Workspot

VDI Reinvented: The Innovation Behind the Revolutionary Workspot VDI Cloud Service

Technical White Paper

Table of Contents

Introduction

Today, IT has three different scenarios to support when looking to deliver applications and desktops:

1. **Deliver virtual applications:** IT uses virtual app delivery when users already have a Windows endpoint. In this scenario, IT typically wants to deliver 5-7 ”problem” applications to those users. The most commonly deployed virtual applications are the browser and SAP.
2. **Deliver server hosted desktops:** IT uses server-hosted desktops for task worker use cases. In this scenario, end users need 3-5 applications and a familiar Windows interface on a thin client. Here, the most common use case is a call center.
3. **Deliver virtual desktops:** IT uses full Windows 7 or Windows 10 virtual desktops for knowledge worker scenarios, in which users may need tens or hundreds of applications.

It used to be that supporting these scenarios meant that IT spent months procuring hardware, architecting a solution, and then deploying it on-premises. However painful and expensive, there were no other deployment options. But with the advent of the public cloud as a viable alternative to on-premises implementations, IT now has the flexibility to deliver virtual desktops and apps from both on-premises and the cloud.

However, with these new options, the solution landscape has become even more fragmented:

The solution landscape is complex and highly fragmented

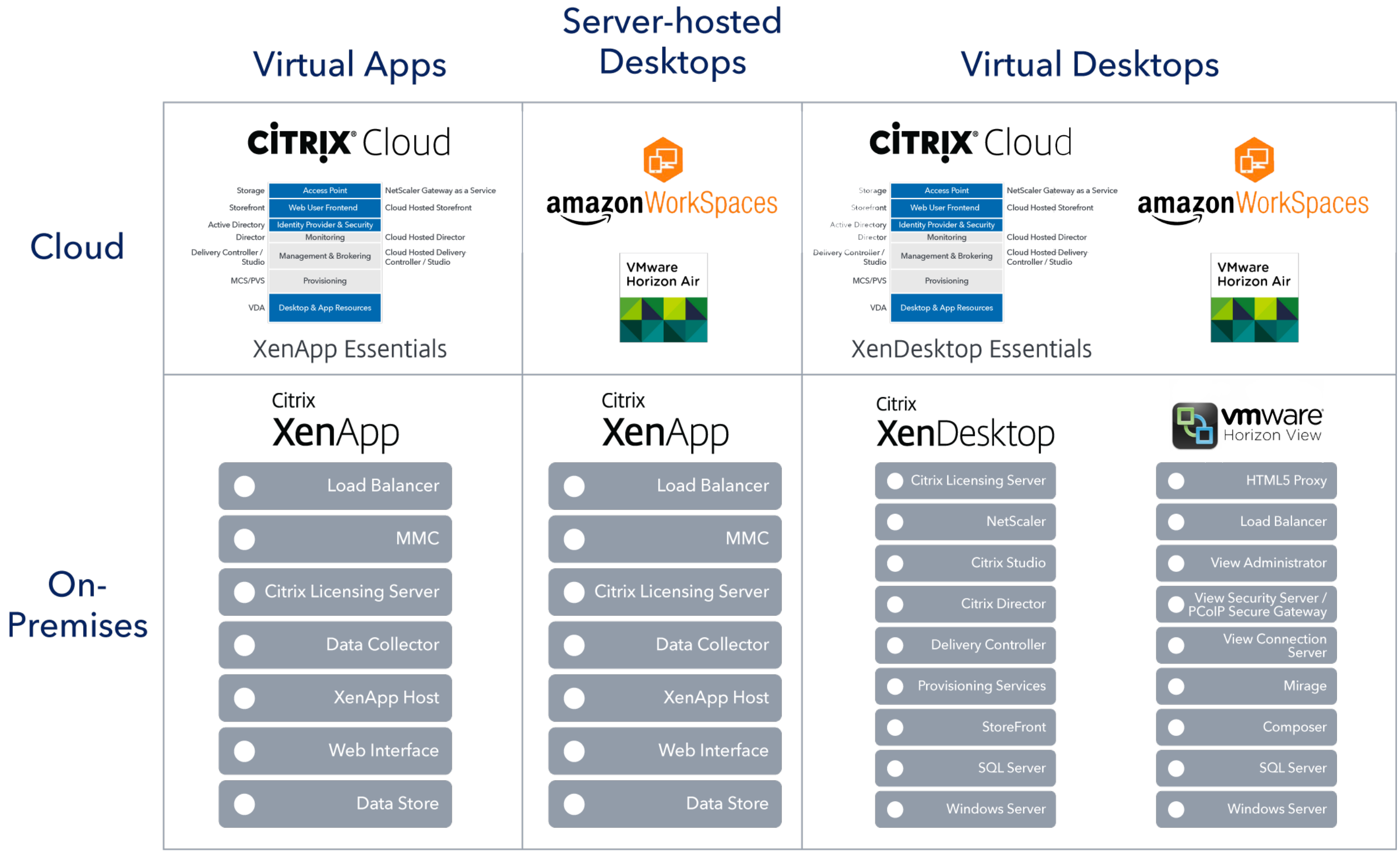


Figure 1: VDI 1.0 fragmented solution landscape.

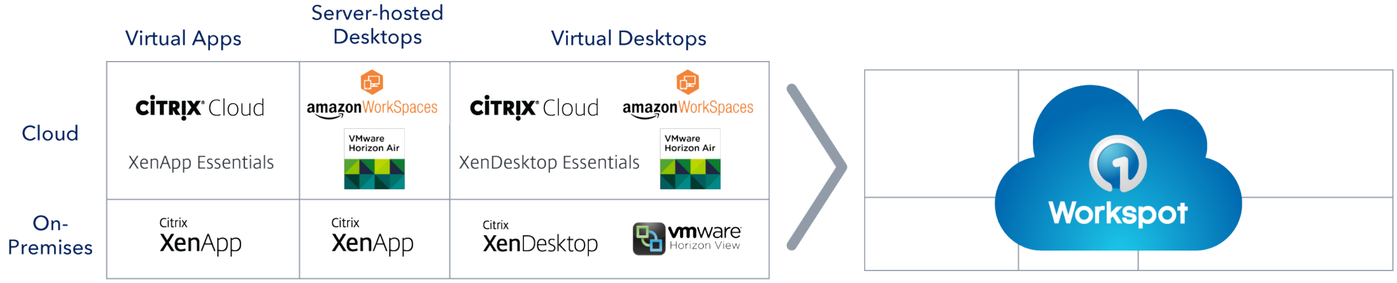
WHAT IF YOU HAVE MORE THAN ONE PROBLEM TO SOLVE?

It's possible that some organizations fit neatly into a single box, but the majority need to satisfy multiple use cases. Why? Because the world and the workforce have become more mobile; different types of workers have unique computing needs; and then there are regulatory and compliance considerations. As a result, most organizations need some things in the cloud and other things on-premises. They need a hybrid solution. With a hybrid solution, they can serve employees who want to use their own devices (BYOD), as well as satellite offices that don't have on-premises datacenters. Unfortunately, the legacy vendors in the diagram above require organizations to buy multiple products to deploy a hybrid solution. The result is even more cost and more complexity.

As IT teams grapple with constant change and relentless demands on constrained resources, there's no justification for investing 9+ months building out a hybrid infrastructure on your own. Old-fashioned approaches to end user computing (EUC) don't make sense any more. If you don't know where to start, or what's available, you're not alone. That's where Workspot can help.

WHERE TO GO FROM HERE

Workspot offers the only solution on the market that enables delivery of virtualized apps, server-hosted desktops, virtual desktops, and GPU-accelerated workstations – from the cloud, on-premises, or both, using a single platform.



	Virtual Apps	Server-hosted Desktops	Virtual Desktops	
Cloud	CITRIX Cloud XenApp Essentials	amazon WorkSpaces VMware Horizon Air	CITRIX Cloud XenDesktop Essentials	amazon WorkSpaces VMware Horizon Air
On-Premises	Citrix XenApp	Citrix XenApp	Citrix XenDesktop	vmware Horizon View

Figure 2: Deliver virtualized apps, server-hosted desktops, and virtual desktops from the cloud or on-premises – or both – with a single platform.

Think about that for a minute. Now all virtual apps, desktops and workstations, regardless of whether they're on Microsoft Azure or on-premises, are managed from a single pane of glass. Workspot is a one-stop shop – there's just one consolidated bill and one console to manage everything, and deployment happens in less than one day.

Workspot ends complexity with a single platform

THE WORKSPOT SOLUTION

Workspot has revolutionized VDI with its award winning, next-generation VDI 2.0 solutions: Cloud Apps, Cloud Desktops and Cloud Workstations. We have solved the cost and complexity challenges customers face with legacy app and desktop virtualization solutions. VDI 2.0 enables IT to deliver virtual apps, desktops and GPU workstations to any device so people can collaborate better and stay productive no matter where they go. In the following sections we'll explore the technology innovations behind this VDI 2.0 revolution. Workspot has engineered VDI simplicity into two primary components:

1. **Workspot Control** is the cloud-based management console. It's the only cloud-native, multi-tenant VDI control plane. It's a single pane of glass that allows IT to configure and set policies for Workspot Client, provision users, and provision applications and data. Workspot Control also acts as a central repository for gathering and storing configuration data, performance data and activity data in the cloud.

2. **Workspot Client** is an application that can be downloaded from the public App Store. Workspot Client is the workspace on the device where the end user can securely access corporate assets including desktops, applications and data.

WORKSPOT'S CLOUD-FIRST APPROACH

Workspot is tightly integrated with Microsoft Azure, allowing customers to enjoy the benefits of the industry's first turnkey VDI cloud service. However, while many organizations have a cloud-first strategy, some prefer a hybrid deployment. Workspot also integrates with VMware vSphere, Nutanix Acropolis, Microsoft Hyper-V, and KVM. Workspot Control supports many platforms, both legacy and hyperconverged infrastructure. Workspot Control is completely agnostic about datacenter infrastructure, so apps, desktops and workstations live wherever it makes the most sense for your organization: on-premises, in the cloud, or both. It's completely up to you, and it's important to note that none of this data or user credentials ever enter Workspot Control. Find more detail in the "Control Plane Architecture" section.

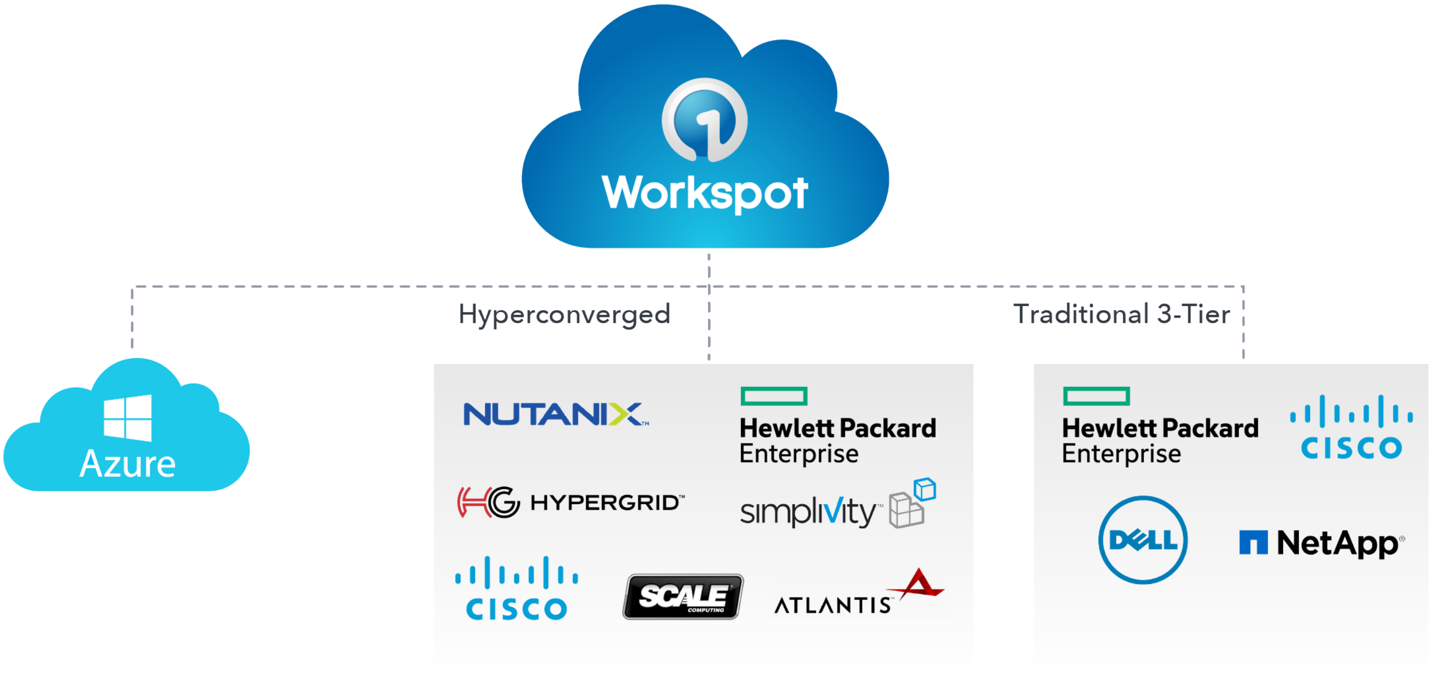


Figure 3: Workspot supports heterogeneous infrastructure.

Workspot Control: Cloud-Native, Multi-Tenant, Infinitely Scalable

HOW DOES IT DELIVER A WORKSPACE?

One of the major challenges with legacy VDI solutions is that their complex architectures require months, sometimes years, to deploy in an organization. IT must invest a significant amount of resources – money, time, and people – to determine the value of the solution, which places all of the risk on the customer.

Workspot takes a completely different approach, originating from the belief that customers shouldn't have to assume all the risk. Workspot's mission is to make virtual application, desktop and workstation delivery insanely simple. Our turnkey virtual app, desktop and GPU-workstation service is an industry first, making it possible for customers to be live in hours.

Workspot Control makes VDI and app delivery insanely simple

At the core of the solution is Workspot Control, the cloud service that brings together the VDI control plane, the broker, and the load balancer into a unified platform that eliminates the complexity around deploying virtual applications, server-hosted desktops and full virtual desktops. Virtual apps and desktops can be deployed on-premises, from Microsoft Azure, or both – simultaneously.

Workspot has re-invented application and desktop delivery with:

- VDI Pools, which enable delivery of VDI either on-premises or in the cloud.
- RD Pools, which enable delivery of applications or server-hosted desktops either on-premises or in the cloud.
- App Delivery 2.0, which enables delivery of Web Applications, SaaS applications and file shares.

There's more detail on each of these later in the document.

SINGLE PANE OF GLASS FOR IT

Workspot Client is managed and monitored using a single pane of glass – Workspot Control. Workspot Control is a 100% cloud-native, 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 also stores configuration and performance data in the cloud:

1. **Configuration data:** Workspot stores configuration information about the VPN, e.g., public URL address, whether it uses RSA or not. Workspot stores a few details about end users, e.g., First Name, Last Name, Email Address, etc.; and stores information about applications, e.g., Application URLs, whether or not the application is behind the firewall, etc.
2. **Performance data:** For each network access, Workspot stores 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:** Workspot tracks 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

CONTROL PLANE ARCHITECTURE

Workspot Control has been architected to be a control plane:

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

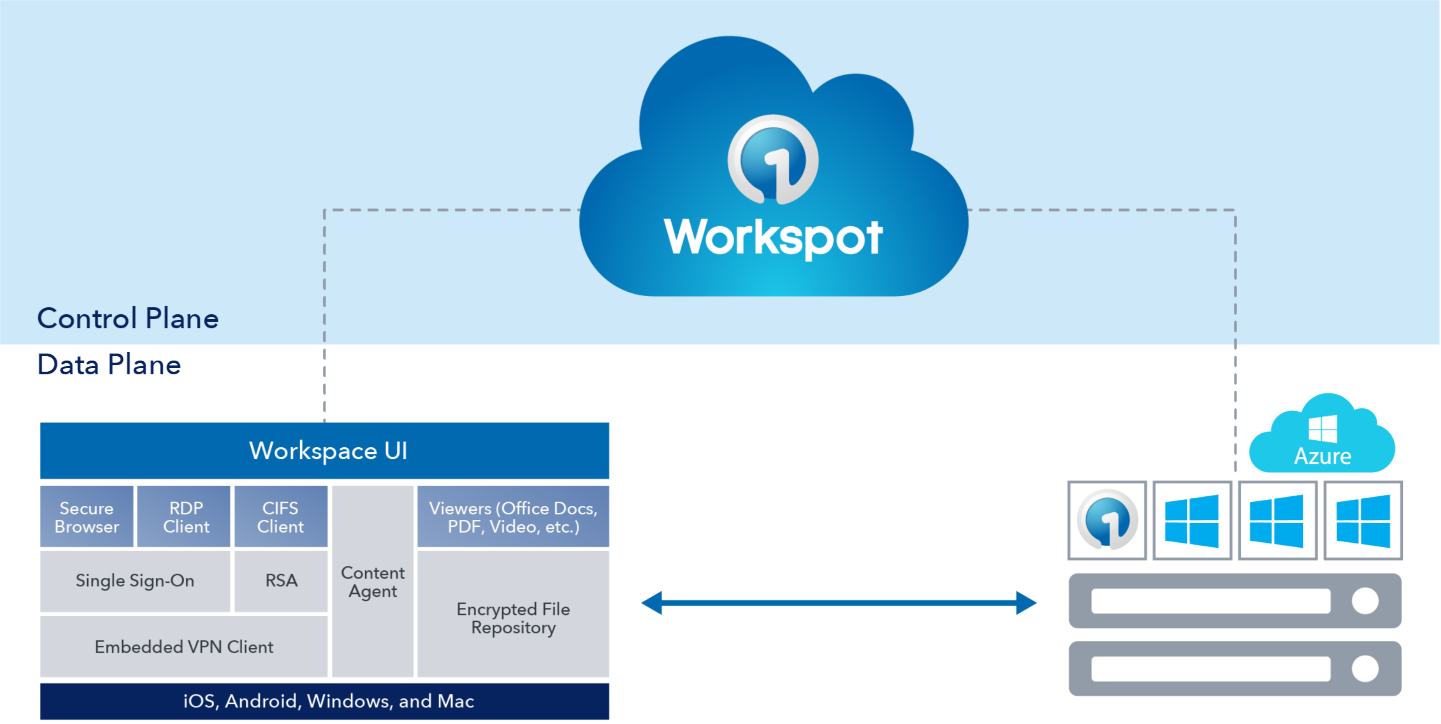


Figure 4: Workspot architecture.

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

The separation between control and data planes is critical for multiple reasons:

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

Separation of control and data planes is critical

Workspot Client: A Unified Workspace for End Users

Figure 5: Workspot Client works on any device.

Workspot Client is a workspace. It is available on any device – PC, Mac, Phone, or Tablet.

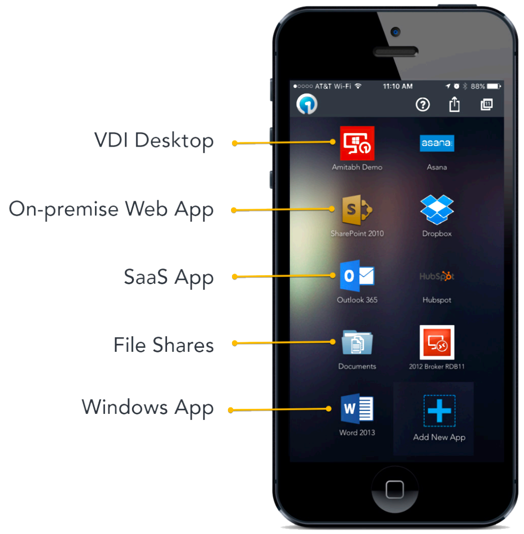


Figure 6: A single, unified client.

Workspot Client is blazing fast!

SINGLE UNIFIED CLIENT

Workspot Client provides unified access to desktops, apps, and data. Users can easily access their virtual desktops, virtual applications, proprietary web applications, SaaS applications, or network file shares through this elegant user interface. Even better, Workspot Client has the fastest connection speeds in the industry.

SECURE ACCESS

Workspot Client is a secure area for users to perform work on any device, whether the device is managed by IT, or unmanaged. The client provides the following benefits:

1. **Desktop access:** End users can access a Windows desktop, whether it's a physical desktop or a virtual desktop.
2. **Application access:** End users can seamlessly navigate between corporate applications – web, Windows, and native. IT has tools to add/delete/update applications on the device. IT also has tools to configure policies that control the behavior of applications, e.g., the ability to print from within an application.
3. **Data access:** End users can securely access documents from SharePoint and Network File Shares, and view and edit documents offline.
4. **Device security:** Workspot Client ensures that the device is safe to use; that it is not jail broken; and that there are no rogue applications on the device. IT can define policies to control the behavior of the workspace, e.g., the ability to copy-paste between applications, download documents, etc.
5. **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. Workspot enables the CISO to get a granular view of end user business activities on any mobile device, for compliance and auditing purposes.

CROSS-PLATFORM ARCHITECTURE

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 a simple and elegant end-user experience with unmatched connection speeds.

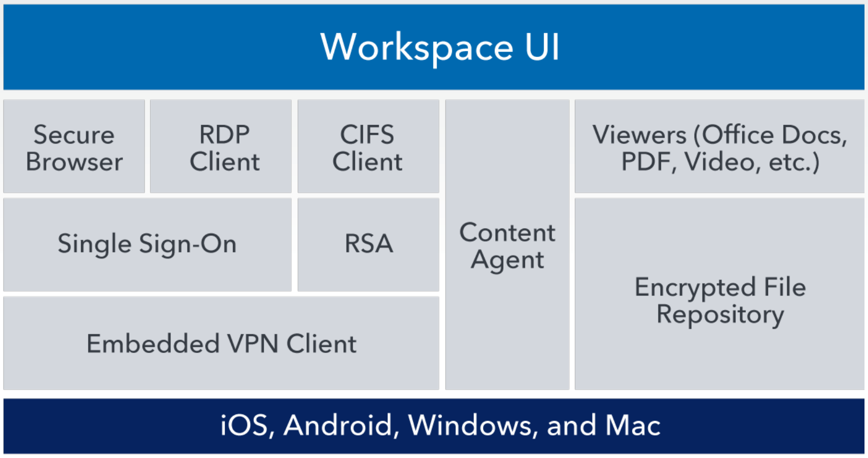


Figure 7: Workspot Client cross-platform architecture.

FIRST-TIME END USER ON-BOARDING PROCESS

To get started, the end user downloads 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, 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. 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. If the VPN box is so configured, the user is prompted for more information, like Group or RSA token. If the end user can successfully authenticate against the SSL-VPN appliance, then Workspot Client is available for use. **User credentials are never routed to, or stored on, Workspot Control.**

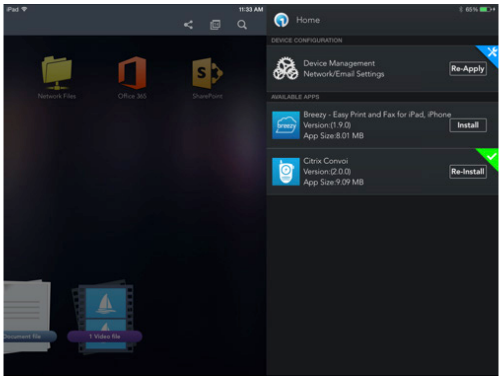
SINGLE SIGN-ON (SSO)

With Workspot, the user can take advantage of single sign-on to access 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 used for documents stored in the Encrypted File Repository ("Secure Application Access"). 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 within Workspot, as shown in Figure 8. End users can select and install applications which IT has made available to them. IT can easily provision and de-provision applications by using Workspot Control.



Device Management
Network/Email Settings

Breezy - Easy Print and Fax for iPad, iPhone
Version:(1.9.0)
App Size:8.01 MB

Citrix Convoi
Version:(2.0.0)
App Size:9.09 MB

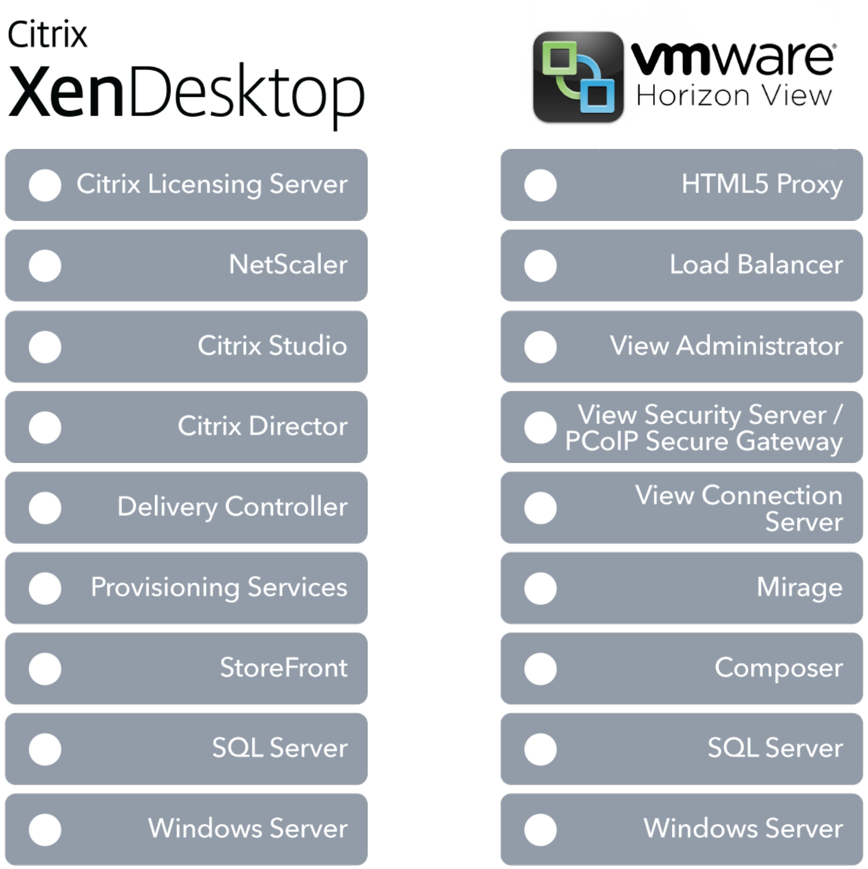
Figure 8: An Enterprise App Store.

VDI Pools

PROBLEMS WITH VDI 1.0

VDI 1.0 solutions are operationally complex. Both Citrix XenDesktop and VMware Horizon have complex stacks. Deployments can take months, if not years, and because of the complexity of these solutions, the OpEx incurred to maintain and troubleshoot them grows over time.

Workspot deploys VDI in a day



Citrix XenDesktop

- Citrix Licensing Server
- NetScaler
- Citrix Studio
- Citrix Director
- Delivery Controller
- Provisioning Services
- StoreFront
- SQL Server
- Windows Server

vmware Horizon View

- HTML5 Proxy
- Load Balancer
- View Administrator
- View Security Server / PCoIP Secure Gateway
- View Connection Server
- Mirage
- Composer
- SQL Server
- Windows Server

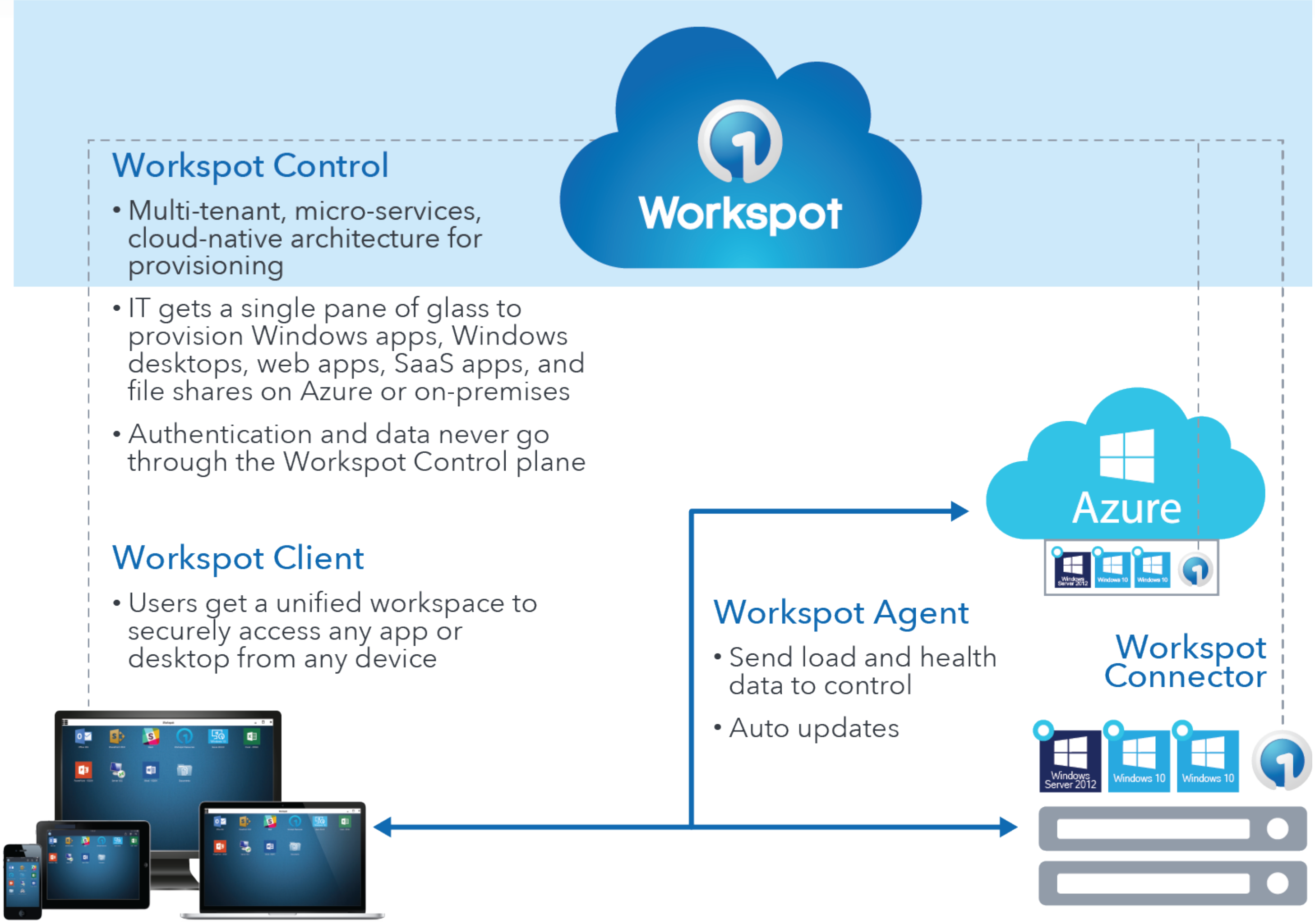
Figure 9: Typical VDI 1.0 architecture complexity.

WHAT'S DIFFERENT ABOUT VDI POOLS?

Workspot VDI Pools are based on a cloud-native architecture that makes VDI insanely simple to deploy. In addition to Workspot Control and Workspot Client, VDI Pools uses two additional components: Workspot Connector and Workspot Agent.

WORKSPOT CONNECTOR

Workspot Connector provisions virtual applications and desktops, and synchronizes Active Directory with Workspot Directory. Workspot Connector is a Windows virtual machine that is installed on the datacenter infrastructure or on Azure. Workspot Connector receives configuration information from Workspot Control, and creates a pool of virtual desktops or applications on the infrastructure.



Workspot Control

- Multi-tenant, micro-services, cloud-native architecture for provisioning
- IT gets a single pane of glass to provision Windows apps, Windows desktops, web apps, SaaS apps, and file shares on Azure or on-premises
- Authentication and data never go through the Workspot Control plane

Workspot Client

- Users get a unified workspace to securely access any app or desktop from any device

Workspot Agent

- Send load and health data to control
- Auto updates

Figure 10: Workspot Connector.

Workspot Connector is:

- **Stateless:** It receives its state from Workspot Control.
- **Highly available:** The connector can be configured in pairs to be highly available.
- **Not in critical path:** The connector is not in the critical path. If the connector is not available, IT won't be able to provision any new desktops or applications. However, users can continue to connect to existing desktops and applications.
- **Auto-updating:** The connector auto-updates itself whenever a new update is available.

WORKSPOT AGENT

The Workspot Agent is installed in a Windows Desktop template. The Agent is responsible for providing load and availability information to Workspot Control. The Workspot Agent also self-updates.

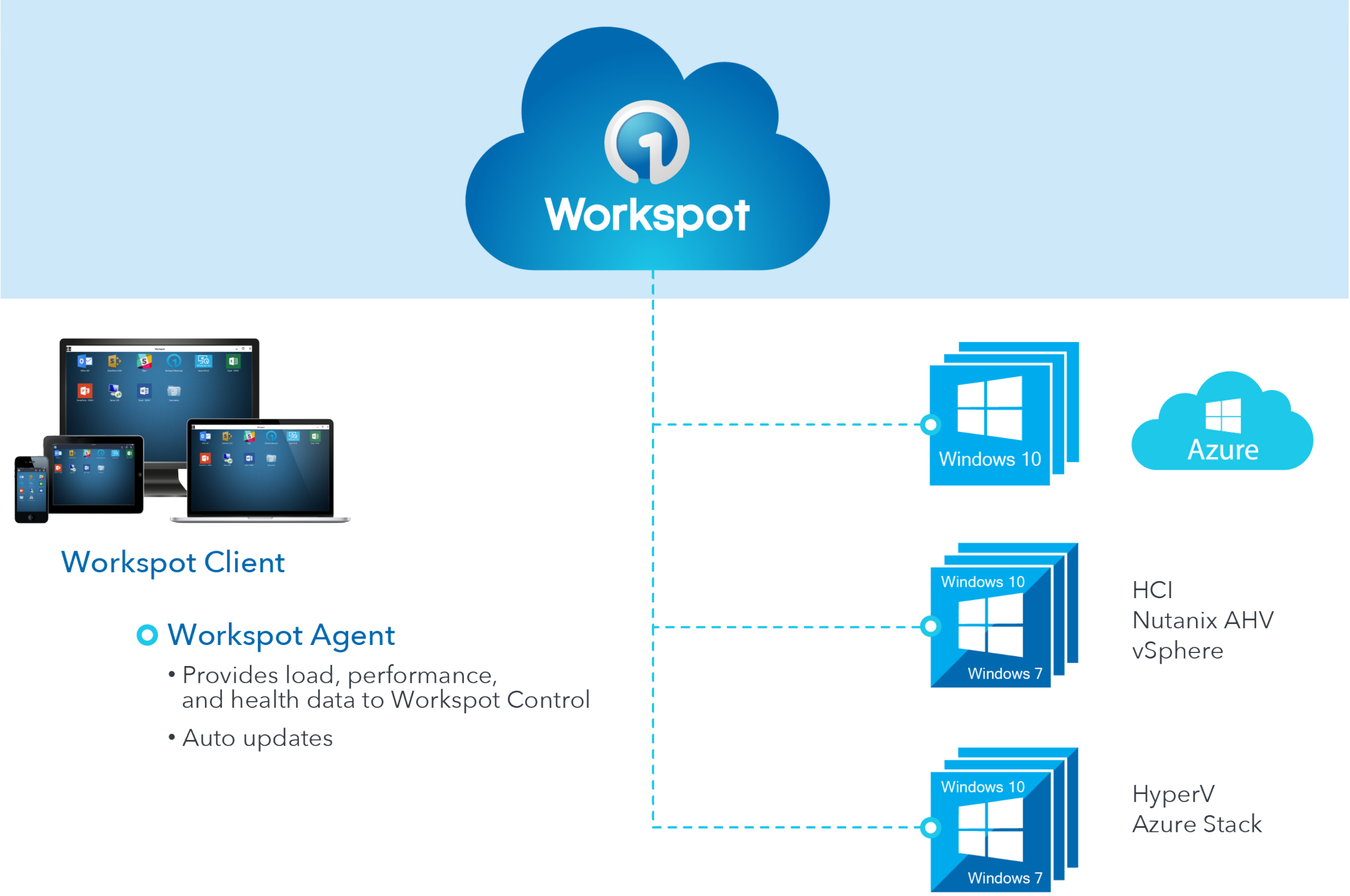


Figure 11: Workspot Agent.

CONNECTING TO A VDI DESKTOP

When a user connects to their virtual desktop or application, there are two scenarios:

- Persistent Desktop
- Non-persistent Desktop or Application

For persistent desktops, the connection information is always available on the device. For users connecting to their persistent desktops, the client connects directly to their desktop as shown in the second step in Figure 13. No communication with Workspot Control is necessary since the configuration information is already resident on the user's device.

For non-persistent desktops, the client asks Workspot Control for connection configuration. Workspot Control evaluates the load information it has from various Workspot Agents and provides the best resource for the user to connect.

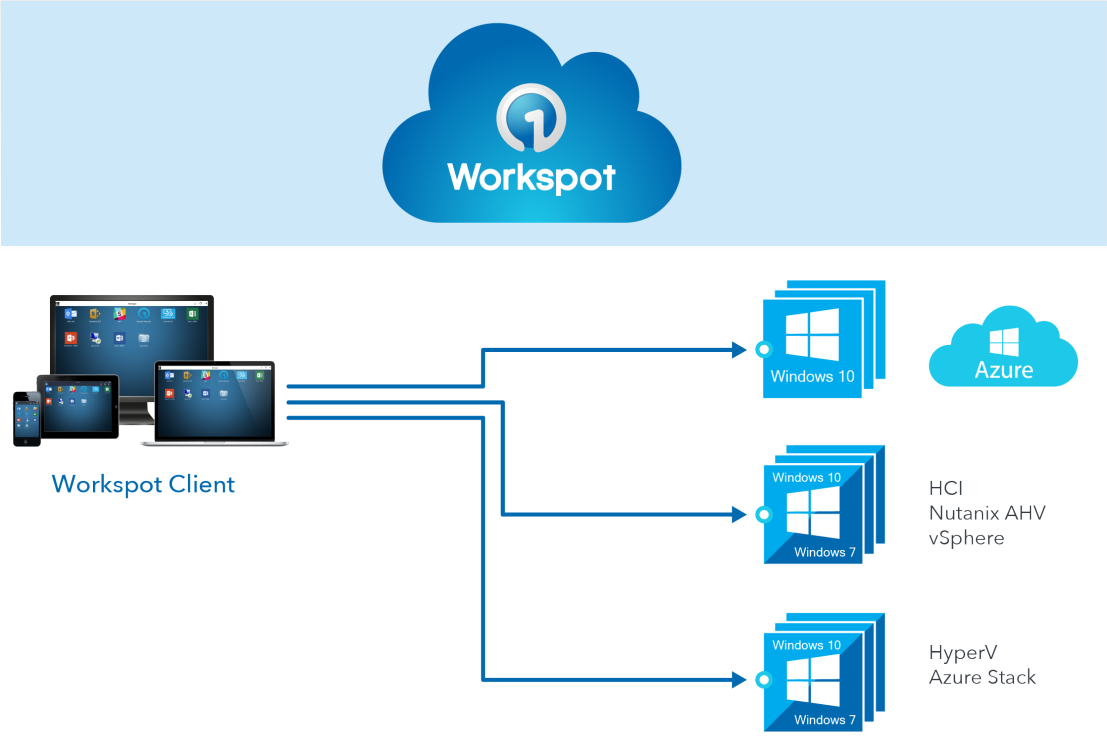


Figure 12: Connecting to a VDI desktop, Step 1.

Step 1: For non-persistent desktops, Workspot Client asks Workspot Control for the appropriate connection configuration, and then proceeds to Step 2. Users with persistent desktops bypass Step 1 and go directly to Step 2.

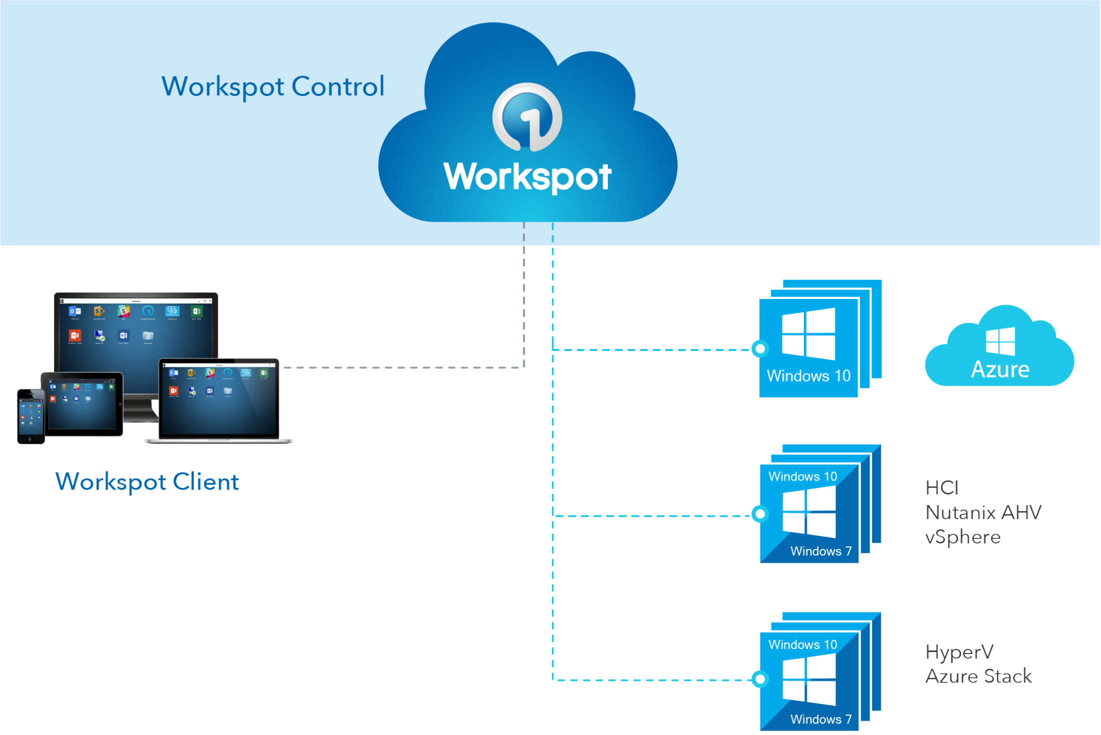


Figure 13: Connecting to a VDI desktop, Step 2.

Step 2: With persistent desktops, the client can go ahead and connect directly to the virtual desktop without asking Workspot Control for configuration information. For non-persistent desktops, once Workspot Client receives its connection configuration from Workspot Control, the user can connect to the configured apps and/or desktops.

PERSISTENT DESKTOPS FOR KNOWLEDGE WORKERS

Since modern datacenter infrastructure has many optimizations built into the architecture – such as de-duplication and high performance Flash storage – IT can choose to cost-effectively create a persistent desktop for each user. This is the same way physical PCs are assigned to users: each user gets their own PC. Similarly, each user gets their own virtual desktop. Workspot recommends that for most knowledge worker use cases, IT create a persistent desktop.

Most IT departments have already invested in PC lifecycle management tools, so they can continue to use the existing tools for persistent desktops. These tools are used to update the operating system, install and update applications, and configure printers and other peripherals. IT can also leverage those same PC lifecycle management tools to manage persistent virtual desktops. No new tools or processes are needed.

NON-PERSISTENT DESKTOPS HAVE THEIR PLACE

For some use cases, e.g., schools, kiosks and call centers, a non-persistent desktop is appropriate. For those use cases, Workspot recommends that customers create non-persistent desktops.

WORKSPOT AUTOMATES MICROSOFT AZURE DEPLOYMENTS

Workspot is tightly integrated with Azure to enable rapid creation of virtual desktops. Workspot automates:

- Azure account creation for the customer
- AD and network integration (Read-only domain controller or Azure AD Domain Services)
- Orchestration required to handle VDI and RD Pools
- Storage and networking
- Cloning/customization of VMs
- Security and public GW
- Win10 VMs and RD Pools

Workspot optimizes usage so Azure bills are predictable

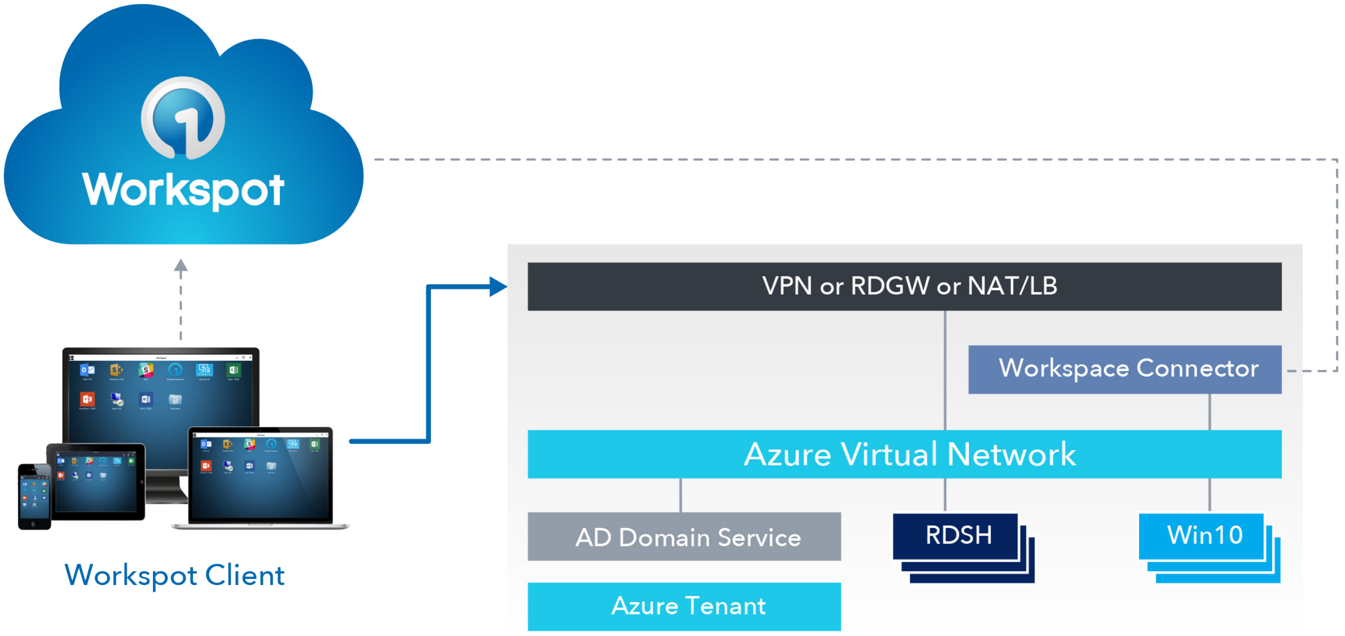


Figure 14: Workspot can rapidly spin up virtual desktops on Azure.

PREDICTABLE BILLING

One major challenge with cloud services is the lack of predictable billing. A virtual desktop running on Azure has to be available at all times, but is being used less than 1/4th of the time. Without the proper optimizations, the Azure per hour billing may end up becoming too expensive for customer deployments. Workspot optimizes power and usage management so customers can enjoy predictable billing.

MULTI-SITE DEPLOYMENTS

IT has spent the last 15 years consolidating datacenters because they were expensive to set up and manage. Today IT might be running XenApp or XenDesktop in a single datacenter in North America, which means that users in Asia Pacific suffer with high-latency connections and a poor user experience.

In response to the datacenter consolidation strategy, legacy software solutions were optimized for one datacenter. This means that in order to distribute datacenters, the entire deployment must be replicated at each datacenter.

Those days are over. Now IT can deploy a datacenter anywhere in the world at zero cost. In theory, IT can have a datacenter per user. Workspot is designed so it enables IT to set up multiple datacenters to address various use cases – some on-premises, and some in the cloud; then they can all be managed from one console – Workspot Control.

Manage on-prem and Azure datacenters from one console

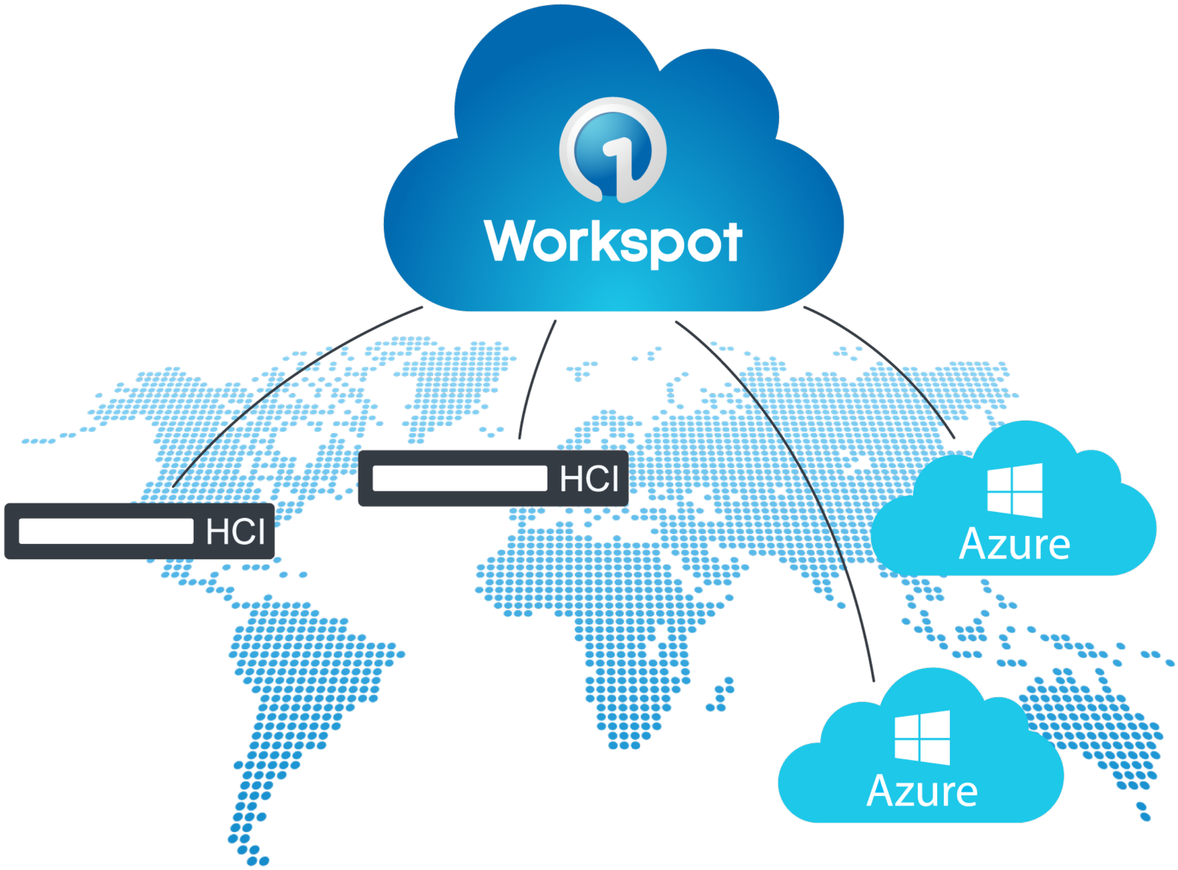


Figure 15: Manage all sites from a single pane of glass.

RD Pools

RD Pools enable the deployment of Windows client-server applications on Terminal Servers.

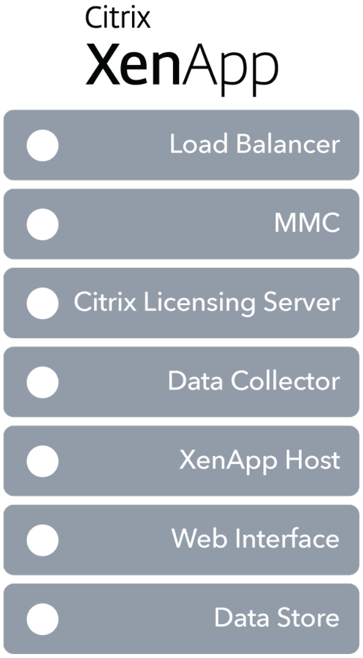


Figure 16: Citrix XenApp 6.5 stack.

PROBLEMS WITH APP VIRTUALIZATION 1.0

First generation solutions, like Citrix XenApp 6.5, are operationally complex. Deployments can take months, if not years, and are very expensive to maintain over time.

WHAT'S DIFFERENT ABOUT RD POOLS?

RD Pools use the same architecture as VDI Pools to deploy virtual applications and server-hosted desktops. They use the same Workspot Connector and Workspot Agent. For RD Pools, the Workspot Agent is installed in a Windows Server template and enables support of multiple users. RD Pools enable you to leverage Workspot's scalable cloud-native architecture to rapidly provision RDSH server virtual machines, delivering virtualized applications through shared hosted desktop sessions. The unique brokering technology within Workspot Control provides an infinitely scalable, highly available solution for application virtualization. RD Pools do not need dedicated hardware to run a controller, load balancer, broker, gateway, web-interface, or a separate SQL database to handle session creation, high availability, and failover. RD Pools provide scalability to millions of users and can be deployed in a day. This solution is vastly simpler than legacy solutions.

Simple, infinitely scalable app virtualization

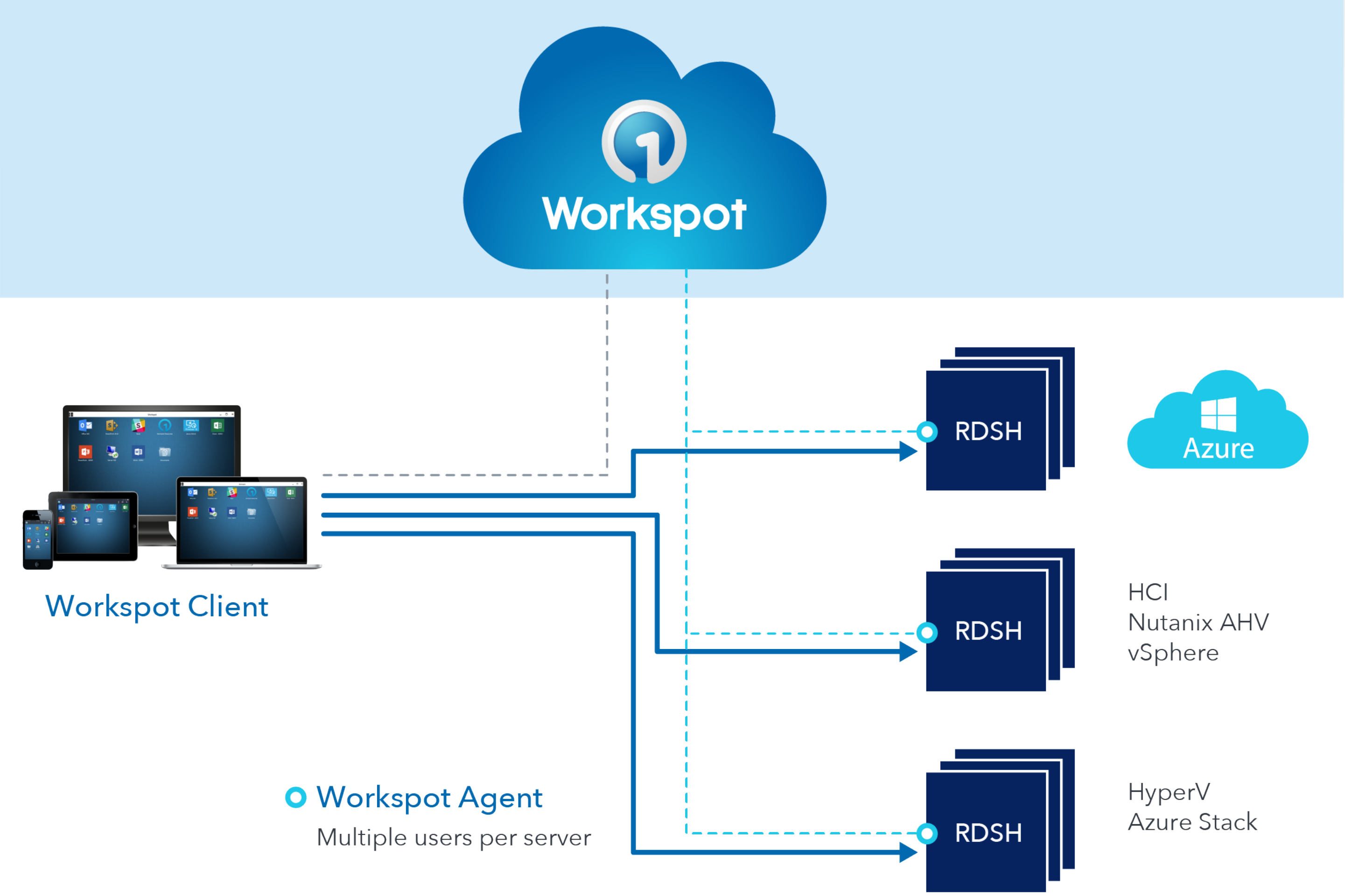


Figure 17: Simple, infinitely scalable, highly available app virtualization.

MIXED MULTI-SITE DEPLOYMENTS

From a single pane of glass, you can now deploy virtual applications and desktops on-premises, in the cloud, or both – simultaneously.

You can now locate "datacenters" close to end users, thereby reducing latency and improving the end user experience.

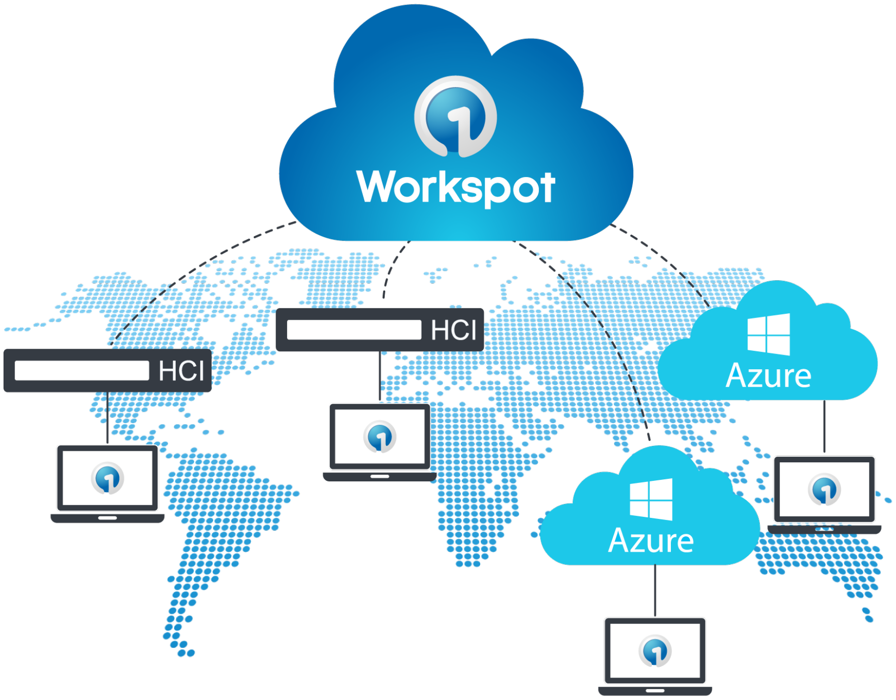


Figure 18: Locate "datacenters" close to end users.

App Delivery 2.0

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

PROBLEMS WITH APP DELIVERY 1.0

App Delivery 1.0 solutions include (a) remoting solutions like Citrix XenApp and (b) PC Lifecycle Management solutions like Symantec 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 today consume these applications from phones, tablets, and Macs, which are mostly personally owned.

WHAT'S DIFFERENT ABOUT APP DELIVERY 2.0?

App Delivery 2.0 securely delivers any type of applications (web, SaaS, Windows, hybrid and native) onto any device (PC, Mac, iOS and Android).

LEVERAGE EXISTING APPLICATION INFRASTRUCTURE

Workspot solutions have been architected from the ground up to leverage existing security and datacenter infrastructures.

Today you're probably running many on-premises business applications: web applications, Windows client-server applications and network drives (CIFS).

In the last decade, companies have deployed VPN and SSL-VPN appliances, like Cisco or Juniper, in their DMZ 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.

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. Workspot believes that the existing datacenter access infrastructure can be leveraged effectively to give employees access to corporate assets from any device. In fact, Workspot has been architected to leverage existing datacenter infrastructure – VPN, applications, and data.

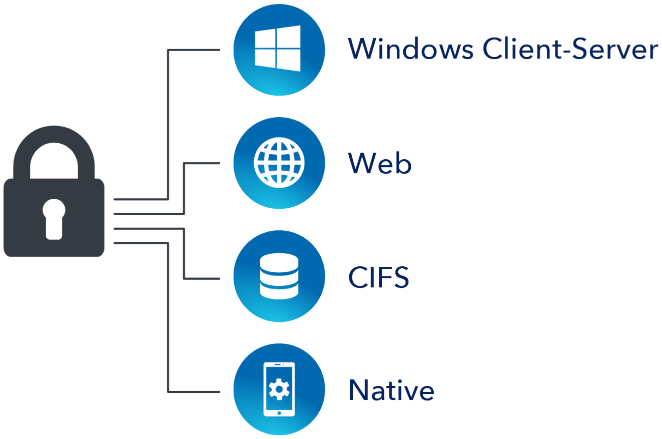
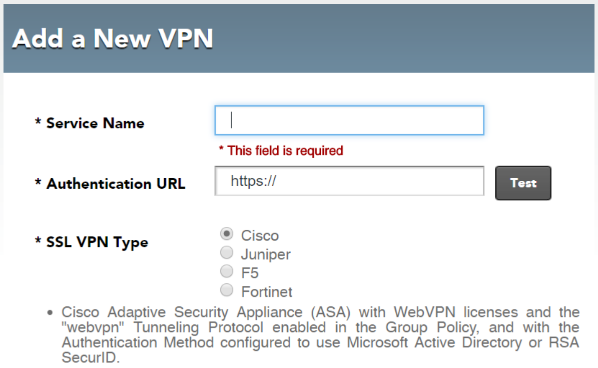


Figure 19: Workspot supports your existing security infrastructure.

CONFIGURING VPN ACCESS

You 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, you simply need to specify the public address of the VPN appliance.


Add a New VPN

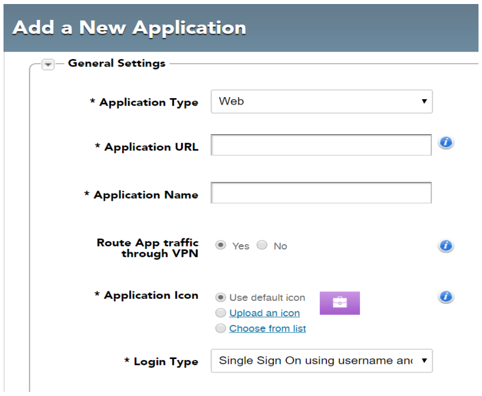
* Service Name |
* This field is required

* Authentication URL https://

* SSL VPN Type
● Cisco
○ Juniper
○ F5
○ Fortinet

- 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 20: Configuring VPN access.


Add a New Application

General Settings

* Application Type: Web ▾
* Application URL:
* Application Name:
Route App traffic through VPN: ● Yes ○ No
* Application Icon: ● Use default icon ○ Upload an icon ○ Choose from list
* Login Type: Single Sign On using username an ▾

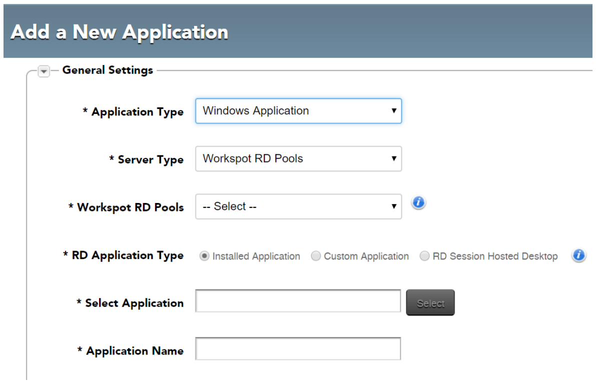
Figure 21: Configuring web-app access.

PROVISIONING ACCESS TO A WEB APP

Most organizations are already running tens, if not hundreds, of web applications, e.g., SAP, SharePoint, Siebel, and many custom applications. In order to provision access to those web applications, you just need to specify the URL of those applications in Workspot Control as shown in Figure 21. You don't need to make any changes to the operations of the applications.

PROVISIONING ACCESS TO A WINDOWS APP

Companies still run many core business applications that were written using Windows client-server technologies. You 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 datacenter. These applications will be accessed using the Remote Data Protocol (RDP). Again, you don't need to make any changes to the operations of the applications.

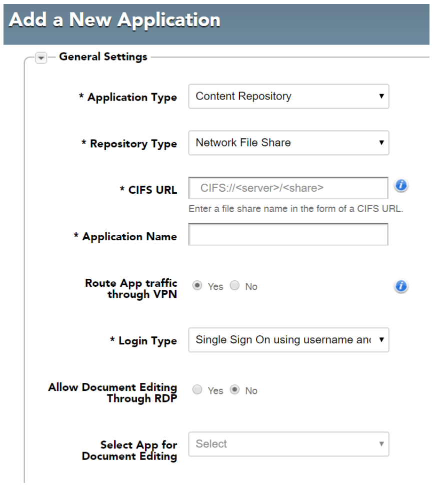

Add a New Application

General Settings

* Application Type: Windows Application ▾
* Server Type: Workspot RD Pools ▾
* Workspot RD Pools: -- Select -- ▾
* RD Application Type: ● Installed Application ○ Custom Application ○ RD Session Hosted Desktop
* Select Application:

* Application Name:

Figure 22: Windows app access configuration.


Add a New Application

General Settings

* Application Type: Content Repository ▾
* Repository Type: Network File Share ▾
* CIFS URL: CIFS://<server>/<share>
Enter a file share name in the form of a CIFS URL.
* Application Name:
Route App traffic through VPN: ● Yes ○ No
* Login Type: Single Sign On using username an ▾
Allow Document Editing Through RDP: ○ Yes ● No
Select App for Document Editing: Select ▾

Figure 23: Provision network drive 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. Workspot also support DFS. And you don't need to make any changes to the operations of the network drives.

PROVISIONING A NEW USER

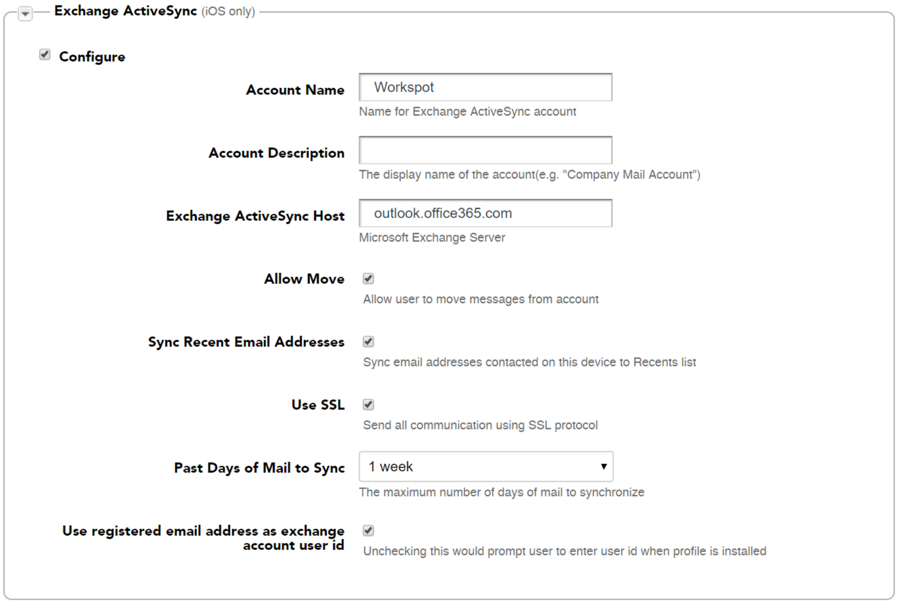
To provision a new user in Workspot Control, the administrator needs the First Name, Last Name, and Email address of the user. They assign the user to a group, which is mapped to a set of applications, a network configuration, and various security policies. If you're using the Workspot self-registration process, you don't need to add the user to Workspot Control.

ASSIGNING APPS TO USERS

There are multiple ways to assign applications to users: (a) assign a set of apps to users; (b) create bundles of apps and assign to groups; (c) assign a bundle of apps to users; (d) assign individual apps to groups.

NATIVE EMAIL CONFIGURATION

You 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 (iOS only)

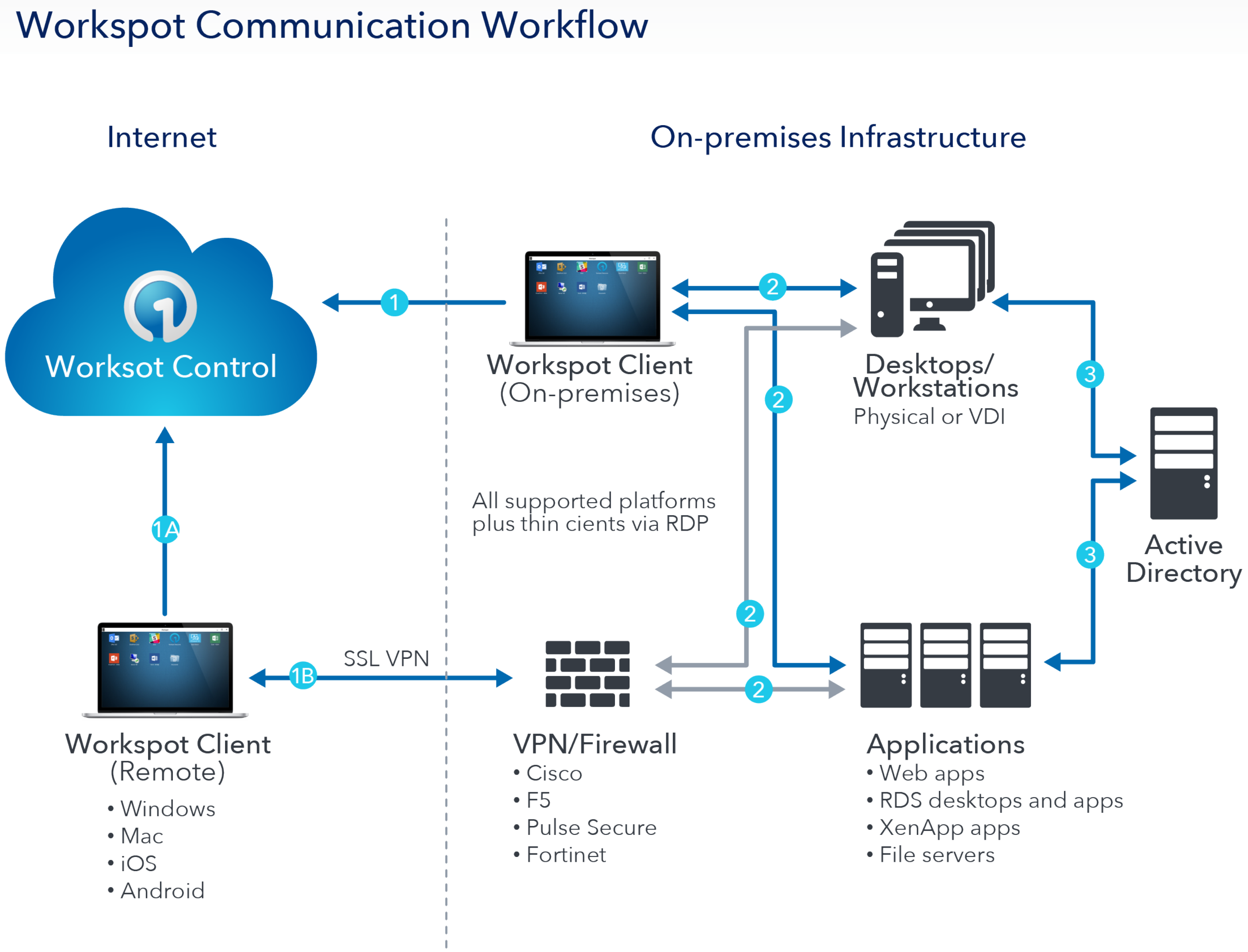
☑ **Configure**

Account Name	Workspot Name for Exchange ActiveSync account
Account Description	The display name of the account(e.g. "Company Mail Account")
Exchange ActiveSync Host	outlook.office365.com 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 24: Provision the native email client on iOS.

CONNECTION WORKFLOW

Figure 26 describes the steps that occur when a user connects either from inside or outside the firewall.



1A Workspot client is launched and checks with Workspot Control (HTTPS/443) for:
* New entitlement (new app or VDI desktop access)
* New security policies
* Performs posture checks

1B User clicks on a resource such as VDI desktop or app to start session. Workspot client is aware it is outside of the internal network and authenticates with VPN to establish a SSL VPN (443) session.

2 User clicks on a resource such as VDI desktop or app to start session. Workspot client establishes RDP/RemoteFx connection to VDI/RDS apps (3389), HTTP/HTTPS (80/443) communicate to web apps or CIFS (137, 138, 139, 445) connection to network file shares.

Or

Leveraging VPN authentication and ACLs, establishes RDP/RemoteFx connection to VDI/RDS apps (3389), HTTP/HTTPS (80/443) communicate to web apps or CIFS (137, 138, 139, 445) connection to network file shares.

3 Resource (VDI desktop or apps) authenticates with Active Directory/Domain Controller.

Figure 26: Workspot communication flow.

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 the 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 5 incorrect entries, the data inside Workspot Client will be wiped from the device, thereby keeping organization assets secure.

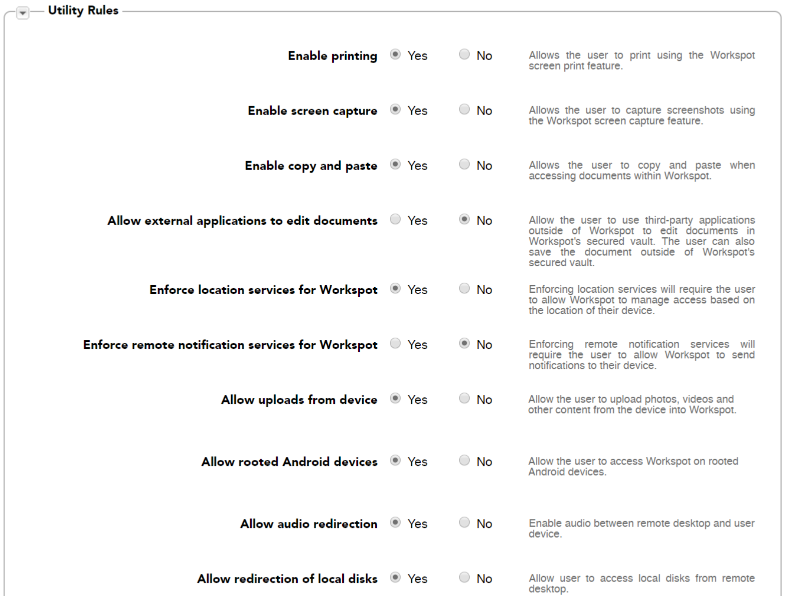
DEVICE POSTURE CHECK

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

CONFIGURING SECURITY POLICIES

Other aspects of Workspot Client behavior can be configured using Workspot Control, including:

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



Utility Rules

Enable printing	● Yes	○ No	Allows the user to print using the Workspot screen print feature.
Enable screen capture	● Yes	○ No	Allows the user to capture screenshots using the Workspot screen capture feature.
Enable copy and paste	● Yes	○ No	Allows the user to copy and paste when accessing documents within Workspot.
Allow external applications to edit documents	○ Yes	● No	Allow the user to use third-party applications outside of Workspot to edit documents in Workspot's secured vault. The user can also save the document outside of Workspot's secured vault.
Enforce location services for Workspot	● Yes	○ No	Enforcing location services will require the user to allow Workspot to manage access based on the location of their device.
Enforce remote notification services for Workspot	○ Yes	● No	Enforcing remote notification services will require the user to allow Workspot to send notifications to their device.
Allow uploads from device	● Yes	○ No	Allow the user to upload photos, videos and other content from the device into Workspot.
Allow rooted Android devices	● Yes	○ No	Allow the user to access Workspot on rooted Android devices.
Allow audio redirection	● Yes	○ No	Enable audio between remote desktop and user device.
Allow redirection of local disks	● Yes	○ No	Allow user to access local disks from remote desktop.

Figure 27: Configuring security policies.

REMOTE WIPE

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

DATA RETENTION

Workspot's current policy is to retain configuration and activity data in Workspot Control for a period of one year. It is important to note that no application traffic flows through Workspot Control, and no user credentials are 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. Workspot is using a FIPS compliant SSL library in the embedded VPN Client.

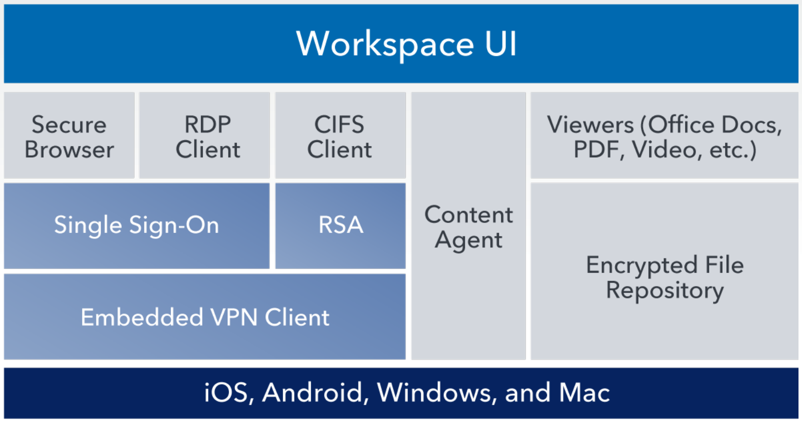


Figure 28: Security for data in motion.

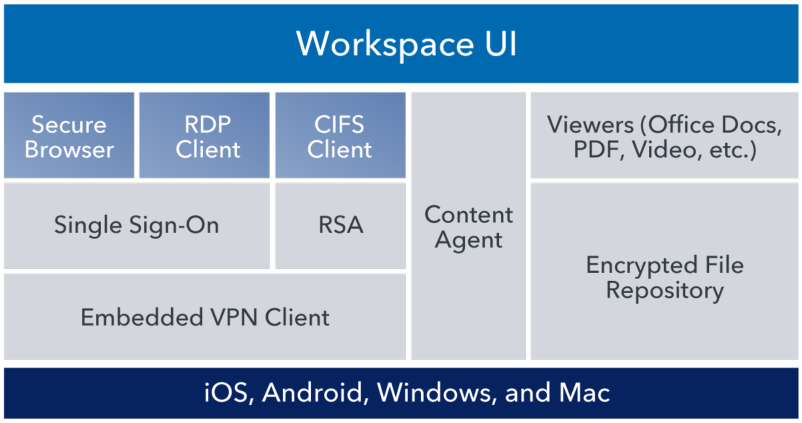


Figure 29: Secure application access.

SECURE APPLICATION ACCESS

Workspot Client enables secure access to different classes of applications running in the datacenter:

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 a Windows desktop.
3. **Network Drives**: There is a CIFS client integrated into Workspot. This enables an end user to access a network drive in the datacenter.

WHITELIST/BLACKLIST TRAFFIC

You can also control which sites the user can and cannot visit from inside the Workspot Client by configuring a blacklist/whitelist. Workspot also enables 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.

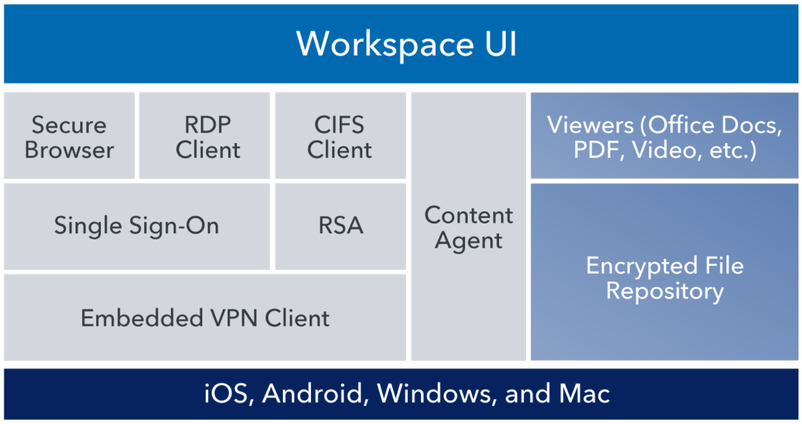


Figure 30: Security for data at rest.

SECURE DOCUMENT VIEWERS

When an end user downloads a document inside Workspot Client, 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 Client. Workspot has tuned the embedded viewers for the best possible rendering experience.

Documents are more secure, because the documents stay within Workspot Client. And 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, Workspot only decrypts the pages of the document that are currently being viewed.

BIG DATA CONTEXT-DRIVEN SECURITY

When a user accesses enterprise assets, Workspot 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 such as Facebook – on the device. This data can be used for compliance, auditing, and adaptive authentication.

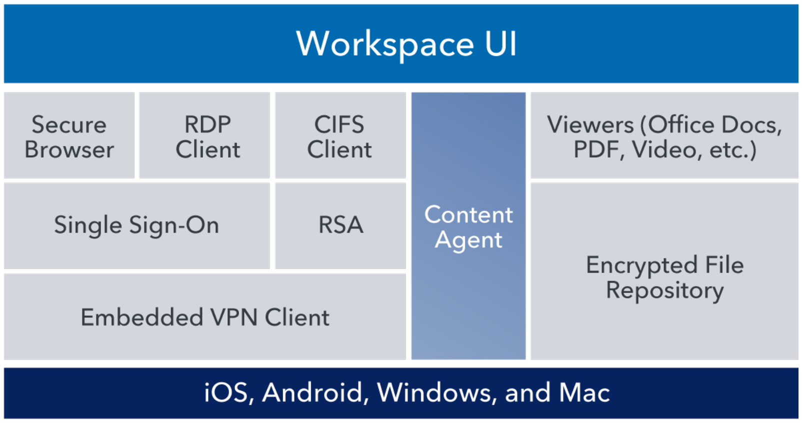


Figure 31: Context-driven security.

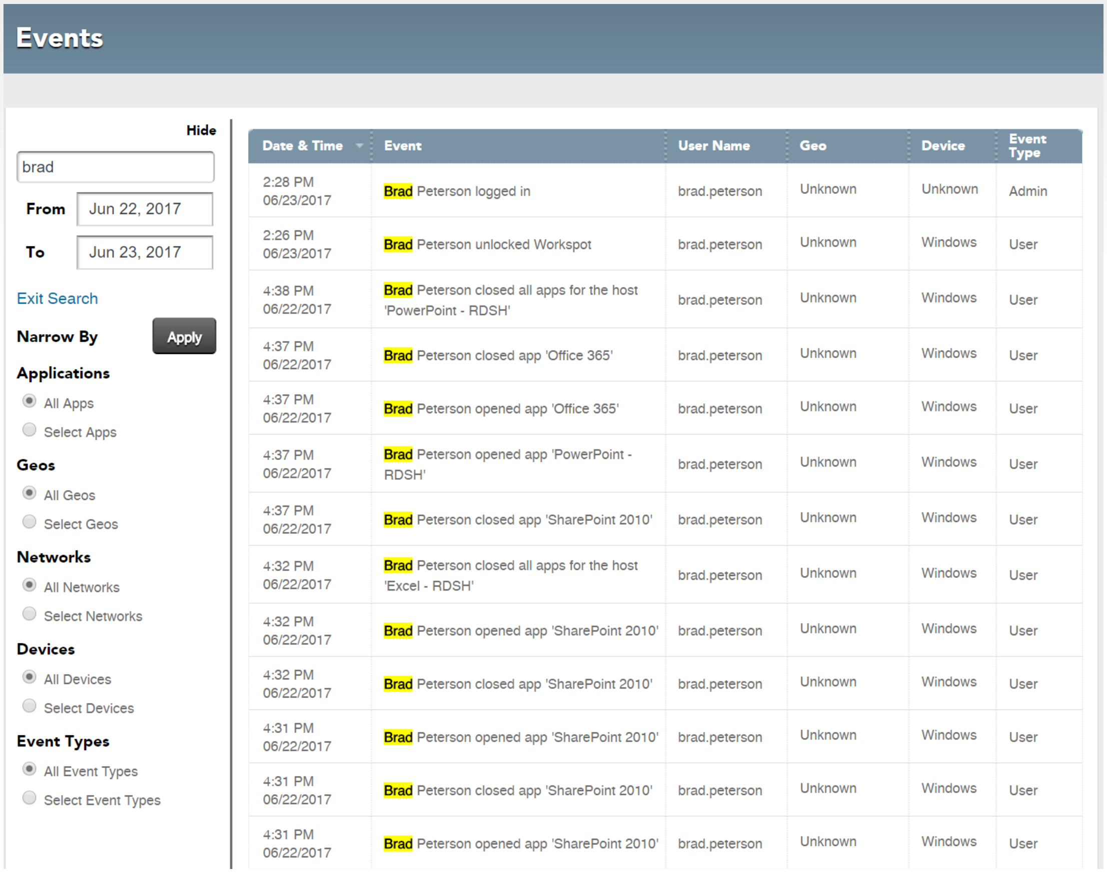
COMPLIANCE AND AUDITING

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; a log entry in SAP indicates that the user logged into SAP, and that an email generated by SAP indicates a purchase order was placed.

Workspot goes way beyond SIEM systems that infer user actions. Workspot collects 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

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



Events

Hide

brad

From Jun 22, 2017

To Jun 23, 2017

Exit Search

Narrow By [Apply]

Applications

● All Apps

○ Select Apps

Geos

● All Geos

○ Select Geos

Networks

● All Networks

○ Select Networks

Devices

● All Devices

○ Select Devices

Event Types

● All Event Types

○ Select Event Types

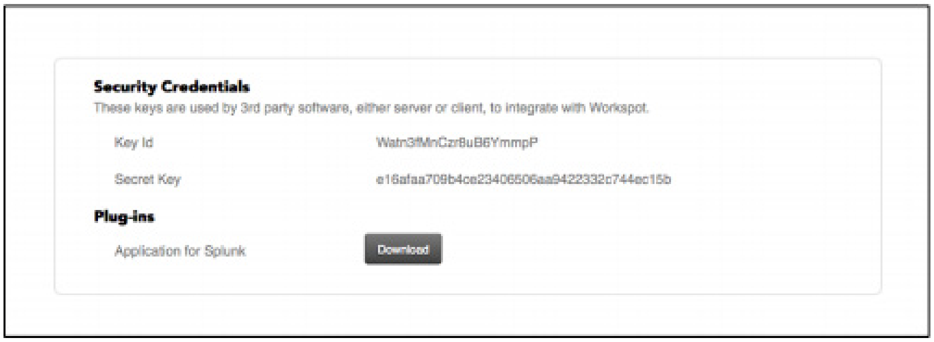
Date & Time	Event	User Name	Geo	Device	Event Type
2:28 PM 06/23/2017	Brad Peterson logged in	brad.peterson	Unknown	Unknown	Admin
2:26 PM 06/23/2017	Brad Peterson unlocked Workspot	brad.peterson	Unknown	Windows	User
4:38 PM 06/22/2017	Brad Peterson closed all apps for the host 'PowerPoint - RDSH'	brad.peterson	Unknown	Windows	User
4:37 PM 06/22/2017	Brad Peterson closed app 'Office 365'	brad.peterson	Unknown	Windows	User
4:37 PM 06/22/2017	Brad Peterson opened app 'Office 365'	brad.peterson	Unknown	Windows	User
4:37 PM 06/22/2017	Brad Peterson opened app 'PowerPoint - RDSH'	brad.peterson	Unknown	Windows	User
4:37 PM 06/22/2017	Brad Peterson closed app 'SharePoint 2010'	brad.peterson	Unknown	Windows	User
4:32 PM 06/22/2017	Brad Peterson closed all apps for the host 'Excel - RDSH'	brad.peterson	Unknown	Windows	User
4:32 PM 06/22/2017	Brad Peterson opened app 'SharePoint 2010'	brad.peterson	Unknown	Windows	User
4:32 PM 06/22/2017	Brad Peterson closed app 'SharePoint 2010'	brad.peterson	Unknown	Windows	User
4:31 PM 06/22/2017	Brad Peterson opened app 'SharePoint 2010'	brad.peterson	Unknown	Windows	User
4:31 PM 06/22/2017	Brad Peterson closed app 'SharePoint 2010'	brad.peterson	Unknown	Windows	User
4:31 PM 06/22/2017	Brad Peterson opened app 'SharePoint 2010'	brad.peterson	Unknown	Windows	User

Figure 32: End user activity data.

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 Figure 33.

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 Figure 34.



Security Credentials

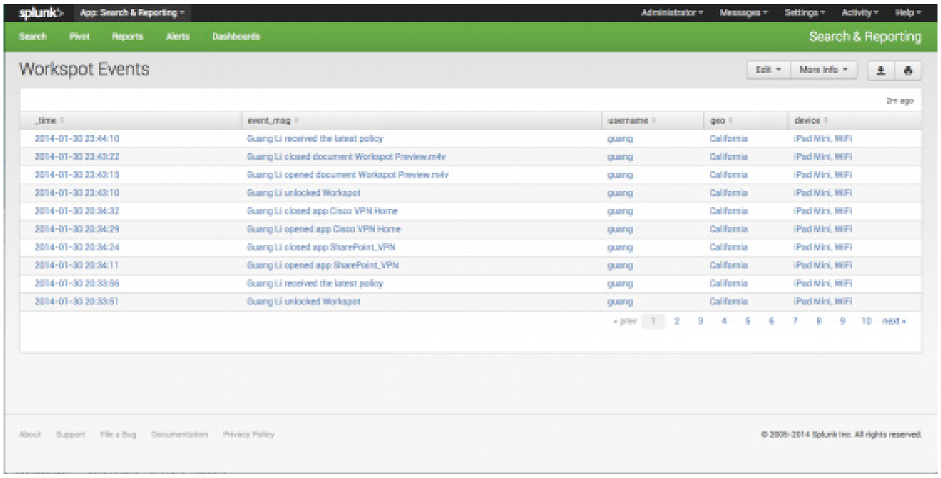
These keys are used by 3rd party software, either server or client, to integrate with Workspot.

Key Id	Watn3fMnCzr8uB6YmmpP
Secret Key	e16afaa709b4ce23406506aa9422332c744ec15b

Plug-ins

Application for Splunk [Download]

Figure 33: Splunk configuration keys.



Workspot Events

2m ago

_time	event_msg	username	geo	device
2014-01-30 23:44:10	Guang Li received the latest policy	guang	California	iPad Mini, WiFi
2014-01-30 23:43:22	Guang Li closed document Workspot Preview.m4v	guang	California	iPad Mini, WiFi
2014-01-30 23:43:15	Guang Li opened document Workspot Preview.m4v	guang	California	iPad Mini, WiFi
2014-01-30 23:43:10	Guang Li unlocked Workspot	guang	California	iPad Mini, WiFi
2014-01-30 20:34:32	Guang Li closed app Cisco VPN Home	guang	California	iPad Mini, WiFi
2014-01-30 20:34:29	Guang Li opened app Cisco VPN Home	guang	California	iPad Mini, WiFi
2014-01-30 20:34:24	Guang Li closed app SharePoint_VPN	guang	California	iPad Mini, WiFi
2014-01-30 20:34:11	Guang Li opened app SharePoint_VPN	guang	California	iPad Mini, WiFi
2014-01-30 20:33:56	Guang Li received the latest policy	guang	California	iPad Mini, WiFi
2014-01-30 20:33:51	Guang Li unlocked Workspot	guang	California	iPad Mini, WiFi

« prev 1 2 3 4 5 6 7 8 9 10 next »

About Support File a Bug Documentation Privacy Policy

© 2005-2014 Splunk Inc. All rights reserved.

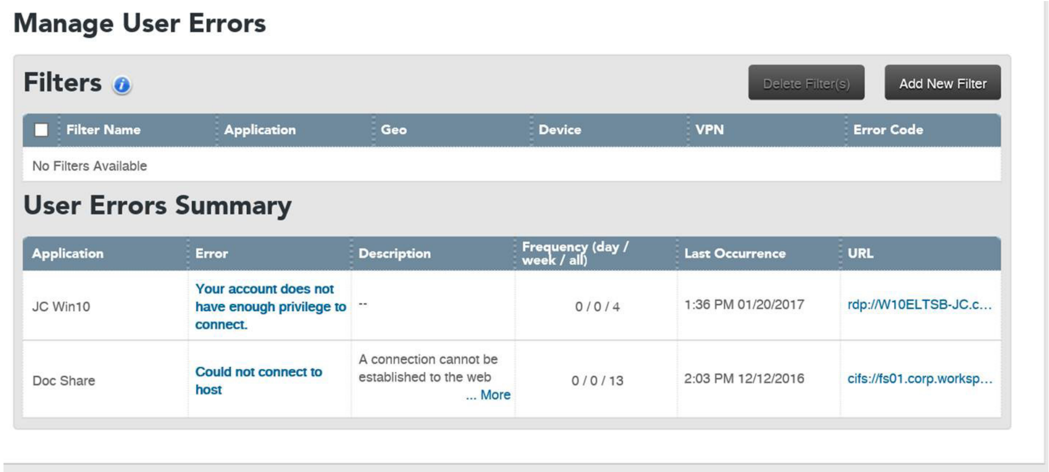
Figure 34: Workspot event data in Splunk.

Context-Driven Visibility

In addition to collecting end user actions, Workspot Client also collects the real-time user experience – how long did an access take, and 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 unsuccessful action inside Workspot Client, it is recorded. Workspot then aggregates and classifies the errors across all the users in an organization. IT has an aggregated view of all the problems in the organization – which application, what error, how frequently, and when did it last occur.



Manage User Errors

Filters

□ Filter Name	Application	Geo	Device	VPN	Error Code
No Filters Available					

User Errors Summary

Application	Error	Description	Frequency (day / week / all)	Last Occurrence	URL
JC Win10	Your account does not have enough privilege to connect.	--	0 / 0 / 4	1:36 PM 01/20/2017	rdp://W10ELTSB-JC.c...
Doc Share	Could not connect to host	A connection cannot be established to the web ... More	0 / 0 / 13	2:03 PM 12/12/2016	cifs://fs01.corp.worksp...

Figure 35: User Errors Summary.

Workspot provides rich data for performance analysis

REAL END USER EXPERIENCE (REUX)

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

Every time a user performs an action inside Workspot Client, Workspot records the user, application, location, device used, network name, performance, availability usage metrics etc., and makes that data available for analysis. For example:

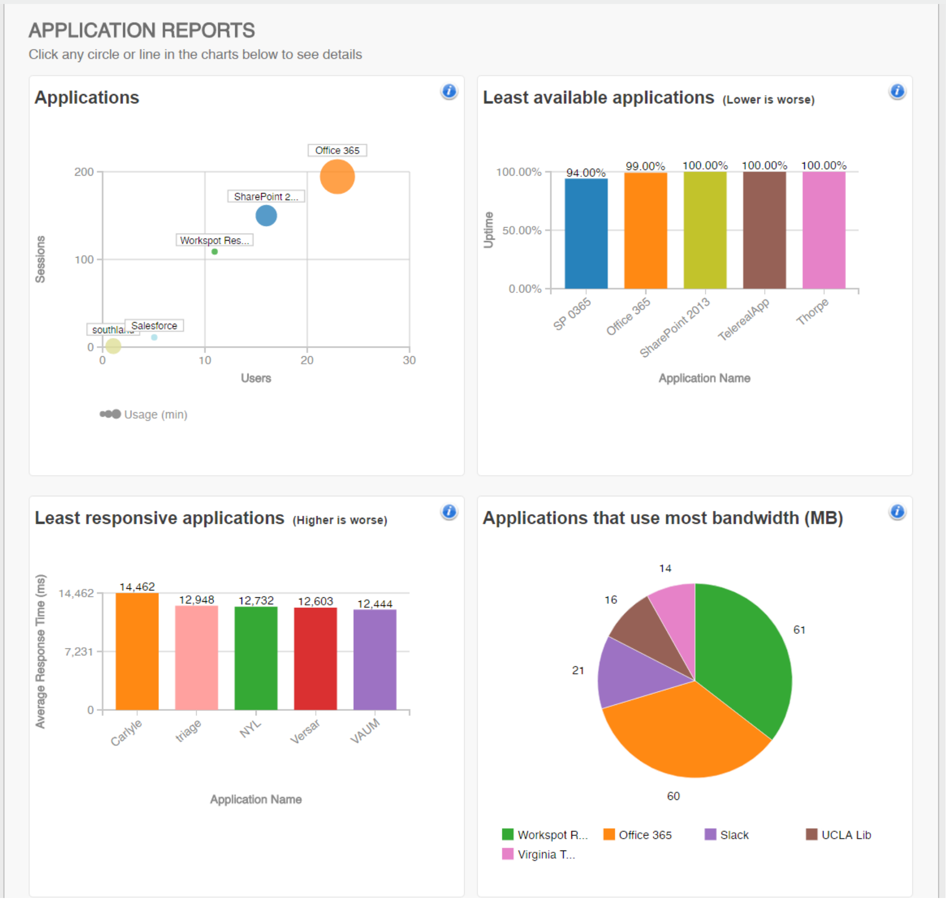
- **Performance** – Average response time of an application by application name, network type (WiFi or carrier), and location.
- **Uptime** – If a user is unable to access an application, attribute the source of the error to application, network, or geo based on a time series analysis.
- **Usage** – Data about usage by application, geo, or network (WiFi or carrier).

Upon analysis, this type of data can yield actionable information:

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

APPLICATIONS

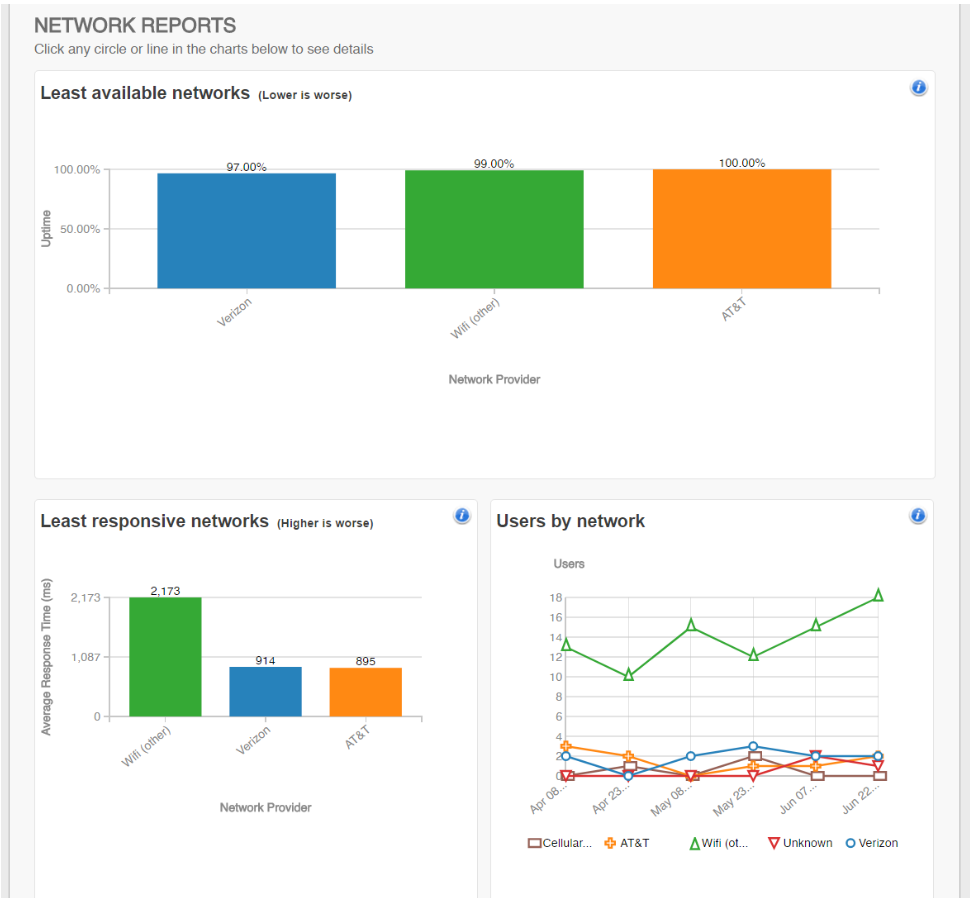
The Application Reports section enables IT to analyze which apps are used, availability of the applications, the slowest applications, the bandwidth consumed by the application, and other metrics.



APPLICATION REPORTS

Click any circle or line in the charts below to see details

Figure 36: Sample applications report.



NETWORK REPORTS

Click any circle or line in the charts below to see details

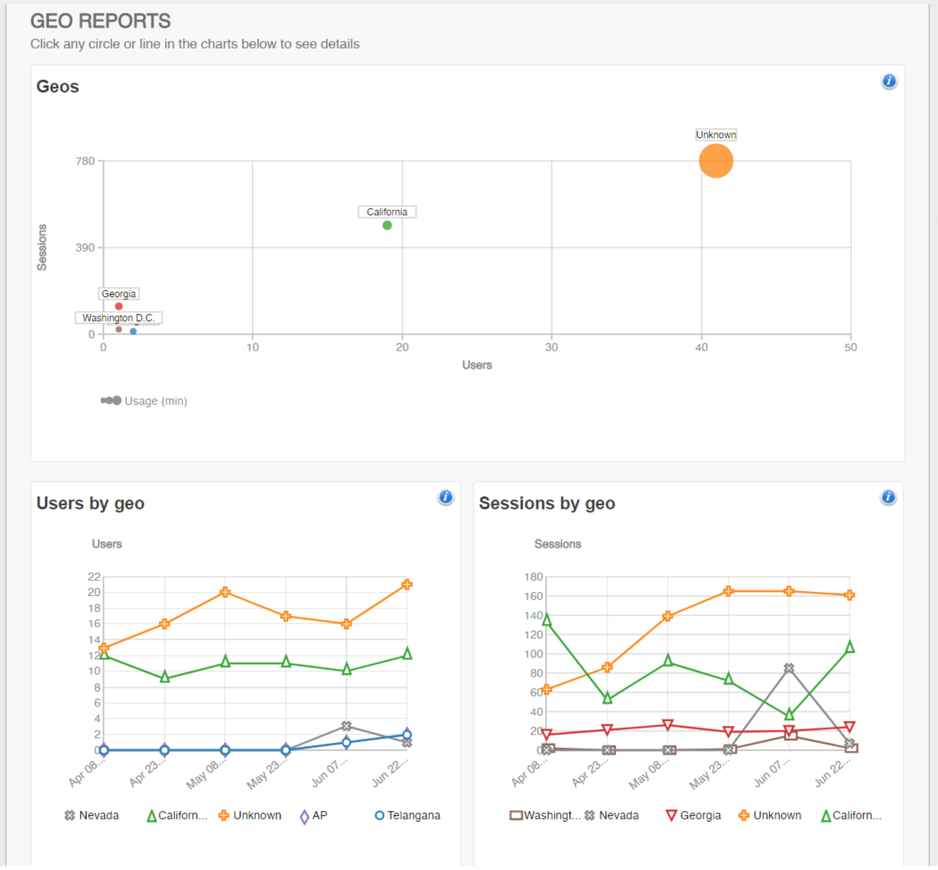
Figure 37: Sample networks report.

NETWORKS

The Network Reports 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.

GEOS

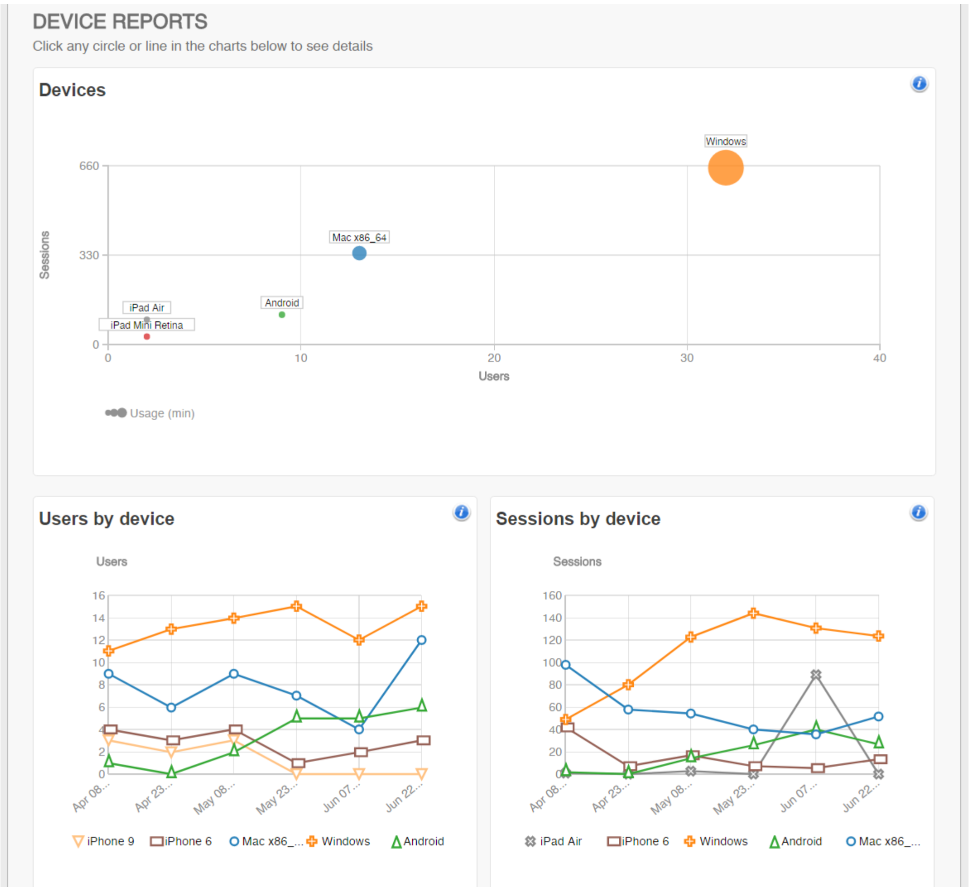
The Geo Reports section enables IT to analyze how users are accessing applications from various geos.



GEO REPORTS

Click any circle or line in the charts below to see details

Figure 38: Sample geographic distribution report.



DEVICE REPORTS

Click any circle or line in the charts below to see details

DEVICES

The Device Reports 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 39: Sample device report.

Summary

Existing solutions to deliver virtual desktops and applications are either complex on-premises solutions, or incomplete cloud solutions. Workspot provides a unified platform to deliver virtual apps, desktops, and workstations to any device, from on-premises, from Microsoft Azure, or both – simultaneously. You'll have a single pane of glass to provision apps, desktops, workstations, and data; manage on-premises and cloud desktops; and monitor security, availability, usage, and performance. End users get an elegant workspace that allows for easy access to any application or desktop, with the fastest connection speeds in the industry, on any device they choose to use.

Compare solutions below and then contact us for a 15-minute demo to learn more about deploying insanely simple Workspot VDI in a day.

Capability	Workspot	VDI 1.0		DaaS 1.0	
		XenDesktop	Horizon	Horizon Cloud	Amazon
Enterprise Class Deployment in a Day	●			●	●
Predictable Subscription Billing	●			●	●
Support for Mobile – iOS/Android	●	●	●	●	●
Support for Desktop – Windows/Mac	●	●	●	●	●
Deliver Server Hosted Desktops	●	●	●	●	●
Deliver VDI to Any Device	●	●	●		
Deliver Web Apps to Any Device	●				
Deliver Windows Client Server Apps to Any Device	●	●	●		
Deployment Choices – On-Premises or Cloud	●	●	●		
Integration w/ Existing Systems	●	●	●		
Offline Document Access	●				
Consistent Experience Across Locations	●	●			
Simpler Access with Single Sign-On	●	●	●	●	●
Visibility into Performance, Availability, and Usage	●				
Granular visibility into end user activity	●				

ADDITIONAL RESOURCES

Video: Workspot Technical Architecture

Schedule a Demo: Just 15 minutes!

ABOUT WORKSPOT

Workspot has reinvented Virtual Desktop Infrastructure (VDI) with a cloud-native architecture that delivers applications, desktops and workstations from the cloud. Workspot's "cloud-first" solution solves the corporate challenge of securely delivering apps, desktops and data from anywhere, to any device, and dramatically reduces the total cost of ownership for virtual apps, desktops and workstations. Organizations of all sizes benefit from the shortest implementation times in the industry, achieving unprecedented time-to-value. With a relentless focus on customer success, Workspot's no-risk customer engagement model is an industry first. The Cupertino, California-based company received the Best of VMworld 2016 Gold Award for Desktop and Application Delivery solutions. For more information on Workspot's risk-free, turnkey solutions, visit: www.workspot.com