From Strategy to Implementation,
Establishing a Managed Cloud Infrastructure

Contents...

From Strategy to Implementation, Establishing a Managed Cloud Infrastructure

Contributor: Michael Stevens

When Should You Put Applications in the Cloud?

By Michael Stevens

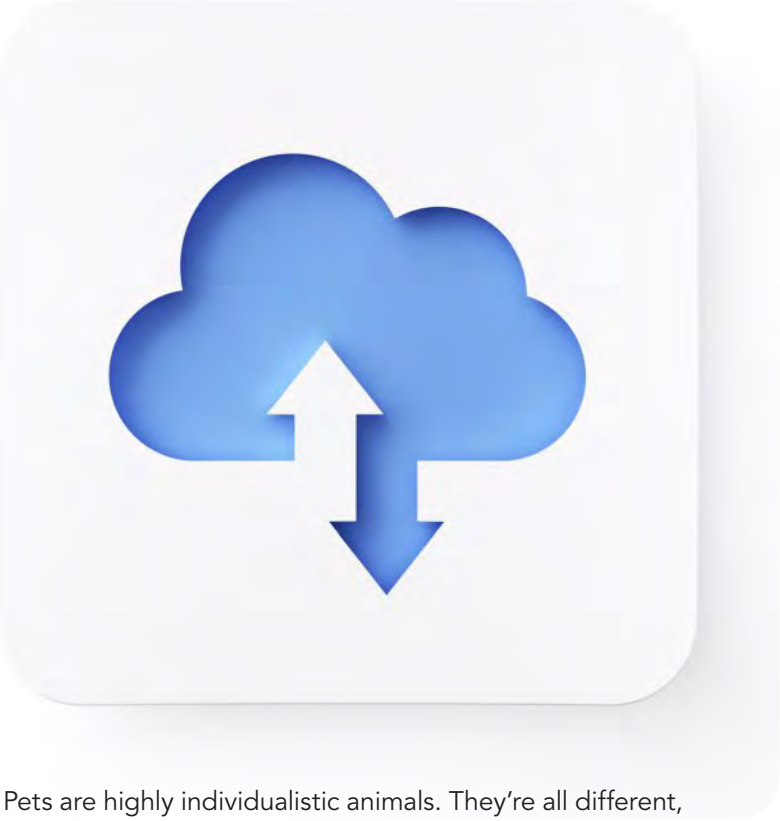
In theory, cloud computing as offered by public cloud providers is an ideal IT solution for midsize businesses. The reality of when to put applications in the cloud is more complicated. While some applications can be migrated to the cloud with relative ease, others require significant work, and some won't work in the cloud at all. This is not to say that cloud computing is a poor strategy. On the contrary, no other approach offers as many capabilities and benefits. But migrating to the cloud is not the proverbial "slam dunk" indicated by the hype.

To begin with, applications almost always need to be modified to fit into any given cloud, which necessitates the writing of new code. Furthermore, all clouds are not created equal. The modifications that enable an application to be migrated to "Cloud A" are unlikely to make it ready for "Cloud B." Another challenge for midsize companies is that the major public cloud providers do not offer the level of support necessary for quick success.

In summary, companies need to respect cloud migration for the challenge it is. While every company's situation is unique, there are two broad areas of concern that every IT department should keep in mind when assessing the feasibility of migrating an application to the cloud.

Will It Work in the Cloud?

The first question organizations should ask about the application they want to migrate is, "Will it work in the cloud?" A huge number of applications have been developed over the years, and some companies run literally thousands of them. As a first step towards determining which of them are web appropriate and which aren't, the pets vs. cattle analogy is helpful.



Pets are highly individualistic animals. They're all different, and they're all adapted to the particular needs, wishes and desires of their owners. They also require constant care and feeding.

In contrast, cattle aren't known — or at least aren't valued — for their distinct personalities. For the people who deal with cattle, one steer is more or less as good as another. Equally important, cattle can be treated in a highly uniform manner in terms of their basic needs. Also, cattle don't require anywhere near the constant attention that pets require.

In the terms of this analogy, pets don't do very well in the cloud, whereas cattle flourish.

The "pets" of IT applications are typically either home-grown applications or commercial legacy applications that are very old or highly modified. They may perform a very ordinary task, such as database management or order entry, but do so in a way that's quite different from the norm. Alternatively, they may be designed for a business with unusual needs — needs that a more run-of-the-mill application couldn't meet without significant modifications. These "pets" often run on an operating system that is no longer in common use or make use of out-of-date drivers.

Another class of applications that may not do well in the cloud are those that are transaction intensive and require high network throughput coupled with low latency. Applications that rely on close, frequent communication with one another such as payroll and HR, or those which have important dependencies, such as major ERP systems, may also have problems for the same throughput-related reasons.

Finally, applications with high availability requirements are often not good candidates for the cloud. This is not because of problems inherent in public clouds, but rather because of potential problems with the internet itself. If an application is being accessed via the internet, interruptions are always a possibility. If brief lapses in the services an application provides can have serious business consequences, the cloud is not a good choice.

Netting It Out

When an IT department has reviewed and eliminated all the "pets" from its cloud migration list, there will most likely be plenty of applications left that are cloud appropriate. The question companies should ask about these applications is, Do they really need what the cloud can offer? While "what the cloud has to offer" is the

subject of considerable debate, most would agree on the following benefits:

• **Reduced CAPEX and maintenance.** First and foremost, cloud computing offloads all the costs and concerns directly related to the purchase and maintenance of hardware and software infrastructure.

• **Flexibility/Scalability.** The cloud is ideal for applications where the workload has pronounced peaks and valleys. Applications in the cloud can scale rapidly and automatically to meet peak needs.

"Applications with high availability requirements are often not good candidates for the cloud. This is not because of problems inherent in public clouds, but rather because of potential problems with the internet itself."

Also, when a work group needs more computing power — for a development project, for example — companies can spin up the necessary virtual machines (VMs) in a matter of minutes. This is in stark contrast to the process of purchasing and installing a new physical server. When a VM is no longer needed, it can be destroyed as easily as it was created. Furthermore, all the administrative work associated with these processes can be automated.

• **Performance.** Provided there are no latency issues, the cloud can often deliver higher performance, which can make an important difference in processing times for complex reports or in the user experience.

• **Reliability.** A public cloud has enormous redundancy available. Infrastructure problems that would cause work to grind to a halt and engage the entire IT team disappear.

• **Security.** Surprisingly, the cloud can often provide better security than midsize businesses can provide for themselves. Cloud providers can afford the latest and greatest security technology, and employ a staff of security experts who devote all their attention to security monitoring on a 24/7 basis.

These are extremely important benefits. For most companies, moving IT expenses from OPEX to CAPEX in itself is a very strong argument for moving applications to the cloud. Gains in the technical benefits related to scalability, performance, reliability and security can also have an important impact on business operations. The bottom line is this: IT groups that are not yet exploring the cloud should begin immediately. Migration is not without its challenges, but the results will almost always be well worth the effort, and with the right partner, the transition can be smooth. ■

For more detailed information on cloud computing, please visit www.sungardas.com/Solutions/Cloud/Pages/cloud-computing.aspx.

Colocation? Managed Hosting? Public Cloud? Which is Best for Me?

By Michael Stevens

Managed hosting, colocation and public cloud computing all have the same goal: getting the greatest business value out of scarce IT resources and limited IT budgets.

Given the time and resources, IT can make important contributions to the success of a business. It has been demonstrated time and again that IT can help companies cut costs by careful monitoring of operations, increase sales with the use of sophisticated database functions like predictive analytics, and provide senior managers with real-time decision support through dashboards they can consult from their smart phones.

Unfortunately, most IT departments don't spend much time on developing and implementing these sorts of business-enhancing functions. Rather, they spend the vast majority of their time managing the keeping the lights on. According to a recent Forrester survey of 3,700 companies, the average IT department spends 72 percent of its time on maintaining the status quo. This figure is often as high as 90 percent in smaller companies.

The idea of offloading routine functions is appealing because doing so means more time is available for new initiatives that can actually drive the business forward. Colocation, managed hosting and the use of third-party (public) cloud resources all eliminate the need for bright — and often highly paid — employees to waste their valuable time on low-level tasks. Furthermore, they eliminate this problem at cost levels that make sense. Colocation, managed hosting and cloud vendors all achieve significant economies of scale, and this allows them to provide services at a reduced cost and still make a profit.

There are, however, very important differences in what they provide, differences which are often a source of confusion.

Colocation — A simple, cost-effective option. Colocation vendors essentially rent space in the form of racks and/or cabinets that are physically secure, and provide what could loosely be termed the utilities necessary to sustain servers. These include power, cooling, cabling and, typically, a dedicated Internet connection with a pre-determined bandwidth allotment – often referred to as "ping, port and pipe." IT departments are responsible for buying their own servers, installing them, maintaining them and ultimately disposing of them at the end of their life cycle.

The advantage of colocation is that companies don't have to deal with the complexities of housing, powering and cooling their servers. The primary drawback is that they are still responsible if anything goes wrong. This means that if something goes wrong, e.g., a server crash, someone has to drive over to the colocation site and fix the problem. (Some colocation vendors will supply so-called "remote hands" at an extra charge to perform routine functions such as re-booting when necessary.)

Managed hosting — For greater focus on business problems. Managed hosting is a much more comprehensive offering. To begin with, managed hosting vendors provide all the physical hardware, which means that a significant portion of a company's total IT spend can be converted from CAPEX to OPEX – a significant benefit and often the primary driver for companies that choose managed hosting. Companies not only avoid initial capital expenditures. They also eliminate the expenses of hardware replacement over time, and the headaches associated with accurate capacity planning. Growing companies in particular avoid the hidden cost of having to buy CPU and storage capacity that may sit unused for months until the company grows into it.

A second economic benefit of managed hosting is that, in addition to power, cooling and a bandwidth allocation, companies receive a range of important services. These include monitoring of server performance, management of the operating system(s), OS updates, patching and back-up. (Some managed hosting vendors move higher up the stack to offer application support as well.)

As any IT manager knows, routine tasks like OS maintenance are costly, because they consume a huge number of work hours. Each task that is off-loaded frees up some of those hours so they can be devoted to tasks that will more directly impact the business. For example, IT can train and develop experts on specific applications for the various departments (marketing, manufacturing, finance, etc.). This enables IT to help maximize the business value of these applications, rather than simply keep them up and running.

With managed hosting, if a system goes down, the IT department can focus on recovery and minimizing user downtime, instead of having to worry about infrastructure downtime.

The major drawback for most companies considering managed hosting is lack of control. For some, control is a non-issue. But for others, the fact that their applications are running on virtual machines that may hop from one physical server to another on a moment's notice and potentially compete for resources poses

"The average IT department spends 72 percent of its time on maintaining the status quo. This figure is often as high as 90 percent in smaller companies."

problems. For example, regulatory compliance in some industries demands that companies know where their data physically resides.

Cloud Computing: Taking Managed Hosting to the Next Level

While there are many issues related to cloud computing – enough to fill a book if not several, three deserve special focus for those weighing the cloud vs. managed hosting.

Firstly, on the plus side, cloud computing isn't only a technical approach to providing IT resources. It's also a business model. In this regard, it can be seen as managed hosting taken to the next level. Cloud customers enjoy all the CAPEX vs. OPEX benefits plus the financial benefits of usage-based pricing.

With cloud computing, companies can very quickly scale up capacity to meet peak needs such as end-of-month financial processing, and then scale back down after the need is over – literally in a matter of seconds. They can therefore avoid paying for unused capacity. This same quick scale-up/scale-down, often combined with self-service provisioning, is the most cost-effective approach to IT development projects.

Secondly, on the technical side, the cloud can sometimes offer substantial performance improvements.

Third, and on the down side, migrating to the cloud is not as straight-forward as the hype would indicate. Most applications require at least some coding modifications to run in a cloud. Some cannot take full advantage of the cloud's benefits. Some cannot be migrated at all. In short, the cloud is most definitely a look-before-you-leap proposition, and small or midsize companies should make sure their cloud vendor can provide adequate technical support for a smooth migration.

The New Hybrid Reality

For many companies, the choice between these three options will not be either/or. Today, most companies have a hybrid environment where some computing services remain on-site, some reside outside the company, and some (in the case of cloud-bursting) actually fluctuate between inside and outside depending on demand. It is extremely important that any vendor chosen for any of these options have a deep understand the complexities of hybrid IT, and be able to support migrations when needed.

Increasingly, computing power is becoming a service companies buy rather than one they provide for themselves, and this trend will surely gain even more momentum over time. There are many options now available, and they are all worth exploring. For more information, please visit www.sungardas.com/KnowledgeCenter/WhitePapersandAnalystReports/Pages/the-compelling-business-case-for-hybrid-cloud-services.aspx. ■

Managed Hosting: Lower Costs, Better Use of Internal IT Resources

By Michael Stevens

IT managers have plenty of practice fielding questions about why it takes so long to "get things done." Most IT departments, regardless of size, spend at least 70 percent of their time, energy and budget simply keeping their systems up and running by diligently performing routine maintenance tasks. In many cases, that number is closer to 90 percent. Given this state of affairs, team members who are often highly trained — and highly paid — don't have time in their day to work on projects that could have a real impact on the business as a whole.

OS upgrades are a good example. To begin with, someone has to be in charge of monitoring when upgrades are available. Then, when a notification arrives, someone has to evaluate the upgrade and decide whether or not to implement it. This is not a trivial decision because, as all IT managers know, upgrades are a primary source of crashes, and there are often incompatibilities to deal with.

The next step is actually installing the upgrade. Often, this activity must take place over the weekend, which is inconvenient and involves overtime. Finally, there are the hours consumed figuring out what went wrong if there is indeed a crash.

Loss of Potential Financial Benefits

In addition to the actual costs of infrastructure maintenance, there are potentially enormous financial benefits that companies don't obtain because IT's time is consumed by so many routine tasks. A host of applications have been developed and refined over time that have the proven ability to increase revenue and cut costs — the two fundamental drivers of most business activity. These are not exotic, "bleeding edge" products. They are well-established in the marketplace, and in common use in enterprise-scale companies worldwide. Here are some examples of where managed hosting proves its worth – taking the burden off the IT department and giving it to a trusted hosting provider:

Predictive analytics is a real time application with a proven track record boosting sales for companies that deal directly with consumers, whether online, via call centers or in brick-and-mortar outlets. Typically, at the moment a customer makes a purchase, the predictive analytics engine calculates what other up-sell or cross-sell products are most likely to be bought by that particular customer. There are plenty of documented case studies where predictive analytics has increased revenues by over 10 percent.

Supply chain management applications enable companies to select, manage and measure their vendors with high levels of efficiency and precision that translate directly into significant savings in inventory (as high as 20 percent), warehousing and transportation costs. There are also customer-facing benefits, including improved on-time delivery and a higher percentage of perfect order fulfillments.

Big data projects are relevant for both increasing revenue and cutting costs. The ability to include huge numbers of variables in a marketing analysis enables companies to improve sales projections at a highly granular level and get the right product to the right place at the right time. On the cost side, big data enables precise analysis of operational metrics, and can have a significant impact on product quality.

These are only three out of many, many examples of IT initiatives midsize companies can explore in their efforts to grow while maximizing efficiency. Arguably, this is exactly what IT should be doing. Failing to explore and implement new business-related applications not only hurts the company as a whole. It also diminishes the perceived value of IT. This in turn can result in tighter budgets and even less time to spend on innovation.

Managed Hosting Makes Financial Sense

Managed hosting provides an alternative vision for IT as a strategic contributor to the business. To be clear about the term, managed hosting involves off-loading everything related to infrastructure to a third party. This includes not only supplying the hardware, power, cooling and bandwidth required, but also the operating system(s), and the monitoring, maintenance and upgrading of all the above. In addition, many managed hosting companies will provide other services, ranging from provisioning of new users to management of actual applications.

For many companies, going outside for computer services makes very good financial sense. Because of their economies of scale, managed hosting vendors can more often than not provide the same infrastructure (and related services) as an in-house organization at a lower cost. Also, significant expenditures can move from CAPEX to OPEX, which is almost always desirable.

From an operational perspective, transitioning to managed hosting offers multiple benefits:

• Many routine tasks disappear, providing IT with the time and energy for researching and implementing innovations that can impact the business.

• IT employees can become experts on mission-critical applications instead of merely repair technicians. In many midsize businesses, the expertise on department-specific applications — CRM, for example — resides in that particular department. Someone has found the time to study the application, take a seminar or two, and become an informal "expert" and problem-solver. With managed hosting, IT can bring the function of application expert back to IT where it belongs.

• IT gains credibility and leverage when budgets are determined. Upper management will listen with new respect when IT is perceived as a strategic contributor to the company's success.

Managed hosting will obviously not eliminate every routine function from the IT department or solve every problem. However, it is an option worth exploring for any company looking to increase the value IT can contribute. For more information, please visit www.sungardas.com/Solutions/hosting/Pages/managed-hosting.aspx. ■

"Managed hosting involves off-loading everything related to infrastructure to a third party. This includes not only supplying the hardware, power, cooling and bandwidth required, but also the operating system(s), and the monitoring, maintenance and upgrading of all the above."

The Ins and Outs of Cloud Bursting

By Michael Stevens

Cloud bursting — the dynamic deployment of applications that normally run on a private cloud to a public cloud — gives companies a new option for expanding their capacity to meet peak demands when the resources of their private clouds are not adequate. It's an important technology because the use of private clouds is expected to increase in the 40 to 50 percent range over the next five years,[1] and cloud bursting can make these private clouds much more cost efficient. The reason is simple. Instead of being built to support peak demands — which means supporting resources that will sit idle most of the time — private clouds can be built to run at high utilization rates because the peaks can be handled by a public cloud. A phrase sometimes used to describe this process from a business perspective is, "buy the base, rent the spike."

Multiple Use Cases

A number of business situations can create spikes that impose an extra burden on a company's private cloud. These include:

Seasonal variations. Many businesses experience seasonal variations in the number of transactions their data center must handle. Nearly all retailers experience a spike during the holiday season, and there are numerous other spikes for more vertically focused businesses such as ski and snowboarding equipment, back-to-school supplies , candy and flowers, health clubs and the travel industry.

Calendar-based spikes. Financial applications often create peaks related to heavy end-of-month, end-of-quarter and end-of-year activities.

Marketing activities. New product introductions, intensive ad campaigns or publicity in the media can lead to temporarily heavy website traffic. For some companies,

high-profile TV ads are a regular event that can be guaranteed to create extra demand for IT resources.

Development projects. Software development teams often need to spin up a significant number of virtual machines for testing purposes, but these VMs are typically required only for a short period of time. Engineering activities in general can also create temporary demands.

Geographical issues. There are times when a data center in one location has a heavy load while another has extra capacity that can be used to ensure optimum application performance and response times that are within SLAs.

The Technical Issues

Cloud bursting enables companies to handle all of these use cases cost effectively. From a technical perspective,

however, "renting the spike" requires careful planning to be successful. To understand the issues and evaluate whether application-tier cloud bursting makes sense in any given situation, it's worthwhile to take a step backward and look at what's driving the popularity of private clouds in the first place. Beyond general efficiency and improved hardware utilization, a number of important benefits are associated with building a private cloud. Cloud bursting technology can enhance these benefits, but to ensure success IT should bear in mind six technical issues.

Scalability. The pooled nature of resources in a private cloud allows applications to scale up and down in a matter of seconds depending on the resources they need at the moment. Cloud bursting dramatically extends this capability. The only concern is making sure that the public cloud vendor has committed resources adequate to the needs of application that will burst.

Performance. Assuming the private cloud is on-premise, transfer rates can be dramatically higher because data is moving over the company's intranet, not the Internet. For the same reason, user access times are consistent and not subject to delays caused by variations in external traffic loads.

In a scenario where data must travel over the Internet, transfer rates may not be fast enough (or reliable enough) to ensure that cloud bursting is a viable option. Poor transfer rates mean user dissatisfaction at minimum and system crashes in the worst case. On the other hand, if the physical location of the public cloud provider is close enough, latency will not be an issue. In an ideal situation, the private cloud and public cloud are co-located.

Committed resources. Many IT managers prefer to have control over their physical resources because they want to know with certainty what resources are available and perhaps tune those resources for maximum performance with a particular application. In a private cloud, companies have that control. In addition, they aren't dependent on the multi-tenant architecture of public clouds where they are compelled to share resources. Today, some public clouds address these concerns by offering dedicated server services. This option may be somewhat more expensive, but it is well worth the cost if dedicated resources are felt to be important.

Security/Regulatory Compliance. While concerns about the security of public clouds have diminished somewhat, security issues as they relate to regulatory compliance are still an important concern. Governmental agencies at the federal and state levels will hold enterprises accountable for the actions of their subcontractors when it comes to compliance.[2] For this reason, companies that must comply with HIPAA, PCI or other such regulations should be sure their vendor is experienced and knowledgeable concerning best practices in this area.

Compatibility. Cloud bursting means operating an application in two different environments. In some cases, the application to be run in the public cloud when bursting may require some modifications to be compatible with this new environment.

Monitoring. While public clouds take care of all the infrastructure monitoring, customers still need to monitor their applications and will probably want to implement an integrating multi-cloud monitoring solution, many of which are available.

None of these issues present serious challenges. Any IT organization that is already operating a private cloud should be able to obtain the benefits of cloud bursting — particularly if the public cloud vendor offers strong customer support. Cloud bursting is an excellent approach to minimizing IT costs, and it also puts companies on the path to hybrid clouds, which many believe will become the norm in the near future. ■

[1] Computerworld, July 17, 2014: http://www.computerworld.com/article/2490138/private-cloud/enterprises-increasingly-look-to-the-private-cloud.html

[2] TechNet Magazine, May 2012, https://technet.microsoft.com/en-us/magazine/hh994713.aspx

Are You Investing in the Right IT Security Technologies?

By Michael Stevens

IT security is not a one-size-fits-all proposition. Every company has its own specific business requirements related to security, and the key word here is business. All too often, companies evaluate their security posture from the perspective of technology. They ask questions like, Do we need ingress filtering? Do we need intrusion detection?

These may well be legitimate questions, but technology is not the right place to begin. When it comes to security, companies should first and foremost determine the business consequences of a security breach, and do so on a system-by-system basis. The successful hack of a database that contains sensitive information like credit card account numbers might cost a company millions – or even billion – of dollars. A hack into a logistics database, on the other hand, would likely have less serious consequences.

Evaluating Risk

When evaluating the security risks associated with any particular application, the informal "CIA" framework is very useful.

Confidentiality. How sensitive is the data, and what would be the consequences of a successful exploit? Obviously, some classes of data — personally identifiable information (PII) data, for example — require the highest level of protection. In fact, PII data is almost always the subject of regulatory requirements with which companies must comply if they want to do business. Other classes of data, like intellectual property or marketing plans, may or may not merit the same high level of security.

Integrity. What would be the consequences if the data were corrupted? Unreliable data in an accounting system could be a disaster. In a warehouse management system, the consequences wouldn't be good, but they would not be nearly so grave.

Availability. What happens if any given system crashes? For an e-commerce company, keeping a website up and running is crucial, as every minute of downtime is a minute with no sales. In contrast, a manufacturing company's website that only exists for promotional purposes has no mission-critical significance.

There are two approaches to evaluating each of these categories: quantitative and qualitative. The quantitative approach asks how much it would cost the company if there were confidentiality, integrity or availability problems with any given system. To give a simple example, the cost of downtime (no availability) for an e-commerce website could be calculated by multiplying the average sales per minute or hour times the number of minutes/hours the site is down. For an engineering company, the cost of downtime due to corrupted data would be calculated as the number of working hours lost times the burdened hourly rate of the engineers who couldn't do their work.

Clearly, the results of these calculations will never be precise. Nonetheless, they can help companies prioritize their security risks. Also, they enable companies to make at least a rough cost/benefit analysis of the value various security measures can provide.

Qualitative decisions are obviously more subjective. For example, a web development company might make a qualitative decision that its own site needed to remain up and running 24/7 as a demonstration of reliability and quality, even though a crash would not have a measurable impact on productivity or sales.

Evaluating Technology

Once a business has prioritized its security needs, the next step in implementing appropriate security is to evaluate the technology. In general, the options are well-known, but here's a brief review that illustrates the complexity of today's security landscape.

Anti-virus and firewalls. These tools both perform ingress filtering. In simple terms, anti-virus systems do so by inspecting email attachments and web pages that have been downloaded, while firewalls detect and block unauthorized attempts to connect with the corporate network.

Intrusion detection and SIEM systems. Intrusion detection systems monitor network traffic searching for anomalies that indicate an attack is in progress. SIEM (Security Information and Event Management) systems also perform this function, but they coordinate this data with data from numerous other sources to uncover patterns typical of a malicious exploit. SIEM systems can also take action to block an attack, e.g., by interrupting network communications, disabling USB devices or killing processes.

Virtual private networks (VPNs). These private "tunnels" ensure the privacy and security of communications such as those between the mobile device of a sales rep and a corporate ordering or CRM system.

Identity and access control. According to one recent survey, roughly one in 10 exploits are inside jobs. It's important to manage who has access to what, and monitor that access so that suspicious activity can be quickly detected. Organizations also need to ensure they can shut down the network access of terminated employees very quickly.

Data loss prevention. Even the most conscientious employees can sometimes put data at risk through carelessness. Emailing sensitive information like social security numbers, bank routing information and the like is a good example. Companies need some degree of egress filtering to spot and block unintentional data loss, as well as intentional theft.

Complexity and Cost

The point here is that all these technologies may be required to establish a strong security posture. Unfortunately, they are all both complex and expensive. Their complexity stems from the fact that they must defend against a growing variety of threats that are in themselves complex, and constantly mutating into new forms. The cost includes not only licensing fees, but the time required for technicians to be trained on half a dozen systems, each with its own quirks.

One option that is becoming increasingly attractive to midsized companies is managed security. Outsourcing security not only eliminates the hassle of licensing, installing and running multiple systems. For many companies, it is the only economically feasible way to ensure that they have the most modern up-to-date systems guarding their data. ■

For more detailed information on how you can get the most out of information security technologies, please visit www.sungardas.com/solutions/consulting/information-security/Pages/information-security-strategy.aspx.

How Managed Security Services Work

By Michael Stevens

In the time it takes to read this article, the IT systems of an average midsize business will be attacked several dozen times. Fighting this constant barrage of exploits takes specialized security skills, time and money — all of which are in short supply in most small IT organizations. Managed security services have emerged as an attractive alternative for midsize companies, particularly in the light of the changes that are taking place in today's rapidly evolving security landscape.

To begin with, hacking is no longer a rogue activity practiced by individuals or even small, loosely organized teams. Hacking is a business, carried out by large, integrated "corporations" with clear divisions of labor and a highly developed supply chain. There are the researchers, whose focus is on hunting for potential vulnerabilities and developing the means to exploit them; the farmers, who develop and grow the botnets composed of large numbers of "zombie" computers that have been infected with malware and can act in concert to carry out an attack; the dealers, who rent botnets and then perform actual attacks, such as data theft or spam distribution; and the consumers, who monetize stolen data, e.g., through fraudulent transactions.

All these specialists are aligned to exploit the sensitive data that resides within the systems of midsize businesses, from credit card numbers to intellectual property.

New Threats, New Defenses

Today's businesses not only face a new and better-organized enemy. They also face new threats. For example, hackers are now employing big data and mass customization techniques to disguise malware-bearing spam. Instead of receiving a thousand identical spam messages from one single source — an attack that's easy to spot — companies may receive a thousand different messages from multiple different sources. Malware is now being designed so that it will only execute correctly on the environment for which it was targeted, thereby defeating current automated malware analysis.

These are only two examples of the numerous new technical approaches hackers are taking to defeat today's defenses.

Obviously, purveyors of security software aren't about to be caught napping. The list of capabilities companies must license and deploy in order to be safe keeps growing and changing. Security Information and Event Management (SIEM) is a good example. Unlike basic intrusion detection software, which looks for anomalous network traffic and behavior, SIEM systems have evolved to collect information from multiple sources and analyze it for patterns that indicate an attack is in progress. They also provide a range of automated responses to such attacks.

The rise of smart phones and the broader BYOD trend has rendered traditional firewalls almost obsolete, and a host of new technologies and products has arisen to protect sensitive data when it's accessed remotely.

Again, these are only examples of the many new options companies need to evaluate in order to protect their data. Keeping up to date on the latest developments can take substantial time and energy, but it's an important task with huge business implications. Some midsize companies hold the belief that they don't have this obligation. They think that because of their relatively small size, they are unlikely targets. Nothing could be farther from the truth. In fact, hacking organizations are aware that this attitude exists, and they exploit it every day.

Midsize companies are at a particular disadvantage because they typically lack the resources needed to give security the sheer number of hours it requires. And that isn't the only problem. Midsize companies also frequently suffer from a lack of experience in the area of security technology. This, by the way, is a problem that is hard to fix through hiring, because the demand for security professionals is so high in today's market.

Managed Security Services: A Better Option

Given the increasing complexity of threats, the plethora of confusing options for defense, and the lack of time, training and experience on most small IT teams, managed security makes a lot of sense.

Managed security vendors typically begin a relationship with an analysis of a company's security needs, which may include consulting services. Customers can then choose from a variety of services such as:

- Intrusion detection
- Threat management
- Log management
- Identity, authentication and access management
- SIEM

These will typically reside on an on-premise server, but be managed remotely. Alternatively, cloud options are available.

Managed security has a number of attractive benefits. To begin with, it puts the safety of a company's data in the hands of people who focus 100 percent on security issues. These people don't see it as boring, or a task that has to be completed so they can get on to something more interesting. Also, they are typically on duty 24/7. This means, for example, that if an intrusion is detected in the middle of the night, there will be people available to handle it instantly, rather than react the next morning when it may be too late.

"The rise of smart phones and the broader BYOD trend has rendered traditional firewalls almost obsolete, and a host of new technologies and products has arisen to protect sensitive data when it's accessed remotely."

Another advantage of managed security is that the companies providing it typically invest in the most advanced technology available —technology that they are particularly qualified to evaluate as it is at the heart of their business.

Finally, because managed security providers achieve significant economies of scale, they can often provide companies with the security they need at a lower price than would be possible were those companies to deal with it directly.

Choosing the Right Managed Security Provider

For all the benefits managed security offers, it's important to remember that not all managed security providers are created equal. Features and capabilities to look for when making a choice include:

- **Full Service.** Midsize businesses in particular will do best to seek a provider that not only offers protection, but takes a partnership approach to designing and implementing a system that's both appropriate and cost-effectively.

- **Industry Awareness.** Security needs vary dramatically from industry to industry, and the provider must have a thorough understanding not only of general security requirements, but industry-specific requirements that must be met to ensure regulatory compliance.

- **Flexible Options.** Managed security is not a one-size-fits-all proposition. For example, the needs of two manufacturers or two banks will vary considerably, even though they may be in the same vertical market. The right provider will offer flexible options and be able to customize its security solutions to meet individual companies' specific needs. In particular, this means being able to deal with increasingly complexity such as that found in hybrid IT environments.

Unfortunately, security in the 21st century has become a complex resource-draining activity, and IT departments often have to choose between security and other pressing projects that the business needs to move forward. Managed security offers a new option that removes a burden from the IT department while providing a high level of protection. For more information on this important new option, please visit www.sungardas.com/Solutions/managed-security-services/Pages/managed-it-security.aspx. ■

About Sungard Availability Services

Sungard Availability Services provides managed IT services, information availability consulting services, business continuity management software, and disaster recovery services.

To learn more, visit www.sungardas.com or call 1-888-270-3657

CLD-EBO-021

