Executive Summary

This paper illustrates how companies can deliver more effective access to many teleworkers and day extenders by augmenting traditional VPNs with Citrix® GoToMyPC® Corporate. Today, many companies are moving to Web-based VPNs and managed services to overcome legacy VPN deployment barriers and reduce costs. GoToMyPC Corporate embraces both trends, helping companies to deliver more convenient, cost-effective secure remote access to targeted users.

GoToMyPC Corporate is an attractive solution for employees who require the same desktop environment, whether working at home or the office. By providing authenticated, encrypted access to office PCs and existing applications, GoToMyPC Corporate can help these workers get their jobs done more productively, from any Internet-connected system.

Companies with VPNs can use GoToMyPC Corporate to augment their remote access strategy by offloading workers who not only cause the greatest IT pain, but can benefit the most from secure remote desktop access. Because GoToMyPC Corporate requires minimal IT effort, it can help companies expand access to fringe users not eligible for VPN services due to the cost and effort required to manage VPN clients and laptops. By enabling secure remote access from any PC with a Web browser, GoToMyPC Corporate can help companies avoid the expense of issuing VPN-enabled laptops to workers who do not need a laptop in their business practice, but still require remote access. GoToMyPC Corporate can also be a convenient alternative to in-house VPNs for companies just getting started with secure remote access.
**Introduction**

Today, many employers offer virtual private network (VPN) remote access to corporate resources to increase productivity for mobile workers. However, as workforces have expanded and needs have grown more diverse, administrative complexity and costs have skyrocketed. In addition to business travelers, companies must now deliver secure remote access to teleworkers, day extenders and others working outside the office. To drive down costs while making secure remote access more readily available, many are now turning to Web-based alternatives.

GoToMyPC is an innovative Web-based managed service that leverages industry trends to speed deployment and reduce operational expense. GoToMyPC Personal is designed for individual use, while GoToMyPC Corporate adds features required to meet business needs for strong two-factor authentication and efficient, centralized control over large workforces. In this paper, we explore how remote access to corporate networks has evolved, why satisfying the needs of today's workforce requires a different approach and how GoToMyPC Corporate can serve as a convenient-yet-secure complement to remote access VPNs.

**The Remote Access Revolution**

New network technologies and business dynamics have changed the remote access landscape. Globalization, high-speed broadband and wireless and a rise in teleworking have escalated demand for anytime/anywhere access to business networks. Employee remote access increases workforce productivity and competitive edge, but it also raises security and cost concerns.

Early remote access was limited to dial-up by business travelers. This was fine when sessions were short and users were few, but telecommunication costs soon became prohibitive. By year 2000, 1 in 5 companies had shifted remote access onto ubiquitous, inexpensive Internet access accounts to eliminate 800-number and long-distance charges. To ensure the privacy and integrity of business data sent over the Internet, VPN client software was installed on company-managed laptops, tunneling to IPSec gateways located at the corporate networks' perimeter. These VPNs cut toll charges, but, as the workforce continued to grow, so did administration costs.

Residential broadband significantly increased the number of workers demanding remote access. According to Gartner, 1 in 3 U.S. employees teleworked in 2005; the number of teleworkers is expected to reach 100 million worldwide by 2008. Many more work occasionally from home at nights and on weekends. For most companies, issuing a laptop with VPN client software to every single employee would be prohibitive due to equipment purchase/lease and IT administration costs. And, while some employers have attempted to install VPN clients on home PCs, this approach has proven largely unworkable due to inherent security risks and significant administration complexities.

Furthermore, mobile workers have started using public PCs with high-speed Internet access, readily available today in hotels, airports and business centers. Installing a VPN client on a public PC is simply not an option, necessitating a completely different kind of solution: Web-based secure remote access. By leveraging the familiar Web browser, present on nearly every desktop, laptop and PDA, employers can avoid installing, configuring and updating VPN clients on remote devices. Web-based services also tend to be easier for employees to understand, launch and use.

To capitalize on surging demand for anytime/anywhere remote access, a new generation of SSL VPN products have emerged. However, like the IPSec VPNs that came before, SSL VPNs still require gateway appliances to be installed within the company network. In-house VPNs can require weeks or months to deploy; they need security-savvy administrators to configure, maintain and monitor them. Long-term investment in VPNs may be justified for a portion of a company's workforce, but it may not be the best way to meet every employee's needs, or to react rapidly to business changes that require immediate response.

For these reasons, secure managed remote access services are gaining popularity. Managed services can facilitate rapid deployment, free up capital, reduce ongoing operational costs and decrease the need for in-house security expertise. By outsourcing remote access services, companies can increase internal focus on their own business goals, leveraging the provider's infrastructure and expert staff to ensure the safety of business traffic over the Internet. According to Gartner, these benefits and growing concern over regulatory compliance drove the managed security services market to reach $1 billion in 2005.
GoToMyPC Corporate is a unique secure managed remote access service that capitalizes on these emerging trends to meet the changing needs of today’s business workforce. As a Web-based managed service, GoToMyPC Corporate can be deployed more quickly than any in-house VPN, with minimal IT impact. By leveraging Web browsers, employee desktops and strong two-factor authentication, GoToMyPC Corporate can also be easier to use and less expensive to operate than client-based IPSec VPNs. To appreciate why, let’s consider how GoToMyPC Corporate meets workforce needs for secure remote access.

**Secure Remote Access Users**

Over time, several distinct remote access user communities have emerged, each with different business objectives and access requirements. According to a 2005 Dieringer Research Group survey, mobile workers in the United States work from an average of 3.4 different locations, including homes, client sites, airplanes, outdoors and on vacations. To satisfy this increasingly large and diverse workforce, a one-size-fits-all approach to remote access may not be sufficient or cost-effective.

### Teleworkers

Teleworkers: Broadband use by teleworkers grew by 60 percent last year, increasing teleworking overall by 30 percent in 2005. Teleworkers require the same computing environment, whether working at the office or from home. This means high-speed broadband access for efficient communication. It means exactly the same desktop and server applications and configurations. It means seamless access to files, folders and databases back at the office. Anything less reduces worker efficiency and increases total cost of operation.

### Day Extenders

Day Extenders: Employees that rarely telework often log into the company network during the evening or on weekends. Employers are highly motivated to facilitate after-hours access because most experience noticeable productivity improvements. Day extender needs vary — for example, a software developer may have requirements similar to those described for teleworkers, while an IT administrator may need broad access to servers and devices at several data centers. Most of these users do not already carry company-managed laptops, and thus might not be considered eligible for VPN access. However, the majority of day extender business needs can be satisfied by enabling secure desktop remote access from that worker’s own home PC.

### Mobile Professionals

Mobile Professionals: According to IDC, the mobile worker population will top 850 million by 2009, representing more than one-quarter of the global workforce. Many will be field workers involved in sales, on-site consulting, support or delivery. Mobile initiatives have been strong in healthcare, financial, manufacturing, retail and education — verticals where employees spend little time at a desk. Mobile professionals require full-time access, but are less likely to have a desktop that requires duplication. Instead, they need convenient access to mobile applications that may accommodate low-bandwidth wireless Web access from small-footprint devices.

### Travelers

Travelers: Many employees have a primary workplace, but travel on business. Their needs differ from full-time mobile professionals. First, most travelers have a desktop back at the office. Second, application and data needs are similar to day extenders — many travelers can be satisfied with basic email, but others require access to their usual desktop applications and files. Access speed can range from low-speed dial-up (particularly for international travelers) to high-speed access from customer sites, hospitality networks or Wi-Fi hot spots. Travelers require dependable access from anywhere, unimpeded by differences in network topology or bandwidth.
GoToMyPC Corporate is an especially strong fit for teleworkers and day extenders because it provides remote access to the worker's own desktop back at the office — including his/her existing mailbox and mail client, enterprise applications, files and databases. For these reasons, and also because it can be used from any Web browser, GoToMyPC Corporate can also be attractive to travelers with at least 56 Kbps network access. In fact, GoToMyPC Corporate can be a better fit than either IPSec or SSL VPNs for many of these users. To understand why, let’s look at VPNs and how they compare to GoToMyPC Corporate.

**Secure Remote Access Solutions**

The following illustrates three solutions for providing Web-based remote access: legacy IPSec VPNs, SSL VPNs and GoToMyPC Corporate managed services. As we will see, all three can be used to deliver secure remote access, but they differ in ways that ultimately impact both the end user’s experience and the company’s total cost of operation.

**IP Security (IPSec) VPNs** extend the corporate network perimeter by using tunnels to add remote nodes — traveler laptops, teleworker PCs and mobile PDAs. IPSec uses various standard cryptographic methods to provide peer authentication, confidentiality, integrity and replay protection for IP packets that traverse the Internet. IPSec VPN gateways control all traffic exchanged between VPN clients on each remote host and authorized subnets inside the company network.

IPSec is a robust, general-purpose platform for accessing any IP-based client/server application. To meet business needs, many companies try to replicate each worker’s desktop on his or her laptop, including applications, configurations and data. However, doing so substantially increases IT costs for laptop leasing and software purchase, setup and maintenance.

Although IP address filters can be applied, most IPSec VPNs tunnel all remote node traffic into the company network. Designed with company-owned laptops in mind, this policy puts the entire network at risk of compromise by unmanaged home PCs that harbor viruses and trojans. To close this hole, IPSec VPNs are now being retrofitted with complex network admission controls that scan the remote end point for compromise before granting tunneled network access.

**Secure Sockets Layer (SSL) VPNs** also provide tunneled remote access, but with more granularity than IPSec. SSL provides asymmetric client/server authentication and standard confidentiality, integrity and replay protection for application data crossing the Internet. SSL VPN appliances control tunneled traffic between remote Web browsers, individual enterprise applications and data objects.
within those applications. By leveraging Web browsers, most SSL VPNs can avoid installing VPN client software, thereby reducing IT impact and cost.

SSL VPNs often use Web portals to let remote users interact with common business applications like enterprise mail and network file access. Support for other applications varies by product. For example, some require custom development to “Webify” less common applications. Others “port forward” just about any application over an SSL tunnel from client to server. To deliver this functionality without installed VPN clients, many SSL VPNs dynamically download Java or ActiveX code whenever the user logs into the VPN’s portal page. A few SSL VPNs use installed VPN client programs to expand application support through port forwarding, but most do not.

SSL VPNs excel at providing selective application and data access to authorized third parties, like contractors, customers, suppliers and other business partners. SSL VPNs also let travelers and mobile professionals enjoy “anywhere” access from public PCs, when permitted by company policy. But some workers may find SSL VPNs limiting. A teleworker may be required to do his job differently when accessing an application at the office or through the VPN. A day extender may unexpectedly find himself at home without access to data on his office PC. Finally, because capabilities vary quite a bit, it is essential to carefully consider current and future workforce and application needs when selecting an SSL VPN product.

IPSec and SSL VPNs can satisfy many remote access needs, but companies do not need to limit themselves to just these two options. Many can also benefit from using GoToMyPC Corporate to deliver secure remote desktop access to authorized PCs inside the company network. End users log into Citrix Online’s managed server from any Internet-connected computer with a Web browser, secured by 128-bit or stronger SSL encryption. This managed server “brokers” connection requests, establishing secure end-to-end sessions between remote users and host PCs.

During session establishment, GoToMyPC Corporate requires at least two levels of mutual authentication. Security-conscious companies can use an optional third level to authenticate the user with One-Time Passwords or RADIUS-enabled two-factor authentication methods like RSA SecurID and SecureComputing SafeWord. GoToMyPC Corporate’s viewer-to-host PC sessions are secured end-to-end with standard 128-bit NIST Advanced Encryption Standard (AES) encryption and SHA-1-based message integrity protection. Secret session keys, known only to the end user and host PC, ensure that not even Citrix Online can access company resources or decrypt session data.

GoToMyPC Corporate is a Web-based managed service. All infrastructure used to deliver this service is located at secure data centers, operated by Citrix Online. No VPN gateway is needed inside the customer’s network. Instead, a GoToMyPC service runs on each host PC. For firewall compatibility, only outbound sessions are used. However, companies remain in complete control over remote access services because GoToMyPC Corporate only lets authenticated users reach individually authorized host PCs. GoToMyPC Corporate account policies, configuration and usage reports are made accessible through a secure Web portal to company-designated, authenticated administrators.

As with SSL, GoToMyPC Corporate users enjoy “anywhere” access from any device with a Web browser and Internet connection, subject to rules defined by the GoToMyPC Corporate administrator. Unlike SSL, GoToMyPC Corporate users have direct access to all the applications already installed on their own office desktop, and all files and network shares normally accessible to that desktop. Users do not have to learn to use “Webified” application interfaces or clients to interact with enterprise applications and data; they can simply conduct their business as usual.

Like enterprise-class VPNs, GoToMyPC Corporate employs industry-standard encryption and optional two-factor authentication. Unlike IPSec, GoToMyPC Corporate does not directly connect a remote node to the entire company network — remote users can only reach authorized PCs that belong to them. And GoToMyPC Corporate is not limited to supporting client/server applications — all of the business applications and data that already exist on the worker’s desktop are readily available to that remote user, just as if he or she was working back at the office.

In short, where VPNs offer different access than workers actually need, GoToMyPC Corporate can leverage existing IT assets to deliver a simpler, more cost-effective solution. Teleworkers, day extenders and travelers can obtain direct access to the resources they need to do their jobs, without the expense of IT-managed laptops. And, although GoToMyPC Corporate cannot directly satisfy mobile professionals that lack office desktops, many mobile workers still find GoToMyPC Corporate convenient for access to their home PCs.
Understanding Secure Remote Access Cost

Because each workforce is different, the most cost-effective secure remote access solution (or combination of solutions) varies. Before adopting any solution, existing and proposed costs should be analyzed to verify positive return on investment. In general, most companies find:

- Capital equipment purchases drive set-up cost for in-house VPN solutions. Managed services that do not use customer premises equipment avoid this onerous up-front expense.
- Administration is the most significant recurring cost for any in-house VPN. Outsourcing administration to a managed service provider is often less expensive because providers can amortize their own costs over many thousands of users.
- Remote access alternatives that reuse existing worker desktops can eliminate corporate laptop purchase/lease expenses, as well as IT administration of those devices.

To more fully explore how various factors influence total cost of ownership, let's compare up-front and ongoing costs associated with IPsec VPNs, SSL VPNs and GoToMyPC Corporate.

1. **Internet Access**: Fees for dial-up, DSL, cable, wireless and global roaming play a significant role in total remote access cost, but they are common across Internet-based alternatives.

2. **Capital Equipment**: Any in-house VPN requires capital outlay to purchase hardware gateways. Most outsourced VPNs also require purchased or leased gateways, deployed at the customer premises. Network-based managed services — including GoToMyPC Corporate — leverage shared infrastructure, already installed at the provider's data center. Thus, companies can adopt GoToMyPC Corporate without incurring any capital equipment expense.

3. **Client Software**: Some VPN products require purchasing VPN client software. Enterprise IPSec products usually include Win32 clients, but non-Windows and SOHO IPSec client licenses must be purchased separately. Most SSL VPNs do not require installed client software, but some have a per-user licensing fee for Java or ActiveX code invoked through Web browsers. Either way, paying for client software often adds to VPN set-up cost. With GoToMyPC Corporate, there is simply no client software or license to purchase.

4. **Managed Service Activation**: Managed service providers charge activation fees to cover their own cost of deployment. Managed IPSec VPN activation fees usually cover gateway installation and per-user client setup. Managed SSL VPN activation fees cover gateway installation and per-application server integration or plug-in development. Because VPN setup is labor-intensive, managed VPN activation costs can be significant. GoToMyPC Corporate customers pay a very modest activation fee that reflects the maximum number of host PCs that can be used with the company's account. Customers can also spread service activation fees over time by activating additional host PCs as the workforce grows.

5. **Installation and Integration**: In-house VPNs require time and effort to install and configure VPN gateways and integrate them with firewalls, authentication servers and other corporate network devices. SSL VPN gateways are less network-disruptive than IPsec VPN gateways, but require installation and integration with authentication and back-end application servers. Because GoToMyPC Corporate has no customer premises equipment, it completely avoids this installation delay, effort and disruption. To enable two-factor authentication, the corporate authentication server is simply configured to listen to RADIUS requests from the host PCs accessed via GoToMyPC Corporate. Furthermore, because remote workers continue using applications on their existing desktops in the normal fashion, there is no need to retrofit applications or reconfigure back-end servers to allow tunneled access.

6. **Administrator Training**: Every remote access deployment requires competent administrators who have been trained to enforce corporate security policy and monitor usage. In-house VPN administration is a complex task that requires considerable systems and security expertise and days or weeks of training. GoToMyPC Corporate administrators need only learn how to use a simple, secure Web portal for group policy creation, user/host management and usage reporting. By exposing only the detail actually needed to implement the company's security policy, this managed service reduces administrator training by an order of magnitude.
7. **Laptop Leasing:** Companies with IPSec VPNs must issue IT-managed laptops to remote access users. SSL VPNs that do not require installed VPN clients may be used on home or public PCs, but some companies are uncomfortable with risks posed by tunneling from those unmanaged PCs. Some companies limit the applications and data that can be reached from unmanaged devices. Others issue IT-managed laptops to SSL VPN users so that they can control the business applications and PC security measures applied on that remote end point. GoToMyPC Corporate does not open a VPN tunnel into the company network, nor does it require VPN client or business application software on the remote PC. As a result, many GoToMyPC Corporate customers find that they can leverage office desktops to deliver remote access to workers without IT-managed laptops. This avoids laptop purchase/lease costs, as well as the burden of laptop administration and risk of laptop theft/loss.

8. **Ongoing Maintenance:** VPN gateways and clients require annual maintenance contracts for software patches, hardware/software upgrades and technical support. There are no ongoing maintenance fees associated with GoToMyPC Corporate. In-house VPN administrators must also maintain those gateways, troubleshoot failed connections and review gateway logs and reports. As a fully managed service, GoToMyPC Corporate does not require that kind of ongoing IT effort. GoToMyPC Corporate administrators may devote some time to help desk and report review, but customers find that these tasks involve very minimal effort.

9. **Ongoing Managed Service Fees:** Every managed service provider covers their own cost of operation by charging customers recurring service usage fees. Managed VPN providers typically charge fees that are based on the number of VPN gateways and maximum number of remote users. These fees vary, but large workforces can end up paying quite a bit for users that do not access the service. GoToMyPC Corporate customers pay recurring fees that are based on the number of host PCs that can be reached through the company account.

10. **User Adds/Drops/Changes:** Adding new users and deleting old accounts can be a very significant cost in large VPNs. With IPSec, this cost is dominated by the IT effort required to install and configure VPN clients. Many SSL VPNs do not require installed clients, but new users must still be configured into VPN gateways. With GoToMyPC Corporate, the administrator uses a Web portal to manage group policies and email user activation links. Each new user simply follows the link to invoke a wizard that activates the GoToMyPC service on their host PC. This self-service approach makes adding users fast and easy, while providing centralized corporate control over who can use the remote access service and how.

11. **User Training:** End users typically require training to learn how to use VPN clients or how to access applications through SSL VPN portals and “Webified” interfaces. With GoToMyPC Corporate, employees continue using their own desktops and applications — in exactly the same way they do back at the office. Customer experience shows that this approach reduces user training from an hour or more with IPSec to just minutes with GoToMyPC Corporate.

Projecting total cost of ownership is no simple task. Indeed, many companies that operate VPNs cannot easily assign a hard number to the annual cost of doing so. But reviewing cost factors can help companies make strategic decisions regarding secure remote access solutions. Business needs and time to deploy must also be considered. As many VPN owners have found, there are hidden costs associated with missed opportunity, unexpected downtime and reduced productivity.

For example, consider a company with a rapidly growing workforce. That company may examine legacy VPN costs to create a business case to add Web-based access to support workforce growth and remote access expansion. The company may then conduct a more detailed analysis to determine which user communities are best satisfied through an in-house SSL VPN, and which can be served more cost-effectively through GoToMyPC Corporate. In particular, workers who would benefit from remote access but do not already have or otherwise need company-managed laptops are prime candidates for GoToMyPC Corporate.

**Conclusion**

In the end, many companies will find that the “best” secure remote access solution is, in fact, a combination of solutions. Some power users, like administrators, may always need the broad network access afforded by IPSec. Mobile professionals and extensive travelers may require the granular, desktop-independent access delivered by SSL VPNs. Teleworkers and day extenders can clearly benefit from easy-yet-secure remote access to their own office desktop.
Long-term investment in a remote access VPN may be justified for a portion of a company's workforce, but it may not be the best way to meet every employee’s needs or to react rapidly to business changes that require immediate response. As we have shown in this paper:

• Companies with existing VPNs can use GoToMyPC Corporate to augment their remote access strategy by offloading workers who not only cause the greatest IT pain, but can benefit the most from secure remote desktop access.

• Because GoToMyPC Corporate requires no capital investment and very little IT support, it can help companies expand remote access to fringe users who are not eligible for VPN services due to the high cost and IT effort associated with managing VPN clients and laptops.

• By enabling secure remote access from any PC with a Web browser, GoToMyPC Corporate can help companies avoid the expense and risk of issuing VPN-enabled laptops to workers who do not need a laptop in their business practice, but still require remote access.

• Finally, GoToMyPC Corporate can also be a convenient alternative to in-house VPNs for companies just getting started with secure remote access.

**About The Author**

Lisa Phifer, Vice President of Core Competence Inc., has been involved in the design, implementation and evaluation of networking, security and management products for 25 years. At Core Competence, she has advised companies large and small regarding security needs, product assessment and the use of emerging technologies and best practices. She teaches about wireless LANs, mobile security and virtual private networking, and has written extensively for numerous publications, including Business Communications Review, Information Security Magazine, ISP-Planet, MobilityLoop and SearchMobileComputing.

**References**


**About Citrix Online:** Citrix Online, a division of Citrix Systems, Inc. (Nasdaq: CTXS), offers the leading Web-based access, support and collaboration software and services. The division offers Citrix GoToMyPC®, the easiest-to-use solution for remote, secure and managed desktop PC access over the Web; Citrix GoToAssist™, the industry-leading remote-support solution; and Citrix GoToMeeting™, the easiest, most secure and cost-effective solution for conducting online meetings. Citrix Online products are used by more than 10,000 companies worldwide, including Verizon Online, Siemens, Cablevision and Microsoft Business Solutions. The division is based in Santa Barbara, California, and is on the Web at www.gotomypc.com, www.gotoassist.com, www.gotomeeting.com and www.citrix.com.

©2006 Citrix Online, LLC All rights reserved. Citrix® is a registered trademark of Citrix Systems, Inc., in the United States and other countries. GoToMyPC®, GoToAssist™ and GoToMeeting™ are trademarks or registered trademarks of Citrix Online, LLC, in the United States and other countries. All other trademarks and registered trademarks are the property of their respective owners.