LEESHANOK
network SOLUTIONS

Basic Cybersecurity The growth and sophistication of cybercriminals, ransomware and hacker attacks continues to grow. The risk is too high for any business to not have these minimum viable security layers.	**Minimum Viable Security**
8x5 Network Operations Center Basic Monitoring and Remediation	
Patch Management Perform routine security patching	
Antivirus/Antimalware XDR Endpoint protection with extensive logging, tracing of threat management between endpoint devices and cloud applications	
Network Web Content Filtering Block malicious domains, links and web content on the network	
DNS protection for mobile devices Block malicious domains, links and web content on mobile devices	
Company Managed Password Manager Store and manage passwords securely within a secure encrypted database, not in Excel documents or auto-saved in web browsers	
Multi-Factor Security (MFA) with Microsoft/Google OTP Authentication method that requires the user to provide two or more verification factors.	
Dark Web Monitoring Monitor for exposed and compromised credentials for your company	
Annual External Vulnerability Scanning Perform scans to detect vulnerabilities within hardware and software	
SaaS protection for Microsoft 365 or Google Backups for Cloud services	
Business Continuity Disaster Recovery (BCDR)/Offsite backup Backup solution for on-premise servers	

Zero Trust Security Application allow-listing only allows approved applications to run on workstations	
Annual Security Awareness Training Annual user education on security awareness	
Monthly Managed Security Awareness Program Train, Phish, Analyze. Continuously educate your users to become a stronger human firewall.	
Cybersecurity Best Practices Disable auto-saving of passwords in web browsers. Users operating computers without administrator permissions	