

## Market Overview: Managed Security Services

*Steve Hunt*

*Contributing Analysts: Philip Rosch, Michael Rasmussen, Julie Giera*

### Giga Position

Managed security services (MSS) is the catch-all expression that encompasses six categories of services: (1) on-site consulting, (2) remote perimeter management, (3) product resale, (4) managed security monitoring (MSM), (5) vulnerability/penetration testing and (6) compliance monitoring. Of course, some of these services do not imply “management” at all. But they are all included in the list of services of vendors that identify themselves in the MSS space.

Given this variety of services under the general market heading MSS, many vendors tend to promote capabilities and services that exceed their strengths or specialties. Therefore, prospective customers are encouraged to select vendors by mapping basic security processes to the categories of strength of a specific vendor. Furthermore, since the sum of all security (policies, procedures, awareness, forensics, human behavior and technologies) exceeds the capabilities of a single vendor, there is no such thing as a “pure” or “comprehensive” security vendor.

Giga clients are turning to outsourced security service providers in growing numbers. Common motivations for seeking outside help include the hope of reducing costs associated with installing, maintaining and monitoring security hardware and software; personnel shortages that plague many companies; and that much of security requires specialized tasks and dedicated staff. That growth reflects a general increase in IT outsourcing, compounded by pressing needs, plus a frenzy of marketing and confusion in the security space. Until now, prospective customers of these security vendors were left with no clear differentiation of the vendors or clarification about the categories of service.

### Proof/Notes

Linda Donner is a security project manager at a large Midwestern bank group. She was tasked with an Internet banking initiative. “That’s when security hit me,” she said. “You can’t work in this environment and not be protected.” She was chatting with her **Unisys** contractors about it when they mentioned the new security services being offered from Unisys headquarters in Blue Bell, PA. Today, Linda relies on Unisys to install and maintain the perimeter firewall, intrusion detection and even watch antivirus updates for the bank group.

Linda is not unique. Hundreds of large and midsize companies are realizing the need for security that exceeds their abilities to supply for themselves. With some luck and due diligence, Linda, and those like her, can contract satisfactory services from local, regional or national service vendors in a variety of categories.

### The Six Categories of Managed Security Services

1. **On-site consulting** — This is customized assistance in the assessment of business risks, key business requirements for security and the development of security policies and processes. It may include comprehensive security architecture assessments and design (including technology, business risks, technical risks and procedures). Consulting may also include security product integration and on-site incident response and forensics.
2. **Remote perimeter management** — This service installs and upgrades the firewall, virtual private

network (VPN) and intrusion detection hardware and software, commonly performing configuration changes on behalf of the customer.

3. **Product resale** — Clearly not a managed service by itself, product resale is a major revenue generator for many MSS providers. This category provides value-added hardware and software for a variety of security-related tasks.
4. **Managed security monitoring** — This is the day-to-day monitoring and interpretation of important system events throughout the network, including unauthorized behavior, malicious hacks and denials of service (DoS), anomalies and trend analysis. It is the first step in an incident response process.
5. **Penetration and vulnerability testing** — This includes one-time or periodic software scans or hacking attempts in order to find vulnerabilities in a technical and logical perimeter. It generally does not assess security throughout the network, nor does it accurately reflect personnel-related exposures due to disgruntled employees, social engineering, etc.
6. **Compliance monitoring** — This includes monitoring event logs not for intrusions, but change management. This service will identify changes to a system that violate a formal security policy — for example, if a rogue administrator grants himself or herself too much access to a system. In short, it measures compliance to a technical risk model.

### **Pricing**

For many of the MSS categories, prices are competitive and fairly stable.

#### ***On-Site Consulting***

Cost is \$2,000/day plus travel and expenses (T&E) for technical staff. It can be up to \$8,000/day plus T&E for senior strategists.

#### ***Remote Perimeter Management***

Simple installation and ongoing management of a firewall and intrusion detection at the perimeter consists of a variety of common charges: hardware and software (\$50,000), ongoing management (\$30,000 to \$40,000), plus setup and other one-time fees of \$10,000 to \$15,000.

Monthly charge by many outsourcers of firewall and intrusion detection monitoring and configuration change management is \$1,500/month to \$2,500/month.

#### ***Product Resale***

Prices vary widely in this category due to the variety of products sold and the extent of “value-added” services.

#### ***Managed Security Monitoring***

Prices vary depending on the complexity of the client’s internal network and the nature of the servers being monitored. Many customers pay between \$100,000 to \$200,000 annually (the equivalent of one to two employees) to start.

#### ***Penetration and Vulnerability Testing***

Vulnerability scans are \$700 to \$1,000 per perimeter scan. Depending on the value added by the provider, prices might drop as low as \$300 each.

Penetration testing pricing can vary greatly, depending on scope. Typical testing might include Internet penetration, dial-up penetration/war dialing, social engineering, denials of service, physical access, even to the point of stealing a laptop or breaking into a home system. It also depends on how deep the engagement goes — penetration testing is much like the game “capture the flag.” The ultimate goal is to get a hold of the company’s critical data. But some penetration tests are limited to penetrating a DMZ (demilitarized zone, see Glossary) Web server.

Penetration testing is best priced by matching the cost and effort a hacker might employ. The skillset of the testers is also very important — the same dollar value does not obtain the same result from different companies (or individuals within the same company). It might take an unskilled, junior hacker two days to compromise a system, while it only takes a skilled and talented hacker 15 minutes. The typical price ranges fall between \$20,000 and \$100,000 based on scope.

### ***Compliance Monitoring***

This type of monitoring is priced on a subscription model. It is not unusual for a customer to pay \$100,000 per physical location.

### **Selected Vendors for Each Category**

The following vendors are representative of the various categories of managed security services vendors.

#### ***On-Site Consulting***

**Guardent**, **Vigilinx** and **Netigy** are examples of vendors whose respective staffs have the experience, perspective and skill to design coherent security architectures. They are gifted in areas as diverse as security policy construction, business risk analysis, public key infrastructure (PKI) design and technical perimeter defense. Of these, Guardent runs the risk of becoming a “one-stop shop” — attempting to be all things to all people. Its lack of focus will be a challenge for its own growth and for its customers. To its credit, it seems to realize it has bitten off a large part of the MSS categories and is not expanding services irresponsibly. **IBM Global Services**, on the other hand, is a large, established consulting firm with tremendous expertise, but erratic delivery. Customers tell Giga that projects begin with very skilled, high-level consultants, but are maintained by junior consultants with limited experience. That is also common feedback regarding very large consulting firms like **PricewaterhouseCoopers** (PwC), **KPMG** and others. These few vendors mentioned are by no means the only competent security consultants, but their sheer breadth of expertise makes them excellent generalists.

#### ***Remote Perimeter Management***

This niche is a commodity. Small regional consulting firms, the Big Five, telcos and software vendors all offer nearly identical services: a managed firewall, perimeter network monitoring and an option for a managed VPN connection. They are priced the same, use the same products (**Check Point** Firewall-1 almost universally) and offer equivalent service-level agreements (SLAs). So how should you differentiate them? We use customer feedback and an assessment of technical security competence to evaluate the vendors. The big firms, like Vigilinx and Guardent, fulfill the requirements well and add other valuable services. But some vendors that specialize in the perimeter management rise to the top.

Unisys, **Genuity** and **Telenisus** are our picks for the most stable support infrastructures, best security skill and highest customer feedback rating. These are no-nonsense security providers whose practices are best limited to firewall and VPN management and one or two intrusion detection monitors near the firewall. Unisys was the first remote perimeter management provider to earn **ICSA.net**'s certification. And Telenisus is an example of a regional consulting firm successfully relaunched as a national service provider.

**Aventail** is a remote perimeter management vendor with a different model. Like Unisys, it rolls a secure rack onto your site and manages it remotely. But unlike others, Aventail includes a potpourri of other technologies on the same rack, including sophisticated VPNs, certificate handling, resource access control and network authentication. Essentially, with Aventail, a company may outsource its entire DMZ.

#### ***Product Resale***

Some vendors are chiefly interested in moving product. Software vendors, like **Internet Security Systems** (ISS) and **Network Associates**, wrap their products with added value services, such as monitoring, vulnerability assessments or security consulting.

Another unique offering in this category is Network Associates' **myCIO.com**. myCIO, using a variety of top-rated products, offers an application service provider (ASP)-like managed service, including virus management, firewall and VPN management, intrusion detection and vulnerability scans. myCIO.com uses only Network Associates products, including **McAfee** antivirus, **Gauntlet** firewall and VPN and **CyberCop** vulnerability scanner. **Global Crossing** resells its services.

ISS is commonly thought of as a leader in this category. It has security expertise to be sure, and it uses first-rate products, but customers report that working with ISS is like working with any software vendor; that is, it views services simply as another channel through which to move more merchandise — in this case, ISS RealSecure intrusion detection software.

As growth in sales of its RealSecure intrusion detection suite slowed in the last 18 months, ISS sought a new business model. It found it in one of its leading resellers. When it acquired **Netrex** in 1999, ISS launched its managed security service, offering a Check Point perimeter firewall and VPN services along with its own intrusion detection products. As with all product vendors turned service providers, the managed service is first and foremost a delivery channel for ISS products. A reseller relationship with **Dimension Data** gives the ISS service strong exposure in Europe, the Middle East and Africa (EMEA). ISS is a respected source for research on technical vulnerabilities.

### ***Managed Security Monitoring***

Founded by security guru Bruce Schneier, **Counterpane** is a focused and successful startup. Its entire business centers exclusively on one managed security category: managed security monitoring. All competitors try to improve the monitoring business model by offering products or on-site consulting, but only Counterpane is positioned to be a vendor-agnostic monitoring-focused service. Counterpane monitors its own direct customers, as well as the customers of its wholesale partners, notably PwC and Aventail. Counterpane's security associates program is an alliance between network product manufacturers, guaranteeing that Counterpane staff have the latest information related to the wide variety of systems they monitor. Its customers rely on Counterpane to monitor events not only at the network boundary, but also on application servers and network devices distributed throughout the corporate network. Their recent acquisition of Security Design International Inc. (SDI), a Virginia-based security consulting and services company that was a wholly-owned subsidiary of Cylink Corp., strengthens Counterpane's ability to analyze events and anticipate security problems.

**Veritect** is a company that is trying to be all things to all clients. Its marketing collateral makes claims of comprehensive security consulting, risk assessments, real-time monitoring, incident response, etc. From what we hear, Veritect is not as strong as it would lead you to believe. However, its parent company, **Veridian**, has deep pockets and extensive experience in IT infrastructure and planning. Therefore, Veritect is worth watching, though not currently recommended.

**Riptech** will claim that it competes with Counterpane in the MSM category and with Guardent as a one-stop shop. Our assessment is that it is neither. Instead, it is a remote perimeter management company with some added vulnerability assessment services. Its attempt to market itself too broadly ultimately will cause it to suffer.

There is still no vendor comparable to Counterpane in the sense that no other service provider is strictly focused on retail and wholesale managed security monitoring services. That lack of distraction is the key strength of Counterpane's business model and value to its customers. **Vigilix**, while not exclusively devoted to monitoring, appears to have the appropriate skills, national support infrastructure and commitment to provide quality monitoring services.

### ***Penetration and Vulnerability Testing***

**Foundstone**, **Guardent**, **Vigilix** and **Netigy** are all exceptional providers of penetration and vulnerability

testing. But that is not to take away from companies like Ripstech or ISS, which may meet all of your needs satisfactorily. The highest rated firms in this category have large customer bases distributed internationally and complement their services with educational or policy development products.

### ***Compliance Monitoring***

To date, this is a niche of one vendor. **TruSecure** offers a service for monitoring logs originating from your network. In that way, it is like Counterpane. But TruSecure is not looking for day-to-day security events and trends. It is watching for unauthorized changes to systems like firewalls, Web servers and application servers. In this way, TruSecure can report to you whenever your security implementation is out of compliance with your policies. Its literature mentions risk profiles, but it is limited to monitoring for changes in your “technical” risks, not business risks.

Guardent and Vigilix have language in their marketing collateral that indicates similar compliance monitoring. And Counterpane claims to be able to offer this service alongside its regular security monitoring. While each of these competitors may offer services that satisfy compliance monitoring requirements, none are as extensive and focused as TruSecure’s.

### **When Do You Use a Managed Security Service Provider?**

Kurt Ziegler is CEO of an e-business startup. He knew the value of security for his organization when he hired Ripstech to manage his perimeter. But he didn’t want to lose control of security. “I liked that I could have a personal relationship with the executives at Ripstech.” The small size of the company and its strong security competence were appealing to Mr. Ziegler.

He has one security manager on staff that manages outsourcing agreements and internal security issues like antivirus upgrades. So, he insists he did not outsource security. Regarding Ripstech, he says, “They are the administrators of *My* security policy.”

Security cannot be entirely outsourced. It is a concept that encompasses many processes within an organization, some of which must be performed by data owners and business managers. By identifying those processes, it is easy to see which categories of vendors can help you with which processes (see Table 1). IT staff and business leaders should work together to build a security posture based on basic processes.

Processes fundamental to a security posture are as follows:

- Security policy development and maintenance: This is the first step in building a security posture. It includes the benchmarking of the current state of technical security, security awareness and standard procedures. Business leaders should be surveyed with a questionnaire designed for identifying and assessing business risks — as opposed to technical risks (see Planning Assumption, [Optimal Extranet Security: A Methodology](#), Steve Hunt).
- Shoring up defenses: A vulnerability assessment of your organization will show glaring problems, such as bad passwords, patches and updates that are missing from servers, ports and services promiscuously open, non-hardened operating systems and unauthorized modems. Rather than paying some outside firm to tell you that these are your vulnerabilities (which they certainly will), spend your money fixing these obvious problems.
- Designing a comprehensive security architecture: Use the four A’s of Security (see Planning Assumption, [Recommendations for Secure E-Business](#), Steve Hunt) to build a security architecture based on the business risk assessment and security policy.
- Implementing policies, processes and technologies: Purchase and install the products and processes that allow you to administer and enforce the security policy (see Planning Assumption, [Securing the Extranet Web Application](#), Steve Hunt).
- Building an incident response (IR) posture: Do this with IR policies, procedures and properly

empowered and trained staff.

- Ongoing monitoring: This includes daily and periodic analysis of events and trends.
- Performing periodic vulnerability assessments: This includes weekly, quarterly or annual checks of certain systems and network segments for emerging vulnerabilities.
- Periodically reviewing and reassessing the quality of policy in light of the vulnerability assessments: Whenever you receive new information about your security posture, consider how it will affect policies, procedures and technical configurations.

**Table 1: Mapping Processes to Service Categories**

Security Process	Managed Service That Applies
Business risk assessment	On-site Consulting
“Level-setting” basic defenses	On-site Consulting
Designing a security architecture	On-site Consulting
Implementing technologies and processes	On-site Consulting Remote Perimeter Management Product Reseller (may require multiple vendors) Managed Security Monitoring
Building incident response posture	On-site Consulting Managed Security Monitoring
Ongoing monitoring	Managed Security Monitoring
Performing vulnerability assessments	Vulnerability Scanning Service Compliance Monitoring Managed Security Monitoring
Reviewing policy	On-site Consulting Compliance Monitoring

Source: Giga Information Group

## Alternative View

If the engagement of an outsourced security provider is truly tactical and temporary, there may not need to be an exhaustive mapping of business needs to the vendor’s strengths — simply select a reasonably competent, multicategory vendor and be done with it. Giga research shows that improper project management and poor cultural fits lead to unsuccessful outsourcing engagements. But that risk may be tolerable while meeting tactical, short-term needs.

## Findings & Recommendations

Outsourcing tactical security tasks is reasonable. The costs associated with security hardware and software are on the rise. Therefore, many companies may avoid the capital expenses by letting outside providers own some of the equipment. Good security staff are difficult to find, and most companies have not elected to train, develop and retain security expertise in-house. For those reasons, leveraging the skills and personnel of an outsourcing vendor is very appealing.

Security outsourcing should be performed tactically, and to some extent, temporarily, and only in accordance with standard security processes (see Planning Assumption, [Outsourcing Security: Strategic Build-or-Buy Recommendations](#), Steve Hunt). A company should engage a MSS provider only to meet identified business needs. For example, the existence of technical threats from Internet hackers may not be sufficient cause to

take remedial action. Technical vulnerabilities must be mitigated following an assessment of business risks, not merely technical risks (for more suggestions, see Planning Assumption, [Optimal Extranet Security: A Methodology](#), Steve Hunt).

Most of the vendors offering security services are technically competent to address technical risks, although many are oblivious to the business impact of their actions. Therefore, you should make sure the vendor you select fits in well with your corporate culture, provides technical services that closely match your business needs and with whom you feel you may develop a close, personal working relationship. Giga finds that when outsourced security services fail to meet business needs, it is very often signaled by the customer's personal or emotional reservations about the vendor's staff.

There are many security outsourcing vendors in the MSS market, but not too many. The number and variety of providers is appropriate to the market because both the size of a firm and its locality limit its success. That is, customers value personal relationships with their security services vendors. Therefore, the larger the vendor, the less chance it will ultimately satisfy the customer. Large firms cannot sustain that personalized value.

Some of the vendors mentioned in this Planning Assumption offer services in several or all of the MSS categories. When selecting a vendor, evaluate the degree to which the vendor meets the specific security process requirements. Just because the vendor is skilled at vulnerability assessments, for example, does not mean it is the right choice for remote perimeter management or managed security monitoring. Require the vendor to bid on meeting these specific business process needs, not merely on the services it prefers to provide. It is acceptable to mix and match vendors with different expertise or to contract separately with a single vendor for different categories of service.

### **Leading Vendors of Each Classification**

It is important to note that some vendors have focused their services are the two categories most directly related to outsource security "management." Those services, remote perimeter management and managed security monitoring, are the foundation services of companies like Vigilinx, Guardent and others. It can be argued that other categories are simply value-add services to complement these two "pure" managed services. Nevertheless, Giga recommends that your need for each category still be considered in light of the security processes listed in this Planning Assumption and not merely on the attractive value-added services a vendor may offer.

On-site consulting — Guardent, Netigy, Vigilinx, IBM Global Services and Big Five consulting firms in general. Consulting covers a tremendous range of activities, from business risk assessments, to architecture design, policy construction and systems integration. Be sure you identify your business needs and select the consultant best suited to those needs.

Remote perimeter management — Aventail, Unisys, Genuity, Guardent and Vigilinx. Managing a perimeter firewall and intrusion detection monitor is a common and not very challenging service. That is why nonsecurity-focused companies like Internet service providers (ISPs) can provide the service adequately. However, the security competence of a more specialized vendor will add value and confidence.

Product reseller — ISS, Network Associates and Telenisus. For commodities like perimeter intrusion detection monitors or perimeter firewalls, seek the reseller that offers complementary services for which you have already identified a need, such as firewalls plus periodic vulnerability scans, or firewalls plus monitoring.

Managed security monitoring — Counterpane and Vigilinx. Even if there were a company sharing Counterpane's model, and there seems not to be, there would still be a sufficient market for multiple vendors. Vigilinx is not focused on MSM, but appears to have a dedication to quality monitoring service and a national

support infrastructure.

Penetration and vulnerability testing — Foundstone, Guardent, Vigilinx and Netigy. Each of these firms brings strong value-added services to the category.

Compliance monitoring — TruSecure. Select TruSecure for a focused and comprehensive compliance monitoring service complemented by its proprietary TruSecure Site Certification. Turn to Vigilinx, Guardent or even Counterpane for limited compliance monitoring that may be satisfactory for your needs.

Click [here](#) to see Table 2: Categories and Vendor Ratings.

## References

### Related Giga Research

Planning Assumption, [Optimal Extranet Security: A Methodology](#), Steve Hunt

Planning Assumption, [Recommendations for Secure E-Business](#), Steve Hunt

Planning Assumption, [Outsourcing Security: Strategic Build-or-Buy Recommendations](#), Steve Hunt

Planning Assumption, [Authentication Is the First Step Toward Secure E-Business](#), Steve Hunt

Planning Assumption, [Securing the Extranet Web Application](#), Steve Hunt

Planning Assumption, [Establishing a Framework for Risk Management](#), Jon Erickson and Chip Gliedman

Planning Assumption, [Ensuring Outsourcing Success](#), Julie Giera

Planning Assumption, [Key Trends for 2001: IT Outsourcing](#), Julie Giera

Planning Assumption, [Service-Level Agreements in an Outsourcing/Service Provider Environment](#), Mike Dodd

Planning Assumption, [Outsourcing Supplier Selection — A Structured Approach to a Critical Purchasing Decision](#), Mike Dodd

IdeaByte, [The Four A's of Secure E-Business](#), Steve Hunt

IdeaByte, [Extranet Partners — Good Fences Make Good Neighbors](#), Phil Rosch

### Relevant Links and Other Sources

“Managing Managed Security,” Edmund DeJesus, Information Security, *Network Magazine*, January 2001

Salinas Group, [www.salinasgroup.com](http://www.salinasgroup.com)

Counterpane, [www.counterpane.com](http://www.counterpane.com)

METASes, [www.metases.com](http://www.metases.com)

Telenisus, [www.telenisus.com](http://www.telenisus.com)

Unisys, [www.unisys.com](http://www.unisys.com)

Foundstone, [www.foundstone.com](http://www.foundstone.com)

TrueSecure, [www.trusecure.com](http://www.trusecure.com) (formerly NCSA and ICSA.net)

Computer Associates, [www.ca.com](http://www.ca.com)

ISS, [www.iss.net](http://www.iss.net)

Ubizen, [www.ubizen.com](http://www.ubizen.com)

F-Secure, [www.f-secure.com](http://www.f-secure.com)

Symantec, [www.symantec.com](http://www.symantec.com) (Axent)

Nai, [www.nai.com](http://www.nai.com) (McAfee.com and MyCIO.com)

Genuity, [www.genuity.com](http://www.genuity.com)

AT&T, [www.att.com](http://www.att.com)

IBM Global Services, [www.ibm.com/services](http://www.ibm.com/services)

Sprint, [www.sprint.com](http://www.sprint.com)

UUNET, [www.uunet.com](http://www.uunet.com)

Savvis, [www.savvis.com](http://www.savvis.com)

Riptech, [www.riptidech.com](http://www.riptidech.com)

Pilot, [www.pilot.net](http://www.pilot.net)

Veritect, [www.veritect.com](http://www.veritect.com)

PresiNET, [www.presinet.com](http://www.presinet.com)

SecureWorks, [www.secureworks.com](http://www.secureworks.com)

Concentric Networks, [www.xo.com](http://www.xo.com)

VIGILANTe, [www.vigilante.com](http://www.vigilante.com)

Vigilinx, [www.vigilinx.com](http://www.vigilinx.com)

## Glossary

**DMZ** — Demilitarized zone. A networking expression denoting a segregated, semitrusted network where semitrusted external users may be granted limited access.

### Table 2: Categories and Vendor Ratings

This table shows the various categories of managed security services offered by each vendor, respectively. The Geography column denotes geographic strengths and customer demographics, if known. The Giga Value Rating indicates the degree to which the vendor offers comprehensive services for each category. The rating also reflects customer satisfaction reports we have collected. Evenly distributed national or international support will score more highly than regional.

Rating Key: 1-5 = not recommended; 6-7 = recommended in light of regional support or specific ability to meet a customer's specific requirements; 8-9 - highly recommended; 10 = best in category, strongly recommended in light of business needs.

Vendors	Categories	Geography/Customer Demographics	Comments	Rating
AT&T Solutions	Remote Perimeter Mgmt. Product Resale	National	Limited security expertise, but acceptable for firewall mgmt.	7
Aventail.net	Remote Perimeter Mgmt.	National/International; Dozens of very large customers	Unique service. Offers other related services that add value to its MSS offering. Nice diversity of products.	10
Counterpane	Managed Security Mon.	Strongest on West Coast. Several dozen customers mostly on West Coast, some in Midwest, East Coast, with a few outside N. America	Very focused security practice. Flexible business model positioned to sell directly, through channels and wholesale.	10
Digex	Remote Perimeter Mgmt.	International	Firewalls hosted off-site. Other hosting services add value.	8
Espira/NETSEC	On-Site Consulting	North Central and	Espira and NETSEC	7

	Remote Perimeter Mgmt. Product Resale	Southwest, becoming national	complement each other well.	
Evinci	Penetration/Vulnerability	Midwest strength	Beginning to remarket themselves nationally	7
Exodus	Remote Perimeter Mgmt.	International	Firewalls hosted off-site. Other hosting services add value	9
Fiderus	On-site Consulting Penetration/Vulnerability	National. Strongest on East Coast	Especially recommended for assistance with forensics	7
Foundstone	Penetration/Vulnerability	National	Focuses on training and policies. Complements other consulting services nicely.	9
Genuity	Remote Perimeter Mgmt. Product Resale	East Coast strength, otherwise well distributed nationally	Limited security expertise, but acceptable for firewall mgmt.	8
Guardent	On-Site Consulting Penetration / Vulnerability	National. 100+ customers.	Great technical skills. Acceptable customer satisfaction.	10
IBM Global Services	On Site Consulting Product Resale Penetration/Vulnerability	International. 1,000+ customers. Mostly Global 1000 and gov't.	Strong experience. High priced. Recommended as technical consultants	9
ISS.net	Remote Perimeter Mgmt. Product Resale	International	Known for an integrated intrusion detection suite of products.	8
METASeS	On-Site Consulting Remote Perimeter Mgmt. Product Resale	National	Leverages a close relationship with Meta Group	7
myCIO.com	Remote Perimeter Mgmt. Product Resale	National	An ASP model of related security services, including antivirus	7
Netigy	On-site Consulting Penetration/Vulnerability	National and Europe	Closest to providing true business risk assessments of any security-focused vendor	10
NetSolv	Remote Perimeter Mgmt.	National. Mostly small to midsize companies	Security is one part of the firm's network management business	8
Pilot Networks	Remote Perimeter Mgmt.	National	Prides itself on a secure hosting infrastructure, but suffers in customer satisfaction	5
Qualys	Penetration/Vulnerability	National	Too new to rate accurately	-
Riptech	Remote Perimeter Mgmt. Product Resale Managed Security Mon. Penetration/Vulnerability	Strongest in South. 100+ customers. 10+ in the Fortune 500.	Recommended for perimeter protection. Especially strong in vulnerability assessments. Its lack of focus works against it.	8
SalinasGroup	Remote Perimeter Mgmt. Product Resale	National	Very early provider of managed firewall services. Good variety of resale products.	8
Telenisus	Remote Perimeter Mgmt. Product Resale	Strongest in Midwest	Very good firewall and intrusion detection skillset	8
TruSecure	Compliance Monitoring	National, but strongest in the East. 400 customers, half in the Fortune 1000.	The only focused player in this category. Leverages a relationship with Gartner Group. Growing rapidly.	10
Unisys	Remote Perimeter Mgmt. Product Resale	National. Mostly US banks as customers/	Leverages access to 100s of technical specialists within Unisys	9
UUNET	Remote Perimeter Mgmt. Product Resale	National	Limited security expertise, but acceptable for firewall mgmt.	7
Ubizen	Remote Perimeter Mgmt.	Europe. Limited US and Asia presence.	A proprietary assortment of perimeter security products and solutions not unlike Aventail.	8
Veritect	On-site consulting	National, though	Subsidiary of Veridian, with	7

	Remote Perimeter Mgmt. Product Resale Managed Security Mon. Penetration/Vulnerability	strongest on East Coast.	roots in gov't contracting. Some reports of inadequate performance. Biting off more than it can chew.	
VIGILANTE	Penetration/Vulnerability	National	Repackages some best-of-breed technologies with additional services	7
Vigilinx	Remote Perimeter Mgmt. Penetration/Vulnerability Compliance monitoring	National, strongest in Northeast	Led by Bruce Murphy, former managing partner of PwC. Strong leadership, technical staff. ifSec and LogiKeep good, complementary acquisitions.	10
Note: National refers to United States. Some vendors serve clients in UK, Europe and Asia, but that is not noted unless Giga recognizes a particular strength of international support.				

Source: Giga Information Group