



**Managed SSL VPN Services
In Key Vertical Industries**



Introduction

There is broad consensus that managed SSL VPN services is the ideal solution for remote access. But which vertical markets have been the fastest to deploy this business transforming technology?

This paper seeks to answer this question by focusing on examples of how companies have implemented SSL VPNs in specific vertical markets and understanding the impact to their business, so that businesses can decide how to leverage it to improve their productivity and competitive advantage.

Industry Experts

There is no shortage of industry experts who have gone on the record to embrace SSL VPNs, even going as far as to declare that SSL is the future of remote access.

Here are a few and the reasons they cite:



SSL is The Future of Remote Access

Robert Whitely

“SSL is simplifying remote access and enabling a level of simplicity and productivity that IPsec could not offer. Specifically SSL VPNs provide increased:

- *Levels of granularity.* Because it's at the application layer, SSL can track more information about the users — such as location, type of computer, and OS — and provides more granularity than IPsec. This allows enterprises to comfortably extend remote access to new areas like Internet kiosks or partner sites where the level of granularity assures the users have access to only the necessary resources.
- *Business Continuity.* Whether it's a severe ice storm, hurricane or earthquake that affects one region for a limited period of time or a national emergency, like a terrorist attack or pandemic, businesses need to provide employees with a way to access business-critical applications and resources from wherever they may be. SSL's clientless access enables them to log in from any home PC or hotel business center via a web portal that can also include vital information on coping with the emergency.
- *Device types.* SSL VPNs are capable of running on a standard browser. As a result, a wide variety of client types like PDAs and cell phones can securely connect remote users via standards-based browsers instead of proprietary IPsec clients that might not be installable or are too resource intensive.”



“Application-layer (SSL) VPN products attempt to solve a deployability and management problem that many IPsec VPN users face. IPsec clients can be a pain to manage, and they provide more access than a lot of users need, since many only access a couple of basic applications. Application-layer VPN products offer an easy-to-manage, easy-to-deploy solution in these environments. SSL also makes good sense in the extranet environments, as it gets around the uncomfortable problem of installing software on computers that don't belong to you.”

- Jeff Wilson, Executive Director



“SSL VPNs are gaining momentum in the secure access market because of their clientless access, proven security, and ease of management benefits. The SSL protocol is well suited for remote access and extranets, largely because it is relatively simple to deploy.”

- Dave Kosiur, Senior Analyst



“We expect many companies will be attracted to a service-based approach for their VPNs. Reduced administrative requirements, the ability to offload or completely avoid equipment purchase and deployment, and quicker time to market with a comprehensive set of capabilities are all very compelling value propositions.”

- Mark Bouchard, Program Director

Business Drivers

As many of the analysts above have pointed out, there are several key benefits that SSL VPNs provide that distinguish them from traditional IPsec VPNs. These benefits relate directly to several specific business drivers that are critical factors within certain vertical markets. Here are three main attributes of SSL VPNs and the types of businesses that can benefit from them:

Ubiquitous Access - Access From Any Device, Anywhere

Clearly the most significant driver for SSL VPNs is having a population of remote users, particularly ones that are mobile and use various types of devices. Traveling executives can use an SSL VPN to securely access all corporate resources using their personal or company-provided PCs and PDAs. And, they can use any type of Internet connection, including 3G wireless and WiFi HotSpots, which are common in many airports, hotels and cafes. This makes an SSL VPN the natural choice for companies with either high-paid professionals, such as lawyers and senior executives, or field services personnel, including technical services and engineering firms. SSL VPNs also provide the unique ability to traverse firewalls, making them ideally suited to professionals that need to access one company's resources from within another company's network, such as consultants, doctors and sales representatives.

Control - Application-level Access

Legacy remote access solutions connect users to the network, whereas SSL VPNs connect users to specific applications. The implications of this fundamental difference are profound. Since SSL VPNs provide application-level access, they are ideally suited to companies with a wide range of applications and/or users that only need access to a subset of these applications. In many cases, IT managers only want to grant access to the applications that an employee needs to his or her job. For instance, sales representatives may only need access to a CRM application, email and the company intranet. Nowhere is this more pronounced, though, than in industries where many of the remote users are not employees. In these industries, companies need to grant customers, suppliers and business partners access to specific applications – but they certainly do not want to grant them access to their entire network. This scenario is prevalent in Manufacturing, for customers and suppliers, and in Healthcare, where doctors frequently need access to data residing in the multiple hospitals where they practice. Some SSL VPN technologies have sophisticated policy engines that allow IT Managers to map resources to individual users based on both who they are (authentication credentials) and the security settings of the computer they are using (see Security below). This capability is of utmost importance when granting access to non-employees, who by definition do not have a company-provided (i.e., trusted) PC. These sophisticated SSL VPN technologies can even provide the ability to control the level of access for any user in any setting, and they provide detailed audit trails for compliance reporting.

Security – AAA & Endpoint Control

Most SSL VPNs offer the robust security required to extend business applications to employees, business partners, and others. Traditional security models address AAA (Authentication, Authorization & Access). Some SSL VPN offerings, though, offer additional security in the form of End Point Control.

- Authentication – SSL VPN technology is compatible with all forms of authentication from user name and password to any of the strong authentication alternatives (certificates, tokens, etc.)
- Authorization – SSL VPN technology is compatible with any authorization store including Active Directory, LDAP and Radius

- Access – SSL encryption is arguably the most widely used encryption technology used to protect billions of dollars of e-commerce transaction annually. A variety of encryption algorithms are available for SSL VPNs, including DES and 3DES.
- End Point Control – SSL VPNs extend access to *both* corporate computers (laptops, PDA's, etc.) as well as non-corporate computers (home PC or Macs, PDAs, kiosks at trade shows or airport lounges, business partner computers, etc.). Determining how these devices are configured and whether they represent a security risk is a crucial step prior to granting access. Very few SSL VPN products provide the in-depth scanning tools to assess risk by looking for malware (Trojans, keystroke loggers, etc.), ensure compliance by examining defensive tools to make sure that they are current and operational (anti-virus, personal firewall, etc.), and offer the level of control required to respond to risks.

The ideal security model allows customers the flexibility to define their own customized security model and build a flexible policy that grants access relative to the security of each user's computer.

Key Vertical Markets

Healthcare

The healthcare industry faces a seemingly insurmountable challenge: to provide doctors, mobile caregivers, technicians, transcriptionists and others with instant electronic access to information from anywhere, while also meeting strict guidelines for keeping patient information confidential. Tight budgets and limited IT resources only add to this challenge.

SSL VPNs enable hospitals and other caregiver organizations to improve patient care by providing physicians and other hospital staff anywhere with secure remote access to patient records, even those stored on legacy terminal applications. Specialists can review X-rays and other clinical data remotely over a secure network. In addition, granular access helps to meet the logging and auditing requirements of HIPAA.

SSL VPNs improve patient care and speed up administrative processes by offering secure access to critical information, such as patient records, lab results, real-time cardiac monitoring and radiology reports from anywhere — including from PCs, kiosks, laptops, or other network-enabled devices. They provide anywhere access to any application — including Web, client/server, file transfer, terminal servers, and mainframe. That includes applications from vendors such as Cerner, Epic, McKesson, SMS, IDX, Misys, Meditech, GE Medical and others.

You can use MegaPath's SSL VPN services to provide users with secure access to applications that streamline:

- Enterprise care management
- Laboratory radiology (LAB/RAD)
- Financial or billing information
- Practice management
- Case management
- Utilization management
- Electronic medical records (EMR)
- Cardiac monitoring

MegaPath's SSL VPNs provide data encryption and authentication, granular access control, policy management, logging capability, and a flexible authentication architecture that can help healthcare organizations comply with the Health Insurance Portability and Accountability Act (HIPAA) regulations for security and privacy. Applicable security features include:

- Strong data encryption for remote VPN access to applications or network resources
- Strong authentication, including support for two-factor authentication
- Centralized policy management across all back-end applications or resources
- Granular access control, down to the specific user, resource, or URL
- Proxy and aliasing technologies to completely hide the back-end network from remote users
- Operating system hardened against external threats
- Administration portals for greater process automation and control
- Auto-detection of personal firewalls and/or virus protection software, so you can make sure these are actively running prior to allowing a user connection

Education

Institutions of higher learning have significantly increased their attention to Internet privacy, security and cyber terrorism. Expanding their ability to share up-to-date information instantly has become critical. Schools and universities must be able to provide secure access to information for students, staff, contractors, and citizens, increasing the demand for solutions that provide access while meeting security and privacy requirements and supporting the wide application types found from school to school.

If you are an IT decision maker for an educational institution, you need to provide secure access to information for students, staff, researchers, and more, quickly easily, and cost-effectively, while maintaining strict privacy regulations on student data and other confidential information.

MegaPath's SSL VPN service can help, with proven technology that provides an integrated method for clientless access to Web applications, client/server applications, and enterprise file shares. Our solutions provide:

- SSL encryption, the most widely used method, available on virtually every browser and platform
- Broadest range of secure remote application access currently available from an SSL VPN
- Enforced end-point security policy from corporate laptops, such as verified anti-virus or personal firewall use
- Significantly reduced 1st tier support costs compared to traditional IPSec VPN solutions

Manufacturing

Manufacturing is changing — with more dependence on access to real-time information for business partners, supply chain partners, employees, and customers spread across the globe. Driving the need for secure, anywhere access to applications are increasingly mobile employees, far flung offices and facilities that need to be in close touch, the growing use of wireless communication devices in manufacturing, and outsourced and contract work requiring close collaboration. Manufacturers need to set up efficient extranets to gain efficiency in the supply chain, and MegaPath's SSL VPN solutions are the quickest, easiest and most cost-effective way to achieve this goal. SSL VPNs can even enable secure access to network application from wireless handheld devices on the manufacturing floor.

MegaPath's secure clientless SSL VPN solutions meet the unique demands and requirements of manufacturers by providing an integrated method for secure access to any user, from anywhere, from any device, to any resource. The SSL solutions are easy for the end user, resulting in lower support costs, and

they are also less burdensome for IT management because they do not require reconfiguration of your network and eliminate firewall traversal or NAT issues commonly experienced with IPSec VPNs.

MegaPath provides manufacturers with:

- Increased employee and partner collaboration for faster design-to-production cycles to ensure their products are in-tune with the market and competitively positioned
- Immediate, secure access to up-to-the-minute information, reducing isolation and increasing the productivity of far flung manufacturing sites, sales reps, and mobile employees.
- Granular control of resources and applications for contract manufactures so they can get the right information they need to work efficiently
- Remote access for "follow the sun" engineering and development teams across the globe who can work on projects 24 hours a day

Law & Professional Services

If your business is providing legal services, management consulting, accounting, IT consulting, auditing or some other professional service, your top assets are your people. And these people are on the road most of the time, meeting with clients and doing their job. So you need to make their every minute count by ensuring that they can stay connected to e-mail, use internal applications, update documents, and search internal knowledge bases. MegaPath's SSL VPN is designed to help your traveling consultants do just that – securely connect to the resources they need from anywhere, using any device.

MegaPath's SSL VPN solutions enable:

- Remote access from everywhere, even behind the firewall at your customer's site.
- Use of broadband access whenever available, for the fastest connection possible.
- Secure use of wireless hotspots, at cafes or the airport, to minimize downtime while waiting.
- Secure remote access from non-corporate laptops, for added convenience from kiosks and guest machines.
- Enforced end-point security policy from corporate laptops, such as verified anti-virus or personal firewall use.

MegaPath's SSL VPN service has already helped leading professional services customers give their users the secure, flexible remote access they need.

State & Local Public Services

The government has significantly increased its attention to Internet security and cyber terrorism. Expanding its ability to share up-to-date information instantly has become critical. Government agencies must be able to provide secure access to information for government employees, contractors, and citizens, increasing the demand for solutions that provide access while meeting government security requirements and supporting the wide application types found from agency to agency.

If you are an IT decision maker for a government agency, you need to find solutions with a proven track record of delivering solid results. MegaPath's SSL VPN solutions, leveraging Juniper's and SonicWall's (formerly Aventail) technology, provide an integrated method for clientless access to Web applications, client/server applications, and enterprise file shares that's unmatched by any other SSL platform in the industry.

MegaPath's SSL VPN solutions enable:

- Improved communication across agencies, as well as increased collaboration with the private sector—without the hassle of managing VPN clients
- Address government-mandated telecommuting requests with end-point security policy for personal PCs, such as verified anti-virus or personal firewall use
- Meet increasing federally mandated security requirements, such as FIPS for the U.S. government
- Broadest range of secure remote application access currently available from an SSL VPN

MegaPath is well positioned to deliver government agencies with the secure access solutions that are required, along with the flexibility that is necessary to access information.

Conclusion

By now you are well aware of the types of businesses that can benefit from this business enhancing technology. However, the technology in-and-of-itself is not enough. Like any technical solution, it needs to be properly designed and implemented, and then professionally managed. MegaPath has over a decade of experience deploying and managing SSL VPN services for some of the largest companies in the world. We remove the hassles, risk and potential delay associated with a do-it-yourself approach, and allow companies to focus their resources on projects that are unique to one's business and cannot easily be outsourced. Plus, there's no equipment to purchase, just a simple, predictable monthly expense that's easy to budget. So, if you want to make sure your security policies are air-tight and your SSL solution is scalable and reliable, choose MegaPath's Managed SSL VPN service.

If you have any questions regarding the content of this paper, or MegaPath's SSL VPN solutions in general, please contact your account manager or 1-877-MEGAPATH.