intel platforms that were patched before they could be exploited

Dell 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 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 decades, Intel and Dell see more and stop more – constantly acting on an immense set of data and telemetry to continually help enable 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, 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. 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.

Learn more…

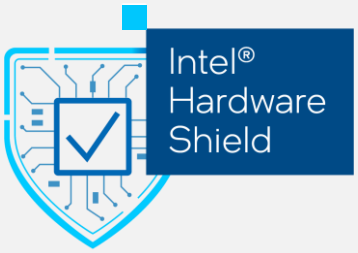
…about Dell Technologies offerings

Dell Technologies Safety and Security webpage
Dell Trusted Devices webpage
Dell Trusted Device Below-the-OS whitepaper
Dell SafeGuard and Response datasheet
Dell SafeBIOS datasheet
Dell Supply Chain Assurance brief

…about Intel offerings

Intel vPro® Platform security manifesto
Intel® Hardware Shield webpage
Intel® Hardware Shield whitepaper
Intel Advanced Threat Protections whitepaper
Intel Virtualization Technologies whitepaper
Intel Below-the-OS Security whitepaper
Intel Transparent Supply Chain webpage
Intel 2021 Product Security Report

Intel® Hardware Shield technologies on Windows-based devices



Below-the-OS Security

Application & Data Protections

Advanced Threat Protections

Below-the-OS Security

Provided by BIOS & boot flow protection technology

- Intel® BIOS Guard
- Intel® Boot Guard
- Intel Firmware Guard Update/Recovery
- Intel® Platform Trust Technology (Intel® PTT)
- Tunable Replica Circuit – Fault Injection Detection
- Intel® Runtime BIOS Resilience
- Intel® System Resources Defense
- Intel® Trusted Execution Technology (Intel® TXT)
- Intel® System Security Report

Application & Data Protections

Achieved through virtualization-based security

- Intel® Virtualization Technology (Intel® VT-x)
- Intel® Virtualization Technology for Directed I/O (Intel® VT-d)
- Intel® Virtualization Technology – Redirect Protections (Intel® VT-rp)
- Mode-Based Execution Control
- Kernel DMA Protection
- Intel® Total Memory Encryption (Intel® TME)
- Intel® Total Memory Encryption – Multi-Key (Intel® TME-MK)
- Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)
- Advanced Programmable Interrupt Controller Virtualization

Advance Threat Protections

Enabled by monitoring CPU behavior & GPU offloading

- Intel® Threat Detection Technology (Intel® TDT)
- Intel® TDT – Accelerated Memory Scanning
- Intel® TDT – Anomalous Behavior Detection
- Intel® TDT – Advanced Platform Telemetry
- Intel® Control-flow Enforcement Technology (Intel® CET)

Dell commercial devices feature end-to-end security, from design to delivery and beyond

Design

Planning, Assessment, and Analysis

Security-Centric Design

Verification and Testing

Release

On the way to you

Secure facilities, vetted staff, and trusted partners undergo frequent audits to help ensure assembled products leave our sites as secure devices

Dell Secured Component Verification or Intel Transparent Supply Chain tools with Intel vPro® platforms offer built-in, hardware-based security verification

Dell devices are delivered through vetted logistics providers and are protected by physical security layers and tamper detection technologies

While in use

Security solutions from Dell and Intel

Dell SafeGuard and Response

Dell SafeData

VMware Workspace ONE®

Above the OS

Below the OS

Dell protections			Intel® Hardware Shield		
Dell SafeBIOS	Dell SafeID	Dell SafeScreen	Advanced Threat Protections	Application and Data Protections	Below-the-OS Security

Ongoing support and threat monitoring from Dell and Intel security teams

Figure 5: Dell and Intel work together to provide secure systems for your business