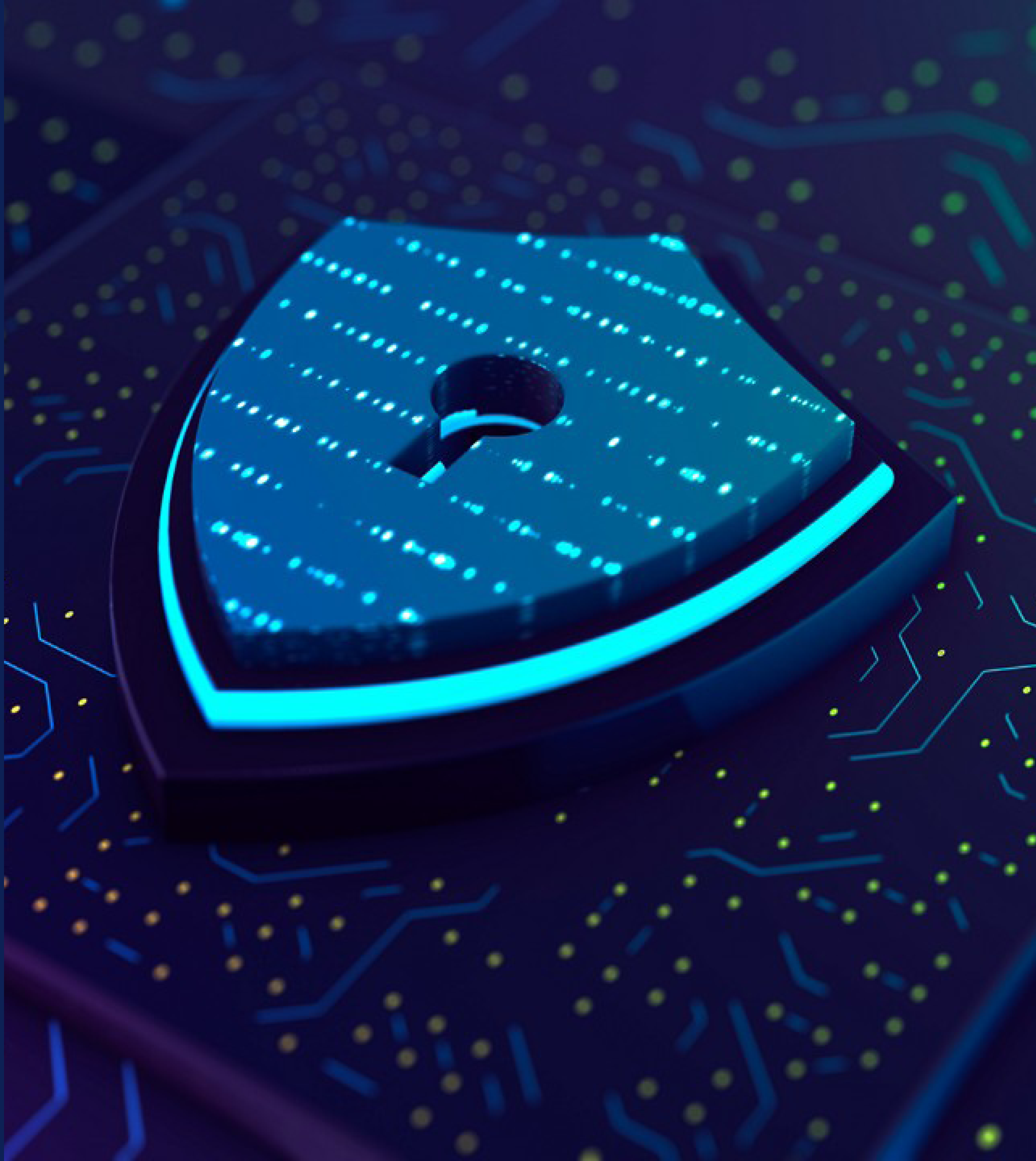
DELL Technologies intel. Accelerate AI with Intel® Windows 11

The anatomy of a trusted workspace

Improve the security of your fleet with multiple layers of defense

Contents



Executive summary

Cyberattacks are inevitable and are growing in volume and sophistication. Endpoint devices, networks and cloud environments have become key targets.

This eBook offers IT and security decision makers guidance on the elements needed for the most effective endpoint defense amidst this evolving threat landscape.

Table of Contents

The threat landscape

The move to hybrid work introduced new complexity and attack vectors—and **endpoints, networks and clouds are expanding attack surfaces.**

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.*

Many organizations have embarked on a journey towards Zero Trust to combat these threats. But to activate Zero Trust principles, you must be able to maintain device trust.

How do you maintain device trust as attacks become more frequent and advanced technology creates new attack vectors?

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

Learn More

Did you know...

71% of attacks in 2022 weren't malware-based, up 9% y/y[1]

Only 41% of organizations surveyed can say, with utmost confidence, that security is embedded into their technology and applications[2]

Exploring Zero Trust to advance your cybersecurity maturity?

See our eBook:
Endpoint security is an essential element of your Zero Trust journey.

1. CrowdStrike Global Threat Report, 2023.
2. Dell Innovation Index, 2023.

Challenges

For effective endpoint security, it’s important to understand your adversary and how they work.

Given the potential payout, **attackers often make several attempts to breach the same organization, leveraging different methods and points of entry to improve their odds.** For example, along the lifecycle of a single device, attackers can attempt to take advantage of vulnerabilities via dozens of vectors.

Legacy defenses aren’t doing enough to keep endpoints secure. As organizations harden one attack surface, threat actors simply move on to softer targets. As the world shifted to hybrid, threat actors identified new endpoint attack vectors which have led to devastating fallouts.

See attack examples to the right

Supply Chain Attack: Targets suppliers to gain access to its systems, data and/or network and, by extension, their customers’.

EXAMPLE: A hardware supply chain attack, initiated by component tampering:

Attackers intercept a PC shipment and change hard drives.

IT deploys the compromised devices across the company.

Attacker installs malware to extract credentials when users log in.

Social Engineering Attack: Tricks end users into providing sensitive information that can be used to gain device and network access.

EXAMPLE: A spoofing attack, initiated by a phishing email:

End user falls for a phishing email and hands over credentials on a spoofed webpage.

Attacker uses the valid credentials to access the network remotely.

Attacker exfiltrates data over a web service, encrypts stolen data and holds it for ransom.

◁ Contents ▷

Securing the modern workspace

When it comes to endpoint protection, you need prevention, detection & response, and recovery & remediation at various states across the entire lifecycle of a device – from the sourcing and manufacture of PCs, to shipping and deployment; in-use through to retirement. Imagine the size of that combined attack surface!

The most effective cybersecurity strategy plans for the worst-case scenario. It assumes a breach is possible and embeds multiple layers of protection to disrupt the attack as quickly and as often as possible. It also includes remediation capabilities to minimize the risk of a repeat occurrence.

PREVENTION
Make yourself a smaller target with defenses designed to block attacks.

DETECTION & RESPONSE
Always assume a breach and stay vigilant.

RECOVERY & REMEDIATION
Mitigate the impact of an attack and get back to business-as-usual.

Did you know:

Only 33%

of organizations are employing a holistic end-to-end security strategy integrating both hardware- and software-based protections.[3]

[3] Dell Innovation Index, 2023.

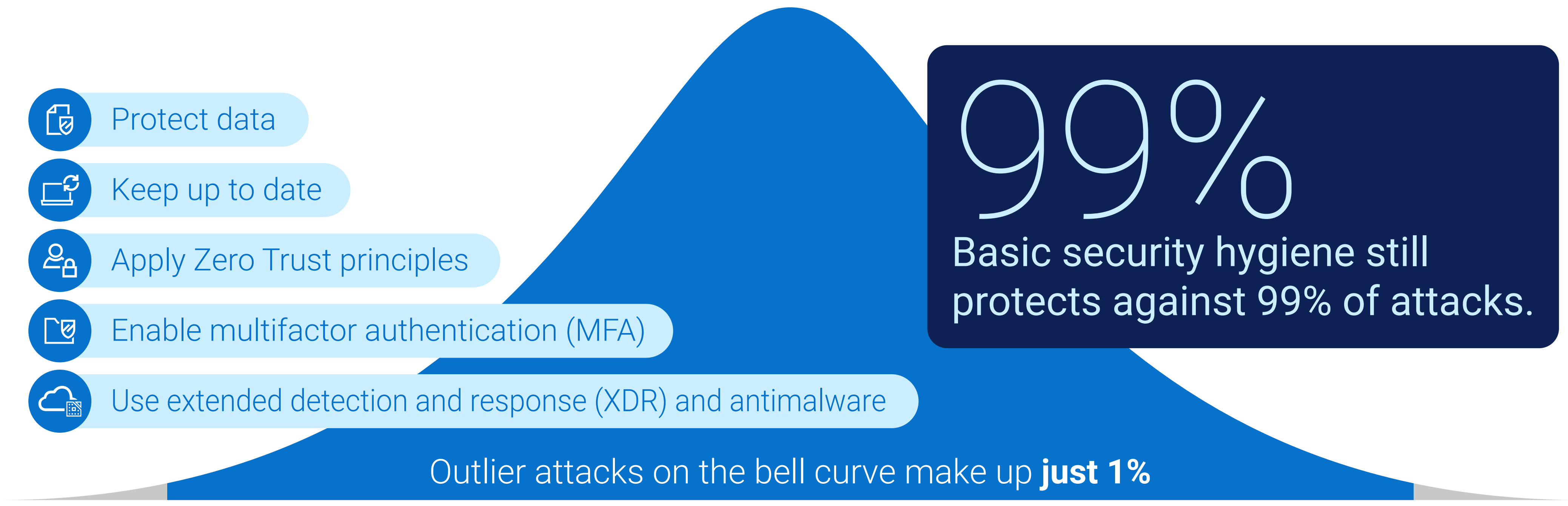
◁ Contents ▷

A complete solution to secure everyday working

With the PC being the new ‘office’ you need a complete solution that keeps things productive, collaborative, secure, reliable and personal. And today’s hybrid workforce needs to adopt a regime of **cyber hygiene**.

Multi-factor authentication (MFA), zero-trust principles, extended detection and response (XDR), and antimalware, patch updates, along with high-value data protection can all secure users against 99% of attacks*.

Fundamentals of cyber hygiene



- Protect data
- Keep up to date
- Apply Zero Trust principles
- Enable multifactor authentication (MFA)
- Use extended detection and response (XDR) and antimalware

Outlier attacks on the bell curve make up **just 1%**

99%

Basic security hygiene still protects against 99% of attacks.

* www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

Looking beyond today’s threats

When designing tomorrow’s systems, Dell and Intel mitigate risks along our supply chains to help ensure devices are secure from the first boot. And for years, Intel has been enabling vendors with base digital supply chain transparency and traceability.

Intel® Transparent Supply Chain (Intel®TSC) delivers Trusted Computing Group TCG platform certificates and component data for supporting Intel-based platforms using a cloud API available to IT through the Intel®TSC web portal.

Combining this with the Dell Secured Component Verification (SCV) solution, provides compatibility and interoperability that improves digital supply chain security assurance for Intel-based devices.

In addition, Dell, Microsoft, and Intel have policies in place around component sourcing assembly, and delivery to minimize the attack surface, protect the integrity of devices, and help ensure commercial devices stay secure.

Hardware-based security from Dell Trusted Device technologies and Intel® Hardware Shield capabilities enhance device defenses through a framework of prevention, detection, and response. And we both have security teams, security to probing products to find new vulnerabilities before attackers do — creating and pushing patches to help keep you and your teams protected.

◁ Contents ▷

A complete solution to secure everyday working

Windows 11 and Microsoft 365 Security: Empowering Secure Everyday Work.

Windows 11, coupled with Microsoft 365 Security, provides a comprehensive solution that ensures robust security for everyday work across all organizational levels. Let's delve into why this security combination stands out.

Elevated Security Baseline:

Windows 11 raises the security bar by incorporating modern CPUs with features like virtualization-based security (VBS), hypervisor-protected code integrity (HVCI), and Secure Boot.

Learn More

Passwordless Authentication:

Windows 11 introduces passwordless authentication, reducing the risk of compromise from password attacks.

Learn More

Multifactor Authentication (MFA):

Windows 11 offers robust MFA features that go beyond passwords.

Learn More

Hybrid Work Readiness:

Windows 11's advanced security features are designed for hybrid work scenarios.

Learn More

Microsoft Defender Antivirus:

Built into Windows 11, Microsoft Defender Antivirus provides ongoing protection.

Learn More

Streamlined Security Features:

Windows 11 simplifies security by enabling features by default.

Learn More

The anatomy of a trusted workspace

Modern endpoint security requires three things:

1 **Software Security:** Today, we find users, devices and data outside corporate networks more than ever before. Software security not only protects devices, but it also extends protection into the network and cloud environments where malicious activity often originates.

2 **Hardware Security:** Devices must include built-in security features. This relates to hardware and firmware security that protects the device in-use. To defend the workspace, you must have functionality built in, that gives you visibility and control over the device.

3 **Supply Chain Security:** Devices must be built securely. This means working with suppliers who a) understand the threat landscape and b) can put that knowledge to use as the landscape evolves. Secure PC design, development, and testing minimizes the risk of product vulnerabilities, while supply chain controls mitigate the risk of product tampering.

A Chief Technology Officer's Vision Board For 2024 And Beyond – Read the Forbes article

Unpacking the Multiple Layers of Security

(Representative examples of security measures listed)

Software Security

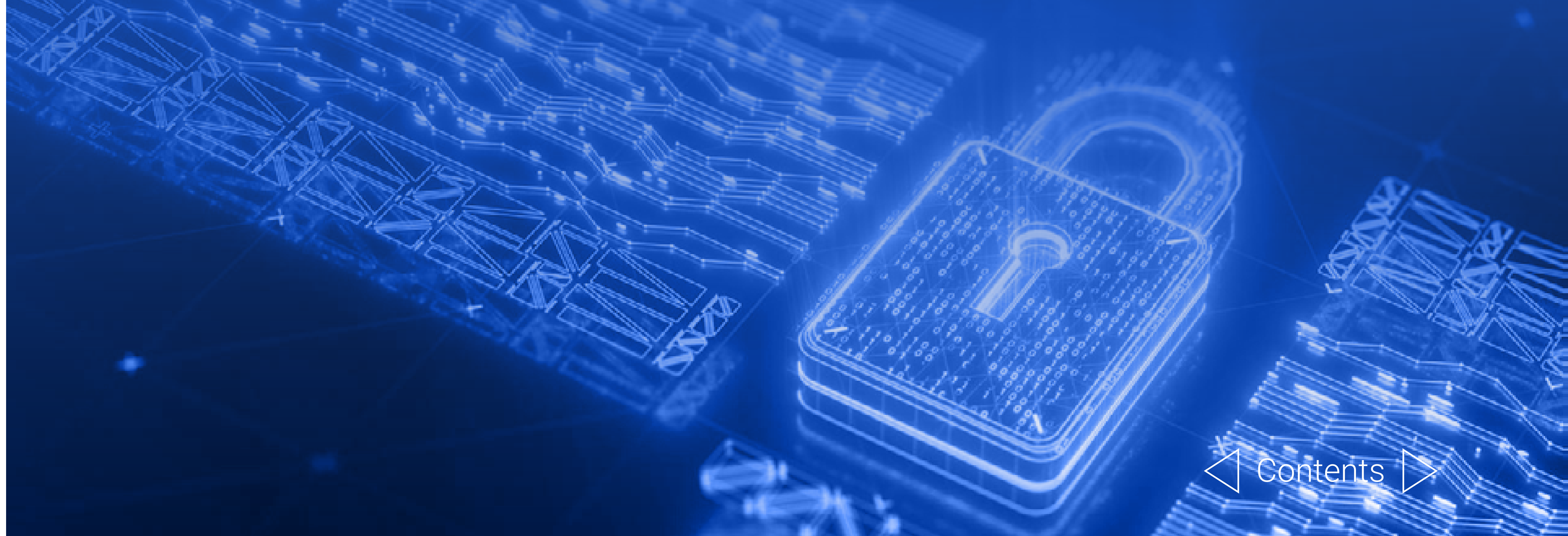
- Next-gen antivirus (NGAV)
- Endpoint detection and response (EDR)
- Extended detection and response (XDR)
- Cloud data protection
- Network protection
- Automated self-healing

Hardware & Firmware Security

- Boot-time verification
- Runtime verification
- User authentication
- Security notifications and alerts/telemetry

Supply Chain Security

- Secure development practices
- Secure supply chain practices
- Component verification
- Tamper-evident packaging



Windows 11 and Microsoft 365 Security

Windows 11 and Microsoft 365 Security create a trusted environment where productivity thrives without compromising safety — from frontline tasks to strategic decision-making.

Copilot in Windows and Copilot for Microsoft 365 play a crucial role in enhancing productivity and security for users.

Microsoft 365 and Windows Copilot's Role at Trusted Workspace PCs
Copilot orchestrates tasks, delivers accurate answers, and enables users to focus on strategic work.

Ensuring Devices Meet Specific Job Requirements
Copilot simplifies device configuration by adjusting settings and installing essential software and assists to meet specific needs, ensuring efficiency and effectiveness.

Easy Management, Upgrades, and Use of Operating Systems
Copilot provides support for managing operating system tasks.

Device Estate Management

Endpoint Security Against Cyber-attacks
Copilot contributes to overall security by adhering to Microsoft 365 and Windows 11 security policies.

Collaborative Apps for Information and Front-line Workers
Windows Copilot and Microsoft 365 Copilot enhance collaboration and productivity for information workers and front-line staff through intelligent assistance and seamless integration across devices.

In summary, Microsoft Copilot contributes to a trusted workspace, streamlining operations, enhancing security, and promoting collaboration across various roles and devices.

Read the Blog

Our approach: Dell Trusted Workspace

Dell is a security and IT partner for organizations worldwide. Unlike point solutions, Dell focuses on overall security outcomes, building a suite of solutions that disrupt kill chains, making you more resilient to cyberattacks.

Dell Trusted Workspace includes:

- Unique **hardware and firmware protections** that make Dell the industry's most secure commercial PCs.[4] *(Built-with and Built-in Security)*
- An ecosystem of **industry-leading software** partners offering advanced threat protection, for the device and into the network and the cloud. *(Built-on Security)*

Built-*on* Software Security from Partner Ecosystem

- **Dell SafeGuard and Response: CrowdStrike, Carbon Black** and **Secureworks** provide threat detection, response and remediation.
- **Dell SafeData: Netskope** offers visibility, monitoring and data loss prevention for cloud-based apps. **Absolute** enables self-healing for apps and networks.

Built-*in* Hardware & Firmware Security via the Industry's Most Secure Commercial PCs[4]

Example features protecting the device in-use:

- **Dell SafeBIOS** off-host BIOS verification* and Indicators of Attack* help catch malicious activity before it compromises the PC.
- **Dell SafeID** secures user credentials in a dedicated security chip.*
- **Off-host firmware verification** protects the integrity of highly-privileged firmware.*
- **With Dell Trusted Device software,** Dell integrates device telemetry with industry-leading software to improve fleet-wide security.*
- **Intel® Hardware Shield** helps to prevent attacks against firmware and protect apps from attacks that run through the BIOS.

Built-*with* Supply Chain Security helps ensure PCs are secure from first boot

- **Dell SafeSupply Chain** add-ons like Dell Secured Component Verification offer extra assurance for product integrity.

* Unique to Dell

[4] Based on Dell internal analysis, September 2023. Applicable to PCs on Intel processors. Not all features available with all PCs. Additional purchase required for some features.

◁ Contents ▷

Put it all together with Dell, Intel and Microsoft

With both hardware and software countermeasures in place, reduce the attack surface with defenses that help prevent common attacks.

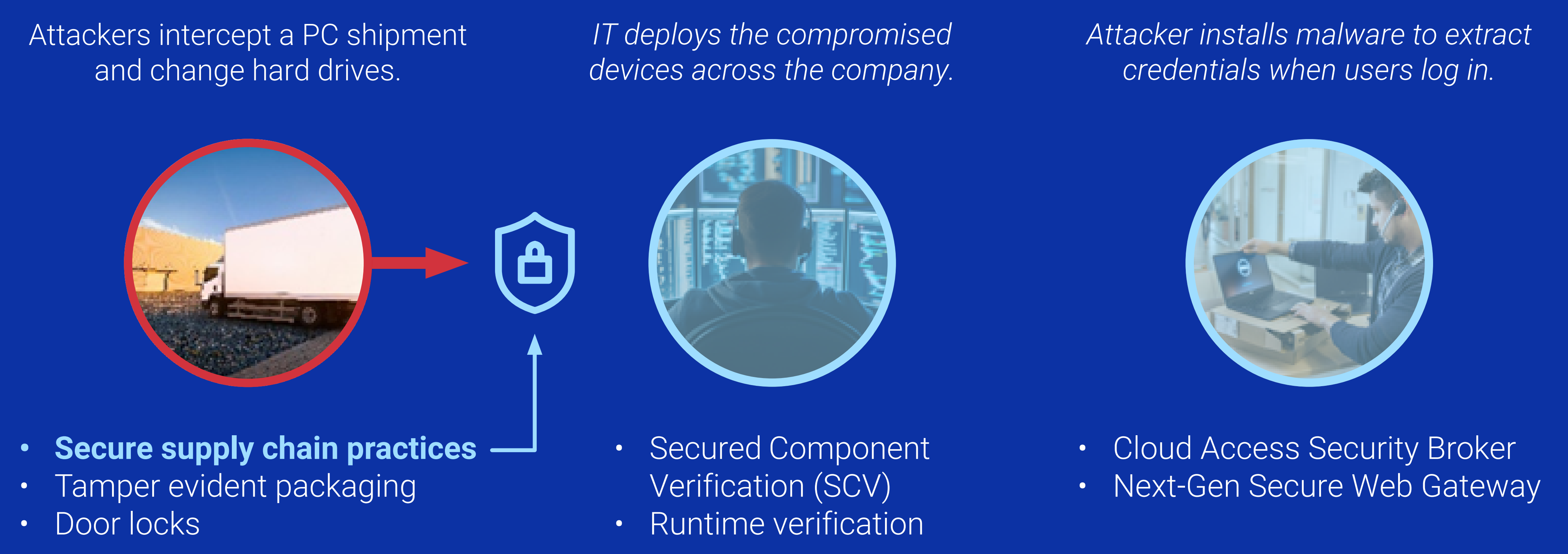
Detection and response capabilities address stealth attacks that may slip through.

In the case of the Supply Chain Attack discussed on page 4, when you work with Dell, preventative measures such as **secure supply chain practices** can disrupt an attack early in the kill chain. If an attack slips through, additional countermeasures – like Secured Component Verification (**SCV)** – are also in place.

In the case of the Social Engineering Attack, even if an attacker successfully tricks a user into handing over valid credentials, **hardware-based user verification like SafeID** can stop the attacker cold in their tracks and deny further access.

Security software like a **Next-Gen Secure Web Gateway** can provide another layer of monitoring protection.

Countering a Hardware Supply Chain Attack
initiated by component tampering.



Attackers intercept a PC shipment and change hard drives.

IT deploys the compromised devices across the company.

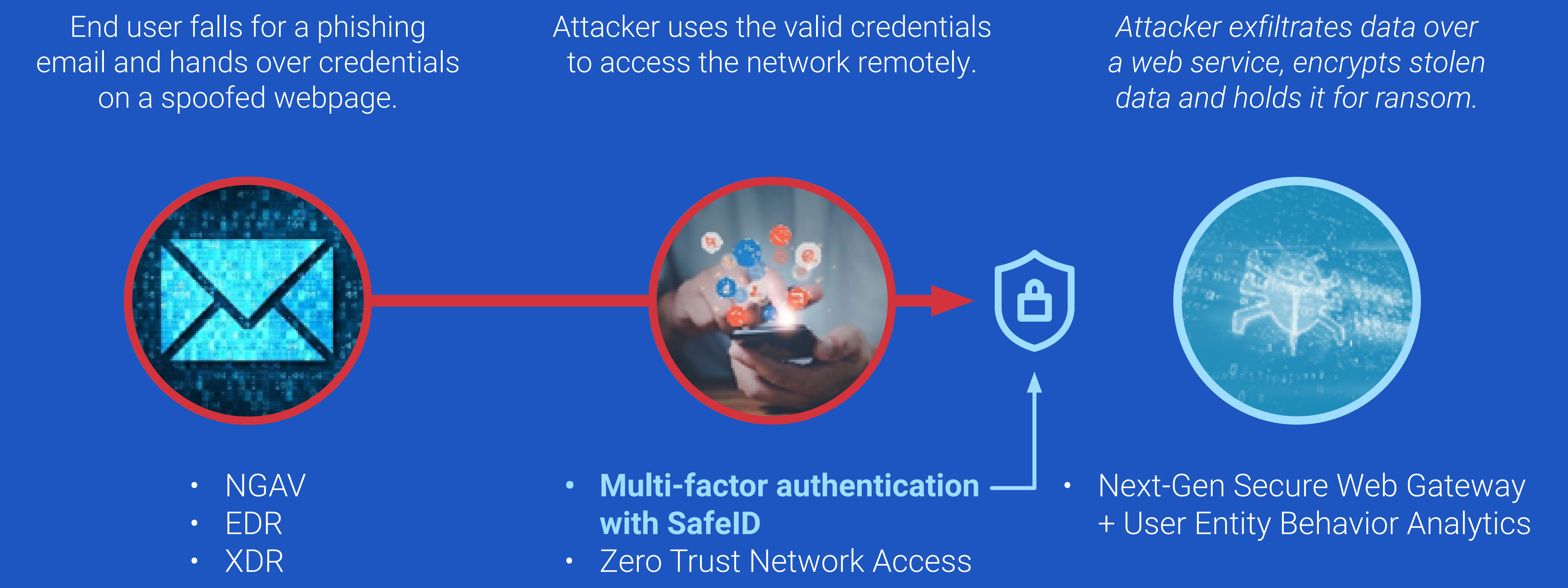
Attacker installs malware to extract credentials when users log in.

- **Secure supply chain practices**
- Tamper evident packaging
- Door locks

- Secured Component Verification (SCV)
- Runtime verification

- Cloud Access Security Broker
- Next-Gen Secure Web Gateway

Countering a Social Engineering Attack
initiated by a phishing email.



End user falls for a phishing email and hands over credentials on a spoofed webpage.

Attacker uses the valid credentials to access the network remotely.

Attacker exfiltrates data over a web service, encrypts stolen data and holds it for ransom.

- NGAV
- EDR
- XDR

- **Multi-factor authentication with SafeID**
- Zero Trust Network Access

- Next-Gen Secure Web Gateway + User Entity Behavior Analytics

◁ Contents ▷

The Zero Trust security model

Windows 11 embraces a concept known as the Zero Trust security model. This idea is built upon three pillars:

1 **No Access Without Proof of Security and Integrity:** Windows 11 operates under the principle that no user or device should have access to anything until their security and integrity are verified. To ensure that a computer has not been tampered with, Windows 11 relies on explicit verification—authentication and authorization—based on all available data points. These include user identity, location, device state, service or workload, data classification, and anomalies.

2 **Least Privileged Access:** Windows 11 promotes the use of the least privileged access. By limiting user access through just-in-time and just-enough-access risk-based adaptive policies, both data and productivity are safeguarded.

3 **Assuming Breach:** In this scenario, it is assumed that a hacker is already within the system. The approach is to operate in a way that minimizes the blast radius and segments access. End-to-end encryption is verified, and analytics are leveraged to gain transparency, advance threat detection, and enhance defense.

This security model ensures robust protection from the ground up, benefiting everyone from frontline workers to senior executives.

Windows 11 Pro:
Empowering Secure Hybrid Work Environments

Windows 11 Pro is purpose-built for hybrid work environments, offering advanced security features and protection against attacks. Dell devices powered by Intel® Core™ Ultra processors, running Windows 11, represent the safest option in the market, featuring integrated hardware-based security. Experience unparalleled productivity and security with Windows 11, equipped with pre-activated security components.

When combined with Microsoft 365, Dell Trusted Devices provide comprehensive enterprise security without the need for local effort. Choose Microsoft 365 for cost savings, robust security, enhanced productivity, and seamless integration. With Dell Technologies, you gain access to a dedicated service team, comprehensive setup and installation support, and 24/7 remote management and assistance.

Learn more about Windows 11 security features

▷ Watch the Widows 11 Security Features Video

◁ Contents ▷

Key takeaways

Breaches are inevitable.
Effective endpoint security always assumes the worst-case scenario and focuses on disrupting kill chains wherever they occur — from device, to network, to cloud.

No one solution blocks 100% of attacks.
Combine hardware and software countermeasures for the best defense.

You're only as secure as your suppliers.
Challenge your suppliers to outline their security measures.

To learn more:

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

Visit us:
Dell.com/Endpoint-Security

Follow us:
LinkedIn @DellTechnologies
X @DellTech

Take the next step

Security is a daunting topic for organizations of all sizes. **Comprehensive hardware and software protections from Intel and Microsoft, and brought together by Dell, work to to create a modernized endpoint security solution.**

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

◁ Contents ▷

DELL Technologies

intel® Accelerate AI with Intel®

Windows 11