PowerTech
your security expert

WHITE PAPER

Build vs. Buy

The Argument Against Developing a Solution for Network Security

By Robin Tatam

Customers sometimes ask whether it's really worthwhile purchasing a product like PowerTech Network Security to protect IBM i data from the potential threat of unauthorized access by PC users on the network. They say, "Why not just develop it ourselves? After all, there are many tools available to make this easy, right?"

Before you commit the resources to develop an in-house solution, read our list of issues to consider. Hopefully, you'll understand that it's neither easy nor cost-effective to set up and monitor your own in-house solution.

Understanding the details of how server exit points work is not easy.

PowerTech Network Security already understands these details and is backed by a team of development specialists to ensure that it's up-to-date with the latest developments—including new IBM i exit points.

IBM might add new exit points with each new release of IBM i.

You can't just write an application and forget about it—it needs maintenance. Just "staying current" requires the dedication and application of programming resources to maintain the exit programs each time the operating system is upgraded.

An easy-to-use interface is fairly difficult to program.

Unless you write a user interface for the exit programs (such as the one provided by Network Security) you must manually add names or TCP/IP addresses into a data area, database file, or the program. Entering data such as TCP/IP addresses manually is extremely error-prone and confusing for non-technical operators and administrators.

Sometimes IBM releases PTFs that break exit programs.

With so many exit programs on the market, it's difficult to ensure compatibility across the range. PowerTech figures out what's failing, reports it to IBM, and works with them to find a solution. In the interim, we provide suggestions or a workaround so our customers aren't adversely affected.

The PowerTech Group, Inc.
www.powertech.com • info@powertech.com
TEL USA: 253.872.7788
TOLL FREE: 800.915.7700

Adding advanced features to developed exit programs takes security expertise and programming resources.

With a solution like Network Security, customers get access control (the ability to control who uses functions such as FTP or ODBC), plus advanced features such as network auditing, message alerts, transaction-level and object-level security, support for supplemental exit programs, and profile switch capabilities.

Software development is very expensive.

It's usually more productive to use an existing application if a viable one is available. The cost is far lower than what it would take to develop, test, and maintain your own application.

- Testing network access is very time-consuming and setting up testing facilities can be complex. Network Security was designed and developed over many years using the experiences, knowledge, and feedback of customers and configurations around the world.
- Maintenance programming requires special personnel. Leaving the responsibility of keeping software up-to-date (and other issues) to external vendors frees internal resources for more productive activities.
- The cost of maintaining a solution used by over a thousand customers is less than developing one internally. Keeping the in-house solution up-to-date costs far more than 20% of the purchase price typically charged for maintenance (which is low in comparison to internal development).
- Keeping the personnel who developed an application is often cumbersome and expensive. And for what—maintaining code that could be outsourced to a vendor, like PowerTech? We often talk to customers who have to scramble to recover from the loss of a key staff member.
- Adopting an outsourced solution achieves the separation of duties required by auditors, guaranteeing higher quality and more reliable security controls.
- Keeping people up-to-date with the latest security issues is expensive and difficult. It's hard to achieve the level of knowledge a company such as PowerTech has gained through daily experience with thousands of customers in a wide range of environments. But, it's easy to purchase this collective knowledge in a product that incorporates it.

What About Auditing Tools?

Most of these arguments also apply to the decision of building a set of auditing tools versus purchasing PowerTech's Compliance Monitor and Authority Broker. Again, why try to keep your set of tools current with each release of IBM i? And, why pore through IBM documentation trying to determine which interfaces you should audit?

Summary

We've talked to many customers who are considering writing and maintaining their own exit programs. Often, after we talk, they agree to try PowerTech Network Security. When you consider all of the costs and hassles of developing new solutions versus the ease of buying existing ones, it's easy to make the smart choice.

About the Author

Robin Tatam is the Director of Security Technologies for PowerTech, a leading provider of security solutions for IBM i servers. A frequent speaker on security topics, he was also co-author of the IBM RedBook "System i Security: Protecting i5/OS Data with Encryption." *Robin can be reached by e-mail at* ***robin.tatam@powertech.com.***