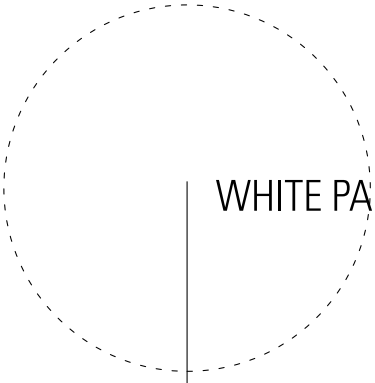
Aventail

# Security for Application Service Providers




www.aventail.com
Tel 206.215.1111
Fax 206.215.1120
808 Howell Street
Second Floor
Seattle, WA 98101

## Overview

Outsourcing is nothing new. Time sharing services for data processing have been around for some time. EDI applications have been at least partially outsourced to value-added network providers, and Web site hosting has been extremely popular. The next big variation on these themes is application hosting.

A number of service firms, large and small, are positioning themselves to be application service providers, or ASPs, to take advantage of a potentially very lucrative opportunity to extend client/server, Web, and object-oriented applications from their facilities to potential clients over the Internet. They bundle a packaged software product with related IT consulting services and deliver it to many clients. Most of these ASPs have no trouble identifying which applications to offer or which clients to target. The key component that has not been apparent is how to provide adequate security and management to enable this new business model.

### The Value Proposition

The most recognizable value proposition ASPs can offer their clients is the ability to derive all the value of an application without the burdens associated with ownership. This simple, attractive message typically takes hold with companies interested in applications like PeopleSoft Human Resources Management Solution, SAP R/4, and Lotus Notes, because those applications can require significant infrastructure changes, a lengthy and complex evaluation cycle, and a skilled staff to implement and maintain the final customized solution.

Application hosting mitigates the cost and disruption of the consulting and integration services that inevitably accompany large ERP systems. Considering that those services can easily exceed the cost of the actual software, using an ASP makes fiscal sense. Also, the time it takes to implement a solution is greatly reduced with an ASP because the requisite software and hardware are already in place at the service provider's location.

The entire process of implementation is streamlined, which allows a business unit or department to take advantage of an application without having to go through many of the internal processes imposed by their own IT organization. For instance, a human resources department can use an ASP to get the benefits of PeopleSoft's powerful HR software without having to assign a large internal team to get up-to-speed on the software or without having to hire expensive external consultants who will not necessarily be available to maintain the application over time. From a maintenance perspective, ASPs, who are closely linked to integrators, simplify life for enterprise customers by

giving them the ability to demand service levels, features, performance, and regular updates from a single source.

The financial model ASPs can offer their clients is also appealing. ASPs essentially lease their services and applications to their clients, eliminating the substantial capital expense that is usually associated with purchasing the application. Instead, clients can draw funds out of their operating budgets, negotiate longer-term contracts and introduce more predictability into their IT expenditures.

**The Security Mandate**

In order for ASPs to be successful in propagating this new model, they have to ensure the highest possible security in a number of areas. In short, the key security elements they need to provide include:

- **Authentication** – *Ensuring that the user trying to access the application and the information is who he or she claims to be.*

  Being able to identify exactly who each user is on the other end of an application is paramount to security. All the encryption in the world won't protect a company if the wrong people have access to critical data. Authentication is potentially troublesome for ASPs because while they may have a preference for a particular authentication technology, they have to be able to support multiple methods to accommodate their customer base. It is the customers who decide what security policies are implemented by the ASP for their particular data. Some clients want simple user-name and password security, while others want to use hardware tokens, of which there are several different, incompatible brands on the market. Still others want to use a Public Key Infrastructure (PKI) to authenticate users. Several PKI vendors, including leaders Verisign and Entrust, have very different implementations of the technology. ASPs need a security architecture that allows them to use multiple and disparate authentication types based on client requests.

- **Access Control** – *Ensuring that users coming in are accessing only appropriate systems and data, and are not able to engage in activity that could compromise a defined security policy.*

  ASPs need access control in order to make sure that their clients are only accessing systems and information that belongs to them. ASPs need to be able to govern the systems that can be accessed by particular users,

protocols that can be used, times when the user can connect, the Web pages that can be viewed, and so forth. Some clients also require customized application filters, which are a subset of access control. Essentially, ASPs need access control to sell their services, because it is highly unlikely that a prospect would use an ASP that does not appropriately regulate and restrict user activity at the hosting site.

- **Firewall Traversal** – *The ability to pass through a firewall or other system designed to prevent unauthorized access to or from a private network.*

  Almost every company, which means almost every prospect for an ASP, has a firewall in place to block unwanted access into its network. An ASP cannot dictate the type of firewall used by its clients, which range from packet filters to circuit proxies to application proxies. ASPs need to use security solutions that allow data to be exchanged securely with clients regardless of the type of firewalls used.

- **Non-Intrusive Client** – *Client software that does not modify a user's desktop applications or environment.*

  Any client software used by ASPs should be easy to install and administer, eliminating support headaches by making the software easy on the end user. More importantly, the client software should not modify any of the existing drivers, transports, or applications on the user's machine. The client should run transparently and allow users to authenticate once rather than for each application. Once authenticated, users should be able to easily access applications on the ASP network based on an access control profile that has been defined by either by the company or the ASP administrator. ASPs should look for client software that can seamlessly integrate with existing WinSock TCP and UDP applications and TCP/IP stacks.

- **Directed Communication** – *A method of communication that prevents the user's network from being vulnerable to attack from inappropriate network connections.*

  Directed communication, unlike encrypted tunneling, eliminates the risk of a "hacker's bridge" being formed because of open-ended, two-way connections. For example, if two companies choose to connect their networks using a technology that allows for communica-

tion that can be initiated by either side, they are creating a tunnel that implies mutual trust. If one of those companies connects to a third, the chain of trust is extended to that firm regardless of whether the first company intended that or not. ASPs want to be sure they are not creating faulty chains of trust between the multiple organizations connected to their facilities, many of whom may not have business relationships or may be competitors.

- **Encryption** – *Providing complete privacy of data in transit across the Internet*.

  Encryption technology is used by ASPs to keep sensitive data from being captured by eavesdroppers on the Internet. The longer the key length of the cryptographic algorithm, the stronger the encryption. Today, 128-bits is the strongest commercially available key length. In the United States and other European countries, there are legal limits on the strength of the encryption that can be exported, and until this controversial topic is resolved, ASPs need to be able to offer multiple levels of encryption to extend their services to users outside of the US and Canada. Also, because encryption can affect performance, being able to turn off encryption when it is not required can be useful.

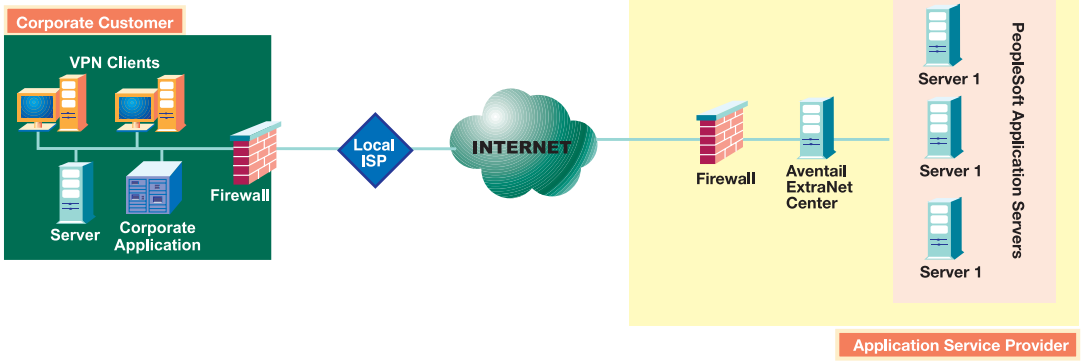
- **Data Integrity** – *Protecting data in storage and in transit from being altered.*

  Data integrity is partially covered by most encryption technologies. SSL for instance has mechanisms built into it to ensure that data is not changed or damaged in transit between the point of encryption and decryption. ASPs need to ensure that information remains intact from one end to another. They also need to take steps to ensure that the information on their sites is not altered while in storage.

**The Aventail Advantage**

Aventail Corporation provides extranet solutions designed to meet the security and management requirements of the new ASP market. The success of an ASP depends greatly on the strength and flexibility of the security and management architecture they choose. ASPs need highly secure extranet technologies that allow them to customize security policies for their clients and traverse multiple firewalls while remaining transparent to end users. Beyond that, they need a solution that does not tie them to IP addresses since their clients may have illegal IP addresses or addresses that overlap with the Internet or ASP. The solution also needs to be able to traverse multiple firewalls and have a low-impact client that is transparent to end users.

## Sample ASP Extranet




Aventail ExtraNet Center is uniquely positioned as the security and management platform of choice for the ASP market. Aventail ExtraNet Center provides the greatest combination of transparency, security, and flexibility available for the successful deployment of extranets and shared applications. Aventail has received awards and industry recognition for providing the most comprehensive and detailed security policy engine on the market. Aventail supports over 16 authentication types and multiple encryption ciphers. Aventail's architecture allows ASPs to tightly govern users' activities and protect all the applications and data residing at their location while offering their clients the greatest variety of applications and services.

Aventail ExtraNet Center provides ASPs with the ability to create a sort of security conduit for any TCP/IP application, not just HTTP traffic, in such a way that ASPs can deploy new applications at will without having to re-implement security for each application. HTTP-only extranets limit the type of applications that ASPs can provide, whereas Aventail's solution enables ASPs to leverage full client/server applications and applications built on platforms like CORBA and D-COM, in addition to Web applications.

Aventail ExtraNet Center was designed with a directed architecture that eliminates transitive trust issues, and thus reduces the liabilities for ASPs and their clients. This unidirectional connection is the result of using the SOCKS v5 security protocol, the

authenticated firewall traversal standard of the IETF that operates at the session layer of the OSI networking model. It links an application to a network as opposed to tying a machine to a machine. Operating at the session layer allows ASPs to separate themselves from problematic IP addressing issues and enables seamless firewall traversal.

## Summary

Application service providers are emerging as an effective channel for providing sophisticated applications to companies with specific needs. Their value-add is about providing total business solutions for processes like supply-chain management and partner collaboration. A core differentiator of ASPs is their ability to provide a high level of security and management.

Analysts are optimistic that the value proposition offered by ASPs can be realized. Aventail is optimistic that ExtraNet Center can offer an unmatched platform for creating secure connections between ASPs and their users. Aventail ExtraNet Center's flexibility and ease of use make it an appealing solution for ASPs trying to deliver premium service to their clients.

---

Aventail is at the forefront of providing extranet security and management solutions. For questions or comments, please call 877-AVENTAIL or send e-mail to info@aventail.com. For more information about the company or its products, please visit www.aventail.com.