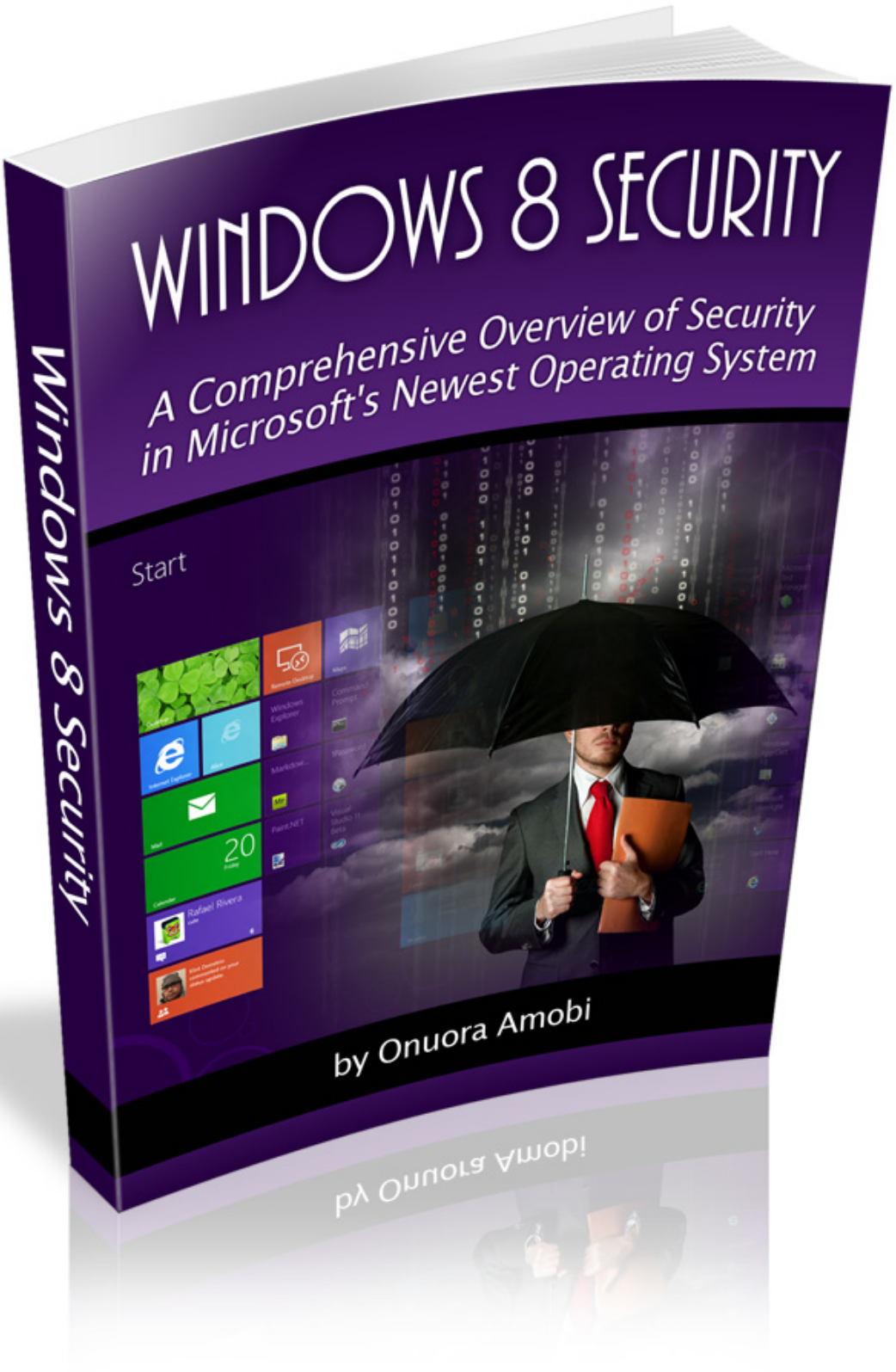


Copyright Notice

Nnigma Inc.

3579 East Foothill Blvd, Suite #254

Pasadena, CA 91107

www.Nnigma.com

Legal Notice

While all attempts have been made to verify information provided in this publication, neither the author nor the publisher assumes any responsibility for errors, omissions or contradictory interpretation of the subject matter herein.

This publication is not intended to be used as a source of binding technical, technological, legal or accounting advice.

Please remember that the information contained may be subject to varying state and/or local laws or regulations that may apply to the user's particular practice.

The purchaser or reader of this publication assumes responsibility for the use of these materials and information.

Adherence to all applicable laws and regulations, both federal, state, and local, governing professional licensing, business practices, advertising and any other aspects of doing business in the US or any other jurisdiction is the sole responsibility of the purchaser or reader.

Nnigma Inc. assumes no responsibility or liability whatsoever on behalf of any purchaser or reader of these materials.

Table of Contents

Introduction

Everyone is talking about Windows 8. Even now, after the first few waves of media hype, interest in this operating system continues.

As an IT professional, you are quite possibly being asked to review Windows 8 and determine if it is a good fit for your organization. Or, you are being asked to implement Windows 8 or develop a transition plan that moves your organization's systems from their current operating system to Windows 8 over time.

Other than the interface, which is of course the focus of the user experience, Windows 8 comes with increased security features designed to make your life as an IT professional easier. These features are supposed to enhance security and give you enhanced tools for support and protection.

Does Windows 8 deliver on this promise?

Windows 8 security is designed with three goals in mind. First, it seeks to protect your network from threats and disruptions created by hackers, malware, and programs designed to wreak havoc on your system.

Second, Windows 8 security is designed to protect sensitive data within your system. This protection includes threats outside your organization as well as data restriction within your organization.

Third, the security of Windows 8 is designed to provide secure access to your network's resources so users can work safely and productively.

We will look that the enhanced security features of Windows 8. We will also highlight issues and concerns that you need to understand as you set policies for system use and administer Windows 8 on your network.

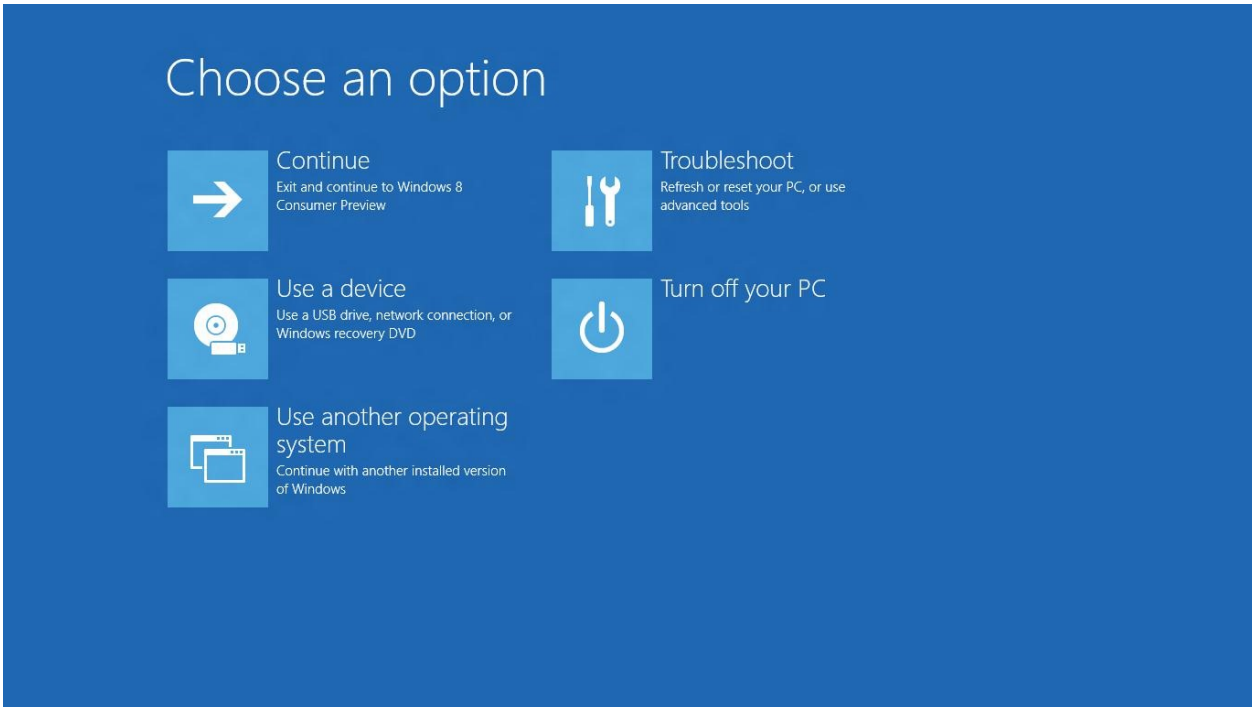
I hope you have as much fun reading this as I had writing it.

Onuora Amobi,

Editor,

Windows8update.com

Windows8enterprise.com



UEFI – Secure Boot

With Windows 8 Microsoft is requiring adoption of a boot solution called United Extensible Firmware Interface (UEFI). UEFI changes the start-up procedure for a computer system, known as a boot or booting and is required on all PCs using the Windows 8 operating system.

UEFI replaces the traditional BIOS system used by PCs. UEFI helps productivity by creating much faster boot times. The handoff from power on to operating system is somewhere around 8 seconds. UEFI also aids productivity by requiring fewer restarts. This keeps your office staff working and saves IT time when applying upgrades or installing software. At least this is the promise.

The most important benefit of UEFI for your organization is security. UEFI is effective at battling rootkits, a class of malware frequently used by hackers to open a backdoor and allow criminals to control a PC.

A rootkit replaces the code used to start a computer within itself and disables antivirus software. UEFI makes loading rootkits difficult by requiring the initial boot up code to be digitally signed with a certificate derived from a key in the WEFI firmware. This feature, known as Secure Boot, ensures that code is from a trusted source prior to loading.

UEFI then leverages Early Launch Anti-Malware (ELAM) to protect against boot loader attacks. ELAM allows anti-virus software to start up prior to other forms of programming. This ensures programs are scanned for viruses prior to start up.

Secure Boot uses three databases. The signature database and contains signatures and hashes of images for UEFI applications and operating system loaders. The revoked signatures database contains images that are revoked or have been marked as untrusted by the system. The Key Enrollment Key database contains keys that can be used to sign updates to the signature and revoked databases.

These databases are put in place when the computer is manufactured. Changes to them are prevented unless the change is signed with the correct signature. In the UEFI Secure Boot process, these databases are used to keep non-trusted software from taking control of the boot process.

These improvements increase the operating system's ability to detect malware before it has a chance to load and run. It also makes it difficult for users to unknowingly install malware in the first place. So UEFI will add a level of protection to your organization, right? Maybe.

Critics and analysts feel that the UEFI platform is still vulnerable to attack. If the Secure Boot technology is turned off, which It must be to allow partitioning and running other operating systems such as Linux alongside Windows 8, then the system is just as vulnerable as BIOS or maybe more so.

Malware is not a stagnant threat. Eventually malware writers will overcome UEFI technology. At this time, however, Windows 8 offers the highest level of security for your organization.

One of the drawbacks of the UEFI or Secure Boot feature is the limitations it presents when you want to install an operating system other than Windows 8 or create partitions within your system. In the past, operating systems have included information on how to disable Secure Boot. This information is not included in Windows 8, although it is possible.

Dynamic Access Control

Tired of maintaining groups in Microsoft Active Directory? If you aren't now, you may soon be with the movement of many organizations to enact BYOD (Bring Your Own Device) policies and use cloud services as a part of their business plan. How do you give everyone access where they need it while making sure sensitive information stays protected? Securing files using folders or shares governed by group policy within the file server is an increasingly complex process.

Dynamic Access Control is Microsoft's answer to this need in the IT world. The idea behind DAC is integrating claims-based authentication using tokens. Users are described by attributes such as department, location, role, title, and security clearance rather than by the security groups they are assigned to. This is a powerful new way to control access and allows flexibility in an increasingly complex data management environment.

Dynamic Access Control works by using a concept of central access rules and central access policies along with claims. Claims are the unique data points that describe the users, devices, or resources involved in the request. For example, a user might have access to a certain file when in the office. That same access may be restricted, however, when the user is traveling due to the sensitive nature of the data or lack of security availability on the user's mobile device.

DAC includes Rights Management Services (RMS) allowing files that are defined as sensitive to be encrypted when they are moved from the file server. You can, for example, encrypt all

documents that contain HIPAA information, vital organizational secrets, or other sensitive data just by applying RMS to documents of that kind.

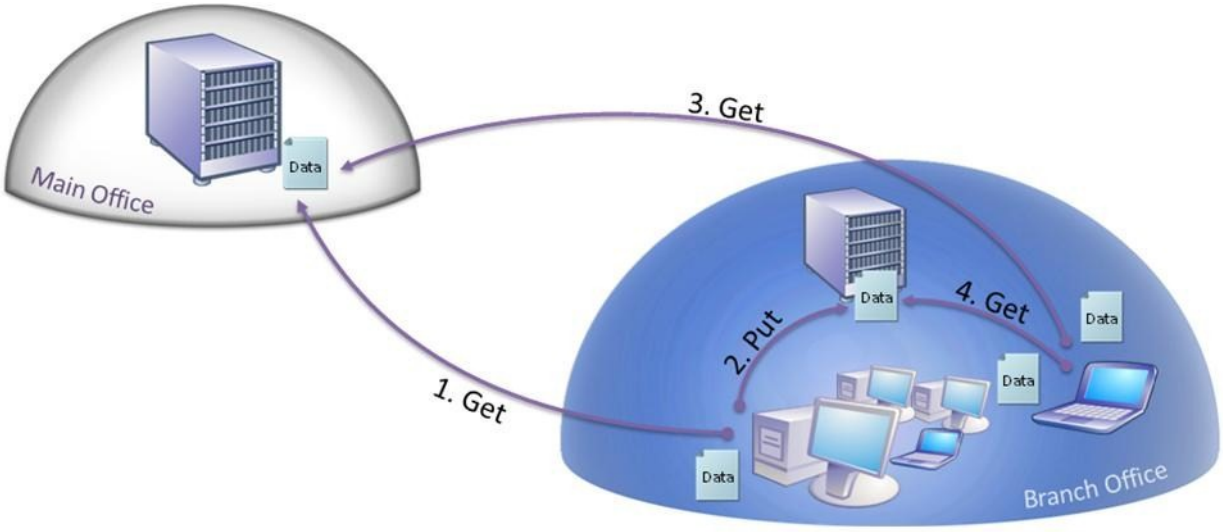
The power of DAC is the ability to tag data, classify it, and apply access control to the data along with automatic encryption when the data is defined as sensitive. It reduces the constraints on IT and allows application of dynamic policies at the resource level. You can make decisions without dealing with a static system of protections that limit your flexibility.

Basically, the DAC allows you to reduce the need for extra active directory groups. It accomplishes this by allowing an "and" function rather than just an "or" function. Here's an example. If a manager in your remote office needs access to a group of files for another remote office, you can simply allow them permission by adding them to the group for those files. They can be in both their current group and have access to the new group. You no longer need to create a third group that allows access to both. As user roles change within the organization, it's much easier to adjust AD tokens and make sure proper access controls remain in place.

DAC also makes it easier to control file access at a more granular level. You can assign policies to files and shares by allowing conditional control such as read-write access to some documents and read-only to others. You can also set conditions based on the device being used to access the data. Full access, for instance, might be restricted when using a tablet or smartphone but full access is allowed on company administered hardware.

Where is Direct Access Control most appealing? Clearly organizations with a high degree of sensitive information, such as government contractors, agencies or healthcare organization will benefit from locking down files through DAC. Even the smallest organizations, however, may rest easier knowing their most sensitive documents are safely protected and encrypted.

BranchCache



Does your business structure include multiple physical locations connected by a wide area network (WAN)? If so, what typical download speeds does your team experience every day? Many businesses experience noticeable delays and bandwidth problems when large amounts of data travel routinely over the WAN. In fact, your business may have a problem you are not even aware of.

Workers in branch office often become accustomed to waiting for data to load from the corporate servers. They refill their coffee cups or find other ways to keep busy while waiting for information to process over the WAN. Slow download speeds are often considered normal when working in a branch office.

Delays do not have to be considered normal working conditions. Windows 8 BranchCache is a utility that increases the availability of information and saves bandwidth over the WAN making everyone more productive and efficient.

BranchCache was introduced in Windows Server 2008 as a way of addressing the issue of network traffic. It reduces this traffic significantly by caching commonly used files at the local level instead of pulling them repeatedly over the WAN. With Windows 2012, BranchCache is improved and more powerful than before.

BranchCache is WAN bandwidth optimization technology and is included in some editions of Windows Server 2012 and Windows 8 Enterprise. BranchCache copies content from your main office servers or hosted cloud content serves and caches the content at branch office locations.

Where does BranchCache store the data? Your data is stored either on servers at the branch office that are configured for hosting the cache or, if no server is available at your branch location, directly on computers running Windows 8 or even Windows 7. After a branch computer requests and receives content from the main office over the WAN, that content is cached at the branch office. This allows data to transfer once over the WAN and then be accessed multiple times as needed by users in the branch office.

There are four main improvements that create additional benefit for you.

- *Simplified Group Policy Configuration*: Prior versions of BranchCache required your IT staff to deploy an Active Directory Group Policy Object (GPO) for every branch office in the organization in order to enable BranchCache. In the new release a single GPO contains all the necessary information for every branch office in the organization. BranchCache will also automatically update and reconfigure settings when a branch office moves from peer-to-peer cache hosting to a server.

- *Integration with Data Duplication*: In the past BranchCache had to process each file requested by a branch office and divide large files into small pieces and eliminate duplicate data to optimize transmission across the WAN. In the new release, if the main office server is already using this technology, BranchCache does not have to do any additional processing. It can use the data that is already optimized.

- *Multiple Hosted Cache Server Support*: Some organizations have large branch offices. This new release of BranchCache allows more than one hosted cache server per branch office. This means as your branch office grows and needs increase, you can add servers to remain responsive and cache more data as needed.

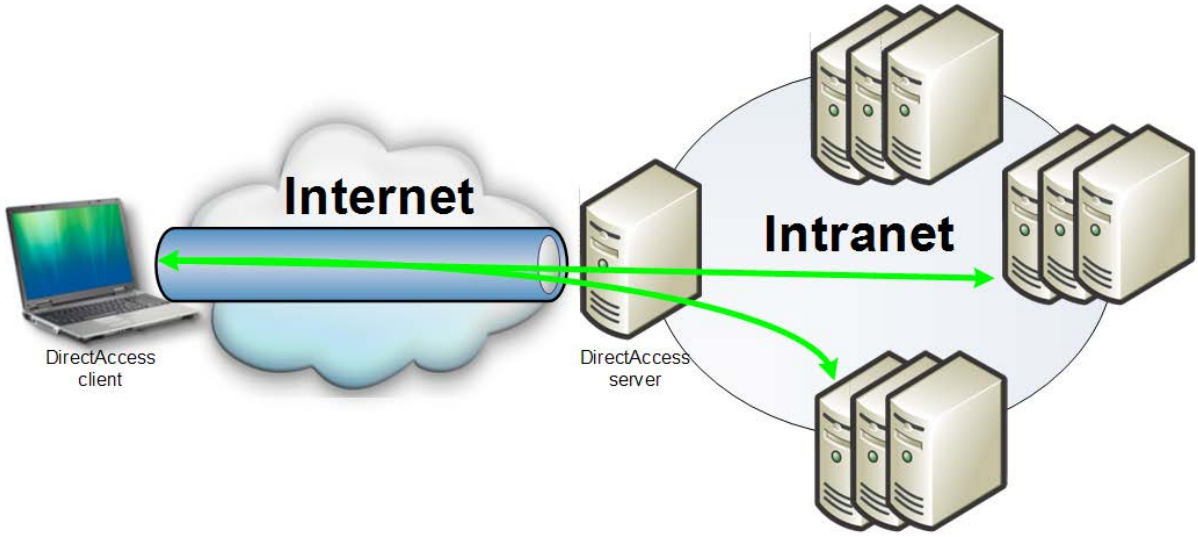
- *Automatic Encryption:* With Windows Server 2012, cached content is automatically encrypted to provide enhanced security. You don't have to worry about information leaks at the cache level with this feature.

BranchCache supports two cache modes. You can implement it using Distributed Cache mode or Hosted Cache mode, depending on your needs and requirements. In Hosted Cache mode, a cache server is designated at the branch office and becomes the central repository of data that is downloaded from the central office. You don't need a dedicated server, but can use space on an existing server at the local branch. When a file is requested, the central server authenticates the request and sends the metadata for the file to the hosted cache. The hosted cache

repository is then searched for the data. It is only sent from the central server if it can't be located in the cache.

In Distributed Cache mode, the cache is housed on each individual client machine. When a file is requested, the central server is contacted and the client's computer is pointed to another client's cache repository. If the file is not located on another machine within the branch office, the file is then retrieved from the central server and cached on the requesting client's machine. This system is best for a small office with only a few machines since it does not required a host cache and is easier to deploy.

DirectAccess



Does your business utilize a Virtual Private Network (VPN) to allow employees remote access to your intranet, servers and company data when working remotely? If so, you may be interested in DirectAccess, Windows 8's answer to a VPN.

Traditional VPN systems require users to log in following an established protocol in order to obtain a secure connection and begin accessing your company's intranet and data. This protocol uses a VPN client and registry. When your employees want to log on they must run the application and use a password to authorize the VPN.

DirectAccess bypasses this traditional protocol. It automatically establishes a bi-directional connection from client computers to the corporate network without requiring your employees to enter a password or wait for a connection. Your employees can simply work as if they were in the office even while remote.

DirectAccess uses advanced encryption, authorization and authorization technologies to allow secure data sharing from all points via the internet. The configuration is relatively simple for your IT team and is available in three configurations depending on the position of your DirectAccess server.

- *Edge Deployment*: In this configuration the DirectAccess server is located on the edge of your firewall and exposed to the internet. This configuration requires two network adapters, one inside the firewall and private and the other public and exposed to the internet.

- *Back Topology*: In this configuration the DirectAccess server is located behind your firewall and is not exposed to the internet. This configuration also requires two network adapters, one inside the firewall and private and the other public and exposed to the internet.

- *Single Network Adaptor*: In this configuration the DirectAccess server is located only in a private intranet setting. This configuration only requires one network adaptor card for the internal network, hence the name.

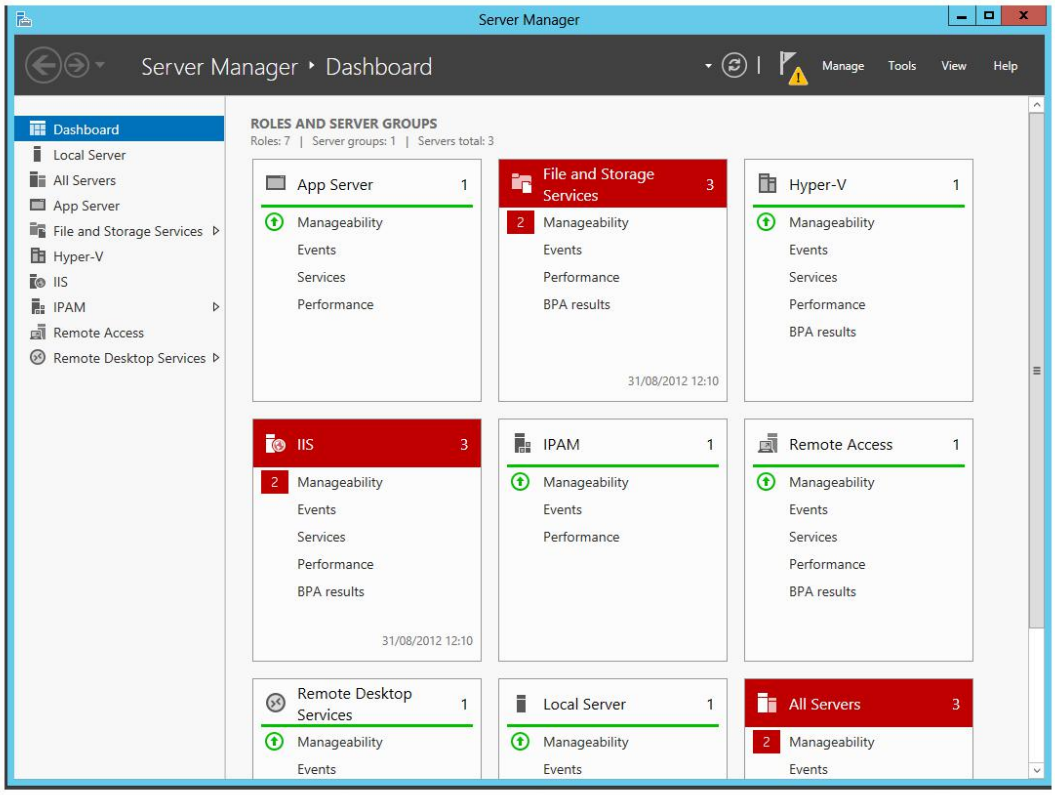
DirectAccess setup requires your organization to identify computers requiring remote access and register them with the server for authentication. Connectivity and security policies are then defined on the DirectAccess server and control access to the intranet. You define the areas of your network that are available remotely, and you are ready to get started.

What are the benefits of Windows 8 DirectAccess? The primary benefit is enhanced security. Your team can securely access your intranet while taking advantage of the enhanced security features of the Windows 8 operating system. This means any remote device using Windows 8 Enterprise can work effectively on your intranet without a VPN.

Windows 8 DirectAccess creates an encryption tunnel on the internet for the free transfer of information. This tunnel allows the user experience to be as fast and smooth as it is when they are in your office and behind your firewall. It does not require frequent logins or access maintenance and even allows remote computer management without an established VPN connection.

Will this make a significant difference in your organization? That depends on your situation. If you allow many of your employees to work remotely or telecommute this can be a great solution. As the changing employment picture moves to virtual teams at multiple locations and remotely, DirectAccess can significantly improve productivity vs. the traditional VPN.

Server Manager



Windows Server Manager allows your team to manage all the remote servers in your network from one centralized console as long as they are running Windows Server 2012. You can also, in some cases, use these tools to manage roles and features of servers running Windows Server 2008 as well.

You no longer need to remote in to each server to change roles or update policies. Administrators can use these management tools right on their desktop. This feature was available in previous Windows Server additions, but is completely new in Windows Server 2012.

Server Manager was rewritten from the ground up and focuses on giving you true multi-server support from a single console. It's quite a change from the MMC-based Server Manager and looks complete different. Once you learn how to navigate the interface, however, you will find it a powerful addition to your toolbox.

Server Manager defaults to the Dashboard configuration view for the local server. On the left side is the primary navigation pane that includes the All Servers group by default. You will also see groups such as File and Storage Services, Remote Desktop Services, and other. Clicking on one of these groups exposes a secondary navigation pane that shows the management hierarchy for that role. You can select entries in this secondary pane to select tasks related to the topic. Most of your management work can then be accomplished, right from this secondary pane.

Server Manager includes a tools menu that lets you launch the most commonly used administrative tools and application right from within Server Manager. You can use the tools and the command bar to perform global tasks that are not specific to an individual server or group. Updating or maintaining an individual server requires you to select that server from "All Servers" or another group listing and then move forward with your desired task.

Server Manager does use the Windows 8 tiled interface. It may take a little while for you to adapt to this change. It's worth the effort, however. The new Server Manager gives you easy visibility to your entire server fleet and is an incredible time saver. The ability to manage any server, even remote servers, from your office and desktop is powerful.

The centralized dashboard includes visual alerts that help you monitor issues on your entire network. These alerts include red and green stoplight type symbols along with messages, making it easy to assess the functions of the system from a quick glance. The reassuring green bar means everything is fine and there's no need to dig deeper. Red anywhere indicates an alert that requires IT attention.

Global management of servers within a group is quite a time saver, but comes with a certain amount of risk. Before you use Server Manager, you will want to create specific change management policies to control decision making within IT. It's important to prevent one bad decision from impacting your entire server fleet.

Windows Defender

Windows Defender is an antispyware program for Windows operating systems. It provides protection from spyware and malware as well as post infection scanning and removal of these types of programs from your system. It's pretty powerful, and it is a useful tool that provides three scanning options.

- *Quick Scan:* You can run a quick scan of the most common and vulnerable areas of a computer or system. Run from the start menu, you simply click the scan icon and select Quick Scan to find and eliminate problems.

- *Full Scan:* This scan reviews your computer completely. It takes a bit longer than a quick scan, but is effective at eliminating issues from a system.

- *Custom Scan:* If you suspect an issue in a selected drive or folder, you have the option of running a custom scan. This gives you the speed of a quick scan but the targeted focus of a specific area. Simply select custom scan and then highlight the drives or folder you wish to scan.

With Windows Defender you can conduct scans upon request or you can schedule them to happen at intervals and times you prefer. For example, you can set each computer to run a quick scan every morning at 2am or a full scan weekly on Sunday afternoon. Real time protection is enabled by default as well. This feature protects systems constantly by monitoring for spyware and other threats while users browse the web.

While Windows Defender is part of the standard Windows 8 installation, Microsoft has allowed OEMs to disable this feature and load other software such as McAffee or Norton instead. Why? Well, OEMs make a lot of money from including trail versions of these other security systems as

part of the bundled software packages on boxed PCs. If Windows Defender is deactivated on machines you bring into your organization, it does not automatically run unless turned on.

Activating Windows Defender is simple, but is a necessary step you should be aware of to avoid security breaches in your system.

BitLocker

Windows BitLocker Drive Encryption is a data-protection feature that encrypts the hard drives on computers and provides protection against data theft or exposure on computers and removable drives that are lost or stolen. It allows secure data deletion when protected computers are decommissioned by making it difficult to recover deleted data from an encrypted drive.

BitLocker encrypts the entire Windows operating system on the hard disk, including user files, system files as well as swap files and hibernation files. It checks the integrity of early boot components and boot configuration data and uses the enhanced security capabilities of the TPM to make sure data is accessible only if the boot components are unaltered.

BitLocker has been around since Windows Vista, but is significantly improved in Windows 8. Protection is now extended to cluster volumes and SAN storage, and is easier to enable than before. Let's look at some of the new enhancements to BitLocker.

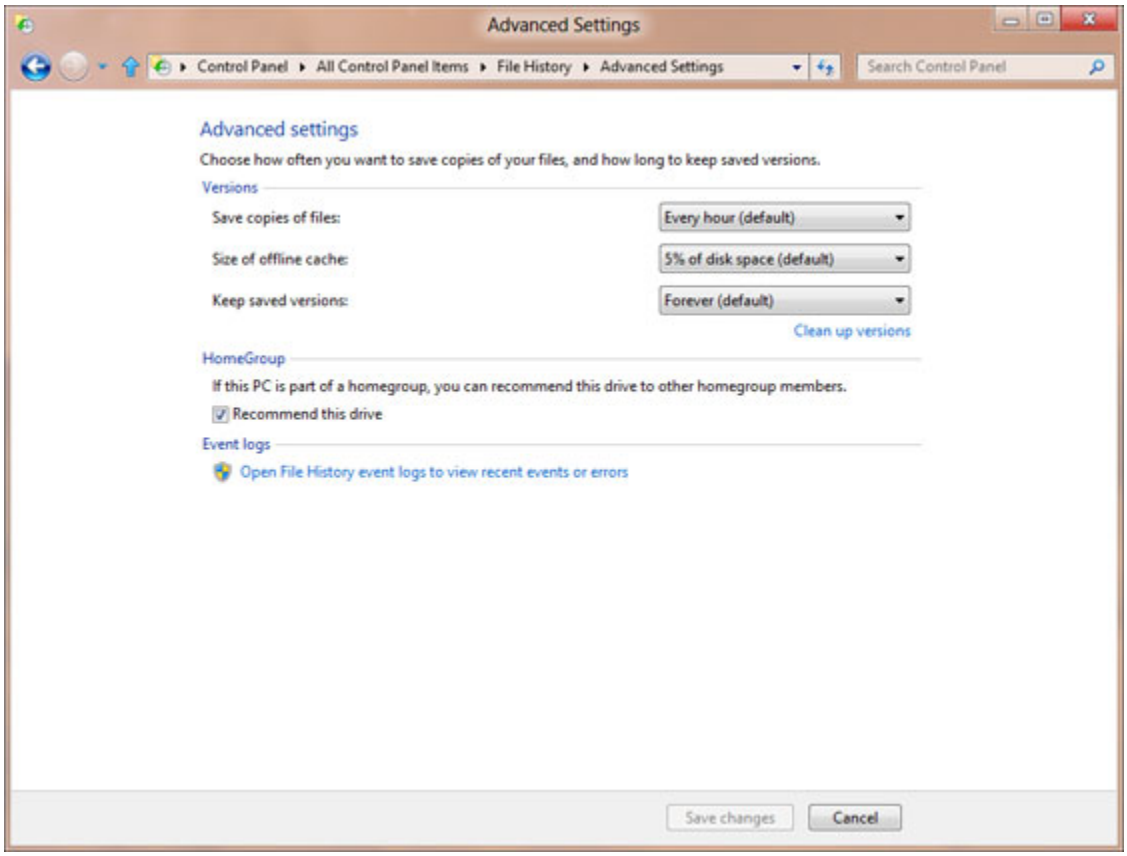
- *Pre-Provisioning:* Administrators can enable BitLocker for a volume before Windows 8 is installed. Windows generates a random encryption key that BitLocker uses to encrypt the volume you set. You can enable this feature from the Windows Preinstallation Environment (WinPE) by using the manage-bde BitLocker command-line utility.

- *Used Disk Space Only Encryption:* Previous versions of BitLocker encrypted the entire volume, even if it was empty disk space. With Windows 8, you can now choose to encrypt only the used space in a volume. This means enabling BitLocker on a largely empty volume takes only a few seconds. This feature is best used on new PCs or

volumes only, since the free space on used volumes can still hold valuable data that is retrievable. Only the full encryption option will protect this information.

- *Standard User PIN and Password Change:* With Windows 8, your standard users are allowed to change a volume's BitLocker PIN or password. Of course, they can only change it if they know the original password – so you can still control access if you like. This feature can make BitLocker deployment easier for you, since you can set the same PIN and password for each PC during the automated deployment process. Users can then change their PIN and password after installation. Make sure you establish a password protocol, however, to guard against user selected PINs and passwords that are simple and easy to hack.

Centralized Backup



Windows 8 has a completely redesigned backup system developed due to the unpopularity of the system in Windows 7. Very few PCs used the Windows Backup feature, so that has been scrapped in favor of Windows 8's File Histories.

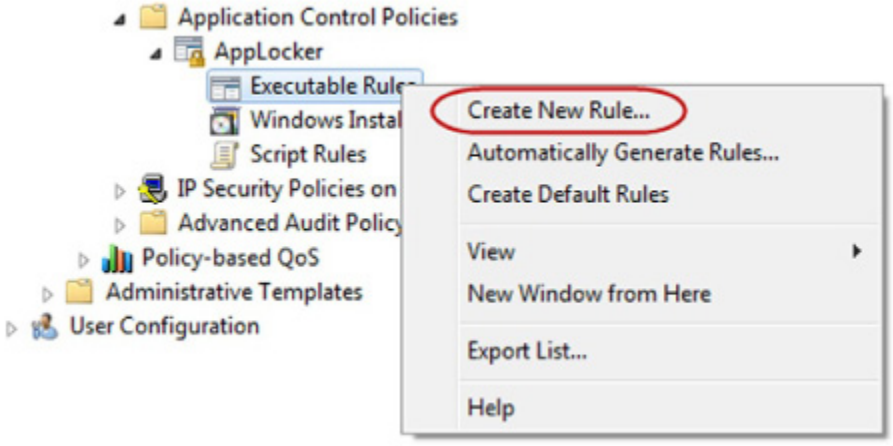
With Windows 8, you can no longer create system images or back up everything on a hard drive. Instead, files are backed up in groups such as libraries, desktop files, or browser favorites. File History is designed to create a continuous backup of the entire system, backing up documents automatically including the most recent changes made by users.

The system is centralized for all PC's and for the servers as well. While image capability is not available at a PC level, the backup capability includes an image based system at the server level. You can even configure a partition and back up the server for restoration after an issue if you like.

Centralized backup takes the decision to protect data out of the user's hands by automating it. File History syncs every hour unless you configure it otherwise. You can map backups to cloud storage if you like, resolving the issue of onsite backup locations in the event of a catastrophic event.

File History is disabled by default in Windows 8. You will need to enable it from the Windows 8 control panel if you decide to use this feature in your organization. You can still run Windows Backup along with File History if you need to restore files form backup sets created in Windows 7, making the system flexible according to your needs.

AppLocker



AppLocker is Microsoft's solution for application control. AppLocker is nothing new; it was introduced as a part of Windows 7. With Windows Server 2012 and Windows 8 it was expanded to include the Modern UI applications used with Windows 8 and Windows RT.

AppLocker allows network administrators to create policies that either restrict specific applications from running on the network and allow all others or allow only certain applications and restrict all others. This is accomplished by creating either blacklists or whitelists of applications. Users are restricted from downloading or running applications based on these lists.

AppLocker is useful to business in many ways. It reduces administrative overhead for your organization by decreasing the number of help desk calls that are a direct result of your team running unapproved applications. Just this reduction in network disruption alone can provide a significant savings for you, depending on the size of your network. AppLocker helps your team in other ways as well.

- *Application Inventory*: In audit=only mode AppLocker will register all application access activity in event logs. These events are collected and can be analyzed by your team. You will know what applications are being run in your organization and by whom.

- *Protection against Unwanted Software*: AppLocker prevents applications from running when you exclude them from a list of allowed applications. These rules protect your organization from any application that is not covered by the allowed rules. It simply cannot execute and run.

- *Licensing Conformance*: With AppLocker you can create rules that prevent unlicensed software from running on your network. You can also create rules to assign and restrict licensed software to authorized users only.

- *Software Standardization*: You can configure AppLocker policies to allow only approved programs and applications to run on computers within a defined user or business group. This allows you to create a uniform application deployment across departments or levels of your organization.

AppLocker is most valuable as a security and administration tool for your business. Information is one of your organization's most valuable assets, and protecting it is a primary concern of information technology.

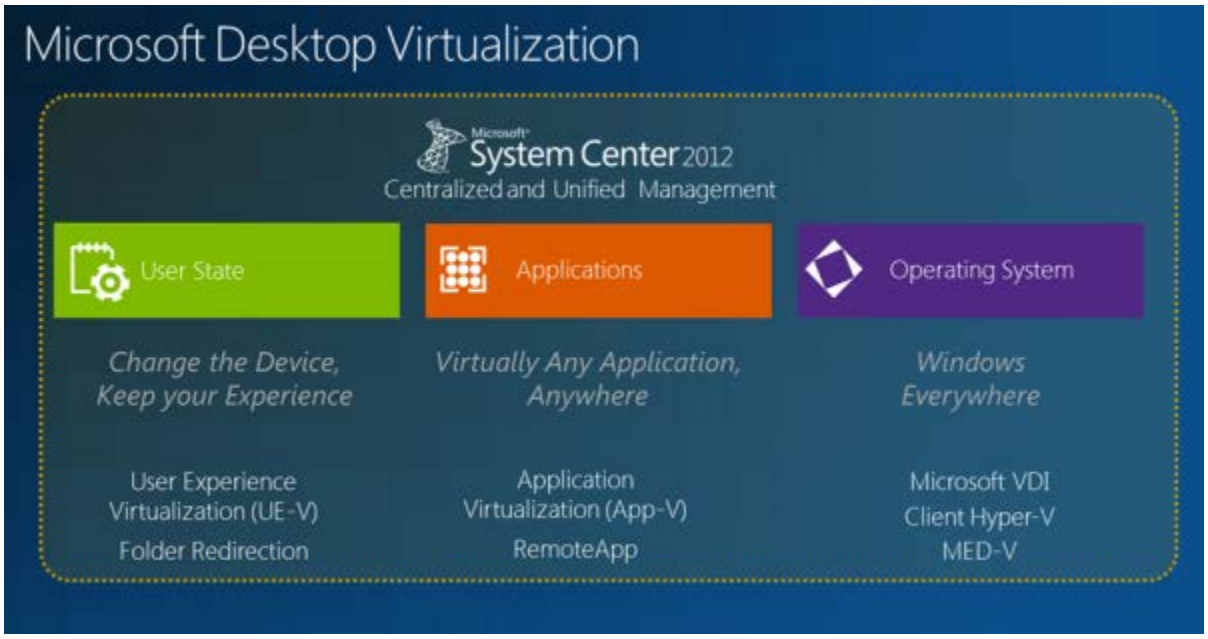
When a user runs a process, the process has the same level of access to the data that the user has. This is not a problem when running approved software applications. What if a member of your team runs malicious software, even by accident? Sensitive information can easily be deleted or even transmitted outside of your organization. AppLocker prevents these scenarios by restricting the files that users are allowed to run.

AppLocker assists administratively in many common business scenarios. When an application is no longer supported you can restrict it using AppLocker. This prevents it from being used by your team. Similarly, when a new or updated version of an application is deployed you can prevent users from running the previous version.

Perhaps you have a single employee or group of employees that needs to use specific applications. If these applications are denied to other employees you can easily restrict access with AppLocker. You can also restrict access to applications by users of a shared computer. Each user logs in and is granted an individual level of access.

AppLocker helps you protect your sensitive information and reduces security threats. It is available through Windows 7 Ultimate or Windows 8 Enterprise. The only significant difference between the two versions is the capability of restricting or allowing Modern UI style applications which is available in Windows 8 Enterprise.

Virtualization and Hyper-V



Windows 8 uses Hyper-V to drive virtualization for your organization. When combined with Remote FX and other technology that is a part of Windows Server 2012, your organization has several ways to implement a strong virtualization strategy.

Virtualization is a technique used in information technology involving creating a virtual, or trial, version of an operating system, hardware platform, or other computer network resource within an existing and operating actual system. It's used by developers as they work on creating a new system or making changes to an existing one. It's also used by information technology professionals to make desktop deployment easier and to test software and operating systems prior to deployment.

Hyper-V Virtualization is technology and software developed by Microsoft that allows a virtual system to run within an existing Microsoft system. Hyper-V Virtualization is not a new development; it has been around for some time. In the past it was only available on server level operating systems. Microsoft has now decided to include in with Windows 8. Hyper-V Virtualization is built into Windows 8, allowing users to work with it without having to download or install any additional tools.

In earlier versions of Windows, Hyper-V used three main storage options: direct attached storage, iSCSI Sans, and Fibre channel SANs. With Windows 8 storage is enhanced making it possible to pool virtual machines.

There are new features in with Windows 8 that allow your organization's administrators to better manage virtual machines and the number of monitors that can be used at specific resolutions. Let's look at each of these new features.

- *GPU Management*: Windows 8 includes a GPU management user interface in the Hyper-V management console. This gives your information technology team a better understanding of the GPUs installed in the server and the ones that are good candidates for associating with a virtual machine. It also allows your team to filter out GPUs that are used for server management only so they are not used with RemoteFX.

- *Multimonitor Support*: In the past, RemoteFX limited the number of monitors that could be used with a virtual machine as the screen resolution was increased. With Windows 8 this limitation is gone and a virtual machine can support the same number of monitors regardless of the resolution of the monitors.

This new version of Hyper-V enhances the productivity and efficiency of your IT system in a few significant ways. First, this version enhances the flexibility of your business by allowing live migration of virtual machines. This means you can move things around and swap storage locations without bringing machines down and with few limitations. This allows administrators to work behind the scenes without impacting organization productivity or disrupting users.

This new version of Hyper-V allows your business to support larger workloads. As your business grows and changes, you can adapt quickly. You can use up to 64 virtual processors and 4000 virtual machines per cluster. This means you can grow significantly before you need to consider other options.

Hyper-V now works in conjunction with Microsoft System Center 2012 to help your team automate many of the virtual management functions they previously completed manually. This benefit reserves your valuable technology time and resources for other functions in your organization.

User Level Security Issues

Security and Social Media

Windows 8 is designed primarily for a consumer driven market. This decision is apparent in the tiled user interface and the prominent role social media plays in the Windows 8 environment. Applications like Facebook, Twitter, and LinkedIn have live tiles that update automatically with posts and contacts.

This live interaction is ideal for individuals who are highly socially connected. Increasingly that group includes your users and employees. Depending on your work culture, you may have some kind of policy in place that limits the use of social media on company time. Windows 8 will make violating that policy more tempting for your team.

If, however, your business is moving in a direction that encourages interaction via social media, Windows 8 may simplify contact for your team. Your sales and marketing group as well as in field service employees may use social media as a way to network and maintain contact with

your customers. In this case, the increased visibility and connectivity of social media within Windows 8 will be a benefit for your organization.

Either way, it's important for IT to consider the role social media plays in your organization and the limits you want to place on it if you upgrade. With Windows 8 Enterprise you can use AppLocker to restrict social media applications and decide which devices, if any, will have access to them.

Restricting social media limits the exposure your data has to the Internet as a whole. It protects user productivity as well. If social media is allowed, you may want to establish limits on data that can be shared, uploaded, or downloaded from within these applications.

SkyDrive

SkyDrive is the cloud computing application created by Microsoft. SkyDrive has been around for a while but is now fully integrated into Windows 8. When you choose to upgrade your organization to Windows 8, you automatically receive SkyDrive as part of the package.

SkyDrive is installed by default with the operating system and is available on the start screen as soon as your users boot up their PCs or mobile devices. At least, it is unless you decide to use AppLocker and block access to this application from within your organization.

SkyDrive works like other consumer based cloud applications. You may be familiar with Dropbox, Box, or iCloud. These competitors are very similar to SkyDrive. SkyDrive offers users 7GB of storage space in the cloud for free and allows individuals to purchase more space if they like.

Using SkyDrive is simple. Users open up the app and drag files into one of the folders. The folders are automatically synched with Microsoft's servers and the data is stored in the cloud. The app works from PCs or mobile devices like tablets or smart phones. All you need is the app and an internet connection.

Users can sync any folder on their PC into their SkyDrive folder automatically if they want. Normally folders must be dragged into the app in order to sync, but your employees can add a shell app available on the internet to provide automatic syncing by including an option to "Sync with SkyDrive" within their Windows Explorer screen.

SkyDrive is enhanced with Microsoft Word capability. Your employees can use Word to edit documents from their web browser and the SkyDrive app. Changes are immediately made in the cloud, giving your team enhanced productivity when working remotely.

SkyDrive can be very useful for collaborative work and remote file sharing. It seems like a simple decision for enterprises, but allowing SkyDrive on your network does expose your organization to some risks you may not have considered.

Personal cloud accounts like SkyDrive and its competitors bypass the normal security protocols and protections established within your network. Sure, an employee can use SkyDrive to enhance productivity and work remotely. Unfortunately, they can also use SkyDrive to transfer company information outside the network. Once data is in the cloud, your organization loses control of its security or its use.

As an IT professional, you should seriously consider how you want to use and deploy SkyDrive. It is incredibly risky to allow free access to SkyDrive from every device in your organization. Instead, consider using AppLocker to pin down use of SkyDrive to limited scenarios or block it completely.

With AppLocker you can prevent SkyDrive from loading and executing on any device that shares your network. If you see value in SkyDrive for some employees or workgroups, AppLocker can help you restrict access to only those individuals you wish to allow.

Microsoft will probably provide other enterprise level security measures for SkyDrive at some point. Currently, however, those protections are not available within the app itself.

BYOD and WindowsToGo

Businesses are increasingly adopting a policy of BYOD. This stands for Bring Your Own Device and is a business policy that allows employees to bring their personal laptops, smart phones and other mobile devices to work. These devices are loaded with company owned software and given access to private company networks and data.

The goal of BYOD is to increase the workplace options employees have and increase mobility and telecommuting without the expense of providing these devices to employees. Employees benefit from having increased mobility and the convenience of personal and work related information on a single device. Employers benefit from increased accessibility to employees and increased mobile capability without investing in the mobile devices themselves.

Is your business considering adopting a BYOD policy? If so, you must plan prior to implementing BYOD in your organization. Here are just a few issues and challenges your business will face.

- How will your organization support employee devices? Will you need additional IT staff or capability?

- How will you maintain the security and confidentiality of your sensitive company data in a BYOD environment?

- Will you limit personal apps? Will you restrict the access those apps have to your company data?

- What will happen if an employee owned device with company data is lost or stolen?

- When an employee leaves your organization, how will you remove data from their personal device and restrict future access?

- What about your company's internet usage policies? Will you restrict employee access on their personal device during non-business hours?

- Who is responsible for lost personal files or employee data as the device is maintained? What if you accidentally delete that critical personal file on your employee's tablet?

Blending personally owned devices and personal applications with company business creates new ethical and security issues you may not have considered. You can minimize your risks by planning ahead and proactively establishing a policy prior to adopting BYOD.

Review your company's current security policies. Your organization should already have internet usage and security policies that control employee access to protected data. These policies can often be adapted to include personally owned smart phones, tablets, and laptops.

Decide which devices your company will support. Control your company's support responsibility by limiting BYOD to specific devices. Which smart phones and tablets will you support and which will you exclude? Require employees who are interested in bringing their own device to supply one from your list of acceptable devices. This allows you to continue to support company supplied hardware while maintaining a limited BYOD fleet.

Establish a defined service policy for employee owned devices. What if your employee drops his smart phone and breaks the display? What if she spills coffee all over her tablet? Will your company assume the responsibility for this level of repair and maintenance? A clearly defined service policy is essential prior to implementing BYOD.

Require security measures including a complex password or PIN. People generally avoid complex passwords on their personal devices. They frequently disable the screen lock functions or use a simple and repetitive motion or code to release the user interface. That's fine if the most important information on the device is a recent Facebook post. It won't work for your company's important data.

Determine which apps are allowed and which are banned. Restrict applications based on your organization's internet usage policies. Understand, of course, your employee's interest in social media and other personal apps that are normally not appropriate for work situations. Consider

also the synchronization feature of many apps. Synchronization can create an unintended portal into your company network and a security risk for your data. You will want to limit this portal and protect data if at all possible.

Clarify ownership of applications and data. It seems logical that you own your company's data and the employee owns personal applications and data, doesn't it? No problem, at least until the device is lost or the employee leaves the company. When you wipe all data from the device, whether on site or remotely, employee data goes with it. Some of this employee data, such as photos and messages, is gone forever. To protect yourself and your employees clearly reserve the right to clear all data from the device and help your employees learn how to back up their personal information so they can restore it later.

If your organization decides to adopt BYOD, you will want to understand and implement Windows To Go. Even without BYOD, Windows To Go is a great feature of Windows 8 that makes company owned mobile devices safer and easy to administer.

Windows To Go is a feature of Windows 8 Enterprise that allows the operating system to start up and run from a USB device. Windows 8 Enterprise is the only version of Windows 8 with this feature. You must have Windows 8 Enterprise, available only through Software Assurance which is one of the volume licensing scenarios available for your business.

Windows To Go does not actually install Windows 8 from a USB drive. The Windows 8 operating system never leaves the USB drive and does not become a part of the device using the USB drive. Instead Windows To Go actually allows your employee to run Windows 8 Enterprise from the USB drive itself.

If the USB drive is removed the entire system pauses for 60 seconds. If the USB drive is replaced within that 60 second time period the system just picks up right where it left off. If the USB drive is not replaced during that time, however, the computer shuts down and Windows 8 will no longer run. This security feature protects your company specific data.

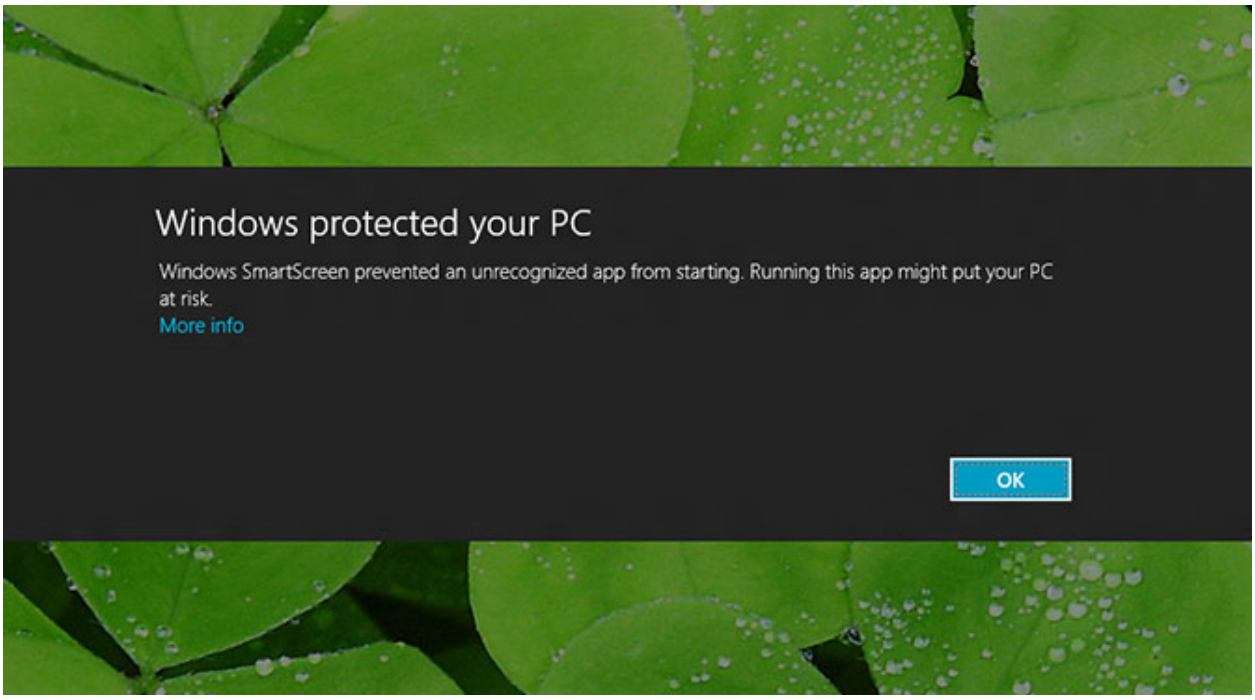
Windows To Go was designed to allow businesses to provide employees with a complete Windows 8 work environment they can use effectively on their personal devices and home computers. This innovation allows employees to take their work station with them when they travel or work securely from a remote location.

Security is not a concern with Windows To Go. The content of the USB drive can be encrypted to prevent access from without authorization. Since the data on the USB drive is locked and does not transfer to the host computer, there are minimal security risks. You can more readily control your information, especially in a BYOD environment, by taking advantage of Windows To Go.

As you can imagine, Windows To Go doesn't work with just any USB drive. Microsoft has established compatibility requirements and has currently approved three Flash memory drives for use with Windows To Go. These three drives are Kingston Data Traveler Workspace, Super Talent Express RC8, and IronKey Workspace.

Windows To Go simplifies your administration of mobile devices in general and BYOD devices in particular. These devices do not need the same data wipe protocols with Windows To Go as they will without it. Since your data is not transferred to the employee's device, there is no need to wipe data to remove it.

SmartScreen



SmartScreen is a phishing and malware filter included as part of the Windows 8 operating system. It is designed to help protect users from attacks associated with downloads that infect a system. In Windows 8 it filters at the desktop level, checking the reputation by default on any file or application downloaded from the internet.

SmartScreen works by sending the source URL of downloaded material to an outside server. That URL is checked against a whitelist of safe sites. Sites are judged as safe by having a certificate purchased from Certification Authorities that verify the identity of the software publisher and their reputation. If SmartScreen does not find a match it displays a warning message before users are allowed to download the file or access the application in question.

When SmartScreen was first introduced, many experts were concerned about privacy issues and the effectiveness of the system. This automatic analysis of files has the potential of building a database of user download information, thus giving Microsoft a possible competitive advantage. Microsoft has addressed this issue by stating that IP addresses are collected on temporarily and are periodically deleted and that the information gathered by SmartScreen would not be used for advertising purposes or sold to third parties.

So, how effective is SmartScreen as a security protocol for your network? SmartScreen does an effective job of filtering downloads and warning users of security concerns. Unfortunately, however, users can easily bypass the warning and download the information anyway. Rather

than relying on SmartScreen to control risks associated with downloads, you are wise to restrict downloads from the internet using AppLocker or other security settings on your network.

Alternate Passwords

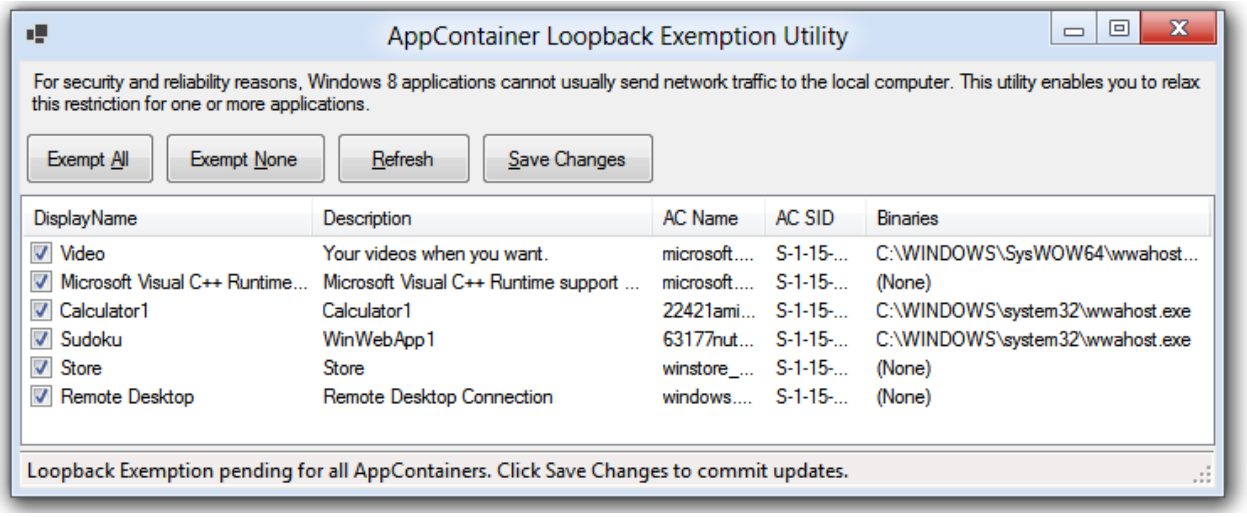
Microsoft included alternate passwords as a security feature in Windows 8. In this feature, users can choose a picture as a password rather than the usual alphanumeric passwords we are all used to. When this picture password feature is enabled, users select a photo from their image library and define three gestures on the photo using a combination of circles, straight lines, and taps using either touch or the mouse. It's also possible to switch to a PIN based authentication system along with the picture if you like.

So, do these passwords actually create an additional level of security? In some ways they are more secure. It's more difficult for someone to guess a password given the random nature of gestures and the number of variations of images that can be used. In other ways, however, these passwords are more susceptible to hacking.

In order to set up an alternate password, a user must first establish an account using a plain text password. Unfortunately, Windows 8 stores these passwords using encryption that can be reversed. Hackers who gain control of a computer along with administrative rights can extract the key for a plaintext password and reverse the encryption to gain access.

To protect your network, it's best to disable the picture password for your internal systems. A strong alphanumeric password is safer, and while it's not as convenient for your users the security benefits outweigh the convenience factor.

App Container



App Container is the security sandbox within Windows 8 that hosts apps. It offers fine-grained security permissions and blocs write and read access to most of the system when using an app. By default, an app can only access its AppData folder and cannot directly access anything else in the system unless the user grants it access.

How does this enhance your security? Basically it protects the system from intrusive applications by keeping them contained in their own micro-environment within Windows 8. This prevents apps from disrupting the operating system.

App Container decides which actions are available to which apps. This feature runs in the background and users are not aware of it when using applications, making it virtually invisible.

App Container establishes a new integrity level in Windows 8 and uses that level to block access to objects marked with a higher integrity level. Apps can make declarations in their application manifest file about the capabilities they need to access and be allowed permission to use things like a user's music folder in order to run. General access, however, is locked down.

App Container provides an additional layer of security against attack from hackers intent on creating a disruption. This feature, combined with Data Execution Prevention (DEP) which prevents data from being executed and Address Space Layout Randomization (ASLR) which randomizes the address space of a process make it much more difficult for an attacker to exploit system vulnerabilities.

Start Button Alternatives

One of the biggest changes to the user experience with the Windows 8 operating system is the lack of a start button. This is one of the most difficult and surprising features for employees in an organization after an upgrade. People resist change, and the start button is a comfortable and expected part of the Windows experience for most of us. It can take a long time for users to adjust and find ways to be productive without it.

Shortly after Microsoft released test versions of Windows 8 to developers, analysts and commentators, alternatives to the start button began to show up all over the internet. Quickly identified as something that would irritate most people, alternatives were quickly developed to ease user pain.

Unless you want to spend hundreds of help desk hours addressing user concerns and frustrations created by the non-existent start button, you may want to explore alternatives and

select one or two to deploy in your organization. Learn them and prepare to install and support these options as users request alternatives, or possibly from day one of Windows 8 launch.

While many of the start button alternatives are free, a few have a slight cost associated with them. Some basically hack into Windows 8 to create their work around. Others lay on top of other Windows 8 features. The displays are varied and each alternative has a slightly different appearance and list of features. Here are some of the more popular alternatives.

- *Power 8:* This free alternative displays a start button in the usual spot on the desktop. Clicking it brings up the familiar two pane menu. There is even a search field at the bottom to allow you to find applications, files or other items on your PC. You can set Power8 to auto start each time you log in to Windows 8 and even block all Modern UI features including the Charms bar. http://code.google.com/p/power8/

- *Win8 StartButton:* This free alternative allows you to change the look and feel of the start menu and customize it. You can disable Windows 8 hot corners if you like, add and remove commands to the menu, and change the appearance. http://windows8startbutton.com/

- *Pokki for Windows 8*: This alternative is very user friendly and well designed. From the created start menu you have access all of your programs and open folders such as Documents, Music, and Pictures. This contains a search field as well as a Shut Down menu with all the familiar functions such as restart, sleep, etc. There is even a folder called Windows 8 Apps which allows you to switch to the new Modern UI apps you want to use. https://www.pokki.com/

- *ViStart:* This alternative displays the familiar Windows 7 orb and pops up to the expected start menu. Unlike other alternatives, though, there is no customization option. What you see is what you get. It does allow you to use hot corners while it's running and lets you toggle to Windows 8 apps if you wish. http://lee-soft.com/vistart/

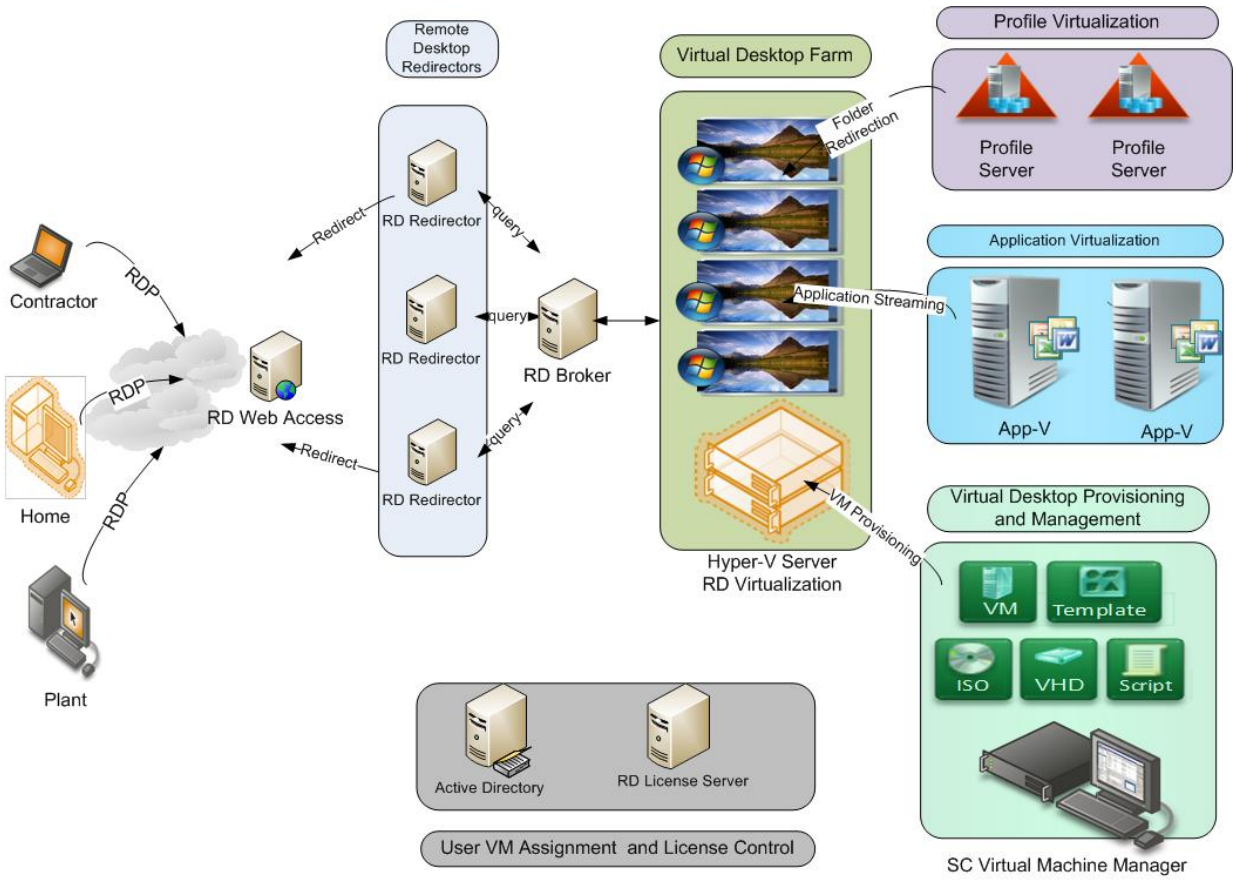
- *Classic Shell:* This alternative is actually a collection of features from prior versions of Windows, but includes a classic start menu alternative. After you install this alternative you can choose between displaying all the settings in the normal start menu or just the basics. It allows you to quickly bypass the start screen and also allows you to search for a launch Windows 8 apps directly from a submenu. http://classicshell.sourceforge.net/

- *StartMenu7*: This alternative allows you to customize the look and the functionality of its start menu. You can resize the menu to take up as much or as little room as you

want. You can even change the Windows orb between the classic Windows 7 look and the new Windows 8 logo. You can set up virtual groups and organize your shortcuts to increase your functionality. This application does not easily let you back into the Windows 8 world, though. There's no good way to access your Windows 8 apps while running this program. https://www.startmenu7.com/index.html

Be sure to test these options for functionality. Since they are applications, they run within the App Container sandbox and may not have complete functionality across your system. You will want to understand the limitations and instruct users in how to access everything required for their daily work flow.

VDI Enhancements / Remote Desktop



Microsoft included a variety of Virtual Desktop Infrastructure (VDI) enhancements in Remote FX and Windows Server 2012 with this round of upgrades and new releases. These enhancements improve the desktop experience of users by allowing 3D graphics, USB peripherals, and touch enabled devices across any type of network.

The graphics enhancements were needed when Microsoft made the change to the Modern UI style interface. Since this interface is graphically driven, it makes sense that the graphics capability of the operating system needed improvement. As a result, the bright, live tiles have a greater graphic intensity than capable with previous Windows operating systems.

The VDI Enhancements include a significant improvement to Remote Desktop Services (RDS) with Windows Server 2012. This enhancement provides a platform for your organization to implement a centralized desktop strategy. This strategy improves flexibility and compliance as well as data security and gives you the ability to manage desktops and applications remotely through your organization.

RDS is a centralized desktop and application platform that uses desktop virtualization and VDI technologies. Your team can run the desktop or applications in a datacenter while users access it from anywhere. This upgrade replaces Microsoft's Terminal Services utility and provides greater flexibility for your team.

Many businesses are using VDI to reduce the overall cost of desktop deployments. The Remote Desktop Management Service and user interface in Windows Server 2012 allows virtual machines to be easily deployed to hundreds of users at a time by duplicating a single master virtual machine image. Your network administrator doesn't need to manually duplicate and create virtual machines or use complex software to manage the automatic creation of virtual machines.

Updates to virtual machines are simplified with Windows Server 2012. The VM Streaming feature allows an administrator to patch and update unused virtual machines in a pool by patching the reference virtual machine and then streaming the updated VM to the user when they next connect. This upgrade eliminated downtime for updates and allows your employees to move uninterrupted through their workday with updates happening automatically on their next log in.

Windows 8 includes Remote FX to further improve the user experience. Remote FX is the set of technologies that enhance the visual experience of users working remotely. Businesses today rely heavily on media consumption as a part of normal activities. In some cases team members are trained remotely using media from the corporate servers. In others demos, marketing materials and presentations are used on outside sales calls and other remote events. When you also consider the opportunities to collaborate online, work in virtual teams, and conduct webinars and virtual conference calls, you see the importance of media to your organization.

Remote FX is improved with the launch of Windows 8 and now integrates network detect, graphics profiles, and remote scenarios to create an excellent media consumption experience for your team. From their perspective there is no difference between media use in the corporate office and media playback in a remote session.

As you would expect, multi-touch integration is a crucial aspect of the new Windows 8 operating system. In order for mobile devices to function well with Windows 8, remote sessions must support the same multi-touch gestures and manipulations used in a local setting.

Microsoft has enhanced the capability of this technology to allow a fluid and responsive touch experience even in a remote session. Users can navigate inside and between local and remote session by touch alone, making mobile devices as powerful remotely as they are locally.

Windows Phone 8

Encryption

Before we get into the applications that allow this smart phone to increase your team's productivity, let's review a few behind the scenes features. Windows Phone 8 integrates with your server level network applications such as Microsoft Exchange, SharePoint, and Microsoft Lync. This means your team can join conference calls quickly, collaborate and share documents remotely, and access network data quickly. Your internal help desk will spend less time dealing with frustrated in-field employees.

Windows Phone 8 has built in MDM technology. This allows you to wipe the device, control access, track, and support the device. The secure boot and "always-on" encryption features keep your sensitive information secure. If your business is part of an industry such as finance or healthcare this encryption provides the added security you need to integrate smart phones into your business model.

The encryption for Windows Phone 8 uses the same technology as BitLocker. There are a few issues you should be aware of, however. First, the encryption is not available in some geographic locations. The mobile phone infrastructure simply doesn't allow the importation of encryption technology. In these areas the encryption feature won't work.

Secondly, encryption does not include the data on the SD card. This is apparently due to unknown issues with the performance of swappable SD cards. As a result, make sure your team knows that only pictures, music and videos should be stored on SD cards. Documents and other data must be stored within the phone itself to be safe and secure.

WISPr Network Authorization

With Windows 8 Microsoft has embraced the mobile technology experience. Microsoft has added several new network authentication types to Windows 8, most importantly WISPr protocols.

WISPr (Wireless Internet Service Provider Roaming) is the network protocol that allows mobile devices such as cell and smart phones to roam between networks and connect to whatever service provider they encounter. Now Windows 8 users can log into available internet connections relatively smoothly as long as the connections are publically available.

While this is not necessarily security related, it does make using Windows Phone 8 easier for your organization. It is now easy to standardize your mobile phone fleet to Windows Phone 8 and provide employees with a tool they can use effectively in the field.

Data Usage Tracking and Monitoring

Windows 8 adds a new feature that is helpful if you are paying for data usage or need to monitor it. Especially useful for mobile broadband accounts that push limits toward the end of the billing period, this feature tracks your data transfers and displays the amount used since the last time you checked when you tap the network.

When you are getting close to your limit or if you use a metered service, simply select the metered service option with a right click and a tap. This disables all but vital security updates from Windows and restricts data flow on certain other sites as well.

Many mobile phone apps and features use a data connection and update at regular intervals without the user requesting an update. The mail app may check the mail server every few minutes. Social media apps may check for updates and changes in status. Data used in this way is called background data and can significantly add to the data usage charges on cell phone billings.

The data usage tracking feature allows users to see the data they are using and voluntarily limit it. As a practical matter, however, most corporate users won't concern themselves with data usage. For this reason, Task Manager in Windows 8 takes tracking and monitoring one step further. It provides a detailed history of data usage and a chart with connection performance. If your organization owns the device your team member is using, this tracking allows you to monitor sources of data transfer so you can limit usage if needed.