Windows To Go: Empower And Secure The Mobile Workforce

CONTENTS

2  Windows To Go: Support New Levels of Secure Mobility
3  Benefits of IT-Managed Windows Workspaces
5  Mobile Workforce Use Cases
5  Superior Mobility Option
6  Test An Affordable Laptop Alternative
INTRODUCTION

With the BYOD movement, IT has a golden opportunity: serve the productivity needs of a fast-evolving, mobile workforce, while simultaneously providing data protection expected by corporate leaders. Great news: you can meet these requirements today by leveraging technology that is secure, manageable and cost effective. Learn how.

BYOD is a game changer for corporate IT — one of the biggest changes to the culture, security requirements and economics of client computing in decades.

Mobile devices and BYOD policies give employees the flexibility to be productive anytime, anywhere while improving their job satisfaction. From the perspective of CIOs and corporate IT, they let employees — as well as contractors and temporary workers — use personal laptops, which often have more computing power and advanced features than corporate systems, saving IT on the cost of hardware.

To get IT’s blessing, devices need to be simple enough for users to embrace while also delivering the security and manageability to meet enterprise IT requirements.

A new Windows 8.1 technology, Windows To Go, makes mobile computing easier to deploy and less expensive than alternatives including dedicated laptops. IronKey™ Workspace delivers enterprise security and manageability for Windows To Go in a ruggedized and secure USB flash drive, thereby protecting company data, hardware and software from being compromised in mobile applications.
Leveraging its track record as the supplier of IronKey, the world’s most secure mobile storage for enterprise IT, Imation Mobile Security applies its expertise to deliver on the promise of mobility while meeting the security needs of business and IT leaders.

Windows To Go: Support New Levels of Secure Mobility

With an IronKey Workspace drive, any computer can operate as a secure, IT-provisioned and managed client. It can eliminate the need for most users to carry a company laptop computer.

Users insert the IronKey Workspace USB and boot the PC from the drive using the installed operating system. Because the configuration of the Windows image is set by corporate IT, the system boots with all the programs and data that are accessible to the user under corporate policies.

Windows runs locally and natively on a system booted from an IronKey Workspace drive. The first time a Windows To Go drive boots, it will detect all the hardware in the system and install any necessary device drivers. If that same drive is subsequently booted on the same system, it recognizes the system and loads the correct drivers, booting more quickly.

Windows To Go drives can support both 32-bit and 64-bit images of Windows. Which image is installed depends on many factors, including whether current applications are 32-bit or 64-bit.

Because IronKey Workspace is the primary storage device for Windows To Go, a user should never remove the IronKey Workspace drive while Windows is running. But if it is removed, Windows will freeze for 60 seconds to give the user an opportunity to reinsert the drive in the same port. If the drive is reinserted, Windows will continue where it stopped operating when the drive was pulled. If it is not reinserted within 60 seconds, the host computer will turn off. That’s another indicator of how IronKey Workspace was designed with the protections and reliability required by enterprise IT organizations.

Any corporate IT organization with a Microsoft Software Assurance Agreement (SAA) has a license for Windows To Go for every computer covered under that SAA, regardless of what OS is installed on the computer’s hard drive. All PCs certified to run Microsoft Windows 7 or higher operating systems meet the hardware requirements to run Windows To Go.

With IronKey Workspace, there is no threat from malware installed on the computer.

Because the host operating system on the PC is not running when IronKey Workspace is operating, there is no threat to the user or network from malicious software that may be installed on the computer. The Windows To Go session writes no data to storage on its host PC, so no company data or programs remain on the system after the user shuts down.
Benefits of IT-Managed Windows Workspaces

By deploying Imation IronKey Workspace drives with Windows To Go, IT organizations will realize a range of benefits that secure corporate data in mobile applications.

- **Security**: IronKey Workspace guarantees all remote access devices are strongly encrypted and corporate data is protected in the event of loss or theft. The low cost of the drives means minimal financial impact if a loss does occur.

- **Flexibility**: Users can run Windows To Go on whatever system they choose, as long as it is certified for Windows 7 or Windows 8. They gain the flexibility to travel light, with only their Windows To Go drive, if they choose.

- **Performance**: When inserted into USB 3.0 ports, Windows runs at the full speed of the hardware from an IronKey Workspace drive. It is no more dependent on the speed of the Internet connection than Windows running off an internal hard disk.

- **Cost**: By providing high-quality, high-speed remote access to users’ corporate Windows accounts for as little as $200 per user, IT can deliver remote access at a flat, predictable cost per user.

IronKey Workspace is built from the ground up to be an enterprise-grade device with advanced features that satisfy the security and manageability requirements of corporate IT while enabling the mobility and BYOD capabilities that users need to maximize productivity. Those enterprise-class capabilities include:

**Administer policies and manage from a central location.** Using the on-premise IronKey Enterprise Management solution, administrators manage policies from a single console. Common policies include managing password requirements for the IronKey drive; locking or unlocking drives; resetting passwords; controlling the deployment of IronKey software updates to the device; and remotely “detonating” — deleting all contents on the drive and making it unusable. The IronKey Enterprise Management solution is the same system that IronKey customers have long used to manage hardware-encrypted secure storage devices.

**Easily and efficiently issue IronKey Workspace drives via Provisioning Tools.** Customize Windows Imaging (WIM) files, for instance, with company logo wallpaper, or install antivirus software. Deploy one or dozens of drives at a time — the process is as easy as “boot and scoot.”

**Protect against confidential data loss.** Because no data is stored on the host computer, but is instead stored on the highly encrypted IronKey Workspace drive, enterprise IT maintains strict adherence to security and compliance mandates. Operating systems and apps on the system’s hard drive aren’t running during the Windows To Go session, so the security of the host computer is not impacted in any way. Because IronKey Workspace provides 256-bit AES hardware encryption, software encryption

With the highly encrypted IronKey Workspace drive, enterprise IT maintains strict adherence to security and compliance mandates.
solutions such as Microsoft BitLocker are not necessary, although BitLocker is supported.

**Solve the device loss/theft problem.** If an IronKey Workspace drive is lost, it’s unusable by whoever finds it, and can be remotely wiped if the administrator considers that step to be necessary. The cost of a lost IronKey Workspace drive is minimal (starting at $175 for 32GB) compared to that of a laptop ($1,500). The value of that lost laptop, moreover, goes well beyond the hardware/software cost, as the laptop likely contains proprietary corporate and personal customer data. While both devices may contain proprietary corporate and personal customer data, secure workspace devices are hardware encrypted to provide persistent data protection.

**Lower support costs and simplify maintenance.** Because the user profile in Windows To Go is entirely managed, many problems typical of remote notebooks are avoided. Users have less opportunity to misconfigure their computer or applications.

As long as any data saved from a Windows To Go system is stored on a server or in a local folder redirected to a server, there is no need for a backup and restore plan for IronKey Workspace drives.

**Deliver high performance.** Windows To Go running on an IronKey Workspace drive connected through a USB 3.0 port is faster than many systems running on internal hard drives. Unlike Virtual Desktop Infrastructure (VDI) clients, Windows To Go does not rely heavily on the performance of the Internet connection for a good user experience. And if additional storage is required, IT can allow users to sync local copies of their network files on the USB drive by using folder redirection and client-side caching.

**Fully leverage Windows To Go.** IronKey Workspace drives are optimized, and certified, to support Windows To Go and run on PCs certified to run Microsoft Windows 7 or higher operating systems. Conventional USB flash drives are optimized for sequential read/write operations, whereas a Windows To Go drive needs to support thousands of random I/O accesses per second to provide consistent performance. IronKey Workspace drives are physically hardened to handle the rough treatment that can be expected for a remote access device.

Getting the system to boot from the USB drive may require the user to enter the BIOS boot settings screen and to know what key to press as the system starts up. Windows 8.1 includes a feature called Windows To Go Startup Options that allows a user to configure their computer to boot from within Windows—without ever entering their firmware, as long as their firmware supports booting from USB (as all Windows 7- and Windows 8-certified systems do).
Windows To Go: Empower And Secure The Mobile Workforce

Manage through Microsoft Active Directory.
Windows To Go systems can be specially managed through Windows Active Directory. Administrators can create a separate Organizational Unit (OU) in Active Directory specifically for Windows To Go accounts, as distinct from accounts for host computers. This allows administrators to set policies only for Windows To Go use, such as different power state controls or to allow the use of the Windows Store app. Windows To Go cannot, by default, hibernate or use the Store, for similar reasons: A hibernated system must always reboot on the same hardware, and apps installed through the store are tied to the hardware on which they were installed. Because a Windows To Go drive is designed to move from system to system, Microsoft changed these defaults as a safety measure.

Mobile Workforce Use Cases
IronKey Workspace enables new levels of flexibility for the mobile worker who needs to get work done anytime, anywhere.

Workers out of the office, whether at home or on the road, can use their IronKey Workspace drive to connect to the enterprise network and all of their needed software and data using any Internet-connected computer. Users who travel and have access to other computers capable of running Windows To Go may choose to travel light and leave their laptop at home.

IT can give contractors and temporary workers secure access to the enterprise network, either on premises or remotely. IronKey Workspace is especially useful in this scenario, as all of a contractor’s work can be stored on corporate servers and no traces will be left on any host systems. IT can feel more confident allowing remote contractors to access the network using IronKey Workspace because communications will be secured automatically and the enterprise network will not be exposed to potentially infected remote systems.

Even for users who have their own laptop computers, an IronKey Workspace drive is a robust, inexpensive backup remote access device. A lost or damaged laptop can be a crisis for users on the road, as well as for IT support. If the user has a Windows To Go drive, they can still have access to all their software and data. In the event of purely software problems on the user’s laptop, the laptop can still be used to launch Windows To Go from IronKey Workspace.

Superior Mobility Option
Laptop computers are far more expensive, difficult to maintain, prone to loss or theft and vulnerable to security problems than a USB workspace drive. By providing Windows To Go drives, IT can cut costs significantly and expand remote access to more employees at the same time. IronKey provisioning and management tools, combined with the integration of Windows To Go into Active Directory, give IT better, easier control over remote users than other remote access methods.
Given the affordability of IronKey Workspace, it provides a low-risk way to test, and ultimately deliver, new levels of secure mobility.

In most instances, IronKey Workspace and Windows To Go represent a user-friendly, cost-effective alternative to Virtual Desktop Infrastructure (VDI) solutions such as those from VMware and Citrix. However, in those cases where VDI is deemed appropriate, it is imperative that the endpoint be trusted (what if, for example, it is compromised by malware?). IronKey Workspace complements VDI in such use cases because IT can install the VDI client on a Workspace Drive, transforming any PC into a hardened, trusted VDI endpoint.

Finally, it’s not uncommon for workers to have a much faster and more powerful system at home than at work. In these cases, users will likely prefer the Windows To Go experience because it lets them leverage the power of a familiar computer they’ve selected.

Test An Affordable Laptop Alternative

Windows To Go provides a clear-cut alternative for employees, remote workers, contractors and business travelers. IronKey Workspace bolsters Windows To Go with industrial strength, enterprise-grade security and manageability. IT pros should consider Windows To Go and IronKey Workspace a viable replacement for laptops that enables them to travel lighter with the most robust security on the market. Given the affordability of IronKey Workspace, it provides a low-risk way to test, and ultimately deliver, new levels of secure mobility.

Imation, the Imation logo, IronKey and the IronKey logo are trademarks of Imation Corp. and its subsidiaries. All other trademarks are property of their respective owners.

This white paper was developed by Larry Seltzer on behalf of Activate Marketing Services for Imation.
About the Author

Larry Seltzer has long been a recognized expert in technology, with a focus on mobile technology and security in recent years. He was most recently Editorial Director of BYTE, Dark Reading and Network Computing at UBM Tech.

Prior to that he spent over a decade consulting and writing on technology subjects, primarily in the area of security. He is the author of three books and thousands of published articles and many more unpublished, private reports.

Larry has been Technical Director at several test laboratories where he both directed and ran product testing, with a special interest in test automation.

Larry began his career as a Software Engineer at the now-defunct Desktop Software Corporation in Princeton, NJ, on the team that wrote the NPL 4GL query language. He also worked on corporate IT and software development at Chase Econometrics.

Larry is a graduate of the University of Pennsylvania with a degree in Public Policy.
activate

About Activate
Activate combines deep buyer insights with a content-led nurturing methodology to engage prospects and convert them to customers.

© 2013 Activate Marketing Services LLC | activatems.com