DELL Technologies

End-to-End Security Solutions for Small Businesses

When you're operating a growing business, you deserve straightforward solutions and ongoing support. That's where we come in—to help align your technology needs with your business goals. Let's explore our evolving work environments and how you can secure your business through trusted devices and infrastructure.

The way people work is changing

It should come as no surprise that work is no longer tied to a location. It's about being productive wherever you work, at any time. In the digital age, workers are connected in more ways than ever as they go through daily routines. And since there's so much information being shared across various devices, your employees' data becomes more vulnerable to external threats. Plus, it's being shared with more people in and outside of traditional firewalls.

Today's end-user behavior

Employees will do anything needed to get their jobs done. Sometimes, that means going around security protocols. However, it's not out of ill will; it's solely to remain productive. Let's examine how employees are sharing information.

Here's what we know:

72%

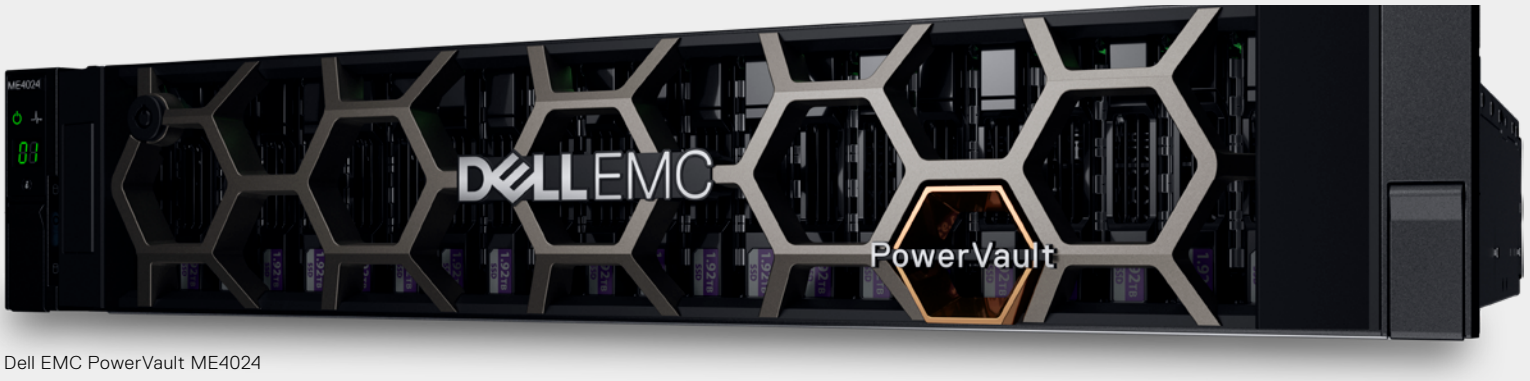
of employees are willing to share confidential data externally.[1]

50%

of employees use personal cloud apps and email to share confidential data.[2]

41%

will work around security safeguards to get work done.[3]



Dell EMC PowerVault ME4024

What does this mean for your business?

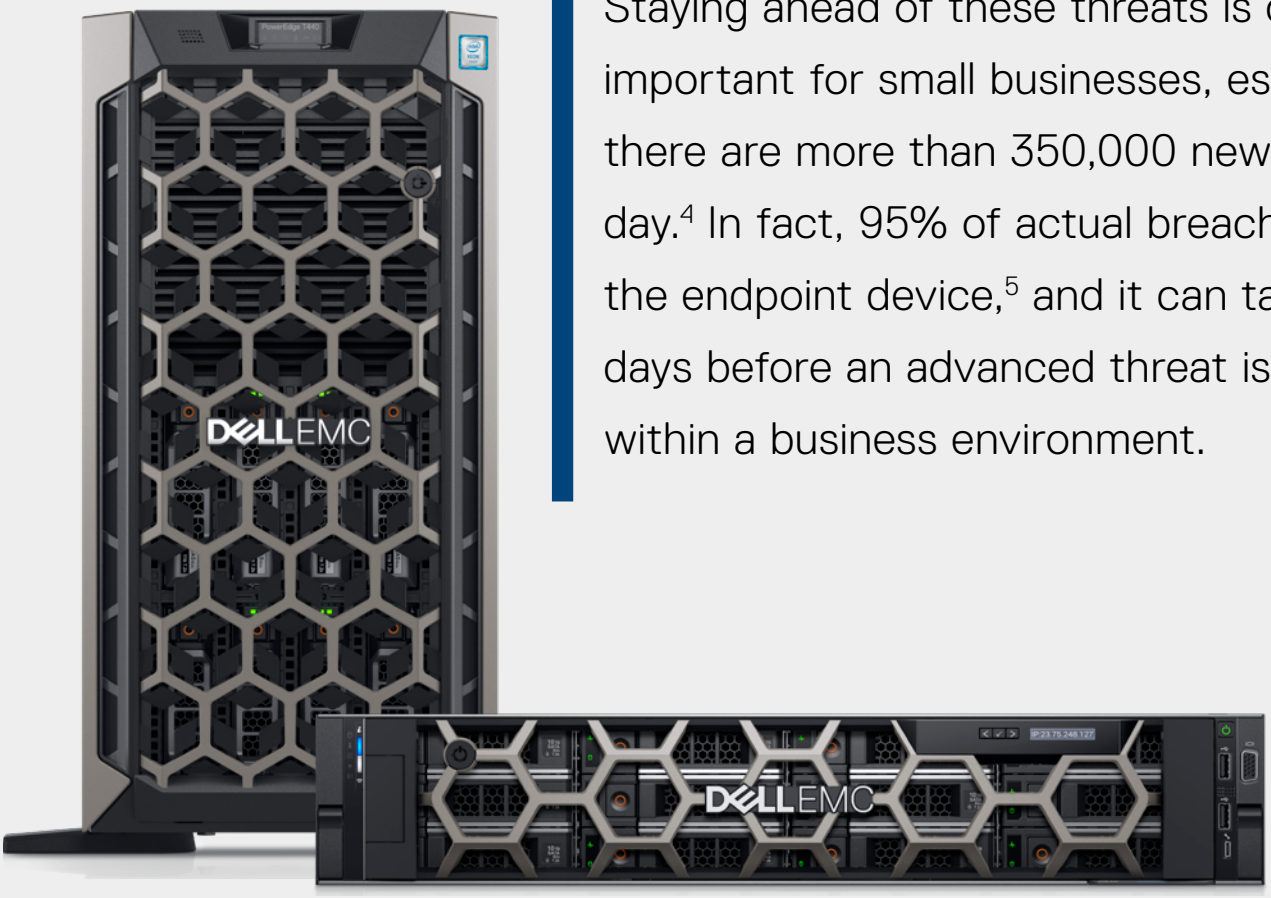
External threats are sophisticated and increasing

No matter the size of your business, it faces threats to its assets, corporate data and customer information. These data threats and attacks are becoming increasingly sophisticated, frequent and widespread.

Some examples of these threats include:

- **Physical theft and loss** – an attack due to human error or the malicious intent of a hardware thief.
- **Denial-of-Service** – a cyberattack in which a legitimate user cannot access information systems, devices or other network resources.
- **Phishing** – a fraudulent attempt by a cybercriminal to obtain sensitive information.
- **Pharming** – an attack that redirects unaware users to a phony website.
- **Ransomware** – a form of malicious software that threatens to block access to a victim's system or data until they pay a ransom.
- **Malware** – software that is purposely created to harm a computer, network or server.

Staying ahead of these threats is critically important for small businesses, especially when there are more than 350,000 new threats every day.[4] In fact, 95% of actual breaches begin at the endpoint device,[5] and it can take up to 108 days before an advanced threat is noticed[6] within a business environment.



PowerEdge T440 Tower Server and PowerEdge R540 Rack Server

Protect, control and monitor

Our Dell Technologies Advisors can help your business navigate our broad selection of technologies and provide ongoing support to help protect your entire ecosystem.

We understand that small businesses need to be able to authenticate users, control access to data and monitor that data use in real time. That's why we offer tailored security solutions that protect your data and prevent threats to keep your business moving forward.

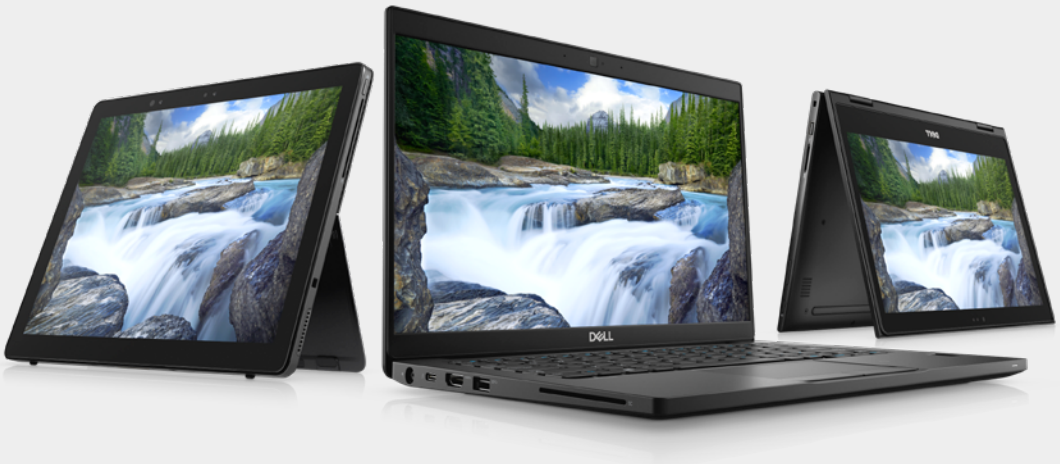
Below are some ways we keep your business secure.

- **Devices designed for secure access**

  Our laptops, servers, storage solutions and appliances are all designed from the ground up with security in mind. Dell builds security in from the very moment a product is conceived all the way through the design and manufacturing process. It's foundational. And data security is crucial to your success.

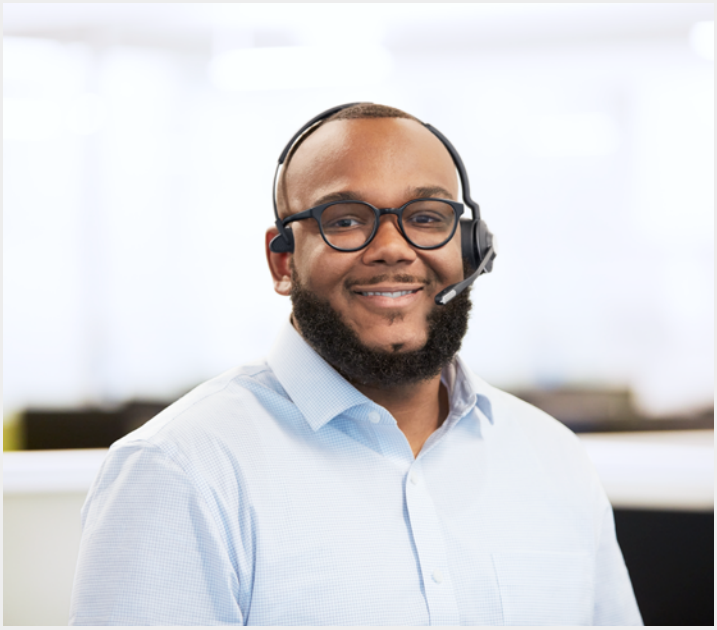
- **Security solutions starting at the endpoint**

  Many Dell devices come with SafeID, a robust safety feature that helps ensure only authorized users can access your devices—and ultimately the rest of your connected data. With SafeID, authentication integrity is gained by securely storing and processing credentials in a dedicated security chip, keeping it protected from outside software attacks. Chip-level authentication works with fingerprint readers, smart cards and Intel Authenticate [7] to safeguard the sign-on process. When used in conjunction with optional identity-secured login features like facial recognition and third-party software, your team gets to enjoy faster system wake-up and desktop environment sign-on functions, boosting productivity and security simultaneously.



- **The award-winning Dell Latitude family**

  The way we work is evolving fast; as more and more people turn to remote work, technology that successfully allows for more flexibility and security will prevail. The Dell Latitude family of PCs and laptops is here to provide your business the most secure, thinnest and lightest business laptops and 2-in-1s.[8] With a wide variety of biometric readers and encrypted hard drives, these devices offer industry-leading encryption and authentication, including an optional fingerprint reader and cutting-edge malware prevention—right out of the box.



A Dell Technologies Advisor can guide you to a scalable server storage solution that perfectly fits your small business—from your first server to public, private and hybrid cloud environments.

- **Security solutions for storage and servers**

  But understanding the products and systems that businesses need to remain secure wouldn't be complete without discussing the IT foundation—the datacenter. Securing the IT ecosystem means building infrastructure that's resilient from the ground up, surrounding data with security no matter where it goes, and giving you greater control over the entire connected ecosystem to protect IT, business, and end-user assets.

- **Dell EMC PowerEdge rack and tower servers**

  Dell EMC PowerEdge rack and tower servers are equipped with end-to-end security, starting at the firmware and hardware levels to provide the best protection. PowerEdge Tower servers can protect the server configuration and firmware from inadvertent or malicious changes via the integrated system lockdown mode. Configuration details, BIOS and firmware are all protected, so if there is an attack, the server can be restarted from a previously saved configuration.

  Built on a comprehensive, cyber-resilient architecture with integrated security features, the PowerEdge T440 server is designed to protect against physical intrusion, malware injection, tampering during transit, malicious firmware updates, rogue configurations, open port attacks, data breaches and more.

- **Storage designed around security and data protection**

  If you're looking for professional-grade storage with self-encrypting drives in a simple, fast, and affordable solution, the Dell EMC PowerVault ME4 is an all-inclusive design providing all the software to store, manage and protect data in every way possible. It offers professional-grade storage with self-encrypting drives in a simple, fast, and affordable solution for small businesses. The ME4 also comes equipped with snapshots and replication capability to reliably deliver data protection to keep your business's and customers' digital assets safe.

When it comes to protecting your network's data while boosting productivity, finding the right storage solution is essential. For personalized support and guidance about end-to-end security solutions that will help you keep your business secure, contact a Dell Technologies Advisor today at 877-BUY-DELL.

SPEAK WITH AN ADVISOR TODAY

877-BUY-DELL CLICK | CALL | CHAT

[1]Dell End-User Security Survey, 2017. [2]Dell End-User Security Survey, 2017. [3]Forrester TAP report, Evolving Security to Accommodate the Modern Worker, October 2017 [4]Source: DeepOrigin: End-to-End Deep Learning for Detection of New Malware Families", September 2018. AV-TEST.org. March 2019.[5]Source: Verizon Data Breach Digest, 2017, [6]Verizon Data Breach Digest, 2017. [7]Intel Authenticate available on Dell devices with Intel® Core™ vPro™ processors. Depends on system configuration and may require enabled hardware, software or service activation. See device configuration. [8]Source: Based on Dell internal analysis, 2019.