Realtime
publishers

The Shortcut Guide™ *To*

User Workspace Management

sponsored by

RES
software

Greg Shields

Copyright Statement

Chapter 3: Tying Security to People, Not Devices

I'm a genuinely optimistic kind of person. I believe in the intrinsic human desire to ultimately do what's right, notwithstanding the circumstances. Although that innate positivity works great for some parts of my IT professional's career, it probably doesn't make me the best IT security person.

Why? Because it takes a certain type of person to be really good at IT security. Those individuals, by virtue of their job's charter, are forced to approach every situation with a critical eye. They seek out weak points in IT architectures, looking for places where bad people can do bad things. Their role is to protect company assets by setting policies, permissions, lockdowns, and security measures.

Yet although the role of the security administrator won't soon be going away, there's an argument that new approaches to security are quickly becoming necessary. Consider once again today's evolving business climate as outlined in Chapter 1. There, I explained how the traditional one-computer-per-person approach no longer makes sense for IT. Today's users find themselves launching applications on their desktops as well as via remote application infrastructures. They connect from home as well as on the road. They leverage certificate-based logins in addition to passwords, but not at every login. In short, today's user behaviors are *unpredictable*.

Complicating this situation further is the recognition that today's user employs multiple mechanisms to access applications and data, often *at the same time*. One user might log in to their local desktop and connect to a remote application, only to find themselves an hour later also using a conference room computer. Another might login twice from home, using at the same time their home computer and their company-supplied laptop.

Yesterday's IT security professional might shudder at these scenarios. When users have the ability to connect from anywhere and use any resource, this immediately complicates the application of security. In an everything-for-everyone environment, comprehensively applying security at every location is a challenging task, requiring meticulous effort to catch every potential endpoint.

Yet the problem with this approach is in its focus. Today's unpredictable user needn't necessarily complicate the application of security configurations. In fact, with the right technology in place, the idea of *where* security is applied grows less important. Replacing it is a new focus on *how* that security is applied. With User Workspace Management, that *how* ties security *to dynamic people and not devices*.

Comfortable Security

Getting to the *how* also solves another conundrum first introduced in Chapter 2. That conundrum deals with the traditional approach to management, including security management, and how IT must be aligned with the needs of its business and users to be fully successful. To quote:

> The problem with traditional approaches to proactive management stems from the nature of policies themselves. Due to limitations in how policies can be applied and enforced, many IT organizations who want to control certain elements of personality ultimately find themselves forced to control all elements of personality. In order to ensure that desktops have the right software, IT must itself do all the installing. In order to protect desktops from bad personality configurations, IT must enforce settings that cannot be overwritten.
>
> Although the net result is a more-secure environment, *it is at the same time a more-sterile environment, devoid of all the elements that make the computer personal and comfortable*.

Yesterday's IT security professional might scoff at the last three words in the previous sentence: *Personal and comfortable? Why should IT care about what is personal and comfortable? We're here to assure the secure access to applications and data. It's up to the user to find their needed comfort.* However, it is exactly that comfortable personality that is fundamentally important to a business' users.

As a result, today's approaches to both managing and applying security require an additional look at how users go about accomplishing their tasks. One mechanism to accomplish this goal is by shifting the application of security from the individual device to a focus on the actual user. Your User Workspace Management solution can go far in enabling this shift.

Centralizing Security with Personality

This guide has already talked about the logical encapsulation of the user workspace that occurs through a User Workspace Management solution. By separating the user workspace layer from the others on every computer—applications, operating system (OS), and hardware—the user workspace becomes fully mobile. And by enabling mobility, it becomes possible to compose a unified workspace for each user atop any application and desktop delivery solution.

Now, here's where things start to get interesting: What also becomes possible is the management of security configurations *within the workspace*. Since the workspace is pervasive, composed dynamically at each login, you gain the ability to assign security configurations to the user *no matter where or how they might connect*. Indeed a lofty statement, but one that can be realized through technologies that are available today.

Let's think of this in another way: By creating this unified and pervasive workspace across delivery mechanisms, you gain the ability to tie security to the tailor-made workspace rather than the devices they use. This is the case because every user *must interact with their user workspace*, no matter which mechanisms they use to connect.

Figure 3.1 shows a representation of how the workspace is the absolute entry point for users. Because it is pervasive across all access mechanisms, the security context can elevate beyond the individual device itself and refocus instead onto the user's workspace. Whether a user connects into a remote application, a local desktop, or via some other future mechanism, the workspace for that user is guaranteed to be composed at the time of login.

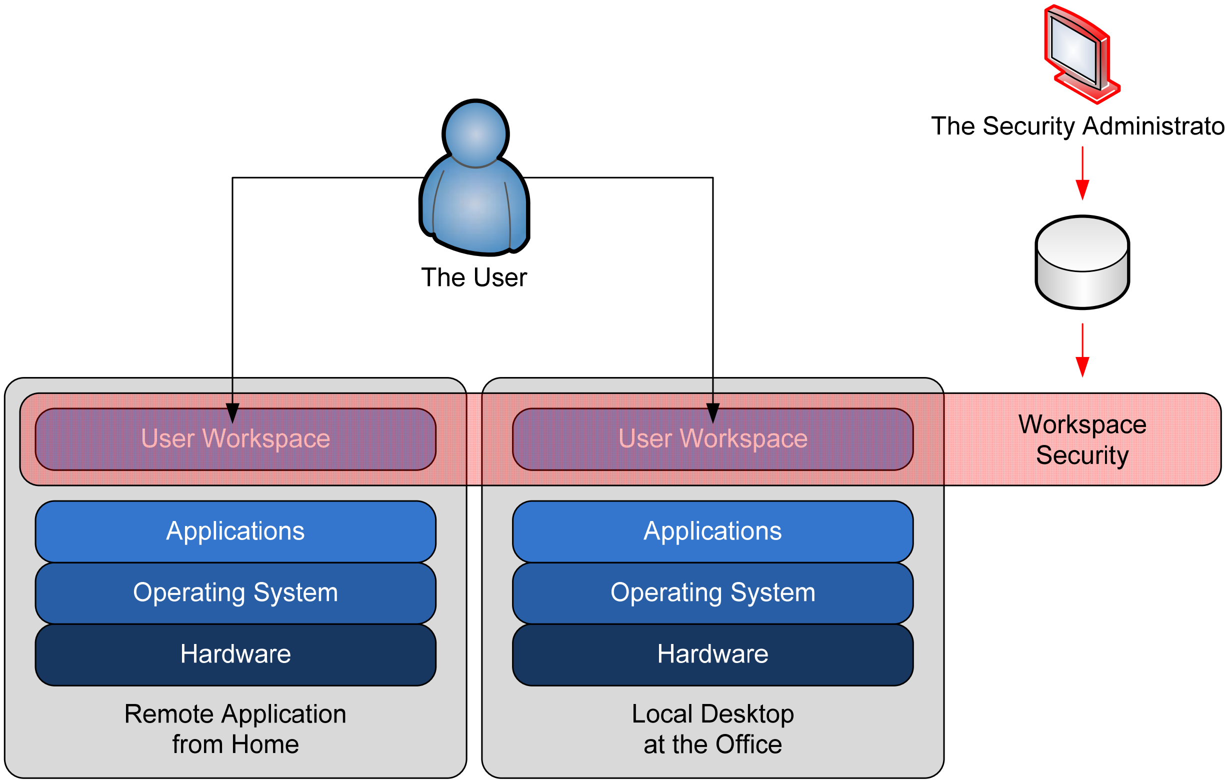

Figure 3.1: Using User Workspace Management, security can be tied to users because users must interact through their workspace. This can be through multiple, or even multiple and simultaneous, interfaces.

It further means that security can be configured once to a centralized location (in this example, the User Workspace Management solution's database) with the assurance of its later distribution to every delivery mechanism.

Note

Chapter 4 will go into the mechanics of workspace composition in greater detail.

Personalization Is Security: An Example

Understanding this new security context is easiest through a simplistic example. You might not necessarily use this example in your environment today, but it shows the power of targeting security to the workspace. Consider the situation where you require a particular folder to be present on each desktop. That folder might contain company data or it might be a pointer to data that is elsewhere. Important to recognize for this example is that the folder must be present and that certain permissions must be set on the folder.

Using the traditional approach, you might ensure the folder's presence through a login script or a Group Policy. Either of these two solutions can indeed create the needed folder on each user's desktop. In fact, creating that folder is a relatively trivial task using either of these solutions. The task of creating that folder is one thing; actually managing it over time and across the many different logins and logouts of that user—some sequential, some concurrent—becomes quite a bit more painful.

The problem lies in the device-centric approaches used by login scripts and policies. The folder in this example can indeed be created using either of these solutions. Once created, however, that folder remains resident in the user's profile. Along with the profile, it then follows the user around among their connections, potentially causing synchronization problems during concurrent logins or leaving artifacts as the profile ages. If, sometime in the future, you need to remove or edit that folder, you'll find a significant lack of easy solutions to do so.

Contrast this limitation to what occurs during the workspace composition process in a User Workspace Management solution. In such a solution, the workspace is dynamically composed at each and every login. Its composition is based on the granular characteristics that are defined within the solution's administrative console in combination with user customizations. There are no worries about artifacts or synchronization problems because the workspace is constructed anew with each and every login.

Using a User Workspace Management solution, both the folder as well as its security privileges can be assured at each and every login—concurrent or sequential—because of this at-every-login composition.

Adding Security to Content and Context

As a result of all this, security can be delivered on-demand in the same way as the previous chapter's personalization settings. In fact, security itself comprises one of the three parts that make up the whole concept of User Workspace Management. Chapter 2 of this guide introduced the three-part color wheel that encompasses these three parts.

Focusing there on the overlap of Content and Context, the previous chapter discussed how content could be delivered to users based on their context. Essentially, the same user can be assigned different content based on who they are or where they are. Although Content and Context are both essential parts of the user's workspace, Chapter 2's discussion fully omitted the third component of workspace security (see Figure 3.2).

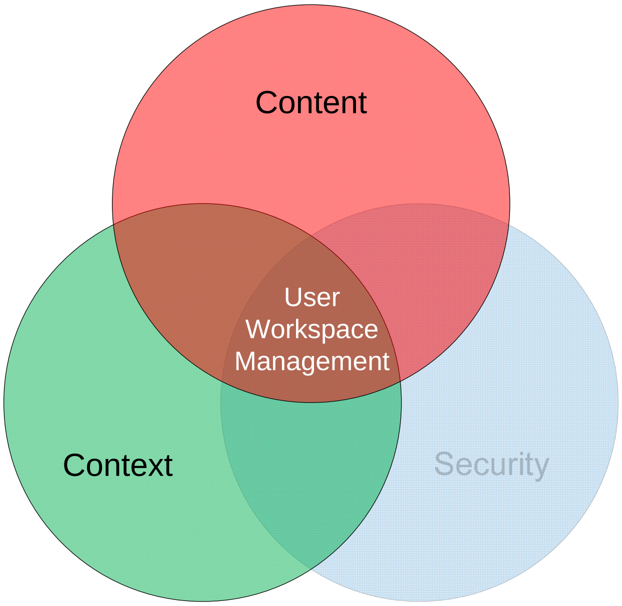

Figure 3.2: User Workspace Management's three components, of which only two were discussed in the previous chapter.

Adding the security component to this discussion, you can see how two new overlaps are immediately created. The first is the overlap of content and security, with the second being the overlap of context and security. Each of these overlaps creates a new area in which User Workspace Management defines and manages the environment.

Content Security

The easier of these two overlaps to initially understand relates to the protection of applications and data. This concept is easy because protecting these parts of the environment are tasks that IT security professionals have done since the very first computers.

As you can see in Figure 3.3, *Content Security* has its focus in exactly that protection of applications and data. Different here, however, is in how those applications and data elements are protected. Traditional IT security solutions, even those based on user profiles, tend to accomplish this by applying security controls at the level of the individual device.

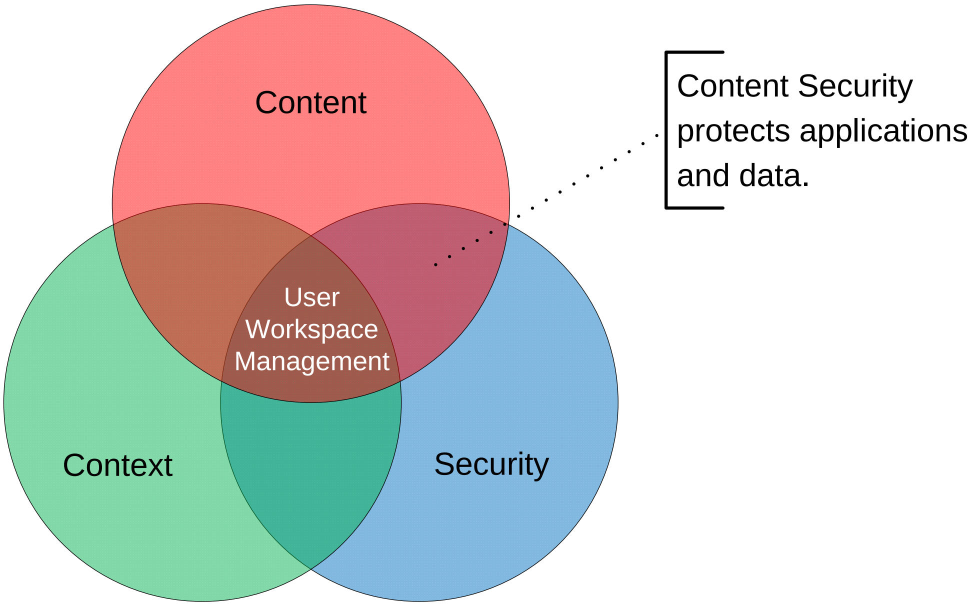

Figure 3.3: Protecting applications and data is the theme behind the overlap in content with security.

However, applying content control through the user workspace layer enables administrators to apply security configurations without needing to care about the device at all. Applications, removable disks, files and folders, network settings, and even session settings are possible elements that can be controlled within the user's workspace.

Security of Applications

Users need applications in order to accomplish their tasks. But at the same time, the principle of least privilege suggests that users should have only those applications that are specifically required. As with data, applications that are not required should be restricted from use.

One challenge in fulfilling this requirement has to do with the limitations of today's application deployment and management solutions. Today's application deployment mechanisms might be able to install applications, *but generally only to a set of computers*. This set of computers might have been created in the deployment tool's management console based on who generally uses which computer; however, at the end of the day, the ultimate installation collection is created as a list of computers.

Today's best-in-class User Workspace Management solutions get around this problem through the granular assignment of application security based on workspace context. Not long ago, this was made possible by pre-installing a set of known applications onto each endpoint. Although each application might be installed everywhere, the permissions to use that application could be granularly assigned to users through the user workspace layer.

This early solution ensured that the right users were always granted access to their needed applications, no matter where they connect. However, as you can probably imagine, the infrastructure requirements to support every application on every device were somewhat non-optimized. Maintaining application installations everywhere often grew to be a challenging task.

A more modern approach integrates the permissions-assignment capabilities of the user workspace layer with the distribution power of application virtualization. In such an infrastructure, the User Workspace Management solution contains and manages the permissions across any and all access points. It then integrates with the application virtualization solution to distribute needed applications to endpoints as needed by the currently logged-in user.

Virtualized applications leave no footprint on the endpoint and can be removed by deleting a set of files, so the reverse can also be true. As the user logs off, their applications are removed from the endpoint, refreshing it in preparation for the next user.

Installing applications is only one component of this category. Once installed, every application has its own set of configurations that IT likely wants to bring under centralized control. Examples of these might be as simple as an Outlook signature file or as complex as a custom application with database configurations. As before, scripting or Group Policies can accomplish this task; however, both of these tools operate with their aforementioned limitations to ongoing management. Further, when applications are provisioned through a User Workspace Management solution, the framework exists in that solution to automatically apply custom configurations as the application is provisioned. As a result, environments that leverage User Workspace Management gain the ability to provision applications and ensure their correct configuration, all within a single solution.

Security of Removable Disks

Removable disks have grown in popularity in recent years. Today, hundreds of models are available that support different capabilities and ever-growing storage sizes. At the same time, removable disks are shrinking in size. Although this makes them exceptionally handy for data transfer, it also makes them a risk for highly-secure environments.

Think for a minute about the last USB hard drive you worked with. In a 2.5” form factor, it is now possible to store upwards of an entire terabyte of information. Drive capacities are only growing, with drives the size of your thumb now supporting multiple gigabytes.

One of today’s biggest security concerns relates to the ability to quietly plug one of these devices into your network and steal critical business data. Yet another security concern relates to removable disks that have been encoded to perform an action as they’re inserted. We’ve all seen the television shows where the bad guys divert someone’s attention, only to surreptitiously plug in a removable device that launches an attack on the local LAN.

The primary issue with these devices relates to the fact that they are at the same time convenient and problematic. Some users have a legitimate need to plug in removable disks for tasks associated with their job roles. Others have no such business need. Unfortunately, as with other all-or-nothing approaches, the option with native solutions is usually limited to either preventing access by everyone or allowing access to everyone. Greater levels of granularity are either impossible or very difficult to manage.

As with applications, a User Workspace Management solution enables removable drive access to be defined by users, instead of by devices. Using such a solution, users who are permitted to use removable devices will be able to do so no matter where they login.

Security of Files and Folders

The earlier section's "folder-on-the-desktop" example does a good job of explaining how file and folder security can be dramatically enhanced through a User Workspace Management solution. Also possible with this example is the ability to deposit necessary shortcuts to files and folders, or other resources on the user's desktop, Start Menu, or other locations.

Yet another useful application of User Workspace Management for files and folders has to do with certain remote application infrastructures. These solutions provide an easy ability to offload application processing back to servers in the data center. However, although their offloading and remoting capabilities are usually well designed, a regularly-occurring problem has to do with provisioning the connections for users to actually navigate to their needed remote applications.

Consider the situation where you have a custom application, ABC App, which is hosted atop Microsoft's Remote Desktop Services or Citrix XenApp. This application provides services that are needed by a limited set of users in your business. Due to limited authentication within the application itself, users who should not have access must not be able to launch the remote application.

Using a User Workspace Management solution, it becomes possible to distribute the individual connection files that relate to this remote application. Rather than storing these files on a file server where they may be difficult to find or available to inappropriate personnel, such a solution can provision the remote application's connection file *into the user's workspace*.

Once the application is a part of the composed user workspace, administrators for the application can be assured that its users will always be able to access the application. No matter whether they're connecting via desktops or even through an external interface, their connection to ABC App is always available. Conversely, those users who should not have access will not have the capacity to locate or use the connection because it is not available in their workspace.

Security of the Network

It has been said before in this guide that an effective User Workspace Management solution can customize the workspace based on the context of the user. That user's context can be related to the delivery mechanism they're using—such as a Remote Desktop Services session versus a traditional desktop. It can also be related to the location from which a user attempts to connect. Users often have access to your network through many different IP address ranges; for example, one range for traditional VPN access, another for internal resources, and even another for users in an extranet.

Your User Workspace Management solution should provide the ability to customize or lock down the workspace based on a user's network point of entry. This context-sensitive network security provides a way to lock down resources when users enter the network through untrusted connections, such as limiting access to sensitive data through outside connections. Its knowledge of the user's entry network further enables administrators to tailor the workspace for added protection, such as adjusting host-based firewalls based on the user's context.

Context Security

The third and final overlap in this three-part color wheel deals with the combination of Context and Security. This guide has many times discussed how users in a User Workspace Management solution can login from anywhere and get the same environment. It has also talked about the security concerns related to the everything-for-everyone configuration.

Most IT organizations build multiple access infrastructures for their users; however, most of those organizations also want to limit inbound users of those infrastructures to only those users who specifically have need for them. Consider the "work from home" scenario that has been discussed a few times to this point. Although some organizations might create such an environment for all of their employees, others might desire to limit work-from-home capabilities to only a limited set of employees.

Context Security (see Figure 3.5) concerns itself with fulfilling the desire to lock down these access infrastructures to predefined individuals. As Figure 3.5 shows, Context Security enables the filtering of available delivery mechanisms based on administrator-defined parameters. Those filters can be based on the user's location or the device they're using to connect.

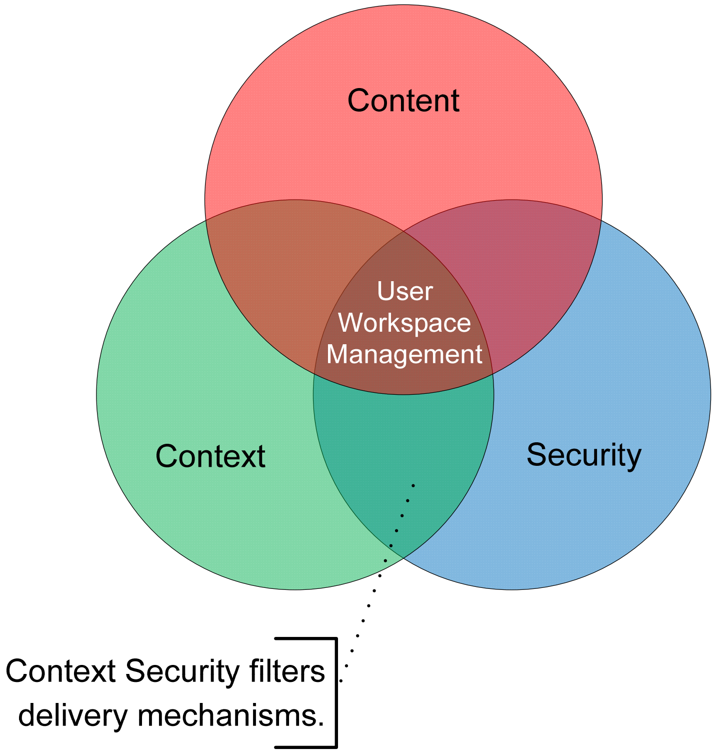

Figure 3.5: Context Security enables administrators to identify which users get which resources based on the user's context.

Location Security

It should be obvious to the security-minded IT professional that delivery mechanisms that are enabled for Internet access can be used anywhere the Internet is available. This empowers users to access and complete their work from anywhere. It also introduces the risk of exposure for data or even litigation when data is accessed in inappropriate geographic areas.

Consider the situation where a business is working on data that is appropriate for its geographic area. That data might be financial data or even governmental data that must not pass outside the boundaries of the country. Location security in User Workspace Management enables the workspace to be granularly provisioned only to those areas that are appropriate for the data.

Device Security

Individual devices themselves can also be a point of security concern. For example, a user's corporate-provided laptop is usually a managed item, containing the necessary protection measures (anti-malware, anti-hacking, firewalls, and so on) that make it an acceptable access point. In contrast, a user's desktop at home has no such protections. That desktop might be installed with anti-malware tools, or it might have been infected with keylogging malware that can capture data from every connection.

Environments that want to provide Internet-based access to their users might also want to control that access to managed assets only, such as the corporate-sponsored laptop. Corporate-managed assets can be further controlled by integrating User Workspace Management with a Network Access Protection (NAP) solution. This integration provides a way to restrict access to only those resources that are properly secured, such as having the right updates, correct firewall settings, up-to-date anti-malware signatures, and other key security configurations. With User Workspace Management's device security capabilities, the user workspace can be granularly provisioned only to those assets which IT and security consider to be appropriate.

Integrating Security with the Delivery Infrastructure

The final step in this process is the integration of workspace security with the rest of the delivery infrastructure. Remember that personalization and security configurations within a User Workspace Management solution tend to enable control for the user workspace layer alone, typically leaving each of the layers below to their own solutions for management and security.

It is for this reason that this chapter's title is, in a way, slightly misleading. Depending on the delivery infrastructure, there are some elements of security that still require a device-specific approach. One example of these elements is the need for regular patching of the core OS. This need fairly obviously is not a configuration that would be applied at the user workspace layer—most users don't have the permissions necessary to apply patches and reboot the computer (not to mention such a task is probably something that administrators wouldn't want).

Properly integrating user workspace security with the rest of the delivery infrastructure requires a holistic approach with other solutions. Those solutions might handle elements such as OS and application patching. They might handle firewalls and core application installations. They might even handle the application provisioning, as explained earlier. Your User Workspace Management solution should include the necessary built-in integrations to enable it to work with your existing security and delivery solutions.

At the same time, incorporating a User Workspace Management solution into an existing infrastructure requires a re-analysis of which solution should provide which services. By adding User Workspace Management into your environment, you might find that configuration control via solutions such as login scripts or Group Policy is no longer relevant. The same addition might eliminate some of the steps necessary for application installation or security configuration control.

Pervasive Personalization Can Mean Pervasive Security

You've likely continued reading this guide because the power of pervasive personalization is attractive. Enabling the decoupling of the user workspace from its underlying delivery mechanism also enables you to pull user customizations "out of the box." Thinking globally about the workspace rather than locally brings significant administrative advantages, while making life easier for your users.

At the same time, as you've discovered in this chapter, creating this environment of pervasive personalization can mean one of pervasive security as well. Security settings that might have been challenging to manage using other solutions grow trivial as they migrate with users and their unpredictable behaviors. In the end, even the least-typical security administrators can see how it improves both their job as well as the experience of their users.

To this point, all three of this guide's chapters have touched on the mechanics of how User Workspace Management actually accomplishes this mission. This light touch on the bits-and-bytes of these solutions is purposeful, and arguably necessary. The paradigm that is User Workspace Management can be entirely new for many IT professionals, making it important to understand *where* it benefits before the conversation on *how* it benefits.

Chapter 4, the final in this guide, finishes with that detailed look at User Workspace Management's technical underpinnings. It will also discuss the steps necessary to incorporate a potential solution into your environment today. You'll find in its pages that although its concepts are indeed a shift in thinking, actually transforming to an environment of User Workspace Management can be easier—and involve less impact—than you think.

Download Additional Books from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this book to be informative, we encourage you to download more of our industry-leading technology books and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.