IRONKEY™

WHITE PAPER

A BLUEPRINT FOR SECURE MOBILE WORKSPACES

What Organizations Need to Consider when Implementing a Secure Mobile Workspace Strategy

September 2015

INTRODUCTION

The concept of "remote work", or teleworking, has become an increasingly important concept for organizations attempting to become more flexible and agile, while driving down costs. IDC reports that the U.S. mobile worker population will grow at a steady rate over the next five years, increasing from 96.2 million in 2015 to 105.4 million mobile workers in 2020. By the end of the forecast period, IDC expects mobile workers will account for nearly three quarters (72.3%) of the total U.S. workforce.

By enabling employees and contractors to work from any location – at home, at customers' sites, in remote offices, organizations can expect increased productivity. Moreover, the US, Canada and other governments have become major proponents of the telework concept as a means of reducing costs, supporting various "green" initiatives and keeping government open when access to the office is not an option.

As organizations rush to implement telework policies, they must face three obstacles before sending employees and contractors out the door with critical data and network access: cost, security, and portability.

This whitepaper examines how enterprises can deploy the Secure Mobile Workspace, or PC on a Stick™ portable desktops. With the advent of Windows To Go as a feature of Windows 10 and 8.1/8, this emerging "bootable USB workspace" category holds the promise of allowing an IT organization to embrace worker mobility, workplace agility and "bring your own device" (BYOD) – while safeguarding data and network access with more granularity and security than with a corporate provided computer.

ENTERPRISE SCENARIOS:

Whether it is a full-time employee needing to work off campus, a contractor or an employee with multiple devices, anyone accessing an organization's data presents security risks. A mobile workspace on a USB drive safeguards a company from data leakage, malicious insiders and breaches.

- **Teleworkers:** Today, the global workforce is more mobile than ever. Forrester Research's US Telecommuting Forecast notes that 34 million Americas work from home. This number is expected to reach a staggering 63 million— or 43 percent of the U.S. workforce by 2016.

- **Contractors and temporary workers:** More often than not, the contractor or temporary employee needs to access sensitive data to do their job. Be it an auditor or project consultant, organizations need to have complete control at all times of the data being accessed, wherever that may be. On the flipside, if the corporate data should happen to walk out the door, then IT can immediately disable access with the portable workspace solution.

Organizations often meet the security requirement by providing a full-fledged laptop to contractors, or implement a virtual desktop. Both approaches can fail from a cost standpoint, and may open security risks as well. A USB mobile workspace would provide a secure, full-featured desktop that could be used on the contractor's own device without compromising security – and implemented at a lower total cost.

- **Multiple devices workers:** With so many different devices being brought within a company's four walls, and potentially accessing the corporate network, the danger of data leakage multiplies exponentially. Every employee has at least one device, most likely a smart phone, and many have multiple devices that they use to be productive. The BYOD (bring your own device) movement has caused more enterprises to allow "non-standardized" devices to attach to the network. A SANS Survey revealed that more than 64 percent of mobile workers can access high-value enterprise data remotely; yet only one in three are managed. The study concludes that the unmanaged personal computers, laptops, smartphones and tablets that make up almost one-third of the mobile BYOD used to access corporate data, combined with lack of controls, leave organizations vulnerable to data exposure.

According to a new forecast from the International Data Corporation (IDC) Worldwide Quarterly Smart Connected Device Tracker, the combined total market of smartphones, tablets plus 2-in-1s, and PCs is set to grow from 1.8 billion units in 2014 to 2.5 billion units in 2019. With each new device entering the market, there is a completely new environment that IT staff must learn, often after the connection to the network has been made. This scenario brings to light two security issues – bringing viruses and malware onto the corporate network as well as putting sensitive corporate information onto any number of devices – most of which are probably not as secure as corporate IT would like.

ENABLING THE MOBILE WORKFORCE: OPTIONS

To efficiently and cost effectively enable telework, three elements are necessary:

- A very simple deployment that will allow the user to use a PC (certified for Windows 7 or higher operating systems and compatible tablets and Mac computers) owned by either the organization or the employee.

- A highly secure environment that will mitigate the potential for data breaches.

- A user experience that will emulate what IT provides when the employee is in the office.

There can be significant expenses in enabling employees and others to work remotely. For example, providing the remote worker with a laptop and all of the application software he or she might require to work effectively can be very expensive when accounting for the cost of hardware, software, maintenance, etc. This is the most expensive solution up-front, but control of the equipment by the IT department lends some piece of mind in terms of security. The IT department can configure and enable the type of protection necessary for the organizations' data.

Providing users with a set of cloud-based applications or a virtual desktop environment that they can access using their own computers can be less expensive and useful in many scenarios. At the same time, this option has some drawbacks. It relies on an always-available, always stable Internet connection. In instances when the user is on an airplane, in remote areas, in foreign countries or in weather related emergencies – or simply getting poor service from their ISP, employees might find an insecure connection – or none at all. Insecure internet connections may lead to data breaches, and lost employee devices open the organization to additional security risks.

In short, while most laptop, cloud-based and virtual desktop approaches are useful at enabling remote work, they have drawbacks as well. Organizations seeking to enable mobility with high security, while delivering a seamless work experience, can now consider what some analysts are calling the next stage in the evolution of personal computing – the secure mobile workspace.

THE PROMISE OF THE SECURE MOBILE WORKSPACE

The idea behind the USB mobile workspace is to enable worker flexibility and business continuity. Essentially a "PC on a Stick™" device, the mobile workspace provides the worker a full-featured version of Windows 10 or 8.1/8, key corporate applications and network access interface that can be booted from the USB stick on nearly any host computer. With IronKey's Workspace, the "PC on a Stick" USB flash drive is kept entirely separate from the host computer's hard drive, effectively sealing off data transfer between one drive and the other – and mitigating transfers of viruses or malware. The advantages are threefold:

- **It may have a lower Total Cost of Ownership (TCO)** because of its lower initial cost and lower lifecycle/refresh costs. The Secure Workspace Solution also offers other advantages like portability, encryption, the minimal learning curve in using the technology (no training required), and its physical durability.

- **It offers greater employee flexibility** because it can plug into any compatible PC, tablet or Mac, and it takes full advantage of the features on that host computer, and is highly secure. The IronKey Mobile Workspace can duplicate the in-office experience by booting an employee's laptop or home computer from the secure USB drive, using the applications that have been provided by the organization. This allows the organization to turn an employee's unmanaged computer into a trusted workstation with full security, and with no impact to the host computer's hard drive or applications. There is nothing to install on the employee's machine.

- **It can reduce security risk.** IronKey's secure mobile workspace solutions for Windows To Go leverage features such as 256-bit XTS-AES hardware encryption to protect the drive's contents. Such a device necessarily includes security to mitigate the risk of liabilities that can result from breaches of sensitive or confidential information. It can prevent data leaks by preventing data from being copied to the host computer's hard drive – it leaves no data footprint on the host computer.

With mobile workspace solutions, IT can issue a full-featured Windows 10 or 8.1/8 environment on a secure, encrypted USB device that employees or contractors can use both in the office and on computers at home or on the road.

IRONKEY™

WHITE PAPER

THE MOBILE WORKSPACE BLUEPRINT – WHAT TO CONSIDER:

When looking at developing a blueprint for how mobile workspaces could help enable teleworkers and secure the organization, IT professionals should consider the following elements:

- **Deployment**
  - o Form factor plays a large role in quickly being able to distribute devices to the end users.
  - o A standard image of the operating system with all corporate applications is necessary for a remote worker to be fully functional.
  - o The ability to re-provision a device so that it can be used by another employee quickly.

- **Management**
  - o As these devices become corporate assets, they need to be managed for accountability and security.
  - o You should be able to assign the devices to individuals automatically through Active Directory, a feature of Windows.

- **Security**
  - o Use of either Microsoft's BitLocker drive encryption or 256-bit XTS-AES Cipher-Block Chained mode hardware encryption to ensure security.

- **Compliance**
  - o Data at rest should be encrypted to avoid data leaks, public disclosure and the costly fines associated with mandates such as HIPAA, PCI and SOX (relevant for healthcare and companies accessing financial data).
  - o Legislative requirements including FIPS 140-2 Level 3 certification

- **Usability**
  - o The solution needs to allow the user to be fully functional, replicating the experience of an employee's normal desktop at work.
  - o The ability to take advantage of all of the hardware capabilities from the system that they are working on (Wi-Fi, Video Card, Webcam, Printers, etc.).
  - o A way to work offline without an internet connection. This is especially important in cases where the user travels and an internet connection may not be available.
  - o An attractive form factor for the mobile device encourages user adoption.

IRONKEY™

WHITE PAPER

PIONEERING THE SECURE MOBILE WORKSPACE

IronKey has been a leader in high-security USB devices and a pioneer in this space, implementing a secure mobile workspace solution using Windows 7 on hardware encrypted flash drives. Today, IronKey Workspace drives are Microsoft-certified for Windows To Go and will help organizations deliver a full-featured Windows 10 or 8.1/8 experience. IronKey Workspace W700, W500 and W300 drives let you control access to your mobile Windows To Go desktops with built-in password protection capabilities and up to 256-bit XTS-AES hardware encryption. And organizations deploying IronKey Workspace W700 and W500 drives can take further control of their portable workspace devices with IronKey's optional centralized management and provisioning tool. To help ensure the delivery of the right levels of utility, security, management, and compliance for their organization, IronKey Workspace features:

• **Full host-computer isolation,** where, after reboot and authentication, the computing environment is isolated from malware and data leakage.

• **Hardware encryption,** including up to 256-bit XTS-AES hardware encryption to lock down content and shield the desktop, preventing tampering, intrusion and piracy.

• **High performance,** delivering read/write performance exceeding the minimum requirements for Windows To Go devices.

• **Ruggedized and waterproof,** helping ensure users get a USB flash drive they can count on.

• **Advanced centralized management and deployment,** that gives IT management the ability to control drive access and usage, set password policies and deploy large numbers of mobile workspaces.

CONCLUSION

With remote working rapidly becoming a standard feature of office life, few organizations can afford not to address the challenges of secure mobility and BYOD. As IT departments grapple with the cost-security-portability equation on remote working solutions, the Secure Mobile Workspace is rapidly emerging as a powerful and useful option.