Security for the future-ready workforce

Empower your employees to be productive and keep your business secure in a rapidly evolving workplace

Today, technology is all about enabling business. Organizations of many types and sizes are developing, upgrading or replacing mobile applications to reflect changes in the workplace. Across industries, employees are working more while mobile, using multiple devices. When they return to the office, they are capitalizing on more flexible work environments and approaches to work.

Many organizations are facilitating this anytime, anywhere work with mobility initiatives that provide mobile devices or allow employees to use their own. They are also modifying workspace designs, creating mobile workstations and mobile "hot spots" to enable workers to easily connect to enterprise systems when they return to the office.

Enabling employees to work better can help organizations boost productivity and improve customer service. The real challenge is to continue supporting new ways of working, now and in the future, without compromising security.

The need to secure employee systems is underlined by the growing number and severity of threats, including advanced

The worker perspective

From the point of view of workers, the future of technology in the workplace is bright:

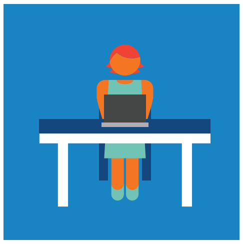
- A 2015 study conducted by Dell found employees feel technology has increased their productivity and enabled them to communicate faster with co-workers, but advancements in technology won't replace the need for people in the workplace.[2]
- Workers are optimistic about the future of technology, believing it will change how people collaborate with their technology and each other.
- As a consequence, they are putting greater pressure on employers to supply the latest technologies.

persistent threats (APTs), zero-day attacks, data breaches and sophisticated, constantly evolving malware. If a malicious attack succeeds, it can be extremely costly for an organization: The average cost of a data breach, for example, is USD 3.8 million.[1]

Facing activity-based security challenges

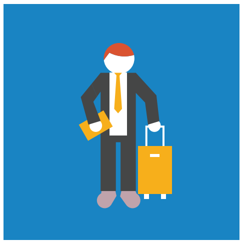
To both empower the workforce and protect the enterprise, organizations must choose the right technologies and match users to the right devices. The key is focusing on how people work. Employee roles and responsibilities should guide technology choices, and those choices should help each worker become more productive, efficient and satisfied while ensuring security.

From an activity-based standpoint, today's employees can be divided into five worker types:

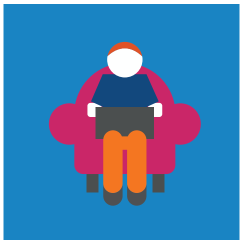


Desk-centric employees work at their own desk in the office more than 50 percent of the time.

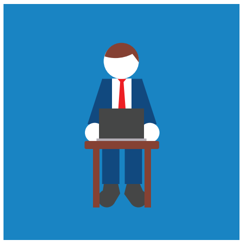
Corridor warriors work from meeting rooms and multiple locations within the company more than 50 percent of the time.



On-the-go professionals work away from the office more than 50 percent of the time because they are traveling or at off-site meetings.



Remote employees work full time — at least 30 hours per week — outside the company buildings, from home or another location.



Specialized users include two groups: those using mobile workstations for advanced graphics and business applications, and people using rugged laptops and notebooks in the field.

Each of these categories comes with its own particular set of security challenges based on the associated worker activities. These challenges are compounded by the number of devices used per employee — workers want to use the right tool for each function whether it's a laptop, tablet or smartphone, and all must be protected.

Desk-centric workers range from accountants to customer support and inside sales representatives. They spend most of their time in their designated workspace, but to stay productive throughout the day, they use the internet, email, productivity applications and online meetings. Attackers might take advantage of these day-to-day activities to try and steal organizations' most valuable data assets. Whenever employees use the internet or open an email attachment, they risk becoming the unwitting accomplices to a data breach. Desk-centric workers need a proactive approach to guarding against untrusted content and defeating malware and APTs in real time — 24x7, 365 days a year.

Corridor warriors are often executives such as marketing, program or warehouse managers who have to move from desk to meeting and beyond on a regular basis. These individuals stay up and running throughout the workday with laptops and other portable devices, often presenting or sharing in meetings and taking advantage of connectivity on the go. They frequently access corporate applications and data, including cloud resources, and organizations need to securely manage this access. Corridor warriors also need the same anti-malware prevention as desk-centric workers.

On-the-go professionals such as consultants, outside sales representatives and service professionals require access to people and data from anywhere, whether in the boardroom or an airport lounge. They rely on devices designed for highly mobile users to support fast sharing and collaboration and to consume and produce content. The need to use public WiFi increases the security threat for many on-the-go individuals. In addition to secure cloud access and malware prevention, these workers require data-centric encryption to protect devices and external media such as USB drives.

Remote workers must turn home environments and even coffee shops into hubs of productivity. They communicate with the core office by phone, instant messaging and video conference. Many access information and corporate tools through the cloud and virtual private networks (VPNs). Remote workers need secure access to corporate resources and data-centric encryption to protect corporate data on their devices. They should also be equipped with security tools that integrate a password manager with hardware-based multi-factor authentication.

Specialized users of mobile workstations include professionals in computer-aided design (CAD), architecture, computer graphics, economics, healthcare and scientific research. Specialized users of rugged laptops and notebooks include those in military and first responder roles, and also in manufacturing, warehousing, the oil and gas industry, and field services.

Addressing activity-based needs with Dell solutions

Dell Data Security Solutions offer comprehensive capabilities that cover the needs of the five future-ready worker categories. The solutions also cover the three essentials for safeguarding data while enabling productivity: authentication, encryption and threat protection. Authentication helps ensure only authorized users have access to data, encryption safeguards the data wherever it goes and threat protection defends users and data from untrusted content.

Desk-centric worker

Dell Data Protection | Endpoint Security Suite Enterprise edition integrates best-of-breed advanced threat prevention, encryption and authentication into an enterprise-class security suite. It requires a fraction of the IT resources that would traditionally be required to maintain individual solutions and includes remote management of all components using a single console with comprehensive compliance reporting.

The suite includes revolutionary advanced threat prevention that stops 99 percent of malware before it can even run — including zero-day threats, advanced persistent threats and commodity malware. This focus on prevention is far superior to the 50 percent efficacy of traditional anti-virus/anti-malware solutions.[3] Workers benefit from all three major endpoint security concerns being addressed: authentication management, advanced malware prevention and encryption tools. Whether all-Dell or mixed-vendor (even Macs), environments are easily protected and easily managed.

Corridor warrior

Corridor warriors will also benefit from Endpoint Security Suite Enterprise protection, especially the included mobile security components to protect data on smartphones and tablets. From a single console, IT administrators can apply security policy to a user's laptop, smartphone and tablet.

On-the-go professional

These professionals benefit from Dell Data Protection | Encryption and Dell Data Protection | Cloud Edition to safeguard data wherever it resides — on devices, external media and in public clouds — with the ability for security administrators to set granular data-centric policies. This approach protects the data itself, allowing it to safely move with the user while IT retains the keys at all times. Additionally, advanced multi-factor authentication capabilities in Dell Data Protection | Security Tools provide secure access control using optional smart card and fingerprint readers with Federal Information Processing Standards (FIPS)-201 certification and an optional contactless smart card reader. Security Tools also supports self-service Windows password reset through smartphone apps. The Security Tools solution is included with all Dell Precision, Latitude and OptiPlex systems.

Remote worker

Wherever they work, in coffee shops, conferences or airports, remote workers need protection from malicious attacks to safeguard data. That is where Dell Data Protection | Protected Workspace can help. It provides malware prevention software that places many internet-connected applications such as Microsoft Office, Adobe, Java and web browsers in a secure container, or virtual bubble. The container watches for malicious software and detects it proactively based on the software's behavior — unlike traditional anti-virus software that only detects reactively. The Protected Workspace container is immediately reset when malware is detected, preventing the malware from reaching the host operating system or memory.

Specialized user

For users of rugged devices in police departments, government agencies or harsh environments, advanced authentication capabilities in Dell Data Protection | Security Tools can be extremely useful. Security Tools enables the local management of authentication options. It also unlocks Microsoft Windows using one or more of the following options: password, fingerprint reader, smart card (including contactless card), reader, smartphone or pre-boot authentication. Security Tools also manages self-encrypting drives.
Dell also provides the strongest authentication capabilities to store, transport and process credentials with Dell ControlVault. Other methods are the equivalent of locking a door but putting the key under the mat — hackers have ways to quickly search hiding places and locate the key. ControlVault isolates secure operations from vulnerable operating systems and hard drives. All processing and storage of critical data takes place on a separate chip, providing a protective and more secure boundary. ControlVault is a dedicated security processor with secure storage that provides hardware isolation for authentication. This reduces the risk of malware stealing critical login information associated with fingerprint readers and smart card readers.

These solutions are complemented by the broad portfolio of Dell security solutions, providing a comprehensive approach to security that helps organizations:

- Proactively protect the whole enterprise — outside-in and inside-out — with connected security
- Achieve consistent, reliable governance and comply with government and industry regulations
- Embrace new ways of working and facilitate implementation of up-to-date technology

Adapting to a changing world

The business world is changing quickly due to the rapid pace of technology innovation, and expectations about how the workforce delivers products and services are changing with it. Dell readies the workforce for the future by supporting employees' needs today and empowering them for tomorrow, while ensuring all the security requirements of the organization are met.

Whether in the office or on the road, Dell helps companies and workers confidently embrace advances — such as bring-your-own-device (BYOD) and the cloud — by ensuring the secure use of mobile technologies and providing the right access to the right resources regardless of the device.

Learn More

To learn more about Dell security for the future-ready workforce, visit: Dell.com/DataSecurity

[1] Ponemon Institute, "Cost of Data Breach Study: Global Analysis," 2015.
[2] Dell Global Evolving Workforce Study, Expert Insights, 2015.
[3] Results from Cylance Unbelievable Demo Tour, Austin, Houston and Dallas Texas, May 2015.

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND