Enterprise Strategy Group | **Getting to the bigger truth.™**

White Paper

RFP Considerations: Workspace Solutions

Achieving Digital Workspace Transformation and Securely Delivering a High Quality End-user Experience

By Mark Bowker, ESG Senior Analyst, and Leah Matuson, Research Analyst

December 2016

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

Contents

Introduction

Purpose of This Guide

This guide is designed to help create a request for proposal (RFP) in support of workspace solutions. Although writing RFPs can be an intimidating task, it becomes easier when goals and requirements are clearly defined and organized to align with business and technology solutions. Understanding the short- and long-term goals, in addition to the unique requirements of your organization, will help you create an RFP that serves as a valuable tool for use in your decision-making process. The RFP Vendor Selection Matrix provided helps summarize the important criteria and rate potential vendors on their ability to deliver key capabilities.

What are workspace solutions?

The goal of business mobility is to create workspaces that improve IT control, enhance the employee experience, and mitigate security risks. When employees have the ability to access their applications anytime, anywhere, and on any device, employee satisfaction improves, hence, the workforce becomes more productive. However, the broad range of devices administrators must support on and off the corporate network makes it difficult to control which users and which devices have access to valuable corporate data and apps; therefore, workspace solutions require strong enterprise mobility management and identity components to ensure only the right users and devices have access. It is also important to highlight the fact that business mobility extends beyond traditional remote access to email and a few SaaS applications to include hybrid consumption models, user-based policy management, and secure access.

Once you have established your initial high-level goals, the next question is: *How can you best achieve these goals and map technology to these initiatives?*

Workspace transformation regarding virtual desktops, applications, data, and mobile experiences offers employees the access they require, though choosing among a wide range of solutions can be a long and time-consuming endeavor. This is owing to the fact that desktop and application experience rests on multiple factors, including:

- Product quality.
- Product flexibility.
- Feature completeness.
- Support quality.
- Future product innovation.

A workspace solution that delivers on just a few of these factors will fall short, likely disappointing you and your employees, and potentially making it more difficult to obtain approvals for future projects. On the other hand, a workspace solution that continues to innovate and deliver on every factor will not only be gratifying to both the business and employees, but will also open up new possibilities.

Digital Workspace RFP Requirements

Device and Application Support

Does the workspace solution support laptops and mobile devices with the same range of applications?

An optimal solution will be a secure enterprise platform that delivers and manages any application on any smartphone, tablet, or laptop. The solution should enable consumer-grade, self-service, single sign-on (SSO) access to cloud and mobile and Windows applications, and include integrated email, calendar, file, and social collaboration tools that engage employees.

Which devices does the workspace solution support?

It is important that the solution provides day-zero support on mobile, as well as desktop, operating systems, including iOS, Android, Mac OS, Chrome OS, Windows OS, and others. *Note*: Capabilities may vary by platform. At a minimum, any device with an HTML5-compliant browser should be able to access an application store for web applications and hosted Windows applications. Additionally, native applications may be installed on Windows 10, Apple iOS, and Android devices while still being managed by the platform.

Authentication and Identity Management

Does the workspace solution support single sign-on across SaaS, mobile, and legacy applications?

It is important to have a workspace solution that supports single sign-on for hosted applications, packaged applications, web applications, and SaaS applications. The goal is to avoid having to remember and enter multiple usernames, and be able to assign single-use passwords and authenticate with consumer-based identities. The solution should:

- Enable access to applications to be turned off at a single point to protect against data leakage in the event of employee separation.
- Establish trust between the user, device, application, and enterprise using certificate-based login.
- Authenticate cloud and on-premises applications across any platform with built-in, two-factor authentication (2FA) or integration with third-party MFA that uses push notifications on iOS or Android devices.
- Federate on-premises Active Directory (AD), LDAP, and open LDAP structures.
- Leverage device trust and PIN/biometric timeout settings for the most secure applications and data.
- Work with your existing infrastructure with support included for third-party authentication services such as RADIUS, Symantec, RSA SecurID, Imprivata Touch and Go, and others.

Does the solution require a username and password, or can it use native platform biometrics?

An ideal solution will:

- Allow users to bypass secondary login requests after initially authenticating, as well as leverage additional PIN/biometric timeout settings for authentication.
- Remove the need for complex logins by establishing trust between user, device, and the enterprise for one-touch authentication. This can include enabling one-touch SSO to corporate applications and resources with a security assertion markup language (SAML) identity provider, or token generator.
- Require additional authentication through a passcode/biometrics at the device or application level for more sensitive applications. This feature should:
    - Require a passcode with configurable complexity and length through compliance policies.

  - Leverage seamless biometric or other multi-factor authentication methods using TouchID for iOS applications.
  - Include additional authentication through third-party biometrics APIs, tap-and-go systems, or adaptive authentication partners.

Does your solution require a third-party identity management solution?

If so, look for solutions that integrate easily with existing identity providers like Ping, Okta, or CA Single Sign-On (SiteMinder), while maintaining a common application catalog for users.

Does the solution require a multi-factor authentication (MFA) provider?

To streamline MFA deployment, look for a solution that has a built-in MFA provider. Integrated MFA providers are often easiest for end-users to use and for administrators to deploy.

The solution should also allow for easy integration with third-party MFA providers. Administrators can use third-party MFA providers to provide additional security through third-party biometrics APIs, tap-and-go systems, or adaptive authentication partners, as well as multi-factor authentication through Remote Authentication Dial-in User Service (RADIUS), RSA Secure ID, RSA Adaptive Authentication, and certificate -based authentication.

Third-party MFA solutions can be integrated using RADIUS or SAML.

Does the workspace solution support managed and unmanaged devices in a single instance?

A true bring-your-own-anything (BYOA) solution gives employees flexibility and device choice, while securing corporate data. Most enterprises support a range of devices, from corporate-issued devices (owned by the enterprise and fully managed by IT) through managed personal devices (owned by employees, but with some management by IT) to unmanaged devices used to access work resources (owned by employees, completely unmanaged by IT). Many end-users are uncomfortable with device management and prefer to access email and other resources from unmanaged personal devices. Therefore, the solution should:

- Allow corporations to differentiate between unmanaged and managed devices, and define the levels of access to corporate information.
- Enable a bring-your-own-device (BYOD) or BYOA program with adaptive enrollment, and separate personal data and corporate data in employee-owned devices.

How can you drive end-user adoption of BYOD use cases for the workspace solution?

Look for vendors that have a BYOD adoption campaign kit to assist administrators in growing employee engagement. To help with driving adoption of the solution, the campaign kit should contain templates, best practices, schedules, and ideas for immediately starting to promote the platform and drive adoption by employees. The kit should also encompass planning and execution in the following five areas: planning, communication, education, promotion, and support.

Can users access corporate resources without enrolling a personal device in enterprise mobility management (EMM)?

Employees should not have to enroll their personal devices in order to access services. Ideally, a standard application may be downloaded from the Apple App Store, Google Play, or Microsoft Store, where an employee may then log in and gain access to applications based on the policies set for those applications.

Does the solution offer conditional prompt for increased management policy based on user activity and security threat, and deliver those policies based on user acceptance?

Adaptive management technology is designed to remove the limitations of standalone mobile application management (MAM) and identity-as-a-service (IDaaS) to protect data inside applications without requiring device management in order to accelerate support for BYOD initiatives. This technology should:

- Use adaptive enrollment to configure the level of access and corresponding management for required and requested applications.
- Guide the end-user through device enrollment when the user tries to access resources requiring enrollment.
- Integrate identity-based, conditional access management with real-time application delivery and enterprise mobility management to deploy a tailored application management strategy to user devices.
- Eliminate the need for complex logins by establishing trust between user, device, and the enterprise for one-touch authentication.

How does the solution help your company manage authentication to applications?

The solution should remove the need for complex logins by establishing trust between user, device, and the enterprise for one-touch authentication. The solution should also:

- Include an enterprise-grade Identity Provider for SAML, OpenID Connect, and Web Service Federation (WS-Fed) -supported applications, and daisy chain to any third-party identity providers already in use.
- Step up seamless biometric or other multi-factor authentication methods for more sensitive applications.
- Deploy built-in multi-factor authentication.

Does the solution offer conditional access (network, identity, device security, etc.)?

Aim for a solution that provides conditional access policy enforcement, combining identity and mobility management. The solution should be able to set different conditional access policies for different apps. There are two types of conditional access:

- The first type of conditional access is based on policies set in the identity provider. The identity provider can limit access based on user, user group, strength of authentication method, or network scope.
- The second type of conditional access checks whether a user’s device complies with requirements set in the workspace solution. Prior to completing authentication, the solution should ensure that the device is compliant with corporate policy by checking whether the device is enrolled in management, whether it is jailbroken or rooted, whether it has blacklisted apps, or whether it has other forbidden device attributes.

Also consider enabling a step-up authentication and policy for access to certain applications from an untrusted network. In this case, you can apply increased security controls (2FA, for example) on a per-app basis.

Does the workspace solution offer integration with third-party enterprise resources?

The solution should securely integrate with existing enterprise resources to preserve your investment, including integration with AD/LDAP, certificate authorities, email infrastructures, and other enterprise systems to centralize mobility management and streamline user enablement.

With which directory services providers does the solution integrate?

Look for solutions that support:

- Microsoft Active Directory.
- Generic LDAP.
- Oracle Identity Manager.
- Microsoft Azure Active Directory.
- Novell eDirectory.
- User databases.
- Federation via SAML and Web Services Federation (WS-Fed).
- User generation via API.

The solution should sync with existing Active Directory services to automatically provision and de-provision access to resources based on initiated updates to permissions. Users should be automatically updated throughout the solution, and associated downstream solutions, upon Active Directory sync.

Is the request process automated, or does it require IT involvement?

The self-enrollment request process should be automated, and no IT involvement should be required. To enroll, an automated prompt should be sent to the user and the company's information privacy policy should be displayed in order for the user to know which information is being collected.

Application Access and Management

What productivity applications does the solution include?

Look for a solution that includes email, calendar, contacts, documents, chat, and enterprise social applications that employees want to use. Additionally, look for invisible security measures to protect the organization from data leakage by restricting how attachments and files can be edited and shared. It's also important to look for encrypted apps that are compliant with FIPS 140-2 and capable of delivering enterprise-grade security and a consumer-grade user experience. Large organizations require flexibility to manage data regionally in on-premises or pure cloud configurations based upon local requirements.

Does the workspace solution offer scalable automation?

The solution should limit the amount of extra work for administrators as more users enroll devices. The complexity of managing increasing numbers of devices should be mitigated via automation, such as remote configuration (profiles), smart groups, virtual applications, desktop delivery, etc.

Can the solution deliver any application, including the latest mobile cloud applications and legacy enterprise applications?

Ideally, the solution will be able to deliver any application—from the latest mobile cloud applications to legacy enterprise applications—and include the following capabilities:

- Entitle apps to users and groups.
- Rapidly deliver apps to all end-users.
- Show apps in the catalog to the right users.
- Launch apps with one touch when a user clicks.
- Provide SSO into apps.
- Provision user accounts
- Manage licensing
- De-provision user if necessary.
- Provide non-federated apps with password vaulting.

Look for a solution that offers an enterprise application catalog in order to deliver the right applications to any device including:

- Internal web applications through a secured browser and seamless VPN tunnel.
- SaaS applications with SAML-based SSO and a provisioning framework.
- Native public mobile applications through brokerage of public application stores such as Google Play and the Apple App Store.
- Modern Windows applications through the Windows Business Store.
- Legacy Windows applications through Microsoft Windows Installer (MSI) package delivery.
- Secure sensitive systems of record apps behind a HTML5 proxy by hosting in the data center or cloud provider.
- Virtualized managed desktops in the cloud, or in on-premises data centers.
- Citrix XenApp published applications.

Does the solution offer a self-service application catalog, and is it accessible from both mobile and desktop devices?

Look for a workspace solution that offers a self-service application catalog in order to deliver the right applications to any smartphone, tablet, or laptop. Mobile users should be able to access the platform through a native application. The application may be downloaded from the Apple App Store, Google Play, or Microsoft Store, where an employee can then log in and gain access to policy-controlled applications.

The solution should also include self-service features and robust customization/branding options.

How does the solution restrict users to view only applications they are entitled to see? Can end-users request application access?

Administrators should be able to define those applications to which users have access, either by allowing access for individual users or groups of users. Users may also request access to specific applications. Employees should be able to leverage the solution to access secured applications to which they are entitled on any device by integrating identity, application, and enterprise mobility management. The solution should be able to:

- Deliver self-service access to cloud, mobile, Windows, and internal web applications through a secured browser and seamless VPN tunnel.
- Provide a SAML-based SSO and provisioning framework for SaaS applications.

What type of customization options does the customer application store offer (administration, metrics, etc.) for the workspace solution?

The platform access on Windows, iOS, or Android should provide employees with a complete, self-service enterprise application catalog that can be easily customized and branded for your company.

Does the workspace solution include application virtualization capabilities?

The solution should provide secure, hosted, virtual applications that allow users to work on highly sensitive and confidential information without compromising corporate data. The solution should also:

- Provide a complete virtual workspace from the cloud, delivering desktops and hosted applications as an easily managed, integrated cloud service.
- Enable access to virtual applications and desktops for optimized flexibility, regardless of location or device type.

Data Protection and Security

How does the workspace solution secure corporate data access from mobile devices?

To protect the most sensitive information, the platform should combine identity and device management to enforce access decisions based on a range of conditions, including strength of authentication, network, location, and device compliance. The solution should include:

- **Compliance check**: Conditional access policy enforcement for mobile, web, and Windows applications on a per-application basis should be configured through an identity manager to enforce authentication strength and restrict access by network scope, or through any device restriction imposed by MDM (rooted devices, application blacklist, geolocation, and others).
- **IT automated workflows:** This provides for compliance, remediation, and operational efficiency.
- **Device management and compliance**: Automated device compliance for advanced data leakage protection including protection against rooted or jailbroken devices, whitelist and blacklist applications, open-in app restrictions, cut/copy/paste restrictions, geofencing, network configuration, and a range of advanced restrictions and policies enforced through the MDM policy engine is a necessity.

- **Per-app VPN:** A secure tunnel should further segregate traffic from applications to specific workloads in the data center. This substantially reduces attack vectors of malware/viruses that could do significant harm to the organization.

- **Intelligent de-provisioning**: The ability to detect changes in the posture of a device and deny access based on the policy engine.

Does the workspace solution provide data loss prevention (DLP) on mobile devices, laptops, and desktops?

Look for a solution that combines native device DLP functionality with additional application-based containerization options to help secure corporate application data on mobile devices, laptops, and desktops. Solution features should include:

- **Native DLP**: Configure and manage iOS sandboxing.

- **Secure productivity applications**: Control data and file sharing for email, documents, and chat.

- **Other application containerization**: Manage DLP settings for applications that are compliant with AppConfig[1] (such as Box, Concur, DocuSign, Salesforce1, Workday, and others) and configure additional DLP settings for applications with app wrapping or an SDK.

- **Email attachment management**: Add further security for email and attachments through the use of a secure email gateway, which can enforce enterprise encryption, wipe, and “open-in” controls, keeping attachments secure.

Additional Selection Criteria

Public Reference Accounts

What are your three largest public customer references for EMM and digital workspace deployments?

The virtual desktops and applications need to be highly scalable. Verify the vendor has a history of supporting large deployments.

What are some examples of successful companies that use your company’s products?

Ensure the vendor has products and services necessary to support the organization. Make sure the vendor has a consistently good track record of supporting well-known companies, and that a number of those companies would be available to serve as vendor references.

Total Cost of Ownership

Does the solution provide lower total cost of ownership than competitors’ solutions? Where are the savings?

Due to discounting and hidden costs, it can be tricky to determine exactly what a solution costs. Validate how much the solution will cost, as well as how much value the business will receive from it.

[1] See: http://www.appconfig.org/

RFP Vendor Selection Matrix

Capability		Vendor A	Vendor B	Vendor C	Vendor D
Device and Application Support					
	Same range of apps across devices				
	Android				
	Chrome OS				
	iOS				
	Mac OS				
	Windows				
	Over the air configuration				
	OS/App lifecycle management				
	Asset analytics, tracking, and inventory				
Authentication and Identity Management					
	Single Sign-on				
	Username and password				
	Native platform biometrics				
	Integrate with third-party IDaaS				
	MFA				
	Managed and unmanaged in single instance				
	Adoption campaign kit				
	Enrollment requirement				
	Conditional access				
	Integrated with third-party enterprise resources				
	Integrated with third-party directory services				
	Automated request process				
Application Access and Management					
	Workpace productivity apps				
	Deliver any application				
	Self-service app catalog				
	Restrict users to view only entitled apps				
	Customizable customer app store				
	App virtualization				
Data Protection and Security					
	Compliance check				
	IT automated workflows				
	Device management and compliance				
	Intelligent network				
	Native DLP				
	Secure productivity apps				
	App containerization				
	Email attachment management				
Additional Criteria					
	Hosted services				
	Public enterprise references				
	TCO savings				

The Bigger Truth

Established Evaluation Criteria for Assessing Proposals

The selection criteria discussed in this guide are key considerations for the RFP process, and will help you establish a combination of both near-term goals and long-term workspace transformation strategies. Use these key considerations to:

- Initiate internal discussion and create goals.
- Establish initial research and evaluation criteria.
- Form the basis for a cost-benefit analysis.
- Develop meeting agendas with IT vendors.
- Input data into an RFP template.

Without a doubt, the decision process can become complex, involving multiple IT and business decision makers, and comprising significant influence from employees (based on their locations, device types, and behaviors).

Leverage the topics and questions presented in this guide when speaking with your vendor to address current challenges as well as when dealing with unforeseen modifications to your strategy. While making your selection, remember that a neutral, agnostic vendor that will work across the entire ecosystem makes the best long-term partner for helping you achieve digital workspace transformation.

Ultimately, this guide will help ensure your decision process is inclusive of an investment that will match your strategy today, while also helping you adapt and scale your plans when necessary—helping build stronger RFPs, setting agendas with IT vendors, and invigorating internal discussion.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

www.esg-global.com contact@esg-global.com P. 508.482.0188