CODE42

White Paper | **Data Protection and Recovery**

6 Ways IT Can Empower Mobile Users

How Endpoint Visibility Helps IT Support Anytime-Anywhere Users

A few years ago, the typical enterprise approach to mobile users could be politely described as "tolerance." Most created policies designed to control mobile users, prioritizing a traditional perimeter-based security paradigm. Today, the priority has shifted. Most organizations now recognize that enabling mobile and remote productivity is absolutely essential to remaining competitive in the fast-paced digital business world. The result: A full 75 percent of the global workforce now regularly works remotely. In the U.S., Gallup found that one in three employees work away from the office the majority of the time (four or five days per week).[1] All those mobile users are working on a growing number of devices (at least three, on average), across an exploding range of applications. A decade ago, all the combined data in the world was less than what today's average digital enterprise worker creates on a daily basis.

75%

of the global workforce works remotely

1/3

of employees work remotely 4 or 5 days per week

An average of **3** devices per mobile worker

Empowering Mobile Users is Now a Must

The need to empower remote and mobile users goes well beyond giving employees the freedom and convenience to work from home. In businesses across every sector, highly mobile, on-the-go users often play a critical role in the organization. Anytime-anywhere productivity of on-site consultants is the core of consulting businesses, as well as companies with professional services offerings. These mobile users are billing by the hour, providing high-value, time-sensitive services. An interruption in productivity—from a lost file or damaged laptop—not only impacts the business' bottom line, but it can cause serious brand damage that limits future consulting engagements. In the medical technology sector, for example, engineers travel to provider sites to provide critical training and best practices for using new tools and delivering new treatments. Downtime can have a cascading effect of missed appointments and delayed training that ultimately limits providers' use of their technologies. Across the broad technology sector, sales "road warriors" visit prospects to give live demos and presentations directly from their laptops. These are typically one-shot opportunities. If the presentation or demo file goes missing, the sale is lost. These examples share a common thread: With mobile users carrying out critical, time-sensitive workflows, businesses must ensure they have continuous access to the information they need.

Mobility Magnifies Endpoint Data Risks

Endpoint data has always presented challenges for IT. Users don't follow policy and IT is left in the dark, unable to see or protect users from their own errors. Mobility greatly magnifies this challenge. With the majority of users regularly working remotely, as much as two-thirds of all enterprise data now lives on endpoints outside the data center. Mobile users prioritize convenience and productivity over security, accessing sensitive data and transferring files via insecure email and file sync and share (EFSS). Three in five admit to ignoring policy in the name of productivity; the remaining two may just be less honest about it.[2]

Business Leaders Want the Benefits of Mobile Productivity—Without the Risks

The high expectations of mobile users—to work where they want, on the device they want, unimpeded by policy—already challenge IT administrators and end-user services directors. But now, end-user pressure is joined by pressure from the top of the organization. Business leaders are not only seeking the proven productivity gains of mobility; they want to create the modern work environment that younger generations expect—something that is increasingly essential for attracting and retaining talent. However, business leaders are also more aware than ever of both the threat and the cost of cyberattacks, data breaches and data loss. All of this adds up to a growing number of mobile users creating and moving an incredible amount of data beyond the visibility or control of IT. The increased risk posed by mobile users comes at a time when awareness of both the threat and cost of cyberattacks and data breaches is greater than ever.

Employees Leave More Often Than Ever—And They're Taking Data With Them

Long gone are the days of the loyal lifetime employee. The generational turnover in the workforce has seen voluntary turnover rates increase by more than five percent every year since 2011.[3] Deloitte says most Gen Y employees will leave an organization in just two or three years.[4] Rapid turnover is a headache in itself. Add in that most employees are carrying around vast amounts of valuable and sensitive business data on their endpoints—largely beyond the control of IT—and turnover becomes a massive data security risk. Three in five employees admit to taking data with them when they leave.[5] They take it because they think it's theirs: 85 percent say they take documents and information they created.[6] But they also take data because they know it's valuable: an estimated 80 percent of an organization's value lies in its intellectual property.[7]

Six Steps to Empowering Mobile Users and Protecting Endpoint Data

All of these expectations add up to a complex challenge that's at the core of the digital business world: How can you grant mobile users the freedom they expect, while simultaneously providing the support they and the business need to maximize productivity and mitigate risk? As IT and end-user services teams look for the right tools and technologies to solve this challenge, here are six key capabilities to consider for empowering and supporting mobile users:

1. **Enable Mobile Users to Work on the Device of Their Choice**
   We now walk around with connected devices at all times, so it's no surprise that device choice is an increasingly important, personal matter. Numerous studies have shown that users are more productive when working on the device and operating system of their choice. This is even more critical for mobile users, who are more likely to be working on their personal devices—whether at home or on the road. While many companies now show a unified front of supporting multiple operating systems, the back end is messy. IT teams often manage unique tools for each OS, leading to headaches

at best and dangerous gaps in coverage at worst. To ensure that all mobile users—and indeed, all users—are covered, IT should look for tools that support Windows, Mac and Linux devices in a single, seamless platform. This empowers end users to work from the devices they choose, without burdening IT or putting data at risk.

1. **Key Takeaway:** **Make sure endpoint backup seamlessly supports Windows, Mac and Linux devices.**

2. Don't Burden Mobile Users with Data Backup

Most users—mobile or not—store sensitive and valuable data on their endpoints. Many organizations still rely on manual, user-initiated data backups, meaning not all of that data makes it to the central server or network drive. For mobile users, the burden of manual backup is particularly painful. Legacy backup products require mobile users to connect via VPN to execute a manual backup. If a business and its users followed current backups best practices, mobile users would have to stop what they're doing every 15 minutes to manually back up. This obviously doesn't happen, nor should it. Instead, look for a backup solution that removes the end-user burden. Backups should happen automatically and continuously, as often as every 15 minutes, with any secure internet connection. The leading endpoint backup tools also provide purpose-built features that make it easy for IT to ensure mobile users' endpoint data is handled and stored in compliance with all relevant regulations.

For mobile users, it's faster restores—not faster backups—that matter most.

2. **Key Takeaway:** **Make endpoint backup automatic and continuous.**

3. Help Mobile Users Bounce Back From Mistakes Quickly

Whether it's user error, device or software failure, or ransomware or cyberattack, data loss is unavoidable. But for mobile users—particularly the "road warriors" who spend their work week on-site with customers—these mistakes can be particularly debilitating. Productivity grinds to a halt for hours or days while IT struggles with limited remote restore capabilities. In some cases, mobile users must wait until they can visit the central office to get their data back. Comprehensive, automatic endpoint data backup is critical for solving this challenge. But backup means little if restoring that data isn't quick and easy—especially when it comes to time-sensitive mobile user needs, from giving a sales pitch or presentation, to on-site project management. While many backup tools highlight lightning-fast backup speeds achieved with global data deduplication, the truth is that both global and local deduplication deliver extremely fast backup speeds—but global deduplication significantly impedes data restores. Instead, IT should look for a backup solution that leverages local data deduplication to maximize data restore speeds. This approach produces five to nine times faster restores, enabling IT to restore a mobile user's missing file in seconds, and an entire system in under an hour.

3. **Key Takeaway:** **Focus on restore speed—not backup speed.**

4. **Enable Mobile Users to Self-Restore Data**
   When every minute counts, mobile users don't want to wait for IT's help in restoring a missing file. The solution: Give users the ability to restore data on their own. Leading endpoint backup solutions now provide mobile users with a simple, intuitive self-restore workflow. They give users easy access to their entire endpoint data backup store but, critically, prevent them from accessing other users' data. Just as mobile endpoint backup shouldn't be dependent on a VPN, IT should look for a solution that enables users to execute self-restores from any secure internet connection.

4. **Key Takeaway:** **Choose endpoint backup that offers self-restore capabilities.**

Empowering mobile users means eliminating the IT bottleneck with self-restore capabilities.

5. **Protect Mobile Users From Data Security Threats**
   Just as mobile users don't want to be burdened with backup or compliance requirements, they also can't be expected to know and recognize the signs of a cyberattack or data breach. Like your local users, mobile users expect IT to keep an eye out for threats and alert them when there is a problem. But traditional perimeter-based security isn't applicable to mobile users. In order to accomplish this risk surveillance and mitigation for mobile users, IT should look for a tool that enables them to see data living on endpoints outside the traditional perimeter. Leveraging this visibility, IT can build a baseline for what "normal" looks like: the patterns around what files a user accesses and how they move data between devices, storage locations and applications. This baseline, combined with ongoing endpoint visibility, helps IT identify anomalies and alert mobile users to a possible attack or compromise.

5. **Key Takeaway:** Leverage endpoint **data visibility to establish a baseline and spot the anomalies.**

6. **Give Mobile Users Immediate Access to the Latest Tools**
   As the pace of innovation continues to accelerate, keeping users' hardware, software and applications updated and patched is a never-ending task. Mobile users are often left behind, unable to update their technology until they have several days in the main office. While some organizations have attempted to shoehorn an enterprise-grade EFSS product like Google Drive or Microsoft OneDrive as a solution for this problem, this approach overburdens the mobile user with manual backup and file-by-file restore. In addition, the EFSS environment is also not designed to secure a business' most sensitive information, exposing the user and the business to a high level of data security risk. However, the same endpoint backup technology that enables self-restores in the case of data loss can transform tech refresh workflows for mobile users. Instead of visiting the office for an IT-heavy tech refresh, users can execute self-migration of all endpoint data as they install a new operating system or migrate to a new device. IT significantly reduces its tech refresh workload, while ensuring all mobile user data is continuously and securely backed up. Moreover, this approach ensures that mobile users gain faster access to the most current technologies—tools that are both more productive and more secure.

6. **Key Takeaway:** Move toward **user-driven tech refresh.**

Endpoint Visibility Solves the Mobile User Challenge

All six of the above capabilities share a common core: endpoint data visibility. With the right tools and technologies in place, IT and end-user services teams can obtain complete visibility into mobile users' endpoint data to both grant freedom and take back control.

- **Mobile users work how they want. IT stays in control.** Users work how they want on the devices of their choosing, with automatic, continuous backup taking the place of burdensome policies. At the same time, IT retains control through comprehensive visibility from a single platform—all users, all operating systems, all data.
- **Mobile users recover from any data incident—in real time.** Whether it's user error, hardware failure or a ransomware attack, IT can guarantee data recovery for mobile users. Moreover, mobile users can execute self-service restores in seconds, and get back to their work.
- **IT can solve multiple business challenges.** The value of endpoint visibility goes well beyond protecting mobile users from data loss. It can also deliver powerful risk mitigation from insider threat and cyber attack, enable fast and cost-effective data migration and tech refresh, and streamline legal hold and e-discovery to produce significant cost savings.

Freedom Through Transparency

The future of enterprise productivity lies in user freedom: users reaching new levels of productivity, job satisfaction and even innovation through working anytime, anywhere, from any device and with any application. To achieve this freedom while also securing and protecting the enterprise requires a fundamental shift. Instead of focusing on barriers to control and limit users, the most successful businesses are trading control for transparency. By leveraging tools like advanced endpoint data backup, the enterprise gains the visibility it needs to fully capitalize on the potential of highly mobile, highly productive end users.

[1] http://www.gallup.com/reports/199961/state-american-workplace-report-2017.aspx

[2] https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-millenial-survey-2016-exec-summary.pdf

[3] CompuData Surveys 2015 BenchmarkPro Survey

[4] https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-millenial-survey-2016-exec-summary.pdf

[5] http://deloitte.wsj.com/cio/files/2016/04/2688954-Insider-Threat_4.pdf

[6] Bitcom Survey, 2016

[7] https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html

FOR MORE INFORMATION: CODE42.COM/CONTACT

CORPORATE HEADQUARTERS | 100 WASHINGTON AVENUE SOUTH | MINNEAPOLIS, MN 55401 | 612.333.4242 | CODE42.COM