“Mobile, and particularly the BYOD aspects of end user device selection, has exasperated an already over burdened IT department. While many organizations eventually discovered a way to accommodate mobile workers’ needs, it was a painful and often inefficient process. With the emergence of a new wave of devices in the Internet of Things that will soon come to market, and an expanded workforce that requires access to all aspects of corporate back end support systems, an updated method of delivering company-wide deployments of needed apps is required.”
Contents

Introduction ........................................................................................................................................... 2
It’s a Diverse, 24x7 World ....................................................................................................................... 2
The Need for Rapid Change .................................................................................................................... 3
Allowing Universal Access .................................................................................................................... 3
A Different App Delivery Model .......................................................................................................... 4
Workspace as a Service .......................................................................................................................... 4
Advantages of WaaS vs. Traditional App Deployments ....................................................................... 6

Figure 1: Comparison of Workspace as a Service vs. Traditional App Deployment ....................... 6
Can WaaS Provide a Good Return on Investment? ............................................................................. 6

PC Migration Costs ............................................................................................................................... 7

Figure 2: PC Migration Cost, Traditional PC Apps vs WaaS ............................................................... 7
Security/Data Breaches .......................................................................................................................... 7

Figure 3: The average per employee cost of a data breach per incident. ............................................. 7
App availability and time to deployment ............................................................................................... 8

Figure 4: Cost of Delay per week and per month per app ................................................................. 8
File sync and share ............................................................................................................................... 8
Disaster recovery ................................................................................................................................. 9
Getting Started ................................................................................................................................... 9
Recommendations ............................................................................................................................... 10
Conclusions ......................................................................................................................................... 10
Introduction
Most enterprises continue to struggle with enabling their entire workforce to efficiently and safely access corporate back office systems on a variety of devices and from any location. Indeed, the advent of mobile, and particularly the BYOD aspects of end user device selection, exasperated an already over burdened IT department. And while many organizations eventually discovered a way to accommodate mobile workers, it was a painful and often inefficient process.

With the emergence of a new wave of devices in the Internet of Things that will soon come to market, and an expanded workforce that requires access to all aspects of corporate back end support systems, an updated method of delivering company-wide deployments of needed apps is required. The move to cloud-centric services is emerging as an important vehicle for next generation corporate systems, enabling organizations to move beyond legacy end user architectures.

Workspace as a Service offers a method of enabling workers to obtain access to whatever app they need, on whatever device, and with minimal IT overhead. This requires a new way of looking at corporate end user computing needs, and does require modifying today’s predominately classical client/server infrastructure. But it offers the potential to provide a far more rapid and flexible way of deploying needed line of business solutions in a timely fashion within a secured data sharing structure. As such it enables an enhanced ability to avoid corporate data breaches, improves end user management beyond current MDM solutions, lowers capital expenses in end user and infrastructure equipment, and maximizes overall Return on Investment (ROI).

To this end, below we look at some of the drivers of this new strategy, discuss the decision points necessary to evaluate this new way to worker enablement, and analyze the pros and cons of the Workspace as a Service model.

It’s a Diverse, 24x7 World
Since most users regularly access corporate systems from 3-5 different devices over their working hours (and potentially off-hours), it is imperative for companies to offer “Universal Access” from any device. And since users often have to access 7-10 mainstream corporate apps on a regular basis (and potentially many more occasionally), obtaining and installing apps on each end user device is a major (and expensive) task. Whether a PC, smartphone device, tablet or other alternative, users simply want to get things done and not be constrained to doing things only on a limited device choice, nor hindered by not having their
required app available. Being able to get productive work done, using the same apps end users are accustomed to, and doing it securely from any device must be a goal of any next generation workspace. But it should also be a way to simplify the complexity associated with supporting the ever changing device preferences of users.

The Need for Rapid Change
Companies can no longer assume that end user devices will remain in use for an extended period of time. In the past, the typical PC was in use for 3 or more years. But new age devices like modern smartphones that are used to access corporate systems often remain in service for as little as 12 months. Further, unlike the relatively standard environment of PCs across manufacturers’ models, current mobile and future Internet of Things devices can have a myriad of operating systems, functions and capabilities. Finally, with the need for companies to react quickly to changes in business conditions, the typical process of taking 6-12 months to develop an app and the expectation it will remain deployed for 3-5 years or more no longer apply.

With so much change in business dynamics coming at an alarming pace, it’s likely that many Line of Business apps will have a useful life of 6-12 months before having to be substantially modified or replaced. And taking a core app and modifying it for 2, 3 or more different end user devices is cost and resource prohibitive. Further, installing multiple versions of the apps on the various device types is a burdensome process, even if it’s partially automated. Finally, in a BYOD world where users choose and own their devices, it’s becoming increasingly difficult to control the end user environment sufficiently to both limit security exposure and minimize IT resources and costs. Resolving these issues requires that organizations change how they deploy solutions to end users.

Allowing Universal Access
Supporting workers on all of their favorite devices used in their work lives (e.g. work PC, home PC, smartphone, Chromebook, tablet, etc.) is problematic. In the past, experimentation with browser-based app delivery systems were promoted as a way around this dilemma, but many limitations exist and proved not to be a universal solution. Indeed, most organizations still required a hybrid approach of browser-based and device-specific apps. However few organizations have the wherewithal to deploy and manage the unique components needed to allow workers to access corporate systems from any device of their choosing, or potentially from multiple devices during a busy day. This is a major impediment to user productivity as well as user satisfaction, and often results in additional burdens on IT. It also often results in users finding ways around corporate systems, which may not be sanctioned, and may not always be safe and secure. It’s imperative that organizations find a way to support users on a variety of devices, in order to achieve the maximum level of workforce productivity.
A Different App Delivery Model

What’s required is a universal way to deliver needed line of business apps to users where and when they need them, without having to expend time and scarce resources to modify them for each end user delivery environment. Any device type (PC, iPhones, Android devices, iPads, and the array of new devices coming on line like car displays, connected appliances, wearables, etc.) should be enabled to act as a workforce access device. This requires that services be introduced that can quickly access the capabilities of the device, deliver a customized package of capabilities to the device based on the identity of the end user and his/her specific role-based needs, secure all interactions on that device, and manage the various aspects of the device effectively, all while having minimal impact on scarce IT resources. Further, user required data must be accessible and secure for use with any device no matter what the source of the data or where it may reside. And while we have come part way towards this goal through many of the Enterprise Mobile Management (EMM) tools and Virtual Desktop Interface (VDI) capabilities available in the market, neither has delivered fully on this vision. Something more is required.

Workspace as a Service

Organizations need to update their operations to respond to and take advantage of the changes in end user workspace requirements. In moving towards a more modern and adaptive approach, Workspace as a Service (WaaS) can provide attractive solutions for a number of challenging enterprise requirements. Among these are:

Identity Access Management - Identity management is both a convenience and a security measure. It is also a way to define and enforce corporate policies. IAM can provide a cross-app and cross-platform approach to true end user identity verification. This is very different when done within individual apps, where there is generally no commonality and few standards yet deployed. Uniform IAM is a major cost saver for IT and also provides an enhancement to the user experience.

Rapid Time to App Deployment – WaaS enables rapid time to app deployment across all device types and with no need for reprogramming legacy apps that often can’t/don’t get changed. For many organizations time to deployment and productivity is mission critical, and any delays can be very costly.

Embedded MDM/MAM/EMM - App and device management must be built in to corporate solutions to achieve the maximum security, manageability and user experience return on investments. But add-on MDM/EMM is often difficult and costly to implement and deploy, with many enterprises purchasing suites but only deploying base-level components. Having a built in vs. an add-on capability is a major advantage for both IT and end users, and a core component of WaaS.

Keeping Data Safe - Many organizations focus on deploying apps and securing local data stores on various devices in the ever evolving mobile world. But few spend as much time
focused on creating a secure file/data sharing environment where the data is protected no matter the user access point or source of the data. Embedded secure data management functionality must be included in any WaaS implementation if an enterprise truly wants to be secure in a mobile world and protect its valuable data assets.

Network access availability and optimization - This is an often overlooked requirement for any workforce that relies heavily on wireless communications. Many connections are not sufficient for high network use environments since they need to maintain maximum user acceptance with minimal delays and latency. This requirement could mean the difference between a solution acceptable to an end user and one that is discarded quickly or bypassed due to negative usability characteristics. Indeed, we estimate that 35%-50% of mobile apps suffer from this problem. There is also a cost advantage in optimizing data flow over wireless connections, as few organizations have truly unlimited data plans. This capability should be part of any WaaS platform decision.

Flexible Cloud - Being able to easily move from an on-prem to a cloud based solution, or easily integrating a hybrid approach, is key to offering a true enterprise class experience to mobile workers. Most custom apps require a pre-determined selection of back end technology, thus limiting options for a company. A platform offering flexibility is the best way for companies to deploy solutions in a world that is evolving quickly and where users often change access models and end user devices.

Desktop as a Service - connecting legacy apps to devices utilizing the latest in modern app technology is not a trivial issue for most organizations. Indeed, we estimate 80%-85% of corporate apps will never be updated, yet they will remain in use for many years to come. How these required apps get deployed to the myriad of new users with modern devices (including iOS and Android) is mission critical. And such capability must be included in any complete WaaS solution.

Lifecycle management – this remains an area where few organizations spend much in the way of resources. Yet proper lifecycle management has the potential to significantly lower overall cost of operations and increase user productivity through limiting the amount of effort IT needs to expend in device, app, and infrastructure upgrades. Indeed, we estimate good lifecycle management practices can lower overall total cost of ownership by 15%-25%. This area needs to be part of any consideration in deploying mobile solutions and/or new app access points for end users.

Expanding Workspace User Access - this not only affects companies starting over and deploying new infrastructure to internal users. It is also a way to increase coverage for a variety of company “customers” that need to either quickly, or perhaps only occasionally access corporate computing resources in a convenient and secure manner. This has wide implications not only for internal users, but also for partners (e.g., real estate agents, independent insurance agents, trusted partners), and may be a key advantage in deploying a WaaS solution...
Advantages of WaaS vs. Traditional App Deployments
There is no one “magic bullet” that solves all challenges in deploying workspaces to end users. But we can compare WaaS components and more traditional components to see which might offer advantages in specific circumstances. Figure 1 provides a comparison of specific challenges faced by most organizations and rates the WaaS solutions against a more traditional “app deployed on a device” solution.

Figure 1: Comparison of Workspace as a Service vs. Traditional App Deployment

<table>
<thead>
<tr>
<th></th>
<th>Workspace as a Service</th>
<th>Traditional App Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>++</td>
<td>+</td>
</tr>
<tr>
<td>Speed to deploy</td>
<td>++</td>
<td>-</td>
</tr>
<tr>
<td>Unified identity management</td>
<td>++</td>
<td>-</td>
</tr>
<tr>
<td>ROI</td>
<td>++</td>
<td>+</td>
</tr>
<tr>
<td>Device Flexibility</td>
<td>++</td>
<td>-</td>
</tr>
<tr>
<td>Agility/rapid change capability</td>
<td>++</td>
<td>-</td>
</tr>
<tr>
<td>Reuse of existing app assets</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>LOB app dev flexibility</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>BYOD support</td>
<td>++</td>
<td>+</td>
</tr>
<tr>
<td>Lifecycle/change management</td>
<td>++</td>
<td>+</td>
</tr>
<tr>
<td>Enterprise back office</td>
<td>+</td>
<td>++</td>
</tr>
<tr>
<td>integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bandwidth requirements</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>Reliable wireless connection</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>need</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure required</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>Data protection</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Preserving app investment</td>
<td>++</td>
<td>-</td>
</tr>
<tr>
<td>Device Independent workspace</td>
<td>++</td>
<td>+</td>
</tr>
</tbody>
</table>

Can WaaS Provide a Good Return on Investment?
There are many potential investments that organizations can make to increase convenience for their end users. But at the end of the day, investments in new solutions must include a payback for the organization. In this section we analyze several key components that can provide enterprises with a significant ROI when deploying a WaaS solution.
**PC Migration Costs**

Our research indicates that the cost of updating/migrating a user to a new enterprise-class PC is $2040. This includes the cost of a new machine, plus the costs involved with migrating corporate apps, setting up the new machine, end user costs, etc. And this expense is required approximately every three years when new machines are deployed, although some organizations stretch this out to 4-5 years, often due to the high costs involved.

However, migration costs utilizing a WaaS approach rather than the more traditional full PC app installation shows the cost to be $1572. These costs are for individual machines and do not include the costs of any new app licenses or infrastructure upgrades. Nevertheless, we estimate a cost savings of $468 per PC when deploying WaaS to power a new machine rather than a more traditional individual app on each machine approach. In a 1000 user organization, that amounts to $468K savings. If we assume that machines are upgraded every 3 years, that amounts to a $156K savings per year, or $156 per device per year.

**Figure 2: PC Migration Cost, Traditional PC Apps vs. WaaS**

<table>
<thead>
<tr>
<th></th>
<th>Traditional PC App Load</th>
<th>WaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC Migration Cost</td>
<td>$2040</td>
<td>$1572</td>
</tr>
<tr>
<td>Savings per Device per Year</td>
<td></td>
<td>$156</td>
</tr>
</tbody>
</table>

**Security/Data Breaches**

While no method is 100% foolproof, WaaS can significantly reduce the amount and severity of enterprise data lost through hacks, malware and end user mistakes that can cost a company millions of dollars per incident. Indeed, the number and severity of data breaches, as well as malware attacks and in particular new threats like “Ransomware” can be dramatically reduced or even eliminated by deploying a properly designed WaaS.

It’s difficult to come up with an average number that can be applied to all companies. The Verizon 2015 Data Breach Investigations Report estimates a company with 1K users experiencing a data breach of 100K records will cost the organization $475K (although in some cases it will be many times more). That’s $475 per employee. According to the Ponemon Institute 2015 Cost of Data Breach Study, the average consolidated total cost of a data breach is $3.8 million or $154 for each lost or stolen record containing confidential information. Figure 3 indicates low to high estimates and an average cost per user.

**Figure 3: The average per employee cost of a data breach per incident.**
## Workspaces of the Future
Enabling work for any user from any device

<table>
<thead>
<tr>
<th>Cost of Data Breach</th>
<th>Low Estimate</th>
<th>High Estimate</th>
<th>Average Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost per user</td>
<td>$475</td>
<td>$15,400</td>
<td>$7,938</td>
</tr>
</tbody>
</table>

**App availability and time to deployment**

Apps optimized for new devices can take 6-12 months or longer to develop and cost $250K-$500K or more. Many enterprise apps used to run businesses would likely never achieve payback using that approach. With more users wanting more apps “mobilized” and available for use on any device, and with extremely limited resources available to transition these apps, it is imperative that enterprises find a way around this dilemma.

The ultimate goal for most organizations should be in preserving and extending their current investments in existing mission critical back office system. Most companies run their businesses on Windows apps and have many legacy desktop apps that can be quickly repurposed for mobile users if done correctly. The trick is to make that process simple and painless.

Our research indicates that delaying an app to users who require it, and consequently impeding their productivity, has real costs. Figure 4 is our analysis of what delaying an app to end users mean, on a per user, per month, and per app basis. In most cases we believe that WaaS can virtually eliminate this impediment and recover the lost opportunity costs associated with delays. While there is a cost to deploying WaaS per device as well, it is spread across all apps and therefore is a negligible cost on a per user per app basis.

### Figure 4: Cost of Delay per week and per month per app

<table>
<thead>
<tr>
<th></th>
<th>Each Week Delay</th>
<th>Each Month Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Each Lower Level Worker</td>
<td>$35</td>
<td>$150</td>
</tr>
<tr>
<td>Each Exec Level Worker</td>
<td>$69</td>
<td>$300</td>
</tr>
<tr>
<td>100 Lower Level Workers</td>
<td>$3,500</td>
<td>$15,000</td>
</tr>
<tr>
<td>100 Exec Level Workers</td>
<td>$6,900</td>
<td>$30,000</td>
</tr>
</tbody>
</table>

**File sync and share**

Properly deployed, file sync and share offers many benefits to both the organization and the end users. For the organization, it provides a way to capture all corporate data so that isolated islands of critical information aren’t scattered on end user devices. Further, the ability to monitor and analyze the use of corporate data means that companies could quickly evaluate data usage for legitimate or nefarious purposes and use this as a tool for
heightened security and loss prevention. The ability to set policies and procedures for use of the data means that the data is far more secure and less likely to be intercepted and/or compromised. Finally, there is one view into data no matter where it is located: on-prem, in public or private cloud, on devices, in different repositories, etc.

For the end user, a properly configured file sync and share capability means that no matter what device, app or location, users will have access to the data they need to complete the task at hand. In an increasingly BYOD environment where users engage corporate systems through multiple devices, this is an attractive option. And when coupled to IAM, this adds a high level of convenience.

**Disaster recovery**

Traditional disaster recovery requires that each data set for each device be continuously backed up and made available to reload to the same or a replacement device as required. Even in an automated system, this approach can cause significant challenges, especially if large data files are included. The time to upload, particularly over relatively slow networks, can be extensive. And the cost if done over a wireless connection on a continuous basis can be substantial.

The primary need for disaster recovery is that all files be available, virtually at a moment’s notice. In a fully functioning WaaS scenario, all data is synced to and shared from a central control point, even if the actual files are dispersed over several locations.

But lost or damaged devices are also a challenge to replace when users must get their apps supported locally on each device. File sync and share capability coupled with app access via WaaS allows an almost instantaneous ability to configure a new workspace on virtually any device. In a situation where the user must be recovered from a lost, stolen or compromised device, this can usually be done in minutes from a central console with IT intervention, and with limited required end user intervention. WaaS is a far superior capability for any business that has disaster recovery needs, and with the current state of malware attacks, this is nearly every enterprise.

**Getting Started**

Organizations can often use/reuse/integrate existing components to get a head start on their move to a WaaS environment. Indeed, companies that already have an EMM solution installed can often incrementally add additional key components of a WaaS solution to enable a more complete WaaS suite. Organizations that have deployed VDI or browser-based app delivery products can often reuse some of those components in moving towards a full WaaS suite. And any cloud systems, whether private or public, can often be used capability as a core component of a WaaS upgrade. The key is to work with your existing vendors to identify which components can be reused, and how connections to a complete WaaS can best be made. And importantly, build a strategy that identifies the path to full WaaS, and creates a time frame for achieving it.
Recommendations

We strongly recommend that companies evaluate WaaS as a way to enhance user productivity, increase security and enable IT to provide improved support. While not a solution to 100% of organizational needs and requirements, WaaS goes a long way towards addressing a number of major pain points IT has been struggling with for a number of years.

We recommend organizations look at the advantages of WaaS in the following situations:

- Any organizations dealing with a wide array of device types and/or large numbers of BYOD should consider WaaS to secure and manage universal user access to corporate apps, at a lower cost and in a more controlled and secured fashion.
- Any organizations that have a need to maintain a portfolio of legacy apps that are unattractive to upgrade should implement WaaS as a way to provide access. This is especially true for apps used infrequently, but still required for business operation.
- Enterprises that struggle with PC device migration costs and lack of necessary resources should look at WaaS as a way to limit the required resources needed while reducing costs. Properly configured, WaaS can offer near instantaneous migrations to almost any device.
- Organizations that are particularly worried about disaster recovery preparedness would do well to implement WaaS, as it can significantly lower the burden of planning and operations if disaster recovery is ever required.
- Companies in regulated industries, requiring total control and management of access and particularly access to sensitive data, will find an advantage in WaaS as it provides a centralized policy and control mechanism, and can provide an analytics capability to fully understand how corporate assets are being used.
- Cross platform unified IAM and policy management is often critical in achieving user enablement, especially in companies where users have dedicated functions and limited/controlled access requirements. WaaS offers unique advantages in these situations.
- Finally, any organization wishing to move on to a future app delivery architecture for any user, any device, even devices not yet available, should be building a strategy for fully deploying a WaaS environment in the next 1-2 years, or face escalating costs and limited end user computing options, thus hampering productivity.

Conclusions

While not a silver bullet, WaaS does offer some very attractive capabilities for many companies struggling with issues of BYOD, data security, cost of operations and policy management. With a need to extend typical end users desktops to any device at any time and any location, while still keeping costs in control and security in place, new architectures like WaaS can offer a compelling way for enterprises to maintain end user productivity while managing to control costs and maximize limited IT resources.
About J.Gold Associates

J.Gold Associates provides insightful, meaningful and actionable analysis of trends and opportunities in the computer and technology industries. We offer a broad based knowledge of the technology landscape, and bring that expertise to bear in our work. J.Gold Associates provides strategic consulting, syndicated research and advisory services, and in-context analysis to help its clients make important technology choices and to enable improved product deployment decisions and go to market strategies.