DELLTechnologies

Data Protection
for Your Small Business

Let's face it—the combination of evolving security threats, constrained security talent and end-user collaborative behavior means that data protection must change, too. Modern security solutions are vital for preventing these threats and protecting your sensitive information. Learn how you can partner with Dell to keep your business safe.

Your trusted security partner

Data protection is an essential part of any business strategy. At Dell, we're committed to equipping businesses with ultra-secure solutions that protect hardware and data. As a trusted security partner, we'll guide you through your security options and help you choose the right solution for your needs.

Evolving to stop data threats

Compared to those of past generations, today's small business employees are performing their responsibilities much differently. With the help of technology, professionals are enjoying more flexibility than ever before. Modern work culture encourages employees to be productive from anywhere. And most importantly, business IT administrators have recognized that there is not a one-size-fits-all device for the varying types of end users.

Key issues businesses face:

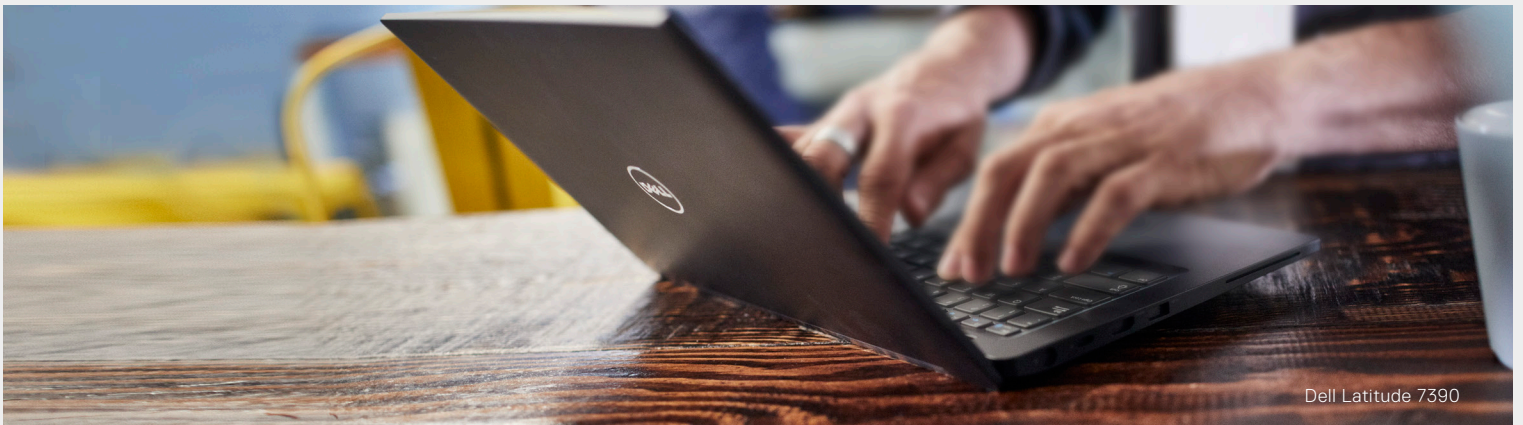**1** **External threats**

2 **User behavior**

3 **Limited security resources**

Complex threats are growing

Every day, an estimated 250,000 variants of cyber threats are produced.[1] Additionally, malware and other malicious software have become more resistant to legacy security protocols. Once an endpoint or user device is infected, the threat can lurk in an environment for an average of 108 days[2] before it's detected—an especially alarming thought since 95% of all breaches occur at the endpoint.[3]

Scope Breakdown

36% MARKETING

34% DEVELOPMENT

30% FINANCE
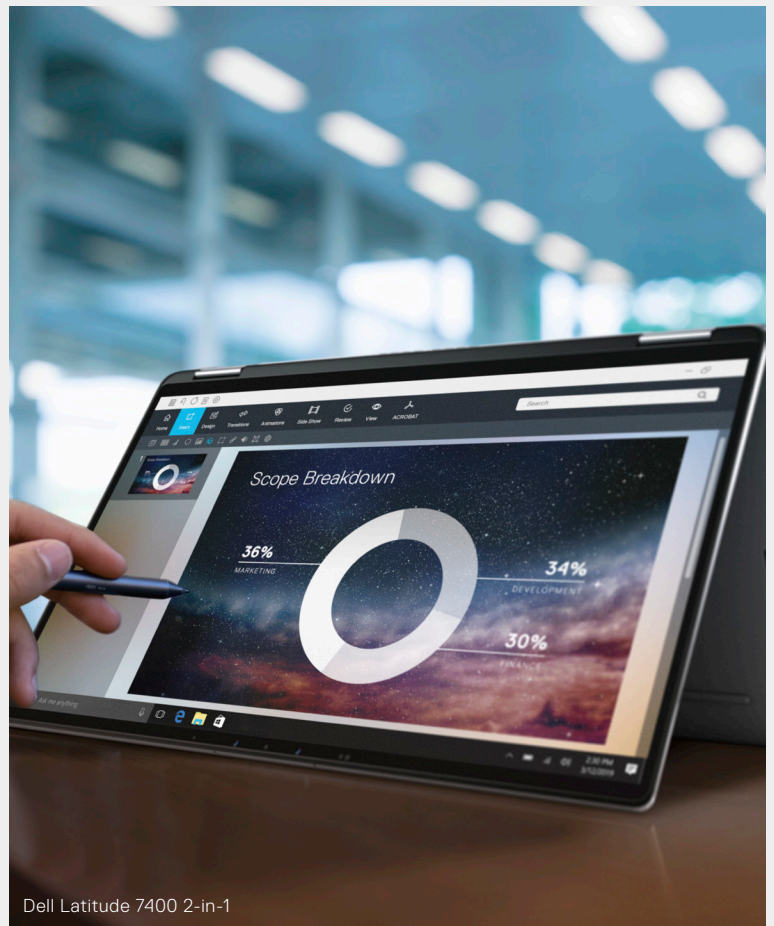
Dell Latitude 7400 2-in-1

Dell Latitude 7390

End users bypass security for productivity

The rise of remote work and collaboration across various devices makes organizations increasingly vulnerable to external threats. Many workers share information without considering potential breach points, such as utilizing an insecure, public network in an airport or café. About 72% of professionals share data externally, with 50% using personal cloud apps to share that sensitive data.[4] If protocols impede their productivity, 41% of these users will bypass proper security measures.[5] Between user behavior and threats morphing at such a startling rate, it's difficult for technology to keep up. Though we have advanced threat solutions that can prevent many viruses or malware breaches, the next level of protection requires human interaction.

Security experts are in high demand

The truth is, organizations are having a difficult time staffing and retaining key security personnel. Over the next five years, the number of unfilled cybersecurity positions will rise to 3.5 million and will continue to grow to 6 million. [6] The good news is, there's hope when it comes to keeping your organization free from cyberattacks. As these threats adapt and evolve, so do the hardware, software and other defenses we use to stop them.

Essential data protection solutions

Trusted Devices

Serving as a foundation for data security, Trusted Devices have protection built into the device itself, such as our XPS, Latitude and Vostro PCs. We unite the built-in security of our devices with unique value-add security software and services. As a result, we're able to protect critical items, such as the end user's login credentials with features like SafeID.

SafeID: Protecting advanced authentication credentials

SafeID makes it possible to store and process end-user credentials in a dedicated security chip, for better credential protection. The Dell-exclusive security chip isolates and processes advanced authentication information for the protection of multi-factor authentication. Because the credential authentication happens in the hardware layer, below the operating system, it's much harder for attacks to compromise end-user credentials and to access company data.

Enhanced security with a Trusted Platform Module

Also built into Dell PCs is a Trusted Platform Module (TPM). A TPM is a specialized security chip in Dell commercial PCs that stores platform certificates or encryption keys for platform

SafeGuard's Incident Response

Data protection has been a tricky hurdle to attempt. Unfortunately, breaches can remain undetected for an average of 108 days,[7] causing large amounts of ecosystem damage in that time. No matter the security measures you take, a security incident can happen despite your best efforts. When it happens, your business can come to a halt, and your brand reputation can be damaged. About 80% of IT business leaders anticipate a critical breach or successful cyberattack over the coming year,[8] and many of these businesses do not have security talent on staff with the right skills and experience to adequately prepare and respond to an active breach. Every second counts when these breaches occur. SafeGuard's Incident Response is a 40-hour retainer for on-demand assistance from the incident response team to take action against and mitigate cyber incidents before, during and after a breach. Using proprietary technology, the incident response team identifies the presence of compromises and entrenched threat actors operating in your network. From there, they conduct a detailed assessment of your existing incident response documentation, personnel and procedures to educate your team on how to avoid future breaches. Through SafeGuard, your organization can prepare itself to withstand security threats that attack the endpoint, freeing up time so you can focus on your business.

Dell is your trusted security partner

At Dell, we pride ourselves on delivering a portfolio that improves your existing security practices. With our built-in security, user credentials for advanced authentication are confined in silicon-based protection via SafeID, allowing your organization to experience control over sensitive information and data.

Through our comprehensive security portfolio, we'll guide your business to a data protection solution that keeps you safe from modern threats. Get started today by calling a Dell Technologies Advisor at 1-877-BUY-DELL.

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] AVTest 2018, www.av-test.org/en/statistics/malware/ [2] The 2018 U.S. State of Cybercrime Survey, in partnership with CSO, U.S. Secret Service, CERT Division of Software Engineering Institute at Carnegie Mellon Universaity, and KnowBe4 [3] 95% of all breaches occur at the endpoint. Source: Verizon Data Breach Digest, 2017 [4] Dell End-User Security Survey, 2017 [5] Forrester TAP report, Evolving Security to Accommodate the Modern Worker, October 2017 [6] Cybersecurity Jobs Report 2018-2021, Herjavec Group May 2017, https://www.herjavecgroup.com/wp-content/uploads/2018/07/HG-and-CV-The-Cybersecurity-Jobs-Report-2017.pdf [7] The 2018 U.S. State of Cybercrime Survey, in partnership with CSO, U.S. Secret Service, CERT Division of Software Engineering Institute at Carnegie Mellon University, and KnowBe4 [8] Trend Micro Cyber Risk Index, https://www.trendmicro.com/en_us/security-intelligence/breaking-news/cyber-risk-index.html