Security Services

	Included Services	Readiness Package	Site Certification Package	Safeguard Package
		$99.50/mo. or $995.00/yr.	**$1595/mo.***	**$5995/mo.***
Security	External Network Vulnerability Scan	✓	✓	✓
	Website Scan	✓	✓	✓
	Security Newsletter	✓	✓	✓
	Email Filtering	✓	✓	✓
	Services Performance Monitoring	✓	✓	✓
	Malware Scanning	✓	✓	✓
	Blacklist Monitoring	✓	✓	✓
	Network Traffic Monitoring	✓	✓	✓
	Internal Network Vulnerability Scan		✓	✓
	24x7 Hardware Monitoring			✓
Compliance	Security Consultation	✓	✓	✓
	PCI Compliance Form	✓	✓	✓
	Vulnerability Reports	✓	✓	✓
	Inventory Asset Report		✓	✓
	Client Document Portal		✓	✓
	Security Audit			✓
Management	Compliance Branding	✓	✓	✓
	Mobile Device Mgt.	✓	✓	✓
	Remediation		✓	✓
	Proactive Network Recommendations			✓

* The monthly price will be increased based on the number of devices being included in the monthly scans and monitoring solutions. Please refer to the Statement of Work for more detail.

Security Services

External Network Vulnerability Scan: IGI conducts scans and assessments to show which external (public) network IP addresses are responding to external exploits. The process consists of scanning the entire range of TCP and UDP ports for each IP address to identify all open ports and to fingerprint services, applications, versions, patch levels, and operating systems as well as gathering public information about your business.

Website Scan: Our WAS (Website Application Scanning) helps you truly reduce risks by finding the official and "unofficial" apps that may be hiding in your website. WAS is designed to reliably find true vulnerabilities such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF) and URL redirection – then prioritize them and focus on the issues that will have the most impact.

Security Newsletter: The IGI electronically distributed security newsletter is devoted to providing our clients with the latest breaches, security alerts and compliance updates.

Email Filtering: Every client will receive our redundant enterprise email security solution to block email-borne attacks while providing the extra features needed to ensure business continuity. This option provides real-time protection from spam and email based viruses while hiding your publicly facing mail server. This solution will increase network performance and staff efficiency by reducing the mass amount of unwanted email sent by spammers. Additionally, all email is temporarily stored allowing for mail to be redelivered as needed. **(Note: An additional fee may be applied to the monthly bill for each email address being scanned.)**

Services Performance Monitoring: IGI's unique all in one service alerting solution automatically helps our clients know when critical services are off-line. This 24x7 service monitors website uptime, website response time, server health, network uptime, and much more. You will now know if critical systems go off-line before your clients do. In short, be it external monitoring or internal monitoring, we've got your back!

Malware Scanning: Malware Detection Service (MDS) allows organizations to proactively scan their web sites for malware, providing automated alerts and in-depth reporting to enable prompt identification and resolution. MDS enables organizations to protect their customers from malware infections and safeguard their brand reputations. Organizations that use MDS on a scheduled basis will be able to quickly identify and eradicate malware that could infect their web site visitors and lead to loss of data and revenue.

Blacklist Monitoring: Email blacklists are a common way for email providers to reduce spam. If your mail server has been blacklisted, some email you send may not be delivered. IGI blacklist service checks your domain for blacklists, at a minimum, once every 7 days on 30 blacklist services so that your business can ensure that all of your email is accepted.

Security Services

Network Traffic Monitoring: Monitoring internet activities 24x7 is critical in protecting corporate networks from spyware, viruses, and adware. Additionally, managing internet usage has been proven to increase staff productivity. This real-time service is handled by IGI's virtual appliance that provides best-of-breed web filtering and internet protection. This solution provides visibility into web activity that lets our administrators create effective web policies which ensures networks maintain peak performance while enforcing that users act online in accord with corporate objectives. **(Note: An additional fee will be applied to the monthly bill for each network device being scanned.)**

Internal Network Vulnerability Scan: IGI's Network Vulnerability Scan tools are designed to discover all your on premise network devices and applications, including desktops, servers, operating systems, applications, routers, firewalls, PDAs, wireless devices, as well as many other network elements. Then the system rapidly identifies, visualizes and organizes your network assets into Business Units and Asset Groups. Define your "mission critical" assets by their importance to your business operations using a 5 tier rating system from Low to Critical. This information is then compiled and easy-to-read reports are generated that provide both executive-level summaries and detailed technical analysis. **(Note: An additional fee will be applied to the monthly bill for each network device being scanned.)**

24x7 Hardware Monitoring: The IGI Cloud monitoring system monitors your critical network device(s) around the clock to ensure your maximum uptime. This solution will analyze memory dumps, performance issues and operating systems or application configurations to ensure your infrastructure remains healthy and optimized for performance. These fully customizable alerts will be delivered to the responsible party by way of emails, phone calls or text messages in order to keep you aware of any critical service issues. **(Note: An additional fee will be applied to the monthly bill for each network device being monitored.)**

Security Consultation: Every client will receive a security consultation consisting of specifically designed questions in order to provide remediation activities and prioritized steps in order to meet your security requirements.

PCI Compliance Form: The PCI DSS Self-Assessment Questionnaire (SAQ) is a validation tool for merchants and service providers that accept credit card payments. The purpose of the SAQ is to assist organizations in self-evaluating compliance with the PCI DSS, and is usually required by your credit card processor or bank. All IGI security clients will receive a SAQ with the required compliance sections completed.

Vulnerability Reports: IGI utilizes enterprise level security scanning tools providing comprehensive reports which will be provided to every client. These reports can be very overwhelming which is why your IGI SSC will review your report with an appointed staff member to ensure your business benefits from the included information. Your SSC will then guide your company through the appropriate remediation steps as needed.

Inventory Asset Report: Clients who receive the Inventory Asset Report will also receive a network topology diagram for their domain or network block. Utilizing these map reports will allow businesses to compare historical and current maps to obtain trend analysis and identify hosts that have been added or removed from the network.

Security Services

Client Document Portal: Eligible clients who receive this feature will never need to worry about where their security documents are located. In the event of a breech or security audit, your staff will be able to retrieve all the documents needed in minutes. This cloud based portal is highly available and backed up on a nightly basis to ensure your information is secure and available.

Security Audit: Each customer will receive an IGI Senior Security Consultant (SSC) in order to perform regulatory reviews in an effort to comply with appropriate security standards. Your IGI SSC will interview key personnel focusing on a variety of security areas including Security Policies and Standards, Vulnerability Management, User Access Management, Business Continuity and Disaster Recovery, Regulatory and Compliance Framework, Network and Infrastructure Management, Physical Security, and Human Resources Controls. Then your IGI SSC will provide recommended security modules needed in order to achieve compliance.

Compliance Branding: Every IGI Security Compliance Customer will receive a certification and a digital logo which can be proudly displayed on marketing material, corporate website, business cards, etc. in order to demonstrate your business's commitment and compliance to digital security.

Mobile Device Management: Uncompromising mobile device management with features that include antivirus protection, secure web browsing, lost device protection, call / sms blocking, GPS tacking and more. This client based application can be installed on laptops, smart phones or iPads. This centrally managed enterprise solution is designed to help small and large companies control multiple endpoints from one easy to use dashboard. Up to 4 devices can be supported with a single user license. **(Note: An additional fee will be applied to the monthly bill for each network device being monitored.)**

Remediation: Eligible Clients will receive remediation consulting services by certified IGI security engineers as part of their monthly contract. The average hourly billing rate for a security engineer can vary from $100 to $500/hr. Our IGI clients will enjoy knowing that they are receiving the best remediation engineers at a low fixed monthly fee. Your Statement of Work agreement will describe this in more detail.

Proactive Network Recommendations: Do you have a large network infrastructure and don't know where to focus your energy or resources to achieve network security? Then you'll really benefit from our unique network security visualization tool. This highly sophisticated cloud software application will allow your company to visually see your critical network components graphically with active and potential vulnerabilities. Using this tool will allow IGI and your network administrators to examine "what if" scenarios while re-using existing network devices. These proactive network recommendations can now be easily implemented and managed to ensure a more secure environment in less time.