Feature	Free	Express	Lite	Full	Description
Staff, Manager and Owner Training Modules	X	X	X	X	IGA and MDT will collaborate to produce training materials specific to this program that all IGA Merchants would have access to as part of the base program. These materials will be targeted to specific groups with the suggestion being general staff, managers and finally owners as each will have specific aspects that require their attention.
Security Best Practices Guide	X	X	X	X	This would be a take-away that every IGA Member would receive whether they took the next steps or not. Our goal is for this to be a simple handout "card" that has the top 5 to 10 items that a merchant can and should focus on to protect themselves from cyber risks including ransomware attacks.
Security Best Practices Assessment	X	X	X	X	The merchant can request a biannual security best practices assessment. During this process, the MDTech Security Team will review the merchant's processes and systems against security best practices and make recommendations.
Managed Endpoint Protection w/Anti-Virus	O	O	X	X	Solid endpoint protection with anti-virus is the merchant's last line of defense against an intrusion such as a ransomware attack. Our managed endpoint protection is an enforced solution ensuring that end-users cannot disable it and is monitored for proper configuration and malware activity. The "Lite" and "Full" packages include 2 licenses to protect the POS equipment with additional licenses available for purchase as needed. This is available as a stand-alone offering meaning anybody can subscribe to this service regardless of whether they have a managed network.
Incident Response Management	O	O	X	X	In the unlikely event of a cyber incident, MDTech's Security Team will activate our Incident Response Plan (IRP) on behalf of the merchant to manage the event and coordinate the merchant's response. This is included at no charge for merchants with a MDTech Managed Firewall in place and is optionally available to others starting at $5,000 per incident.
Advantage Comprehensive Breach Indemnity	O	O	O	X	Breach indemnity provides an extra layer of coverage for merchants against data incidents and ransomware attacks. This program provides $100,000 in breach indemnity coverage in the event of breach regardless of fault.
Policies and Procedures Templates		X	X	X	Merchants should implement policies and procedures related to their operations and IT practices. These templates can be customized by the merchant to create a secure environment both operationally and technically for their business. Some standards and regulations such as PCI-DSS, HIPAA and PII laws require these to be implemented.
PCI-DSS SAQ Assistance and Filing		X	X	X	For merchants that must submit PCI-DSS related documents such as their annual SAQ and/or scan results, MDTech will assist the merchant with document completion as well as submitting the documents to the merchant's acquiring banks and/or card brands as necessary.

Management Portal Access		X	X	X	The merchant can access the management portal anytime to initiate scans, verify scan status, retrieve scan reports, check network uptime and access other resources.
External Network Vulnerability Scans		X	X	X	The merchant's network perimeter begins at the device that separates their private network form the public Internet. It is crucial for the merchant to monitor this connection to ensure that it is secure and that no unexpected changes have taken place. Unfortunately, many well intentioned attempts to increase security have resulted in significant security holes exposing the merchant's private network. One example is a merchant adding a camera/DVR system to increase their visibility into the location. However, unknown to the merchant, some of these devices have weaknesses that would allow an Internet attacker easy access the merchant's private network. These scans monitor the merchant's public network at least quarterly looking for insecure devices and any changes that may have occurred allowing the merchant and their vendors to take action before an incident occurs.
Internal Network Vulnerability Scans			X	X	These scans inspect a merchant's critical systems from the inside as if an intruder has already gained access to the private network as would be the case once malware or ransomware was installed on a system. These scans are designed to detect security issues such as vulnerable operating systems, missing Windows Updates, critical patches that haven't been installed, system misconfigurations and other vulnerabilities that could allow an intruder exploit and compromise a system.
Managed Firewall with IDP/IPS			X	X	A commercial-grade managed firewall provides a secure and monitored border between the merchant's private network and the public Internet. The firewall inspects traffic providing intrusion detection and prevention to block potentially harmful traffic from entering the merchant's network.
Comprehensive Managed Network Solution			X	X	MDTech will manage or co-manage (as applicable) the internal network providing additional technology resources to the merchant. In cases where the merchant utilizes other MDTech solutions such as managed switches and access points, MDTech can provide end-to-end, single-contact network management greatly streamlining the support process.
24x7 Network and Emergency Support			X	X	The MDTech Support Team is available on a 24x7 basis for network and emergency support of the merchant's network. In many cases, smaller/independent merchants use our support team as their own in-house IT to coordinate with other vendors on projects or to resolve general support issues.
Quarterly Status Report(s)			X	X	The merchant will receive quarterly reports showing their security status as well as a simple/pass fail status for key components. The MDTech Support Team will assist the merchant and/or their other vendors with remediating any issues that are detected.

Secure Remote Access Accounts with Multi-Factor Authentication			X	X	Many merchants have a need to securely connect to their network remotely. Merchant's with a MDTech Managed Firewall can setup SSL-VPN remote access accounts providing secure, multi-factor remote access to the network. These are often used by owners, managers, other vendors, accountants, etc. to connect to the store remotely.
SD-WAN Site-to-Site Network			X	X	For merchants with more than one location and/or a corporate office, the SD-WAN solution allows a secure network to be established between locations. This can be used for internal communications such as file transfers, remote system access, price file updates, time clocks, domain computer management, etc.
NetGuard Internet Backup			O	X	Stable and reliable Internet access is more important than ever for merchants as every day more of their systems rely on Internet connectivity to properly function. This need has grown far beyond payment processing and can impact nearly aspect of the store from HR to checkout flow to product ordering and more. NetGuard provides a full-time cellular backup connection that automatically fails over in the event that the merchant's primary Internet connection fails. This avoids costly downtime and frustration for both the merchant and their customers.
Ransomware Advanced Capture Protection			O	X	The Capture ATP service runs on the managed firewall and provides advanced detection capabilities to protect against zero-day threats such as ransomware. This works by scanning for a broad range of file types and analyzing potentially suspicious files in a sandbox environment forcing malware to reveal its true intent in a secure environment. Detected malware is blocked before it can even enter the network thereby protecting the merchant from the threat.
High-Performance Firewall			O	X	The high-performance firewall option has double the firewall inspection throughput of the standard firewall and is great for merchants with high-speed Internet connections faster than ~100-200 Mbps.
Fully Segmented Network with PCI & PII Protection			O	X	Network segmentation is an important element to protecting the merchant's mission critical systems. A segmented network breaks up a merchant's network into different segments based on function and sensitivity. For example, in a segmented network, the POS computers, manager computers and WIFI would each be broken out into a separate network. All traffic between the segmented networks would be monitored and controlled by the firewall. This configuration vastly improves security and mitigates the risk that an infection on a more vulnerable system such as a manager computer can jump to a more sensitive computer such as the POS Server. Systems that are mission critical, sensitive or that handle or store protected information such that covered by PCI, HIPAA or PII should be segmented.