

## Security Issues for Application Service Providers

Look past the hype and like many you will see that application service provision is considered good for both ASPs (Application Service Providers) and customers. Economic and technological pressures drive this outsourcing of business applications over the Internet. These include a chronic shortage of IT skills, constant hardware and software investment/upgrades, pressure from competitors, and the need for greater financial control.

Using an ASP brings major benefits to large corporations and small and medium sized enterprises (SMEs). By outsourcing applications to ASPs and renting software on a per seat, per month basis, companies are free to:

- focus on their core competencies
- use new business applications faster to increase responsiveness
- control cash-flow and software costs
- eliminate IT headaches from finding staff to rolling out new applications across multiple sites
- utilize the latest supported enterprise, e-business, office productivity and messaging software.

ASPs meanwhile consolidate their applications and support packages and receive a guaranteed monthly income from customers while delivering applications on a global scale.

As with any new product or service, however, particularly a new Internet service, what should you look for as a customer when selecting an ASP?

- Reliability - 99.999% or 100% availability
- Scalability - automatic network load and application load balancing, capacity planning to ensure applications are available when needed
- Data management - automated backup, storage management, data and disaster recovery
- On-line support and documentation
- Performance - network tuning, application monitoring, operating system tuning
- Rapid deployment and ease of new user additions
- Ability to upload and download data
- An acceptable price structure
- SLA agreement covering service levels, speed and availability and problem resolution standards to ensure a mutually acceptable performance.

First, reliability. Choose a company with a good service level agreement, bandwidth/capacity, load balancing, data backup, technical support and disaster recovery

facilities. In many cases, everything you do in terms of web hosting and applications will be held by the ASP. If the ASP has an outage, your business may lose substantial revenue and your reputation will be tarnished, even if the ASP was at fault.

Second, specialty. Find an ASP that hosts the solution and applications you want and preferably a solution that is web-enabled rather than an adaptation of a client-server solution. Increasingly, ASPs are building clientele in specific vertical markets such as retailing or IT manufacturing, as the market develops. These vertically integrated suppliers will have a greater understanding of your business and its requirements.

Third, business need. As with ISPs, assess your requirements. Do you need high levels of customer support or does your in-house ITS staff intend to back up the ASP service? How great is the need for confidentiality and security? Do you need flexible pricing tailored to your specific business? Does the ASP have automatic load balancing to ensure you can use applications when you need to? Can you upload and download databases easily?

Fourth, hosting. Establish the level of hosting you require: ASPs deliver economies of scale by providing standard applications to multiple users. Your site may be hosted with others on a single server (shared hosting); it may be on a single server provided by the ASP, but connected with others to the ASP's high speed network (dedicated hosting); or on a server your company purchases and installs itself (collocation) which again makes use of the ASP's network capacity and expertise. These all have different cost, performance, support and security implications.

Fifth, but most importantly, security. Choose a secure host environment. With threats to Internet based businesses increasing, the dependence of customers on outsourced applications adds a further risk to businesses for which the Internet is a mission-critical communications and sales medium. In the current climate, Web servers are being attacked for their content (financial assets and information) and as gateways to backend systems and networks. Given the conduit from the Internet to concentrations of application software and customer data, ASPs can be considered high risk from threats including theft, manipulation of stocks, manufacturing processes, ordering, sales information, etc.

With co-hosting, there is also the problem of confidentiality and security of intellectual property. If you choose a vertical market ASP it is highly probable that your chief competitor's site and applications may be hosted on the same server as your own. This opens the way to theft or manipulation of applications related to product design, manufacture and pricing through to accounts, customer and supplier databases, personnel records, payroll and others.

ASPs as central applications repositories are also at risk from new, immature versions of software, rapidly developed and deployed to meet changing customer requirements. Such software gives hackers the opportunity to exploit bugs to gain system-wide access.

In 2006, a Computer Security Institute/FBI study of 616 large organizations including banks and government agencies confirmed that 52% of respondents had experienced security breaches over the last 12 months. The total losses reported in this study exceeded \$52 million.

The critical questions when looking at ASPs is, "What would make us believe that an ASP architecture relying on Internet connectivity to a shared resource would be more secure than current e-commerce systems?"

So, as an ASP, how do you convince your customers your site is not prey to hackers or their sites open to intellectual property theft and misuse? What security measures do you employ to keep competitors apart and hackers out?

ASPs recognize that along with products, pricing, reliability and support, security is key to their commercial success. The right security can give an ASP an edge over its competitors, particularly where the ASP is hosting a number of competing customers.

So what security technologies do ASPs employ? Common security practice advocates security, firewalls, encryption/PKI, intrusion detection and host security applications to provide partial hardening of server operating systems.

This traditional security model is ill suited to the ASP environment that must deliver high security and service standards at low customer cost. Its complexity and non-scalability to meet growing business means it is costly to install, staff and maintain while multiple devices reduce application performance. Its security is also ineffective. Firewalls, encryption, IDS and limited host security are insufficient protection against high stakes cyber criminals.

However, a new security paradigm is in place. Ideally suited to the simplified, cost-effective ASP environment, trusted operating system (TOS) security eliminates the need to invest in numerous security technologies. The TOS solution delivers all the benefits ASPs are looking for:

- effective foundation security
- high performance
- scalability to rapidly accommodate new users and applications
- low levels of investment in systems and manpower
- customer savings.

Installed on an ASP's web and application servers, TOS security

- protects the system from flaws in commercial software
- protects applications from other potentially flawed applications
- limits applications to authorized functions
- limits and contains damage from bugs in immature, web-enabled applications
- protects from manipulation of administrator accounts.

In effect, an TOS enables ASPs to create secure and completely isolated virtual machines. Using an TOS, multiple compartments can be created for applications and web sites, some or all of which can have access to intranets or extranets. Multiple customer sites can be hosted on the same server. If a hacker or customer attempts to tamper with another compartment on the server he is prevented from leaving the compartment to

which he has access by the TOS. No hacker or customer can exploit bugs in commercial software to break out of one compartment into another. Thus a resource that has access to the sales application cannot access ERP or human resource functions. By the same token a customer cannot use an application to access a rival's site or databases.

As a further safeguard, trusted operating systems allow administrators to isolate system resources, applications, and administrative functions so that security holes and programming errors in software cannot be exploited to gain system wide access. Even if one compartment is compromised, the damage is contained within that compartment, and cannot compromise the system as a whole.

The simplicity and multiple hosting security provided by a TOS deliver: a low management burden for the ASP; low initial and lifecycle costs; high availability (as there are fewer components to fail); high levels of administrative control; high levels of privacy and data integrity for their customers. This is demonstrated by the three ASP environments below:

ASP Solution	Customer Cost	Initial Customer Investment	Administration/ Maintenance Costs for ASPs	Server Architecture	Security Risk
Shared server	Low	Low	Low	Complex	High
Shared servers (with TOS)	Low	Low	Moderate	Moderate	Low
Server farm (each company with own server)	High	High	Moderate	Simple	Moderate

#### ASP Solution 1 - Shared Server

In the case of shared servers there are benefits of low cost per customer, low initial customer investment and low administration/maintenance costs for the ASP. However, the security of individual customer data is low and the risk high. This solution also requires complex architecture to support multiple customers and applications in a shared environment.

#### ASP Solution 2 - Shared Servers with Trusted Operating Systems Installed

With shared TOS-protected servers installed, customers and ASPs achieve the joint benefits of very high security with low cost per customer as a result of shared software licenses, low hardware costs and low initial customer investment. A TOS also has moderately simple architecture and moderate administration and maintenance costs for the ASP.

#### ASP Solution 3 - Server Farm

Within a server farm, each company has its own server. Thus the architecture is simple and there are moderate administration and maintenance costs for the ASP. However, the cost per customer and initial customer investment are high due to high hardware costs from multiple servers and the need for multiple software licenses. Bugs in commercial software also compromise the security of individual customer data.

The bottom line is that customers expect products from ASPs to be easy to use, reliable, well supported, well resourced and responsive to customers' changing needs. The expectation is also that applications and data will be secure. With Trusted Operating Systems, ASPs and customers receive all the benefits of shared applications, with risk *and* at minimum cost.

#### **About Argus Systems Group**

*Argus Systems Group, a privately held company headquartered in Savoy, Illinois, offers a full suite of e-commerce security solutions and applications including PitBull® Foundation® and PitBull LX®, both based on trusted operating system (TOS) technology. Argus is committed to providing state-of-the-art security solutions for Internet-based computing environments. Argus supplies the only Common Criteria and ITSEC certified trusted platform available to support multiple platforms, from desktop to enterprise server, in a networked configuration.*

*For more information about Argus Systems Group, visit the Company's web site at [www.argus-systems.com](http://www.argus-systems.com). Email [info@argus-systems.com](mailto:info@argus-systems.com). Or contact Argus Systems Group at +1-217-355-6308.*