White Paper

Workplace Mobility, Consumerization, and Alternative IT Strategy Drive End-user Computing Transformation

By Mark Bowker, Senior Analyst

December 2013

This ESG White Paper was commissioned by VMware and is distributed under license from ESG.

© 2013 by The Enterprise Strategy Group, Inc. All Rights Reserved.
Contents

Workplace Mobility and the Consumerization of IT ................................................................. 3
Influence of Line of Business (LOB) Owners ........................................................................... 4
Moving from Device-centric to User-centric Management ...................................................... 5
Centralized Management ......................................................................................................... 6
Application Migration ............................................................................................................... 7
Mobile Access to Applications ................................................................................................. 7
Holistic Management Visibility ............................................................................................... 8
Embracing the Cloud ................................................................................................................ 9
The Bigger Truth ...................................................................................................................... 10

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

© 2013 by The Enterprise Strategy Group, Inc. All Rights Reserved.
Workplace Mobility and the Consumerization of IT

The key challenges in managing today’s desktop and mobile computing environments are security, cost, and compliance. More specifically, these challenges relate, respectively, to the needs of IT to secure confidential data resident on endpoint devices, the operational costs related to endpoint device management, and the enforcement of end-user compliance with regulatory requirements (pertaining to information security, privacy, and retention) as shown in Figure 1.¹

![Figure 1. Top Five Most Significant PC Challenges](image)

These challenges are made exponentially more difficult by three recent trends:

- Application and desktop transformation (alternative application delivery models)
- Workplace mobility
- Bring your own device (BYOD) initiatives

As the technological sophistication of employees grows, so does the complexity of end-user computing environments. Traditional methods of managing the desktop and delivering applications to users do not provide the flexibility IT departments need to support modern-day organizations. Moreover, IT departments now need to deal with a surge in the number of remote and mobile employees; a proliferation of alternative endpoint devices, such

¹ Source: ESG Research Report, *Desktop Virtualization Market Evolution*, February 2013. All ESG research references and charts in this white paper are taken from this research report unless otherwise noted.
as smartphones, tablets, and thin clients; and smartphone users who want instant access to corporate applications across all their devices—with the same optimal experience.

If one trend is most responsible for changes inside the IT department, it’s employees’ desire for consistent, secure access to their applications and data on their smartphones, iPads, and Android devices. Once an employee takes her smartphone to an app store, she’ll want that same instant access to applications in her corporate work environment. For this employee, patiently waiting for IT to roll out a new application is a thing of the past.

This new mindset of tech-savvy employees is putting pressure on IT departments. The big challenge for IT is securely supporting and managing employee-owned devices across heterogeneous platforms while keeping personal and business environments separate. In parallel, IT also has to manage a growing number of applications and aging PCs, and provide 24/7/365 service levels that meet the demands of the business. To solve this problem, CIOs have turned their search to a control plane that brokers multiple connections, delivers to multiple endpoints, and enables their IT administrators to set and maintain policy while improving the end-user experience and, ultimately, employee productivity.

CIOs are responding to the rapid proliferation of endpoint devices and new applications by:

- Thinking of end-users as IT consumers of alternative deliver models. This begins by shifting away from a device-centric model to a strategy that focuses on user centricity.
- Understanding the business drivers and use cases of the line of business owners.
- Measure IT services and support effectiveness by the way it affects a business’s top-line revenue.
- Centralizing desktop and application management.
- Providing centralized access to desktops, applications, and data.
- Positively impacting users’ productivity and computing experience.
- Leveraging cloud consumption models as part of a holistic application and data delivery strategy.

Influence of Line of Business (LOB) Owners

The IT evaluation and purchase process is also changing, with business managers getting increasingly involved in these two areas. Many are spearheading IT product and service selection; some even act as the lone decision makers. These managers are also contributing to the rise of “shadow” or “rogue” IT by making technology purchase decisions without involving the IT department. (Their unilateral decision making is due partly to the shortcomings of in-house IT and partly to the availability of cloud computing services.) The choice to source infrastructure and business applications as cloud-based services is being driven by several factors, including lack of understanding on the part of the IT organization about solution requirements; length of purchasing and deployment processes; and, simply, convenience. There’s no better example of the part that convenience plays in the IT purchasing process than the fact that in many organizations, LOB owners have discovered they can order and run SaaS applications without IT knowing about it.

That situation is the reason so many employees use online applications like Dropbox: They have discovered that if they leave their employer suddenly, they can still retrieve their files by downloading them online. For IT, this represents a problem—there’s no corporate account set up to control user access to those files, which may be critical to the organization. So IT is currently trying to figure out how to have corporate users consume a Dropbox-type environment through IT, or how to enable some type of authentication and single sign-on in that environment.
Be involved:
- Create a new collaborative engagement model: Plan strategy sessions with LOB owners to understand their business and IT requirements.
- Demonstrate how technology has advanced and share alternative computing experiences with LOB owners.
- Present short-term goals and long-term strategies that are inclusive of their requirements, business policy, and any unique end-user responsibilities.
- Share economic impact including annual benefits and any investment plans.

Moving from Device-centric to User-centric Management

In addition to an influx of devices, applications, and LOB activity, desktop transformation is also being driven by the need to simplify application or operating system deployments and upgrades, patch management, desktop provisioning, and endpoint management. Desktop transformation strategies need to be targeted at reducing endpoint costs and management complexity by taking the user settings profile, the operating system, and the application out of the locked-down desktop environment and managing them separately through a universal delivery access point.

The proliferation of devices and application delivery models in today’s organization means that all organizations will need to shift from a device-centric management environment to a user-centric one. And that shift means that, in all likelihood, the IT department needs to deploy at least several of these six application desktop delivery models:
- Traditional – locally installed application coupled to the endpoint
- Desktop virtualization – centrally hosted image that is delivered over the network
- Application virtualization – locally encapsulated applications, shared executable, and centrally executed and streamed to endpoint
- SaaS – applications are hosted by a vendor or server provider and made available to users over the network, typically the Internet
- Web applications – i.e., HTML5, Java, or Visual Basic/.NET
- Mobile application development – i.e., Apple AppStore or Windows Phone Marketplace

An IT department that focuses on just one way to deliver applications and desktops may miss out on the advantages of the others. This theory holds true in ESG research that validates how IT is transforming its application delivery strategies as shown in Figure 2. Applications are being driven toward a web interface and designed for mobile, but still require a central access and control point. It’s the job of today’s CIOs to invest in a desktop transformation strategy that incorporates all aspects of the delivery models, endpoints, and user roles.
Centralized Management

When user desktops are virtualized and centralized in the data center, IT can simplify desktop management, increase control over desktop assets, and improve user service levels. Desktop management optimization controls enable IT administrators to customize protocol settings to adjust bandwidth use and session density by user, use case, or available network conditions. Centralized desktop management can also enable IT to deploy lower-cost, stateless desktops while providing users with a consistent, personalized experience and faster desktop log-in times.

By centralizing Windows desktop image management and delivering Windows as a service, IT can streamline tasks like updates, migrations, backup, and recovery. Windows desktop images can be delivered to physical endpoint devices and unmanaged virtual machines where they are run to ensure users get the best experience by taking advantage of local compute resources. Once on the local endpoint device, the desktop image stays in sync with the centralized desktop image, helping to simplify backup and recovery tasks while minimizing the effects of device failure and reducing user downtime.

The desktop experience can also include VoIP, with users able to access an integrated softphone. Even USB-based webcams and microphones can now be optimized to work with consumer-oriented communications software. As such, communication and collaboration should be considered as a larger part of the overall strategy that enables users to consume desktops, applications, and data from a secure centralized location. Many companies are looking to create an application store for the business where IT controls who can provision desktops and applications, and end-users are empowered to self-provision, self-help, and self-maintain their workspaces based on predefined IT and business policies. The value for IT and the end-user is a single access and control point for desktops, applications, and data.
Aggregate the control point:

- Point solutions may provide a short-term stop gap, but a holistic management approach will help streamline and secure for the future.
- Consider how a storefront for users would benefit both IT and its consumers.
- Be prepared to demonstrate any new policies and highlight advantages from an end-user perspective.

Application Migration

Organizations frequently need to migrate an application from one environment to another. The process of application migration—which encompasses user downtime, cycles of QA, and uncertainty about whether the application being moved will have conflicts or run seamlessly with other applications—is one that IT organizations perennially brace themselves for.

Most applications are not portable; they are designed to run on the platforms they were developed for. Migrating legacy applications has always been a Herculean task, but the truth is, migrating “modern” applications is no piece of cake—the platforms and operating systems they are developed for are in a constant state of flux. Try moving a piece of software from an on-premises application server to a cloud computing environment. It should run fine. But often it doesn’t.

Virtualizing an application—running it centrally from the data center and deploying it locally to physical or virtual desktops or on USB drives—can take the sting out of application migration. Application virtualization aids in application migration by separating applications from their underlying operating systems, thereby reducing conflict between the operating system and other applications. Desktop administrators using application virtualization can eliminate application conflicts by isolating applications from one another and the underlying operating system and putting the application into a single executable file that can be easily deployed to many endpoints. By delivering this file to a variety of, for example, Windows platforms, the virtualized application is completely isolated from the operating system and behaves the same way across platforms.

Mobile Access to Applications

IT departments must not only support a widening variety of endpoint devices, but they also need to deal with mobile workers who will be connected to the corporate WAN one moment and a Wi-Fi network in a coffee shop the next. The employee who used to have one device for work now may have three devices—a laptop, a smartphone, and a tablet—if not more. He will use the laptop for work that requires his highest productivity, use the smartphone for viewing e-mail, and use the tablet as an in-between device. IT needs to provide this multi-device employee with mobile access to all of his applications by creating policies that give that user secure and flexible anytime access and a familiar desktop experience on all his devices. That policy needs to include context-awareness—the ability to inform IT who the specific user is; what device he is on; what network he is on; which operating systems applications, files, and data the user needs access to; and that the proper security policies are applied automatically.

A common mobile application is online file sharing (OFS), which has proven useful in employees’ personal lives, but danger looms when it is used in a corporate environment. ESG asked respondents who indicated that their organizations are neither using nor currently interested in OFS to explain why this is the case. As clearly demonstrated in Figure 3, concern over potential security vulnerabilities—such as data loss, theft, or risk of regulatory compliance violations—is the most-cited reason respondent organizations are not deploying OFS.

---

IT essentially loses control of data and security vulnerabilities are opened with OFS use. This promotes an even greater need for a holistic approach that incorporates mobile applications, SaaS applications, and web applications under a single management umbrella and control point. Trying to individually manage and control these different application delivery models will be cumbersome and fall short of the agility required to support modern applications.

**Holistic Management Visibility**

As companies aggregate application and delivery models across its end-users, they also have the opportunity to improve the visibility into the end-user’s workspace and analytics across the company. The many benefits IT stands to achieve center around the ability to automate tasks that have been cumbersome and time consuming. As these technologies automate deployment and updates, and enable self-service, IT also needs to capture a complete picture of the environment that projects usage information, potential trouble zones, and overall system health. Real-time analytics will help with faster remediation and should ultimately include automated chargeback and showback capabilities to assist IT with transparency back into the business around costs and utilization.

The consumption models may differ in delivery and management operations, but IT needs to keep a full perspective on the holistic environment. Planning to embrace multiple delivery models such as SaaS, VDI, or application virtualization through a centralized control plane enables IT to capture ingress and egress analytics that can be

---

**Figure 3. Top Five Reasons Organizations Have Not Deployed OFS**

Why do you believe that your organization has not deployed and has no plans or interest in deploying Online File Sharing and Collaboration solutions? (Percent of respondents, multiple responses accepted, N=86)

- Security concerns: 57%
- Current tools meet our needs: 37%
- Service cost: 34%
- Don't require collaboration and document management capabilities provided by Online File Sharing and Collaboration solutions: 30%
- Data ownership concerns (i.e., employer vs. employee): 27%

**Source: Enterprise Strategy Group, 2013.**
turned into reports, real-time analysis, and a system that captures meaningful intelligence, which is used in planning, remediating, and, ultimately, in delivering the optimum end-user experience.

**Embracing the Cloud**

Many CIOs looking to extend existing desktop virtualization, SaaS applications, and user data management as they transform their organizations’ desktops into highly available, agile services are virtualizing their on-premises applications and putting them into a public or private cloud. This “hybrid” approach introduces capabilities where desktops can be delivered through the cloud, but all of the control can reside on-premises, delivering the best of private and public cloud together. More companies are turning their physical data centers into virtual data centers hosted by regional suppliers, with their applications and an infrastructure of virtual servers and desktops pumped over the Internet. This approach enables customers to deliver services via the cloud in a much more controlled and secure way.

Remote desktop virtualization provided by a cloud computing provider is similar to SaaS and is called desktop-as-a-service (DaaS). DaaS provides flexible deployment options and removes many infrastructure costs. In this scenario, the DaaS service provider hosts and maintains the customer’s compute, storage, and access infrastructure, and also is responsible for the applications and application software licenses needed to provide the desktop service in return for a fixed monthly fee.
The Bigger Truth

To streamline the process of maintaining desktop environments, many IT managers are turning to desktop virtualization. But as end-user computing environments become increasingly more complex due to trends in BYOD, changing application delivery models, and worker mobility, IT managers need to think beyond desktop virtualization.

Until recently, IT departments responded to desktop security challenges by controlling the endpoint device—locking it down and “hot-gluing” the USB drives shut. That is no longer possible in the organization of today. It’s only a matter of time before IT will be managing the user rather than the user’s device. Today’s desktop and application delivery strategies entail shifting from a device-centric approach to a user-centric one, and IT managers need to think beyond desktop virtualization and incorporate a contextual awareness that will tell them which user is working on which endpoint device.

But at the end of the day, it’s not just about putting Windows on a smartphone or an iPad—it’s about how delivering Windows or an application to any device truly improves end-user productivity. At the same time, IT needs to be able to maintain efficient control and security measures through a single control point and common policy engine that aligns with business process and policy. This control point ensures that real-time analytics will capture information displayed in a management platform that enables IT to maintain the delivery of applications, desktop, and data, as well as arming IT with intelligence on usage, chargeback, and performance information that can be shared with the business owners.

As businesses build out desktop transformation strategies, they should consider solutions that incorporate the multiple delivery models, embrace endpoint choice, and incorporate a safe and secure environment. Trying to piece parts together may help with short-term challenges, but look to discover solutions that holistically tie together multiple delivery models, physical PC management, and user data management. In doing so, IT can help embrace new applications and devices without compromise.