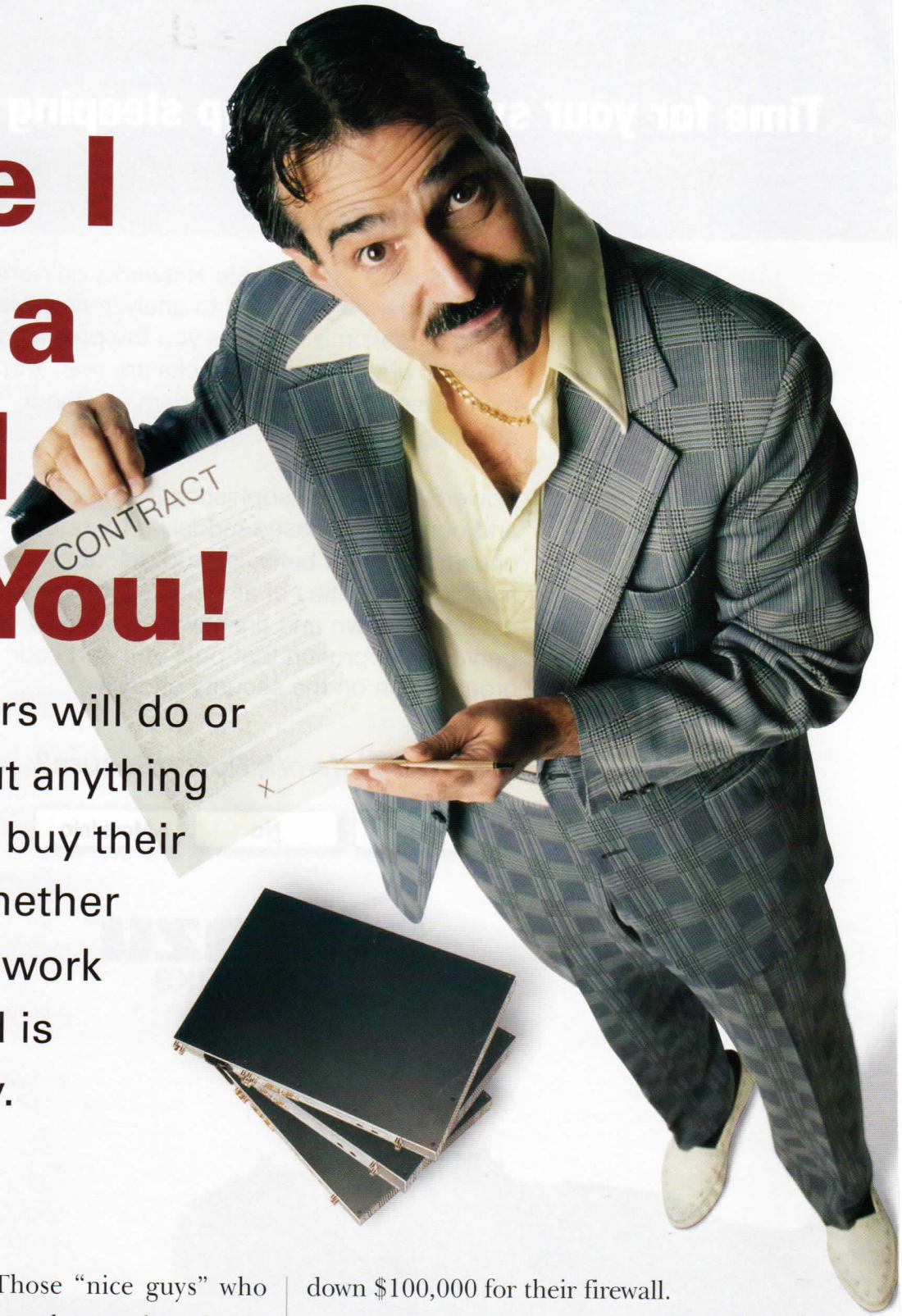
Have I Got a Deal for You!



Some vendors will do or say just about anything to get you to buy their products. Whether the products work as advertised is another story.

by LINDA WISE

Caveat emptor. Those "nice guys" who took you to dinner last week and sent you an Eddie Bauer windbreaker may not be acting in your interest after all. Better you discover that now than after you've plunked down $100,000 for their firewall.

Not all infosec vendors are charlatans and snake oil salesmen. But how do you spot those who are? Here are some common scenarios and practical tips.

Purposeful Ambiguity

Vendors love to tout how their new technology is the greatest thing since sliced bread. Boisterous claims are often a sign of immature technology or ambiguously defined solutions.

Those solutions are often explained with fashionable security terms in marketing brochures—intrusion detection, cybervaults, digital rights management, behavior-based anything, etc.

"Terms get co-opted, and people will use buzzwords that don't actually reflect what the product does," says Paul Proctor, president of **Practical Security** (**www.practicalsecurity.com**).

Probably the fuzziest term in infosec today is "intrusion prevention." Billed as the proactive alternative to reactive IDSes, intrusion prevention sounds good. But oftentimes it's no more than an existing technology that's been repackaged under the intrusion prevention banner.

"What is intrusion prevention, really?" says Jack Danahy, a former VP at firewall vendor **WatchGuard Technologies** (**www.watchguard.com**) and now president of infosec consultancy **The Danahy Group** (**www.danahy.com**). "If you look at the technology, it contains everything but the kitchen sink. Someone merely created a new category for everything that didn't fit neatly into traditional categories."

Don't get sucked in by hype. Determine a solution's true capabilities and buy what you need, not what's "hot."

Does Size Matter?

Smaller security vendors and startups often offer fresh and innovative solutions to longstanding security problems. However, they may be plagued by product immaturity, poor engineering support and financial instability.

The security marketplace is littered with the carcasses of vendors that went legs up, which has sapped confidence among prospective buyers. The managed security services market still grapples with the ghosts of The Salinas Group and Pilot Networks, both of which closed their doors in 2001 with little or no notice to customers.

Conversely, large companies have money and track records, but not always the best solutions. They use their market presence to pressure deals.

"There's an old saying, 'No one ever got fired for buying IBM,'" says Cindy Boyd, president and CEO of consulting firm **Sentigy** (**www.sentigy.com**). "But the big companies can be just as bad as the small guys. Buyers have to use a criteria-based selection process or they can still get burned."

Weigh your needs for product innovation against performance risks. Examine vendors' financial health, evaluate their track records, and be sure they have adequate resources to fulfill their obligations. Talk to existing customers to identify potential problems—and make sure they're fixed before you sign on the dotted line.

Who Needs a Test Drive?

Anne Rogers, director of information safeguards for Houston-based Waste Management, has seen so many vendors who misled with their sales and marketing tactics that she has stopped paying attention to product literature.

"If we can't do a field test or proof-of-concept trial, I won't take it," says Rogers, whose company provides refuse removal for 27 million commercial and residential customers and has more than 57,000 employees in 48 states.

Pilot testing seems like a no-brainer, but many companies still blindly trust vendors' brochures and sales pitches. Rogers made this mistake early in her career when she purchased a security information management system. It was only after she bought the product that she discovered incompatibility issues with existing systems. Her company ended up canning the project and building a homegrown solution.

"A slide presentation or demo doesn't do it," she says.

Enterprises want to know what security solutions will do for them once they're deployed, but the installation process may reveal problems. If the first version of a product is late to market, software companies will often skimp on the installer. If the installer is flawed, there might be more serious issues.

"Ask for a copy of the software or a live demo in your environment to see how hard it is to install," says Dr. Rich Murphey, CEO and chief scientist for security provider **White Oak Labs** (**www.whiteoaklabs.com**) and the former principal architect at **NetIQ** (**www.netiq.com**). "If they tell you they need to send out a team of three people who will take a week to install it, that's a bad sign."

Alarms should also go off if a vendor is sending its CTO or top developer for installation or service calls. Typically, this isn't a reflection of "excellent customer service," but of a product that requires a lot of watering and feeding.

Buying Tips

1. Don't be swayed by fancy marketing terminology or "dog and pony show" sales pitches. Evaluate security products in terms of how well they fit a defined need.
2. Size matters. Find a good balance between new security startups with unproven technologies and ponderously large vendors for which you'll be "just another customer."
3. Test-drive all products in your environment before agreeing to anything. If you can't use the product without the help of the vendor's CTO, it's a good sign that something's wrong.
4. Make sure you understand regulatory requirements before deciding how well a particular solution helps you meet those requirements.
5. Read the fine print in all contracts before signing off. Don't assume the vendor is operating in your best interests. ◗

photograph by ROSS ANANIA/GETTY IMAGES

Regulatory Pressure

Mike Siegel laughs when asked if his consulting firm, **Sirius Solutions** (**www.sirsol.com**), is partnering with security vendors who have "proven track records" in helping companies comply with the federal Health Insurance Portability and Accountability Act (HIPAA).

"A track record?" says the IT manager. "No one can legitimately claim they have a long track record in helping companies comply with HIPAA security standards." The privacy rules weren't released until February and didn't go into effect until April.

Spending blindly in the name of regulatory compliance is a common mistake made by companies, says Siegel. Laws—such as HIPAA, the Gramm-Leach-Bliley Act (GLBA) for the financial services sector and Sarbanes-Oxley Act for publicly traded companies—telegraph future security requirements. However, while many laws' security requirements are defined late in the regulation development process, vendors are quick to push "probable solutions."

"Anyone who bought HIPAA-compliance services before the ruling was final took a big risk," says Siegel. "While [a nonrequisite item] might add an extra layer of security, you wasted your money if [the product] wasn't in your business plan to buy anyway."

When it comes to regulatory compliance, look before you leap. Vendors will say their solutions are based on best practices, which provide good security regardless of a law's final requirements. But if the regs aren't set and you don't have an immediate need, you may want to delay your purchase.

Fine Print Has Meaning

Vendor salespeople have financial incentive to accentuate their offering's strengths and conceal its weaknesses. That can give an impression that features and support are included when they're not.

Security consultant T.C. Lipe, a former senior systems analyst for BASF, says he has encountered several companies whose brochures said one thing, but delivered another.

"One company that sells scanning and vulnerability testing said if we were to hire them, they would find all the vulnerabilities on our network," Lipe says. "After we contracted with them, they only ended up finding a few."

If that wasn't bad enough, the vendor, which Lipe declined to name, tried shaking down BASF for additional fees for work Lipe thought was included in the negotiated contract. It was a hard lesson for Lipe, who says the original terms were changed by the vendor somewhere in the approval process.

"All their brochures said 'complete, total, the entire network,'" he says. "The final contract did not."

Bottom line: Always pay attention to the fine print.

Power Schmoozing

Three martini lunches. Fine gourmet dinners. Lavish cocktail parties. Sales retreats at exotic locales. Expensive gifts. These are examples of "power schmoozing," or using any excuse to get salespeople in front of prospects.

Take last year's Gartner Group Security Conference. Several large infosec vendors—**RSA Security** (**www.rsasecurity.com**), **BindView** (**www.bindview.com**) and **PricewaterhouseCoopers** (**www.pwcglobal.com**)—hosted after-hours wine tasting events, golf clinics and parties. The next morning, no one mentioned products. Instead, they talked about who had the best party.

Few buyers will admit that junkets influence their purchasing decisions. Nevertheless, relationships are the name of the game in technology sales. And if they're not courting you, they may be entertaining the higher-ups, leading to power plays with games like "my VP knows your VP."

"This kind of sales pressure can cloud a buyer's judgment," says Sentigy's Boyd, whose firm helps organizations optimize their processes in networking and security. "It moves away from being what's really good for the company to corporate politics."

Schmoozing and power plays are nullified by scoring systems. Through predefined criteria, enterprises are able to evaluate and compare different product offerings, and choose the best solution for their needs.

Too Good to Be True

Remember the adage, "If it's too good to be true, it probably is." On paper, there isn't a product or service that doesn't solve an enterprise's security needs. But the reality is no product or service solves every security headache, even when it's designed for specific problems.

"Some people are so afraid, they will buy just about anything," says Danahy. "Vendors, because they understand this, can often position their product as something to mitigate their fears rather than solving problems."

Experts agree that recognizing sales spin and building processes to neutralize it in the product evaluation and acquisition process is critical. Yes, it's expensive and time consuming to predefine security needs, evaluation criteria, a formal RFP, pilot or beta testing program. However, the upfront effort will pay high dividends once the purchase order is executed.

"If you buy based on criteria, a vendor hasn't sold you snake oil," says Practical Security's Proctor. ◗

LINDA WISE (**linda@wiseconsultants.com**) is principal of Wise Consultants, a marketing and corporate communications consulting firm, and an officer of the Houston InfraGard chapter. She is the former director of marketing for Blue Lance.