Cloud versus On-Premise Service Management: Which Makes Sense for Your Organization?

Solution Overview: IT Service Management

Overview

If you're looking for a service management solution for tracking, managing, and resolving support incidents while complying with IT governance and risk management requirements, you may be considering a cloud-based solution. After all, cloud applications are hot and tend to top every IT buyer's list. And, in some cases, cloud applications are a great selection.

However, when it comes to an integrated service management solution, on-premise might be a better choice depending upon what you need the application to do and your business goals. This solution brief will help you evaluate if a cloud or an on-premise service management solution is a good fit for your organization.

Budget Considerations for Service Management Solutions

A cloud-based service management solution has distinct benefits for certain organizations. For instance, it might be beneficial to charge a cloud-based service management solution to your operational expense (OpEx) budget rather than incur capital expenses (CapEx) for purchasing on-premise software and equipment. Since there's no hardware to buy or maintain with a cloud solution, CapEx is reduced while OpEx increases to pay for ongoing cloud application subscription fees. With no additional hardware to buy, you might also assume you'll need fewer, less experienced IT staff to manage a cloud solution.

However, perception is often different than reality. If you look a bit closer, you'll find the ongoing subscription costs for cloud-based service management solutions may exceed what you'll pay for an on-premise application's hardware. Cloud solutions often aren't truly maintenance free as your IT staff will likely still need to perform some ongoing maintenance. And IT labor costs often aren't reduced, because managing cloud-based applications requires the same expertise and skill set as on-premise applications.

When Does Cloud-Based Service Management Make Sense?

There are situations when it clearly makes sense to use a cloud-based service management solution as it can potentially save you time and money. Based on your organization's technical requirements, here are situations when the cloud is a good choice:

- You won't be synchronizing CMDB data between a cloud-based service management solution and on-premise IT management tools. If you need a relatively simple service management application that won't be sharing data with on-premise IT solutions, such as those that manage your client devices, assets, and servers, then the cloud can be a good choice. If you do have on-premise management tools, you'll be required to maintain multiple Configuration Management Databases (CMDBs) – one in the cloud and one on-premise – so synchronizing data between them means bandwidth issues and time lags in replicating information.

- Your service management application won't require much customization or configuration (such as to support government or compliance regulations). The cloud is a good choice if your business needs won't require customizing a service management application. Some cloud-based service management solutions don't support customization, or if they do, your changes may be lost the next time the cloud vendor upgrades its application.

For instance, if your company isn't subject to legal restrictions such as HIPAA requirements or privacy laws prohibiting personal information from crossing country borders, then a cloud application will suffice. Or, from a technical standpoint, if you won't be

executing client-side scripts, or tasks for deploying applications, running patch updates or other remediation scripts, then the cloud is also a good choice.

- You won't be linking to an external data source like an ERP system. A cloud-based service management solution can be a good fit if you don't need it to link it to another data source, such as Microsoft® Active Directory®, an ERP application, or a Human Resources system.

- You don't need to control when application updates are made. One of the benefits of using a cloud-based service management application is the cloud vendor takes care of much of the maintenance including maintaining and updating the application.

However, these updates might occur at a time that isn't convenient for your company and could cause unanticipated downtime. For instance, most retailers have change freeze windows during the busy selling season of November-December, and cannot incur the risk of a change during this time. With a cloud application, however; it's tough to control these types of changes since they're under the vendor's control.

- Sharing server space with other companies (like competitors) isn't a concern. Cloud applications are typically single "instance," with the data for each cloud customer residing in the same database, but individual companies' information is segregated via filters. This means that you may be sharing server space with competitors, which can introduce security and data breach concerns.

Cloud-Based Service Management might be a good fit for you if:

- You need a relatively simple solution.
- You don't mind managing two separate CMDBs - one for your cloud solution and one for your on-premise management tools.
- You don't need to connect to external data sources.
- You don't need much customization (such as to support government or compliance regulations).
- You don't need to control when application updates are made.
- Sharing server space with other companies isn't a concern.

When Does On-Premise Service Management Make Sense?

In general, if you need more control over the application to meet your service management requirements, then an on-premise application is likely a better fit. If the following criteria are true for your organization, then consider on-premise service management:

- Your Help Desk team needs accurate information to quickly resolve tickets. For optimal efficiency and high productivity, your Help Desk team needs up-to-date information about all relevant devices, software versions, and servers when they're resolving issues. One of the best ways to achieve this is using an on-premise service management solution that shares a common CMDB with your on-premise IT management tools. Your team will always have access to the latest information about your infrastructure, which can make a real difference in solving issues quickly and accurately.

- Your network can't tolerate bandwidth intensive data synchronization. Another distinct disadvantage of putting your service management solution in the cloud while using on-premise management tools is you'll have two CMDBs – one for each set of applications. If you want your team to access real-time information about your network and devices, you'll need to sync the CMDBs as often as possible, which can cause severe bandwidth issues.

- You need to link your service management solution to external data sources like Active Directory or an ERP system. To maximize efficiency, you may want to link your service management solution to an external data source, such as Active Directory (AD), LDAP, an ERP, a Human Resources system, or an asset tracking application. This allows Service Desk personnel to quickly complete common tasks such as entering a purchase order for a new laptop without logging into multiple systems.

- Cloud-based service management applications normally don't offer this degree of customization. An on-premise service management application that supports this type of flexibility is a better choice.

Linking a cloud-based service management solution to Active Directory comes with trade-offs: If the cloud application supports integration with AD, security risks are potentially introduced as network passwords will need to be regularly synchronized with it. If the cloud application doesn't support AD integration, then your Service Desk team must login twice – once to the network and again to the cloud service application – which takes time and reduces efficiency.

- You need to customize the service management application (such as to support government regulations or compliance standards). Almost all service management solutions, whether cloud or on-premise, support some degree of customization. Most cloud-based systems, though, only support limited customization that might not be adequate for your needs.

If your industry requires compliance with government regulations like HIPAA, your service management application may require specific customization. For HIPAA, you may need to encrypt data in sensitive fields so only authorized users can see or change it. This is the type of deep customization that cloud applications often don't support.

If you do business in Europe where privacy laws limit sensitive human resources information from crossing country borders, a cloud solution with physical hardware that's located outside a country, or that has no ability to control data access from specific locations, could violate country-specific laws. In this case, an on-premise solution is a better fit.

On-Premise Service Management might be a good fit for you if:

- You want your service management solution and IT management tools to use the same central CMDB.
- You don't want your Help Desk team logging into separate systems and duplicating data entry to resolve tickets.
- You want to connect to external data sources, such as an ERP or Human Resources system, asset tracking applications, Active Directory or LDAP.
- You'll need deep customization.
- You need to comply with government or industry regulations.

Additional Considerations When Choosing Between Cloud-Based and On-Premise Solutions

Maintaining a Single Source of Truth

Service management applications create large amounts of transactional data that is changed frequently. To work well, they need constant, real-time updates about your IT infrastructure so help desk personnel can resolve issues quickly and efficiently. Generally information about your infrastructure resides in the Configuration Management Database (CMDB). The majority of on-premise IT management tools populate and utilize an on-premise CMDB. If you want to associate your service tickets with your assets, then your service management tool will need access to the CMDB. Utilizing a cloud-based service management tool may require a second CMDB in the cloud to support that tool. However, if you have two CMDBs, one for your cloud-based service management application and another for your on-premise IT management tools, then keeping data up-to-date in both systems is challenging.

Sharing data between on-premise and cloud systems means time-consuming, bandwidth intensive replication and syncing. Data sharing isn't required, of course, if you're using a hybrid approach. But not sharing CMDB data means your help desk personnel must take extra steps to resolve incidents such as logging into multiple systems to get information about OS and

software versions in order to fix a user's laptop. A hybrid environment may force them to do duplicate data entry and take longer to resolve tickets. It could also compromise thorough incident management reporting.

If you do decide to go the hybrid route and have cloud-based service management and on-premise IT management, there are a few options for sharing data between the two applications.

Your first option is to replicate your on–premise CMDB to the cloud-based CMDB. The second option is to install an additional agent on every endpoint so the agent can collect inventory data and pass it to the cloud-based CMDB.

- Replicate the CMDBs frequently. You could replicate the on-premise system's CMDB to the cloud but, as mentioned before, there's a negative trade-off between real-time replication and bandwidth – the more frequently you sync CMDBs, the poorer the bandwidth. Plus there will likely still be a lag in synchronizing the CMDBs due to WAN performance from your internal network to the cloud solution.

- Install a second agent on every device. If you choose not to replicate your on-premise CMDB to your cloud-based service management solution, you may have to install a second agent on every endpoint so the agent can collect and send inventory data to your cloud-based CMDB. If you already have an agent on every desktop, laptop, and server that's updating your on-premise management system, adding a second agent means additional support and maintenance. Another downside is the on-premise and cloud-based CMDBs will be updated at different rates, so you won't have one true source of information.

Impact of Cloud-Based Service Management on Help Desk Productivity

Using a cloud-based service management application can have ramifications on your Help Desk team's productivity. For instance, it's harder to manage change effectively, such as refreshing a server or installing patches, because they'll be using two systems that aren't integrated.

The more your team can do from one system, such as pushing out a new Microsoft Office application to a user or refreshing a server, the faster and more efficient their service levels. This is an important step for increasing First Call Resolution rates and meeting SLAs.

You'll also save your team time by giving end users self-service options such as requesting a new hire's computer setup or making facility and maintenance requests. Supporting a web-based service portal is a common feature in on-premise service management applications. You can customize the service portal to reflect your end users' common support requests and give them the ability to self-service where it makes sense. This type of deep customization requires end- to-end service delivery that may not be possible in a cloud application.

Finding the Right On-Premise Service Management Solution

When you're looking for an on-premise service management solution, consider Symantec™ ServiceDesk. It's a modern, automated incident response and problem resolution solution for quick remediation of end-user incidents, systemic problems, and change management.

By utilizing a common CMDB and software resources with your on-premise service management solution, you will achieve gains in automation, improved quality of service, and drive down long-term costs.

ServiceDesk features a rules engine for efficient configuration and customization and is designed for full integration of IT processes. It's flexible and can be easily customized to support external data sources and comply with government regulations. You can also offer end users self-service options, like a consolidated support portal and Service Catalog, so your team is free to focus on more strategic issues.

The ServiceDesk installation is fast and configuration is simple and easy so your team can be up and running quickly. And it natively integrates with the CMDB used by Symantec's endpoint management, asset, and server management tools for one source of truth.

Integrated Service Management with Symantec

If you don't already own Symantec endpoint management tools or you're a Microsoft System Center Configuration Manager customer and want a natively integrated management solution, then consider ServiceDesk plus Altiris™ IT Management Suite from Symantec™.

Altiris IT Management Suite provides complete endpoint management with heterogeneous platform support for all your computing devices. ServiceDesk's native integration with IT Management Suite helps reduce total time to resolution, first call resolution, and other important performance metrics.

Other Symantec solutions that integrate with Symantec ServiceDesk include Symantec Mobile Management Suite, Control Compliance Suite, and Critical System Protection.

Symantec™ Control Compliance Suite — enables IT risk to be communicated in business-relevant terms, to prioritize remediation efforts based on a composite view of risk, and to automate assessment processes to improve overall security and compliance posture. Integrating ServiceDesk with Control Compliance Suite facilitates the communication and remediation of issues that are found by Control Compliance Suite.

Symantec™ Critical System Protection — identifies potential vulnerabilities or changes in your IT environment. Integrating ServiceDesk with Critical System Protection helps your operations group remediate critical items discovered by Critical System Protection.

Symantec™ Mobile Management Suite — combines scalable device management, innovative application management and trusted threat protection technology to provide all the capabilities needed for enterprises to enable, secure and manage mobile devices, applications and data. ServiceDesk integrates with Mobile Management Suite to enable the tracking of incidents involving mobile devices.

Learn More

- Get ServiceDesk product information: http://www.symantec.com/service-desk
- Get Altiris IT Management Suite product information: http://www.symantec.com/it-management-suite
- Get Symantec Mobile Management Suite product information: http://www.symantec.com/mobile-device-suite
- Get Control Compliance Suite product information: http://www.symantec.com/control-compliance-suite
- Get Symantec™ Data Loss Prevention product information: http://www.symantec.com/data-loss-prevention
- Get Critical System Protection product information: http://www.symantec.com/critical-system-protection
- Visit our Connect Community and learn how our customers use ServiceDesk: http://www.symantec.com/connect/groups/servicedesk
- Try out a trial version of ServiceDesk in your environment: https://www4.symantec.com/Vrt/offer?a_id=159497

More Information

Visit our website

http://enterprise.symantec.com

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec protects the world's information, and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

05/13

Confidence in a connected world. Symantec.