PCI-DSS COMPLIANCE MATRIX

Build And Maintain A Secure Network And Systems	Safe-T
Install and maintain firewall configuration to protect cardholder data	* Supports logical segmentation by closing incoming firewall ports * Solutions can be placed within the LAN without exposing it to the DMZ
Do not use vendor-supplied system passwords or other default security parameters	* Default accounts can be removed from Safe-T solutions
Protect Cardholder Data	
Protect stored cardholder data	* Supports encryption for data both at-rest and in-transit * Safe-T solutions do not store any cardholder data
Encrypt transmission of cardholder data across open, public networks	*Data exchange solution provides full auditing of all data exchange flows *Supports encryption for data both at-rest and in-transit
Maintain A Vulnerability Management Program	
Use and regularly update anti-virus software on all systems commonly affected by malware	N/A
Develop and maintain secure systems and applications	*Solutions are continuously patched and go through penetration testing

Implement Strong Access Control Measures	Safe-T
Restrict access to cardholder data by business need-to-know	* Supports RBAC permissions * Access level for employees starts at lowest level
Assign a unique ID to each person with computer access	* MFA-supported * Assigns unique IDs to all users * Tests user access privileges * Monitors user accounts when not in use * Blocks user IDs after three failed attempts * Supports regular reset and strong composition of as well as credential encryption * Implements multi-factor authentication
Restrict physical access to cardholder data	* Creates user authorization and access controls to ensure identification
Regularly Monitor And Test Networks	
Track and monitor all access to network resources and cardholder data	* Implements audit trails for all systems * Tracks all activity, login attempts, account changes and pauses in the audit trail * Supports audit logging * Keeps all audit logs for at least a year with the last three months available for analysis * Prevents audit trail tampering
Regularly test security systems and processes	* Safe-T performs regular pen tests on all solutions
Maintain An Information Security Policy	
Maintain a policy that addresses information security	N/A