WHITE PAPER

The Benefits of Vendor Consolidation and Centralized IT Management

An Osterman Research White Paper

Published June 2014

SPONSORED BY

INTERMEDIA

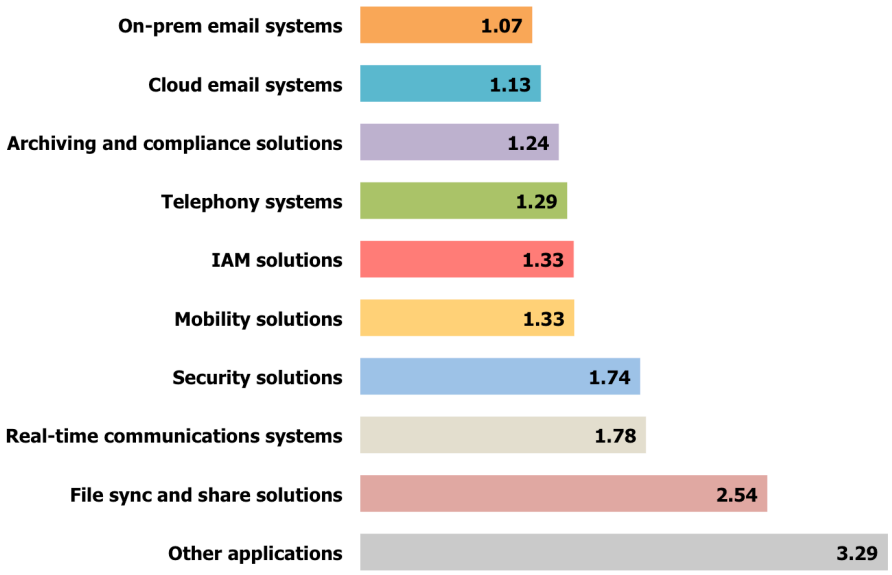
The Business Cloud™

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

EXECUTIVE SUMMARY

Most organizations have a large number of IT systems upon which they rely for email, telephony, real time communications, cloud storage, file synchronization, managed file transfer, mobile device management and a wide range of other capabilities. In fact, an Osterman Research survey of organizations with up to 10,000 email users conducted during April 2014 found that the typical organization supports a mean of nearly 15 major applications, most of which are from a variety of vendors, as shown in Figure 1. Moreover, there are likely other applications about which IT is not aware as a result of individual users downloading and installing their own applications for accessing and generating work-related resources.

Figure 1
Mean Number of Applications in the Typical Organization by Type



Source: Osterman Research, Inc.

This large and growing number of applications and vendors makes life more difficult for IT because they must spend a significant amount of time learning unique management capabilities, security models and configurations for each application. They must resolve difficulties when an upgrade for one application causes a problem in another. They must manage a number of different vendor relationships and billing issues. Finally, they cannot realize economies of scale to the same extent that they could if they managed fewer applications or licensed them in larger numbers from a smaller number of vendors.

This multi-application/multi-vendor environment also makes life more difficult for end users. Not only must users learn different vendors' interfaces, they must spend more time logging into the variety of applications they use on a regular basis, often using the same login credentials for multiple applications. This creates security risks for an organization and leads to a greater chance of data leaks and other security problems.

KEY TAKEAWAYS

This white paper discusses the problems associated with having too many applications that are managed individually, and it discusses the problems that can arise from having too many vendors from which IT solutions are sourced. We contend that:

An Osterman Research survey…found that the typical organization supports a mean of nearly 15 major applications, most of which are from a variety of vendors.

- Some IT services are so foundational that organizations should source them from a single provider whenever possible. This includes critical IT services like email, IP-based telephony and organization-wide collaboration tools.

- Some solutions are highly specialized, and so while it may not be possible to *consolidate* them under a single vendor, their *management* can be centralized.

- While organizations may not want to consolidate all of their best-of-breed solutions (and often should not do so), they can centralize management of them.

Our survey confirms these arguments. For example, we found that 69% of those surveyed consider a centralized management console for as many systems as possible in their organization to be "desirable" or "very desirable", while another 29% consider such a capability to be "somewhat desirable". Moreover, 83% believe that consolidating as many systems as possible to a single vendor would be this desirable.

ABOUT THIS WHITE PAPER

This white paper presents the results of a survey of 121 organizations that were surveyed by Osterman Research during April 2014. The paper discusses the problems associated with managing large numbers of applications and vendors, and it provides an overview of Intermedia's relevant solutions that can help decision makers understand how they can consolidate vendors and centralize management of critical IT solutions.

THE CURRENT STATE OF IT MANAGEMENT

NUMEROUS VENDORS AND POINT SOLUTIONS

Most organizations operate a large and growing number of point solutions offered by a variety of vendors. For example, our research found that across all of the organizations we surveyed, there is a mean of 14.3 different applications used for email, telephony, real time communications, file sharing, mobility, archiving, compliance and other systems. While larger organizations (more than 1,000 email users) operate a larger number of different point solutions, even smaller organizations must manage a large number of solutions.

83% believe that consolidating as many systems as possible to a single vendor would be… desirable.

There are good reasons that many organizations have so many different point solutions in place:

- Many organizations operate legacy applications that have been in place for many years.

- Some IT organizations permit individual workgroups or departments to make their own decisions about which applications will be deployed. This can be a problem, but particularly in organizations with decentralized IT functions.

- The Bring Your Own Device (BYOD) and Bring Your Own Application (BYOA) mindsets are well entrenched, resulting in individual users being permitted to decide from among the thousands of cloud-based, mobile and other solutions available to them.

- Many organizations today are the result of mergers and acquisitions, and so some IT departments will maintain the systems that were in place at the acquired company, often waiting for the next upgrade cycle before integrating disparate solutions, if ever.

SIGNIFICANT LEVELS OF IT ADMINISTRATION

While there are several problems associated with managing such a disparate number of applications and vendor relationships, arguably the most serious repercussion from maintaining highly heterogeneous environments is the significant level of IT administration required to manage the various applications that are in use. For example, our research found that when a new employee joins the organization, there is a mean of between 3.7 and 8.3 different systems on which he or she must be provisioned depending on the role of the employee. Each of these applications can require a significant amount of effort for provisioning, since each one often employs a different management console, integrates differently with backend applications, and requires IT training on each one in order to properly implement all of the capabilities required by new employees.

Moreover, day-to-day management of this collection of applications is more time-consuming than it would be if fewer applications were in use, again because of the different management consoles in use, time spent by IT in solving incompatibilities between systems, upgrading applications on a variety of schedules, and other product support and training.

Another serious problem with managing so many different applications is the high cost of the IT labor required to keep everything running simply because more IT staff are required to maintain so many applications. For example, our research found that there is a mean of 452 users supported per full-time equivalent (FTE) staff person at the organizations surveyed. If we assume a fully burdened, annual labor rate for an FTE IT staff member of $100,000, this translates to an IT labor cost of $221 per user annually, or a monthly cost of $18.44. This cost of support often exceeds the actual cost of the new service. However, because larger organizations enjoy economies of scale for IT labor that their smaller counterparts cannot realize, the cost for smaller organizations is significantly higher. Moreover, smaller organizations often have IT generalists who are less equipped to handle the wide variety of specialized applications.

If we assume a fully burdened, annual labor rate for an FTE IT staff member of $100,000, this translates to an IT labor cost of $221 per user annually, or a monthly cost of $18.44. This cost of support often exceeds the actual cost of the new service.

A GROWING NUMBER OF APPLICATIONS

The problems discussed above are not going away: in fact, there is a growing number of applications employed by end users as vendors introduce new and better tools for the myriad mobile and cloud-based tasks that users carry out, and as IT departments continue to yield to the growing tide of BYOD and BYOA. While virtually every decision to implement a new tool, storage solution or other capability makes sense at a micro level, this creates the macro problem of managing all of these tools, as discussed later in this report.

WHAT ABOUT A BEST-OF-BREED APPROACH?

Does the large number of applications in use argue against a "best-of-breed" approach in managing the various capabilities that users need to do their work? Not really. In fact, best of breed makes a great deal of sense in many situations. For example:

- There are some applications that are clearly superior to their competitors' offerings, and so employing these applications is justified, even if it means maintaining an additional vendor relationship.

- Some organizations may require highly specialized applications in industries like geophysical exploration, architecture, certain healthcare disciplines, etc. Organizations that run Macs instead of or in addition to Windows PCs often find there are typically fewer business applications available for the former.

- Best of breed makes sense in order to provide greater security. For example, an IT department may decide that it wants to run two different vendors' anti-malware solutions in order to maximize the potential for filtering malware out of email and increasing their chances of finding zero-day threats.

In these types of situations, using a best-of-breed approach makes sense and can provide some obvious advantages. However, operating a number of solutions from different vendors complicates both the management of these offerings for IT, and it makes the user experience more difficult.

WHAT IS THE COST OF HAVING MULTIPLE VENDORS?

THE PROBLEMS ARE SERIOUS…AND OFTEN EXPENSIVE

Ultimately, there are a number of problems – some of them quite serious – when multiple applications and multiple vendors are used:

- **Excessive time spent on IT administration**
  Best of breed requires more IT effort because there are more interfaces and management consoles at which to become proficient, more time spent in training, more applications on which to provision new users, and less integration between solutions. Moreover, security management becomes more difficult and more time-consuming because each application may have its own unique security model that IT must learn and manage. Reporting also becomes more difficult because IT cannot generate common reports across all systems. All of this ultimately results in higher IT costs.

- **User problems**
  The need to employ a number of different applications means similar types of difficulties for users: there are more interfaces to learn, more applications to sign into, a reduced ability to share data between applications, and a longer learning curve that ultimately reduces user productivity.

- **Reduced economies of scale**
  Organizations that do not consolidate vendors or applications rarely can benefit from the economies of scale that result from using fewer of both. This results in higher licensing costs, higher training costs and less synergy between applications or systems.

- **Increased integration requirements and complexities**
  One of the benefits of employing fewer applications and vendors is that leading vendors normally provide an integrated experience and management capabilities across their offerings, resulting in better and tighter integration between applications. This benefits IT and end users, since both can come down the learning curve more quickly and there are fewer problems in getting disparate applications to speak to one another. Some companies deploy complex data bus systems to shuttle data between applications. This too adds cost and complexity and is outside the scope of what a smaller organization can address.

- **More difficult provisioning**
  The more applications deployed, the greater the number of users that must be provisioned. This not only requires more IT time, but can result in more mistakes, such as misassigning user privileges for new or changed users. The result is higher cost of onboarding new and deprovisioning departing employees from every application to which they had access.

- **More complex billing and relationship management issues**
  Another problem with a highly heterogeneous environment is that the complexity of billing increases, as does the management of the relationships with the various vendors. For example, in a single vendor environment, a faulty patch in an email-enabled application that shuts down an email system is more easily addressed by customers in a single-vendor environment than if multiple vendors are involved. The "one-throat-to-choke" approach to relationship management makes life much easier for IT and can lead to more rapid problem resolution and

There are a number of problems – some of them quite serious – when multiple applications and multiple vendors are used.

possibly, greater system uptime.

- **Reduced security**
  A heterogeneous environment can also result in reduced security. Users that employ a variety of applications will employ easy-to-remember – and often insecure – passwords or employ the same password across multiple systems in order to remember them more easily. Worse, employees will often write down passwords on sticky notes or in other insecure places. An environment with a large number of applications and different vendors in use will allow IT to have less insight into the overall IT footprint. Plus, ex-employees are more likely to have continued access to one or more applications and/or data sources simply because IT forgot to deprovision these users in a timely manner or at all.

- **Legal and regulatory problems**
  An organization that operates a heterogeneous environment can face a variety of legal and regulatory problems. For example, if an organization has multiple archiving solutions, such as one for email and one for files, this increases the amount of time required to search for content during eDiscovery or compliance activities, and it can also increase the likelihood that information will be missed because multiple interfaces will be used. Implementing legal holds can be more time-consuming and more complex because there are more systems in which data needs to be held, increasing the likelihood that a legal hold might not be implemented on one system or another or might not be implemented in a timely manner.

  Moreover, multiple applications from multiple vendors or providers means that there can be an increased number of points for data leakage or evidence spoliation, the result of which can be fines, sanctions and a variety of other problems.

Multiple applications from multiple vendors or providers means that there can be an increased number of points for data leakage or evidence spoliation.

RECOMMENDATIONS

Osterman Research recommends that every organization undertake four important steps in evaluating their IT infrastructure in order to determine if it can be made more efficient or less expensive.

ANALYZE YOUR IT INFRASTRUCTURE

First, understand each and every application that is running on the corporate IT network, both IT-deployed and employee-deployed applications, and on every platform that these applications might run – desktops, laptops, smartphones and tablets, both employee-owned and company-owned. The goal of this exercise is three-fold:

- Identify the solutions running today that can be consolidated to a single vendor. Email, voice and collaboration solutions are often the most likely candidates, although there are many other tools that can be consolidated to a single solution and vendor, as well.

- Identify the solutions that should remain best of breed, such as CRM solutions, industry-specific and specialized applications, and legacy applications that would be too expensive or too disruptive to consolidate.

- Identify integration points and methodologies to support the remaining best-of-breed and single vendor solutions. Keep in mind that a larger number of applications typically requires more infrastructure to integrate their capabilities, and so consolidation can provide additional cost benefits by eliminating some or all of this infrastructure.

EVALUATE AND COMPARE TCO

Next, evaluate and compare the total cost of ownership (TCO) for maintaining multiple vendors vs. consolidating on a single vendor (or fewer vendors). Also evaluate and compare the TCO for maintaining separately managed vs. centrally managed solutions.

Evaluating and comparing TCO can be a difficult exercise for a couple of reasons. First, many organizations often lack the data necessary to conduct a thorough and accurate analysis. Good sources of information include consultants, analysts and vendors themselves, but each situation is different and may require somewhat extensive internal analysis. Second, the benefits of migrating to a single vendor, for example, can be obvious, but might be difficult to quantify if an organization lacks experience in doing so.

CONDUCT AN ROI ANALYSIS

Next, we recommend conducting a thorough analysis of the return-on-investment (ROI) that can result from migrating to fewer vendors or a single vendor, as well as migrating from separately managed to centrally managed systems. The TCO analysis noted above is a critical element of the overall exercise, but the ROI analysis can be trickier because it involves quantifying the future benefits that an organization will realize from this consolidation of vendors or centralization of application management. We recommend taking a fairly conservative stance on evaluating the benefits. Although the benefits of undertaking these initiatives are quite real, it is essential to set realistic expectations with decision makers charged with approving them.

It is also important to note that consolidating applications and reducing the number of vendors that must be supported is beneficial to managed service providers. Doing so will reduce the amount of time they spend on application and vendor management, thereby increasing their profitability and/or giving them more pricing flexibility.

We recommend conducting a thorough analysis of the return-on-investment that can result from migrating to fewer vendors or a single vendor.

SERIOUSLY CONSIDER SINGLE SIGN-ON

Single sign-on (SSO) capabilities are an important best practice that all organizations should consider because of the benefits that an SSO portal provides for both end users, IT and the entire organization:

- End users benefits from having to remember only one password in order to access all corporate applications instead of a large number of passwords. This is particularly important in organizations that follow the best practice of changing passwords on a regular basis.

- IT benefits from the use of an SSO portal because users are less likely to forget their single password (compared to multiple passwords) and so will need less support from IT and help desk personnel.

- The entire organization benefits from the improved security that comes from users not writing down their passwords on sticky notes or using the same passwords for multiple applications. As a result, an SSO portal can significantly reduce the likelihood of data breaches and unauthorized access to computing resources.

EVALUATE VENDOR OPTIONS

Finally, conduct a thorough analysis of the vendor options that are available. Some vendors offer solutions for consolidating existing applications under their umbrella of offerings, while others offer solutions for centralizing management of applications – fewer vendors or providers offer both of these capabilities that we believe are best practices for virtually any organization to consider. Although there are a number of solid vendors in the marketplace, Osterman Research recommends using a vendor that can provide both capabilities, since this will provide an organization the flexibility

of a) consolidating on one vendor to manage both capabilities, and b) it will enable a more measured migration to these best practices.

ABOUT INTERMEDIA

Intermedia is the world's largest one-stop shops for cloud business applications. Its Office in the Cloud™ suite integrates all of the essential IT services that SMBs need to do business, including email, voice, file sync and share, single sign-on, security, mobility, archiving and more. Office in the Cloud goes beyond unified communications to encompass the widest breadth of fundamental IT services delivered by any single provider.

Think of it as a "Business Cloud Platform." All of Intermedia's services are integrated into its HostPilot® Control Panel. There's just one login, one password, one bill and one source of support, which creates tremendous cross-service efficiencies for both users and IT administrators. And, all its services offer enterprise-grade security, 99.999% availability and 24/7 phone support with hold times of less than 60 seconds.

Intermedia has 60,000 customers over 1,000,000 paying users, and 5,000 active partners – including VARs, MSPs, telcos and cable companies. Its industry leading Partner Program lets partners sell under their own brand with full control over billing, pricing and every other element of their customer relationships. Intermedia is the world's largest independent provider of hosted Exchange.

Intermedia has 600 employees in three countries who manage ten datacenters to power its Office in the Cloud – and who work relentlessly to assure customers and partners of a Worry-free Experience™.