



ESG Market Summary: Workplace Delivery

Desktop, Application, and Mobility Platforms for Hybrid End-user Computing Environments

This report addresses:

- The market status of workplace delivery today, and related issues challenging IT.
- The workplace delivery platform, what it is, and how it addresses the IT security conundrum of securing corporate access while improving the end-user experience.
- The current, planned, and future market vision and transition strategies.

Publication date: Monday, 12 January 2015

This export was generated by user irp-guest@esg-global.com at account Guest on 5/25/2019 from IP address 54.167.47.248.

© 2000 - 2019 Enterprise Strategy Group, Inc. All Rights Reserved

Using Interactive Document Server technology from Publish Interactive

Table of Contents

Introduction	3
Mobility is Driving a Change in Desktop and Application Delivery Trends.....	3
The Transition from a Locked-down Environment to a User-centric Environment.....	4
The State of Workplace Delivery	5
Top Challenges Confronting Corporate IT	6
The Hybrid Delivery Environment	7
The “Dissection” of the End-user Work Environment	8
Workplace Delivery Platform	10
Complexity Breeds Opportunity for a New Approach	10
Determining Appropriate Consumption Models	11
Workplace Delivery Strategy.....	13
Context Awareness.....	14
Market Vision.....	15
Current, Planned, and Future States	15
The Bigger Truth	17

Introduction

Mobility is Driving a Change in Desktop and Application Delivery Trends

The desktop and application delivery market has experienced tremendous change over the past several years, affecting organizations' mobility strategies. A wide range of new solutions, devices, and service-based delivery models have proliferated and evolved. This "consumerization of IT" has resulted in a plethora of alternative endpoint devices flooding the corporate landscape. Today's knowledge worker no longer consumes information solely on a single company-issued device, but rather on a combination of laptops, smartphones, tablets, and thin clients.

Given that, organizations are increasingly embracing a variety of alternative desktop and application delivery models, which often use a combination of software-as-a-service (SaaS), Web-based, and mobile applications for their flexibility, convenience, and ability to scale on demand.

Lying at the heart of these alternative desktop and application delivery models is something that can be characterized as a business goal as much as it is an IT headache—namely, the need to meet end-user demand for convenient and reliable access to applications and IT services from any location via any number of devices.

Previously conducted ESG research found that end-user demand for alternative devices was cited by 44% of respondents as a factor responsible for the changing profile of endpoint device usage among those organizations surveyed.¹

While these alternative delivery models are more user-centric, they are also more challenging for IT to manage and keep secure. How? Traditional, manual methods used for supporting, managing, and securing these alternative endpoints on a device-by-device basis—along with numerous and disparate operating systems—are rapidly exhausting IT resources and rendering tactical IT approaches untenable. Without automated processes to monitor, manage, assess, and remediate prospective threats and suspicious or malicious behavior on the network, the enterprise is left virtually unprotected.

In tactical-focused, hybrid delivery environments, (where a hybrid delivery environment is defined as a combination of traditional, private, and public cloud environments), policies and settings across endpoints and application delivery models fail to propagate. In this scenario, disparate applications and systems live in their own silos, and don't "talk" to one another. Not only does this create a significant gap in network security, but it also creates a significant gap between business objectives and IT objectives.

While alternative delivery models may allow IT to plug holes and address short-term tactical requirements, a long-term, strategic solution for managing applications and IT services, and how they are delivered to end-users, suffers in the long run.

¹Source: ESG Research Report, *Mobile Device and Application Usage Trends*, August 2013.

The Transition from a Locked-down Environment to a User-centric Environment

With the transition from a “locked-down” corporate end-user environment (information is delivered from the data center to the endpoint), to a user-centric common access and identity model (applications are user-driven and installed on demand), IT professionals are confronted with multiple challenges. They include:

- Meeting end-user expectations.
- Improving business processes.
- Meeting mobility initiative requirements.

To reduce IT complexity while catering to the tractability of a flexible, self-service approach demanded by end-users, the industry requires a unified approach that aggregates delivery models, centralizes management and security, and supports a wide variety of endpoint devices. ESG defines this unified approach as Workplace Delivery Platform.

Though current delivery models fall short of this business demand, a growing number of vendors have stated their intentions to innovate workplace delivery platforms that focus on the management and support of various delivery models and devices.

This report addresses:

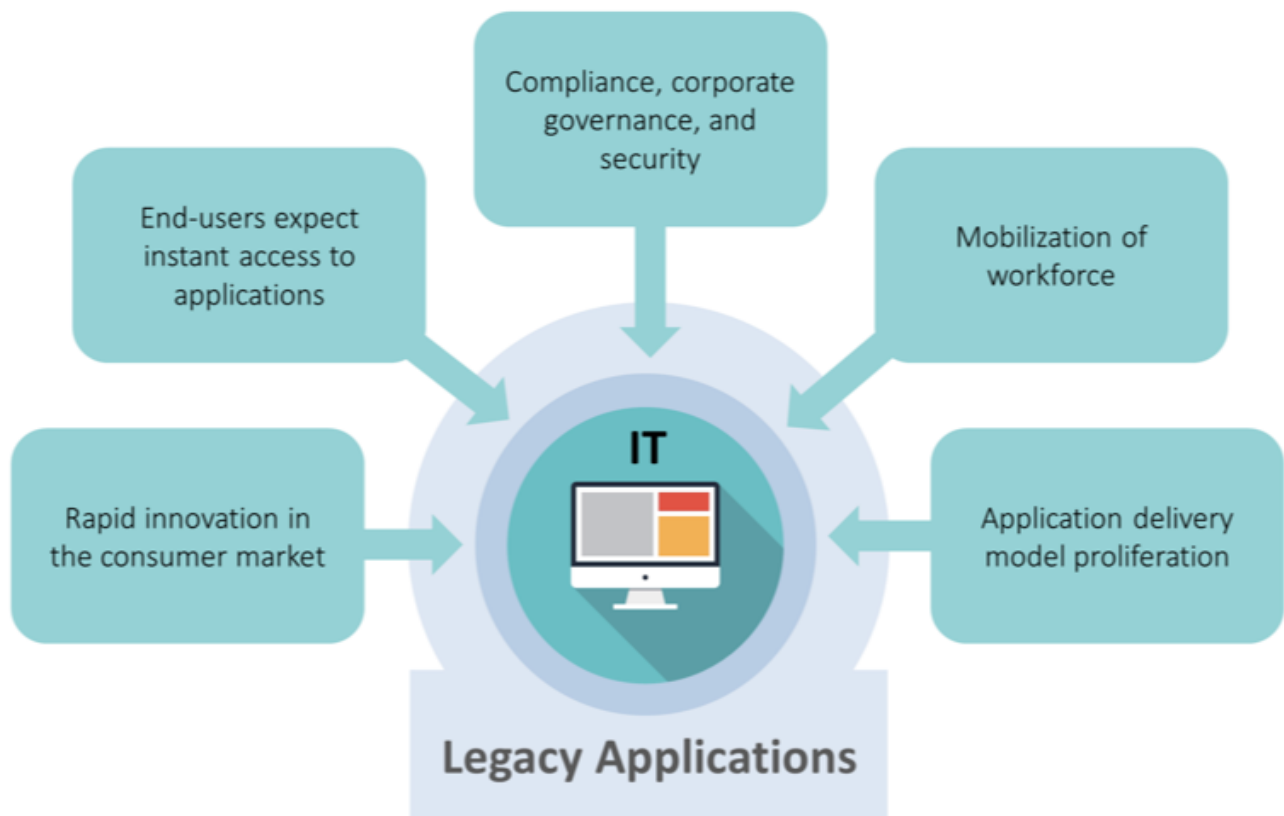
- The market status of workplace delivery today, and related issues challenging IT.
- The workplace delivery platform, what it is, and how it addresses the IT security conundrum of securing corporate access while improving the end-user experience.
- The current, planned, and future market vision and transition strategies.

The State of Workplace Delivery

Organizations today are delivering applications and data across a myriad of devices via a number of delivery models. The traditional method of deploying corporate desktops, projecting applications to an end-user environment, locking down mobile devices, and securing the environment is becoming increasingly complex and extremely hard to manage. This creates additional challenges for IT organizations already struggling to maintain application performance while meeting the growing demand for an improved end-user experience.

With the fast pace of consumer technology innovation, in a market continuously flooded with new devices, managing, maintaining, and securing applications and desktops have IT scrambling. The rapid influx of end-user computing devices, the onslaught of application and desktop delivery models, and the ability to meet compliance and government regulations are challenging corporate IT on multiple fronts (see Figure 1).

Figure 1. Corporate IT is Being Barraged with Multiple Challenges



Source: Enterprise Strategy Group, 2015.

Top Challenges Confronting Corporate IT

With more directives and initiatives being piled on daily, corporate IT's greatest challenges are:

- Securing and managing numerous applications, devices, and endpoints.
- Creating, managing, and enforcing corporate policies for applications, devices, and endpoint data.
- Maintaining performance and improving end-user experience and productivity.

In addition to supporting a huge and ever-increasing number of endpoints per user in the workplace, IT must secure these devices—many of which are used for both business and personal use—in order to safeguard critical data. This means not only managing increased endpoint security requirements, new data protection strategies, and new application access control policies, but improving end-user experience and productivity as well.

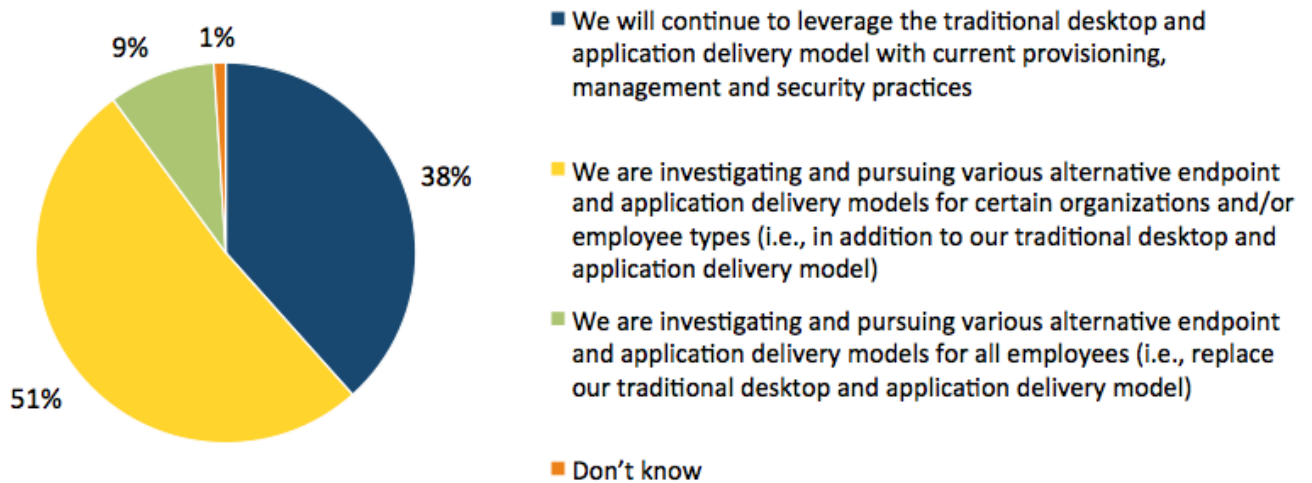
Further adding to the proliferating IT to-do list, is the transformation to a user-centric computing model. The user-centric computing model requires organizations to evolve their endpoint computing strategies. This entails rethinking about how to develop and architect applications so they can be easily accessed by a user on any device.

As individual use cases vary, companies will require a multifaceted approach that identifies various end-user profiles and pairs them with the appropriate long-term strategies—including alternative application and desktop delivery models—for achieving ubiquitous accessibility and enhanced end-user experience.

In addition to the challenges associated with supporting endpoint device environments, a number of trends such as “bring-your-own-device” (BYOD) and alternative application delivery models are forcing IT organizations to reevaluate the manner in which digital workspaces are provided to employees. It follows then that 60% of organizations are investigating and pursuing various alternative endpoint and application delivery models for either certain employees or everyone (see Figure 2).¹

Source: Ibid.

Figure 2. Changes in the Desktop and Application Delivery Landscape



Source: Enterprise Strategy Group, 2015.

The Hybrid Delivery Environment

The hybrid delivery environment is a combination of traditional, private, and public cloud environments. With today's diverse business landscape, devices and applications are doing double duty—working within the corporate network as well as outside it. It's not just a one-to-one relationship anymore. Data is not just being tied to a corporate laptop or desktop; data is being used, shared, and stored locally. End-users are keeping files outside the corporate network on file sharing solutions—without any common IT policy tying together their personal computers, tablets, and smartphones.

Presently, the transition to IT service-based delivery models for application and desktop delivery has been largely tactical. So while businesses are still focusing on high-level goals like improving flexibility and agility while managing costs, many organizations have begun deploying assorted delivery models to achieve smaller tactical objectives.

For example, virtual desktop infrastructure (VDI) has experienced some success when deployed to end-users who have predictable roles and responsibilities, but this technology has not been able to break through boundaries to demonstrate the value to a mobile worker. The same holds true for software-as-a-service (SaaS) applications that are independently used, but lack centralized control. But employing a strategy to satisfy immediate needs with temporary solutions is ultimately myopic. Why? Because these solutions fail to aggregate across endpoints and delivery models, complicating IT management and impeding end-user access. In essence, these solutions are unable to address the long-term goal of IT—securing, managing, and improving business processes.

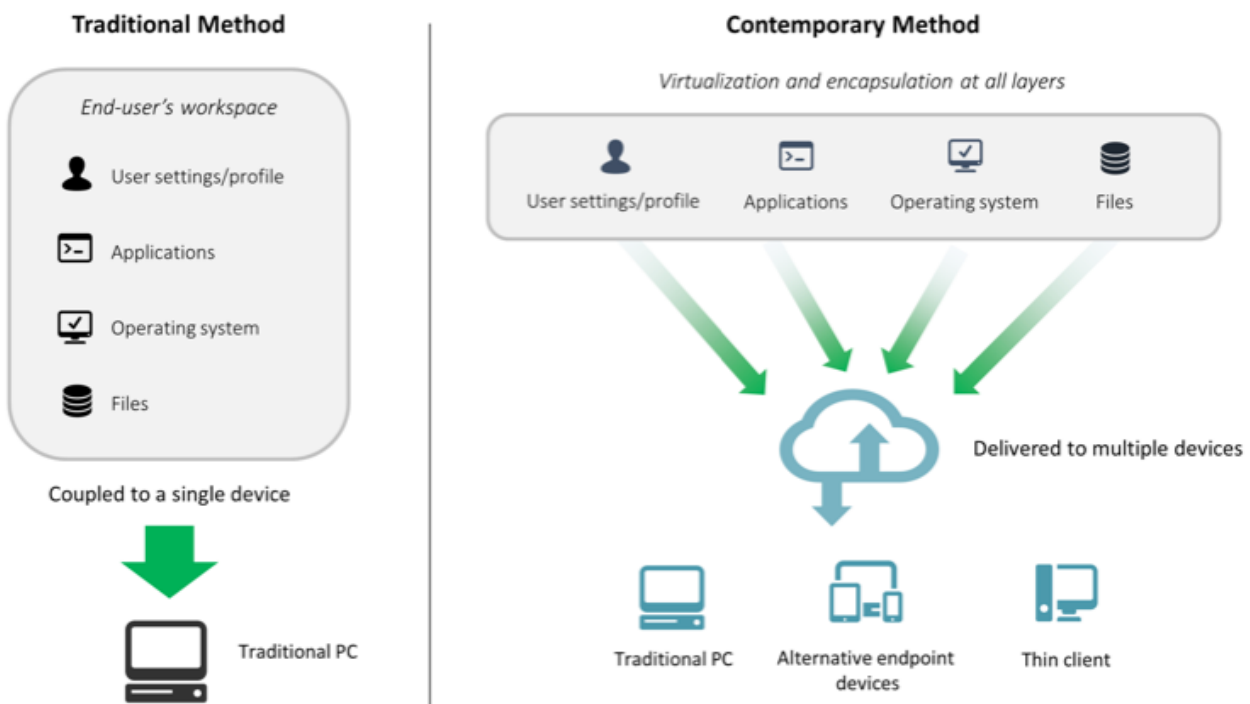
To be able to secure, manage, and improve business processes, it’s essential for organizations to put into place a federated workplace delivery platform—one that centralizes IT management, provisioning, and security on an intelligent infrastructure, and provides end-users with a common, easily accessible interface. Simply put, IT must find a way to aggregate different applications, desktop, and data delivery and consumption models in a hybrid delivery environment, and maintain control over them while providing easy access for end-users.

The “Dissection” of the End-user Work Environment

Traditionally, organizations have delivered end-user desktops as a single, bundled unit. User settings, applications, operating systems, and data were coupled to a traditional desktop or laptop, and delivered as a packaged unit (see Figure 3, Traditional Method). This method doesn’t take into account the resources an end-user requires at any given time, so everything associated with that particular end-user is delivered in total, expending unnecessary time and resources.

With the Contemporary Method, virtualization has thrown a wrench into the works of convention by enabling the parsing and encapsulation of all layers. Now organizations are able to deliver each layer independently of the other (see Figure 3). Orchestration and management software works dynamically to assemble the various components needed at run-time. By delivering each level independently of one another, IT is better able to streamline desktop and application delivery, and can cater to specific networks and device types.

Figure 3. Traditional and Contemporary Methods of Workplace Delivery



Source: Enterprise Strategy Group, 2015.

And while traditional desktops and virtualization at multiple layers are both valid means of delivering end-user work environments, IT can further improve on workplace delivery models.

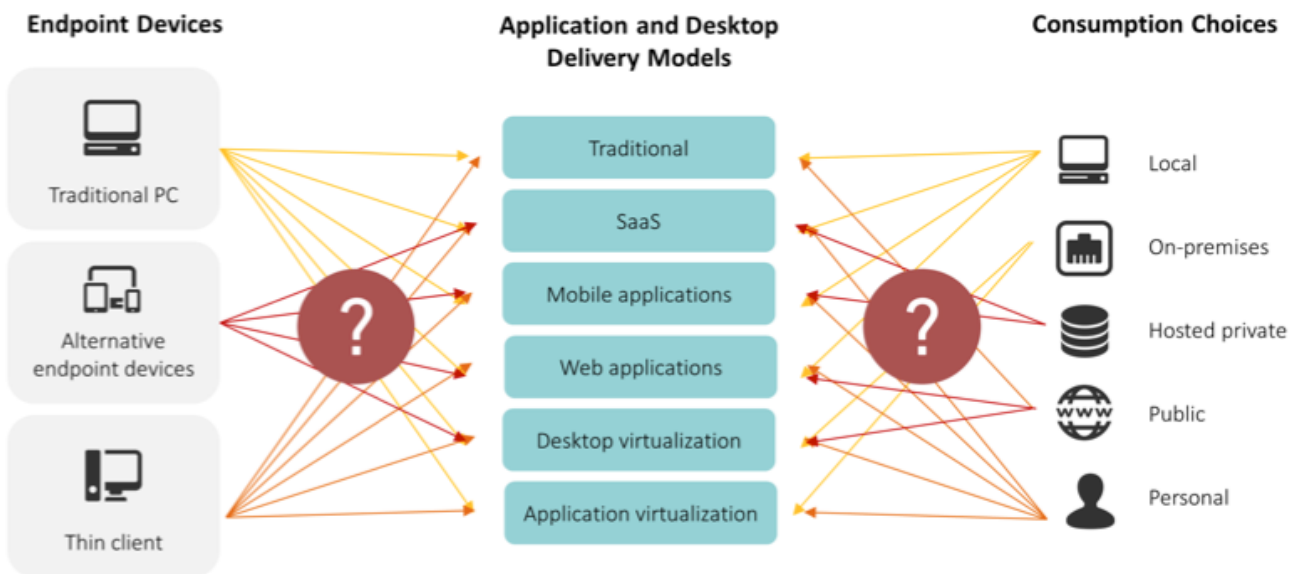
Workplace Delivery Platform

Complexity Breeds Opportunity for a New Approach

The growth of consumerization and innovation around service-based delivery models have given rise to hybrid delivery environments spanning a number of platforms and devices. Many organizations continue to deploy and expand point solutions focused on addressing short-term, isolated needs without looking at the long-term picture.

Compounding the current complexity of workplace delivery is the fact that these disparate solutions, often acquired through several vendors, are deployed via a local device, on-premises data center, or hosted in a private, public, or personal cloud (see Figure 4). These solutions lack unity and centralized management. As long as companies address individual use cases, point solutions will continue to have traction, forcing organizations to support, manage, provision, and secure exceedingly complex application and desktop environments rather than seeking out long-term business and IT strategies.

Figure 4. Current Complexity of Workplace Delivery



Source: Enterprise Strategy Group, 2015.

While the IT vendor market remains hyper-focused on addressing one point at the expense of others, businesses still must consider a vast array of endpoint possibilities, application and desktop delivery models, as well as how to secure, maintain, and deliver a highly efficient and productive environment. In addition, businesses must also consider online file management solutions, collaboration tools, and unified communication strategies.

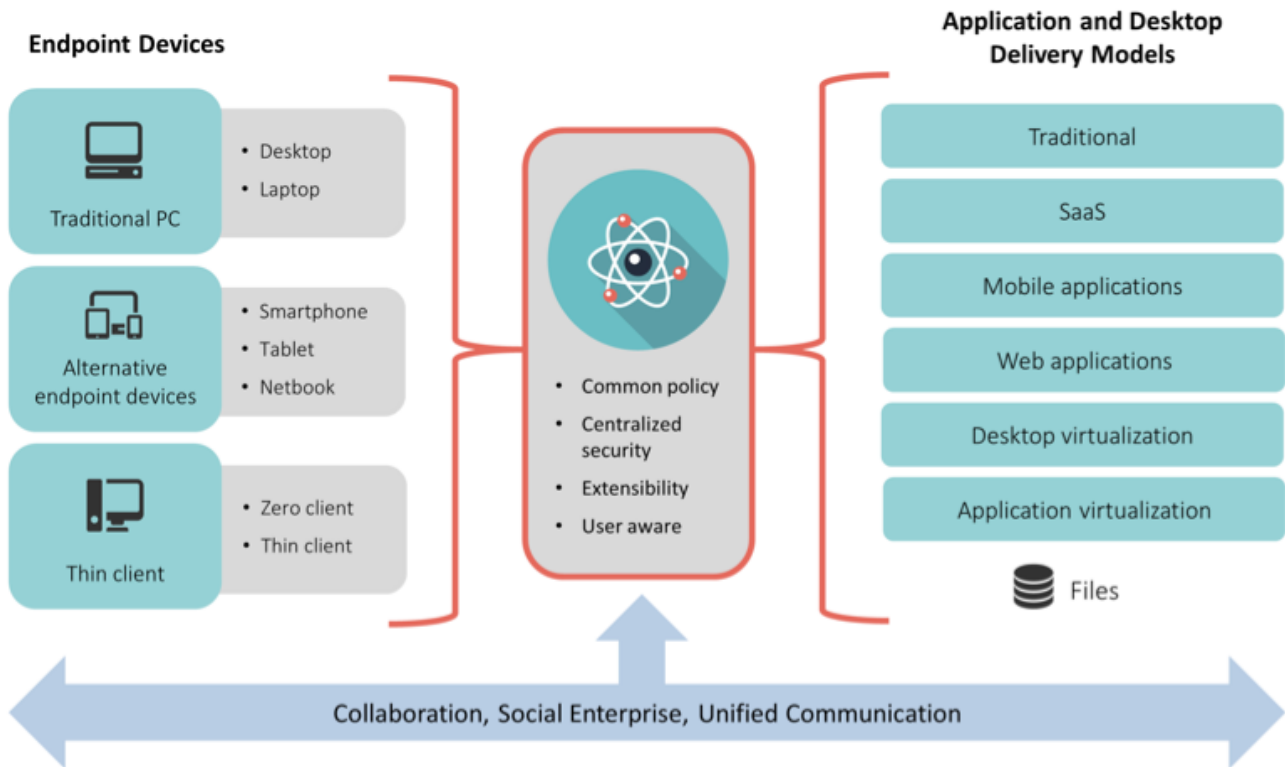
Focusing on a single endpoint strategy or delivery model to address an individual use case will only delay long-term success. Typically, these point solutions are independent of one another and thus fail to aggregate, making them increasingly difficult to orchestrate, resource, and manage. Since productive end-users have and will continue to consume multiple devices, IT must capture control, simplify management, and maintain security from within the data center.

Determining Appropriate Consumption Models

The proliferation of endpoint devices and delivery models are not the only factors affecting IT decision making regarding application and desktop delivery. Businesses must also consider a variety of consumption models. Along with continuing to manage locally installed applications and data, IT will need to address a number of other alternative consumption models currently being built into many IT strategies—ranging from colocation facilities to applications executed and managed in the public cloud. Successful high-performing companies will learn to select the delivery models that best align with their business processes based on considerations such as economics, risk mitigation, and end-user satisfaction.

The complexity created by the adoption of multiple endpoint devices combined with the rapid evolution of delivery and consumption models breeds a great opportunity for businesses to exponentially improve the way end-users “consume” a workspace. Businesses require a long-term unified computing strategy that centralizes IT management and control, and caters to the flexibility and freedom of choice that end-users desire. Though current delivery models fall short of that business demand, vendors have explicitly stated their intentions to innovate workplace delivery platforms that focus on the management and support of various delivery models and devices (see Figure 5).

Figure 5. Innovative Workplace Delivery Platforms Centralize IT Management and Support Various Delivery Models and Devices



Source: Enterprise Strategy Group, 2015.

A workplace delivery platform is a unified set of strategies that enable businesses to aggregate delivery models, centralize management and security, and flexibly support various endpoint devices. From the IT perspective, workplace delivery platforms vastly alleviate the complexity associated with managing desktop and application environments on a case-by-case, and device-by-device basis.

The advantages for end-users are significant:

- Improved accessibility
- Flexibility
- Overall simplicity
- For example, rather than requiring multiple sign-ons for each application or device, workplace delivery platforms are being developed to include a common policy for authentication and access control. As a result, end-users can sign-on just once, accessing all of their applications without having to contend with cumbersome processes associated with launching isolated applications in a hybrid delivery environment.

While taking into account the proliferation of endpoints, vendors are readily expanding the breadth of devices that they support within their workplace delivery strategies. Rather than just focusing on traditional PCs,

burgeoning user demand has forced organizations to support alternative endpoint devices, tablets, smartphones, and thin clients, which is being reflected in vendor innovation. The result is that employees and customers will be able to access their applications and desktops ubiquitously on any device of their choosing.

By federating application and desktop environments within a single interface and simplifying both end-user access and IT management, a workplace delivery platform creates a user-centric computing model that improves business processes and user productivity.

Workplace Delivery Strategy

An effective workplace delivery strategy begins with:

- **Users:** Segment users based on their roles and responsibilities through a common access and identity platform. Consider both your current user base as well as any planned or potential new roles.
- **Devices:** Devices should not dictate a strategy, but IT should maintain an inventory of current, planned, and future device options. Revisit your device support policy and determine how, if, and when you will modify and enhance device support. The workplace delivery platform should be able to adopt to any device.
- **Application and desktop delivery models:** Create a list of current, planned, and future application and delivery models. Map the delivery models to a timeline that is targeted to the user segmentation.
- **IT consumption models:** Determine the prevailing IT consumption models in your organization, how they are used, and their benefits and challenges. Collaborate as a team to determine the adoption cadence of alternative consumption models that align with the strategic direction of the company.

Upon discovery of these items, you will start to assimilate the relationship between device adoption and delivery models, as well as factor in how and where your business will consume. As the strategy quickly evolves, the next area of consideration is policy and management. Consider these key factors:

- Common policy creation and enforcement
- Centralized security
- Extensibility
- User centricity
- Shared identity and authentication
- Seamless integration of devices and applications
- Orchestration and dynamic workflow
- License tracking

- Analytics and reporting
- Help desk/self help

Context Awareness

There are certain scenarios you will want to walk through as you build your strategy. Begin by thinking about context awareness. How will you consistently, predictably, and reliably deliver an application across multiple devices and networks? If the application requires the use of a mouse and keyboard when accessing the application on a laptop or desktop, *and end-users expect it*, how will that experience change when they access the same application on a smartphone? Sometimes the answer is simple, but much of the time it involves a careful walkthrough of how, when, and where a user will access an application. You may choose to restrict or, depending on the use case, limit access and application functionality based on device type and location. The most important factor to keep in mind is how you are going to track and manage these policies, in addition to the other delivery models you already have in place.

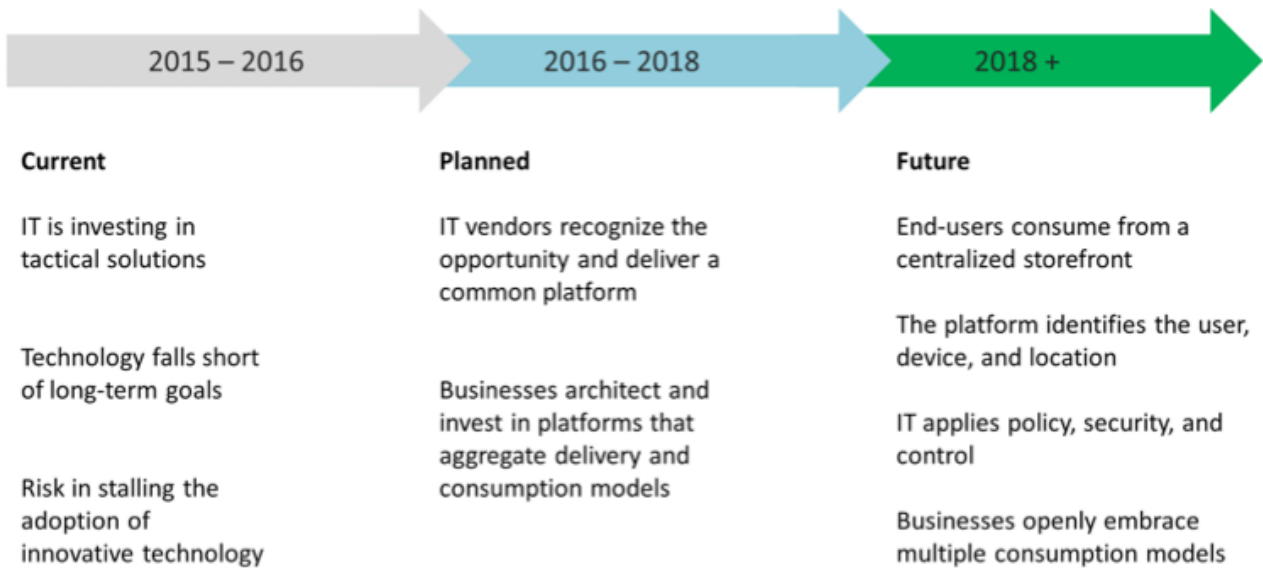
Market Vision

Current, Planned, and Future States

The mastery behind any long-term vision and execution strategy is timing. More specifically, timing that successfully aligns business goals and vendor product lifecycles. To help reduce some of the guesswork as you build your strategy, think of the market in three states: current, planned, and future (see Figure 6).

While some IT vendors intend to develop a product that externalizes the control plane and brokers content within a single interface, others will focus current and future product innovation on the user, multiple devices, and a variety of consumption models. Understanding both approaches is critical to success. Moreover, organizations need to take a long-range, strategic view in order to determine the best way to implement new strategies into their current technology and business environments.

Figure 6. Timeline for a Comprehensive Workplace Delivery Strategy



Source: Enterprise Strategy Group, 2015.

The Current State: To date, most organizations have taken a very tactical approach, which can limit the potential benefits of technology. As previously mentioned, VDI is a good example of this. Software-as-a-service (SaaS) is also another good example. Both are good solutions for a focused use case, but rarely, if ever, is a company able

to implement common access and identity management across both solutions. Moving forward, there is an opportunity to:

- Shift away from a device-centric model in favor of a user-centric one.
- Develop and implement a comprehensive device support policy, taking BYOD into consideration.
- Prepare new and legacy applications for centralized management and remote delivery.

In the current state, IT is in the position to progress to the planned state of a workplace delivery strategy. Laying the foundation early in the strategy will greatly simplify and accelerate an organization's success.

The Planned State: The planned state is still in its early stages, with vendors starting to help their customers transition to a viable workplace delivery platform. As we move through the planned state, IT organizations that have not incorporated a long-term strategy and direction will find themselves playing catch up with the market. The planned state is about expansion that will:

- Focus on platform investment and long-term strategy.
- Prepare for further centralization and adoption of multiple consumption models.
- Accelerate the onboarding of end-users.

The Future State: Today many consumers use smartphones, downloading and using applications with minimal training or support. This is a perfect example of ease of use. Ultimately the goal of most, if not all, organizations, is to be able to translate the simple, consumer ease of use of a smartphone to the corporate environment.

While this sounds great in theory, most organizations are light years away from living this scenario. Many organizations still must go through a lengthy approval process just to install an application on a desktop. The future state will:

- Aggregate applications, desktops, self-service, and promote a social enterprise in a common application storefront, for ease of use for end-users.
- Deliver applications from the most cost-effective, secure, and productive consumption models.
- Improve management, security, and IT policy enforcement while delivering the most productive work environment, enabling IT to identify users, devices, and locations of endpoint devices to apply appropriate policy, security, and requisite control measures.
- Allow businesses to openly embrace multiple consumption models based on economics and freedom of choice.

The Bigger Truth

One of the most interesting initiatives inside businesses today is observing how companies are building mobility centers of excellence and looking to improve the way end-users interact with their environments—and how IT looks at ways to manage, secure, and deliver new means of access and productivity inside the business. The initial results we are observing are sparking further innovation in the IT vendor marketplace and are changing the way companies operate. Some companies have simply improved access to applications and data, others have streamlined business processes, and some have completely transformed the way they secure, manage, and access the end-user work environment.

Many businesses continue to embrace a single product, but vendors are beginning to map their products into workplace delivery platforms that have helped raise the level of awareness around the value that a more holistic approach can yield. Companies looking to solve a single application or endpoint security concern have the opportunity to engage with vendors that have expanded their platforms and incorporated their technologies into a suite of products, which will likely help deliver value beyond a current single-threaded initiative.

Leading vendors in the workplace mobility space include Amazon, Citrix, Google, Microsoft, and VMware. While each of these vendors offer varying degrees of capabilities, and some lean further toward cloud-delivered options, each are participating at a level that deserves attention. We should expect to see change, further investment, and innovation from each of them. Organizations considering ways to improve the user experience and take back a measure of IT control should look to these vendors as a means of addressing their application, desktop, and mobility initiatives.