

*Grant Thornton Extends Business Reach
with Fiberlink's Policy-Based Remote Access Solution
By-Leslie C. Wood*

With today's ever-growing number of remote workers and mobile users, providing effective and secure remote access is critical to the success of any enterprise. Enterprises today rely on multiple devices (laptops, desktops, personal digital assistants, and mobile phones) and multiple mediums (dialup, DSL, cable, wireless, and satellite) to connect remote users to corporate data. While the technology deployed for remote access must offer reliable, seamless function for the user, it must also provide security at the enterprise level.

The Challenge

Grant Thornton is a leading UK business and financial adviser to mid-corporate businesses and their owners. The company provides a comprehensive range of business advisory services in over 110 countries and employs over 3,000 mobile and remote workers who must be able to connect quickly and easily to the company's business-critical applications.

With the growing popularity of broadband technologies such as DSL and cable at home, as well as Wi-Fi at airports and hotels, Grant Thornton employees clamored for faster access and greater flexibility than what the company was offering with its dial-up service. In addition, the increasing number of employees accessing the network through transport technologies not supported by corporate IT not only raised security concerns, but also inflated access costs beyond the company's budget.

Grant Thornton required a more comprehensive remote access strategy that would consolidate the myriad of connectivity options available to employees, and ensure that anyone connecting to the network was compliant with corporate security and usage policies.

Access vs. Security: Finding a Balance

"Supporting a diverse mobile workforce can create enormous complexities for IT. Trying to keep up with today's rapidly changing protocols, incompatible access technologies, complex infrastructures, and mounting security threats is like running in quick sand," said Dave Johnson, director of infrastructure technology at Grant Thornton.

As Grant Thornton considered options for improving remote access and security, the company recognized the importance of simplifying the remote access experience for its remote and mobile workforce. The IT department needed to take the guesswork out of how employees connect to corporate resources by automatically presenting users with one-click access to optimal connectivity options.

"We didn't want users to worry about the logistics of one type of access over another," said Jim Moore, the firm's senior technology manager.

In order for Grant Thornton to ensure seamless connectivity and total compliance with corporate policies regardless of user's access type, device or location, the company needed a unified client to bring together all of the necessary connection and security elements of remote access into an intuitive user interface.

The Solution

Grant Thornton decided that Fiberlink's remote access solution would best meet its needs for global access by providing a full suite of transport options, as well as robust security through integrated, best-in-class technologies such as VPN, personal firewall, anti-virus, and centralized policy management. Within 30 days of deployment, all 3,000 Grant Thornton employees were up and running.

"While we had a hardware-based firewall, anti-virus software, and a VPN solution -- integrating and managing these effectively was a challenge before we had the Fiberlink solution," said Johnson. "Now, the Fiberlink solution integrates best-of-breed security from system start-up to shutdown so that users are always protected," he continued.

With the Fiberlink solution, Grant Thornton can now set policies that ensure that a connection to the Internet cannot be established unless the VPN client and software-based firewall are both running and updated on the end-user's corporate-issued laptop. In addition, the solution provides the company's IT department with unmatched control over the firm's expanding business ecosystem, controls costs, and minimizes business risk.

Results

Since implementing Fiberlink's remote access solution, Grant Thornton has achieved 100 percent compliance with its network access and protection policies, dramatically improving security across the enterprise. With unified management and control, infected machines can no longer compromise the network. So far, Fiberlink's layered security has isolated all high-traffic viruses even before anti-virus vendors sent out alerts. This has spared the firm from productivity losses and the costs incurred when IT resources must be diverted to recover from an attack.

The freedom of a mobile employee to connect to the network via multiple forms of access, anytime, anywhere has accelerated how quickly Grant Thornton's professionals can access the network at the end of a workday to enter billable hours into the firm's billing system. By receiving this information in a more timely manner, Grant Thornton has shortened the time from when services are provided and when payment for those services is received, ultimately improving cash flow for the firm.

Fiberlink's CostView reporting system has saved Grant Thornton's IT staff hours each month by generating a summary of each employee's network access charges so the IT department can accurately track and charge back each user's costs to their respective office. Previously these time-consuming reports were compiled manually, making them prone to error.

Another module of the reporting system, ConnectView, enables IT to identify and proactively troubleshoot end-user connectivity challenges, thus reducing help desk calls.

Fiberlink has enabled Grant Thornton the ability to facilitate its mobile working environment and identify new ways of doing business. “Our tax department will start sending tax professionals to client sites the same way we send *auditors* to client sites. This was inconceivable before because the tax professionals relied so heavily on the network to access applications and research,” said Moore. With Fiberlink, we can support them as if they were in the office, without worrying about the security issues associated with working at a client location,” he continued. When its tax professionals begin working at client sites, Grant Thornton plans to add 700 employees to its list of heavy network users.

Recently, the firm started working with a major client in a state without a Grant Thornton office. By implementing Fiberlink’s remote access solution, close to 200 Grant Thornton professionals at that site will have access to the firm’s network. “Having the ability to move hundreds of tax professionals anywhere in the country, at any given time, in order to support the needs of our clients is extremely valuable to us,” said Moore.

As the needs of the business change, Grant Thornton’s IT staff will require an increasingly dynamic way to set and enforce policies. Fiberlink’s new Extend360 client provides Grant Thornton’s IT team with the control and flexibility they need to extend corporate security policies to any remote endpoint. When a user connects to the network, any policies set by IT will be actively pushed out to the user and automatically implemented. IT will even be able to set different policies for different groups, all the way down to individual users.

Looking Ahead

Now that the firm has implemented a comprehensive enterprise remote access solution, its IT department is positioned to be more aggressive about deploying Wi-Fi – treating it as a strategic decision to further drive productivity. Previously, the security and management concerns associated with wireless prevented the firm from pursuing a broader deployment.

“Because the nature of our business has always required our employees to be mobile, we have consistently outpaced the competition in taking our business as close to customers as possible,” Moore said. “With Fiberlink, we feel well equipped to face the new complexities of remote access as computing environments evolve, ubiquitous wireless becomes a reality, and online threats become more sophisticated,” he concluded.