For Project BUGBOX:

Full Network Security Evaluation: The ability to assess local systems or networks for any breaches, including identifying unauthorized remote access to surveillance systems.

Device Scanning: Capability to scan for unknown or undetected devices at the victim's location that could pose a risk.

Real-Time Alerts: Immediate notifications for any suspicious activity detected.

Data Encryption: Ensuring all data within the app is encrypted for security.

Remote Access Block: The ability to block unauthorized remote access attempts in real-time.

Incident Logging: Detailed logs of all incidents for review and analysis.

User Authorization: Strict user authentication processes, including biometric authentication, to ensure only authorized personnel can access the app.

Behavioral Analysis: AI-driven analysis to detect unusual patterns in network traffic or device behavior.

Counter-Surveillance Measures: Features to identify and disable unauthorized surveillance devices.

Decoy Networks: Creation of virtual decoy networks to mislead potential intruders.

Automated Threat Response: An automated system that can take immediate action against detected threats.

Deep Scan Capabilities: Technology to penetrate through standard security measures to uncover hidden devices or software.

Honeypot Traps: Setting up honeypots within the network to attract and trap hackers.

AI-Powered Encryption Breaking: For extreme cases, an AI module capable of breaking through encryption barriers.

Stealth Mode Operations: Ensuring that the app can operate undetectably.

Leave Behind Device/System: A device or system left at the client's location post-evaluation for ongoing monitoring and alerting GrizzlyMedicine upon future unauthorized access attempts.