



Workspace as a Service  
enables  
Secure Access to  
Desktops, Applications and  
Data from Any Device

Technical White Paper

## Table of Contents

<b>Introduction</b> .....	4
<b>Challenges with Virtual Desktop Infrastructure (VDI)</b> .....	4
<b>Challenges with Mobile Device Management (MDM)</b> .....	4
<b>The right solution is Workspace as a Service</b> .....	5
<b>What is a Workspace?</b> .....	5
<b>What is Workspace as a Service?</b> .....	6
<b>Workspot is Workspace as a Service</b> .....	6
<b>Workspot Client</b> .....	7
<b>Cross-Platform Architecture</b> .....	8
<b>First time end user on-boarding process</b> .....	8
<b>Single Sign-On</b> .....	9
<b>Enterprise App Store</b> .....	9
<b>Workspot Control</b> .....	10
<b>100% Cloud Architecture</b> .....	10
<b>Leverage Existing Infrastructure</b> .....	11
<b>Control Plane Architecture</b> .....	12
<b>Configuring VPN Access</b> .....	13
<b>App Delivery 2.0</b> .....	14
<b>Challenges with App Delivery 1.0</b> .....	14
<b>App Delivery 2.0</b> .....	14
<b>Provisioning Access to a Web App</b> .....	14
<b>Provisioning Access to a Windows App</b> .....	15
<b>Provisioning Access to a Network Drive</b> .....	15
<b>Provisioning a New User</b> .....	15
<b>Assigning Apps to Users</b> .....	16
<b>Native Email Configuration</b> .....	16
<b>Delivering Native Applications</b> .....	17
<b>Virtual Desktop Infrastructure 2.0 (VDI 2.0)</b> .....	18
<b>Problems with VDI 1.0</b> .....	18
<b>VDI 2.0 is 10x simpler because of cloud and hyper-convergence</b> .....	19
<b>Workspot Enterprise Connector</b> .....	19
<b>Persistent Desktops</b> .....	20
<b>Leverage Existing PC Lifecycle Management Tools</b> .....	20
<b>Provisioning Access to Virtual Desktops</b> .....	20
<b>Remote Office Branch Office (ROBO)</b> .....	20
<b>Security</b> .....	21
<b>Secure Access with PIN</b> .....	21
<b>Device Posture Check</b> .....	21
<b>Configuring Security Policies</b> .....	21

<b>Remote Wipe .....</b>	<b>22</b>
<b>Data Retention.....</b>	<b>23</b>
<b>Securing Data in Motion .....</b>	<b>23</b>
<b>Secure Application Access .....</b>	<b>24</b>
<b>Whitelist/Blacklist Traffic.....</b>	<b>25</b>
<b>Securing Data at Rest.....</b>	<b>25</b>
<b>Secure Document Viewers.....</b>	<b>26</b>
<b>Big Data Context Driven Security.....</b>	<b>27</b>
<b>Compliance and Auditing.....</b>	<b>28</b>
<b>Integration with Splunk .....</b>	<b>29</b>
<b>Context Driven Visibility .....</b>	<b>30</b>
<b>Errors.....</b>	<b>30</b>
<b>Real End User Experience (REUX) .....</b>	<b>31</b>
<b>Applications.....</b>	<b>32</b>
<b>Networks.....</b>	<b>33</b>
<b>Geos .....</b>	<b>34</b>
<b>Devices.....</b>	<b>35</b>
<b>Summary.....</b>	<b>36</b>

## Introduction

A few years ago an employee used two devices to perform work – often a Windows laptop and a Blackberry phone. Both of these devices were purchased and managed by IT. Increasingly today employees have 3+ devices – phone, tablet, and laptop - the majority of which are owned by the employee. How does IT enable secure access to business apps and data (Windows, Web, SaaS, Hybrid, Native and CIFS) from a variety of devices (iOS, Android, Windows OS, Mac OS) most of which are not owned by IT as shown in the figure to the right.

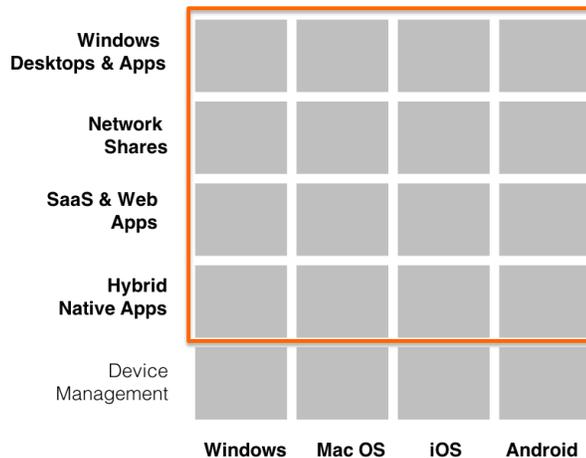


Figure 1 4x4 Matrix used by IT to assess secured access

There were two promising solutions: Virtual Desktop Infrastructure (VDI) and Mobile Device Management (MDM).

### Challenges with Virtual Desktop Infrastructure (VDI)

On the surface, VDI is a very simple solution. Just virtualize a desktop in the data center using standard server virtualization technology. Then the virtual desktop is securely accessible from any device. However, VDI creates a new set of challenges for IT in terms of poor user experience and high total cost of ownership, and often takes several quarters to deploy.

### Challenges with Mobile Device Management (MDM)

The basic tenet of MDM is to enable IT to gain control and lock down a device. This matches the current best practice in most companies, which use Enterprise Software Distribution (ESD) tools to fully manage corporate owned PCs.

MDM creates two challenges for IT. First, end users don't want IT to lock down their devices. Second and more importantly, MDM does not enable access to business applications and data. In order to solve this problem, MDM solutions evolved to add an alphabet soup of capabilities: Mobile

Application Management (MAM), Mobile Content Management (MCM), Secure Browser, Per-App VPN, Container, and others. The result is a disjointed end user experience, low adoption rate by end users, and a complex solution for IT to deploy.

### The right solution is Workspace as a Service

We believe that the right solution is a Workspace as a Service, which enables IT to securely deliver desktops, apps and data to any device in 60 minutes. Workspace as a Service is a combination of next generation app delivery and next generation virtual desktop infrastructure.

### What is a Workspace?

A workspace is a secure area for work on any device, whether the device is managed or unmanaged.

What are the requirements of a workspace?

1. **Desktop Access:** The workspace must provide end users the ability to access a Windows desktop, whether it's a physical desktop or a virtual desktop.
2. **Application Access:** The workspace must provide end users the ability to seamlessly navigate between corporate applications – web, windows, and native. IT needs tools to add/delete/update applications on the device. IT also needs configuration policies tools to control the behavior of applications, e.g., printing from within an application.
3. **Data Access:** The workspace must provide end user the ability to securely access documents from SharePoint and Network File Shares, view and edit documents offline. The solution must incorporate data leakage prevention mechanisms.
4. **Cross-Platform Architecture:** A workspace needs to be portable across different kinds of devices. A workspace should be available on iOS, Mac OS, Windows OS, and Android. It should be available on phone, tablet, and laptop form factors.
5. **Device Security:** The workspace needs to ensure that the device is safe to use: it is not jail broken and that there are no rogue applications on the device. IT should be able to define policies to control the behavior of the workspace, e.g., copy-paste between applications, download documents, etc.

6. **Contextual Security:** In an environment where IT doesn't fully manage the device, IT needs analytics, reports and tools to understand what the end user is doing with work related assets. The solution needs to enable the CISO to get a granular view of end user business activities on a mobile device for compliance and auditing.

### What is Workspace as a Service?

One of the major challenges with any new infrastructure software is that it often comes with a brand new architecture that needs months, sometimes years, to deploy inside a business. IT has to invest significant amount of resources – money, time, and people – in order to determine the true value of the infrastructure.

Unlike traditional infrastructure software, Workspace as a Service is a 100% cloud service. That means:

- Web scalability. Instantly scales for new users without installing new servers.
- Control plane architecture. Apps and data stay in your datacenter and not copied to the cloud. No corporate data flows through our cloud. We do not store credentials in our cloud.
- No special training required for IT resources to manage workspace.
- Workspace as a Service can be in production in 60 minutes.

### Workspot is Workspace as a Service

The Workspot solution has two components:

1. **Workspot Client** is an application that can be downloaded from the public app store. The Workspot Client is the single place on the device where the end user can access corporate assets including desktops, applications and data.
2. **Workspot Control** is a single pane of glass that allows IT to configure and set policies for the Workspot Client.

The Workspot solution combines App Delivery 2.0 with VDI 2.0 to enable IT to deliver any app or any virtual desktop to any device.

## Workspot Client

The Workspot Client is a workspace on any device – PC, Mac, Phone, or Tablet. The workspace provides unified access to desktops, apps, and data on any device. The Workspot Client provides a consistent user experience across different platforms and form factors.



Figure 2 The Workspot Client on different devices

Desktops could be physical desktops or virtual desktops running on hyper-converged infrastructure. Applications can be on-premises and behind the firewall like SharePoint, SAP, etc. Applications can also be SaaS applications like Salesforce.com, Netsuite, etc. Documents can also be downloaded into the Workspot Client from SharePoint and other document repositories. Documents can be made available offline inside the Workspot Client.

### Cross-Platform Architecture

The Workspot Client is a secure container on the device. The container can be fully managed and secured by IT, without interfering with the rest of the device. The UI layer delivers the end user experience.

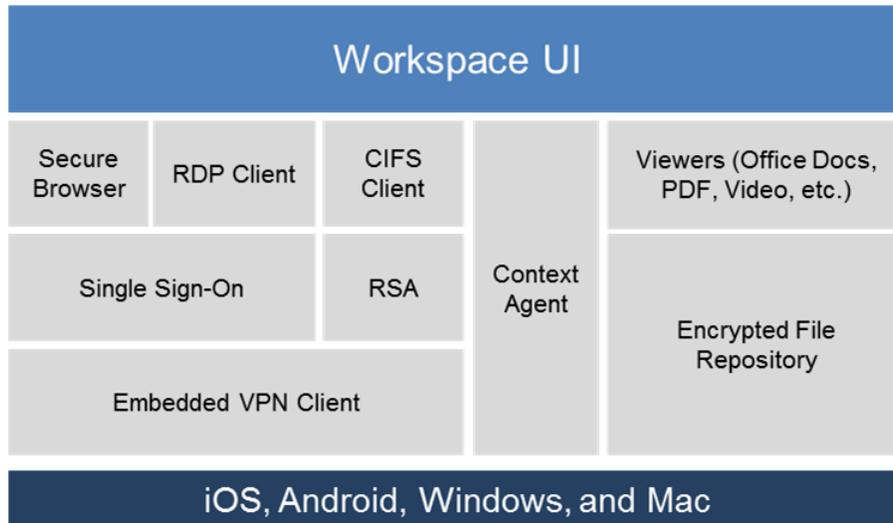


Figure 3 Workspot Client Architecture

### First time end user on-boarding process

The end user downloads the Workspot Client from the App Store. The end user is prompted to enter their business email address. If the email address has been provisioned in Workspot Control, an email is sent to the user with a four-digit token. Once the user enters the token in the client, the Workspot Client downloads the relevant configuration for that user/company from Workspot Control. The configuration information includes the public address of the SSL-VPN appliance against which the user must authenticate. The Workspot Client prompts the user for their Active Directory credentials. Workspot Client then initiates a call to the known SSL-VPN appliance sitting in the corporate DMZ and presents the credentials for verification. The user is prompted for more information, like Group or RSA token, if the VPN box is so configured. If the end user can successfully authenticate against the SSL-VPN appliance, then the Workspot Client is available for use. **Note that user credentials are never routed to or stored on Workspot Control.**

## Single Sign-On

Workspot can single sign on the user onto various business applications either using enterprise SSO mechanisms, like CA Siteminder, or cloud SSO mechanisms, like Okta, Ping Identity, etc.

The Single Sign-On feature requires storing sensitive information like username and password on Workspot Client. These credentials are encrypted using the same mechanism described above for documents stored in the Encrypted File Repository. Besides usernames and passwords, any other information required for auto login like RSA token PIN or RSA secrets will also be encrypted.

## Enterprise App Store

IT can also enable an enterprise app store, as shown in figure below, within Workspot. End users can select and install applications made available to them by IT. These applications can be provisioned and de-provisioned by IT using Workspot Control.

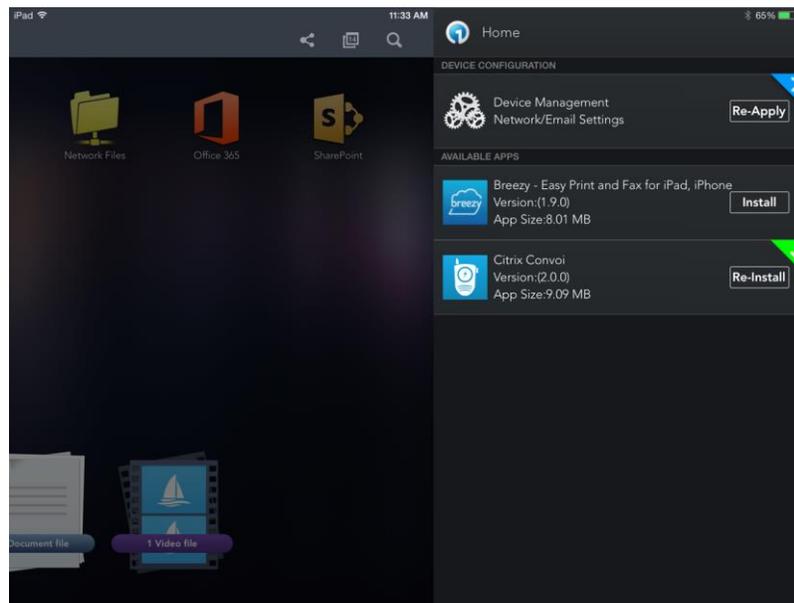


Figure 4 On-device App Store

## Workspot Control

The Workspot Client is managed and monitored using a single pane of glass called Workspot Control.

### 100% Cloud Architecture

Workspot is a 100% cloud multi-tenant architecture. The Workspot Control service runs on Amazon Web Services. IT uses Workspot Control to configure policies, provision users, and provision applications and data. Workspot Control stores configuration and performance data in the cloud:

1. Configuration Data: We store configuration information about the VPN, e.g., public URL address, whether it uses RSA or not. We store a few details about end users, e.g., First Name, Last Name, Email Address, etc. We store information about applications, e.g., Application URLs, whether or not it is behind the firewall, etc.
2. Performance Data: For each network access, we store the amount of time it took to fetch a response from the application (e.g. SharePoint), the device used (e.g. iPad, Windows, Android), the network used (e.g., AT&T), and the location (e.g., California).
3. Activity Data: We track different kinds of activity on the device, e.g., Open/Close Workspot, Open/Close Application (e.g., SAP), Open/Close Document, and View/Print Page of Document. All activity data is anonymized.

## Leverage Existing Infrastructure

The Workspot solution has been architected from the ground up to leverage your existing security and data center infrastructure. The Workspot solution has zero additional footprint in the data center.

Today IT is running many on-premises business applications: web applications, Windows client server applications, and network drives (CIFS).

Companies have deployed VPN and SSL-VPN appliances, like Cisco or Juniper, in their DMZ in the last decade to provide secure remote access to enterprise applications. These appliances have been integrated into identity systems like Active Directory, and security systems like RSA SecurID.

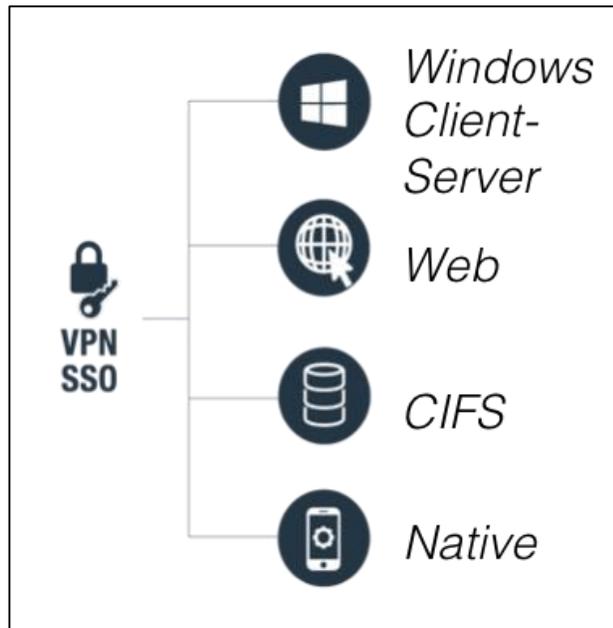


Figure 5 Your current data center

The advent of mobile devices, like smart phones and tablets, has introduced another set of devices that need access to corporate assets. In terms of access these devices are very similar to previous remote access end points. We believe that the existing data center access infrastructure can be leveraged effectively to give employees access to corporate assets from any device. The Workspot solution has been architected to leverage existing data center infrastructure – VPN, Applications, and Data.

## Control Plane Architecture

Workspace Control has been architected to be a control plane:

- No application data flows through Workspace Control
- No user credentials are stored in Workspace Control
- No business applications or data is moved to Workspace Control

When the user is accessing business apps and data on the device using Workspace, all the data flows back and forth directly between the client and the business applications (e.g., Exchange, SharePoint, Salesforce.com). If the applications are behind the firewall, then they go back to the corporate network. If the applications are external, then the traffic directly goes to the external application.

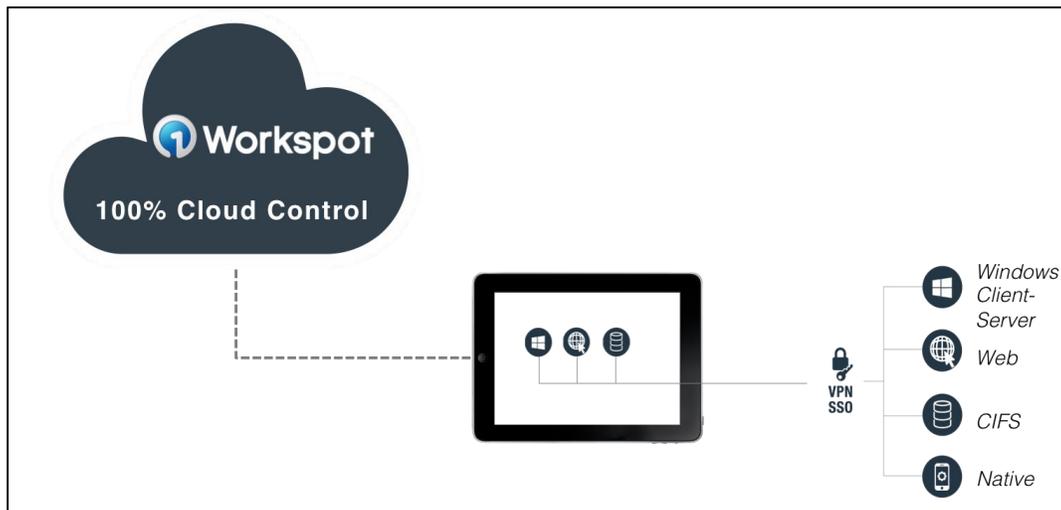


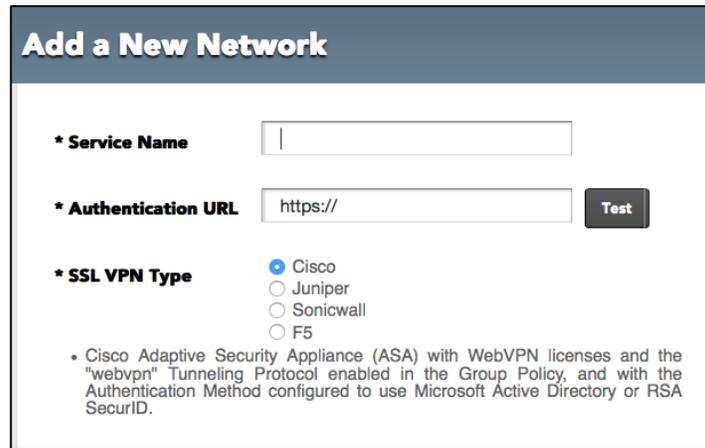
Figure 6 Control Plane Architecture

The separation between control and data planes is very critical for a number of reasons:

- **Security:** Data flows directly between the client and the applications; it does not flow through Workspace Control
- **Availability:** Since Workspace Control is not in the data path, the availability of applications is independent of the availability of our service
- **Performance:** Since Workspace Control is not in the data path, there is nothing to impede the end user experience

## Configuring VPN Access

IT can use Workspot Control to configure VPN access for Workspot Client. Workspot has deep integration with Cisco ASA and Juniper (Pulse Secure) SA appliances. Once the clientless mode is enabled on the appliance, IT needs to specify the public address of the VPN appliance.



The screenshot shows a web form titled "Add a New Network". It contains the following fields and options:

- \* Service Name**: A text input field.
- \* Authentication URL**: A text input field containing "https://", with a "Test" button to its right.
- \* SSL VPN Type**: A radio button selection with four options: "Cisco" (selected), "Juniper", "Sonicwall", and "F5".

Below the radio buttons, there is a note: "• Cisco Adaptive Security Appliance (ASA) with WebVPN licenses and the "webvpn" Tunneling Protocol enabled in the Group Policy, and with the Authentication Method configured to use Microsoft Active Directory or RSA SecurID."

Figure 7 Configure VPN Access

## App Delivery 2.0

The Workspot solution enables IT to securely deliver any app or data onto any device. The applications remain in the data center. In order to provision access to different kinds of applications, IT needs to “point” the Workspot solution to those apps.

### Challenges with App Delivery 1.0

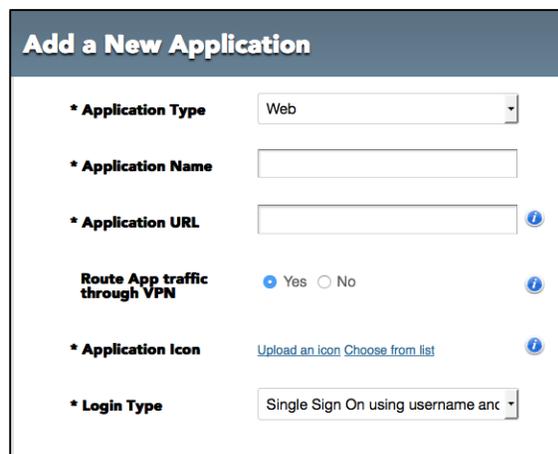
App Delivery 1.0 solutions include (a) remoting solutions like Citrix XenApp and (b) PC Lifecycle Management solutions like BMC Altiris, Microsoft System Center Configuration Manager, IBM BigFix, and others. Remoting solutions were useful to deliver Windows client server applications onto any device. PC Lifecycle management solutions were used to manage and deliver applications onto PC endpoints. Both these solutions don't meet today's requirements, where IT runs web apps, SaaS apps, and increasingly hybrid and native apps. And users consume these applications from phones, tablets, and Macs, which are mostly personally owned.

### App Delivery 2.0

App Delivery 2.0 solutions securely deliver any type of applications (Web, SaaS, Windows, Hybrid, and Native) onto any device (PC, Mac, iOS, and Android).

### Provisioning Access to a Web App

An organization is already running tens, if not hundreds, of web applications in their organization, for example, SAP, SharePoint, Siebel, and many custom applications. In order to provision access to those web applications, IT needs to specify the URL of those applications in Workspot Control as shown to the right. IT does not need to make any changes to the operations of the applications.



**Add a New Application**

- \* **Application Type**: Web
- \* **Application Name**: [Text Input]
- \* **Application URL**: [Text Input]
- Route App traffic through VPN**:  Yes  No
- \* **Application Icon**: [Upload an icon](#) [Choose from list](#)
- \* **Login Type**: Single Sign On using username and password

Figure 8 Provision Web App Access

## Provisioning Access to a Windows App

Companies still run many core business applications that were written using Windows client-server technologies. IT can configure access to these applications by specifying the address of the XenApp broker or the Terminal Server or the Terminal Server broker on which these applications are running in the data center. These applications will be accessed using the Remote Data Protocol (RDP). IT does not need to make any changes to the operations of the applications.

The screenshot shows a web form titled "Add a New Application". The form includes the following fields and options:

- \* Application Type:** A dropdown menu with "Windows Application" selected.
- \* Application Name:** An empty text input field.
- Allow user to specify server address**
- \* Server Address:** An empty text input field with an information icon.
- Route App traffic through VPN:** Radio buttons for "Yes" (selected) and "No".
- \* Application Icon:** A link to "Upload an icon" and a link to "Choose from list", both with information icons.
- \* Login Type:** A dropdown menu with "Single Sign On using username and password" selected.
- Advanced Settings**

Figure 9 Provision Windows App Access

## Provisioning Access to a Network Drive

There is a lot of corporate data on network drives. Today these network drives are accessible as drives mounted on a Windows PC. In order to enable access to existing network drives from Workspot Client, IT needs to provide the CIFS path of these network drives. We also support DFS. IT does not need to make any changes to the operations of the network drives.

The screenshot shows a web form titled "Add a New Application". The form includes the following fields and options:

- \* Application Type:** A dropdown menu with "Content Repository" selected.
- \* Repository Type:** A dropdown menu with "Network File Share" selected.
- \* Application Name:** An empty text input field.
- \* CIFS URL:** A text input field containing "CIFS://<server>/<share>" with an information icon. Below the field is the text "Enter a file share name in the form of a CIFS URL."
- Route App traffic through VPN:** Radio buttons for "Yes" (selected) and "No".
- \* Login Type:** A dropdown menu with "Single Sign On using username and password" selected.
- Allow Document Editing Through RDP:** Radio buttons for "Yes" and "No" (selected).
- Select App for Document Editing:** A dropdown menu with "Select" selected.

Figure 10 Provision Network Drive Access

## Provisioning a New User

A new user is provisioned in Workspot Control. The administrator needs the First Name, Last Name, and Email address of the user. They assign the user to a group, which is mapped to a set of applications, a network configuration, and various security policies. We have also enabled a self-registration process, in which case IT doesn't need to add the user to Workspot Control.

## Assigning Apps to Users

Users can be members of groups. There are multiple ways to assign applications to users: (a) assign apps to users (b) create bundles of apps and assign to groups (c) assign a bundles of apps to users (d) assign apps to groups.

## Native Email Configuration

IT can use Workspot Control to configure the native email client on an iOS device. Workspot uses standard iOS MDM profiles to provision enterprise email on the device.

**Exchange ActiveSync**

**Configure**

**Account Name** [required]  
Name for Exchange ActiveSync account

**Account Description**  
The display name of the account(e.g. "Company Mail Account")

**Exchange ActiveSync Host** [required]  
Microsoft Exchange Server

**Allow Move**  
Allow user to move messages from account

**Sync Recent Email Addresses**  
Sync email addresses contacted on this device to Recents list

**Use SSL**  
Send all communication using SSL protocol

**Past Days of Mail to Sync** 1 week  
The maximum number of days of mail to synchronize

**Use registered email address as exchange account user id**  
Unchecking this would prompt user to enter user id when profile is installed

Figure 11 Configure Native Email

## Delivering Native Applications

IT can use Workspot Control to deliver both iOS applications from the public app store or homegrown iOS applications. IT can enable standard iOS policies for the applications, like auto-removal when the MDM profile is deleted, and/or to not backup the applications' data onto iCloud.

**Add a New Application**

\* **Application Type**  \* **Add to Bundles**

\* **Application Name**

\* **IPA File** [Upload](#)

Remove this app when MDM profile is removed

Do not backup data generated by this app when the device is synced

**Prevent Backup**

All Apps

Amitabh's Bundle

Express Setup Bundle

Puneet's Bundle

Recycle bin

RS Investments

Scholle

Scripps

Special-Office365-Bundle

Stacey bundle

**Cancel** **Add Application**

Figure 12 Provision Native Application

## Virtual Desktop Infrastructure 2.0 (VDI 2.0)

VDI 2.0 combines hyper-converged infrastructure and Workspot cloud control plane, and delivers virtual desktops to any user on any device.

### Problems with VDI 1.0

One major problem with VDI 1.0 was the poor User Experience for many classes of apps and on mobile devices. Since all applications in the desktop are remoted, the user experience of web applications, video apps, real-time apps, VOIP applications, and others suffer. Users cannot work offline. Users don't want a Windows desktop on their mobile devices. Our App Delivery 2.0 provides IT an alternate way of delivering these classes of applications directly onto the devices and thereby solve the user experience problem.

The other issues with VDI 1.0 result from legacy data centers not being optimized for desktop workloads. A data center has been optimized for server workloads. A typical data center runs tens, maybe a **few hundred** virtual machines, each requiring tens of gigabytes of storage and doing **mostly reads**. A desktop workload breaks the data center architecture. A medium-sized VDI deployment can have a **few thousand** virtual machines, each requiring tens of gigabytes of storage and doing **mostly writes**. A VDI workload needs both high performance Flash storage and lots of storage.

VDI 1.0 software was designed to work around the problems with the legacy data center. In order to reduce the amount of storage required, VDI solutions introduced golden images, app layering, dynamics desktops. In order to work around the performance problems of spinning disks, VDI solutions leveraged local disks on servers.

In order to work around a data center architecture not optimized for desktop workloads, VDI 1.0 solutions became operationally complex. These result in high operational expenses and many support issues, because every problem results in five different teams being involved to do root cause analysis: server, storage, network, server virtualization, and desktops.

## VDI 2.0 is 10x simpler because of cloud and hyper-convergence

The advent of cloud and hyper-converged technologies enables a new architecture for VDI. We call this VDI 2.0. Our VDI 2.0 solution is purposefully built to leverage hyper-convergence and cloud technologies. Hyper-converged appliances consolidate storage, networking, compute, and virtualization layers into a single appliance with predictable scalability. These hyper-converged appliances work very well for desktop workloads and a number of the VDI 1.0 workarounds become unnecessary.

Virtual desktop workloads can now run on hyper-converged appliances. Our VDI 2.0 solution leverages the cloud control plane architecture to allow IT to manage and operate the workloads from the cloud.

### Workspot Enterprise Connector

Virtual desktops are created on hyper-converged infrastructure by the Enterprise Connector. The Enterprise Connector is a Windows virtual machine that is installed on the hyper-converged infrastructure. The Connector receives configuration information from Workspot Control and creates a pool of virtual desktops on the hyper-converged infrastructure.

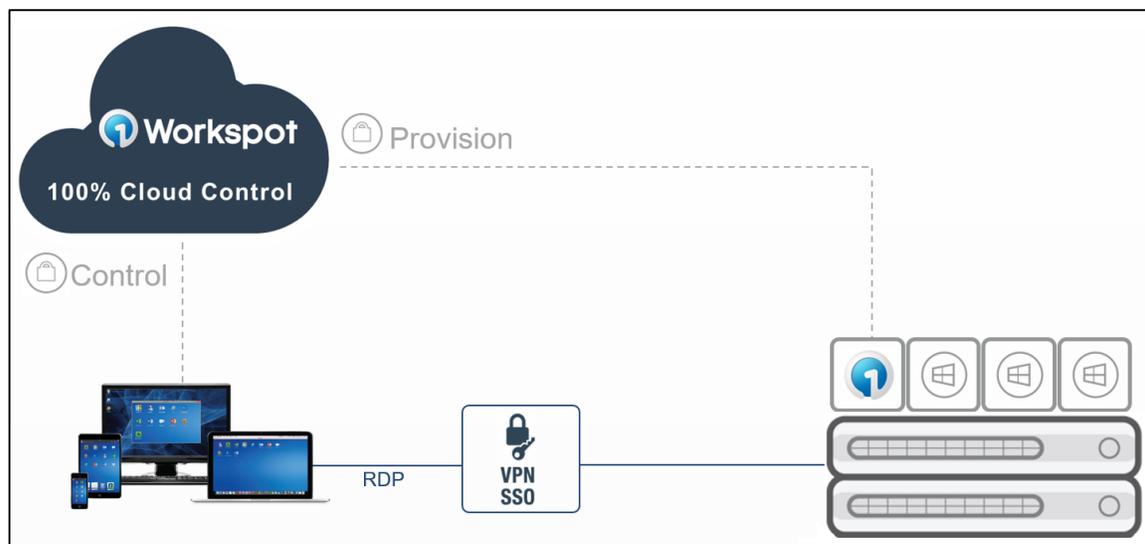


Figure 13 Deployment Architecture for VDI 2.0

### **Persistent Desktops**

Since hyper-converged appliances have many optimizations built into the architecture like de-duplication and high performance Flash storage, we have chosen to create a persistent desktop for each user. This is how physical PCs are assigned to users: each user gets their own PC. Similarly, each user gets their own virtual desktop.

### **Leverage Existing PC Lifecycle Management Tools**

IT already has made lots of investment in PC lifecycle management tools. These tools are used to update the operating system, install and update applications, and configure printers and other peripherals. IT can leverage those same PC lifecycle management tools to manage persistent virtual desktops. No new tools or processes are needed.

### **Provisioning Access to Virtual Desktops**

Once IT has created a pool of virtual desktops, they can bulk-assign the pool of virtual desktops to a group of end users.

### **Remote Office Branch Office (ROBO)**

VDI 1.0 solutions were too complex to be deployed at a branch office. The desktops at a branch could not be centralized because nobody at the branch could work if the network connectivity was down.

The VDI 2.0 architecture enables IT to deploy hyper-converged appliances at the branch office. The virtual desktops will run on the local appliances. The desktops can be operated from the Workspot Control. This way IT can benefit of desktop virtualization, but also provides the best experience for end users at a branch office.

## Security

### Secure Access with PIN

When a user taps on Workspot Client on their device, they are prompted for a PIN. The PIN is validated against client master secret (CMS). If the CMS can be decrypted then the PIN is deemed valid; otherwise the PIN is invalid. The Workspot Client will allow up to 5 invalid PIN entries after which Workspot Client will wipe all the data on the device.

### Device Posture Check

As soon as the Workspot Client is started, it conducts a posture check to determine whether the device has been jail-broken or rooted. An evolving set of checks to verify supported versions and platforms are performed, and only when the device is determined to be secure is the Workspot Client launched.

### Configuring Security Policies

IT can configure other aspects of the behavior of the client using Workspot Control:

- Restricting access to application or documents by user
- Restricting access to applications or documents
- Enabling/disabling offline usage of the application
- Restricting copy and paste
- Restricting printing within geography

## Workspace as a Service enables Secure Access to Desktops, Applications and Data from any Device

Utility Rules

<b>Enable printing</b>	<input checked="" type="radio"/> Yes	<input type="radio"/> No	Allows the user to print using the Workspot screen print feature.
<b>Enable screen capture</b>	<input checked="" type="radio"/> Yes	<input type="radio"/> No	Allows the user to capture screenshots using the Workspot screen capture feature.
<b>Enable copy and paste</b>	<input checked="" type="radio"/> Yes	<input type="radio"/> No	Allows the user to copy and paste when accessing documents within Workspot.
<b>Open documents using an external viewer</b>	<input type="radio"/> Yes	<input checked="" type="radio"/> No	Allowing open in an external viewer may save the document outside of Workspot. The document will not be secured within Workspot and can be accessed by other third-party applications.
<b>Enforce location services for Workspot</b>	<input type="radio"/> Yes	<input checked="" type="radio"/> No	Enforcing location services will require the user to allow Workspot to manage access based on the location of their device.
<b>Enforce remote notification services for Workspot</b>	<input type="radio"/> Yes	<input checked="" type="radio"/> No	Enforcing remote notification services will require the user to allow Workspot to send notifications to their device.
<b>Allow uploads from device</b>	<input type="radio"/> Yes	<input checked="" type="radio"/> No	Allow the user to upload photos, videos and other content from the device into Workspot.
<b>Allow rooted Android devices</b>	<input type="radio"/> Yes	<input checked="" type="radio"/> No	Allow the user to access Workspot on rooted Android devices.
<b>Allow audio redirection</b>	<input type="radio"/> Yes	<input checked="" type="radio"/> No	Enable audio between remote desktop and user device.
<b>Allow redirection of local disks</b>	<input type="radio"/> Yes	<input checked="" type="radio"/> No	Allow user to access local disks from remote desktop.

Figure 14 Setting security policies from within Workspot Control

### Remote Wipe

Workspot Control provides IT the capability to remote wipe any data, including documents, cached objects and cookies, inside the Workspot Client. Data outside the Workspot Client is unaffected by the remote wipe operation.

### Data Retention

Our current policy is to retain configuration and activity data in Workspot Control for a period of one year. Note that there is no application traffic through Workspot Control. Also no user credentials is ever sent to or stored inside Workspot Control.

### Securing Data in Motion

The embedded VPN Client is a full L4-L7 stack and implements a split tunnel that allows the Workspot Client to be connected simultaneously to both the corporate and public networks. Application traffic can be routed to either network based on IT policies. We are using a FIPS compliant SSL library in the embedded VPN Client.

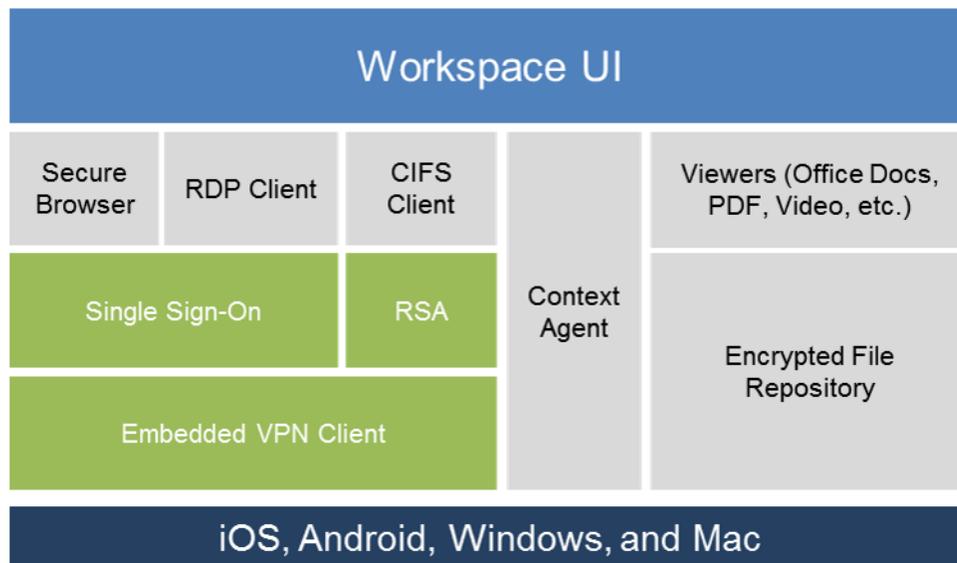


Figure 15 Virtual Network

## Secure Application Access

The Workspot client enables secure access to different classes of applications running in the data center:

1. **Web Applications:** There is a secure browser bundled into Workspot that enables access to web applications like SAP, SharePoint, etc.
2. **Windows Client Server Applications:** There is an RDP client integrated into Workspot that enables access to an app running either on XenApp or Terminal Server. The Terminal Server may be running a Windows application, a Windows server, or even a Windows desktop.
3. **Network Drives:** We have integrated a CIFS client into Workspot. This enables an end user to access a network drive in the data center.

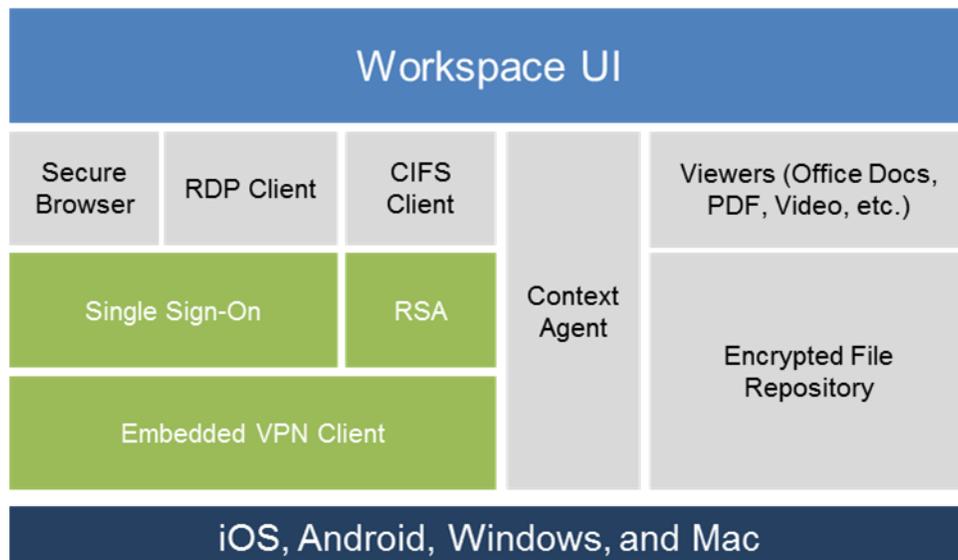


Figure 16 Securely accessing applications and data

### Whitelist/Blacklist Traffic

IT can also control which sites the user can and cannot visit from inside the Workspot client by configuring a blacklist/whitelist. We also enable dynamic blacklisting of known malicious URLs.

### Securing Data at Rest

The encrypted file repository stores documents downloaded by the user. All the documents in the file repository are encrypted with a multi-layer scheme:

1. All assets are encrypted in memory before they touch the file system. Every object is encrypted using a different key.
2. Each key is encrypted using a master key.
3. The master key is encrypted with a user specified PIN that is not stored on the device. The user can access the Workspot application only when they can successfully provide the PIN.

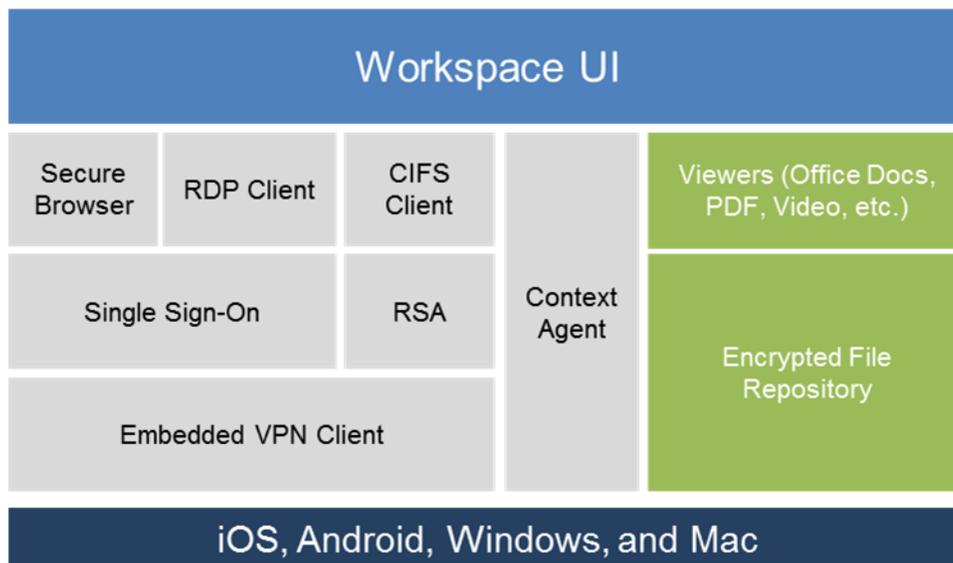


Figure 17 Virtual File System secures all data at rest with AES 256-bit encryption

## Secure Document Viewers

When an end user downloads a document inside the Workspot application, it is encrypted in-flight. The file system remains in an encrypted state even when the end user is within the container. Only when the end user wants to view a document, for example an Adobe Acrobat document, does the Workspot Client decrypt the selected document and present it inside a viewer that is embedded within Workspot. We have tuned the embedded viewers for the best possible rendering experience. Documents are more secure, because the documents stay within the Workspot Client. As soon as the end user finishes viewing the document and closes the viewer, the document is restored to its encrypted state on the device. For large documents, we only decrypt the pages of the document that are currently being viewed.

### Big Data Context Driven Security

When a user uses Workspot to access enterprise assets, the client collects contextual data (as shown below – who did what, when, where, and how. Workspot only collects this data for business activity – not for personal applications like Facebook on the device. This data can be used for compliance, auditing, and adaptive authentication.

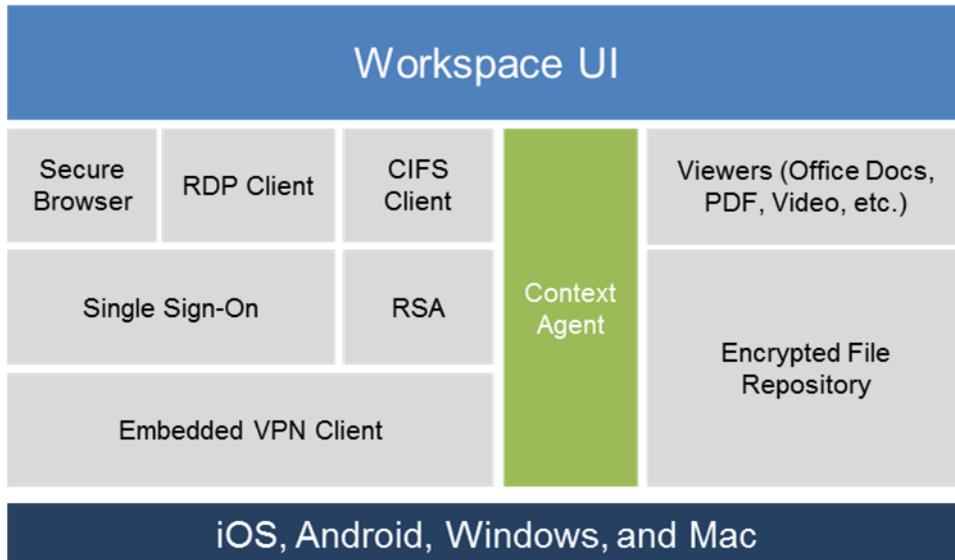


Figure 18 Context Collection is built into Workspot Client

## Compliance and Auditing

Organizations with compliance and auditing needs are using SIEM systems. Until now SIEM systems have tried to infer user actions with data from various systems like card swipe, login, logout, system logs, etc. For example, based on a card swipe, the system can detect that the user was in a certain office in China, followed by a log entry in SAP that the user logged into SAP, and finally an oval email generated by SAP for a purchase order.

We collect end user activity data in Workspot client. This is granular data of the activity performed by the end user on the device, and includes the following:

- Location and Time of activity
- Device used to perform activity
- Application accessed
- Documents downloaded, pages viewed and/or printed

Our Events module provides a searchable view of the end user activity data as shown in the figure below.

Date & Time	Event	User Name	Geo	Device
12:10 PM 07/11/2013	<b>Amitabh</b> Sinha accessed 1st page of document App Store Review Guidelines (1).pdf	amitabh	California	iPad 3, WiFi
12:10 PM 07/11/2013	<b>Amitabh</b> Sinha opened document App Store Review Guidelines (1).pdf	amitabh	California	iPad 3, WiFi
12:10 PM 07/11/2013	<b>Amitabh</b> Sinha downloaded document App Store Review Guidelines (1).pdf from https://share.o1works.com/Shared%20Documents/App%20Store%20Review%20Guidelines.pdf	amitabh	California	iPad 3, WiFi
12:10 PM 07/11/2013	<b>Amitabh</b> Sinha opened app Sharepoint	amitabh	California	iPad 3, WiFi
12:08 PM 07/11/2013	<b>Amitabh</b> Sinha accessed 7th page of document Analyst Briefing.pdf	amitabh	California	iPad 3, WiFi
12:06 PM 07/11/2013	<b>Amitabh</b> Sinha accessed 6th page of document Analyst Briefing.pdf	amitabh	California	iPad 3, WiFi
12:05 PM 07/11/2013	<b>Amitabh</b> Sinha accessed 5th page of document Analyst Briefing.pdf	amitabh	California	iPad 3, WiFi
12:04 PM 07/11/2013	<b>Amitabh</b> Sinha accessed 4th page of document Analyst Briefing.pdf	amitabh	California	iPad 3, WiFi
12:03 PM 07/11/2013	<b>Amitabh</b> Sinha accessed 3rd page of document Analyst Briefing.pdf	amitabh	California	iPad 3, WiFi
12:02 PM 07/11/2013	<b>Amitabh</b> Sinha accessed 2nd page of document Analyst Briefing.pdf	amitabh	California	iPad 3, WiFi

Figure 19 Context Collection is built into Workspot Client

## Integration with Splunk

IT can download the Splunk plugin from Workspot Control. The Splunk plugin needs two keys for configuration – these are available inside Workspot Control as shown in the figure below.

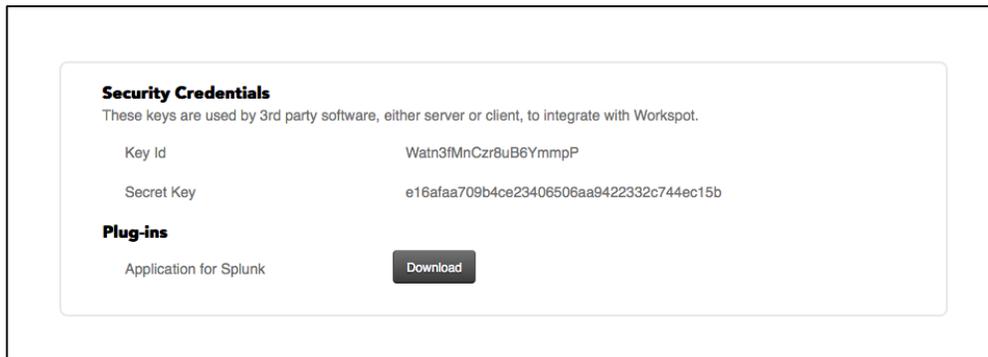


Figure 20 Configuring Splunk Integration

Once integrated the Events data from Workspot is delivered into Splunk. They can be viewed, searched, and manipulated with standard Splunk tools as shown in the figure below.

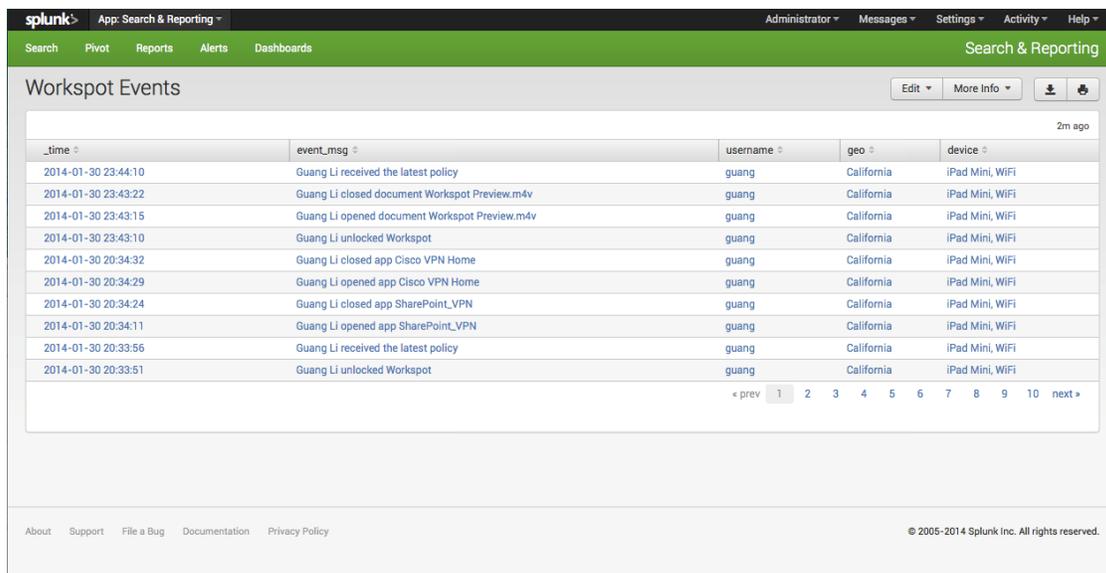


Figure 21 Workspot Context Data in Splunk

## Context Driven Visibility

In addition to collecting end user actions, the Workspot Client also collects the real time user experience – how long did an access take, whether or not it was successful. Each such data point is tagged with location, device type, application, user, and network used.

### Errors

Any time a user takes an action inside Workspot Client that is unsuccessful it is recorded. We then aggregate the errors across all the users in an organization and classify them. IT has an aggregated view of all the problems in the organization – which application, what error, how frequently, and when did it last occur.

User Errors Summary					
Application	Error	Description	Frequency (day / week / all)	Last Occurrence(UTC)	URL
Outlook 365	<b>Http error 404 (Not Found)</b>	The web server responded but the requested page or content was not ... More	4 / 40 / 58	9:27 PM 10/16/2015	<a href="https://outlook.office365.com/owa/manifests/appCacheManifestHandler.ashx?owamanifest=1">https://outlook.office365.com/owa/manifests/appCacheManifestHandler.ashx?owamanifest=1</a>
SharePoint Documents	<b>Http error 404 (Not Found)</b>	The web server responded but the requested page or content was not ... More	0 / 2 / 183	4:04 PM 10/16/2015	<a href="http://sp2010/SitePages/_vti_bin/Webs.aspx">http://sp2010/SitePages/_vti_bin/Webs.aspx</a>
SharePoint Documents	<b>Http error 404 (Not Found)</b>	The web server responded but the requested page or content was not ... More	0 / 2 / 184	4:04 PM 10/16/2015	<a href="http://sp2010/SitePages/Home.aspx/_vti_bin/Webs.aspx">http://sp2010/SitePages/Home.aspx/_vti_bin/Webs.aspx</a>
SharePointOnline	<b>Http error 500 (Server Error)</b>	The application server responded but encountered an error. Verify that the ... More	0 / 2 / 219	4:04 PM 10/16/2015	<a href="https://workspot.sharepoint.com/_layouts/_vti_bin/Webs.aspx">https://workspot.sharepoint.com/_layouts/_vti_bin/Webs.aspx</a>
SharePointOnline	<b>Http error 500 (Server Error)</b>	The application server responded but encountered an error. Verify that the ... More	0 / 2 / 220	4:04 PM 10/16/2015	<a href="https://workspot.sharepoint.com/_layouts/15/_vti_bin/Webs.aspx">https://workspot.sharepoint.com/_layouts/15/_vti_bin/Webs.aspx</a>
SharePointOnline	<b>Http error 500 (Server Error)</b>	The application server responded but encountered an error. Verify that the ... More	0 / 2 / 170	4:04 PM 10/16/2015	<a href="https://workspot.sharepoint.com/_layouts/15/start.aspx/_vti_bin/Webs.aspx">https://workspot.sharepoint.com/_layouts/15/start.aspx/_vti_bin/Webs.aspx</a>

Figure 22 Contextual error summary speeds diagnostic

### **Real End User Experience (REUX)**

The Reports module in Workspot helps IT analyze the real end user experience on any devices for all applications, including SaaS.

Every time a user performs an action inside the Workspot client, we record the user, application, location, device used, network name, performance, availability, etc. The data is then available

For example:

- The applications that are least available
- The applications that have the slowest response time
- The slowest devices for your applications
- The slowest wireless network for users
- The least reliable network for users

## Applications

The applications report section enables IT to analyze which apps are used, availability of the applications, the slowest applications, the bandwidth consumed by the application, and other metrics.



Figure 23 Deep insights into application performance from user perspective

## Networks

The networks report section enables IT to analyze which networks are used by users, availability of different networks, the slowest network, the numbers of users using different networks, and other metrics.

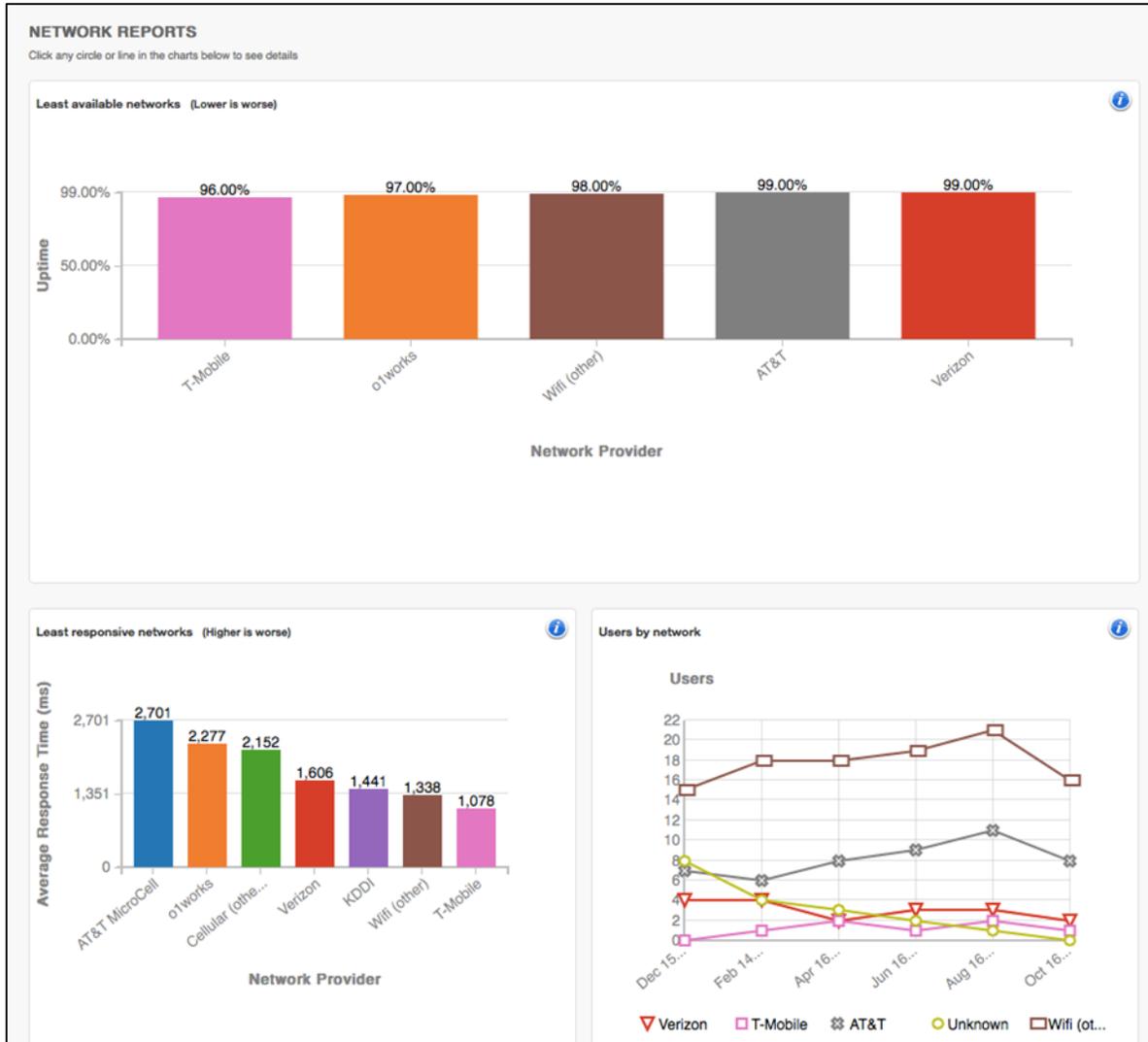


Figure 24 Single view on performance across multiple networks

## Geos

The geo report section enables IT to analyze how users are accessing applications from various geos.

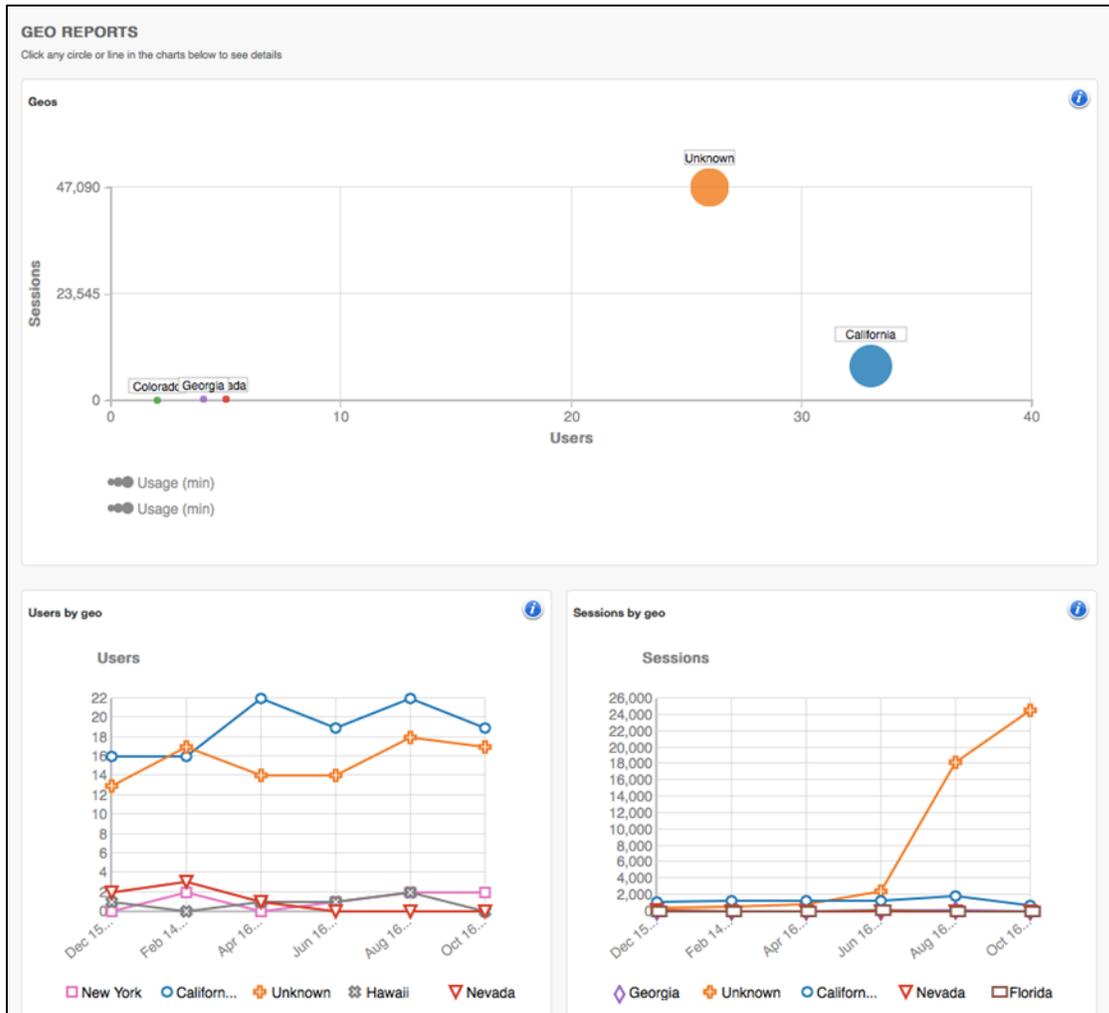


Figure 25 Location aware detection of usage and performance

## Devices

The devices report section enables IT to analyze which devices are being used – how many users, how many sessions, and trends in usage over days, weeks, and months.

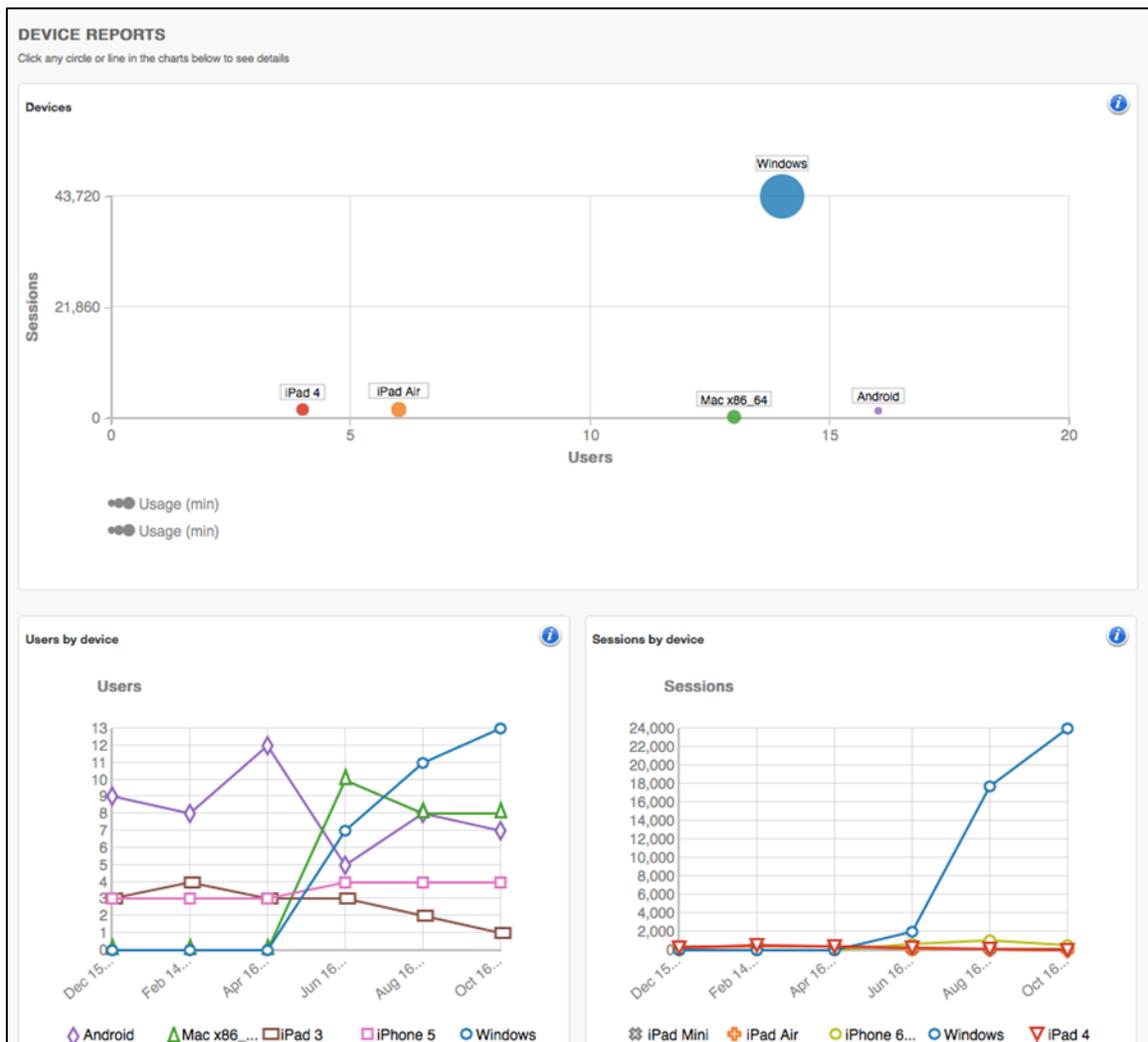


Figure 26 Performance metrics by device

## Summary

Existing IT solutions to deliver, manage, and secure enterprise desktops, applications and devices rely on employees using devices that are purchased, provisioned, and managed by IT. These solutions don't transfer to an environment where the devices are increasingly employee owned, and hence not under IT control.

The Workspot Workspace as a Service leverages existing infrastructure for applications and security and enables IT to rapidly deliver desktops and applications onto any device. Our solution enhances the security, compliance, and auditing capabilities of IT for applications delivered using Workspot. Finally, and most importantly, our solution is designed with the end user in mind, and will simplify their experience in accessing business applications and data on their personal devices.