Keeping Mobile Workers Secure for Less
Helping employees and contractors work remotely can save money — if it’s done securely.

What do the Swine Flu, gas prices, the economic recession and shrinking budgets all have in common? They’re all fueling the current push toward remote teleworking.

The number of Americans who worked from home or remotely at least one day per month for their employer increased from approximately 12.4 million in 2006 to 17.2 million in 2008, according to a study by The Dieringer Research Group Inc. for WorldatWork, a global human resources association.

In the five-year period since 2003, the total number of once-a-month telecommuters of all kinds (self-employed, contract or employee) in the United States has risen by 43 percent, from 23.5 million to 33.7 million Americans. The International Telework Association and Council estimates that by 2010, the number of U.S. employees teleworking will increase to 100 million.

There’s no question the web has changed how we work, and more importantly where we work. Today nearly every job can be done from home via teleworking. What’s more, research continues to show that teleworking can contribute to productivity, build morale and boost cost efficiencies.

Just remember to keep telework safe and secure. While mobile security need not be expensive, it does need to be effective. The key is to adopt simple yet potent processes for mobile security. And for cost-conscious IT departments, there is a silver lining — allowing secure remote access to the office can actually save money.

Today’s Teleworker
Ten years ago, it was relatively easy to support a small number of high-level employees with notebook PCs. It only required poking a few holes in the firewall and these remote users had access to the entire corporate network.

Fast-forward to today. Broadband connectivity is available in every home. Organizations, in a challenging economic environment, are looking for ways to cut costs. And some are turning to outsourcing to get the job done, which invites outside workers into company networks.

What’s more, the number of remote devices connecting remotely to central systems has exploded. Notebook computers, smartphones, Personal Digital Assistants (PDAs) and travel drives are common business travel accessories.

But with the good news for workers comes a host of security issues for IT departments. Remote access policies must go beyond verbal instructions and include solutions to protect the remote user, the remote device and the data being transported.

“You can’t really cover such a large number [of remote workers] with a paper-based policy that says, ‘Will you please promise to be good?’” says Chris Witeck, director of Secure Remote Access (SRA) product marketing at SonicWALL Inc. in Sunnyvale, Calif.

“At large organizations, we’ve seen trends toward strong authentication policies, endpoint assessment of devices before the device is on network,” he says. “And we’ve seen a very granular strategy that differentiates access to data by employee.”

Compliance mandates, such as Payment Card Industry (PCI), Sarbanes Oxley and the Health Insurance Portability and Accountability Act (HIPAA) are also driving efforts for secure remote access policies and appliances, adds Upasona Hazarika, SonicWALL product manager, SRA for small and midsize businesses.

“There is no such thing as absolute security. It will never exist,” says Craig Mathias, principal at Farpoint Group, an Ashland, Mass.-based advisory firm specializing in wireless communications and mobile computing.
“The nature of [remote access and devices] simply introduces vulnerabilities in the process,” he adds. “The objective, then, is to make remote access as foolproof as possible.”

**Cost Savings**
In addition to the productivity gains that companies see by deploying secure remote access, some companies are also realizing cost savings. For instance, companies are looking at ways to save money by taking components of their business and handing it off to a partner.

With secure remote access, these outside partners can easily collaborate in real time with internal employees. Also, allowing employees to use their own PCs, notebooks, PDAs and phones for corporate use, part of what Gartner Inc. calls the consumerization of IT, can mean huge hardware savings for businesses.

With secure remote access in place, employees have the ability to use their own equipment for work-related activities. “Perhaps you have a program for compensating some of the cost of owning a notebook,” Witeck says. “Then if they have a device capable of remote access, there’s a good chance they’ll use it.”

SRA can be vital in keeping business moving during a disaster, flu outbreak or weather-related issue. With a remote access solution, employees can keep working, and ultimately keep the company from losing money.

**Changing Requirements**
The primary purpose of Secure Remote Access solutions is to provide workers with access to IT resources. IP Security (IPsec)-based remote access solutions, that have been popular since the mid-1990s, are giving way to solutions that have more granular policies.

“Increasingly, the business-line managers and legal departments are getting involved in the security policy,” Witeck says. “And IT is realizing it can’t enforce that policy with some of the legacy tools out there.”

Part of that is driven by compliance mandates. However, companies are also looking for ways to give business partners access to specific applications, for instance, or require different authentication policies for different types of employees and the systems they use to do their jobs.

**SRA Strategy**
There are four things that IT decision-makers should consider for a SRA strategy. The answers will depend on the size of the organization and the depth of the company’s security policy.

Trusting the User — Take a look at solutions that establish trust of the user, based on the company’s authentication strategy. “I highly recommend that an organization with remote users use some sort of two-factor solution, such as a token or certificate on the device,” Witeck says.

“That way if the [user] is moving around from hotspot to hotspot or the password is stolen, that adds a measure of protection.” Though, he adds, he believes that the majority of businesses in the U.S. aren’t using two-factor solutions today.

Trusting the Endpoint Device — IT decision-makers should establish some trust point for the end device through Network Access Control (NAC) or endpoint assessment solutions. Large and midsize organizations usually differ in their approach to endpoint authentication.

Large companies will often have a dedicated appliance to authenticate that the device being used remotely has active and up-to-date antivirus and firewall capabilities. Smaller businesses can achieve the same benefits with multifunction appliances that cut costs, resources and maintenance.

Trusting the Traffic — IT decision makers should have a Secure Sockets Layer (SSL VPN) solution run in conjunction with a firewall solution so that firewall can perform the traffic inspection.

“That’s a best practice because the SSL VPN traffic is going to come in encrypted and so it may bypass your existing edge firewalls,” Witeck says. “It’s a good idea to make sure you route that traffic, once it is decrypted through the SSL VPN, back through the firewall for traffic inspection.”
Creating an Application Layer Access Control Policy — The forth consideration, perhaps the most important piece, is leveraging the trust that is now established for users and the devices and turn it into an application layer access-control policy.

Based on what the IT department knows about its remote users and their devices, they can be granted access to approved applications, based on need.

**Security Solutions**
Several vendors, including SonicWALL, Juniper Networks Inc., Check Point Software Technologies Ltd. and others, offer secure remote access solutions for large and midsize businesses.

SonicWALL offers six products focused on remote access control as part of its Aventail line. For midsize businesses, those include the SSL VPN 200, SSL VPN 2000 and SSL VPN 4000, the latter which can support up to 200 concurrent users.

On the enterprise side, the Aventail EX-750, EX-6000 and SRA EX-7000 have capacity up to 2,000 concurrent users. Firms can also cluster appliances.

Juniper Networks offers solutions for a variety of environments, including large enterprise and small branch exchanges. It’s SRX5800 and SRX5600 services gateways, for example, offer gigabit firewall, Intrusion Detection and Prevention (IDP) and more, in a scalable and operationally simple package suited for enterprise data centers.

Juniper also offers the SRX650 for large branch and regional offices, the SRX240 for small- to medium-sized branch offices, and the SRX210 and SRX100 for telecommuters and small offices. These competitively-priced boxes also provide a foundation for integrated antivirus protection, web filtering and Unified Threat Protection (UTM).

Says Michael Flaum, product marketing manager for Juniper Networks: “Organizations are finding that a single box solution with highly available routing, switching, adaptive threat management and other security protections is efficient and cost effective.”

Check Point offers Connectra, a unified remote access gateway that allows mobile and remote workers to connect easily and securely to critical resources while protecting enterprise networks from external threats.

“It also manages all endpoints in the workforce — laptops, smartphones, Windows mobile devices and others — from one central location,” says Dan Frey, product marketing manager.

The firms SSL Network Extender is a browser plug-in that provides SSL VPN-based clientless remote access, while delivering full network connectivity for any IP-based application.

SecureClient Mobile provides uninterrupted remote access for Windows mobile devices. Check Point Endpoint Security is a single agent for total endpoint security that combines firewall, network access control, program control, antivirus, antispyware, data security and remote access.

Secure remote access doesn’t need to be expensive, says Farpoint’s Mathias. Just keep in mind the basics of information security — encryption and “Triple A,” authentication, authorization and accounting — and apply that universally. “If you have a good plan in those areas, you’ll probably be OK.”

**Developing a Mobile Worker Security Plan**
A compromise of security can do enormous damage to an organization.

We’re not just talking financial damage, we’re talking about reputation and goodwill, competitive position in the marketplace,” says Craig Mathias, principal at Farpoint Group, an Ashland, Mass.-based advisory firm specializing in wireless communications and mobile computing.

“People do lose their jobs and careers over errors in security. Developing a mobile worker security plan involves policy, education and keeping employees’ consciousness level raised. It starts with a basic security policy,” Mathias says.
Policy makers should ask themselves, what information is defined as sensitive? What are the criteria for information to be considered sensitive?

Once those definitions are in place, the questions should include: Who should have access to this data, under what circumstances and with what devices? What should the employee or company do if that information is compromised?

“You might allow unsecure access to the site,” Mathias says. “But if they want access to sales files, for instance, that would require a different password.

“Or both of those connections [onto the website and file access] might be secured using a Virtual Private Network [VPN],” he adds. “And this says nothing about the security of the information at the end, which should always be encrypted.”

Farpoint recommends that all sensitive information be stored encrypted anywhere it resides — whether it’s a server farm, data center or on a mobile device. Microsoft’s BitLocker utility is readily available on notebooks using Windows Vista Ultimate or Enterprise. For other Windows, Linux and OS X systems, the open source TrueCrypt application offers encryption for free.

**Education**

Employee education about secure remote access not only benefits the company, but it raises employees’ consciousness. “A lot of people have a somewhat lackadaisical attitude toward security,” Mathias says.

They pick passwords that are clearly subject to a dictionary attack, such as a cat’s name for password, etc., and then they don’t change passwords on a regular basis,” he adds. Educating employees on the dangers of security breaches and their responsibility to prevent them go a long way toward prevention.

**Keeping Travel Drives Safe**

Portable drives, where company information can be saved, transferred and potentially lost or stolen should be encrypted, security experts say. When choosing an encryption solution, make sure it won’t be too intrusive or complex for employees to use easily, says Craig Mathias, principal at the Farpoint Group advisory firm.

Check Point’s Endpoint Security Suite, for instance, allows users to manage all the ports on a notebook — as well as any devices connected to it that can store data, such as travel drives or iPods.

“You can enforce automatic encryption on all [attached devices], or you can manage by brand, device type or serial number of the device,” says Dan Frey, product marketing manager at Check Point Software Technologies Ltd.

In those cases, the drive is encrypted, as well as any data written to it, he adds. The Endpoint Security Suite also keeps a log of all files that have been transferred onto a flash drive or CD.

“A lot of what’s driving [heavy encryption] right now are regulations — PCI [Payment Card Industry], HIPAA [Health Insurance Portability and Accountability Act] and Graham Leach Bliley,” Frey says. “It’s for auditing purposes. They want to prove they’ve been locking down their endpoints.”

**CDW OFFERS TECHNOLOGY SPECIALISTS TO HELP PROVIDE A CUSTOMER SECURITY SOLUTION FOR YOUR BUSINESS. CALL 800.800.4CDW TO TALK TO A SPECIALIST TODAY.**

090617