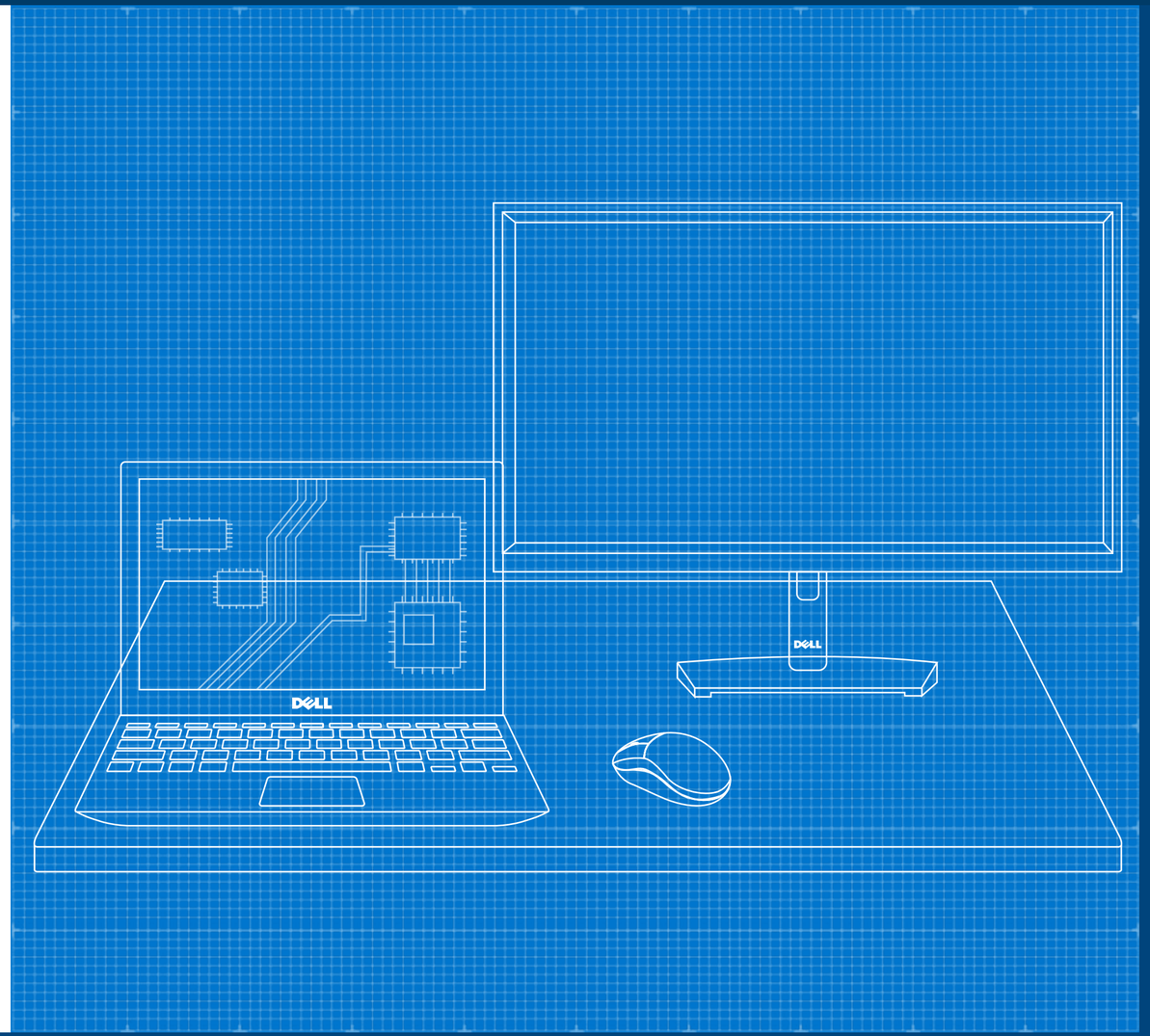
DELL Technologies

The anatomy of a trusted workspace

Improve the security of your fleet with multiple layers of defense



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*.

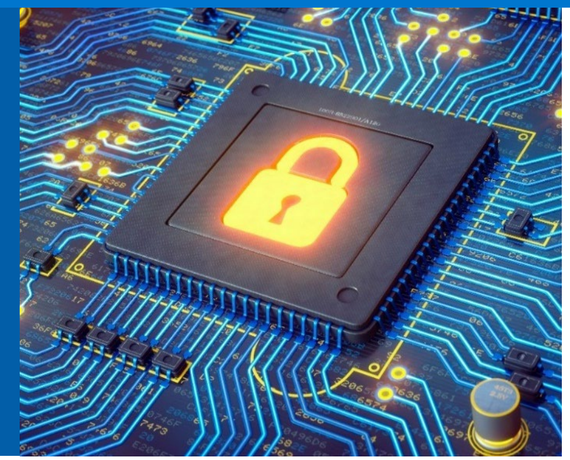
Many organizations have embarked on a journey towards Zero Trust to combat these threats. But to activate Zero Trust principles, you must be able to maintain device trust.

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

[1]CrowdStrike Global Threat Report, 2024.
[2]Dell Innovation Index, 2023.

Did you know…

75% of attacks in 2023 weren't malware-based[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*.

Challenges

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

Given the potential payout of a breach, **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 went 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.

Securing the modern workspace

When it comes to endpoint protection, you require 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, while in-use and through 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 protections to disrupt the attack as quickly and as often as possible. It also includes remediation capabilities to minimize the risk of a repeat occurrence.

[3]Dell Innovation Index, 2023.

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.

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.

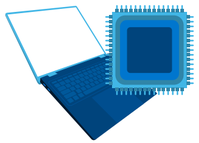
3. **Supply Chain Security:** Devices must be built securely. This means working with suppliers who a) understand the threat landscape and b) can put that knowledge to use as the landscape evolves. Secure PC design, development and testing minimizes the risk of product vulnerabilities, while supply chain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

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

Our approach: Dell Trusted Workspace

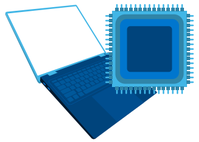
Dell is a security and IT partner for organizations worldwide. Unlike point solutions, Dell focuses on overall security outcomes, building a suite of solutions that disrupt kill chains and make you more resilient to cyberattacks. **Dell Trusted Workspace includes:**

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

[4]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.

Built-*on* Software Security from Partner Ecosystem

- **Dell SafeGuard and Response: CrowdStrike** 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 World's Most Secure Commercial PCs[4]

Example features protecting the device in-use:

- **Dell SafeBIOS** off-host BIOS verification*, Indicators of Attack* and CVE Detection* 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 the **Dell Trusted Device App**, Dell integrates device telemetry with industry-leading software to improve fleet-wide security.*

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

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

* *Unique to Dell*

Put it all together with Dell

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

Detection and response capabilities address stealthy 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 **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 provides another layer of monitoring protection.

Countering a Hardware Supply Chain Attack initiated by component tampering.

Attackers intercept a PC shipment and change hard drives.

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

IT deploys the compromised devices across the company.

- Secured Component Verification (SCV)
- Runtime verification

Attacker installs malware to extract credentials when users log in.

- 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.

- NGAV
- EDR
- XDR

Attacker uses the valid credentials to access the network remotely.

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

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

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

Key takeaways

Breaches are inevitable. Effective endpoint security assumes the worst-case scenario always 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.

Latitude Laptops and 2-in-1 PCs

Take the next step

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

Dell Trusted Workspace helps secure endpoints for a modern, Zero Trust-ready IT environment. Reduce the attack surface 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.