Increase Productivity and Reduce Security Risks for Teleworkers

Aventail

Executive Summary

Today, people work in more places more often. They use corporate laptops, home computers, or airport kiosks. And they expect access to corporate resources from as many places as possible. With expanded access capabilities, enterprises improve employee productivity. Yet, as productivity increases, so do risks to your network.

You want to give your users a solution that offers complete mobility and transparency so they can work more productively from anywhere. But to an IT professional, it's unthinkable to give users anywhere access without an underlying platform that makes it secure, scalable, and manageable. That's where Aventail's proven experience puts us ahead. Aventail SSL VPNs are designed specifically to enable increased productivity for teleworkers and other remote users, while minimizing many associated risks and costs.

This paper provides an overview of how teleworking helps meet today's productivity demands, what additional network security risks anywhere access can create, and how Aventail addresses these concerns while offering additional benefits for today's mobile workforce.

Anywhere access and extended hours boost employee productivity

Ubiquitous computer technology and connectivity enable people to do their jobs virtually anywhere and at any time—while traveling or at home. Increasingly, "the office" is anywhere employees can get an Internet connection to access the resources they need. As a result, workers enjoy more flexibility in their work hours and work locations, leading to increased job satisfaction. Companies benefit from extended work hours and improved employee productivity and morale. Several factors contribute to the growing number of teleworkers and increase in alternative work environments.

Inexpensive computing equipment and broadband connectivity

A desktop PC that used to cost $2,000 three years ago is under $500 today, and the cost of portable PCs has dropped even more dramatically. At the same time, the subscription costs for residential broadband service have decreased to $25-$50 per month. As a result, the number of high-speed connections has more than doubled, to 22.3 million U.S. households at the end of 2003 from 10.7 million in 2001, according to Yankee Group.[1] Many more employees can be cost-effectively equipped to work anywhere, any time.

Increased employee comfort with technology and connectivity

As the 10-hour work day is now typical at many companies, employers and employees increasingly blend professional and personal tasks. Many employees regularly respond to e-mail and work on critical projects from home. People have formed new habits of accepting and relying on technology in everyday life—regardless of their location.

Employees prefer flexible, around-the-clock, anywhere access

For maximum efficiency, today's mobile workers need around-the-clock access to key information, collaboration tools, and business applications. Research shows that employees who telework often express greater job satisfaction than their on-site peers, and they may also experience reduced levels of stress, due to control they have over organizing their tasks on a day-by-day basis.[2] Anytime, anywhere access can contribute to worker satisfaction by enabling increased flexibility in work hours, better work/family balance, reduced commute times, and therefore, improved morale.

Tangible ROI for corporations

According to "Economics of Teleworking" by Noel Hodson, the average worker spends the equivalent of 30 working days per year commuting, traveling, or engaging in office chit-chat. Converting some of this down time into productive time is a clear win for employers. For example, IBM believes that teleworking boosts employee productivity about 20 percent, and eliminating office space for 10,000 teleworkers saves the company $75 million a year.[3]

Employers also gain increased productivity and organizational responsiveness resulting in faster completion times for important initiatives. Since the start of the recession in March 2001, U.S. worker productivity has increased 4.6% annually. Due to the significant technology investments made in the late

[1] Telecommunications; What's On? The battle among broadband providers has moved to a new arena: content Peter Grant. Wall Street Journal. (Eastern edition). New York, N.Y.: Mar 22, 2004.
[2] Life Lines, Susan Hirshorn. Occupational Health & Safety Canada. Don Mills: Dec 2003. Vol. 19, Iss. 8; pg. 22
[3] Lisa Phifer. Business Communications Review. Hinsdale: Oct 2003. Vol. 33, Iss. 10; pg. 28

1990s, more industries are now realizing increased workforce efficiencies. Companies are gaining this productivity by using technology to enable current workers to do more work, by hiring temporary workers, and by outsourcing, instead of hiring more full-time employees.[4] For distributed organizations, secure, available, and cost-effective remote access is key to increased productivity.

Anytime, anywhere access is here to stay

Your employees, customers, suppliers and business partners expect anytime, anywhere access. According to a recent Nemertes benchmark, "87% of employees work at locations other than the headquarters building or campus, typically at a regional facility sales office, retail store, or a home office."[5]

Your organization needs a solution that can address the needs of these users, and handle the additional risks they bring about.

What risks does your organization face if you don't secure remote users?

Without proper security measures in place, anytime, anywhere access introduces a number of risks for organizations. For example, unsafe user behavior can leave sensitive corporate information behind on a public machine, easily accessible to curious outsiders. More serious risks can come from viruses that may be inadvertently transmitted from an infected end-user device to other computers on your

Risks to remote user devices and your network

Out-of-date or improper settings increase security risks. Without IT oversight, home computers are more likely to be improperly configured for file and printer sharing, potentially exposing sensitive information to roommates, spouses, and children. Teleworkers may not be using the latest operating system or application software. They may not have installed the latest security updates or kept up with their anti-virus definitions. All-in-all, home PCs are more likely to get infected by viruses or malicious code than corporate PCs. And infections are slower to be detected and cleaned up on home computers. Teleworkers increase corporate risks by potentially infecting other corporate machines and by spreading infections to customers and business partners.

Malicious software poses risks to users' PCs. Worms and viruses cause damage by slowing down infected systems and networks, corrupting files and applications, and stealing bandwidth. Frequently, worms and viruses spread by e-mailing themselves to everyone in a user's contact lists or by exploiting network connections. Worms often install a back door on the infected computer (e.g., SoBig.F and Mydoom) that can later be used by spammers for sending junk e-mail or to infect other unauthorized traffic on the network. Although most viruses are successfully controlled by corporate anti-virus software, they still pose significant risks to home computer users.

Trojan horses and zombies are malicious processes disguised as familiar objects, such as shareware programs, pictures, or music files, so that even educated users feel safe launching them. Both Trojan horses and zombies may be dormant until a predefined event occurs and then are controlled by a remote hacker. For example, SubSeven and BackOrifice Trojan horses let attackers control infected PCs remotely. Unless appropriate information security products are deployed, hackers can use this type of malicious software to access corporate resources through an unprotected VPN tunnel, unbeknown to the authorized user.

Wireless LANs are insecure by default. Additional risks come from the nature of home computing environments. Today, many home computers are connected to wireless home networks (based on IEEE 802.11 wireless LAN standard). Most wireless network equipment is shipping with Wired Equivalent Privacy (WEP) security features turned off (to simplify installation), and many non-technical people do not turn on even rudimentary encryption and authentication available with WEP. Since wireless networks extend outside of the physical property boundaries, anyone just outside of the building can eavesdrop on traffic going through the wireless network or access file shares. Furthermore, sophisticated hackers can easily defeat WEP by exploiting its widely publicized security flaws.

Broadband exacerbates home PC's vulnerability to hackers. With always-on broadband connections, hackers can take their time penetrating a home PC. Unless products like a personal firewall are properly deployed, port scans, and other hacking attempts and intrusions can go undetected for a long time. And hackers can exploit all open ports to steal resources or to damage unprotected connected systems.

[4] The price of efficiency, James C. Cooper, BusinessWeek, March 22, 2004, pg. 40
[5] Handling the remote-office revolution, Johna Till Johnson. Network World. Framingham: Feb 16, 2004.

Benefits of Aventail SSL VPNs

For the Enterprise: Increased employee and partner productivity

For the Business User: Transparency and ease of use, flexibility to work anytime and anywhere

For the IT staff: Strong security, scalability, manageability, and cost-effectiveness

corporate network. The biggest risk comes from sophisticated malicious hackers. They may launch a full-fledged attack against your company in an attempt to hijack your computing resources and sabotage your operations and reputation.

In many cases, IT doesn't control the end user's environment

The remote user's PC or access device could be a home computer, a friend's computer, a shared computer on another company's network, or a public airport kiosk. This remote user device tends to be the weakest point of security, due to non-technical users' inexperience and IT's lack of control over the configuration settings and software updates. It is subject to a number of potential risks, including improper system or networking settings, or lack of the latest operating system or security updates. The PC may be subject to a virus or a worm infections, Trojan horses, and zombies.

Aventail's strong, adaptable security can help you defend against these risks.

Aventail SSL VPNs are designed for secure anytime, anywhere access

You know that it's not realistic to give your users the benefits of an anywhere access solution without an underlying platform that makes it secure, scalable, and manageable. Aventail's proven SSL VPN solutions give IT the control that makes this type of end user convenience possible.

Aventail's strong security protects corporate networks

Aventail's reverse proxy and granular access control technologies eliminate direct network connections, making your internal network topology invisible to outsiders. With no visibility onto your corporate network topology, remote hackers are unable to launch the denial of service and other malicious attacks against your mission-critical resources through the VPN tunnel.

Aventail's strong security reduces network risks including stolen bandwidth and launched spam, malicious attacks and infections on your corporate resources, and use of your corporate resources to attack others. Without proper precautions, these activities can all take place through the VPN tunnel while your authorized user is connected to your corporate network, unbeknown to your end user. If your mission-critical systems are attacked, infected, or hijacked, their response times may become unacceptably slow or they may become altogether unavailable. Your sensitive information stored on attacked or infected systems may become compromised or corrupted, requiring significant audit, cleanup and restore efforts and costs. Additionally, user confidence may suffer due to unmet service level agreements. If outsiders are impacted, risks and costs can become astronomically high, especially in cases of corporate liability and damaged brand equity.

For teleworkers in particular, the increasing availability of always-on broadband access and local area wireless networks gives hackers high-speed 24 x 7 opportunity to snoop and cause damage to the teleworker's PC. If successful in penetrating the teleworker's PC, hackers can try to use the compromised device and high-speed connection to go after your corporate network.

By adding Aventail's proven technology to your information security infrastructure, you can minimize your security risks. Aventail SSL VPN hardened appliances or managed services automatically perform the following functions at the edge of the network:

- **Authentication** of the user through your authentication infrastructure, with support for SecurID, certificates, and other strong authentication methods that prevent password stealing.
- **Encryption of the communication session** using the strongest encryption available and making information in-transit unreadable by outsiders.
- **Enforcement of your access control policy**, providing an additional level of protection so that your most-sensitive resources are completely invisible to remote users who are not using corporate laptops.

The following table summarizes different teleworker risks and how Aventail can help you control these risks.

Risk	*Aventail Solution*
Sensitive corporate information inadvertently left behind on public computers, such as kiosks	Aventail auto-completion blocking prevents the browser from retaining user names and passwords. At session end, Aventail automatically disconnects after a pre-determined period of inactivity. Also, at the end of the connection, Aventail Cache Control sanitizes the remote PC by removing sensitive files created during the connection. Optional Aventail Secure Desktop offers more security with a temporary "encrypted vault" where all downloaded data is safely stored during the secure connection, and then deleted at the end of the session.
Viruses, worms, Trojan horses and zombies that may be present on end user devices and risk infecting connected corporate resources	Aventail's reverse proxy technology prevents malicious software from spreading to the corporate network by sheltering internal network topology from remote connections. Aventail End Point Control enforces safe computing practices at the end-point device by seamlessly integrating with personal firewalls and anti-virus software. Aventail ensures that end-user devices are properly protected before allowing connections to corporate systems.
Out-of-date software, improper system and networking settings on end user devices and wireless gear. Improper settings may inadvertently make files on end user devices viewable or accessible to outsiders.	Optional Aventail Secure Desktop temporarily encrypts and safely stores all downloaded data during the connected session, and then automatically deletes it at the end of the secure session.
Insecure connection common with broadband and wireless networks where an intruder may view sensitive information in transit. Additionally, intruders may inject malicious traffic into the secure connection, stealing or damaging connected systems.	SSL-encrypted and authenticated VPN session ensures privacy and authenticity of the communication, preventing outsiders from viewing or altering sensitive information in transit. Aventail's SSL VPNs provide strong security that protects corporate communications independently of the wireless LAN settings and WEP.
Intruders, masquerading as a legitimate user, may try to access sensitive corporate resources.	Aventail supports numerous strong authentication options (including tokens, LDAP, RADIUS, and certificates), ensuring authenticity of the user before allowing for a secure connection. Aventail's reverse proxy technology reduces risk of attack by preventing outsiders from seeing internal network topology.

Aventail End Point Control protects remote users' PCs—which protects your network

What is Aventail® End Point Control™ ?

Aventail End Point Control is designed to help IT proactively control the security of the remote user's PC. With Aventail, you can manage access according to the user's environment, making those environments safer, and delivering secure access from virtually anywhere over any network. Aventail encrypts and authorizes access to all corporate resources with access control policies based on both the user's identity and the security of the user's environment. Aventail's best-of-breed technology partners enforce policies for firewalls, intrusion detection, virus protection, and other client-side security issues.

Additional protection for corporate laptops

Most risks associated with the remote users' PCs are due to numerous Windows vulnerabilities and the lack of security vigilance on the part of end users. To reduce these risks, IT needs to exert some level of security enforcement over the end users' computing environment. If the user's PC is a corporate laptop or desktop, you can first deploy a personal firewall or other desktop security product on your users' laptops. Then, you can use Aventail® Connect™, our award-winning SSL VPN Windows client, to enforce activation and usage of desktop security software before allowing users to connect to the corporate network. Additionally, Aventail Connect provides source-based access policy rules and control over split tunneling to prevent hackers from hijacking the remote PC.

Monitoring of home PCs or partners' PCs

Limiting access to only corporate laptops is expensive, cumbersome to manage, and may severely limit users' productivity. So, most organizations are backing off from this restrictive policy. Instead, you can rely on Aventail End Point Control to ensure that a home PC or a partner's PC is protected with the latest desktop security software.

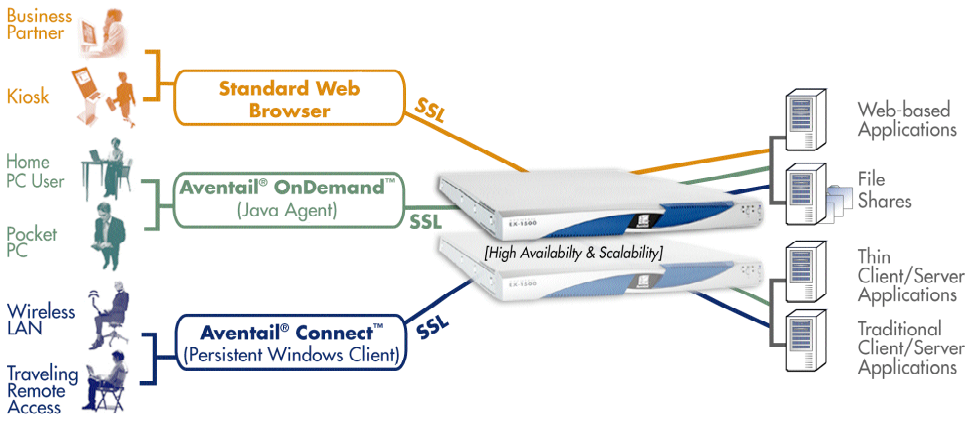
Reduced risk for access from kiosks and PDAs

On public machines, you can use Aventail Secure Desktop to create a temporary secure workspace and you can also restrict access to just a handful of applications. For example, many organizations allow the use of public computers to check work e-mail and to access some Web applications, but disallow access to certain file shares and more sensitive corporate resources. Aventail's object-based access control helps you manage user access rights according to the user environment. Additionally, you can reduce the risks of public PCs with Aventail Cache Control, Aventail Secure Desktop, crypto-level access control, and auto-completion blocking.

Aventail Cache Control sanitizes the user's remote PC by removing sensitive files created during the session—including Web pages, temporary files, viewed e-mail attachments, browser history, cookies, auto-complete or stored passwords, and other temporary or downloaded files.

Aventail Secure Desktop, an optional feature, provides even stronger end-point security by creating an "encrypted vault" where all data that is downloaded in a Web session—attachments, cookies, cached content and the like—is safely housed for the duration of the session. Users see a virtual workspace that looks similar to a standard desktop; however, their session is being secured and that they can browse Web sites or run other applications without leaving a trail. At the end of their session, their virtual workspace and encrypted vault are destroyed, erasing any information that was viewed or saved.

Aventail SSL VPNs offer secure yet convenient access from diverse environments to a broad ranges of applications.



End-user convenience with flexible access options and broad application support

Aventail's strong emphasis on security alone would not provide your teleworkers and other remote users with the access they need to do their jobs. That's why Aventail offers a full range of clientless access options plus the award-winning Aventail Connect Windows SSL VPN client, giving users convenient yet secure access from un-trusted, semi-trusted, and trusted Internet-enabled devices. The Aventail SSL VPN

is flexible enough to work well in any remote access situation, providing you with the best possible security for that environment.

Aventail provides three flexible access options:

- **Browser-based access** for Web applications and file shares
- **Aventail® OnDemand™**, a Web-delivered Java SSL VPN agent for secure client/server application access
- **Aventail® Connect™**, a cost-effective, easily-managed, Windows SSL VPN client for full secure access to network resources from corporate laptops

In its SSL VPN offerings, Aventail combines the security and full Windows functionality you would expect from an IPSec VPN and delivers it with the convenience and cost-savings of a clientless SSL VPN. Aventail's multiple access options enable secure, transparent access to virtually any application or corporate resource from any device.

Broad application support

Aventail's SSL VPNs have been tested and deployed with hundreds of different applications and platforms. In addition, Aventail SSL VPNs can seamlessly interface with leading portal products. Plus, Aventail offers its own built-in Aventail® ASAP™ WorkPlace portal that provides end users with intuitive access to information and resources.

Manageability and cost-effectiveness enhance IT productivity

With recent staff reductions and increased workloads, organizations need products that are easy for end users, and are easy for IT to manage and support. In fact, one of the reasons many organizations are adopting SSL VPNs is to reduce the cost and complexity they are experiencing with IPSec. Built for site-to-site VPN, IPSec technology has been unable to adapt to changes inherent with mobile workforces.

With IPSec, many end users are unable to access the information they need. Corporate help desk staff may spend hours on the phone with end users, trying out different client software and networking configurations to work around the access issues. Complex technology leads to dissatisfied end users, overburdened support staffs, decreased productivity, and increased costs. With SSL VPNs, the reduced complexity and increased end user self-sufficiency quickly translates into improved user productivity and reduced workloads for IT.

Aventail's SSL VPNs connect to the enterprise, traversing all network boundaries

Aventail SSL VPNs traverse firewalls, Network Address Translations (NAT), and proxy services, preventing configuration conflicts common with other remote access products. Aventail's SSL VPN works trouble-free and consistently in virtually any environment, with no client or server changes.

Aventail's SSL VPNs work great with broadband

Residential broadband connection ($35-50 per month) is less than half the cost of the business broadband connection ($100+ per month), although the speed and service levels are the same. Occasional day extenders and teleworkers use their at-home broadband connection to do company business, especially while sick, on vacation, or snowed-in. Since many organizations use IPSec for remote access, service providers are beginning to block IPSec traffic over residential broadband connections, in an attempt to get home workers to upgrade to business-level pricing.[6]

Aventail's SSL VPN is an attractive alternative for these situations. SSL is a commonly used Internet protocol, and service providers cannot distinguish between SSL used by a person logging onto eBay and SSL used to connect to the corporate network. Additionally, Aventail automatically adapts to NAT, wireless switches and routers, and dynamically assigned IP addresses common with home networks.

Aventail's flexible, object-based policy model simplifies management

You can easily manage any resource, application, or network file share for all of your remote access policies and user organizations from a centralized location. Aventail approaches access control policy using the same security and management principles that underlie leading firewalls. This offers administrators a robust—yet familiar— model for handling their every-day organizational complexities.

[6] Residential broadband for home workers, David Passmore, Business Communications Review, Nov 2003

Scalability to thousands of users and connections

As additional users start accessing your corporate network remotely, scalability of your infrastructure becomes a real issue. Add new high-bandwidth applications like voice over IP and document sharing, and scalability and reliability quickly percolate to the top of your list of concerns.

Your scalability risks are exacerbated if you have a large, distributed organization with highly mobile employees who may need to access different applications from different parts of the world. Lack of availability or slow access to corporate resources quickly translates into lost productivity for end users. Users get frustrated and complain. And their phone calls and trouble tickets increase the burden on your already overworked IT staff.

Multiple authentication realms provide added flexibility and scalability

Aventail SSL VPNs can support more than one authentication repository (e.g., Active Directory and RADIUS) as well as differing methods of authentication (e.g., Username/Password & tokens), providing more flexibility and scalability. This makes it easy to support a policy model spread across multiple directories or to support situations where differing authentication credentials are required.

High availability is key for predictable performance and service level agreements

Aventail's scalable, reliable equipment can be easily added to your infrastructure with minimal configuration changes. Aventail is the first SSL VPN provider to offer integrated active/active high availability that makes it easy for organizations to roll out and implement a reliable and scalable SSL VPN solution. Aventail's integrated load balancing with stateful failover means that you do not have to add a third-party load balancer. However, for distributed installations supporting hundreds of thousands of users, Aventail also works with third-party load balancers to provide secure, fault-tolerant, and scalable anywhere access.

Aventail SSL VPNs: Best choice for remote worker productivity and security

Technology, economics, and competitive pressures are forcing enterprises to enable workers to work more places more often. Users' own expectations for anywhere access reinforce this need. For economic and technical reasons, older IPSec-based technology is no longer adequate to support the nearly constant need for secure anywhere access.

Because they combine the IT need for advanced security with the end-user's need for convenient, flexible access, Aventail SSL VPNs are today's best choice for remote worker productivity. Every day, hundreds of thousands of users and thousands of organizations depend on Aventail SSL VPN appliances and managed services. Aventail helps them to securely and cost-effectively access protected network resources from the broadest range of remote locations and devices of any SSL VPN vendor today. Aventail SSL VPNs offer easy, flexible access options to secured resources and reduce companies' information security risks. By extending secure remote access from more places and to more resources at a low total cost of ownership, Aventail increases productivity for teleworkers and all mobile and remote users.

Aventail: the leading SSL VPN product company

Aventail is the leading SSL VPN product company and the authority on clientless and client-based anywhere secure access. We are investing more development resources in this technology than any other company, large or small. Our appliances and services lower costs and increase the productivity of end-users and IT professionals by ensuring access to any application from any device. Customers including Aetna, DuPont, Mount Sinai NYU Health, Office Depot, and Sanyo, and leading service providers including AT&T, IBM Global Services, MCI, Sprint, and Bell Canada rely on Aventail technology. Aventail was positioned in the Leader quadrant in Gartner's 2004 SSL VPN Magic Quadrant.

Aventail

WP-4084-0604/1

Corporate Headquarters
808 Howell Street
Seattle, WA 98101
Tel 206.215.1111
Fax 206.215.1120
americas@aventail.com
www.aventail.com

Aventail Europe Ltd
Tel +44 (0) 870.240.4499
emea@aventail.com

Aventail Asia-Pacific
Tel +65 6832.5947
asiapac@aventail.com