Flexible Workstyles and Enterprise IT
Supporting the Consumerization of IT with an Intelligent Infrastructure

January 2012
www.microsoft.com/workstyle
CONTENTS

Contents .........................................................................................................................3

Executive Summary .................................................................................................1

Introduction .................................................................................................................2

The Evolving Enterprise: Consumer Technology, Flexible Workstyles 3
Accelerated Device Innovation and Mobility ...............................................................3
Embracing the Trend ....................................................................................................3
The Challenge: From Device-Centric to User-Centric IT ..........................................4

Microsoft: Providing Flexible Workstyles Using Intelligent Infrastructure ..........5
Providing an Optimized Application Infrastructure ......................................................5
  Device-Optimized Applications ..............................................................................5
  Web Applications ..................................................................................................6
  Virtual Desktops and Applications ........................................................................6
Unified Management On-Premises and from the Cloud ..............................................7
  User-Centric Application Delivery ........................................................................8
  Unified Asset Inventory ..........................................................................................8
  Unified Settings Management ................................................................................9
Cloud Management of Devices Running Windows .......................................................10
End-to-End Security and Access ..............................................................................10
  System Integrity and Device Encryption ................................................................10
  Antimalware Software ............................................................................................11
  Access ....................................................................................................................11
  Information Protection ............................................................................................12

Conclusion .................................................................................................................13
EXECUTIVE SUMMARY

More enterprise organizations every day face the question of how to deal with the large and growing presence of consumer devices users bring to work. This “consumerization of IT” is both a logical and irreversible trend that stems from technology advances in consumer hardware, ubiquitous information access, and the blurring of the lines between work and personal lives. Microsoft believes organizations should embrace this trend, and provides products and technologies to help support today’s modern workstyles.
INTRODUCTION

The influx of consumer-oriented technology into the enterprise, including smartphones, tablets, and user-owned laptops, has gone from a trickle to a steady and virtually unstoppable flow in the space of just a few years. IT professionals today are facing challenges that can’t be addressed adequately by policies and paradigms designed for the workplace of 5 or 10 years ago.

Microsoft recognizes the consumerization of IT as an important transformational force, and believes that organizations should embrace it for the benefit of both the users and the enterprise. To assist IT departments in managing their evolving environments, Microsoft provides a range of solutions that can help with tasks such as identifying non-corporate devices, establishing and enforcing policies, delivering applications and data with the best-possible user experience, and maintaining security.

This paper provides a brief overview of how the consumerization trend has accelerated over the past several years and how that trend is both spurring and supporting the more flexible, modern workstyles preferred by today’s users. This paper looks at the benefits and challenges of consumerization, including the need for IT departments to consider a more user-centric approach to client management instead of an outdated device-centric approach. The paper also provides details on how Microsoft solutions can help IT departments support flexible workstyles by optimizing the application infrastructure, providing unified management, and supporting modern security and access models.
Only a few years ago, it was unusual or even forbidden in most organizations for users to bring personal devices to work for business-related tasks. IT professionals were justifiably concerned about the potential problems that these consumer devices could cause in the workplace, such as drains on IT resources, unauthorized access to sensitive information, and the likelihood that malware could be easily introduced into the network.

However, the workplace culture is changing rapidly, and so are the tools that employees need to get their jobs done. Several factors are driving these changes.

**Accelerated Device Innovation and Mobility**

First, there is the accelerated pace of technology innovation in the consumer market. Remarkable advances in hardware appear on the market regularly, contributing to the allure and prevalence of powerful, compelling devices. People are increasingly mobile and expect to have access to information, and to be productive, from anywhere. They are also accustomed to accessing social networks, such as Facebook and Twitter, to stay in touch with others and share information about both their personal and professional lives.

The combination of consumer-device prevalence and ubiquitous information is changing the way that people perceive their technology, and how that technology shapes their personal and work lives. The constant use of information technology throughout the day, along with the easy access of information, is blurring traditional boundaries between work and home life. These shifting boundaries are accompanied by a belief that personal technology—selected and customized to fit user’s personalities, activities, and schedules—should extend into the workplace.

**Embracing the Trend**

The consumerization of IT will likely continue across the enterprise. Many workers typically own multiple devices, and often bring their devices to work. Often they believe that their technology is superior to what their employer provides, or they simply want to use the same technology at work that they are accustomed to in their personal lives. Regardless of the specific reasons, the bottom line is that the growth of consumer devices in the enterprise is a real and growing part of daily corporate processes.

Users want their own devices at work, and if they face restrictions, the chances are good that they’ll find ways to circumvent these barriers. Worse, they might try to find an employer that will support their preferred workstyles.
By embracing the trend, organizations can turn what used to be perceived as a loss of control into a benefit for everyone. Giving users complete or even partial freedom to choose their own devices can help boost morale and productivity. Offering this freedom to choose technology at work could even be a differentiator for employers who are competing for qualified job candidates.

**The Challenge: From Device-Centric to User-Centric IT**

Accommodating the trend of consumerization entails a variety of challenges. Chief among these is changing how the organization thinks about client computing. Historically, policies and process were almost always focused on the device; however, the number and variety of devices were far smaller. Consumerization of IT increases device diversity and volume in the enterprise, and brings more consumer devices that are replaced more frequently. In this scenario, device-centric management becomes more challenging for IT administrators.

The best way for organizations to respond is to have IT policies that match business realities and priorities, moving toward a user-centric model that replaces the older paradigm of device-centric policies and management. This shift in focus requires policies and processes that give users far more freedom to select the devices they want to use, while maintaining access to applications and data regardless of the device.

To execute that vision, IT professionals need to carefully plan and manage an environment that supports users and the organization in three essential areas. First, they have to provide easy access to applications and data so that users can remain productive. Next, they need to implement technologies and procedures to manage disparate devices. Finally, they need to establish security measures that will protect the organization’s systems, data, and network.

The next section looks at these areas in more depth, including how Microsoft provides solutions that address these issues and, in the process, helps organizations support flexible workstyles in the enterprise.
MICROSOFT: PROVIDING FLEXIBLE WORKSTYLES USING INTELLIGENT INFRASTRUCTURE

Microsoft has a history of providing rich IT-infrastructure solutions to help manage every aspect of enterprise operations. The current set of Microsoft management solutions expands this history with products and technologies that can help IT departments deal with the influx of consumer-oriented technology and the workstyle expectations of users.

The following sections illustrate how Microsoft management technologies can address key scenarios for supporting flexible workstyles.

Providing an Optimized Application Infrastructure

Users need applications to get their work done. Providing an optimized application infrastructure for users equipped with a range of devices is central to ensuring productivity.

There are different methods to accomplish this. Each method has advantages that stem largely from the type of device a user has, the user’s role and responsibilities within the organization, and how the user is accessing an application—that is, what kind of connectivity is available. The types of application infrastructure include device-optimized applications, web applications, and virtualized desktops and applications. The following sections provide more detail on how Microsoft products support these application access models.

Device-Optimized Applications

Device-optimized applications are designed for a specific device or group of devices. The advantage for users is that device-optimized applications provide a rich, full-featured experience, including appearance and performance features that are supported by device-based storage and processing. These applications can be customized to fit the processing power, screen size, and input capabilities—such as touch screen or physical QWERTY keyboards—of particular devices. However, device-optimized applications, like their desktop counterparts, require deployment, maintenance, and upgrade processes.

A great example of a device-optimized application is Microsoft Office Mobile. this version of Microsoft Office give users of Windows Phone devices access to the same familiar productivity applications they have on their desktops, including Microsoft Word, Excel, PowerPoint, OneNote, Outlook, and Microsoft Lync. These mobile versions are optimized for devices with a smaller screen, touch input, and constant network connectivity.

When planning an organization’s application infrastructure, device-optimized applications typically result in the best customer experience. However,
investments in testing, migration, deployment, and maintenance need to be considered.

**Web Applications**

If ubiquitous access is the primary requirement, then web applications that are available through the Internet are an ideal solution. The majority of consumer devices on the market today are equipped with web browsers, and in most situations it is relatively easy for a user to get on the Internet by using a smartphone, tablet, or laptop. However, the user experience can vary depending on latency issues and the fact that web applications are not tailored to individual devices, which can affect the appearance and overall performance of some applications.

Microsoft supports the web-application experience with a number of cloud-enabled products. Key among these is Microsoft Office 365, which provides security-enhanced access to email, shared calendars, instant messaging, video collaboration, and document creation and collaboration. Office 365 includes the Office productivity suite, with web-application versions of Word, Excel, OneNote, PowerPoint, and Outlook. It also includes enterprise services that support communication and collaboration. These include Microsoft Exchange Online for email, Microsoft SharePoint Online for group collaboration and document sharing, and Microsoft Lync Online for communications using tools such as instant messaging, video calls, and online meetings.

Creating a web-based application infrastructure can provide ubiquitous access. It also requires that devices have standards-compliant browsers to ensure a consistent, easy-to-maintain, and continuously up-to-date application experience. The downside of web-based applications is that device-specific capabilities are not maximized, leading to a user experience that can be less than optimal. Additionally, continuous Internet connectivity is usually required and might be an issue in some remote locations.

**Virtual Desktops and Applications**

Virtual desktops and applications are the best option if you need a consistent application experience for users, in addition to application-version compatibility.

Microsoft provides a comprehensive set of technologies through Microsoft Desktop Virtualization that help organizations provide users with the flexibility to access applications virtually anywhere on a range of devices, while simplifying compliance and management through a centralized and unified infrastructure.

The Microsoft Desktop Virtualization portfolio offers an array of virtualization options that streamline the application experience for users and provide management tools for IT administrators.

Several key features in the Microsoft Desktop Virtualization offering benefit users. For example, Microsoft Application Virtualization (App-V) provides anywhere, anytime access to corporate applications from virtually any authorized device,
without the need to install the applications locally. With App-V, applications are deployed and maintained on a central server, giving users access to the full range of an application’s functionality while eliminating the time and resources traditionally needed to install, maintain, and update locally installed applications.

Users might appreciate the experience of RemoteApp, which lets remotely accessed applications appear as if they are running on the user’s local device. Instead of being presented to a user in the “desktop” of a remote session, the RemoteApp program runs in its own resizable window, can be dragged between different monitors, and has its own entry in the Windows taskbar.

When users are mobile, they can benefit from Microsoft User State Virtualization (USV), which keeps user data and settings on a centralized server. This alleviates the constraints of using local (client-based) computing resources, such as storage, while giving users access to the applications and data that help them do their jobs. Users can access their folders from any location or device after logging on and can work with files in offline situations.

The Microsoft Desktop Virtualization portfolio also includes a number of technologies that support rich application access. Delivering session-based desktops is easy using Microsoft Remote Desktop Services (RDS) Session Virtualization. IT administrators can use Microsoft Virtual Desktop Infrastructure (VDI) to provide access to personalized, server-hosted desktops that can run in a virtual machine on remote devices. A similar functionality can be achieved for older operating systems and applications, such as Windows XP and Internet Explorer 6 or Internet Explorer 7, with Microsoft Enterprise Desktop Virtualization (MED-V). MED-V is used to deploy virtualized legacy systems onto modern platforms for legacy application compatibility. Finally, application integration with System Center provides a rich, unified solution for managing both physical and virtual environments.

Microsoft Desktop Virtualization solutions provide a consistent way to access applications with a familiar user experience. These solutions are optimized for compatibility and increased security. However, the Microsoft Desktop Virtualization solutions are not optimized for specific devices, especially smaller mobile devices that lack the traditional input capabilities found on a laptop or PC. Organizations should invest in this infrastructure for legacy-application access and to service users who do not need a full-featured, traditional desktop.

**Unified Management On-Premises and from the Cloud**

Once application infrastructures are enabled, providing access to those applications on the devices is the key to enabling flexible workstyles. The tool an IT administrator chooses to use to manage the proliferation of consumer devices within the organization will affect the IT management experience. Microsoft provides several products that support key management tasks, including deploying applications, asset inventory, and configuration settings management on-premises and from the cloud.
User-Centric Application Delivery

System Center 2012 Configuration Manager makes it easy to establish a user-centric application delivery model. IT administrators can use Configuration Manager to deploy full Office installations to desktops and App-V versions of applications to virtualized desktops. Configuration Manager uses variables such as user identity, application dependencies, and network and device characteristics to dynamically determine the appropriate deployment type for a specific device.

A user-centric approach lets IT administrators deploy an application to a user, regardless of the devices used. When a user brings a new device into the enterprise, Configuration Manager can help deploy the appropriate applications to that device without requiring an administrator to manually push those applications.

Case Study: Ministry of Foreign Affairs of Denmark

The Ministry of Foreign Affairs of Denmark has 2,500 employees in 105 embassies, consulates, and trade offices around the world. The IT staff, based in Copenhagen, manages 5,000 devices, including desktop and portable computers, servers, and smartphones. To improve efficiency and move to a user-centric computing model, the ministry IT staff uses Microsoft System Center 2012 Configuration Manager for self-service application deployment, streamlined mobile-device management, and efficient management of organization infrastructure. The IT staff uses Configuration Manager to apply security updates to mobile devices, achieving an unprecedented 90 percent update rate and enhanced security for the ministry’s far-flung IT infrastructure.

Case Study: New York City Department of Education

The New York City Department of Education—the largest public school system in the nation, with 1.1 million students and an annual budget of $24 billion, needed a systems management solution to centrally manage common IT tasks. It decided to implement Microsoft System Center 2012 Configuration Manager and enable self-service software provisioning. Now, two IT administrators can centrally manage clients and easily handle a workload that used to require 60 employees traveling around the city. The organization has reduced the time and money required for IT personnel to travel to schools, and it has gained comprehensive visibility into IT assets and has improved service level response.

Unified Asset Inventory

One of the biggest concerns facing administrators is the need to capture and analyze all assets connected to corporate resources. Configuration Manager provides IT administrators with a comprehensive view to identify and inventory mobile, physical, and virtual assets. This improves your ability to map devices to users, which aides in implementing user-centric policies and deploying applications to users. It also delivers an advantage over other solutions that might offer information on mobile devices and virtual and physical assets, but through different management consoles that make it more difficult to get the complete picture.
To bring mobile-device asset inventory into the same console, Configuration Manager uses Microsoft Exchange ActiveSync (EAS) to automatically pull data from Exchange when users log on to check email. Information such as the device’s hardware ID and operating system and the user ID is delivered through EAS, recorded, and available in the same standardized reports used for traditional desktop and laptop inventories. This gives administrators the ability to see the complete collection of devices used by particular users, from their smartphones and laptops to tablets and desktop PCs. The result is a single platform that administrators can use to inventory Windows, iOS, Android, and other EAS-compliant devices.

Configuration Manager is also "virtualization aware," so administrators can conduct inventories on virtual desktops and virtual sessions. The improved virtualization support in Configuration Manager helps you to consistently treat virtualized environments in a dedicated manner without "ghost asset" issues and duplication that can plague non-virtualization-aware management solutions.

Configuration Manager remains a useful tool for pulling hardware and software inventory information from traditional devices, like laptops and desktops. More advanced capabilities, such as licensing information and software metering, are also available to help you track usage of applications within the organization.

**Unified Settings Management**

Configuration Manager allows consistent settings across a diverse range of devices. Configuration Manager provides a unified interface that helps IT administrators manage the configuration and compliance of a full range of enterprise devices, including servers, laptops, desktop PCs, and mobile devices. The compliance settings tool in Configuration Manager helps administrators assess the compliance of users and client devices in relation to any number of configurations. For example, determine whether the correct Windows operating system versions are installed and configured appropriately, whether required applications are installed and configured correctly, and if a user has installed prohibited applications. Administrators can also check to see if laptops are in compliance with software updates and security settings.

Configuration Manager, using EAS, also lets administrators push basic policies such as PIN/password and remote wipe to specific user devices. Because Configuration Manager is virtualization aware, it is possible to deploy policies that either exempt or specifically target virtual desktops. This is important to prevent issues such as overloading physical hardware with synchronized policy tasks, also known as VDI storms. Configuration Manager automatically randomizes tasks to prevent overloading of physical hardware in a virtual environment.

Another tool to assist with unified settings management is Microsoft Advanced Group Policy Management (AGPM), part of the Microsoft Desktop Optimization Pack (MDOP). With AGPM, administrators can access functions such as policy
versioning, rollback, and views of resulting policy changes to help manage enterprise devices more efficiently through Active Directory Domain Services.

**Cloud Management of Devices Running Windows**

Microsoft also provides Windows Intune, a lightweight, cloud-based solution hosted and maintained by Microsoft. Windows Intune is designed for businesses that need the essentials of management and protection and want access to the latest version of Windows. It can also deploy software, software updates, and malware protection, in addition to performing inventories on devices running Windows.

Windows Intune is a good option for organizations with fewer than 5,000 devices and access to high-bandwidth connections. It offers management of Windows without a larger infrastructure investment, along with access to the latest versions of Windows in a predictable, subscription-based billing model. Typical scenarios for using Windows Intune might include managing devices for employees who work from home or from coffee shops, or field and contract employees. Organizations can also use Windows Intune in scenarios with large numbers of personnel who are constantly on the road, such as sales employees, or in situations where there is a large influx of new employees as a result of a merger or acquisition.

**End-to-End Security and Access**

With a management and application infrastructure in place to help support the IT consumerization trend, the last major focus area is providing end-to-end security and access for employees. Without security and access, the promise of flexible workstyles cannot become a reality in the modern workplace. Microsoft provides end-to-end solutions for system integrity and device encryption, antimalware software, access, and information protection.

**System Integrity and Device Encryption**

Configuration Manager can be used to deploy operating systems with Microsoft BitLocker Drive Encryption, a data protection feature available in enterprise editions of Windows Vista and Windows 7 that reduces the threat of data exposure due to lost, stolen, or inappropriately decommissioned computers. With Bitlocker installed on a device, Microsoft BitLocker Administration and Monitoring (MBAM), part of MDOP, can be used for provisioning, deploying, and recovering BitLocker-enabled mobile and remote devices running Windows.

For devices with Windows and third-party devices, administrators can use Configuration Manager and EAS to enforce encryption of devices using EAS. Some EAS-compliant platforms also provide the ability to encrypt devices for an added level of security. This is especially important on mobile devices, which are more prone to loss or theft.
**Antimalware Software**

There are a variety of tools available to protect the organization against malware. Windows Defender is built into consumer and enterprise editions of Windows. Microsoft also provides Microsoft Security Essentials, a free security software product geared for consumers and small businesses to help secure devices running Windows against the threat of malware.

In a corporate environment, System Center 2012 Endpoint Protection provides antimalware protection for laptops, desktops, and virtualized environments. It helps protect devices running Windows against the threat of malware with the added benefit of cost savings through reduced infrastructure. Eliminating the duplicate infrastructure for antimalware software and systems management can save thousands of dollars each year, depending on organization size.

Having management and security functionality in the same console provides a number of benefits, such as a better correlation between malware protection and the update state of a specific machine. Because device infections are often a result of user computing habits, Configuration Manager and Endpoint Protection help IT administrators to easily determine which users are most prone to malware and target those users with additional training to help reduce the likelihood of infection.

**Access**

Rapid turnover in consumer devices means the organization will constantly face the challenge of providing access to employee devices. The best way to accommodate modern workstyles is by using DirectAccess and Internet Protocol Security (IPSec) domain isolation.

IPSec domain isolation ensures that only trusted devices can access back-end corporate resources. If a device does not have the required certificate to pass IPSec authentication, it will fail to establish a network connection to corporate resources and will be required to communicate through a proxy device in a quarantined virtual network.

In this scenario, Windows-based devices that have a trusted certificate can establish network communication with other trusted devices. This provides ubiquitous access to corporate resources on the intranet.

When these Windows-based devices are outside the organization, DirectAccess helps remote users securely access enterprise shares, websites, and applications without the need to connect to a VPN. This “always on” form of access provides bi-directional, secured corporate access without having to go through extra steps to connect. A key benefit to this is the availability of “split-tunneled” Internet access and simultaneous secured corporate connectivity when users are traveling, which reduces corporate bandwidth costs when compared to a traditional VPN.

Because DirectAccess is bi-directional, Windows devices can be managed as if they were connected on the local network, improving security.
Information Protection

When devices are secured and access policies are in place, the IT department should ensure that sensitive data is protected. Microsoft provides protection for information using Active Directory Rights Management Services (AD RMS).

AD RMS helps administrators employ persistent, identity-centric usage policies and encryption that is embedded with data. With this technology, users can, for example, use a Windows-based PC, slate, or Windows Phone 7.5 device to send an email or work on an Office 2010 document stored on SharePoint while use rights and data encryption are maintained. AD RMS works on a range of platforms, and helps IT administrators to create granular use rights, such as “Read Only,” “Do Not Forward,” or “Cannot Copy.” These rights stay with the documents and data so if a user’s phone is lost or stolen, or if the user inadvertently sends a protected document to a third party, that information is protected and cannot be viewed by an unauthorized person.
CONCLUSION

The consumerization of IT is a large and growing trend in enterprises. Organizations that recognize the trend and view it as a positive development can develop some clear goals to accommodate the flexible workstyles that characterize the prevalence of consumer-oriented devices in the workplace.

By supporting flexible workstyles, organizations can balance the needs and demands of users who want to bring their personal devices to work, giving them the applications they need to be productive while protecting the information that helps run the enterprise.

Microsoft supports and enables the consumerization of IT and the associated flexible workstyles. With an intelligent infrastructure built on Microsoft technologies, organizations can provide easy access to applications and data so users can remain productive. With the Microsoft tools, IT professionals can implement technologies and procedures to manage disparate devices. They also have the tools to protect the organization’s systems, data, and network.

For more information about flexible workstyles and creating an intelligent infrastructure to support them, please see the following resources:

- **Flexible Workstyle**  
  [www.microsoft.com/workstyle](http://www.microsoft.com/workstyle)

- **Microsoft Desktop Virtualization**  
  [www.microsoft.com/dv](http://www.microsoft.com/dv)

- **Microsoft System Center**  
  [www.microsoft.com/systemcenter](http://www.microsoft.com/systemcenter)

- **Windows Intune**  
  [www.microsoft.com/intune](http://www.microsoft.com/intune)

- **Microsoft Desktop Optimization Pack**  
  [www.microsoft.com/mdop](http://www.microsoft.com/mdop)

- **Springboard Series** (technical resources and tools for deploying the Microsoft Optimized Desktop)  
  [www.microsoft.com/springboard](http://www.microsoft.com/springboard)