WHITE PAPER
FEBRUARY 2017

IT@INTEL

Secure, Remote Access with a Portable USB Operating System

The USB operating system offers Intel's provisional workers a user-friendly, cost-effective alternative to company-provided PCs.

Shmuel Ber
Systems Engineer, Intel IT

Sharon Biton
Information Security Engineer, Intel IT

Ehud Eitan
Product Manager, Intel IT

Edgar Farji
Team Manager, Intel IT

Executive Overview

Intel IT supports a variety of provisional and external workers and contractors who access Intel resources for collaboration and productivity. Providing Intel-deployed PCs is not always an ideal option. Some of these workers require higher levels of security access than these PCs allow, and most of these workers already have their own company PCs and do not want to carry a second one.

We have explored various ways to make provisional workers more efficient, including enabling them to work on their own PCs. This option presents challenges, of course, since those PCs are not managed by Intel IT and lack the required security controls to safely access corporate resources.

Previously, we provided a client-hosted virtualization (CHV) platform to give these workers necessary access without compromising security. In these cases, the user experience was sometimes problematic due to lack of performance.

To solve this challenge, Intel IT designed a solution that uses an operating system that runs on a USB drive. The portable USB drive solution consists of the Microsoft Windows To Go* feature of the Windows* OS, wrapped with additional security and manageability capabilities such as hardware encryption, a management console, and embedded McAfee® security tools. The USB OS solution can be deployed to users who have different security requirements, so they can securely access top-secret Intel content from their own PCs.

The USB OS solution offers the following benefits:

- **Security.** Embedded USB encryption and remote manageability capabilities (disable device, delete device) include McAfee security tools to protect the device from malicious software (malware) and other potential threats, as well as prevent data loss and content leaks.
- **Performance.** Workers who use their company PCs for Intel work can experience performance that is consistent with Intel-deployed PCs.
- **Flexibility.** The plug-and-play USB drive can be used on any PC.
- **Manageability.** A management console can remotely access the USB OS to push updates and track specific devices.
- **Cost-effectiveness.** A USB OS can be deployed faster and at a lower cost than a PC.

In our pilot test, user feedback was overwhelmingly positive. While we still provide PCs to some workers, the USB OS offers a portable, user-friendly, cost-effective alternative. It is rapidly becoming the solution of choice among provisional workers and Intel IT.

Contents

Contributor

Julian Braham
Staff Engineer – Client Engineering
Intel IT

Acronyms

CHV	client-hosted virtualization
ODC	offshore development centers
VDI	virtualized desktop infrastructure

Business Challenge

Like many IT organizations, Intel IT faced the challenge of how to provide different types of employees access to the Intel corporate network and compute environment without the need to deploy and maintain Intel-owned PCs. New acquisitions, offshore development centers (ODCs), and standalone subsidiaries are examples of users who are located outside of an Intel standardized environment and already have their own company-issued PC. The ability for external workers and contractors to use their PC to securely access the Intel corporate network is a great benefit for both users and Intel.

Collaboration is an important reason that provisional workers need access to Intel resources. For example, during mergers and acquisitions, transition teams may comprise workers from various businesses and corporate entities. It is critical that these people collaborate on legal documentation, roadmaps, employee and customer communications, and other important tasks. Some team members may need access to top-secret information, while others may not, making it impossible to create a one-size-fits-all solution.

To enable these workers to access Intel resources from their own PCs, we need to provide a secure computing environment while effectively managing the user experience. In the past, client-hosted virtualization (CHV) platform has helped us manage the end-to-end process by allowing bring-your-own (BYO) devices to securely access Intel resources. But CHV does not provide the best user experience because the memory capacity of non-managed PCs is beyond our control, causing potential performance issues.

As we considered alternatives to CHV that better met the needs of our users while complying with our security requirements, Intel IT evaluated and ruled out the following:

- **Virtualized desktop infrastructure (VDI).** VDI is sensitive to network conditions, especially in regions where bandwidth is poor. The user experience, especially in ODCs, was often problematic and the overall solution for a limited number of users is much more expensive.
- **Provisioned PCs.** Deploying standard Intel-deployed PCs can be more expensive and time-consuming for Intel technicians, which may result in a loss of productivity for remote users when PCs are sent in for service.
- **Web-based access.** Web-based solutions also present unique usability problems. Not all client applications include a web version. Also, many web applications do not include the full features of the native application, limiting worker productivity.

We needed a solution that was secure and easy to manage remotely, and that could be tailored to user-specific security classifications. We also wanted to enable workers to easily collaborate, be productive, and enjoy a hassle-free experience.

Solution

Intel IT designed a solution that uses an operating system that runs on a USB stick. The portable USB OS solution consists of the Microsoft Windows To Go* feature of Windows* 8 or Windows 10, a management console, and McAfee® security tools. The USB OS enables Intel IT to provide a fully secured and managed OS that can boot on any Windows or Mac* PC, even on a device that has no OS installed on it (see Figure 1). The solution is designed to utilize the host computer's native resources, enabling users to run applications on their own PCs.[1]

With McAfee security tools built into the USB image, Intel IT can deploy specific solutions based on security classifications and other user needs without compromising data on the Intel® network and other assets. The physical size of the device is also an advantage, allowing us to easily and inexpensively ship it to any location. Users no longer need to carry multiple PCs and can take the USB anywhere.

When Intel IT receives a request for remote access, we provision a USB drive with specific security requirements and appropriate access and send it to the user. When the user receives the USB drive, they boot their own PC from the USB drive and begin working.

We used self-encrypting, high-capacity portable drives that can be managed using a third-party enterprise management service. If a USB drive is lost or stolen, we can deactivate it remotely. This solution requires much less management infrastructure than VDI.

[1] This solution is not specific to media streaming and heavy CPU processes.

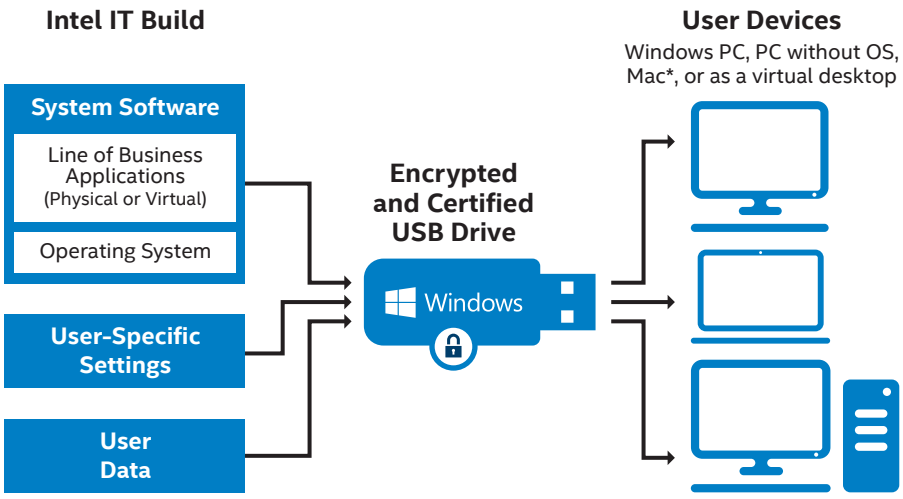


Figure 1. Using a USB OS solution that meets Intel IT's security requirements, users who provide their own PCs can securely access the Intel® network for productivity and collaboration.

Configuring the USB Windows To Go* Feature

Microsoft Windows To Go* is an enterprise feature of Windows* 8.1 and Windows 10 that creates a Windows To Go workspace. It can be booted from a USB-connected external drive on PCs that meet the Windows 7 or later certification requirements, regardless of the operating system running on the PC.

When choosing the USB OS solution, Intel IT needed the internal disks to remain offline. To help prevent data loss, internal hard disks on the host computer remain offline when booted into a Windows To Go workspace. If the USB is inserted into a running system, the Windows To Go drive will not be listed in Windows Explorer*.

Solution Benefits

The USB OS solution provides benefits to both Intel IT and the workers who use them. Users gain two main benefits:

- **Performance.** The USB drive uses the local PC resources, providing the same user experience and performance the worker is accustomed to.
- **Flexibility and portability.** The USB drive's lightweight plug-and-play design makes it easy to access the necessary Intel resources from any location.

Intel IT realizes these benefits:

- **Security.** Data on the device is encrypted using a key which is derived from the personal device password and is protected by a built-in hardware chip. The portable USB drive also includes McAfee security tools, which protect the device from malware and other potential threats as well as prevent data loss and content leaks. With Group Policy Object (GPO), we can push standard Windows security policies to connected devices automatically.
- **Manageability.** The management console allows us to remotely enforce policies on the device, such as password refresh. It also gives us the ability to disable user accounts, wipe USB drives, unlock files, and reset passwords as needed.
- **Cost effectiveness.** The USB OS solution provides an affordable alternative, whether IT issues a new PC or even a previously deployed machine to provisional employees. While deploying PCs may be the best solution in certain cases, for provisional workers who already have a PC, we can deploy a USB OS faster and at a lower cost (see Figure 2).

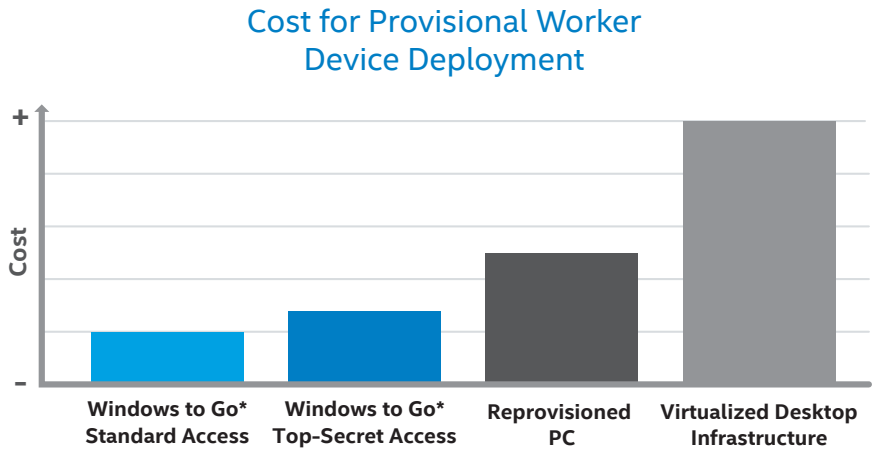
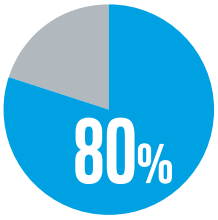


Figure 2. The total cost of deploying and managing the Microsoft Windows To Go* feature on a USB drive, even with additional security tools, is a fraction of the cost of deploying a reprovisioned PC or VDI.

Remotely Managing Data Security

To ensure that data and intellectual property are secure on something as small and portable as a USB drive, the standard Microsoft Windows To Go* solution requires additional security measures to meet Intel's security standards. Intel IT configured the USB drives to include the following security tools:

- **McAfee® Data Loss Prevention (DLP).** DLP safeguards intellectual property and ensures compliance by protecting sensitive data, which helps monitor and address day-to-day end-user risky activities such as emailing, web posting, printing, clipboards, screen captures, device control, and uploading to the cloud.
- **Windows to Go Management Console for self-encrypting, high-capacity portable drives.** This enables IT to remotely enforce policies, such as refreshing passwords, wiping lost USB drives, unlocking files, and disabling user accounts.
- **Group Policy Object (GPO).** GPO allows Intel IT to set different domain- and operating system-related security policies that enable better protection to the devices.



Positive User Feedback for the USB OS

Of the 100 responses, an overwhelming 80 percent were positive.

Pilot

In early 2016, Intel IT launched a pilot project to measure the value of the USB OS solution and gather user feedback. Our primary goals were to improve the user experience over previous solutions, such as CHV and VDI, and to maintain our security standards. In April 2016, we conducted a usability survey of 120 users who had received a USB OS. Of the 100 responses we received, an overwhelming 80 percent were positive. Users liked the familiar performance of their own PC and the ability to take the USB drive anywhere when policy allowed it. Users especially liked that problems could be resolved more quickly because they were not required to ship a PC from a remote location to IT and wait for it to come back. They stated that the plug-and-play model was easy and saved time.

During the pilot we created additional user documentation to better assist remote workers with the USB drives. During the deployment process, we learned that one technician can provision seven devices in parallel in approximately 30 minutes, significantly faster than the two hours needed for a single PC.

We identified some use cases in which workers required side-by-side computing on a given PC, such as using locally installed applications while accessing Intel resources. For example, during an acquisition, workers needed to use the same PC to run certain local applications while using collaboration tools on the Intel network. Because the USB drive's mutually exclusive boot function suppresses the native operating system, the solution did not allow users to run the USB OS and the native OS at the same time. For these use cases, we implemented a virtual-machine instance that runs from the USB. This solution requires a more powerful computer, taking advantage of Intel® Virtual Technology (Intel® VT) for the best user experience.

Next Steps

Since completing the pilot, Intel IT has deployed over 600 USB operating systems, which exceeded the number of CHV deployments. By the end of 2017, we expect to deploy approximately 1,500 USB operating systems. Based on the overwhelming positive feedback from users, we expect that the USB OS will soon become the standard solution for provisional workers, as well as some Intel employees.

Conclusion

Provisional workers need to access Intel resources for productivity and collaboration. These workers can be in remote locations, or they can be representing agencies and partners with specific projects, such as mergers and acquisitions. Deploying PCs is not always the best solution because of the added cost as well as the fact that these workers often already have their own machines. In the past, CHV and VDI solutions presented usability problems for these workers, impeding collaboration and slowing productivity.

Intel IT has designed a portable, user-friendly, and secure USB OS solution that uses the native resources on workers' PCs. The user experience provides a level of performance that matches their own PC, and IT can provide user-specific security access, prevent data loss, and manage the devices remotely. The solution costs a fraction of what it takes to deploy a company-owned PC and users are happier not carrying multiple laptops, thus increasing productivity.

For more information on Intel IT best practices, visit **intel.com/IT**.

Receive objective and personalized advice from unbiased professionals at **advisors.intel.com**. Fill out a simple form and one of our experienced experts will contact you within 5 business days.

IT@Intel

We connect IT professionals with their IT peers inside Intel. Our IT department solves some of today's most demanding and complex technology issues, and we want to share these lessons directly with our fellow IT professionals in an open peer-to-peer forum.

Our goal is simple: improve efficiency throughout the organization and enhance the business value of IT investments.

Follow us and join the conversation:

- Twitter
- #IntelIT
- LinkedIn
- IT Center Community

Visit us today at **intel.com/IT** or contact your local Intel representative if you would like to learn more.

Related Content

If you liked this paper, you may also be interested in this related story:

- IT@Intel Enabling BYOD with Application Streaming and Client Virtualization White Paper

Printed in USA Please Recycle 0217/JGLU/KC/PDF