

Mobile *and* Secure – It Can Be Done

Information security should protect to enable – providing security for personally owned devices while enabling Federal employees to be mobile and productive.



IT@Intel Federal Insights
Key Learnings from the Private Sector
Mobility and Security
June 2014

The use of personally owned devices in the workplace is a significant trend that transcends the boundaries between the public and private enterprise sectors.

What has a presence in more than 100 countries, a large and highly mobile workforce, and a commitment to maintaining a maximum level of information security? If you answered “the U.S. Federal Government,” you’d be right; but another correct answer is “large enterprises such as Intel.” Both are experiencing a burgeoning of the consumerization of IT as well as increased focus on security.

The use of personally owned devices in the workplace is a significant trend that transcends the boundaries between the public and private enterprise sectors. Even after the Office of Management and Budget published the Toolkit¹ for implementing a BYOD program in August of 2012, Federal agencies have been challenged to develop an overall process that preserves the same level of security.

Intel IT chose to embrace BYOD because of the significant benefits to the organization

and employees. For example, allowing employees to use their own devices enables them to work on more familiar platforms and thus increase their productivity. However, in addition to the benefits, Intel also needed to protect data and intellectual property. A methodical, well-planned approach to BYOD helped Intel IT realize the benefits of mobility while maintaining the same level of information security.

This approach included evaluating mobility solutions and ensuring connectivity was adequate for new mobile usage models (see Figure 1). With these two steps complete, Intel IT has deployed BYOD on a large scale.

This same approach, along with guidance from the National Institute of Standards and Technology (NIST)², can help agencies that have yet to implement BYOD while still meeting their stringent policy and information security requirements.

To learn more, contact your Intel account manager,
or visit intel.com/federal >

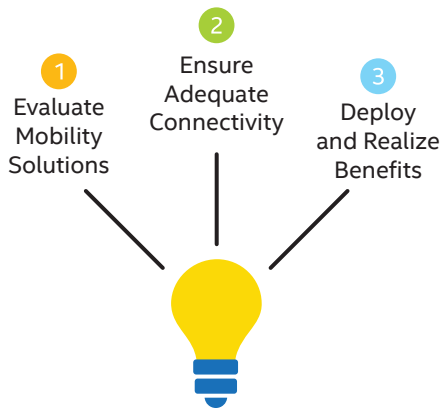


Figure 1. A well-planned approach to BYOD can help realize the benefits of mobility while maintaining the same level of information security.

Evaluate Mobility Solutions

Consumerization of IT—employees using their personal devices to access data at work—is not a passing trend. Offering a BYOD program can increase employee productivity and help reduce the likelihood of unsecured devices accessing the network.

Federal agencies can use the same techniques Intel IT did to identify the unique security challenges associated with BYOD and define the requirements of an IT consumerization policy. These tasks involve close collaboration with the Legal and Human Resources (HR) departments. Information security risks can be mitigated with technology, employee agreements, and employee training and awareness programs. To learn more about how Intel IT has successfully embraced BYOD go to www.intel.com/federal and search for “Granular Trust Model Improves Enterprise Security.”

Consumerization of IT has moved beyond smart phones to also include tablets. Based on an ecosystem review and a

hands-on product evaluation, Intel IT has determined that Intel® architecture-based tablets (Intel® Atom™ processor-based tablets and Intel® Core™ vPro™ processor-based tablets) running Windows* 8 can enhance information security associated with small form factor devices. These evaluations indicate that the combination of Windows 8 and Intel architecture offers flexible device management, alternative authentication options, and support for legacy applications (see Figure 2). For more information about these evaluations, go to www.intel.com/federal and search for “Evaluating Microsoft Windows 8 Security on Intel® Architecture Tablets.”

Ensure Adequate Connectivity

To take advantage of the consumerization of IT and better manage the proliferation of smart phone use, Federal agencies should develop a roadmap for connecting smart phones to the Wi-Fi* network. This roadmap should take into account advances in smart phone technology such as better encryption, network authentication, and other important

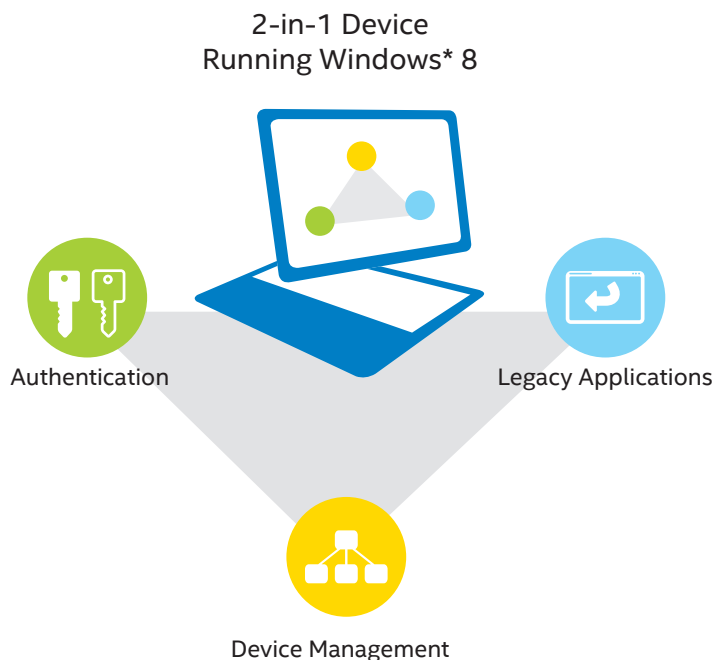


Figure 2. The security and manageability capabilities of Intel® architecture-based 2-in-1 devices and tablets can help mitigate the risks of a BYOD environment.

security and manageability requirements. In addition, agencies should also plan to accommodate additional devices such as tablets and 2-in-1 devices.

Enabling smart phones to connect to an agency's Wi-Fi network offers several advantages over using the cellular network:

- Avoidance of costly cellular usage fees
- More reliable voice reception and coverage, supporting enhanced mobility and productivity
- Faster and more reliable data transmission

In the future, the Federal workplace will comprise multiple devices per employee and advances in device technology that will require more bandwidth and connectivity options. To stay ahead of demand, agencies should evaluate their network architecture and consider new networking technologies that are easier to deploy with lower cost.

For more information about how Intel IT approached Wi-Fi connectivity for personal devices, go to www.intel.com/federal and search for "A Roadmap for Connecting Smart Phones to the Intel Wi-Fi Network" and "Evolving the Mobile Employee Hotspot for IT Consumerization."

Deploy and Realize Benefits

Evaluating the available technology and laying a solid groundwork for security and success can help Federal agencies confidently deploy BYOD solutions. For an overview of Intel IT's best practices for BYOD smart phone deployment, go to www.intel.com/federal and search for "Best Practices for Enabling Employee-owned Smart Phones in the Enterprise." You can also search for "Deploying Windows 8 on Intel® Architecture-based Tablets: Intel's Approach" to get information about how Intel IT has expanded BYOD to tablets.

Android* devices provide an excellent example of how, with planning and the appropriate technology, it is possible to support BYOD securely. Intel IT has added Android-based devices to the network by adapting the same BYOD best practices developed for other devices, enabling employees to access their email, calendar, and contacts using the native applications on their Android devices. For more information on BYOD with Android devices, go to www.intel.com/federal and search for "Android Devices in a BYOD Environment" and "Enabling Native Email, Calendar, and Contacts on Android Devices."

Intel IT and Intel employees have reported the following benefits of the BYOD program:

- **Increased productivity** – up to 57 minutes per day.
- **Improved flexibility** – sending millions of work-related email messages each quarter from corporate and personal handheld devices.
- **User satisfaction** – exceeding 90 percent among users of personally owned devices.
- **Relatively low cost to IT** – employees usually pay for the service plans, so the cost of adding new devices is low.
- **Minimal impact on IT support** – Intel Help Desk tickets related to handhelds has not increased significantly, despite the addition of more than 40,000 personal devices. Averaged across all corporate and personal handheld devices, the number of tickets per user has actually decreased.

By following the practices that Intel IT has developed for their BYOD program, Federal agencies can experience similar benefits.

To learn more, contact your Intel account manager, or visit intel.com/federal

¹ Bring Your Own Device: A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs, August 23, 2012; www.whitehouse.gov/digitalgov/bring-your-own-device

² Guidelines for Managing the Security of Mobile Devices in the Enterprise, June 2013; http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf


INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

Copyright © 2014 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel Atom, Intel Core, vPro, Look Inside., and the Look Inside. logo are trademarks of Intel Corporation.

*Other names and brands may be claimed as the property of others.

Printed in USA

0614/SLIO/KC/PDF

 Please Recycle

