



IDC PERSPECTIVE

Third-Party Enterprise Software Support: Key Risks and Questions to Ask

Rob Brothers

Elaina Stergiades

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: What to Consider When Evaluating Third-Party Support Providers for Enterprise Software

Digital transformation is a key strategic imperative in 2017, but replacing existing IT infrastructure is not an option for most enterprises. CIOs must innovate, evolve, and optimize their IT infrastructure for critical business processes. The right support provider can help minimize risk and maximize performance at this critical time. With the emergence of third-party support for enterprise software, IT organizations evaluate potential support providers across five criteria to determine the best provider for their IT road map.

Key Takeaways

- For many IT organizations, *security* and *compliance/governance* will be the key factors when selecting support providers. Maintaining access to security patches and demonstrating IT compliance in a regulated industry are top priorities.
- In certain circumstances, *software support features* and *overall IT expertise* will be primary factors in determining the appropriate provider to maximize enterprise software performance.
- Given the state of IT budgets, IDC expects *annual support costs* will always remain top of mind as IT organizations try to keep the lights on and fund innovation simultaneously.

Recommended Actions

- Evaluate potential support providers across the enterprise software stack, with the appropriate considerations according to business process and workload.
- Examine the IT footprint and road map carefully, including the plan for digital transformation – with a specific focus on what the IT landscape will look like in one, three, and five years.
- Consider the plan for software vendor engagement during the course of your digital transformation journey and how that affects any requirements for maintaining legacy infrastructure during migration.

Source: IDC, 2017

SITUATION OVERVIEW

Enterprise IT is continuing its historic trajectory of change to achieve digital transformation, with enterprise software a critical component in determining success. But maintaining and optimizing new and legacy IT remain key concerns for CIOs and IT managers. To maximize the performance of IT infrastructure, most IT organizations rely on external support providers for their enterprise software. Historically, this support was only available from the original software vendor. But in recent years, an alternative has emerged – third-party support for enterprise software.

While third-party support is well established in the hardware market, the proprietary nature of software makes it a newer concept for enterprise software. In this model, IT organizations sign an agreement with a third-party support provider for a specific business application, instead of a maintenance and support agreement with the original software vendor. Given the IP in enterprise software, third-party support providers are limited in their deliverables – they do not have access to proprietary software code from the original vendor, including software patches, so they can't fix any problems that occur in that code. However, they do offer other support activities that can help IT organizations with workarounds and custom code fixes for their solutions.

CIOs and IT managers planning their digital transformation road map should closely examine the potential benefits and risks of vendor and third-party enterprise software support. IDC recommends carefully considering the five key areas outlined in the sections that follow as a way to approach this exercise.

Security

As the threat of cyberattacks from hackers and state actors increases, CIOs are painfully aware of how vulnerabilities in their IT infrastructure leave them at potential risk. Data breaches, consumer exposure, and IP theft can quickly turn into damaged reputations and lost revenue. Unfortunately, making sure that enterprise software is updated with the latest security patches remains a key challenge for IT organizations. IDC recommends making sure security policies and procedures include the latest best practices regarding security hygiene across all vulnerable enterprise systems.

What Are the Potential Risks to My IT Environment?

- Losing access to regular security patches and updates that are required to minimize the risk of exposure to external and internal cyberattacks
- No direct vendor oversight of the software, which can include proactive monitoring of solutions for potential vulnerability and corresponding "rapid response" security patches
- Potential issues with regulatory and compliance requirements regarding software readiness (especially relevant in highly regulated industries)
- Limited security "around the edges" from a third-party support provider, leaving gaps in coverage with business applications vulnerable to external and internal attacks

What Questions Should I Ask a Third-Party Support Provider?

- How will the third-party provider address any security concerns in your enterprise software, especially as new threats arise and new vulnerabilities are discovered?
- What are the specific details in any security offerings from the third-party provider? Can it share examples and customer case studies demonstrating compliance?

- How will the third-party provider manage data privacy? Does it have confidentiality policies and training? Can it protect confidential software IP configuration information? How will it protect any information/insights gained after having access to your custom code?

Compliance and Governance

For most CIOs and IT managers, compliance and governance are critical components of IT operations. And in 2017 and beyond, compliance and governance are not just about software maintenance coverage. An area of intensifying concern is audit trails, a fundamental part of demonstrating compliance. Maintaining these audit trails increasingly requires in-depth skills in big data and analytics – which can be difficult to perform manually. With the growing threats in cybersecurity, and regulation intensifying across industries, companies can face potential fines and penalties for violating government/industry compliance procedures. As security incidents receive more attention, and happen more frequently, these punishments become much more costly – not to mention the potential damage to revenue, branding, and customer trust.

What Are the Potential Risks to My IT Environment?

- No access to the vendor's network of online patches, as well as software updates critical for ongoing security and compliance issues
- Third-party support provider likely to not have the right to convey, relicense, or sublicense a vendor's software to its customers
- Very limited access to the vendor's technical assistance resources, technical documentation, and other critical IP
- Ability to remain in licensing and regulatory compliance across integrated systems when growing, merging, or upgrading hardware

What Questions Should I Ask a Third-Party Support Provider?

- Is the third-party provider capable of meeting the procedures and regulations required by your auditing and compliance team? Can it follow your governance guidelines?
- Can the third party demonstrate skills with audit trails that meet your security and compliance requirements?
- Does the contract include detailed, clear, and concise language regarding how the third party will handle the software vendor's IP? Can it certify its processes are in accordance with IP law?
- Will the third-party provider furnish proof of its legal right to access any elements or features that could be termed "vendor IP?"
- Can the third-party provider furnish contract terms stipulating who is responsible in the event of any potential litigation involving software vendor IP?

Software Support Features and Functionality

When comparing software support features and functionality, vendors and third-party providers each offer a distinct set of capabilities. Original software vendors can offer access to engineering talent with advanced expertise, as well as support features and functionality that incorporate machine learning and automation. In addition, software vendors are consistently expanding advanced support IP to detect, isolate, diagnose, and repair issues before they affect end users. Finally, customers can leverage an array of expanded toolsets and utilities from software vendors – including expanded portals, knowledge bases, training, expert guidance, assistance transitioning from custom code to standard functionality, and upgrade assistance.

However, third-party enterprise software support providers also include a notable feature: most offer direct access to a personal support engineer for the majority of support interactions. Because they serve a much smaller client base, these providers can use a direct-to-customer support model – instant access to high-level engineers with direct knowledge of the customer environment. In addition, third-party support includes coverage for custom code. Many problems that occur in enterprise software have their origin in custom code, which is typically not covered in vendor support agreements. Finally, most third-party support providers will provide access to a support account manager as part of their support package, regardless of software licenses and installations.

What Are the Potential Risks to My IT Environment?

- Limited access to new features or functionality from the vendor in your enterprise software, which assumes user needs will not change in the future (except for custom code changes)
- Limited access to development engineers at the software vendor to address code defects
- Limited access to advanced vendor support features that can help detect, diagnose, and resolve potential issues – increasingly through automated, remote support delivery
- No access to vendor support features like portals, communities, and knowledge bases

What Questions Should I Ask a Third-Party Support Provider?

- Does the third-party provider offer a direct-to-customer support model, with instant access to a high-level engineer on every phone call?
- Will the third-party support provider include coverage for all the relevant custom code in your enterprise software? Does that include modifying existing code, or does coverage extend to developing new code when necessary (i.e., for workarounds, to compensate for lost functionality)?
- Can the third-party provider guarantee access to the same team for the duration of your contract?
- Can the third-party provider meet any specific SLAs that are required for internal or external customers?

Overall IT Expertise and Support

When considering overall IT expertise and support, both software vendors and third-party support providers can offer potential benefits in distinct situations. The dramatic changes required for successful digital transformation initiatives require specific expertise in advanced new technologies like IoT, mobile, and cognitive solutions across hybrid IT. Historically, software vendors have had an advantage when working with new technologies in the IT environment – especially their own IP. With expanded advanced support technology and application life-cycle management tools, software vendors are well positioned to help IT organizations manage these migrations.

On the other hand, third-party support providers can provide coverage for legacy IT infrastructure – a significant component of many IT environments. Since most third-party providers in the software space use the direct access model, most customers will have a primary contact with extensive knowledge of their IT environment. These support professionals should be able to answer questions regarding strategies for existing IT assets and managing custom code going forward. Their knowledge of these applications in real-world scenarios could prove helpful for CIOs and IT managers that plan to maintain their legacy infrastructure for quite some time.

What Are the Potential Risks to My IT Environment?

- Losing access to expertise from the original software vendor for managing the existing environment during planning and execution for digital transformation
- No direct guidance from the software vendor during migrations and integrations, especially for advanced innovations in cognitive computing, artificial intelligence (AI), IoT, and big data and analytics
- Limited insight from the vendor on any new implementations or deployments for related technologies that are no longer covered under support

What Questions Should I Ask a Third-Party Support Provider?

- What kind of coverage can the third-party provider include for my legacy infrastructure software environment? What specific software can be covered?
- To what extent will custom code modification and/or expansion be relevant in supporting this software going forward? Can the third-party provider furnish customer testimonials or case studies of existing work?
- Can the third-party provider guarantee the direct access model for all of the covered enterprise software, regardless of original vendor or implementation?
- Can the third-party provider include specifics in support details and delivery in the contract? This includes escalations, detailed plans for issues that cannot be resolved (especially in source code), and provisions for access to workarounds via custom code modifications.
- Does the third-party support offering include specific guidance, features, or deliverables that can help on a digital transformation journey?

Annual Support Cost

The annual support cost from software vendors has been consistent for many years. Basic support purchased from enterprise software vendors can range from 18% to 22% of license fee, with any additional features costing an additional annual fee (like direct access to a designated engineer or a technical account manager). Most enterprise software support providers include a substantial portfolio of support features and functionality along with regular patches and updates for that fee, from automated diagnosis and resolution to expanded portals and online resources to instant connection with support experts via chat technology.

In contrast, most third-party enterprise software support providers charge 25-50% less in annual support fees than software vendors for their services – a considerable savings for most customers. They are not maintaining extensive proprietary code bases or investing in and creating new product features and functionality. Because of their smaller customer base and lower-cost model, these packages typically offer direct access to support engineers and an account manager as part of their base support package. It should be noted that customers must consider the potential costs of forgoing software upgrades, and especially security patches, into these prices going forward.

What Are the Potential Risks to My IT Environment?

- Potential cost of losing access to software upgrades and new functionality, especially security patches and code fixes
- Planning for any additional risk mitigation if unexpected compliance and/or governance issues arise with third-party support

- Penalties that could be imposed by the software vendor if/when you return to vendor support after engaging with a third party

What Questions Should I Ask a Third-Party Support Provider?

- Can the third-party provider include specific details about support cost for the life of the contract? How long can it guarantee the savings for these software applications?
- Does the third-party provider require you to download, store, and maintain access to all available patches and updates from the vendor? Are there any fees associated with these downloads, or with this process?
- Can the third-party provider help at all with risk mitigation in the event of a security breach?
- Will the third-party provider share its growth and plan forecast? Is it sufficiently staffed for growth, since the direct-to-engineer model can be challenging to maintain?

IDC'S POINT OF VIEW

IT organizations are facing a daunting challenge as they plan their digital transformation journeys. Creating an environment that is easy to maintain, can be robustly supported, and offers a manageable TCO are critical steps to success for CIOs and IT managers. With a wide variety of options for IT consumption, from legacy on-premises to "as a service" infrastructure to the latest cloud applications to key innovations around IoT and mobility at the edge, managing an IT environment is becoming more difficult every year – especially given the persistent threats from criminal hackers and state actors.

With security a key concern for most IT organizations, CIOs are especially careful when ensuring the protection of enterprise systems and data. IDC believes updating IT processes with appropriate security hygiene is critical to maintaining compliance – from a robust, proactive change management process to appropriate patching and security fixes when necessary. With a growing focus on liability and negligence when hackers gain access to IT infrastructure, proper security policies for systems and data are essential to avoid significant consequences to business reputation – and the bottom line.

That being said, in the right circumstances, it can make sense to consider a third-party support provider for some enterprise software. IDC recommends paying special attention to the advantages outlined previously in specific scenarios, with a focus on the special circumstances that surround your IT environment and the road map for digital transformation in your enterprise. A good place to start can be a careful examination of the current IT footprint and a comprehensive consideration of what your IT landscape might look like in one, three, and five years.

IDC also cautions enterprises to be careful when considering the length of time to retain legacy assets. The move to digital is real, and the benefits of fully automated systems that leverage AI and machine learning can be significant. The rapid expansion of technology is adding significant complexity to the enterprise IT landscape – and it cannot be managed by humans alone. Managing the complex interactions of cloud, on-premises, virtual networks, IoT solutions, and especially security requirements will demand advanced autonomous, remote capabilities. Cognitive computing, artificial intelligence, and machine learning are key to the enterprise IT of the future – especially in support.

ADVICE FOR THE TECHNOLOGY BUYER

With a market shift to cloud technologies underway at all levels of the datacenter, IDC expects the software support landscape to undergo significant shifts in the coming years. While enterprise IT still

moves slowly, the pace of adoption for platform as a service, infrastructure as a service, and software as a service is accelerating every day. In addition, business process support is becoming a critical deliverable for most IT organizations – it's not just about uptime and maximizing system performance anymore. CIOs and IT managers need to work closely with business managers to improve adoption and utilization and ensure the enterprise realizes the promised value out of the solution.

To help IT organizations along this journey, software vendors are expanding investment into advanced IP for their support offerings to improve the customer experience and take advantage of machine learning and automation. The incredibly rapid pace of technology change means that AI, cognitive computing, automation, and IoT solutions are likely coming to software support services faster than currently predicted. IDC recommends carefully considering each of the five criteria outlined previously, as well as getting detailed answers from prospective third-party support providers during the vetting process. For the foreseeable future, software support that can leverage these advanced technologies will only be available from the original software vendor.

In fact, many enterprises will want to maintain their software vendor relationships as they build out their digital transformation road maps and consider other solutions from their vendors. IDC believes many CIOs and IT managers will prefer to buy support directly from software vendors – particularly for access to security patches and updates and to ensure regulatory compliance as well. CIOs and IT managers also want to work with their software vendor support teams to leverage their expertise adopting new, innovative technologies as quickly as possible. Software vendors will have firsthand experience with new implementations and deployments and can offer guidance on the necessary back-end integrations required to support legacy infrastructure.

However, third-party support providers for enterprise software will continue to appeal to IT organizations with specific, limited support requirements for their legacy enterprise software. With a focus on cost savings as their key feature, and the appealing "direct to engineer" support model, third-party software support providers will attract customers with stable installations that don't want or need new functionality and – because of current security procedures – are willing to risk losing access to security patches going forward. However, IDC notes that as third-party support providers grow in size, customers should make sure they can guarantee access to the qualified engineers that will be necessary to support their direct service model. IDC recommends using the criteria and questions presented in this document as a guide to making these decisions.

LEARN MORE

Related Research

- *SAP DBS: Can Enterprise Software Support and Services Really be Transformational?* (IDC #EMEA43190217, November 2017)
- *Market Analysis Perspective: Worldwide Software and Hardware Support and Deployment Services, 2017* (IDC #US43058016, September 2017)
- *Worldwide Storage Support and Deployment Survey: TPMs* (IDC #US42991716, August 2017)

Synopsis

This IDC Perspective reveals what to consider when evaluating third-party support providers for enterprise software.

"While most enterprises are devoting significant resources to digital transformation initiatives, replacing existing IT infrastructure is not an option for most enterprises. CIOs must balance innovation with maintaining legacy infrastructure for critical business processes," said Elaina Stergiades, research manager, Software and Hardware Support Services. "The right support provider can help minimize risk and maximize performance at this critical time. With the emergence of third-party support for enterprise software, IT organizations should evaluate potential support providers across five criteria to determine the best provider for their IT road map."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights.

Copyright 2017 IDC. Reproduction is forbidden unless authorized. All rights reserved.

