DELL EMC

Securing User Devices and Data in the Age of Digital Business

Midmarket businesses must implement security methods to fit new workstyles

Introduction

In the digital business era, a highly productive workforce is essential. Today, knowledge workers at midmarket businesses are mobile and often work from remote locations. To achieve the level of productivity they and their companies demand, those knowledge workers want and expect to collaborate with co-workers and interact with customers and partners wherever they might be in the world, securely, at any time of day or night.

Before the digital age, employees spent their days in an office building and the security perimeter was the building itself. But with a workforce that is often mobile or remote, traditional ideas for perimeter defense are no longer relevant. Technology decision makers face a formidable challenge: Security must be implemented for each user and each device across the enterprise, not just on a local-area network within the walls of a single building.

To shed light on the security issues facing technology decision makers at midmarket businesses, Dell EMC commissioned a study that is the subject of this report. This report takes you through the survey results and assesses their meaning.

With a workforce that is often mobile or remote, traditional ideas for perimeter defense are no longer relevant.

Types of workers

To get an accurate picture of knowledge workers' data security needs, technology decision makers at midmarket businesses will benefit from analyzing their workforces in terms of four fundamental types of users. The types are flexible and overlap to a degree, and many companies have unique types that are hybrids of these four. The survey found workers fall into these types:

1. Desk-centric workers (70%) are primarily office-based at a desk.
2. Corridor warriors (12%) are primarily office-based but mobile within the office or factory floor.
3. Remote workers (8%) are not office-based but still primarily at a desk.
4. On-the-go pros (10%) are primarily mobile.

Security threats and regulatory demands

Today's workstyles increase the challenge that organizations face in keeping data secure. Threats continue to expand in number, sophistication and severity. Attacks come not only from isolated hackers, but also from nation-states bent on industrial espionage or cyber sabotage. Criminal organizations, meanwhile, seek to hold data hostage in exchange for ransom, and seek to steal personally identifiable information for the purpose of identity theft.

Phishing and spear-phishing are popular vectors for advanced persistent attacks, which might remain active within an environment for many months. Attacks that target the BIOS of computers can be particularly dangerous, as they will remain active even after a computer is wiped clean and the operating system is reinstalled.

Insider attacks, in which current or former employees siphon off data, must also be guarded against. The mobile workstyle means laptops, 2-in-1 devices, USB drives and smartphones are all highly vulnerable to theft.

If all that weren't enough, regulatory mandates place a strong emphasis on the protection of personal data. For example, the General Data Protection Regulation (GDPR) of the European Union went into full effect in May 2018, with severe penalties for noncompliance. GDPR has global implications. Any midmarket company doing business in EU countries or having EU citizens as customers must comply or face penalties.

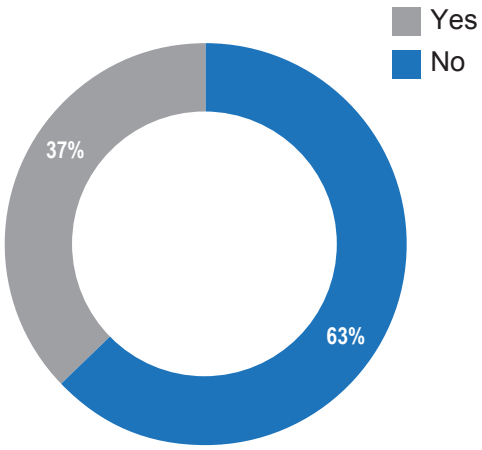
In addition to GDPR, industry-specific regulations remain in force. For example, midmarket organizations in the medical industry must comply with the data protection provisions of the Health Insurance Portability and Accountability Act (HIPAA), and companies in the financial services and retail sectors must comply with the Payment Card Industry Data Security Standard (PCI-DSS) guidelines for protecting payment card data.

Security and productivity

Most technology decision makers are well aware of security threats and have implemented data protection measures at their organizations to some degree. Even so, employees at midmarket organizations often circumvent corporate security protocols. The survey found that 37% of respondents sometimes work outside organizational security [see chart below]. That number might be on the low side, however, since survey respondents self-report and they might be inclined not to admit such activity.

37% of workers admit to sometimes working outside corporate security protocols.

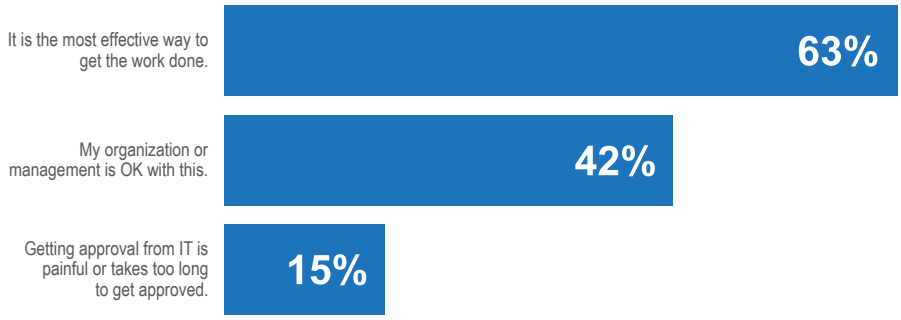
Do you sometimes work outside your organization's security protocol?



Why do employees do this? 63% say it is the most effective way to get work done. In one scenario, a project manager might find him or herself at home after a business trip and in need of checking data within a corporate application. If corporate security protocols are too cumbersome, that manager is likely to avoid them and access the data and application on a home system instead.

Interestingly, the survey found that 42% of workers say their organization or management is OK with this behavior [see chart below].

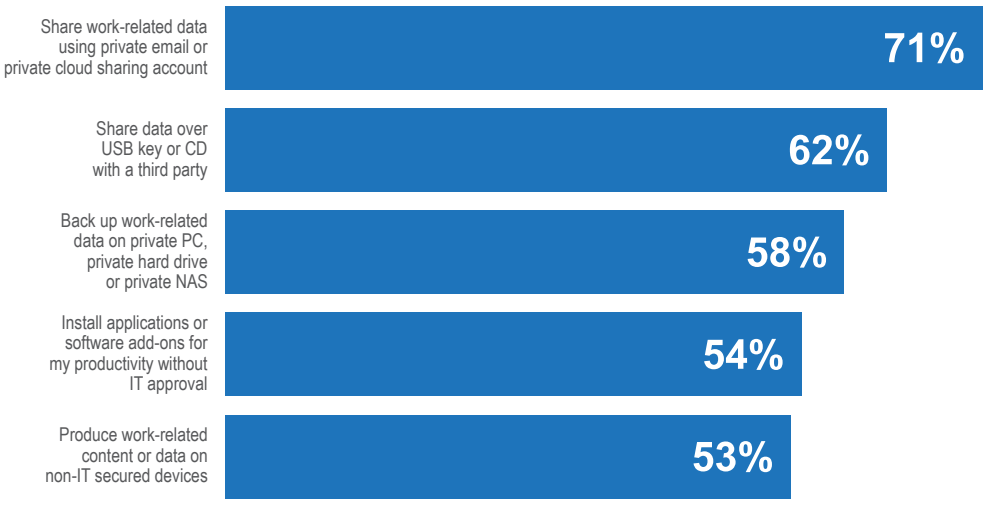
Why do you sometimes work outside your organization's security protocol?



The survey uncovered a broad array of activities carried out beyond corporate security protocols. 71% say they share work-related data using private email or private cloud sharing multiple times per month. However, the frequency with which respondents share data using a USB key or CD with a third party should be a particular cause for concern. Such behavior is a frequent cause of data loss, and 62% say they do this multiple times per month [see chart below].

42% of workers say their organization or management is OK with them working outside security protocols.

How frequently do you:

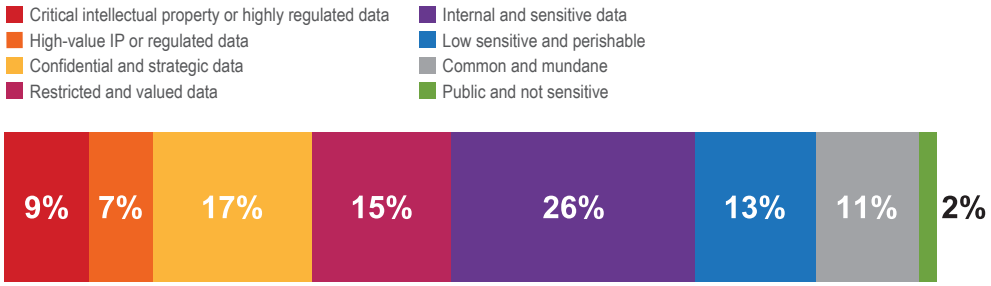


Collaborating with sensitive data

Collaborating is an essential activity for midmarket workers. Since data is typically shared during collaboration, the sensitivity of the data that is shared is an important concern. Accordingly, the survey inquired as to the level of sensitivity of data most frequently shared [see chart on next page]. Significantly, 33% of the shared data falls into the top three categories of sensitivity (critical intellectual property or highly regulated data, high-value IP or regulated data, and restricted and valued data).

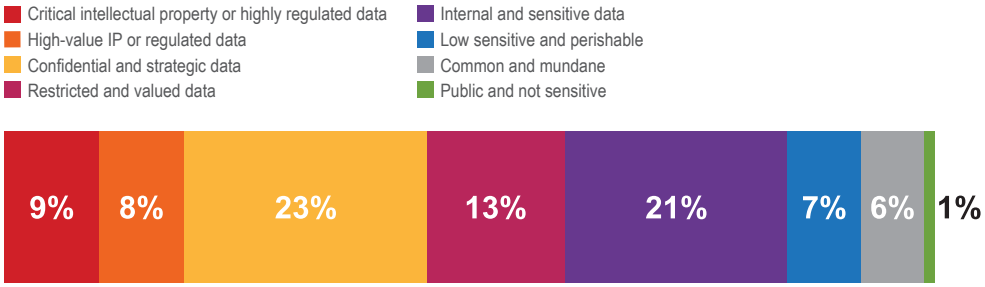
DELL EMC

How would you describe the level of sensitivity of the data you share most frequently?



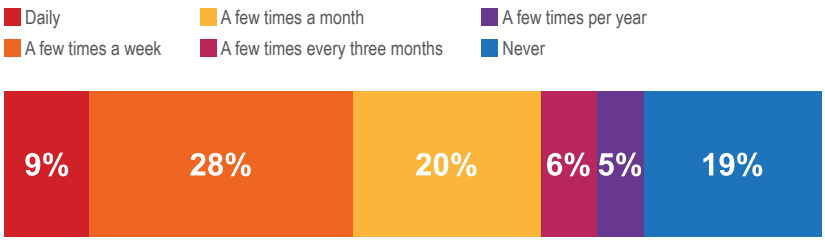
The sensitivity of data shared across an organization tends to be even greater. 40% of data shared is in the most sensitive classifications [see chart below].

What is the highest level of sensitivity of data that you share over the organization's network?



Oftentimes, workers find themselves in meetings using IT equipment, whether giving presentations or participating in team meetings. In these gatherings, data is typically shared, and because it is, security is a concern. 37% of workers meet weekly to share and collaborate in meeting rooms using a projector or TV [see chart below].

How often do you share/collaborate in meeting rooms using a projector or TV?

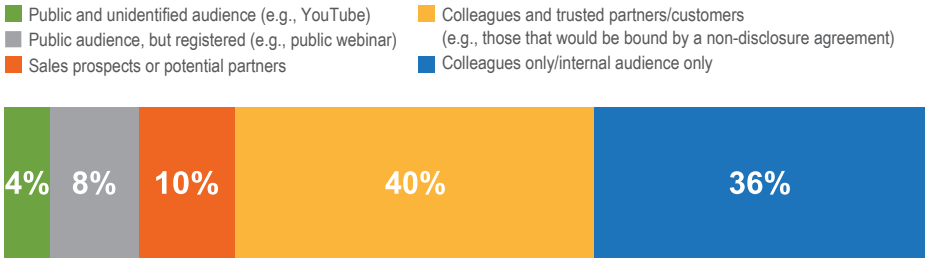


Delving deeper, the survey found that although sharing takes place most often among colleagues and trusted parties, 22% of the time sales prospects and the public, whether the press or the general public, take part in sharing and collaboration. This pattern indicates that sensitive data could be exposed to individuals outside the company more often than some might realize.

33% of workers most frequently shared data of the highest levels of sensitivity.

DELL EMC

What audience do you most often share/collaborate with in meeting rooms using a projector or TV?



Strategic security requirements

The mobile workstyle and the sharing of often sensitive data create a daunting security challenge. All organizations implement security measures, but when they are bypassed, data is exposed to the growing number of sophisticated security threats. As most business leaders are aware, the consequences of data loss can be devastating.

For example, the loss of intellectual property to competitors or nation-states can subvert a company's business model. Should offshore, low-cost producers gain knowledge of trade secrets, a company can quickly be faced with a market flooded with inexpensive products containing once-proprietary intellectual property. A scenario like this has the potential to drive a company out of business.

When customer data is stolen, losses can total in the hundreds of millions of dollars, resulting from damage claims due to identity theft as well as regulatory compliance penalties. In a well-publicized case, a large U.S. retail chain met with this very fate. Healthcare organizations, meanwhile, frequently face fines of varying severity when data is compromised in violation of HIPAA regulations. In the financial services and retail sectors, fines for PCI-DSS noncompliance are not uncommon.

Necessary security measures

To avoid the consequences of data breaches and data loss, security measures are essential. Devices must be secure, data must be encrypted, user permissions must be in place. Here are four key security steps that every midmarket business should take:

1. BIOS protection. A corrupted BIOS can harbor malware that survives a system's being "wiped clean" and the operating system re-installed. A system that includes BIOS protection can prevent this from happening.
2. Encryption. An essential data protection tool, encryption should be implemented where needed for data at rest (stored on a system) and data in motion (traveling over a network).
3. Advanced authentication. Making sure users are who they say they are is essential to keeping data safe. Two-factor authentication is recommended wherever it is feasible to implement.
4. Next-gen malware protection. Traditional antivirus and anti-malware software can't keep up with today's threats. Artificial intelligence and machine learning can stop even zero-day threats.

When customer data is stolen, losses can total in the hundreds of millions of dollars, resulting from damage claims due to identity theft as well as regulatory compliance penalties.

Conclusion

The mobile and remote IT landscape of the digital business era is here to stay. The ability of workers to access data and applications, whenever they need to and wherever they happen to be, is a game-changing productivity enabler that midmarket organizations and their workers highly value.

However, this workstyle tends to expose data to threats as never before, particularly when sensitive data is accessed and shared and when corporate security measures are circumvented. As a result, technology decision makers face significant challenges in securing data — challenges that must be met if they are to enable the productive workforces their organizations require. Above all, workers' devices and the data on them must be secured with technology that is streamlined and does not get in the way of workers as they go about their tasks.

Technology decision makers should pay heed to the results of the survey described in this paper. They should deploy a comprehensive array of technologies, such as those from Dell EMC, that deliver maximum data protection while enabling the workstyles of the digital business era.

Since the vast majority of breaches begin at endpoints, a focus on endpoint security is critical.

A robust security strategy that includes authentication, encryption (both file-level and dual-level) and advanced malware prevention, utilizing AI and machine learning, enables an organization to keep data safe while enabling the way people work.

Dell - the right security partner to protect data and devices

IT leaders should look for a single provider of security technologies that both protect data and prevent threats. A valued partner should implement both hardware and software protection. For example, a hardware provider should, where appropriate, embed security into the devices and software it produces. And the provider should take care in the design, manufacturing and delivery processes to mitigate the risk of counterfeit parts or malware introduction.

Dell's innovative security solutions are made for the way people work, enabling efficient and secure collaboration and a better employee experience. Dell provides both hardware and software protection, reducing the number of different security vendors an organization must use. Dell incorporates its own intellectual property as well as the technology innovations of strategic partners into its products. In addition, Dell leverages its PC heritage to bring security to the firmware layer through such features as BIOS protection.

Dell offers the world's most secure commercial PCs, powered by Intel® Core™ vPro™ processors with industry-leading endpoint security solutions that include BIOS protection, data encryption, advanced authentication and next-gen malware protection options.[1] Dell delivers on its promise of Trusted Devices with a portfolio of products and features including:

SafeBIOS

- SafeBIOS provides exclusive off-host BIOS verification to gain visibility to potential BIOS tampering, which could be a sign of a highly technical and invasive attack.

SafeID

- SafeID, available only from Dell, provides authentication integrity by securely storing and processing user credentials in a dedicated security chip, away from software attacks.
- SafeID uses features like integrated fingerprint reader, smartcard or contactless authentication to access connected credentials and verify users are authorized.

SafeData

- Smart collaboration is secure collaboration. Enable end users the freedom to collaborate smartly knowing data remains secure, even in diverse environments.
- Protect. Data is secure on device with file-centric encryption, and remains secure even when it is shared via email, cloud services, FTP and portable storage devices, by employees, contractors, vendors and partners.
- Control. Administrators define parameters for who has access to what data and when, as well as how the data can be used.
- Monitor. Perform analytics on data access, activity and location, enabling administrators to spot potential security risks.

SafeGuard and Response powered by Secureworks

Comprehensive threat management with intelligent and prompt security decisions powered by endpoint telemetry and validated by dedicated security experts can:

- Prevent 99% of threats from malware at the endpoint.[2]
- Detect non-malware threats already lurking in the environment and obtain an action plan for focused remediation.
- Respond to cyber incidents quickly and efficiently or even prepare in advance –for the unthinkable.

End-to-end Security from Dell

With a multilayer approach to security across Dell EMC solutions, featuring industry-leading rack and tower servers, storage and HCI solutions, Dell EMC delivers a secure, modern datacenter that's resilient from the ground up. Dell security solutions work together to surround data with security that moves with data wherever it goes across the IT infrastructure and beyond. The result: IT managers gain greater control over the entire connected ecosystem to protect IT, business, and customer assets.

Best of all, because Dell Financial Services solutions can cover everything Dell Technologies offers — including hardware, software and third-party IT — midmarket organizations can get all the necessary security technology and software upfront to protect their hardware investments.

1. Based on Dell internal analysis, October 2017. Legal AD#: A13001497
2. CrowdStrike Endpoint Protection Platform, Anti-Virus Comparative October 2018 AD#19000006

To learn more about how Dell EMC can help midmarket businesses with their technology needs, please visit our dedicated website on midmarket solutions.

For a more detailed study, read the research report, "The Workers' Experience: Survey reveals the importance of technology to spark motivation, enhance productivity and strengthen security."

Additional resources

- Dell Endpoint Security
- Dell ProSupport
- Dell Financial Services

About the survey

Dell EMC sponsored a survey of 1,327 workers at midmarket companies. The midmarket is defined as organizations with between 100 and 499 employees. The survey covered the regions of North America, Western Europe, Japan, Latin America and India. Vertical industries included Education, Energy, Finance, Manufacturing Logistics and Retail, Healthcare, Media & Entertainment, and Technology and R&D. Survey respondents were polled in the summer of 2018.