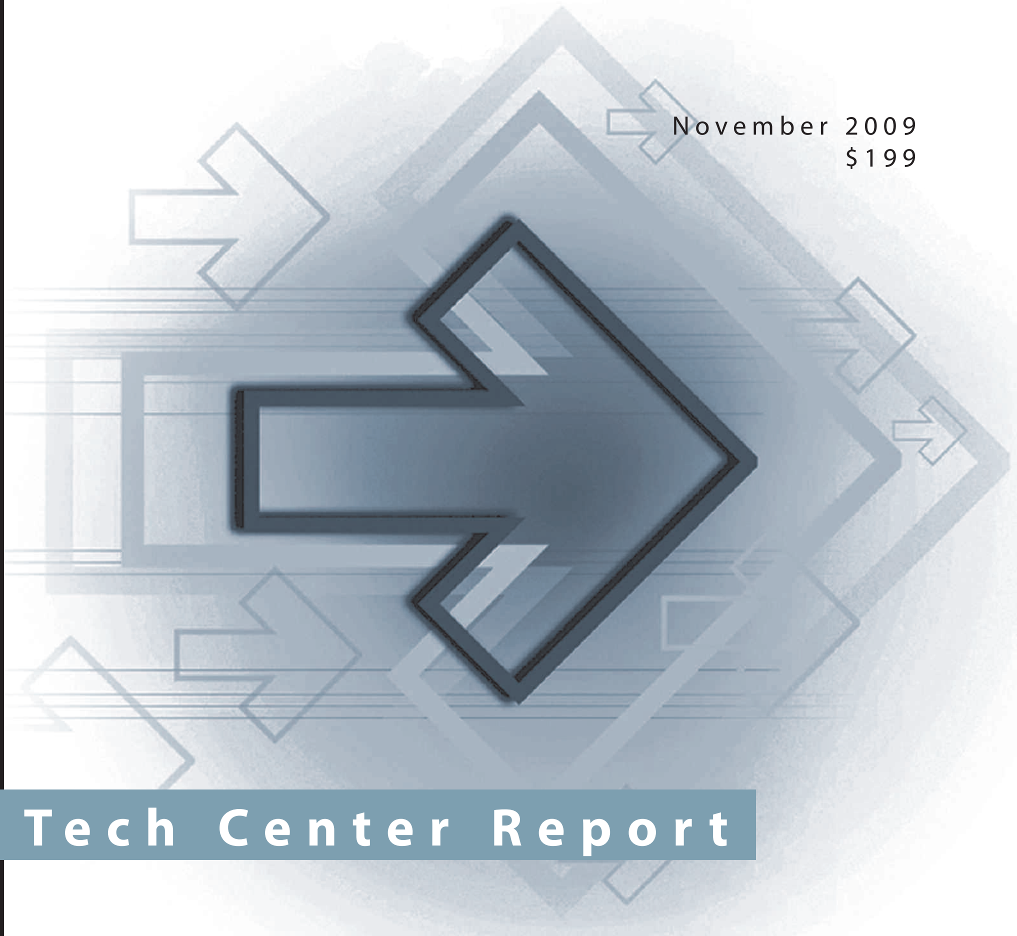
InformationWeek
:: analytics

November 2009
$199



SECURITY
dark READING Tech Center Report
Protect The Business Enable Access

Security Services Strategies For Small and Midsize Firms

Infosec managers in small and midsize enterprises often feel like an army of one, constantly pinching pennies. But the paradigm shift from expensive on-premises management to off-premises hosting is good news for you, because today more than ever, the small business has access to large-enterprise security technologies via the phenomenon of subscription-based licensing. By using security services strategically, you can gain economies of scale—and a really deep bench.

By Randy George

Contents

Randy George
InformationWeek Analytics

Randy George has covered a wide range of network infrastructure and information security topics in his three years as an *InformationWeek* and *Network Computing* contributor and security beat owner. He has 13 years of experience in enterprise IT as a senior-level systems analyst and network engineer and holds professional certifications from Microsoft, Cisco and Check Point.

Randy earned a BS in computer engineering from Wentworth Institute of Technology and an MBA from the University of Massachusetts Isenberg School of Management.

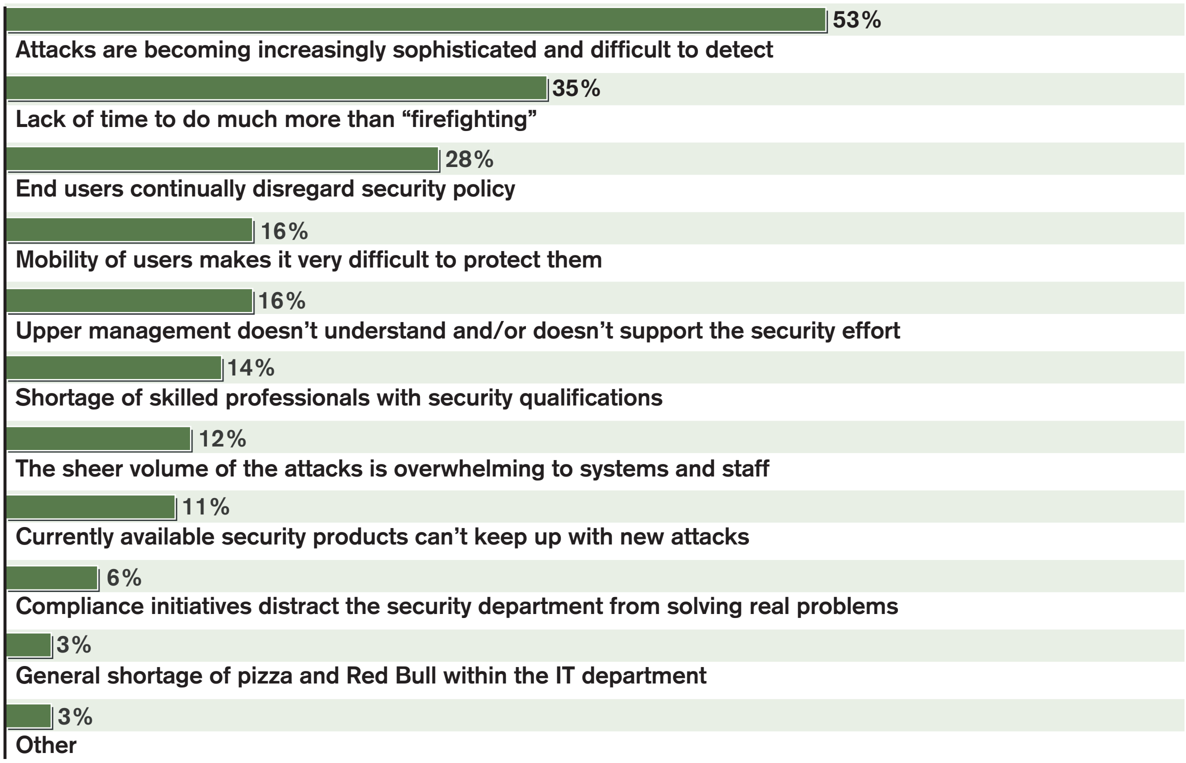
Home Field Advantage

The downturn in the economy coupled with a credit crisis that has hit small businesses disproportionally hard make it challenging to move security initiatives forward. In addition, SMBs, as shown in our *InformationWeek Analytics*/Dark Reading survey of 250 business technology professionals at companies with fewer than 1,000 employees, face a lack of specialized expertise and time constraints. Meanwhile, data and network assurance requirements imposed by governmental and industry mandates like PCI-DSS are reaching down to impact even the local pizzeria. We all know that allocating resources to network security initiatives is tough when dollars are tight. However, doing nothing could cripple your business, land you in court—or both.

Figure 1

Greatest Security Challenges

Which would you say are the greatest challenges facing IT security departments today?



Note: Two responses allowed
Base: 250 respondents at companies with fewer than 1,000 employees
Data: *Dark Reading/InformationWeek* Analytics Security Survey of 414 business technology and security professionals

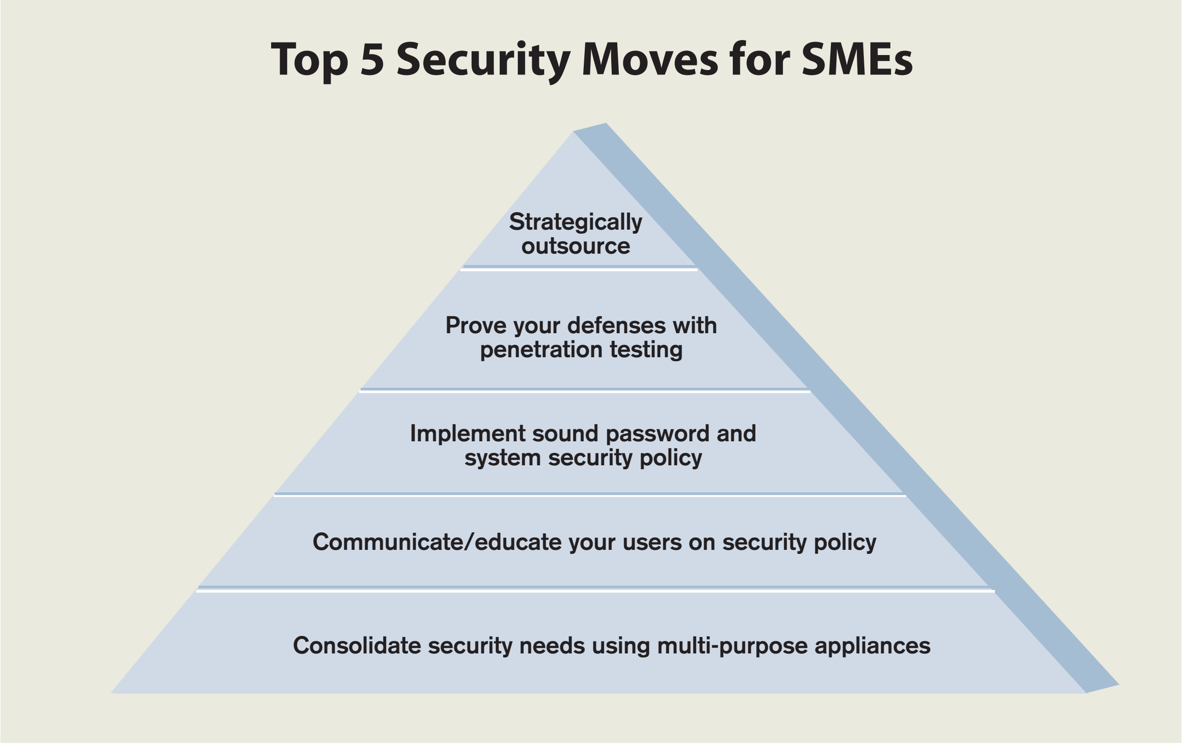
Fortunately, security vendors are not only sharing in your macroeconomic pain, they're changing their business models in the face of cutthroat competition. Consumers and enterprise IT groups alike are demanding that which Salesforce.com made cool when it opened its doors back in 1999. Purchasing software or infrastructure via a SaaS-based model is now universally embraced as a safe and effective alternative to expensive on-premises systems.

That's bad news for some security vendors, because now that enterprises trust SaaS, we're demanding *everything* in a subscription-based model. It used to be that outsourcing security was well nigh unthinkable. Imagine going to your favorite Web security company 10 years ago and saying, "I like your WAF, but I don't want to buy it, I only want to rent it. Oh, and can you host and manage it for me?" Such a request would almost certainly been met with derision.

Who's laughing today?

The question then becomes, how do SMBs leverage this new way of doing business to meet their security needs? In this *InformationWeek Analytics*/Dark Reading Tech Center, we'll explore

Figure 2


Top 5 Security Moves for SMEs
Strategically outsource
Prove your defenses with penetration testing
Implement sound password and system security policy
Communicate/educate your users on security policy
Consolidate security needs using multi-purpose appliances

strategies that small businesses can use to evaluate their requirements and map them to some of today's innovative SaaS-based offerings. Along the way, we'll plant the seeds of what could grow into a comprehensive security plan for your organization that actually frees up dollars, and resources, by "renting vs. buying."

Small Is Beautiful

The biggest thing SMB IT pros have going for them is an intimate knowledge of how the business operates, where its sensitive data resides, and what its weak points are. By contrast, big business IT execs must unwind complex business processes and navigate large organizational structures in order to clearly understand the security landscape. Enterprises' weak points are tough to evaluate, and even tougher to plug. And sensitive data? It's everywhere.

Data thieves today are motivated by money, and they make money by trading control of spyware-infected PCs on the black market. Attackers don't generally care anymore about corrupting your employees' master boot records—they need those computers running so they can steal data or use them as drones for mail blasting or DDoS attacks. If a single PC gets turned into a zombie, that's an issue, but the damage can be contained. But if a piece of malware goes after the source code to a very critical, and valuable, application, then you have a real problem. As a result, when evaluating your security needs, do so with a keen eye on protecting data first, with system integrity being a secondary priority.

First, ask yourself three important questions, with a data-centric focus:

1 | Put yourself in your CEO's shoes. What data would she be most upset about losing?

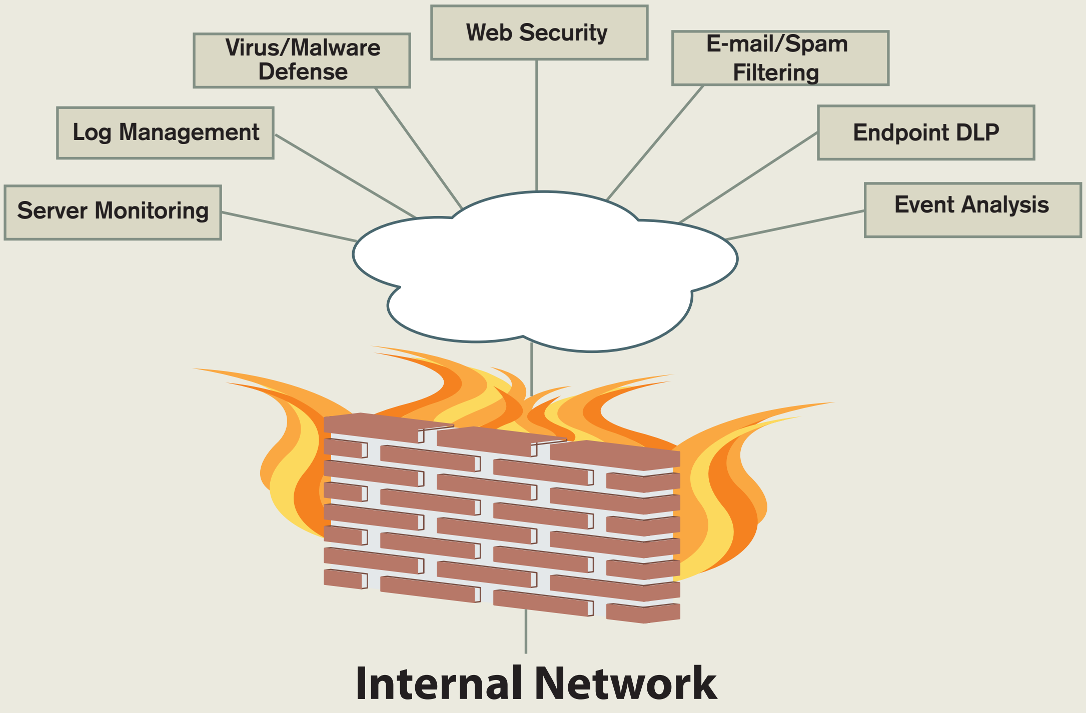
To map out a truly effective security plan, you need think like the boss and view the world from that vantage point. You already know that you need to protect credit card data, Social Security numbers and other personally identifiable information (PII). But what about a customer database? What about your company's R&D roadmap? Or how about the M&A plans that a management consulting company is clandestinely working on for your organization?

In some respects, losing this ancillary, company-specific information is much more damaging to your organization compared with some annoying worm or virus.

2 | What data privacy regulations are you subject to? And don't say "none."
This might not be as easy as you think to determine, so spend some time here, because it's a critical facet to the development of a proper security plan for your organization. In our *InformationWeek Analytics* 2009 Strategic Security survey, 32% of respondents said they're required to comply with HIPAA. That's up 12 points from 2008, when just 20% said they needed to comply. What worries us is that some respondents are clearly in a state of denial—could it be true that 68% never handle credit card data? Because if you do, and you're careless with how you processes credit cards, you could be setting yourself up for a PCI audit and/or scrutiny from a state governmental body that's enforcing local data privacy laws. So while Nick's Pizza needs only a small subset of compliance systems compared with a medical office, it's important that you map out a plan with an eye on what's expected of you from a legal standpoint.

Figure 3

What's Available From MSSPs?



The range of options for shifting some or all of your security needs to the cloud is evolving by the day. These are just a few examples of services that you can obtain in the cloud for relatively short up-front capital.

If you aren't sure what data privacy laws you're subject to, ask your security vendor or systems reseller. And realize that a growing list of legislators from states including California, Massachusetts and Michigan, to name a few, are imposing aggressive state-mandated data privacy rules on businesses of all sizes. Now, stronger data privacy awareness, and even legislation, is certainly a win for consumer privacy advocates. Unfortunately, that win comes at the expense of SMBs, which generally have a difficult time fully funding IT initiatives related to the core business, let alone projects to ensure compliance with an ever-increasing set of vague, state-mandated data privacy laws. Regardless of your political feelings, these laws are likely coming to your state soon, if they haven't already. For example, when the Massachusetts law goes into effect in January 2010, any out-of-state company that holds the PII of a state resident is on the hook.

3 | Where exactly is your data?

In the world of physical security, it's difficult to defend a person or item over which you have little control. The challenges around protecting IT assets are no different. You must have intimate knowledge about all data sources in use, both structured and unstructured (database and flat file), you must know what sensitive information is contained in those data sources, and you must know everywhere they are.

In our experience, SMBs tend to have sensitive data on employee's home machines; on removable media; or if you use cloud computing, on 100 file servers scattered throughout the globe. If you're not sure where your data is, you need to find out, because you can't protect something that you can't see. If necessary, purchase a robust data discovery product, like Symantec's DLP (formerly Vontu) or RSA's DLP (formerly Tablus), so you can proactively crawl all data sources and systems for sensitive content. It's the only foolproof way to determine your actual exposure. Once you know where your data is, you can move to protect it via a combination of in-house and SaaS strategies.

Fast-Tracking Security

Salesforce.com's marketshare has exploded over the past few years for one simple reason: Customers can flip a switch and rent a CRM app that has 95% of what they needed with minimal hassle and upfront cost. When it comes to analyzing what security service providers bring to the table, the real value does not necessarily lie in cutting costs, because over time, a SaaS approach might actually cost you more. So don't try to make the case based on cash savings.

Rather, for most SMBs, the benefits of SaaS and third-party security fall into three areas:

> Cutting down on the stress associated with managing complex security apps in house.

> Getting up and running quickly. No procuring servers or training on an unfamiliar interface while your systems remain exposed.

> Letting you focus on your business without having to worry about installing updates, patches and firmware updates.

Sound great? Well, just as saving a few hours by hiring a landscaper to help with your lawn might be ideal in theory, you're on the hook if they do a bad job or fail to show up at all. Just because a third party is managing a given security function doesn't necessarily mean the outcome will be what you expected. With on premises equipment, if you don't like the results, you're on the hook to suck up the capital costs of the gear. With SaaS, if you're not happy with your vendor of choice, cutting over to a different vendor once any contracts expire is generally easy. Without a big up-front capital investment, you have no skin in the game. The vendor is on the hook to prove its value.

Renting vs. Owning Via SaaS

The number of SaaS-based offerings is growing quickly, so the question is not so much whether a particular security function is available, but rather, can a cloud-based service perform a given function for me faster and more reliably and for less money–or at least, for not much more than we're paying now? The answer depends on many organizational variables. However, if Cisco's recent acquisition of ScanSafe, and Baracudda's recent acquisition of Purewire are any indication, big names are putting their chips on the table and betting that you'll eventually embrace cloud security.

With SaaS, your analysis boils down to a decision of renting technology vs. owning it and renting management vs. owning it, and the decision is not an easy one. Let's take a real-world example that illustrates the decision.

As you can see from the Year 1 TCO, you're going to shell out around $38,000 to get up and running with an on-premises Web security system. Contrast that with the $15,000 you'll pay a

SaaS provider during Year 1. For smaller companies that have cash flow concerns, that’s a big deal. Now extrapolate your total cost of ownership into Year 5. As you’ll see, you can generally expect on-premises hardware to reach end of support and end of life. Assuming you’ll purchase new hardware at the same price point as in Year 1, this is where the numbers really skew the advantage toward a cloud-based system from a cost perspective alone.

We didn’t add in increases in pricing from the provider, but outside a contract, that could be a consideration. From an IT labor point of view, the benefits of rent vs. own cancel themselves

The Rent vs. Own Decision for Web Security

Own and manage Web security in house	Price	**Rent Web security from cloud provider**	Price
Blue Coat SG510 appliance with the Blue Coat Web Filter	$19,195	Annual subscription to Purewire’s Web security cloud (500 users @ $30/user/year)	$15,000
Blue Coat enterprise reporter	$6,741		
Server/storage required for reporting and logs	$3,000		
Annual maintenance/support*	$9,469		
Year 1 TCO:	$38,405	Year 1 TCO:	$15,000
Year 2 TCO:	$47,874	Year 2 TCO:	$30,000
Year 3 TCO:	$57,343	Year 3 TCO:	$45,000
Year 4 TCO:	$66,812	Year 4 TCO:	$60,000
Hardware end of life, must replace in Year 5	$38,405	Year 5 TCO:	$75,000
End of Year 5 TCO	**$105,217**	**End of Year 5 TCO**	**$75,000**

* IT labor cost of $500/month for backup and server maintenance plus utilities.

out. Typically, an administrator might spend a couple of hours a week managing a smaller Web security environment. Conversely, cloud Web security requires that each employee's laptop be reconfigured, and accounting for client-related issues that are bound to arise, an admin might spend a few hours a week supporting a cloud-based option.

Other non-financial variables skew in SaaS' favor for SMBs. Upgrades and management are done offsite, log management and reporting are included, and additional features such as basic DLP are typically available as part of the core cloud offering, for an extra fee.

Conversely, if you have tight security controls and strict log management needs, that might require an onsite system. Organizations with significant existing hardware investments will also have a more difficult time making the numbers work.

While Web security is just one course of the SaaS menu, what if circumstances dictate a completely outsourced model? What would that cost? To answer that question, we issued a fictional scenario to a major security services provider:

"The Velodyne Group is a hedge fund that's been operating under its parent company since its inception. At some point next quarter, it's getting spun out and will operate independently. Velodyne has no internal IT staff, only a part-time contractor responsible for various aspects of infrastructure management. As a result, Velodyne is investigating outsourcing its desktop/server virus defense and its e-mail and Web security needs vs. purchasing the required software licenses and appliances for in-house management. To perform a proper analysis, Velodyne needs approximate list pricing for what it would cost to protect its 100 employees and five servers."

The estimated total monthly charge to service this scenario in an MSSP model is $1,775 with a $3,000 installation charge. That includes completely managed, on-premises desktop and server virus defense and cloud-based e-mail and Web security. For an additional premium, complete desktop and server management can be had as well, which would negate the need for a full-time IT resource except for ad-hoc break/fix work.

Working the Cloud Into Your Security Plan

It's clear that SaaS has the potential to help small businesses drive down costs and acquire technology that they otherwise couldn't afford or manage themselves. However, cloud security providers and MSSPs are only building blocks toward a comprehensive security and compliance plan. A SaaS or MSSP player may do the heavy lifting for you, but you're still on the hook if things go bad. However, with some help from cloud providers, MSSPs and automation, the typical small business IT manager can recover enough time to keep the house safe and secure from both inside and outside threats.

Take a risk- and product-oriented approach to working cloud security providers into the mix; the following chart is an example of the range of options you might explore for testing the SaaS waters. Clearly, in a high-risk, high-compliance environment, careful consideration should be given to any effort to outsource a strategic security requirement to the cloud. But in environments where security allows for some flexibility, it makes sense to pilot a low-impact, low-risk test of an outsourced security function.

SMB Security Checklist

Small, low-risk environment, no compliance mandates		Medium-risk environment, some compliance mandates		High-risk environment, significant compliance mandates	
Must have:	Available via SaaS?	Must have:	Available via SaaS?	Must have:	Available via SaaS?
Desktop virus defense	Yes	Desktop virus defense	Yes	Desktop virus defense	Yes
Server virus defense	Yes	Server virus defense	Yes	Server virus defense	Yes
Desktop malware defense	Yes	Desktop malware defense	Yes	Desktop malware defense	Yes
		URL filter, Web security	Yes	URL filter, Web security	Yes
		Spam filter, E-mail security	Yes	Spam filter, E-mail security	Yes
		Endpoint DLP	No	Endpoint DLP	No
		Endpoint encryption	No	Endpoint encryption	No
				Network DLP	Partially
				Log management	Yes
				Two-factor authentication	No

The lowest-hanging fruit on the outsourced security tree is Web security, URL filtering and malware protection. Companies like Perimeter, Purewire, ScanSafe, Webroot and zScaler often offer free trials where you can test their services for a limited group of users. Simply sign up, configure your policies through their admin GUIs, point your client to the service provider's proxy server, and you're done.

Smaller organizations can take advantage of integrated suites from companies such as McAfee, Symantec and Perimeter that provide desktop/server antivirus and anti-malware protection, as well as e-mail, Web security protection and more with unified management. Often, these suites start in the $50 per client per year range and provide much of what a small business needs from a product perspective, in a turnkey fashion, with the ability to add functionality as needed.

Using the medium-risk scenario presented above, that leaves IT managers to fill in protection gaps in the way of endpoint DLP (if necessary) and endpoint encryption, which is increasingly a requirement for state mandated data privacy laws. The product mix shown above is a general guide for the small business, and should be used in tandem with strong password policy and user education as part of a comprehensive security plan.

Mixing in SaaS where possible and recovering some man hours to actually define, manage and enforce your security plan is becoming an increasingly attractive option.