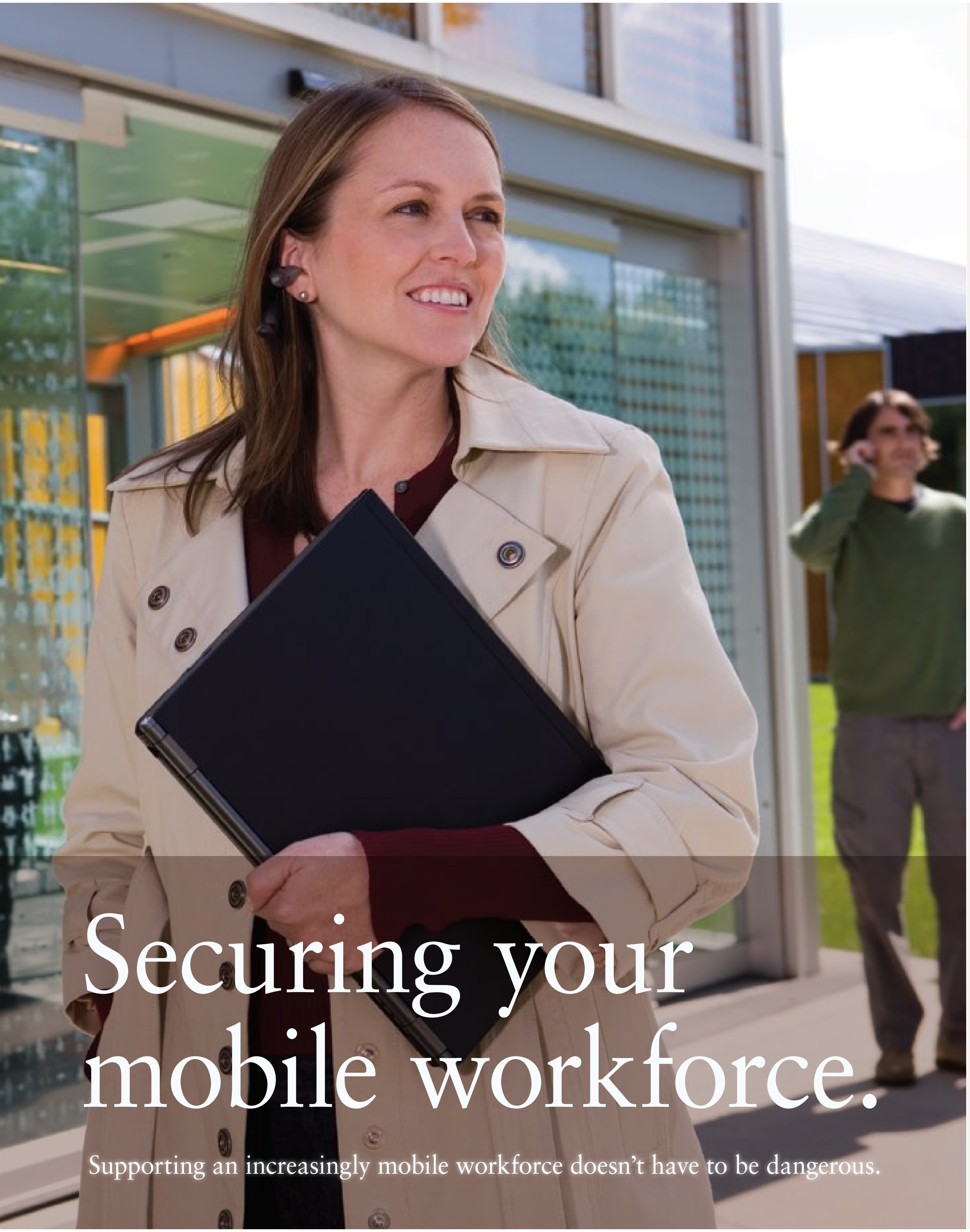

Securing your mobile workforce.

Supporting an increasingly mobile workforce doesn't have to be dangerous.

Mobility is the buzzword in today's workplace. Not only are new business roles outside the corporate campus constantly emerging, new employees are coming into the workplace expecting to be able to work from home, from the road — from anywhere they happen to be.

A more mobile workforce has many benefits for the enterprise. However, providing a roving workforce remote access to IT assets comes with new security concerns.

Making corporate resources available from anywhere adds a whole layer of complexity to the corporate network. And more complexity means new security risks.

Fortunately, a range of affordable tools exists for providing safe, secure access to network data from almost any device, whether it's a home computer, a notebook PC on a public Wi-Fi connection or a smartphone. Coupled with strong corporate security policies and smart computing practices, your mobile workforce can be as secure as your onsite staff.

The shape of remote access

Any remote-access system consists of three parts that need to be secured. Each of these is subject to different kinds of attacks and so needs to be protected in different ways.

1. **Endpoint.** This consists of the computer or smartphone that is used to access corporate resources.
2. **Endpoint Connection.** This is used to connect the endpoint to the corporate network.
3. **Enterprise Network.** It must be configured to provide the resources needed by the remote worker without exposing the network and the corporate systems within it to attack.

Because the endpoint is outside the direct control of the corporate home base, it is the piece of the remote-access system most vulnerable to attack. Notebooks are lost or stolen, cell phones disappear or break, and home computers are subject to malware of various types.

"The endpoint is risky for a number of reasons," says Sai Aloazarpu, senior director of product marketing for security and acceleration at Citrix Systems. "Each device comes with its own applications with their own risks, which need to be updated and patched. And you're dependent on the user to maintain the system and its security."

Simple carelessness on the user's part can be bad enough. But machines outside of the corporate environment are also subject to both incidental loss and intentional hacking — either of which can result in nonemployees gaining access to corporate data and resources.

Security problems at the endpoint can easily affect the corporate network if not adequately defended against. Viruses, Trojans and other malware can migrate from an infected notebook onto the corporate network causing system failure, use of network resources for sending spam or launching attacks on other systems, and loss of employee hours during recovery.

What's more, they can allow an attacker access to data on corporate desktop systems and servers. Or a keystroke logger on the endpoint can reveal network logins and other information to allow an unauthorized stranger to access the system elsewhere.

Lastly, remote workers have little control over the network connection they use to access the Internet (and thus the organization's network). Even a home network can be compromised by other computers on the network or by an improperly secured router or Wi-Fi access point that allows hackers to view Internet traffic. >>>

Steps toward mobile security.

Developing a security plan for mobile workers starts with asking these important questions:

1. **Who will be using remote access?** The policies you use to control access will depend on who will be using the network remotely and what they will be doing with it.
2. **How many workers will use remote access?** Your answer will determine not only how much server power you'll need to sustain the connections, but how many IT employees will be needed to maintain the system.
3. **How much access do we want to offer?** Few employees need to access everything on the corporate network. Knowing what access is needed and by whom will help keep the network safe.
4. **What are we trying to protect?** Different kinds of data and applications have varying security needs.
5. **How secure is the network before remote access?** Remote access places local resources at risk too. Any existing problems are going to be magnified when you add remote access to the mix.
6. **What kind of encryption do we need?** Do you need full disk encryption, which trades performance for security, or can you just encrypt specific folders or files?
7. **What policies do we need to enforce?** If you don't have clear security policies in place, configuring remote access will be challenging.
8. **What additional staff and training will we need?** Your IT staff needs to install and configure remote-access clients and protective software, manage updates and patches, and provide help-desk support.
9. **How will we manage installation, configuration and updates?** A small number of remote workers can be supported individually; for large remote workforces, tools such as a network access controller can help manage hardware and software in your extended network.
10. **How will we evaluate performance?** Successful attacks often leave no trace, so how will you know if your system is vulnerable? You need to establish networking monitoring and auditing best practices.

<<< The danger is multiplied when using completely foreign networks. These can include airport kiosks, Wi-Fi hotspots or hotel business centers to connect to the corporate network.

Endpoint security

It's true much of the work of providing secure access to the network for mobile users is handled by tools installed and run from inside the corporate network. Still, maintaining that security starts with protecting the most vulnerable part of the system: the endpoint.

Securing the endpoint begins with the same safe computing practices and tools you would use on any computer. Effective antivirus protection, a strong firewall and malware detection are all crucial to ensure that the endpoint itself is not leaking data to a third party.

Symantec's Endpoint Protection, for example, combines traditional virus and malware protection. Also included is a firewall and behavioral scanning that identifies suspicious activity due to threats that might not have been identified yet, such as zero-day exploits.

The use of hard drive encryption, for example Microsoft Windows 7's built-in BitLocker system or Symantec's Endpoint Encryption, is essential for mobile devices such as notebooks and smartphones that can be easily lost or stolen. Such protection can be applied either across the whole drive or in particular files and folders.

But keeping valuable data off the hard drive in the first place is equally important. Most current browsers offer a privacy mode that prevents logins and passwords from being saved and clears any cached data when the browser is closed.

These tools can drastically reduce the risk of an unauthorized person accessing either the corporate network or any restricted data, even if they get physical control of the device.

Couple them with strong passwords and multifactor authorization — biometrics or a tool such as an RSA SecurID device — for even greater levels of security.

Protect users from themselves

Even the most conscientious user can run into trouble. And most users do not fall into the most conscientious category.

"A lot of the advances in security boil down to protecting users from themselves," says Tamir Hardof, product marketing manager for network security at Check Point. A simple mistake can leave an endpoint wide open, and unfortunately most mistakes aren't easily visible, even to trained users, he says.

One way to reduce the threat of a remote employee's mistake is to bypass all or most of the endpoint. This would essentially turn the notebook or smartphone into little more than a screen with which to view remote data.

Citrix's Access Gateway, for example, serves as a virtualized desktop to the remote computer. An employee can view and interact with data and applications without ever transferring any actual data to the local computer.

"Desktop virtualization addresses endpoint concerns by eliminating the user's device from the equation," says Aloazarpu. "Even if you happen to access the network from an airport kiosk or hotel business center, you can still have access to the network's full resources, without compromising security." Virtualization functions as effectively as if the worker were sitting in front of a terminal in the office.

A new product by Check Point takes a slightly different approach around an endpoint's vulnerabilities. The Abra is a thumb-drive-sized USB device that can be plugged into any computer to create a preconfigured, secure virtualized workspace that does not interact with the host file system in any way.

Both of the above tools are variations on the virtual private network (VPN), which is the standard for connecting remote devices into an organization's network. VPN creates a secure end-to-end tunnel between the end user's machine and the server.

Traditional IP Security (IPSec) VPNs, which rely on resource-hungry and preinstalled clients at the endpoint, are rapidly being replaced by Secure Sockets Layer VPNs, which use the SSL protocol already used for everything from online banking to credit card transactions and webmail. In many cases, users can log into an SSL VPN from any machine, usually using a Java client that is downloaded on demand.

One of the features built into the VPN protocol is host checking, which allows the host server to remotely scan the endpoint for compliance with a range of security policies and to install and remotely run software if needed. For example, Juniper Network's SRX Series Service Gateways scan the endpoint to determine both the identity of the user and the health of the endpoint before allowing access to the network.

"If there's a problem, we offer self-help and remediation. The user is put into a quarantined virtual LAN and offered the ability to install the files and updates needed to secure their computer," says Greg Maudsley, Juniper Networks' senior manager of product marketing for access and acceleration.

Symantec's Protection Suite and Check Point's Connectra VPN gateway offer similar capabilities, using security policies to determine the level of access to be extended to the endpoint. "If the user is not behind the corporate firewall, you need to know what's coming into the environment," says John Engels, Symantec's group product manager in endpoint security.

Despite their more limited capabilities, smartphones are becoming increasingly popular as tools for accessing corporate resources. Symantec's Mobile Security Suite helps to secure Windows Mobile and Symbian-based phones with malware protection and encrypted folders.

Remote access and disaster recovery.

Network access is absolutely essential should there be a business interruption. It's during these times when alternate forms of connectivity and communication for employees are even more important.

To help, Juniper Networks offers a short-term "In Case of Emergency" license that lets a company drastically increase the number of remote users on its system in the wake of a natural disaster or other problem that prevents employees from coming into the office.

Likewise, Citrix recently introduced a virtualized version of its Access Gateway that runs as a virtual server. "When a snowstorm or other disaster strikes, you can just download and run additional instances to add capacity," says Sai Aloazarpu, senior director of product marketing, Citrix Systems.

Most smartphones can be configured for VPN access. However, Cisco's recently announced AnyConnect Secure Mobility Client aims to simplify the process of accessing the home network. It detects the capabilities of the endpoint and automatically provides the services appropriate to it. This allows workers to seamlessly and transparently shift from smartphone to Linux netbook to Windows or Mac desktop without any configuration.

Finally, there is an element of remote security that is often overlooked: backup. "Data security and reliable on-the-road strategy involves backing up," Engels points out. "If anything goes wrong, you can get that user back up and running fast."

Anything can happen out on the road. Regardless of whether a notebook is dropped in the street and run over or wiped out by malware, the data — and the work that went into it — is still lost.

Going mobile

Aside from increased peace of mind — a valuable benefit in its own right — an effective remote-access plan can vastly increase business productivity while lowering costs. By unchaining workers from their desks, onsite staff can extend their workday to accommodate larger projects, and remote teleworkers and mobile staff can be added without the increased overhead of providing office space.

Because remote access offers workers far more flexibility about where and when employees work, they can more easily balance their workplace obligations with the demands of their home life, which improves morale and increases productivity. As part of a business continuity plan, remote access can recover hundreds or even thousands of work hours by allowing employees to stay productive even when they can't get into the office.

All of these benefits come at the cost of increased complexity and security risk, but are manageable with solid planning. "When people build insecure solutions," says analyst Mark Kadrich, CEO of the Security Consortium, "it's almost always because they didn't take the time to plan, and that leads to a haphazard implementation."

Ultimately, remote access is simply another part of the enterprise network, and securing it relies on the same principles already in use in securing the LAN. "IT directors don't need to ask what policies they need for remote access," says Maywun Wong from Cisco's security marketing team. "They need to ask, 'What are the policies we want to enforce for both mobile and onsite access?'" ◊