

White paper

10 Trends and technologies driving Secure Teleworking

September 2008

**Tim Clark, Partner
The FactPoint Group
300 Third Street, Suite 10
Los Altos, CA 94022
(650) 233 1748
tclark@factpoint.com**

10 Trends and technologies driving Secure Teleworking

TABLE OF CONTENTS

Introduction.....	3
<i>Sidebar: Global governments encourage teleworking.....</i>	3
Technology #1: Broadband connectivity tops 50%	4
Technology #2: Collaborative apps emerge: Web 2.0, Web meetings, VOIP	4
Technology #3: Smartphones and PDAs abound	5
Trend #4: Put money back in employees' pockets to keep them loyal, productive	6
<i>Sidebar: Sun shines in telework in 2007</i>	6
Trend #5: Save on operations and real estate.....	7
Trend #6: Shrink the carbon footprint	7
<i>Sidebar: Family-work balance vs. carbon footprint</i>	7
<i>Sidebar: Passed over for promotion?.....</i>	8
Trend #7: Boost business continuity, bounce back from disasters	9
Trend #8: Regulatory compliance.....	9
Trend #9: Bad guys are getting better.....	10
Technology #10: Telework prerequisite: Secure remote access technology	10
Conclusion	11

About SonicWALL

SonicWALL is committed to improving the performance and productivity of businesses of all sizes by engineering the cost and complexity out of running a secure network. For more information, visit the company web site at <http://www.sonicwall.com/>. Secure remote access information is available at http://www.sonicwall.com/us/products/Secure_Remote_Access.html.

About The FactPoint Group

The FactPoint Group (www.factpoint.com) is a Silicon Valley-based market research, publishing and consulting firm specializing in the early adoption of new technologies. The FactPoint Group has been producing world class research, analysis, and consulting since 1993 and continues to help its clients sell and use new technology solutions. FactPoint partner Tim Clark was, until 1999, a senior editor with CNET News.com, where he covered Internet security. Clark authored two white papers on secure remote access for Aventail, which SonicWALL acquired in 2007. He has telecommuted since 1993.

Introduction

“It’s been a perfect storm. Rising gas prices, leading-edge technology, and the push for work-life flexibility have all come together in the past 12 months to create a pretty dramatic increase in telework across the U.S. and Canada.”

—Anne C. Ruddy, president, WorldatWork (August 2008)

Many employees are feeling the pinch of inflation, rising gasoline prices and the prospect of an extended economic downturn. By expanding telecommute programs, employers can save workers hundreds of dollars a month in commute costs.

And companies are doing just that. WorldatWork, a global human resources organization, found in its annual survey that 42% of U.S. companies now say they have a telework program, up from 30% in 2007. In Canada, the 2008 figure jumped to 40% from 25% in 2007. The latest survey was fielded in April 2008.¹

Once the key drivers for teleworking were productivity and flexibility—the so-called “work-life balance” that many workers strive for. Those “soft benefits” still exist, but increasingly financial considerations such as gas prices, the credit crisis and hard cost savings drive teleworking programs. Teleworking programs help companies strengthen the loyalty of their workers.

Whether driven by hard or soft benefits, teleworking programs have one core requirement: Give telecommuters secure access to corporate networks, applications and data. For workers at remote sites, IT and corporate security managers must select secure remote access technologies to make teleworking not just viable but safe.

Global governments encourage telecommuting

European Union: 4.5 million teleworkers in 2007 growing to more than 17 million employees by 2010. In 2002, the EU agreed on a framework to regulating telework in areas such as employment conditions, health and safety, training and collective rights. In the UK, 39% of firms offer flexi-time.

U.S.: 41% of federal employees are eligible for telecommuting but only 19% do so. In June 2008, the House of Representatives voted to require federal agencies to expand telecommuting.

Japan: Offers tax breaks to companies that allow telecommuting, which has become widespread in the electronics industry. Matsushita Electric Industrial Co has 3,000 working from home. At NEC Corp., 20,000 employees telework one day a week.

Thailand: Starting in July 2008, more than 40% of staffers in a Finance Ministry unit are eligible to work at home one day a week.

Singapore: Started a fund to help companies to implement work-life or family-friendly work practices such as telework.

¹ WorldatWork 2008-2009 WorldatWork Salary Budget Survey.
<http://www.worldatwork.org/waw/adimLink?id=28062&from=pressall>

This white paper addresses today's drivers of teleworking and the technologies that enable it.

Technology #1: Broadband connectivity tops 50%

Broadband and collaboration software could increase the number of telecommuters from 10% to 20% of the U.S. workforce over the next 10 years and reduce carbon emissions in the U.S. by 45 million tons annually.

—*Joseph Fuhr Jr. and Stephen Pociask, American Consumer Institute (2007)*²

As the number of homes with broadband Internet access grows, working from home becomes more viable. In mid-2008, Gartner Inc. put broadband access from U.S. homes at 54%³, and even higher in six European Union nations (Netherlands, Switzerland, United Kingdom, France, Sweden, and Belgium) plus South Korea, Hong Kong, Canada, Singapore and Taiwan. By 2012, Gartner sees broadband connections in 77% of U.S. homes.

Telecommuters can work more effectively with broadband connections because enterprise applications run closer to real-time when accessed over a fast connection instead of dial-up. Broadband also makes VoIP (voice over IP or Internet phone) and other bandwidth-hungry new applications viable when they would not be with a slower connection.

Technology #2: Collaborative applications emerge: Web 2.0, Web meetings, VoIP

“Web 2.0 applications are already present on the majority of corporate networks, whether they’ve been formally/centrally approved or not.”

-- *Mark Bouchard, Missing Link Security Services*⁴

New applications such as wikis and VoIP are key enablers of online collaboration so that employees don't have to be in the same location to work together. For telecommuters, remote collaboration is a huge productivity gain, as proven by the growth of Web conferencing for meetings. Today Web meetings have become commonplace within companies that have distributed workforces, whether in remote offices or home offices. Web meetings not only boost collaboration but keep remote workers from feeling isolated from central office contact.

In terms of office culture, outsourcing and extended supply chains have given many organizations new lessons in real-time collaboration—online or by phone—with

² Broadband Services: Economic and Environmental Benefits, American Consumer Institute, 2007. <http://www.theamericanconsumer.org/2007/10/31/broadband-services-economic-and-environmental-benefits/>.

³ Gartner press release, July 24, 2008. Leichtman Research Group puts U.S. penetration at 53%, Leichtman, press release June 25, 2008.

⁴ See http://www.sonicwall.com/downloads/voip_wp.pdf

suppliers, partners and outsourcers. Now employees can apply those skills to collaborate with each other remotely.

Today, VoIP's great appeal is that it allows telecommuters to use a phone from home at little additional expense to either themselves or their employers, although not without beginning to be integrated into enterprise applications themselves so users can talk to each other through the application.

At F.W. Honerkamp, a Long Island laminate distributor, has found VoIP gives the company the flexibility to hire and retain workers who cannot come to the office, offering customer service reps a chance to work while living in other states.

Software as a Service (SaaS) or hosted applications play into the telework theme because they can be accessed online from anywhere—there's no advantage to be in company headquarters instead of working at home.

However, like many new technologies, VoIP, wikis and particularly Skype are still working out technical glitches that potentially create security vulnerabilities. IT departments are rightly concerned about potential security, but Gartner recommended in March 2008 that, instead of blocking Web 2.0 technologies, enterprises should focus on providing secure ways to develop and deploy them because they can “unlock huge business value.”⁵

Technology #3: Smartphones and PDAs abound

“82% of smartphone owners said they use their devices to read business e-mail, 80% surfed corporate Web sites, and 61% accessed enterprise data.”

—Information Week (July 2007)

The proliferation of smart phones, PDAs, other handheld communication devices (Blackberries, Symbian devices, etc) and together with laptop computers has given millions of workers the tools to telecommute, work while commuting or otherwise work remotely. But mobility also challenges corporate IT departments concerned about security of not just the devices but also the wireless networks they utilize. In an Information Week online poll in July 2007, 70% of 405 readers said they were currently accessing corporate data over a wireless network⁶—enough to send shudders through any security-minded IT manager.

In corporations, PDAs tend to be managed (even issued) by corporate IT, so they are more likely to be configured to access the corporate network securely. Smartphones are most often owned by the employee and then used to access the company network for work. Both types of devices open corporate networks to new threats, not the least of

⁵ See “A Security Strategy for Web 2.0 and Social Networking,”

http://www.sonicwall.com/redirect_whitepaper.asp?url=569_8087.html

⁶ Information Week, Feb. 11, 2008,

<http://www.informationweek.com/news/mobility/security/showArticle.jhtml?articleID=206105247>

which is that small devices are easier to lose than larger ones. Plus IT departments are responsible for smartphones without controlling them.

For teleworking, the growing number of devices telecommuters can use simply makes it easier for workers to stay productive from their home environments. At one time secure remote access required a specific device, often company-issued and configured by IT, to connect. Falling prices and greater horsepower of handheld devices, not to mention laptop computers, put the technology of teleworking within the reach of many organizations and their workers.

Trend #4: Put money back in employees’ pockets to keep them loyal and productive

“Corporations may want to consider enabling more tech employees to telecommute, not merely because gas prices are spiraling, but because this may be a way to attract and keep talented individuals.”—Tom Silver, SVP, Dice Holdings

Economic conditions—inflation, rising gas prices, the housing bust and downturn—are affecting many workers. Working from home can trim commute costs in a family budget and allow for greater flexibility.

Sun shines on telework in 2007

- Almost 18,000 Sun employees worked away from the office 1-2 days/week. (54% of global employees)
- Average time worked at home: 2.1 days/week in U.S.
- Prevented CO2 release: 29,000 metric tons
- Saved commute time: 104 hours/year (2.5 weeks vacation)
- Average of 3,700 miles of commute avoided, saving \$906 in car wear and tear (\$.24/mile)
- Employee gasoline expense saved: \$870/year
- Electricity saved: 66 watts/hour for home workers compared to Sun facility
- Sun saved nearly \$68 million on real estate costs.

Teleworking is such a prized job perk that 37% of IT workers say they’d accept up to a 10% lower salary to work full-time from home.⁷ In that context, the telecommute proposition can suit both employers (who save on salaries) and workers (who save on personal commute expenses).

Or, without cutting salaries, telework programs can cement employee loyalties. Sun Microsystems say its telecommuters cite the Open Work program as the No. 1 reason they would recommend Sun. With revenue growth flat-lining, employee incentives such as bonuses are unavailable. By reducing costly job turnover, employers also save the very real costs of training new hires

Companies also may gain a competitive edge in being able to hire better talent because they offer teleworking as a job perk. In a May 2008 online survey, the Telework Coalition found that 87% of respondents would limit a job search based on potential commute costs.

⁷ The Dice Report, June 2008, a survey of 1,500 users of the technology job site. The question: “With gas prices soaring, would you accept slightly less pay to telecommute full-time?” 36% answered “no way.”

Indeed, 28% said they're already looking for a new job because of the cost of commuting.⁸

Companies also may get higher productivity from telecommuters simply because avoiding two stressful commutes a day makes them fresher and more creative. Employers also get productivity gains as time spent commuting is now time spent working—Sun found that its telecommuters gave 60% of their saved commute time back to the company in extra work time.

Trend #5: Save on operations and real estate

“Hot desking’ involves one desk shared between several people who use the desk at different time. A primary motivation for hot desking is cost reduction through space savings—up to 30% in some cases.”—Wikipedia⁹

In the big picture, telecommuters also help companies lower their operating costs. When telecommuters use their own space, power and cooling to work from home, savvy employers adjust their facilities practices to pocket that savings.

The Canadian Telework Association (CTA) puts some numbers to the “hot desking” phenomena, suggesting that employers need one less office for each three teleworkers or about \$2,000 per teleworker per year. AT&T saved \$550 million by eliminating or consolidating office space (\$3,000 per office) in its telework program, CTA states, About 25% of IBM's 320,000 workers worldwide telecommute from home offices, saving \$700 million in real estate costs, per CTA.

Trend #6: Carbon footprint

A company’s carbon footprint has become a key indicator of its environmental record, so companies keen to be “green” measure their carbon footprints. The carbon footprint measures the amount of carbon dioxide and other greenhouse gases emitted by using carbon-based energy. It includes all direct (on-site, internal) and may count indirect emissions (off-site, external, upstream, downstream) too. Among the items taken into account are travel by car, airplane, rail and other public transportation. Energy for heating, cooling and electricity also count. Carbon emissions from consuming goods and services also may be included.

Companies have a carbon footprint, but people do too. Individual employees may seek to telecommute to reduce

Family-work balance vs. carbon footprint
 A survey of 700 white-collar workers found that 61% of telecommuters did so to balance their family and work life; 37% sought to reduce their carbon footprint. The survey was conducted for office furniture manufacturer Steelcase and reported in August 2008.
Steelcase, 2008

⁸ Canadian Telework Association, <http://www.ivc.ca/costbenefits.htm>

⁹ “Hot desking,” Wikipedia, (http://en.wikipedia.org/wiki/Hot_desking).

their personal carbon footprints.¹⁰ Or they take public transportation with its near-zero carbon footprint. Transit agencies, transportation companies and employers such as Google and Microsoft are adding Wi-Fi to their commute vehicles to provide Internet access.

Fortunately for the environment, going Green often reduces both carbon footprints and costs. Thus as Sun reduced the carbon footprint of its U.S. buildings, the company cut electricity consumption by 22%, gas by 32%, and carbon emissions by 21%.¹¹

How does teleworking affect carbon footprints? In one sense, telecommuters are simply shifting energy consumption from the employer's building to their own homes. However, recent research by Sun reports that its telecommuters use roughly half as much energy at home as they do in the office, in part because many use Sun's low-energy thin client called Sun Ray instead of conventional desktops with monitor.

However, just as fewer offices reduce rent, fewer offices also shrink carbon footprints and utility bills. Fewer workstations mean lower power bills. In 2006, for example, IBM avoided the consumption of 180 million kilowatt hours of electricity and 2.4 million gallons of fuel, representing the avoidance of 99,000 metric tons of carbon emissions. The conservation projects also avoided \$18.6 million in energy spending.¹²

Passed over for promotion?

Research suggests that employee enthusiasm for telecommuting is dampened by a fear that working home can hurt his or her career. A survey of 700 white-collar workers for Steelcase, the office furniture manufacturer, found that 46% of respondents' employers allow them to telecommute but only 32% do.

Other findings:

- 64% respondents are concerned about a lack of contact with their employer.
- 71% think their employer prefer them to work in the office to prevent declines of productivity
- 72% think employers prefer them in the office to control their work environment.

The latest Steelcase findings, issued in August 2008, are consistent with the 2005-2006 National Technology Readiness Survey by the University of Maryland. In the NTRS results, 25% of respondents cited favorable employer telecommuting policies or jobs but only 11% telecommuted.

¹⁰ As discussed above in Trend 2, another high-impact way companies can reduce corporate carbon footprints is by limiting business travel. The growing use of Web meetings and other virtual events makes cutting travel less painful and more cost-effective.

¹¹ Sun Microsystems, 2007 corporate social responsibility report.
http://www.sun.com/aboutsun/csr/report2007/eco/carbon_greening.jsp

¹² "IBM and the Environment 2006,"
http://www.ibm.com/ibm/environment/annual/IBMEnvReport_2006.pdf

Trend #7: Boost business continuity and bounce back from disasters

“When things get busy, like in a weather event, we can send an email to all [at-home] agents asking them to log in to help. The response is immediate—we don’t have to wait for them to come in.”—JetBlue Airways spokeswoman¹³

Teleworking also dovetails nicely with another key corporate objective—Continuity of Operations, also called disaster recovery or business continuity.

Teleworking by definition distributes employees away from central offices that may be knocked out through power outages, weather, traffic jams or localized disturbances. Even a few miles make a difference in those situations, when companies can operate business as usual, maintaining revenue streams and delivering an “always on” image with customers, partners and investors.

Disaster recovery has become an increasingly important objective in the era of globalization. An outage at a distant but strategic facility can cripple work not just locally but at every other company location.

And catastrophic events seem to be increasing of late: Avian flu, hurricanes, tsunami, fire at a data center, a heavy rain or snow storm, a lightning strike, traffic jams, a car into a power pole or a cyber-attack can turn a normal business day into a crisis. The continuing trend of outsourcing exposes the company to outages that affect their outsource partners.

Disaster recovery solutions, however, generally include not only a back-up data center but decentralizing company operations to areas that may escape any outages. Teleworking should be part of any enterprise business continuity plan.

Trend #8: Regulatory compliance

The number of regulatory compliance issues has multiplied in recent years—Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley (GLB) PCI. Virtually all of them spring from two goals:

- Protecting customer information from unauthorized access or
- Make corporate information public to all audiences, not just insiders.

Telecommuters are not excluded from these compliance mandates, so the viability of a telework program requires having technology in place that closely monitor teleworkers and onsite employees: Such technology must be able to:

- Identify who requires access to the data.
- Enforce access to sensitive information.
- Segregate users, resources and communications between the two.
- Verify the processes are being followed, and audit processes for compliance.

¹³ “Call Centers Come Home,” HR Magazine, January 2007.

Those requirements for regulatory compliance fit neatly within the capabilities of an SSL VPN, as outlined in the previous section on secure remote access. The goal is to prevent unauthorized access to data, and the SSL VPN's granular access policies let users see only what they're supposed to see and block unauthorized users from inappropriate access. SSL VPN's utilize what is called "application-level" security. In short, the same security technology that enables secure teleworking also addresses multiple regulatory compliance issues.

Trend #9: Bad guys are getting better

Not only are attacks on networks growing more sophisticated, but the cyber-criminals are become more sophisticated in organizing themselves.¹⁴ No longer are culprits simply brilliant teens or other amateurs. Organized crime has moved into the Internet age.

To growing hacker sophistication, add the reality that tough economic times force companies to cut their work forces, potentially creating a new class of security threats: Disgruntled ex-employees. What if those unhappy ex-employees become potential partners to professional bad guys?

As with regulatory compliance, the technology that keeps hackers away from sensitive data is secure remote access or SSL VPNs. Because SSL VPNs grant granular access to which applications a user can see, a hacker might break through a network's perimeter but kept away from sensitive data. The unauthorized hacker would not only need to break through the perimeter but also get access to the specific application where sensitive data is used.

SSL VPNs, the basic security requirement for secure teleworking, also address the growing sophistication of hacker attacks and the organizations behind them. Teleworking, which on the surface might seem to open new security vulnerabilities, should not if enterprises insist on secure remote access technology.

Technology #10: Telework prerequisite: Secure remote access technology

Secure remote access and virtual private networks (VPNs) are essential for sending critical information over the Internet. VPNs essentially drill a "secure tunnel" through the Internet from the corporate data center to a remote location or mobile worker so sensitive data can pass over the Internet safely.

With teleworking and transit-based Wi-Fi, VPNs are no longer a "nice to have" but a key requirement. Modern VPNs, meaning those called SSL VPNs after the SSL protocol they utilize, can detect the identity of remote users, their network, location, and endpoint device and its security state. That allows the remote access solution to protect against malware and block unauthorized access based on a granular policy. Authorized users can

¹⁴ Finjan Malicious Code Research Center, May 2008. (www.finjan.com).

connect to the mission-critical applications, databases and other network resources that are appropriate for them—but not to anything else.

These secure remote access capabilities are not unique to teleworking. More employees, partners and customers are connected to corporate networks in a widely-distributed, mobile enterprise. They come from many locations and devices—PDAs, laptops, smartphones, home computers, PCs at a customer's location, etc. Demand for a single, centrally-managed gateway to control access to applications and network resources has never been higher.

Fortunately, those VPN capabilities can be leveraged not only for teleworking but also for other purposes—extranets, executive travel, disaster recovery, mobile sales people and field personnel. That means enterprises with telework programs may be able to leverage existing investment in VPNs for their teleworking program. Alternately, if teleworking is the first use case for their VPN, they will enable other remote use cases too, not just telework.

Conclusion

These 10 trends and technologies put teleworking on the cusp of a period of rapid growth. Two general categories are stronger today than they have been anytime in the last five years: Financial drivers and enabling technologies.

The technology enablers of teleworking work include reliable secure remote access, wider access to broadband Internet, new collaborative applications, and the popularity of PDAs and smartphones. Add heightened public awareness of global warming and the original push from employees seeking better balance between their work and family lives. This time telework may actually work.