Enterprise Strategy Group | Getting to the bigger truth.™

White Paper

Workplace Mobility, Consumerization, and Cloud Drive End-user Computing Transformation

By Mark Bowker, Senior Analyst

January 2016

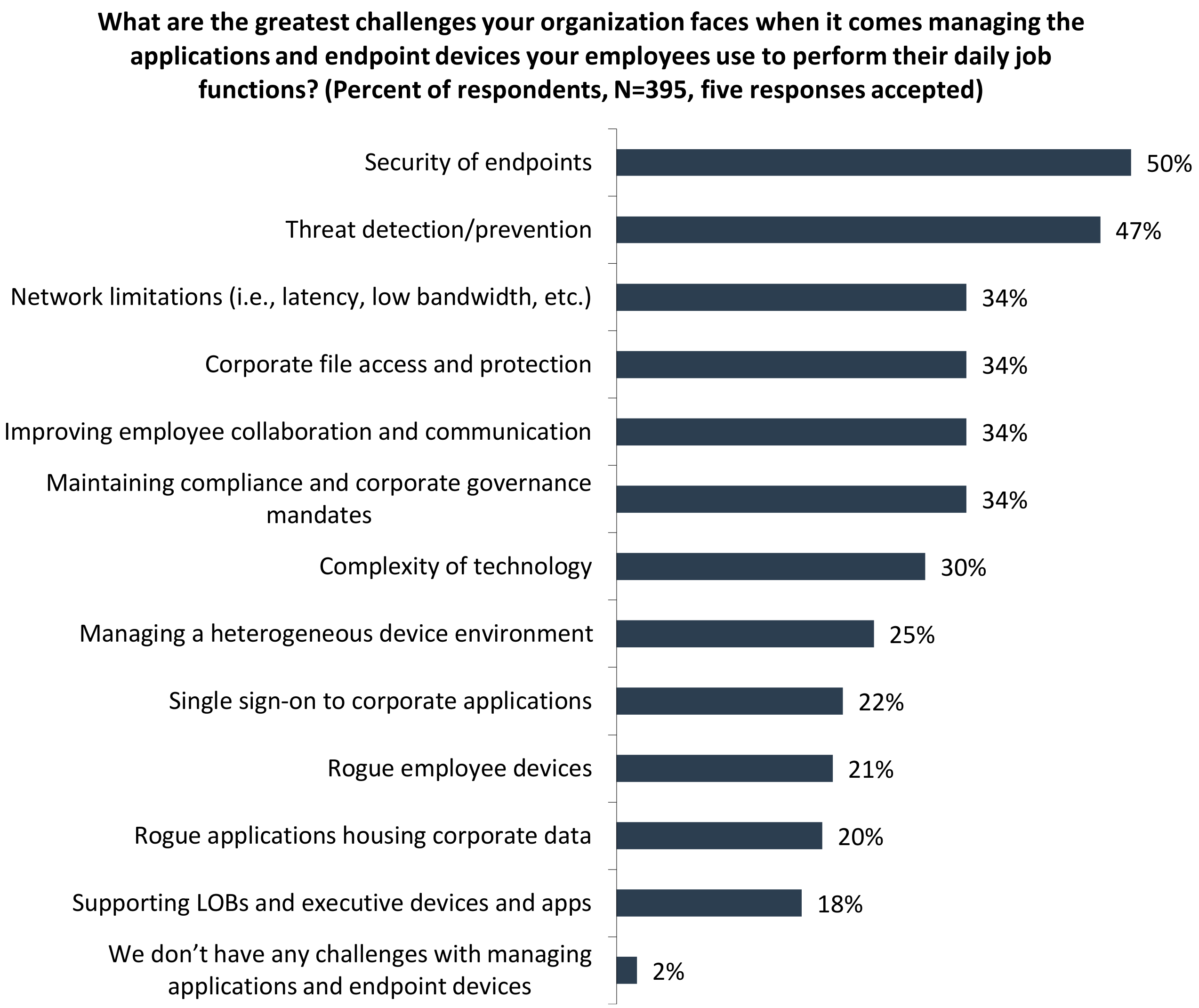
This ESG White Paper was commissioned by VMware and is distributed under license from ESG.

Contents

Workplace Mobility and the Desktop Transformation

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. Most Significant Challenges with Application and Device Management



Source: Enterprise Strategy Group, 2016

These challenges are made more difficult by three recent trends:

- Application and desktop transformation (alternative application delivery models)
- Bring your own device (BYOD) initiatives
- Competing desktop and application delivery models that lack unified management
- The desire of organizations to embrace a cloud-first approach with faster speed of scale and elasticity

[1] Source: ESG Research Report, Security, Productivity, and Collaboration: Trends in Workforce Mobility, February 2016. All ESG research references and charts in this white paper are taken from this research report unless otherwise noted.

- New security considerations posed by virtual workspaces

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 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 makes use of an app store on her smartphone, 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.

The big challenge is the confluence of the proliferation of devices, the multiplicity of application types and delivery technologies, the need to support greater business agility with a cloud-like mentality around workspace service delivery, and the need to do all of this with a multi-layered, defense-in-depth approach to security. CIOs are responding to these challenges by seeking a new architecture optimized for the mobile cloud era and are also responding to the rapid proliferation of endpoint devices and new applications by:

- Unification of the management environment that can bring together previously disparate pools of desktop services capacity across hybrid environments that straddle on-prem and cloud-hosted.
- Enabling "just-in-time"desktop and application delivery, which offer personalized/customized digital workspaces with:
  - A contextual, role-based security policy that follows users.
  - A consistent user experience across any device, optimized for mobile endpoints.

CIOs are also exploring alternative security technologies to detect and prevent threats in an increasingly virtualized end-user computing landscape.

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.

As a result, IT needs to enable the delivery of workspace services with the speed and elasticity of capacity that LOBs are finding in cloud-hosted services. Addressing this requires a new paradigm for managing a portfolio of desktop delivery technologies that straddle the right mix of on-premises, cloud-hosted, and hybrid cloud infrastructure, supported with a flexible, real-time policy system that's centrally administered with intelligent, fine-grained control of the user experience, combined with single sign-on.

Be involved:

- Plan to manage capacity across any combination of on-premises and cloud for a future-proofed purchasing model.
- Set the bar high and target a high-performance user experience that adapts to challenging network conditions, and that is optimized for mobile device, built for the cloud, and accessible on multiple device types.
- Create a new collaborative engagement model: Plan strategy sessions with LOB owners to understand their business and IT requirements. Include security, compliance, and collaboration in these discussions.
- 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

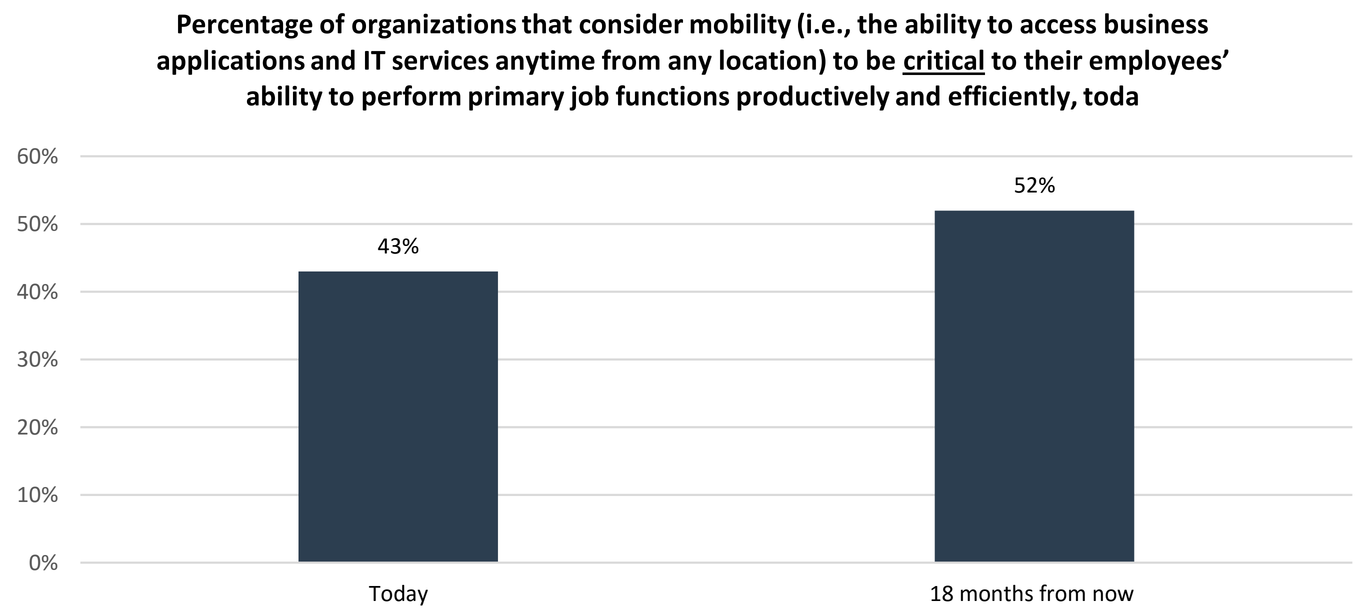
In addition to an influx of devices, applications, and LOB activity, desktop transformation is also being driven by the need to simplify application or operating system deployments and upgrades, patch management, desktop provisioning, and endpoint management. Desktop transformation strategies need to 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 as businesses look to improve their enterprise mobility strategies, which can enable organizations to seamlessly connect a mobile workforce to business and productivity applications and related content for the ultimate goal of increasing productivity and/or revenue. The strategy includes the ability to balance employee privacy requirements with enterprise security goals, enable seamless connectivity across a variety of device types (whether corporate or employee-provided), and improve the way employees collaborate and communicate. ESG research validates the importance of these strategies for employees to perform their primary job functions productively and efficiently, as shown in Figure 2. It's the job of today's CIOs to invest in mobility strategies that incorporate all aspects of the delivery models, endpoints, and user roles.

Figure 2. Percentage of Organizations that View Mobility as Critical to Their Employees Set to Increase



Source: Enterprise Strategy Group, 2016

Centralized Management and Just-in-time Delivery

When taking a mobile-first cloud-first approach in which user applications and desktops are virtualized and centralized in the data center or from an as-a-service-based licensing consumption model hosted in the cloud, IT can simplify desktop management, increase control over desktop assets, improve user service levels, and manage and secure data more effectively. 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 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 image management, 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.

IT can also deploy desktops at scale with unprecedented speed, leveraging technology for fast, pain-free delivery of desktops that are freshly provisioned at login. It becomes possible for IT to rapidly create thousands of desktops in minutes, making maintenance windows a thing of the past. Architectures can also be created that improve failover and survivability for maximized session uptime at massive scale. The ultimate goal is to achieve a desktop experience for the end-user that feels persistent, but is built on stateless, floating pools of desktop capacity that are simply managed by IT. New capabilities and tools that can leverage the underlying hypervisor in a VDI environment can take a live running virtual desktop and rapidly clone it as access is required. In addition, IT can use technologies that "virtualize above the OS" with application and user-writeable layers that attach role-based stacks of applications and user personalization, on the fly as the user logs in. When IT taps into these capabilities, they have achieved the nirvana of VDI, realizing the benefits of creating a stateless, non-persistent desktop for its end-users that feels customized and personalized, but that is destroyed upon logout.

The combination of rapid provisioning technologies, application layering, and user personalization is delivering a new reality for IT that enables them to offer LOB owners the virtues of cloud-like elasticity of scale, but that is securely hosted within private data center infrastructure, combined with a user experience that feels personalized, and akin to a physical laptop, as well as a rich multimedia desktop experience.

The desktop experience can also include enhanced collaboration capabilities, with users able to access an integrated softphone or applications such as Microsoft Skype for Business. 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 an overall IT 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:

- Deliver a persistent experience without having to manage a discrete desktop image that is tied-up or dedicated to each user.
- Enable cloud-like speed and elasticity of scale with technologies that rapidly turn up virtual desktops as users need them.
- Use above-the-OS virtualization technologies to layer-on role-based application suites and user personas for a fully customized user experience that feels persistent.
- 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.
- Take on the challenge of speed of deployment at scale.

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, the smartphone for viewing e-mail, and 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.

Threat Detection and Prevention in a Virtualized World

Today's CIO and CISO are continually working to ensure their organizations stay out of the security-breach headlines. The virtualized, mobile workstyle is creating new security considerations for IT. These concerns are related to i) the proliferation of virtual users and their ability to access sensitive data from a wider array of devices and network locations, and ii) the sprawl of virtual users within the data center itself, hosted in close proximity to other mission-critical assets and infrastructure.

The first concern creates risk of the typical Edward Snowden scenario with an insider being permitted to offload sensitive information either intentionally as in the case of espionage, or unwittingly as in the case of bypassing a security practice in order to streamline a task. Now IT can use workspace environment management technologies that can define and enforce role-based policies. These policies can dictate what security-sensitive client-side features (e.g., clipboard, USB access, printing, client drives, etc.) should be enabled/disabled, and under what circumstances. For example, a user accessing her virtual desktop from an unsecured, potentially hostile network location should have most of these disabled upon login.

The second concern is related to the proliferation of "east-west" traffic between virtualized and non-virtualized workloads within the data center. This scenario creates the opportunity for cross-contamination or spread of user-originated malware or viruses that gain entry via corporate e-mail or web, within the virtual desktop. In this scenario, an unknowing worker is the first touchpoint in a breach that works its way across the infrastructure, exiling sensitive data to the outside world as machines are compromised.

Both of these scenarios require new tools and capabilities. IT needs a combination of i) centralized management of client side features through policy that's smart, dynamic, and contextually-aware, along with ii) a software-defined data center with network and security virtualization that's able to place each virtual user in a micro-segmented network container that controls the flow of traffic with the surrounding infrastructure.

Holistic Management Visibility

As companies aggregate application and delivery models across their end-users, they also have the opportunity to improve visibility into the end-users' workspaces and analytics across their organizations. 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 (either from private data center or cloud-hosted), or private-infrastructure-managed through a cloud-hosted control plane enables IT to unify all pools of desktop or application capacity, no matter where they reside, while capturing meaningful real-time analytics that can be turned into reports, real-time analysis, and a system that places IT managers in a proactive management stance instead of one that's reactive, 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.

Display Protocols Matter

The display protocol has always been a primary decision factor, but the next generation of remoting protocols is creating an even higher priority to ensure that it is optimized for the mobile cloud era. CIOs and their architects need to look for solutions that offer multiprotocol functionality that can target various use cases including zero clients, thin clients, PCs, and mobiles, with the right protocol optimized for each scenario. Next-generation protocols based on H.264 are dramatically improving the mobile user experience with heterogeneous endpoint support, lower bandwidth consumption, TCP and UDP support, lower battery consumption on the device, and adaptive adjustment to high latency or lossy networks. The benefit is that IT can handle a much wider spectrum of use cases with minimal impact to the endpoint device so that the experience can be preserved.

The Bigger Truth

To streamline the process of maintaining desktop environments, many IT managers are turning to mobile cloud-first approaches to application and desktop delivery. 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 about hybrid consumption models that work at scale and address security threats.

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 embrace a single sign-on experience for end-users 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 delivering applications to any device and improving 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, and arms 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 organizations should 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.

ESG Enterprise Strategy Group | Getting to the bigger truth.

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.esg-global.com